Debevoise & Plimpton

Cybersecurity Desk Guide for Counsel



Foreword

Compared to other areas of business risk, the rapid rise of cybersecurity as a key business priority has been unprecedented. As the risks and regulations surrounding cybersecurity continue to evolve, so does the role of counsel.

Just ten years ago, legal departments were fortunate if they had a dedicated privacy counsel, and a dedicated "cybersecurity counsel" was virtually non-existent. There were very few regulations covering cybersecurity, and even those were high-level.

Today, new cybersecurity specific laws and the expectations around "reasonable security" borne out from litigation and enforcement actions have greatly changed the relationship between the legal function and information security teams. Many organizations have a dedicated cyber lawyer, and highly regulated companies may even have a team of cyber lawyers. In contrast, others rely on privacy or regulatory counsel to cover cyber, and even smaller legal departments may leave it to one of the generalists.

Though counsel have an increasingly important role to play here, cybersecurity can often feel like an impenetrable subject. It is a vast, fast paced, and quickly developing area that combines legal analysis, risk and compliance. It can be highly technical, and has increasingly serious consequences for getting it wrong.

Unsurprisingly, we are therefore often asked by clients: But what does cybersecurity involve? Where should I start? Who should I work with? And what should I look out for?

This guide is meant to serve as a desk reference for counsel on the many facets in which the legal department could engage in the cybersecurity function. Whether it is a small legal department without a dedicated cyber counsel or larger department with dedicated counsel, we hope this serves as a helpful guide.

Please reach out to us if you would like to discuss any of these topics in more detail.

Debevoise Data Strategy & Security Team

© 2023 Debevoise & Plimpton LLP. All Rights Reserved.

Debevoise & Plimpton LLP is offering this guide for informational purposes only. The guide is not intended nor is it to be used as a substitute for legal advice. This publication is neither a solicitation nor an offer to represent you. The information provided to you in the guide is not intended to create and does not create an attorney-client relationship with Debevoise or with any lawyer at Debevoise. You may inquire about legal representation by contacting the appropriate person at Debevoise.

Index

Compliance & Governance

1. Compliance with the legal landscape 1
2. Security technology counseling: cybersecurity by design 2
3. Managing the relationship between InfoSec and Inhouse Counsel 5
4. Managing the relationship between Board and Inhouse Counsel 7
5. Cybersecurity training & awareness 10
6. Data minimization & hygiene 12
7. Insider risks 14
8. Managing the relationship between Privacy and Inhouse Counsel 17

Incident Response

9. Incident response: preparation and vendor engagement 20
10. Incident response: during an incident 23
11. Incident response: post incident / lessons learned 26

Partnerships

12. External engagement: law enforcement, regulators, trade groups 29
13. Cybersecurity insurance 31
14. Bug bounty & vulnerability disclosure 33
15. Third party risk management 36
16. Diligence, corporate transactions & integration 37

Other Topics

17. Other topics of interest 40

1. Compliance with the Legal Landscape

While counsel is a *legal* role, it often requires substantial compliance work, including tracking, understanding and implementing changes required by new laws and regulations. Unlike lawyers who deal with a settled body of law, like the Employee Retirement Income Security Act ("ERISA"), lawyers working in cyber law must respond to a legal landscape that is constantly in flux and developing in tandem with the proliferation of new technologies. Additionally, many organizations have not yet staffed a cybersecurity subject matter expert on the compliance team. As a result, counsel with responsibilities for managing cyber-related legal risk should be constantly monitoring for potentially relevant new developments and compliance obligations.

Traditional Compliance & Mapping

Just a few years ago, there was no true cyber regulation to "comply" with. But regulations such as NYDFS's Part 500 changed that. Now there are numerous regulations with elements that require certifications to regulations. Part 500, for example, requires Covered Entities to sign a yearly certification. Other states have similar rules. Somebody needs to monitor these laws and track compliance with them.

On a broader scale, when new regulations are promulgated, it might be helpful for counsel to spend time with their team to map the regulatory requirements back to the company's existing information security controls. Such mapping can be critical in developing a roadmap for future improvements and in senior management briefings. Consider using the Cyber Risk Institute's free Cyber Profile tool to simplify this mapping exercise, with much of the work already done by the Institute.

Finally, compliance testing in the cyber realm is important. The SEC has issued orders against broker dealers for failing to have multi-factor authentication rolled out across an organization.

Monitoring Legal & Regulatory Developments

Monitoring the development of new laws can seem tedious or overwhelming. We suggest subscribing to blogs – like the Debevoise Data Blog – and news outlets like Law360 and Bloomberg Law to make this a streamlined process. Other legal resources are increasingly covering cyber, including the IAPP's newsfeed, and notifications from paid services.

Cross Department Collaboration

Beyond mapping, it helps to hold frequent cross-functional team meetings to understand how other departments interact with cyber-related content. Based on what counsel learns in these meetings, they might consider creating new policies and procedures to ensure consistency and alignment company-wide.

It may also be helpful to think of the counsel role as one of "connector." Not only is counsel the binding force between disparate teams as they deal with cyber issues. counsel will also be the point of contact for external engagement. *See Chapter 12 on External Engagement.*

2. Security Technology Counseling: Cybersecurity by Design

The President's National Cybersecurity Strategy calls for a fundamental shift in liability for software vulnerabilities. Whether adopted or not, the perspective is important: security by design is top of mind to the government and regulators. Security technology counseling goes beyond a typical "legal role." This is more "legal adjacent," as it calls on the counsel's role to bring the lens of information security regulations and jurisprudence to new issues relating to new technology. This will require partnering with Risk, Compliance, and many other teams in order to (i) evaluate product security, (ii) design new product/service offerings, (iii) determine the ramifications of certain features, and (iv) implement user security initiatives.

Security by Design

Security by design means that safety is at the forefront when a new product or service is designed. This means that companies take greater responsibility for the security outcomes produced by their offerings rather than leaving it to the end users to fend for themselves. Certain regulations explicitly have security-by-design call outs.

COPPA – FTC regulations implementing the Children's Online Privacy Protection Act ("COPPA") require that certain privacy and security to be addressed for products that collect data from children.

NIST Framework – The National Institute of Standards and Technology ("NIST"), created a Framework, which outlines best practices for reducing cybersecurity risks and has become the standard for assessing cybersecurity maturity for organizations of all sizes. While adherence is voluntary for most organizations, regulators, insurers and policymakers have looked to the Framework as one of the ways to assess whether an organization has implemented reasonable security.

UK/NCSC Principles – Companies that have products with international scope might benefit from reviewing the secure design principles promulgated by the National Cyber Security Center.

U.S. National Cybersecurity Strategy – The strategy calls for a shifting of liability for software products and services to companies that specialize in these areas in order to promote secure development practices. This means that software companies will need to balance the tradeoffs between innovation and security, noting that they can no longer disclaim away software vulnerabilities.

Where to Get Involved

Counsel should understand the basic security offerings of the technology products and services that the company offers, and the networks on which the products run, in order to advise on the associated legal and regulatory risks.

Technologies to Consider – Getting involved begins with new software under development. But counsel should consider how security features can be added to existing products. These technologies include, but are not limited to, technologies that protect data and additional measures, like MFA, software updates, and

password security products, as well as products that are wholly dependent on secure networks, like Internet of Things ("IoT") and non-local data products/storage (*i.e.*, Software as a Service products). Moreover, counsel must understand how to configure the technologies so that they pass regulatory scrutiny. For example, be aware of which factors would meet regulatory approval for an MFA program, and which factors might not (*i.e.*, some companies do not think that social security numbers are suitable for MFA after so many breaches have made exposure of such numbers commonplace).

Cloud Products – As more companies look towards cloud-based solutions, it is important to understand the risks associated with a shared (*i.e.*, public) cloud solution, as opposed to a private cloud arrangement (*i.e.*, wholly owned by one entity). While migration to the cloud might enhance the business's access and collaboration opportunities, cloud storage is not infallible and its security requires exacting attention. Yet it still may be more secure than some on-premises applications. When contracting with a cloud provider, clearly delineate the amount of responsibility they will have for securing your data, and how much responsibility will remain with you. Last, even where risk is allocated contractually, consider the need to audit or otherwise ensure counterparty compliance with contractual expectations.

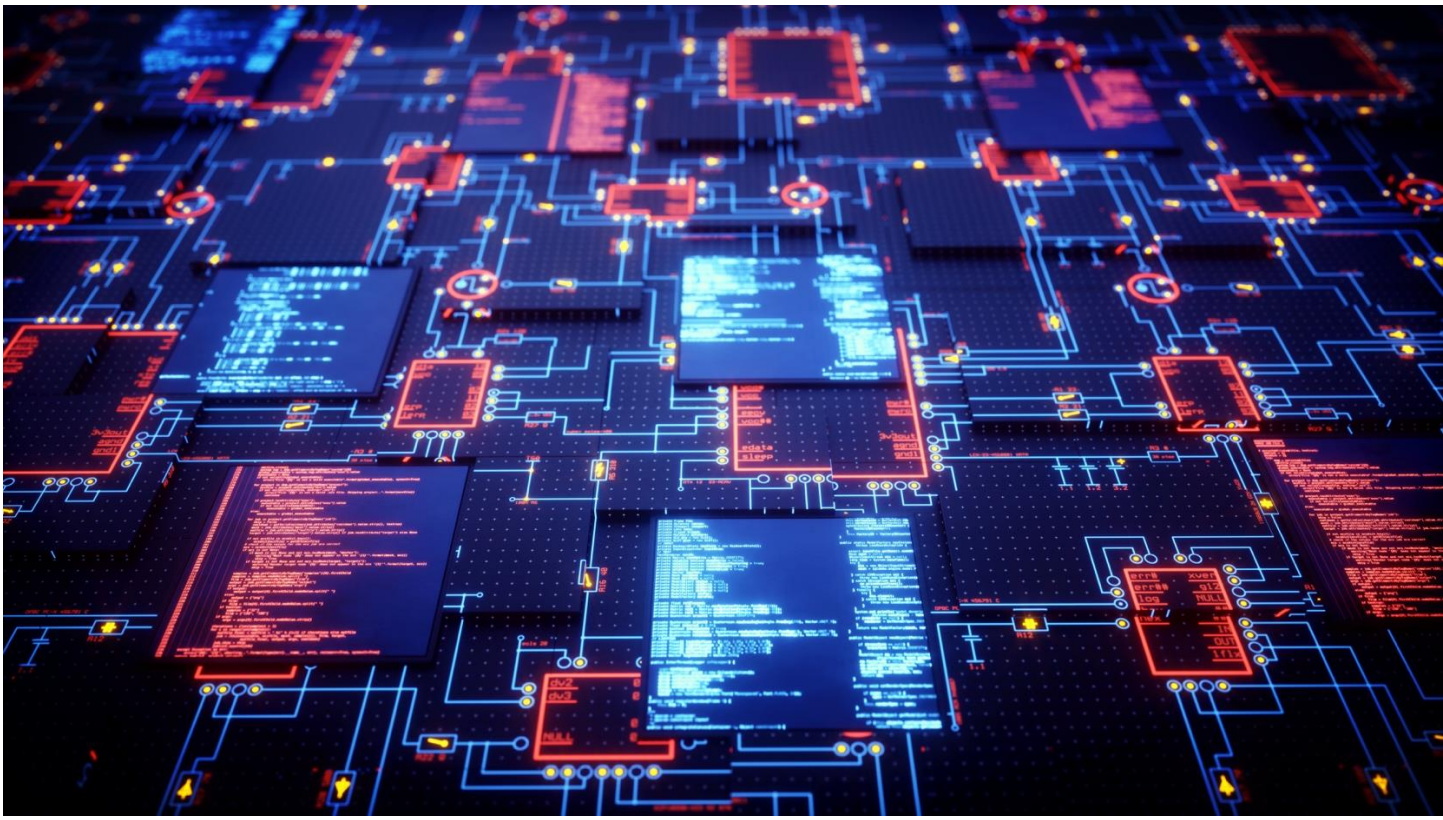
Ramifications of New Features – All new features have the potential to weaken the security of the product. Moreover, products/services that ask for personally identifiable information ("PII") need to be treated with additional scrutiny given the increase in state and international data protection laws. counsel should consider joining the product team's road-mapping exercises so there is full transparency and collaboration as new features are developed. While this is not a traditional "legal" skillset, counsel should also consider offering suggestions of features that carry less risk, are more "secure" and privacy friendly, and are more compliant with existing regulations.

Collaboration with InfoSec and Privacy Counsel

Most security technology counseling will also occur with frequent, specific input from InfoSec, from an IT angle, and privacy counsel, to ensure that security and privacy are in alignment regarding end goals. Because security technology counseling is such a large multi-stakeholder affair, it is important that these conversations happen at a regular cadence, rather than waiting for a new feature, technology, account creation process etc. to be implemented. Counsel should ideally be acting from a proactive stance to avoid future regulatory action. If a technology or development committee exists, joining the committee and reviewing the roadmap would be helpful.

Key Security Technology Questions for Counsel to Ask

1. What will the end product/service look like?
2. What are the features of this product or update? How does it operate?
3. Who is the target audience (*i.e.*, children)?
4. What is the worst-case scenario if it turns out the product can be breached by hackers?
5. What type of data are you collecting (*i.e.*, PII)? Why? How are you using and securing that data?
6. What security by design initiatives have you implemented?
7. What are the risks with this product or update? Can they be mitigated?
8. Where will this product be deployed?
9. How frequently do you envision rolling out software updates, or the equivalent?



3. Managing the Relationship Between InfoSec and Counsel

When it comes to managing cybersecurity risk, counsel can serve as true partners to the information security team, integrated with them and even sitting with the Securities Operations Center. Counsel in this capacity may have a function outside of legal role, opining on risk, governance and many of the other issues in this Handbook. Sometimes the model is different, with counsel serving solely as advisers on legal issues. In either model, and those in between, a strong and dynamic partnership between these two roles is key to maintain the entity's security.

> *"As cybersecurity leaders, we have to create our message of influence because security is a culture and you need the business to take place and be part of that security culture."*
>
> *— Britney Hommertzheim, Director, Information Security, AMC Theatres, at SecureWorld Kansas City*

Practice Tips on InfoSec Relationship Management

The Relationship Is Not Limited to Incident Response or Pure Legal Advice – Counsel and the InfoSec teams should coordinate on a range of cybersecurity-related matters, not just incident response, though the role they play in relation to each of those matters may differ. For example, the InfoSec team might be involved in contractual negotiations with customers and vendors in order to help answer questions about, or ensure compliance with contractual clauses regarding, the company's information security procedures or its data uses.

Know What InfoSec Is Seeing – As counsel, you naturally will be somewhat removed from the day-to-day operations of the InfoSec team. However, it is still important to have a high-level understanding of the company's security technology and practices. Take the time to learn about the technical infrastructure your company has in place, and what issues the InfoSec team are seeing on the ground. It is also worth noting how the team responds to the myriad of different circumstances presented to them each day. This will help you to understand the cybersecurity issues the company faces and assess the legal risks accordingly.

Know When InfoSec Has Something Big – An effective counsel/InfoSec relationship is underpinned by effective communication. By maintaining a healthy relationship with the InfoSec team, the counsel should be aware of when they are dealing with something big. Having this type of judgement is very much dependent on the counsel's insight into InfoSec's day-to-day and the strength of their relationship.

Sit In on InfoSec Staff Meetings – By sitting in on these staff meetings, you can learn and provide helpful knowledge to the entire security team.

- Learn about what technologies are being implemented, where these technologies may have shortcomings, and provide insight into the company's overall level of risk tolerance. When asked about compliance with regulations, you'll have first-hand knowledge of the types of technologies, and their attendant risk levels, that the company is using.

- Provide relevant updates to the security team, particularly on regulatory and law enforcement actions in the security space. Solicit their input on how the company should respond to new regulations or guidance.

Have Clear Allocation of Responsibility between Teams – Many cybersecurity laws and regulations are becoming steadily more prescriptive in nature, meaning that cybersecurity compliance efforts that were previously overseen by the InfoSec team may now require assistance from counsel. You should continue to assess how workstreams are divided between the two teams in accordance with current requirements, while being mindful that ultimately everyone is working toward the same goal: to reduce the company's cybersecurity risks.

Best Practices

1. Sit in on InfoSec Staff meetings.
2. Review reports by the SOC about incidents.
3. Join the CISO or others in the security organization in meeting with the FBI or other law enforcement.
4. Review risk assessments, SOC-2 reports and other briefings provided by the InfoSec team.



4. Interacting with the Board of Directors

CISOs have been providing cybersecurity briefings to the board for years, or at least to the audit or risk committees. These briefings were helpful for the board to fulfill its obligations to oversee risks to the enterprise, but they were not technically required.

In 2017, NYDFS passed Part 500, which included a requirement of board reporting. Even for those not regulated by NYDFS, the wave of regulations upped the ante on what "reasonable security" consists of, and it certainly consists of board updates. Sometimes counsel joins, but even without joining for the briefing, having counsel check compliance with regulatory expectations is critical.

Topics About Which the Board Should Be Apprised

Counsel may be tasked with contributing to or reviewing materials related to cybersecurity that are circulated to the board. In doing so, it may help for counsel to consider the scope and breadth of topics covered in these materials, as well as whether they are presented in a manner that will best facilitate the board's review.

Topics related to cybersecurity that counsel may want the board materials to cover include:

Cyber Incidents – The vast majority of cybersecurity incidents at a company will not rise to a level that requires briefing to the board, let alone real-time involvement by the board. There are some incidents, however, that can be sufficiently material or significant so as to merit board notification and briefing. The triggers for board notification will vary (at times significantly) by company, and will likely be the product of iterative discussions with the board and senior leadership. Where the board is notified, Risk and Legal should offer an appropriate cadence and means for providing continued updates, while being mindful also that information shared with the board should be vetted carefully and handled in a way to maximize the basis for asserting or maintaining attorney client privilege or work-product protection. Having a plan in place that outlines board notification in cyber incidents will be very helpful to an organization.

With respect to routine incidents that do not rise to a level requiring real-time involvement, the board may still benefit from periodic (*e.g.*, quarterly, annually, or semi-annually, depending on the circumstances) reporting of summary information regarding lesser incidents in order to facilitate their oversight of the company's security risks and of the effectiveness of management's approach. counsel should review any descriptions of the incidents to ensure accuracy, and appropriate phrasing and level of detail.

Current Cybersecurity Risks and Mitigation Measures – Boards should receive information regarding the unique cybersecurity risks faced by a company, as well as regarding the measures currently in place at the company to mitigate or address those risks. Topics to consider for periodic updating include: details regarding changes in the industry-specific threat landscape, how employees are trained to respond to incidents, the frequency with which cyber-prevention methods are tested, and any ongoing risk mitigation plans. These materials could serve as road maps for plaintiffs in a post-breach lawsuit, and counsel should ensure the descriptions are clear and to the point.

The Regulatory Landscape

Major regulators like the SEC, FTC and NYDFS have demonstrated an interest in elevating responsibility and accountability for the effectiveness of corporate cybersecurity programs, including by proposing or adopting measures to increase board involvement and liability for cybersecurity risks.

SEC Issuer Cybersecurity Rules

Will require public companies to identify:

- Who, whether it be the entire board or a subcommittee, is responsible for cyber risk oversight;
- How the board is informed of cyber risks and the frequency of these briefings; and
- How the board oversees the assessment and management of risks posed by cybersecurity threats.

NYDFS Cybersecurity Requirements for Financial Services Companies ("Part 500")

While the rules are currently undergoing revision, the latest draft amendment to the Part 500 rules would require the board to have "*sufficient understanding of cyber security-related matters to exercise such oversight*", which may include using advisors to help explain such matters.

FTC Safeguards Rule

An appointed "Qualified Individual" in charge of overseeing data security must report annually to the board on:

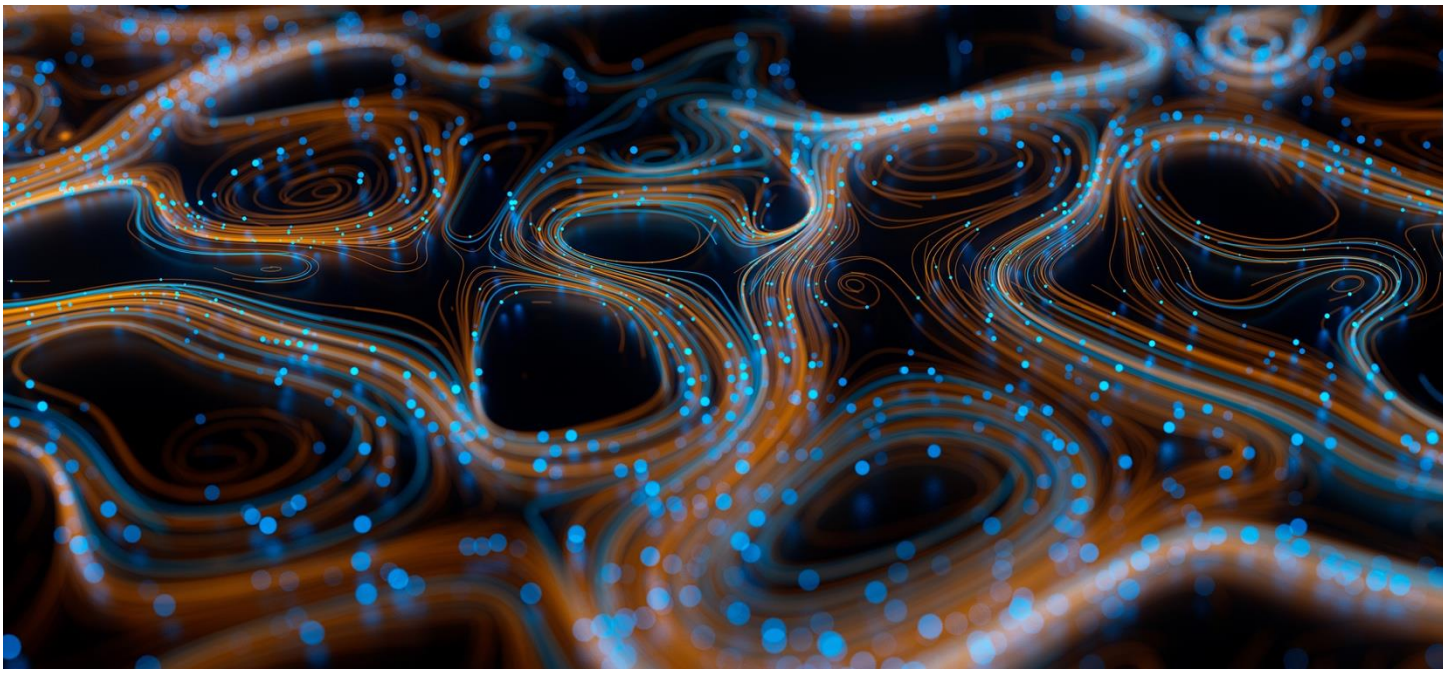
- The overall status of the company's information security system and Safeguard Rule compliance, and
- Material matters related to the information security program.

Board members may look to counsel to provide guidance on regulatory requirements and expectations under these rules and regulations, as well as on how the company will provide the board with sufficient information to meet their obligations.



Best Practices for Communication with the Board

1. **CISO to Attend Relevant Meetings of the Board** – when cybersecurity issues are to be discussed at a meeting of the board (including either a meeting of the full board or a meeting of a relevant board committee), it is advisable for the CISO or another high-ranking team member in IT or InfoSec to attend so that board members can ask questions and be up-to-date on company procedures.
2. **Quarterly Updates** – even when there are no pressing cybersecurity matters for discussion with the board, the board or relevant committee should receive updates on a regular basis to keep them apprised of ongoing initiatives and risk management efforts.
3. **Board Education Opportunities** – as with the senior leadership, there may be value in having board members view or participate in a tabletop exercise that is structured to test scenarios in which your company must respond to a simulated cyber incident. Outside counsel or another response vendor may facilitate these kinds of exercises and help you and your team assess areas for improvement.
4. **Documentation** – counsel should consider how best to document – and at what level of detail – the board's receipt of information (including briefing, training, or other updates) as well as the board's activity related to cybersecurity issues and risk management.



5. Cybersecurity Training and Awareness

Comprehensive cybersecurity training and awareness is a key pillar of any effective cybersecurity program. Particularly as workplaces continue to employ hybrid and remote work models, counsel should consider how best to ensure that all employees understand and follow the company's cybersecurity protocols. Companies may benefit from providing role-based security awareness training that is tailored for employees or affiliated persons in particular roles, such as members of technical teams, incident response teams, persons who wire money, executive management and board members. Typically, CISOs and privacy counsel are in charge of developing cybersecurity trainings for employees; but counsel can collaborate with these stakeholders to develop cybersecurity trainings for employees to ensure they meet applicable legal requirements.

There are two types of employee training sessions that companies typically implement: (i) onboarding sessions to get employees acclimated to a new workplace environment, and (ii) periodic sessions for all employees, at a regular cadence, to remind them of ongoing cyber threats and new threat actor techniques.

Both forms of training can address how the company's policies and procedures mitigate risks across the threat actor landscape and across attack types (including, for instance, social engineering, phishing, smishing, etc.). Counsel should review the training to ensure it meets all the applicable requirements.

Industry Specific Training Requirements

Cybersecurity training requirements exist in several jurisdictions as well as specific industries. Counsel need to understand which, if any, apply to their business.

A sample of requirements includes:

For Lawyers – New York now requires lawyers admitted to the bar to have one hour of cybersecurity training as part of its bi-yearly CLE requirement.

For Financial Entities – Some states, including New York, require financial entities regulated by the state to conduct security awareness trainings for employees.

For Insurance – States that follow the National Association of Insurance Commissioners ("NAIC") model rule require employee security awareness trainings for insurance providers.

For Healthcare – HIPAA requires both privacy and security awareness trainings for covered entities.

For Certain States – Some states require all businesses that collect personal information to conduct trainings. Counsel should assess whether their business is subject to the requirements of these states.

Training Content

Counsel should consider what elements and features are required for trainings to meet applicable legal requirements. These elements may include:

Frequency – Different laws require trainings at different cadences. Counsel should proactively track frequency requirements to ensure compliance.

Confidentiality and Privilege – Certain professions may need to consider how they navigate their confidentiality or privilege obligations when responding to an incident.

Risk Identification – Counsel may need to conduct and incorporate information to address findings of cybersecurity risk assessment into trainings, in order to comply with legal requirements.

Applicable Personnel – Counsel should consider whether trainings are required only for employees or also for temporary hires, such as contractors.

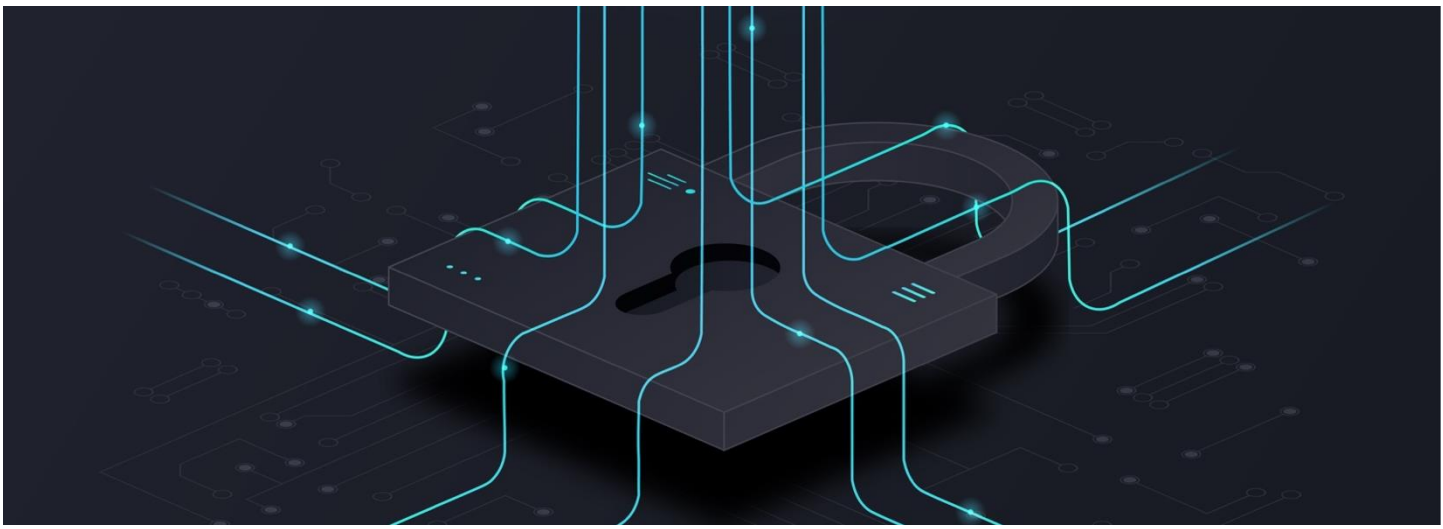
Counsel should also consider whether the training sessions can be delivered internally or whether it is preferable to have an external vendor deliver any of the sessions. For example, tabletop exercises may carry more weight with a regulator when delivered by an external party.

Common Pitfalls

One-Size Fits All – Industry-specific training may need to address sufficiently nuanced elements where a general training would not meet all the requirements.

One-and-Done Trainings – Providing training only during employee onboarding and not periodically thereafter may not be as effective, and may not meet ongoing training requirements in all jurisdictions.

Lack of Urgency – Failure to enforce participation and compliance may leave the business vulnerable to cybersecurity threats and legal exposure.



6. Data Minimization & Data Hygiene

Data is vital for businesses and also a source of risk. Various cybersecurity and privacy laws now require companies to dispose of certain categories of data when no longer needed for a legitimate business purpose. To help the company comply with these obligations and otherwise mitigate risk, counsel should take steps to understand (i) what types of data the company collects, processes, or retains, (ii) for what purpose the company is collecting that data, (iii) with whom that data is shared, and (iv) the company's retention, security and data governance policies surrounding that data.

Data Minimization Versus Data Hygiene

Data minimization generally refers to the set of policies and procedures by which a company aims to systematically reduce the amount of sensitive data they handle through document retention policies and similar best practices.

Data hygiene generally refers to the best practices for handling sensitive data and related data governance issues. Together, implementing these policies reduces the risk your organization may face from cyber incidents, privacy incidents, or litigation.

Why Data Minimization & Hygiene Matters

Until recently, it was accepted practice to retain electronic data indefinitely. Data storage was cheap, preserving data was seen as preserving potential value, and companies feared that deleting old data would be viewed negatively if it turned out that any documents relevant to litigation or regulatory inquiry had been inadvertently deleted.

Today, it is clear that the growth of most companies' electronic data is unsustainable, and that retaining large volumes of old data (when no longer necessary for business operations or for other legitimate purposes) carries significant cybersecurity, privacy, and operational risk—and those risks now often outweigh the risks associated with deletion. Further, there is an increasing body of regulations that reflects a new attitude toward data retention that focuses on whether companies are retaining data reasonably and for legitimate purposes.

- Under Section 5 of the Federal Trade Commission (the "FTC") Act, retaining data for longer than necessary for a legitimate business or legal purpose is considered an unfair practice.
- Numerous data privacy laws – including the European General Data Protection Regulation ("GDPR"), the California Privacy Rights Act ("CPRA") and the New York Shield Act – require companies to retain personal data only for as long as necessary for the purpose(s) for which the data was originally collected.

Top Tips

Review your Current Policies – Does your organization have clearly defined retention and handling policies for the various kinds of sensitive data it controls? If so, do the terms of the policy reasonably match up with the nature and purpose of the data you control? For example, it may be reasonable to keep records of major contracts indefinitely but may not be reasonable to retain fingerprint data related to employee timekeeping on that same basis.

Be Realistic – If you are crafting a data retention policy for the first time in your organization, it is better to have a "good enough" policy that has a high compliance rate than it is to have a perfect and far-reaching policy that has a low compliance rate. A lack of adherence to existing policies also is an area of focus for regulatory action. Small successes can be built on, especially if you encounter resistance to new policies early on.

Start with Data Mapping – Before you can begin to minimize data, it can be helpful to map out the various data flows in your organization, including noting which department(s) collect and store which data, for what reasons, and where that data is stored. Mapping data in this way will help you understand vulnerabilities or areas where data security needs to be shored up. Special attention should be paid to high-risk data elements, such as financial or biometric data. Remember also to include employee data and data from other administrative sources in your analysis, as well as vendors and any data they receive.

Triage Your Sources of Data Risk – Once you have mapped data flows within your organization, the next step is to triage the different data types using risk-based categories. Email is often a prime candidate for a first step in terms of crafting/implementing a retention policy: (1) email typically represents a significant portion of data held by a company; (2) the overwhelming majority of emails are not business-critical records; and (3) email data presents the greatest risk in terms of litigation (it is often the main focus of discovery) and cybersecurity (email is a clear risk for a phishing attack).

Best Practices for AI

While there are few AI-specific regulations currently in force, AI is likely to be a target for future regulation and lawsuits. Because complex AI systems require colossal volumes of data for training and development, and because many proposed frameworks for regulating these systems will require critical examination of that training data, AI poses unique data minimization and data hygiene problems. Counsel can help manage these tensions and risks by developing policies and procedures for proactively documenting and then curating training dataset contents and sources. These controls should be designed to triage among the various data elements, prioritizing those that are only strictly necessary for the model's performance and eliminating those that carry excess risk.

7. Insider Risks

Not all cybersecurity risks originate from external sources or threat actors. Counsel need to be prepared to deal with potential insider threats that affect critical assets.

Similarly, not all insider threats emanate from malicious actors. Some threats stem from well-intentioned insiders whose conduct can still put the confidentiality, integrity, or availability of the company's data or IT systems at risk. In managing insider threat risks, counsel should ensure close coordination with the company's Human Resources team, especially where disciplinary action may need to be considered.

Counsel can serve as the coordinator and glue between all the different players of a mature insider risk program. Proper oversight to avoid a police state is critical in rolling our insider monitoring controls. Counsel should work with key players from InfoSec, Risk, Compliance, HR, IT and the business more broadly to create a set of protocols for the insider risk program and procedures for different use cases.

Insider Threat Red Flags

Examples of insider threats and risks may include:

- Increased accesses to sensitive data after receiving a notice of termination.
- Downloading large volumes of data to external storage devices.
- Use of unauthorized external storage devices.
- Frequent access to workspaces outside of normal working hours.
- Attempts to bypass security controls.
- Requests for clearance or higher-level access without a clear business need.

Whistleblower Policies

Employees can be the first line of defense in identifying and reporting anomalous behavior.

Counsel should ensure that there are robust whistleblower policies and procedures (which cover insider risks) in place to report and investigate any suspected unauthorized behavior at the company. This is especially important for companies operating within government contracts, given the new DOJ Civil Cyber Fraud program, which seeks to investigate companies for fraudulent statements about cybersecurity maturity and has a built-in incentive for whistleblowers, and companies subject to the SEC's jurisdiction and its Dodd-Frank whistleblower protections.

Key considerations for your insider risk whistleblower programs include:

- The whistleblower policy should be placed in a clear, prominent location *e.g.*, the employee handbook or the intranet.
- The policy should explain how the internal whistleblowing process works, what the reporting channels look like, and how reports are investigated and escalated.

- Ideally, individuals should be able to anonymously report their concerns.
- It may not be obvious to employees how insider risks can manifest themselves. The policy should provide examples of potential misconduct that could be reported, including cybersecurity concerns.

Insider Risk Program Elements

Counsel may be asked to create or review elements and protocols for an insider risk program. While these protocols may fall within the InfoSec's purview, counsel may have an important collaborative role alongside HR and Legal in developing these procedures, given the increasing legal implications of poor cybersecurity hygiene. Such protocols might include:

- **Cyber Monitoring Tools** – protocols establishing the company's approach to data access and monitoring. This includes user and entity behavior analytics, data loss prevention monitoring, key logging and remote access tools, physical access restrictions, internal and external network traffic monitoring tools, access and connection review tools, and related Bring Your Own Device management tools. Each such tool and monitoring use case needs careful review.
- **Role-Based Access Restrictions** – protocols that clearly set out who does – and does not – have access to critical cyber infrastructure, including protocols that address when previously granted access privileges should be revoked.
- **Robust Cybersecurity Training** – protocols that set out the company's approach to regular employee cybersecurity training to reduce the likelihood of individuals becoming unintentional insider risks, e.g., by accidentally attempting to bypass security controls.

See Chapter 5 on Cybersecurity Training and Awareness.

Investigating an Insider Threat

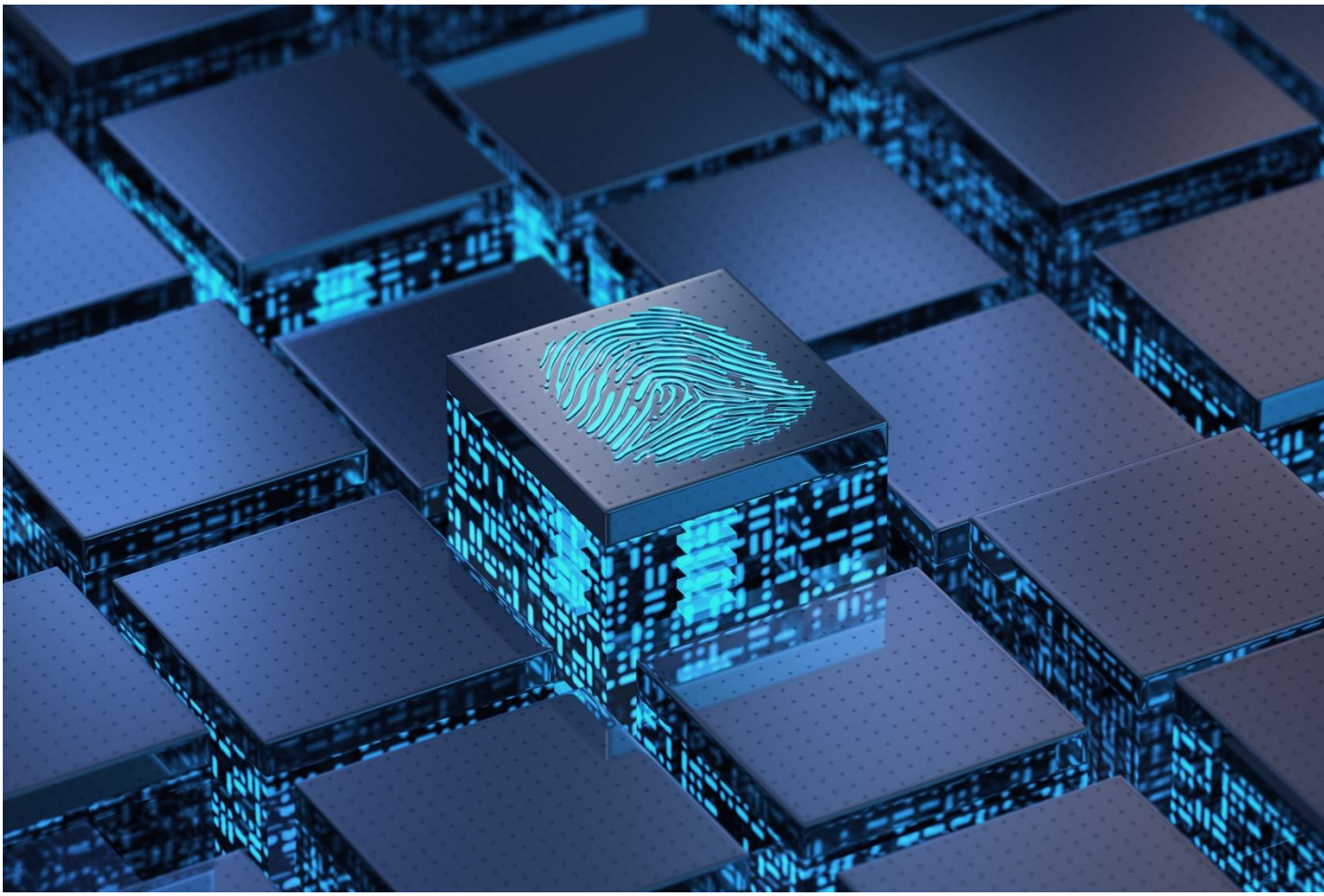
Once the company has received intelligence on a suspected insider threat, either from a whistleblower or via an internal monitoring alert, counsel might assist with the subsequent investigation. Considerations include:

- Determining if the investigation should be conducted under legal privilege.
- Considering whether to issue a document preservation notice to the insider and other relevant parties, especially if important evidence is ordinarily subject to auto-deletion rules.
- Determining whether to interview the suspected insider and, if so, considering who will conduct the interview (including whether HR should be involved).
- Assessing whether the initial investigation findings should be escalated to senior leadership for further review.
- Considering whether it is appropriate to inform the suspected insider's supervisor or line manager about the concern.

If the investigation confirms the existence of an insider threat, counsel may need to:

- Opine, alongside employment law counsel, on HR's decisions on whether any disciplinary action is warranted and, if it is, whether it is proportionate.
- Determine if any contractual or regulatory breach notification obligations have been triggered if the insider's actions have compromised any nonpublic, confidential, or personally identifiable information.
- Consider whether any voluntary regulatory notifications should be submitted based on the incident, even if not legally required.

If notifications are made, counsel can assist with drafting talking points for follow up communications with regulators, commercial counterparties, clients, or the media.



8. Managing the Relationship Between Privacy & Counsel

Cybersecurity and data privacy are two sides of the same coin. In the broadest possible terms, cybersecurity looks at protecting data from the outside (and inside), whereas data privacy is concerned with what a company does with the personal data. For many companies, the same attorney is counsel for both cyber and privacy. But increasingly, cyber counsel and privacy counsel are different roles. For companies that implement separate roles, it is therefore important for the two roles to closely collaborate.

Cybersecurity and Data Privacy Overlap

There are a growing number of data privacy statutes and regulations in the U.S. and abroad that require companies to implement various cybersecurity measures to protect any personal information held by the company – such as the CPRA, COPPA, GBLA and GDPR. For example, these may include requirements surrounding the confidentiality, integrity, and availability of personal information, including the encryption and pseudonymization of such data, or unauthorized data access preventions. Counsel should consider working with privacy counsel to help the company understand and adhere to these requirements.

In contrast, at other times a company's cybersecurity proposals may not neatly align with privacy law requirements, especially in jurisdictions with more stringent regimes. For example, the capabilities of certain insider threat tools could trigger potential concerns under data privacy or employee monitoring laws in some jurisdictions, even if in other jurisdictions there are requirements to have insider threat controls. It can be complex to navigate these tensions within a company's risk appetite. Counsel should therefore consider collaborating with privacy counsel and any other relevant stakeholders, which may include the Legal and Compliance team, CISO and (where relevant) Works Councils, on these points.

Potential Areas for Collaboration

These are some of the most common areas in which cyber and privacy counsel may consider collaborating.

Data Collection and Security – Understanding what data is being collected and from where, the integrity of that data, and where and how it is being stored are important considerations for both cybersecurity and data privacy. Counsel should consider contributing to the company's policies and procedures on these points, including external-facing privacy policies and terms of use. In particular, counsel may want to consider the balance between ensuring the policies comply with applicable data privacy laws while giving the company sufficient flexibility to use the data for its intended purpose(s) and any new purposes that arise in the future (such as providing the data to law enforcement in the future if required or otherwise lawful to do so).

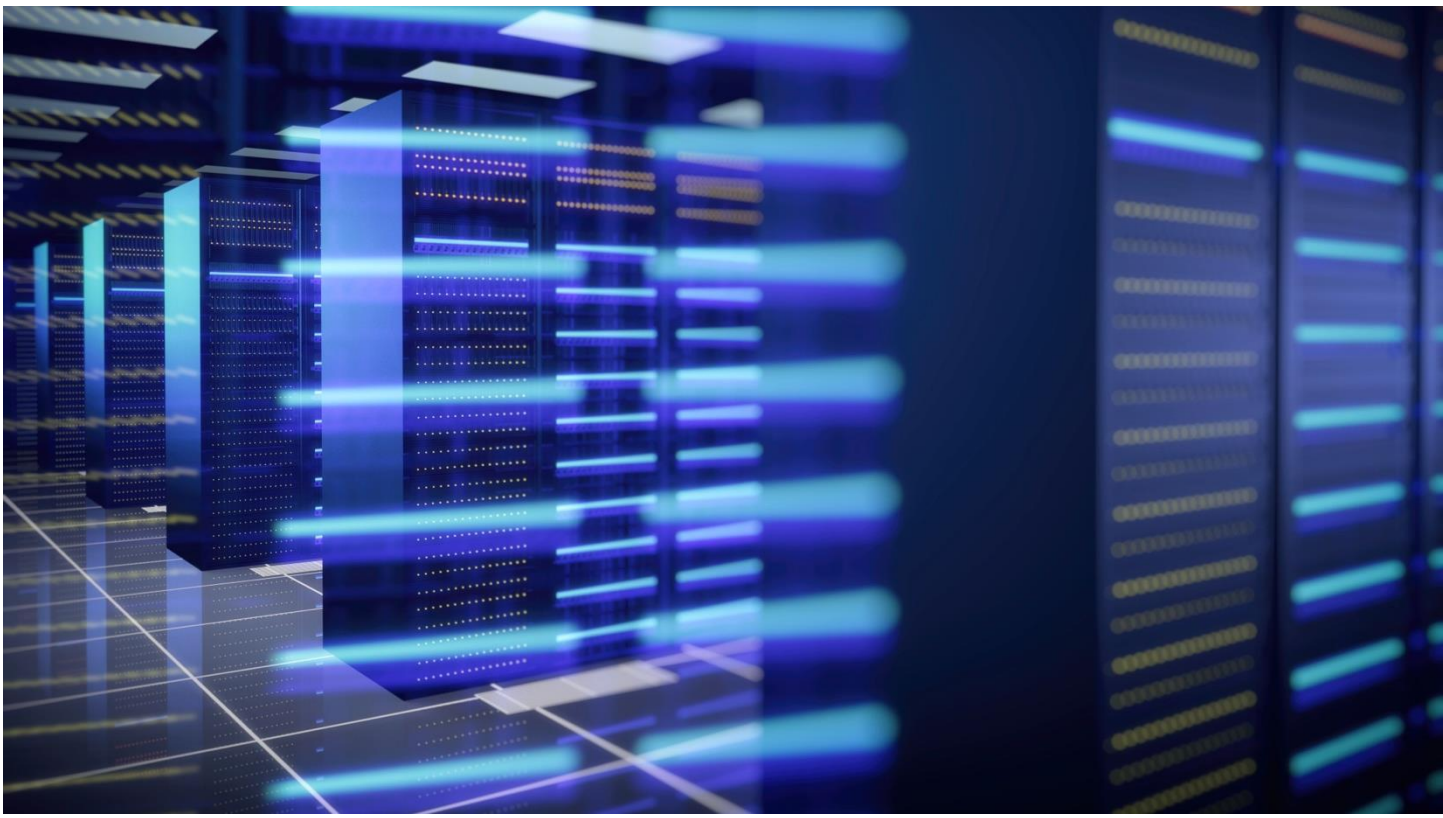
Data Retention and Disposal – While cybersecurity may focus on secure data storage and disposal, data privacy is more concerned with how long the data is being

kept and for what business purpose. The two groups should work together on defining a data retention policy that both complies with privacy requirements and meets applicable security needs. *See Chapter 6 on Data Minimization and Data Hygiene.*

Insider Risk and Support Analytics – Counsel typically has the responsibility of overseeing and mitigating internal risks within a company that could lead to a breach. This may include implementing employee monitoring tools and analytics to help reduce risk. However, there can be a tension between these practices and data privacy or employee monitoring laws in some jurisdictions. Cyber and privacy counsel may want to collaborate on navigating these tensions. *See Chapter 7 on Insider Risk.*

Privacy-by-Design – There has been a recent trend in both cybersecurity and data privacy towards 'privacy-by-design' – or integrating data privacy considerations into all business activities from the design stage and throughout the lifecycle. Cyber and privacy counsel are both well positioned to help the company understand its legal obligations in relation to the data it holds, and establish privacy-by-design standards that the company can implement into its data practices.

Vendor Engagement – Many vendors engaged by the company will process some sort of personal information when providing their services to the company, given the very broad definition of the term in certain data privacy laws (including the GDPR). Cyber and privacy counsel should consider working together to ensure the contract complies with applicable privacy requirements – including any contractual requirements for third country data transfers – and that the vendor's privacy practices meet the proper legal standards. *See Chapter 5 on Third-Party Risk Management.*



9. Incident Response: Preparations

It is common (and at times required) for companies to have a suite of policies and procedures in place that will allow them to effectively respond to a range of incident types. Counsel should help prepare incident response plans and participate in tabletop exercises and onboarding of vendors.

The Plan: IRPs and Playbooks

Companies should implement incident response plans to guide the company's response to a comprehensive range of cybersecurity incidents. Often a company will have a technical incident response team for the operational teams that are conducting the blocking and tackling of the incident. A separate document, or set of documents, will exist for the C-Suite.

Creating the incident response plan should take significant time. An effective plan is bespoke to the company. Off the shelf plans that do not account for the company's risks, culture and existing response procedures will be ignored during an incident, which creates more risk than it solves. Instead, counsel should work with the information security team, business leaders, communications, HR and other functions to create a plan tailored to the business and to specific people who will have responsibilities for carrying out the plan. The plan should detail the roles and responsibilities of core responders, the actions the responders are expected to take, which Company functions to involve in responding to which types of incidents, escalation triggers, and additional details regarding each of those procedures.

Given recent law, enforcement actions and court decisions, it is important that counsel ensure all the required elements are in the plan.

Supplementary Plans for Incident Response

Depending on a company's size and complexity, the materials can be comprised of a core IRP and a complementary set of threat-specific playbooks, such as a ransomware playbook, a vendor breach and software supply chain attack playbook, an insider threat playbook, and wire diversion playbook, and external auditor and insurer engagement protocols.

Preparing to Respond: Tabletop Exercises and Trainings

A particularly effective way to prepare for an incident, and to test the company's incident response procedures, is to conduct tabletop exercises. Tabletop excises are often run by a facilitator (*e.g.*, outside counsel or a consultant), and involve the core incident response team running through how they would respond to a fictitious (but realistic) cyber-attack. Some tabletop exercises are geared towards the tech teams (typically facilitated by consultants), while others are geared towards the C-Suite (typically facilitated by outside counsel). They can be helpful for highlighting weak areas in company security and chains of command. Counsel can both participate in the exercises and help to facilitate logistics and development of relevant scenarios.

In addition to full-scale tabletop exercises, counsel may consider implementing smaller-scale exercises that test components of the IR team's response procedures, such as an exercise designed solely to ensure that the IR team members know how to activate and access the kind of out-of-bands communication channels discussed below.

See Chapter 5 on Cybersecurity Training and Awareness.

Communications Templates

Rather than scramble to draft communications from scratch in the midst of a live incident, it can be useful for companies to prepare a set of internal and external communications templates that can immediately be adapted and disseminated in the event of a cyber incident. Counsel may be involved in the drafting or reviewing of such communications, including to ensure that the content is legally defensible and does not expose the company to unnecessary risk. Points to consider include:

External Communications – These materials may include templates for communications with clients (including incident notifications, talking points and FAQs), media outlets (including a media leak plan, press holding statement and draft news releases), external vendors, and template data breach notifications for any individual whose personal data was impacted by the incident.

Internal Communications – Companies should consider whether to prepare stock materials that can be used to alert internal employees to the existence of a cyber incident, as well as template FAQs for employee questions. Companies may wish for these materials to remind employees to be factual and avoid speculation, preserve all relevant documents and evidence, mark privileged communications as "privileged & confidential" to protect any potential privilege claims, and to refrain from distributing confidential information to third parties (other than forensic experts).

Establishing OOB Communications Channels

An out of bands ("OOB") communications channel is a way for employees to communicate outside of official company email channels during an actual or suspected security incident. Counsel can assist InfoSec in securely establishing and maintaining an active OOB system so that one is available if needed.

OOB Considerations

When creating an OOB domain, it can be helpful to avoid using the actual company name in your domain, which can limit the likelihood of alerting threat actors to the existence of the OOB system. It also may be a good idea to pre-populate one user account (who will be responsible for forwarding these documents to other OOB communications system users in the event of a breach) with the company's IRPs and playbooks, and a copy of your insurance plan.

Regulator and Law Enforcement Outreach

Counsel can facilitate the creation a company-wide checklist (including contact details) of all of the potential regulators and law enforcement officials with whom the company may need to connect during a breach. It is important to remember that sharing privileged or confidential work product with law enforcement or regulators may impact the company's ability to protect any such materials in the future. So, the timing and content of any communications should be considered carefully. *See Chapter 12 on External Engagement: Law Enforcement, Regulators, Trade Groups.*

Selecting and Engaging IR Vendors

Prior to an incident occurring, companies may want to identify and make arrangements with vendors they might want to engage in the event of a breach. Potential categories of vendors include: outside counsel, forensic investigators, technical remediation teams, ransom negotiators (for ransomware or extortion incidents), and crisis communication firms. For each role, it can be useful to select at least two options for each vendor in case one is unable to assist in the context of a particular incident.

Taking these steps in advance not only allows the company to select the most appropriate vendors for its size and risk profile; it also allows the company to negotiate any contractual terms (rather than having to accept the standard clauses in the heat of the incident). Counsel can assist the company with the vendor due diligence process and any subsequent contractual negotiations.

An important consideration when engaging IR-related vendors is whether the vendor will be engaged by outside counsel or by the company itself. There are significant differences between the two structures, and companies should confer with incident response counsel on the best structure to be used in the context of a particular incident. *See Chapter 15 on Third Party Risk Management.*

Considerations when selecting IR vendors:

1. Is the vendor approved by your insurer? Most insurers have panels of pre-approved vendor options.
2. What is the depth of the vendor's experience? How long have they provided incident response services and in which markets?
3. What are the vendor's response times and resource activation times? Are they able to scale an investigation to meet the company's needs?
4. What are the vendor's intelligence capabilities? How do they apply them to incident response services?
5. What level of support does the vendor provide for incidents? Are they also responsible for lessons learned, root cause analysis and remediation?

10. Incident Response: How to Respond to an Incident

Given the myriad of potential legal and regulatory issues involved, counsel has an important role to play in cybersecurity incident response ("IR"), although the nature of that role will vary significantly based on the structure of the company and how IR roles are delineated. At a minimum, it can be helpful for counsel to be aware of the general steps that occur when a breach happens, so they can provide advice and assistance when needed during the overall IR process. The timeline and events described herein are provided for illustrative purposes only, as they will vary significantly company-to-company and incident to incident.

Areas to Cover in the First 24 Hours

In the first 24 hours of a breach, the incident response team will be in triage mode to assess the incident. There will be many legal workstreams for counsel to lead, and other workstreams for counsel to weigh in on.

Activation

- The incident response process should track the relevant playbooks, and counsel should ensure that nothing is missed.
- If the matter is significant, counsel should issue a letter to the company instructing that the investigation is being directed with counsel under privilege.

Assessment

- Consider if the company's email can be used or whether the company needs to move to an out-of-bands system.
- Determine if outside counsel should be engaged for legal advice and to retain incident response vendors under privilege.
- Assess what regulatory and contractual notification obligations are triggered.
- Consider whether any systems should be disconnected. Would that have legal or regulatory risks or ramifications?

Notices and Disclosures

- Assess whether to alert customers, employees, investors, shareholders, vendors, contractors, or auditors about the incident.
- Determine whether to contact law enforcement.
- Assess whether to notify regulators.
- Inform certain employees of the need for records preservation, and assessing whether a litigation hold should be implemented.
- Review any draft communications, both internal and external.

Preservation

- Maintain a record of the incident, the facts and key decisions.
- Determine whether to contact the company's insurer or insurance broker.
- Remind individuals involved in the incident response to ensure that all relevant documents are preserved, information is only distributed on a need-to-know basis, and communications remain factual and avoid speculation.

External Communications & Media Inquiries

Counsel may want to be involved in reviewing external communications and responses to media inquiries to ensure that they are accurate, do not reveal privileged information and do not expose the company to unnecessary legal risk.

Counsel should also ensure that information in these communications does not contradict information that has been provided to regulators or other authorities. *See Chapter 12 on External Engagement.*

Role of PR/Communications Firms in Incident Response

PR and crisis communications companies bring valuable experience to the process of managing external communication during an incident. They may be focused on particular aspects of the communications and may not be sensitive to certain areas of risk, which counsel may be better positioned to evaluate.

Notification Considerations

Cybersecurity incidents may trigger a range of legal, regulatory and contractual notification obligations for the company. Counsel will likely be involved in assessing whether these obligations are triggered and, if so, responding to them.

Regulatory Notifications – Regulatory notifications are not just limited to data protection authorities. Counsel should consider whether any other regulators, such as banking and financial regulators (for financial institutions), or other industry or professional regulators, need to be notified. Be sure to keep track of notification deadlines as they can vary widely; outside counsel might be a useful partner here. Similarly, regulators may have different information requirements in their breach notification rules, so a one-size-fits-all approach may not be appropriate when drafting notifications.

Individual Notifications – Individuals may need to be notified about the incident if their personally identifiable information ("PII") was impacted. In the United States, notification triggers and notification requirements vary by state. For example, in some states, individuals are only required to be notified if the incident may cause them a risk of harm. Similarly, in some states electronic notification is always permissible whereas in others it is only allowed in certain circumstances. For certain types of impacted PII, the company may be required to provide complimentary credit monitoring to affected individuals.

Contractual Notifications – Aside from its regulatory obligations, the company may have a contractual obligation to notify customers, clients and vendors of cybersecurity incidents in certain situations. Counsel should review such contracts, starting with those from key third parties, to assess whether notification is required.

Ransomware Incidents

Ransomware incidents have some additional considerations compared to other IR work. The Joint Ransomware Task Force has published a #StopRansomware Guide for navigating these attacks. Counsel may initially want to consider:

- Was there a ransomware notice? If yes, does it contain a demand deadline?
- Do we know the threat actor group? Do they have a history of releasing data if the payment actually goes through?
- What systems were encrypted? How important are they? Do you need the decryption key or can you restore from backup?
- Did the group exfiltrate data? If it did, what type of data?

Once this information has been identified, it is then up to the IR team to determine whether and how to approach the ransom negotiations.

- **Evaluate the Payment Options** – Most companies approach ransomware with a view that they won't negotiate with terrorists. But there are many considerations involved, and about 50% of companies make ransomware payments. Counsel can help the company assess the value of the stolen data/encrypted systems to its business.
- **Assess the Legality of Payment** – If payment is considered, counsel should help the IR team assess the legality of payment, including from a sanctions perspective. Law enforcement may be able to provide helpful intel to assess the compliance risks, as well as ransom negotiators and forensic investigators.
- **Communicate with Your Bank & Insurer** – Banks have their own internal compliance assessments they have to complete before they will authorize a ransom payment. These assessments can be onerous and can require extensive documentation from the company. Similarly, counsel should keep the insurer involved of any developments to ensure the payment is covered by the insurance policy where applicable.

11. Incident Response: Post Incident

After an incident is remediated, contained and systems are restored, the post-incident process begins. Companies may find it useful – and some make it part of their written response plan – to take steps to review and document the incident, and to consider opportunities for improvements to its cybersecurity program and IR policies and procedures.

Forensic Investigations

Counsel might assist in determining whether a forensic investigation report is necessary. Courts have not always afforded privilege protection to incident response reports. A company may wish to consider whether a written report is critical for documenting the incident or whether a verbal update will suffice. Those companies that rely on written reports in order to ensure future remediation may wish to have a report even with the risk of privilege being pierced.

There are multiple forms that a forensic report may take, including:

- no report, with only a verbal assessment;
- an executive summary that memorializes key details regarding the incident in language that can be understood by a non-technical audience;
- a technical report explaining and memorializing IOCs discovered during the incident;
- a complete report including a mixture of technical and narrative features that describe the incident and the company's response; or
- some mixture of the former options. For instance, it could consist of a complete report including a technical summary, but with a short-form executive summary that can be separated and provided to various constituents, when needed.

The question of which form a report should take can have important implications, and any decision should be made keeping in mind the potential audiences and risks from the various approaches.

Ultimately, the choice of whether to have a report prepared and, if so, in what form, should be made based on careful consideration of the facts and circumstances of each incident.

Post-Incident Investigation and Lessons Learned

For medium- and high-severity incidents, companies often conduct post-incident reviews designed to identify strengths, weaknesses, and opportunities for improvement. These efforts often produce reporting or documentation that is separate from the forensic reports that may be prepared by or with assistance from technical experts.

Counsel may want to take a lead role in preparing post-incident review work-product. Counsel are uniquely positioned to gather feedback from all the functional teams in

anticipation of regulatory action and litigation, and they can then document the findings in a privileged and confidential document. The review can commence with meetings with the IR team members and other key IR participants to walk through and document the lessons learned from the incident and any potential areas for future improvement. These lessons will be especially helpful when responding to future audit inquiries.

Reports following post-incident reviews can be prepared by either counsel or outside counsel, and they are often distributed only by counsel and only to a select few. Counsel, working with the other functional teams, may then help advise the Board and C-Suite on which of the post-incident findings should be adopted (if any) in light of the potential benefit to the company, balanced against the company's business interests, risk appetite and budget constraints.

After an incident, companies often find that their response procedures did not match the procedures laid out in the incident response plan. Sometimes the IR plan calls for one team to perform a function when in fact another team handled that. Other times the response plan is missing key activities altogether and needs to be updated to account for those. Counsel typically gather feedback from all the incident response teams in conducting the plan review. If changes are implemented, the company may want to stress-test those areas in the company's next tabletop exercise. Similarly, counsel may consider whether any of the lessons learned can become the focus of company-wide trainings, attorney-specific CLE sessions, or internal publications and knowledge management tools.

Evidence Preservation

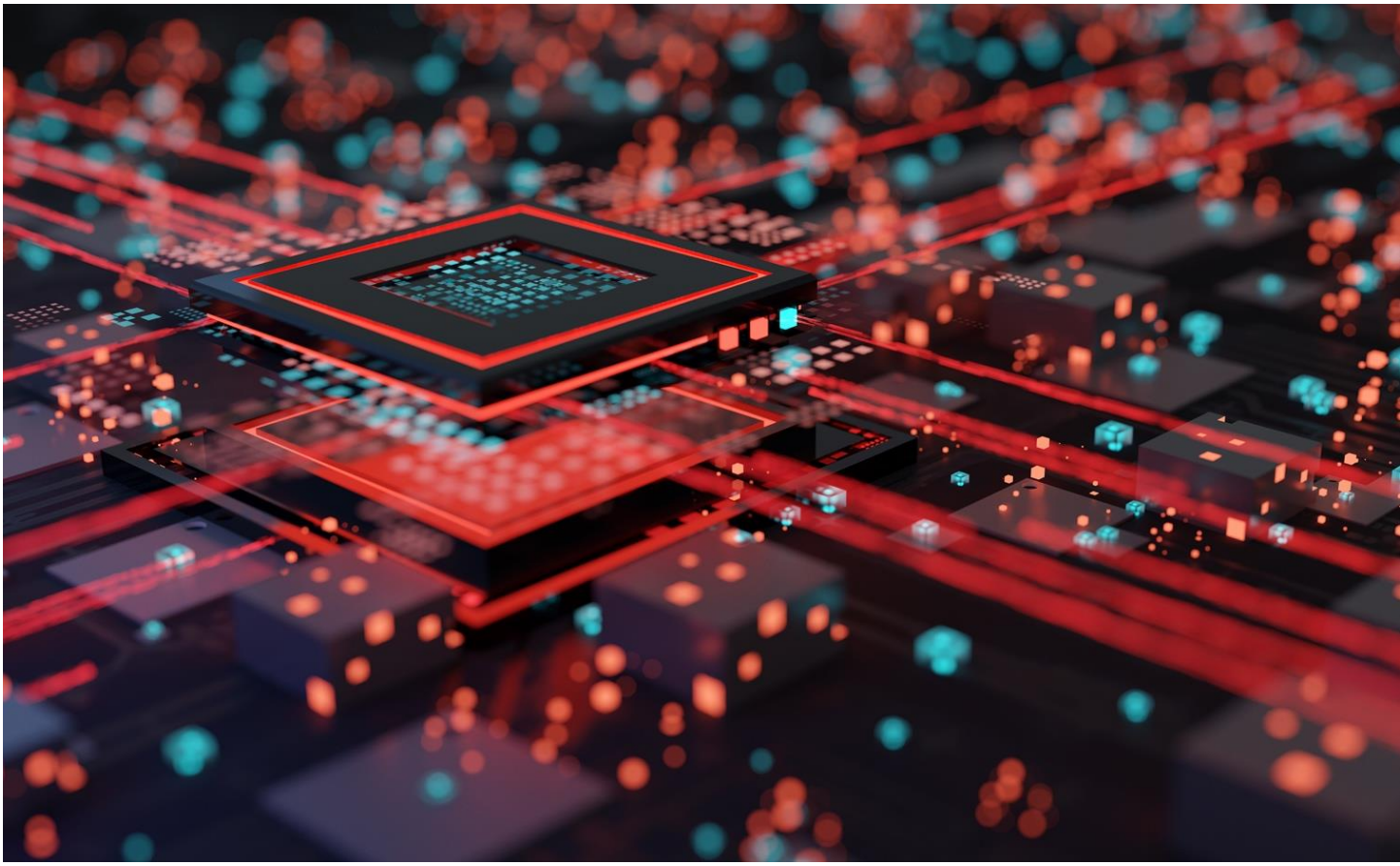
Evidence preservation, including post-incident preservation, may have been contemplated as the incident unfolded. However, often there are new questions post-incident. Counsel is often asked to coordinate the identification and preservation of all key evidence relating to the incident, and the company's response to it, in anticipation of any future litigation, or legal or regulatory action.

Closing Down OOB Communications

If the IR team established an OOB communications channel specifically for the incident – once the company's usual communications platform has been reinstated and any particularly sensitive incident discussions (such as determining the ransom negotiation strategy while discussions are ongoing) have concluded – counsel should consider whether all OOB communications should be transferred to the usual platform or otherwise retained, and the OOB channel shut down. Not only will this help protect the security of the data, as the Company's usual platform is likely to be more secure than the OOB channel, but it also helps ensure that all IR data is retained in one location.

After-Incident Items for Counsel to Consider

- Conducting after-action interviews.
- Developing and/or memorializing "lessons learned."
- Overseeing production of forensic report(s), if any.
- Reviewing IR plan for possible revisions.
- Ensuring necessary preservation of evidence.
- Tying up alternative communications channels (*e.g.*, out-of-band communications).
- Revisiting scope of insurance coverage.



12. External Engagement: Law Enforcement, Regulators, Trade Groups

As a field with rapidly evolving threats, law and regulations, it is critical for counsel to stay abreast of developments. Additionally, understanding how other companies are dealing with the regulations is a critical piece of information to help benchmark. Counsel can assist the company's cybersecurity risk management by facilitating strong external connections between the company and law enforcement, regulators, and trade groups. In other fields (*e.g.*, white collar crime), law enforcement and regulators are often adverse to companies. But for cyber there is a shared purpose, even with most regulators. Building trust and cooperation is key.

Stay Engaged

Even in the absence of a live incident, counsel can consider reaching out to local law enforcement (including the local FBI field office and their state or municipal counterparts) to schedule a meeting. Through this kind of informal outreach, counsel can better understand how to work with law enforcement proactively. Similarly, with permission, counsel can schedule time with sectoral or other primary regulators to foster introductions and understand how the company can be effective in cybersecurity compliance.

Join Trade Groups

There are numerous different trade groups related to information security that counsel might consider joining. For companies that are owners or operators of Critical Infrastructure, there are over two dozen sector-specific Information Sharing and Analysis Centers (or "ISACs") that provide a forum and a venue for collection, analysis, and dissemination of threat intelligence among business in the relevant sector.

These government-sanctioned organizations exist alongside various industry-specific trade groups that also provide cybersecurity coordination vehicles. So for example, in addition to the ISAC for financial services companies – called the Financial Services Information Sharing and Analysis Center ("FS-ISAC") – there are multiple financial-services-specific trade groups – including the Financial Services Sector Coordinating Council ("FSSCC"), and Securities Industry and Financial Markets Association ("SIFMA") – through which counsel can share and receive valuable cybersecurity intelligence.

Beyond trade associations, Debevoise maintains close ties to a large group of cyber counsel and is always happy to connect new practitioners in the field to the larger group.

Prepare for Change

Risks related to cybersecurity are constantly changing – new threats, new regulatory expectations, and new commercial arrangements can develop quickly and often without much notice. Counsel's role in protecting the company therefore need not be purely reactive; counsel can be forward-thinking and can help gather information from colleagues, peer companies, and regulatory counterparts to inform the company's security posture and legal strategies. By helping the company prepare for change, counsel can help create durable defenses and effectively limit the company's risk in the face of uncertainty.



13. Cyber Insurance

Cyber insurance can be essential in helping companies deal with the expense of responding to, and recovering from, a cybersecurity incident. Counsel and CISOs should be closely involved with all insurance-related interactions to ensure that the company has suitable policy coverage, and that the coverage is not accidentally invalidated by the company's action when responding to an incident.

Three Current Trends

1. **Higher Pricing and Deductibles** – The costs of obtaining insurance coverages have been increasing over the last few years due to large loss ratio increases, primarily driven by ransomware payments.
2. **Lower Policy Limits** – The insurance industry has been reducing the maximum amount they will pay for a claim, with some insurers cutting their coverage by 50 percent.
3. **Move Towards Underwriting Major Cyber Events** – Underwriting processes for major cyber events have become much more involved processes, as insurers look to reduce their exposure to an increasing number of claims. Some providers are now more selective over the types of industry, or size of company, they will cover.

Negotiating Insurance Coverage

Negotiating cyber insurance policies is a multi-party affair that can take several weeks to complete. It should include representatives from the IT and InfoSec, Legal, Risk and Finance teams. The cybersecurity landscape is rapidly evolving; you should ensure that your policy covers a range of incident types.

Here are some things to consider when negotiating coverage:

- Does the covered "computer system" include third-party service provider systems?
- Is there affirmative coverage for cyber extortion response expenses and ransom payments?
- Do the business interruption losses include losses:
  - from preventative shutdowns in response to a suspected cyber incident?
  - from unintentional and unplanned outage or failure of the network?
  - due to a cyber event or system failure at a "dependent business"?
- Is there coverage for social engineering fraud losses or transfer of funds?
- Does the policy include hardware replacement costs if a device is "bricked" following an incident?
- Is there an option to assume the defense of any legal claims relating to the incident, including determining the settlement or resolution strategies?

Communicating with Insurers during a Cyber Incident

When to Notify

When deciding whether to notify the cyber insurer of a potential incident, you may want to consider:

- Is the incident likely to incur costs in excess of the deductible? If not, consider the pros/cons of notifying. If the incident involves a ransom demand in excess of the deductible, the insurers should be notified.
- Could the incident trigger litigation from customers, other third-parties or employees whose confidential information is impacted?
- Are the relevant carriers under NDA? If not, ensure one is executed before sharing confidential information with them.

What to Tell Them

Insurers should be provided with factual information about the incident and the response; you should not share legally privileged information with the insurer.

- **Initial Questionnaire** – the insurer may ask the company to complete a pro forma intake questionnaire after the initial notification (which is typically done verbally).
- **Vendor Engagement** – notify insurers of any vendors you are using that are not on the pre-approved vendor list. In these situations, insurers may only pay vendors up to their panel rate with the company covering the difference.
- **Budgets & SoW** – insurers may want to see budgets and the statements of work for all incident response vendors (counsel, forensic, eDiscovery, crisis communications etc.).
- **Ongoing Updates** – some insurers may expect to receive periodic updates. If a written notification is not required, consider setting up recurring calls so that updates can be delivered verbally; Risk should lead the calls, along with InfoSec and Legal.

Common Pitfalls

- **Failure to Obtain Consent** – the insurer can reject costs of vendors that are not on the pre-approved list if the insurer did not consent to their engagement.
- **Information Relied Upon in the Underwriting Process was Inaccurate** – the insurers can reject coverage if the information they relied upon was inaccurate, incomplete or false.
- **Breach of the Conditions Precedent** – such as failure to provide timely notices, failure to co-operate with the insurer's investigation, or insufficient proof of loss.
- **Failure to Mitigate** – the insurers can reject coverage if the insured failed to mitigate or act reasonably in limiting any further losses.
- **Terms of the Investigation** – some insurance carriers may dictate what the investigation looks like, despite the GC/CISO not agreeing with those terms.

14. Bug Bounty and Vulnerability Disclosure

In order to respond to increasingly sophisticated and diverse cyberattack techniques, companies have to take proactive measures to reduce the likelihood of a cybersecurity incident. In addition to incident response preparation *(see Chapter 9 on Incident Response – Preparation and Vendor Engagement)* **and educational tools** *(see Chapter 5 on Cybersecurity Training and Awareness)***, this may include implementing technical-facing measures such as a bug bounty and vulnerability disclosure program.**

While they can provide invaluable feedback to companies on the strength of their environment's security, the legal and risk landscape surrounding bug bounty and vulnerability programs can be complex to navigate. Counsel can add value by remaining closely involved in creating and overseeing these programs, by ensuring they operate as intended, and by helping flag any activities that exceed the parameters of the program, which can turn a controlled exercise into an official cybersecurity incident.

What is a Bug Bounty Program?

Bug bounty and vulnerability disclosure programs give companies an opportunity to discover vulnerabilities, or "bugs", in their software before they are exploited by a threat actor in a cybersecurity event. This is achieved by offering third parties (usually so-called white-hat hackers) an incentive (usually financial) to identify and report bugs in the company's software, provided they do not exploit them. This gives the company an opportunity to remediate any issues, hopefully before they are exploited by malicious threat actors.

Counsel's Role in Bug Bounty Programs

Legal Analysis – Bug bounty programs present complex questions that can put certain aspects of the programs in a legally gray area. For instance, just because a company "consents" to hacking under the program does not mean that hackers will have blanket immunity from legal proceedings for otherwise criminal conduct. Counsel can help conduct or supervise the legal analysis into any consequences that may arise from the creation of a bug bounty program in order to help safeguard the company from any unexpected consequences. Specific legal considerations may include:

- Whether the hacking activities fall within the scope of the bug bounty program or should be escalated as a formal cybersecurity incident. In particular, if a hack occurs before a bug bounty program exists, counsel should carefully consider options on classifying hacks in these circumstances, being mindful of the issues that arose in the Joe Sullivan (former Uber Chief Security Officer) prosecution.
- Whether public disclosure that a vulnerability exists is required – the DOJ provides guidance on when the discovery of a vulnerability triggers public disclosure requirements.

- Similarly, a new resource, disclose.io, has created a database of bug bounty and vulnerability disclosure programs that are in current operation, where vulnerability reports should be submitted, and what details they should include, as well as whether safe harbor status exists for hackers acting within the confines of the program.

External Vendors – Counsel can advise on whether outside expertise is needed to create or operate a bug bounty program, including legal counsel and security vendors. A company may prefer to engage a security company that specializes in vulnerability identification. Well-known companies include: HackerOne, Bug Crowd, and Immunefi.

Program Scope – Counsel can advise on whether any parts of the company's IT system should or will be "off-limits" to bug bounty programs. Counsel can work with technical teams to implement measures ahead of time to protect any systems they decide are out of scope.

Drafting Program Terms – Counsel can assist program stakeholders in deciding key bug bounty program features and assist in documenting the terms and conditions for participants. Questions to be addressed may include:

- Key scope and timing parameters such as how long the program will run, and whether the program is being limited to a specific software application being tested.
- How the company will structure incentives offered under the program. For instance, the company can decide how much they are willing to pay, how many hackers they are willing to pay, whether payments will be based on a severity scale, and whether the company will offer non-monetary forms of recognition.
- Whether the company's bug bounty program will be internal- or external-facing. For instance, a company can have a bug bounty program setup without making it known to the public.

Incident Escalation – Counsel can assist in monitoring the performance of the bug bounty program, including carefully assessing whether hacking activities have evolved outside the scope of the bug bounty program such that they should now be escalated as cybersecurity incidents. Counsel also can assist by being prepared to react in the event a bug bounty program reveals the presence of threat actors already in the company environment.

Potential Pitfalls

Unverified or Anonymous Hackers – Given the potential legal risks for individuals who hack companies - even with the company's invitation - white-hat hackers can be highly protective of their identities. Companies should take steps to ensure that they have verified the identity of the hacker prior to any payment being made. Failure to verify hacker identity prior to payment may lead to legal consequences, including inadvertent sanctions violations.

Unintended Consequences – Failure to limit the scope of a bug bounty program – both technically and legally – could lead to a range of unintended consequences from the program, such as the theft of data or finances, disclosure of material non-public information, excessive payments to hackers where the payment

mechanisms do not operate as anticipated, or hacking activities having adverse effects on third-party vendor systems utilized by the company. Counsel can help ensure that the terms of the program are carefully drafted to avoid these risks and are regularly reevaluated to address new or unexpected issues.

Non-Escalation of an Incident – Failure to realize that the bug bounty program has turned into, or uncovered, a formal cybersecurity incident can lead to the violation of legal and regulatory cybersecurity requirements.

Goals of Bug Bounty Programs vs. Penetration Testing

- Bug Bounty Program Goals: to find potential bugs and points of exploitation.
- Penetration Testing Goals: to test external network surfaces for security vulnerabilities.



15. Third-Party Risk Management

Vendors, service providers, and other third-parties likely play an important role in your company, but these key relationships could also present unique cybersecurity and privacy risks if not managed and monitored diligently. Counsel may want to be involved in reviewing and overseeing these relationships to help minimize the risks.

Third-Party Risk

1. 71% of organizations say the number of third-parties with whom they do business has increased in the past three years and they expect that this number will continue to grow.
2. 83% of legal and compliance leaders say risks with third-parties arise and are identified only after initial due diligence.

The Importance of Third-Party Risk: Spotlight on Regulations

Regulators understand the key role that third-parties play for organizations, but also recognize the importance of ensuring that those relationships remain secure. As such, there are several regulations that impose requirements for third-party relationships. Counsel should continue to stay abreast of these regulations, and others, that may have specific requirements for third-party relationships.

FTC Safeguards Rule – Under the FTC's Amended Safeguards Rule, covered financial institutions must take "reasonable steps" to ensure vendors maintain proper safeguards, contract to require vendors to institute such safeguards, and periodically evaluate vendors for the adequacy of their safeguards.

NYDFS Part 500 – Covered entities are required to implement written policies and procedures that will ensure the security of information held by, or accessible to, third-party service providers. This includes conducting due diligence on third-parties.

SEC – The SEC's Issuer Cybersecurity Rules require public companies to disclose whether its cybersecurity risk management processes are designed to oversee and identify cybersecurity risk associated with third-party service providers. As of Fall 2023, the SEC's pending cybersecurity rules for other SEC registrants would require entities to impose certain cyber contractual provisions on third parties.

CCPA – Under the California Consumer Privacy Act, a "sale" of data is defined broadly to encompass "selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to a third party." This exchange of personal information to certain vendors, with the absence of certain contractual limitations, would make them third parties and requires businesses to offer an opt-out mechanism.

36 Hour Breach Notification Rule – Under the Federal bank regulatory agencies' "Final Rule," bank service providers are required to notify a designated contact at each affected banking organization as soon as possible after experiencing a computer-security incident.

GDPR – The EU and UK's GDPR imposes rigorous requirements for third party risk management depending on whether the third party is a "data controller" or "data processor" of the relevant personal data. These include requirements to conduct risk assessments and document the security controls and privacy standards of the third party, (for data processors) to monitor third parties for security risks, and to implement appropriate safeguards if personal data is transferred to a third party located outside of the EEA or UK respectively.

Other Regulations to Keep in Mind: HIPAA, PCI-DSS, SOX.

The Three Roles for Counsel in Third-Party Relationship Management

Advising on Diligence – Counsel will play a critical role in advising on the scope and procedure for third party diligence. Once the scope has been established, counsel should help draft the due diligence questionnaire to ensure it reflects the proposed scope. A great starting point is the Standardized Information Gathering (SIG) Questionnaire, which aligns with the most updated domestic and international regulatory guidance on third-party diligence requirements. When the questionnaire is returned, counsel should help ensure that any medium or high risks are remediated or mitigated accordingly.

Crafting Contractual Terms for Third-Party Agreements

Counsel will help craft the minimum acceptable contractual terms for vendor contracts. This stock language can also be incredibly beneficial when negotiating with vendors. Review an assortment of third-party agreements and select a few different samples to have on hand for different types of vendor relationships. You should also track any contractual clauses you agree to that differ from your standard terms.

Counsel should also be prepared to review and respond to any contracts that the company receives from third parties, including vendors and clients. It may be helpful to prepare a checklist of key points to look out for, including any stock responses or mandatory contractual terms, to speed up the process.

Third-Party Breaches – Counsel should be alerted to, and prepared to respond to, any third party cyber or privacy breaches that affect the company's data. Counsel should compile a checklist of questions for the third-party in anticipation of this scenario, and be aware of which of the company's regulators it would have to notify in the event of a third-party breach, and the timeframe for doing so.

16. Corporate Transactions: Cyber Diligence Integration

Nearly every transactional deal requires cybersecurity and privacy diligence to understand the key cybersecurity issues faced by the target, including its technical frameworks for identifying, treating, and managing cyber risk. While information security teams are tasked with a review of technical controls, often they are not given hands-on access to assess those controls. Counsel are uniquely positioned to work alongside the InfoSec teams to spot potential issues through the target's reports, regulatory reviews, and other documentation. Counsel can then communicate these concerns to the management team in a clear and non-technical description so they can help evaluate the transaction and address any transition.

Cautionary Tales

In 2016, Verizon was in the process of purchasing Yahoo. In the course of diligence, Yahoo disclosed that it had undergone three major data breaches. As a result, its sale price to Verizon was discounted by **$350 million, the Yahoo CEO took a multi-million dollar haircut on her bonus, and the General Counsel resigned**.

In 2014, the guest reservation system of the Starwood hotel group was compromised, which exposed the data of 339 million individuals. This data breach was not discovered until **2018**, after Marriot had acquired Starwood. The **ICO then fined Marriot over £18.4 million** for failure to process personal data in a secure manner after the acquisition and once the GDPR came into force.

Risks That May Affect the Value of the Target Company

Legal Risks

- Post-close regulatory enforcement or litigation.
- Additional steps needed to comply with existing law.

Cyber Risks

- Existence of undisclosed and still unknown incidents.
- Likelihood of future incidents.

Practical Risks

- Remediation costs for noncompliance or existing vulnerabilities.
- Whether data sought in the transaction can be used as intended.
- Reputational risks from incidents or system vulnerabilities.
- Costs associated with integrating inconsistent or incompatible security measures.

Six Deal Areas for Counsel to Be Involved With

1. **Diligence Oversight** – Counsel can help draft appropriate cybersecurity diligence questionnaires and review the responses. While the scope and type of cyber diligence is tailored to the target's business, key areas of review may include the target's:
   - Compliance with applicable cybersecurity laws;
   - Controls, monitoring and testing for key systems and data sets;
   - History of cyber incidents and investigations or complaints;
   - Documented cyber policies and plans, and whether they are tested;
   - Network and system tests, audits and assessments;
   - Vendor risk management practices and policies;
   - Cyber insurance coverage; and
   - Board and senior management briefings on cybersecurity.

2. **Drafting the Diligence Issues List** – It is not enough for counsel to identify areas in which the target faces cybersecurity risks; these risks then need to be effectively communicated to management in a way they can understand, so they can be mitigated accordingly. Counsel may, therefore, be involved in drafting a summary of the cybersecurity issues identified in the diligence process, and proposing proportionate mitigatory measures.

3. **Drafting Purchase Agreements** – Counsel can assist with the drafting of the purchase documentation to ensure that the liability for any cyber issues identified in the diligence is appropriately allocated between the parties. Such issues may be addressed through reps and warranties, pre- or post-closing covenants, special indemnities and closing conditions. Counsel should also consider whether the company should obtain rep and warranty insurance for any cybersecurity-related provisions.

4. **Maintaining Awareness of the Target's Legal & Regulatory Environment** – The legal and regulatory environment for cybersecurity is rapidly evolving, and the acquirer may be liable for the target's non-compliance once the transaction has occurred. To minimize the changes of this happening, counsel should help monitor any upcoming changes to the target's legal or regulatory cybersecurity requirements to ensure that any developments are flagged and responded to pre-completion. Counsel can enlist outside counsel and a third-party consultant to identify threat intelligence regarding the target and to perform a public-facing scan for vulnerabilities. *See Compliance with the Legal Landscape chapter for more information.*

5. **Increase the Target's Cyber Monitoring at Key Milestones** – It is increasingly common for threat actors to time the execution of ransomware attacks in connection with the signing or completion of a deal to exert maximum leverage, or to launch wire diversion attacks in anticipation of upcoming fund transfers. Counsel should work with the Information Security teams to ensure that the target is subject to an appropriate monitoring at key milestones in the transaction timeline.

6. **Facilitating Integration** – The company and the target should prepare to face additional cybersecurity risks once the transaction has completed, as the company works to integrate the target and align the target's software, systems and policies and procedures with its own processes. Counsel can help coordinate the process by identifying all the integration workstreams, and clearly allocating responsibility for them to bespoke working groups. Counsel should set up regular check-in meetings with the working groups to monitor and ensure timely completion of the integration efforts.



17. Other Topics of Interest

Cybersecurity is a vast, multifaceted subject area that cannot be condensed into one desk guide. In our final chapter we highlight other topics of interest that should be on the radar of counsel. The Debevoise Data Strategy and Security Team is always happy to discuss these issues in further detail.

Takedowns – Scam websites, domains and social media pages are a common tool used by unauthorized actors to perpetrate fraud or other malicious attacks. Counsel may want to consider how the company would respond when it discovers the existence of a website, domain or social media page that is designed to impersonate the company or one of its employees. There is value in responding as quickly as possible to any spoofed domains or fake websites or social media pages to minimize the risk of any harm to individuals who interact with these pages and who may believe they are legitimate.

Electronic Communications – Counsel should consider the company's policies and procedures surrounding the use of personal devices or messaging apps to conduct business, and how these communications are captured and recorded. Different approaches may be required depending on existing practices and the communication tools being used. In particular, counsel may want to consider regularly reviewing and tailoring the company's electronic communication policies and procedures, especially to adapt to new communication apps and changing work practices, and asking staff to provide a specific periodic attestation that they are adhering to the procedures.

Lost Devices – Counsel should consider the need for internal policies and procedures regarding the steps the company will take if and when work devices are "lost." These may address reporting requirements around events that are not obviously cyber events or that may be viewed as minor and not worth reporting, such as a temporary loss of control over a mobile device. Infosec can be a helpful partner regarding "bricking" or remote wiping electronic devices in these circumstances.

Responding to Phishing, Smishing and Vishing – Phishing (emails), smishing (texts) and vishing (phone calls and voicemails) are common entry points for threat actors into your internal company systems as they target human error, one of the top causes of cybersecurity incidents. However, there are nuances in responding to these types of attack that may not be included in your company's standard incident response plan. As counsel, you may be involved in implementing a tested response plan for phishing, smishing or vishing attacks.

Wire Diversions – Wire fraud and diversion scams (some of which take the form of so-called Business Email Compromise scams) typically arise when a threat actor has obtained payment invoices (that are either directed to the Company, or are from the Company directed to third parties) and uses those details to deceive a payor into transferring money to the threat actor instead of the intended recipient. Counsel may be involved in drafting policies and procedures for identifying and responding to potential wire diversions. This may include a "kill chain protocol" to request a recall or reversal of any fraudulently transferred funds.

Vulnerability and Patch Management – All software applications contain vulnerabilities. To ensure appropriate direction of attention and resources, companies can often benefit from taking a risk-based approach to vulnerability and patch management practices – with the goal being to minimize the attack surface of systems, applications, and services, and to identify new vulnerabilities and potential fixes on a regular basis. Similarly, companies can actively work to phase out "legacy" or "end-of-life" systems, for which updates and patches are no longer being developed. Counsel can assist in implementing an appropriate risk-based approach to vulnerability and patch management that is appropriate for company's potential exposure and risk appetite.

Risk Assessments – A risk assessment is a process undertaken to identify and evaluate the cybersecurity risks faced by a company and to analyze the effectiveness of defenses and mitigation measures implemented to protect against those risks. The assessment usually categorizes identified risks based on severity and specifies potential third parties who might be implicated in the event of an actual cyber-incident. Counsel can benefit from having a thorough understanding of what is required in a risk assessment process and should be familiar with the components of their own company's risk assessment.



Glossary List

36 Hour Notification Rule – Federal bank regulation requiring certain financial services providers to notify a designated contact within 36 hours of a qualifying cybersecurity incident.

Bug Bounty – Programs where organizations pay outside actors when they detect cybersecurity vulnerabilities.

CCPA – California Consumer Privacy Act. State law, effective 2020, implementing certain privacy rights to California residents and regulations on groups doing business in California.

CISO – Chief Information Security Officer. C-Suite executive responsible for cybersecurity.

Cloud – Term for off-premises IT systems.

COPPA – Children's Online Privacy Protection Act. Federal law imposing requirements on operators of websites directed to or knowingly collecting personal information online from children under 13 years of age.

CPRA – California Privacy Rights Act. State law, effective 2023, amending CCPA to impose further privacy requirements on businesses in California, and creating the California Privacy Protection Agency to implement and enforce state privacy laws.

Cybersecurity by Design – Approach to business operations wherein all corporate procedures and activities consider cybersecurity in the first instance.

Cybersecurity Mitigation – Tools and procedures set in order to minimize the impact of a successful cybersecurity incident.

Data Controller – Under the GDPR, an entity which "alone, or jointly with others, determines the purposes and means of the processing of personal data."

Data Processor – Under the GDPR, an entity "which processes [i.e. analyzes, collects, stores, transmits, or otherwise uses] personal data on behalf of the controller."

Data Hygiene – Process of ensuring organizations do not collect or store unnecessary, inaccurate, or old data that may violate cybersecurity regulations.

Data Minimization – The principle that entities should limit the collection of personal data to what is directly relevant and necessary to accomplish the specified purpose for which it was collected, and retained only as long as necessary to fulfill that purpose.

DOJ – the U.S. Department of Justice. The legal unit within U.S. federal law enforcement.

DOJ Civil Cyber Fraud Program – DOJ program, with whistleblower incentives, that investigates companies for fraudulent statements about cybersecurity.

EEA – European Economic Area, consisting of all EU Member States plus Iceland, Liechtenstein, and Norway, to which the EU GDPR applies. Note that the law also applies to businesses established outside the EEA but with certain operations within the jurisdiction.

FBI – Federal Bureau of Investigation. Th enforcement unit within U.S. federal law enforcement.

FS-ISAC – Financial Services Information Sharing and Analysis Center. Financial services trade group which provides forum for sharing cybersecurity intelligence.

FSSCC – Financial Services Sector Coordinating Council. Financial services trade group which provides forum for sharing cybersecurity intelligence.

FTC – Federal Trade Commission. Federal U.S. consumer protection agency, prosecutes companies for cybersecurity weaknesses that harm U.S. consumers.

FTC Safeguards Rule – FTC regulation imposing cybersecurity obligations, including annual reporting, on covered entities.

GDPR – The General Data Protection Regulation 2016, as incorporated into EEA and UK law. The GDPR governs how the personal data of individuals in the EEA and UK respectively may be processed and transferred by businesses.

GLBA – The Gramm-Leach-Bliley Act of 1999. U.S. law which requires financial institutions to safeguard sensitive consumer data and imposes reporting requirements.

HIPAA - Health Insurance Portability and Accountability Act. U.S. law which imposes cybersecurity obligations on anyone with certain sensitive health information.

IAPP - International Association of Privacy Professionals. A data privacy trade group.

ICO – the UK's Information Commissioner's Office. UK regulator which upholds information and data privacy rights, and enforces regulations.

InfoSec – Information Security. May refer to a business' information security posture (i.e. the physical and environmental security, access control, and cybersecurity) or be a shorthand reference to the Information Security team.

IOC – Indicator of Compromise. A piece of digital forensic evidence that suggest that a device or network may have been compromised.

IoT – Internet of Things. Refers to a network of objects that can connect to the internet, interact with each other, and freely exchange data and information (e.g. cars, fridges).

IR – Incident Response. Shorthand term referring to individuals involved in or actions taken pertaining to cybersecurity incidents.

IRP – Incident Response Plan. A bespoke document or set of documents meant to guide an organization's response to a comprehensive range of cybersecurity incidents. Different teams (for example, technical incident response, C-Suite, and operational teams) often have different IRP documents.

ISAC – Information Sharing and Analysis Center. Sector-specific fora for collection, analysis, and dissemination of threat intelligence.

MFA – Multi-factor authentication. Cybersecurity tool where users must verify their identity with at least two tokens in order to access a network or system.

NAIC - National Association of Insurance Commissioners. Insurance trade group with cybersecurity wing.

NCSC – UK National Cyber Security Centre. Government agency that provides advice, guidance and support on cybersecurity.

NIST Framework – National Institute of Standards and Technology Cybersecurity Framework. A voluntary set of organizational cybersecurity recommendations considered the gold standard for industry compliance professionals.

NYDFS – New York State Department of Financial Services. State regulator with cybersecurity responsibilities.

NYDFS Part 500 – A New York State regulation establishing cybersecurity requirements for financial services companies.

NY Shield Act – State law imposing cybersecurity notification requirements on covered entities doing business in New York.

Notification – Standardized communications to regulators, individuals, and third-parties regarding a cybersecurity incident. Legal and contractual obligations often set the form, content, and timing of notifications.

OOB – Out of bands communications. A method for employees to communicate outside of corporate channels. Often used during cybersecurity incidents when corporate channels are compromised.

PCI-DSS – Payment Card Industry Data Security Standard. Industry cybersecurity standard for credit card transactions.

Phishing – The practice of sending emails pretending to be someone else in order to gain access to a private network or to obtain sensitive information.

PII – Personally identifiable information. Term referring to sensitive information that may be linked to an individual and is protected by various cybersecurity regimes.

Privacy-by-Design – Approach of integrating data privacy considerations into entire lifecycle of business activities.

Ransomware – Cybersecurity attack where the threat actor compromises an organization's IT systems and threatens adverse action (widespread distribution of exfiltrated data, permanent encryption of organization's IT) unless target group pays a ransom.

SaaS – Software as a Service. Business model of selling access to software platform.

SEC – Securities and Exchange Commission. Federal agency that regulates public companies (including some financial services providers), broker-dealers, investment advisers, trading exchanges, and other securities market participants.

SEC Issuer Cybersecurity Rules – SEC rulemaking imposing additional cybersecurity and reporting obligations on public companies in the U.S.

SIFMA – Securities Industry and Financial Markets Association. Financial services trade group which provides forum for sharing cybersecurity intelligence.

SIG – Standardized Information Gathering (Questionnaire). Widespread industry tool disseminated by nonprofit "Shared Assessments" to collect and share cybersecurity information.

Smishing – The practice of sending text messages pretending to be someone else in order to gain access to a private network or to obtain sensitive information.

SOC – Security Operation Center. A centralized function within an organization employing people, processes, and technology to continuously monitor and improve an organization's security posture while preventing, detecting, analyzing, and responding to cybersecurity incidents.

SOC-2 – A voluntary compliance standard for service organizations, developed by the American Institute of CPAs (AICPA), which focuses on a business's non-financial reporting controls as they relate to Security, Availability, Processing integrity, Confidentiality, and Privacy.

Social Engineering – The practice of using psychological manipulation to gain access to a private network or to obtain sensitive information.

SOX – The Federal Sarbanes–Oxley Act of 2002. Imposes cybersecurity and reporting obligations to covered entities.

TTX or Tabletop – Tabletop Exercise. An exercise and/or training session where an outside facilitator gathers stakeholders to test the organization and IRP reaction to a simulated cybersecurity incident. Tabletops often highlight areas for improvement in company security and chains of command.

Takedown – Preventative measure for legitimate organizations to take against fraudulent actors impersonating them.

Threat Actor – Term referring to perpetrator of cybersecurity attack.

Vishing – The practice of sending voice calls pretending to be someone else in order to gain access to a private network or obtain sensitive information.