Time to Update Cyber Incident Response Plans, Especially for Banks Subject to the New 36-Hour Breach Notification Rule

January 19, 2022

The Value of Cybersecurity Incident Response Plans

As cyberattacks continue to plague U.S. companies, cybersecurity remains a core risk, even for businesses that have invested heavily in technical measures to protect their systems. As a result, cybersecurity best practices have evolved to include not only preventative measures, but also robust preparations for responding to cyber incidents, so that companies can improve their resilience, decrease the time it takes to detect and effectively respond to an attack, and reduce the overall damage. Because nearly every company will at some point face a successful attack, regulators, insurers, auditors, and investors view an incident response plan ("IRP") as a key element of a reasonable cybersecurity program.

Part of the value of an IRP comes from the process of drafting it, which involves making decisions about how an incident will be handled (e.g., who should be drafting communications to impacted employees, who has the authority to shut down parts of the network, which incidents will be escalated to senior management, etc.). Determining these issues over the course of several weeks while drafting the IRP and consulting with the relevant individuals is much better than working through them for the first time under the stress and time constraints of an actual incident. Well-drafted IRPs also provide checklists of things to do when an incident occurs (e.g., preserve evidence, contact the FBI, notify the insurer, draft a public statement, determine a point-of-contact for external inquiries, etc.).

Increasing Regulatory Requirements for IRPs

Many cyber regulations and standards also expressly require written IRPs. For example:

- Part 500.16 of the NYDFS Cyber Rules requires regulated entities to have an IRP that is designed to promptly respond to, and recover from, any material cybersecurity

event and that provides for clear roles, responsibilities, and levels of decision-making authority.

- The National Association of Insurance Commissioners (NAIC) Insurance Data Security Model Law (MDL-668) requires licensees to establish a written incident response plan as part of its information security program.

- As part of a significant update to the Safeguards Rule, the FTC requires covered financial institutions to adopt a written incident response plan that is designed to assist in responding to, and recovering from, a security event. The revised rule became effective on January 10, 2022.

- The HIPAA Security Rule also requires a covered entity to implement policies and procedures to address security incidents.

Shrinking Deadlines for Breach Notification

Another important reason to have an effective IRP is that it can assist companies in meeting their breach notification deadlines, which are getting shorter. For example, both the NYDFS Cyber Rules and the European GDPR breach notification requirements have a 72-hour deadline. As anyone working in this field knows, meeting those requirements can be extremely challenging, and having a clear protocol for escalating incidents, drafting the notifications, and obtaining the necessary approvals can make the difference between (1) meeting your notification deadline and gaining credibility with the applicable regulator, and (2) missing the deadline and starting off having to explain to the regulator why the notification was late, which can undermine the regulator's view of the overall competence of the response.

Accordingly, having an effective breach notification section of an IRP is especially critical for financial institutions that are subject to the federal bank regulatory agencies' new 36-hour *Final Rule on Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers* ("Final Rule"), which we covered in depth in a November 2021 Data Blog post and discuss further below.

Why Many Companies Don't Use Their IRPs During Incidents

Our experience over the last several months has shown that many companies do not actually use their IRPs during cyber incidents because they are either too long or too technical, or because they have not been revised recently and therefore are not helpful

for responding to the current threat environment. In addition, many IRPs are overly prescriptive and do not permit sufficient flexibility when companies face an incident involving novel threats, tactics, or vulnerabilities. In such cases, not only are the IRPs of no assistance at the time they are most needed, but they actually put the company at risk of regulatory noncompliance, or at least of having to explain to regulators why the IRP was not followed. Likewise, it is now a common part of cyber diligence to ask whether the company followed its IRP during a recent significant incident.

Tips for Updating IRPs

Companies should therefore consider reviewing and updating their IRPs, and then testing them with a tabletop exercise using a specific scenario to see whether the revised IRPs prove to be helpful during an incident.

Key considerations when evaluating and revising IRPs include the following:

- **Usability**: The IRP should be clear, practical, well-organized, and easy to use by all teams involved in a typical incident. It should be actionable at a tactical level and avoid theoretical, policy-type statements that make it harder to use in "break glass" situations.

- **Flexibility**: The IRP should recognize that not all incidents and responses can be anticipated, and therefore provide guidance and recommended actions, but avoid being too rigid in mandating that certain steps must be taken (or must not taken) without exception. The IRP should also account for how deviations from a general mandate should be documented.

- **Clearly Defined Roles and Responsibilities**: The IRP should define the response teams, their respective levels and responsibilities, and the flow of incident escalations. Consider also listing the core incident response team members, their contact information, their team assignments, and their individual responsibilities, as well as anyone who will be added to the core team for specific types of incidents.

- **Triggers for Escalation**: Consider defining how various types of cyber events should be categorized by severity level and whether and how they should be escalated within the organization.

- **Separate Playbooks for Different Kinds of Incidents**: Different types of incidents require different responses. Some attacks do not involve the compromise of data, and are largely handled by technical teams (e.g., DDoS attacks and cryptojacking). Other

attacks often merit a less involved role for the information security teams, but require significant involvement from legal and privacy teams (e.g., a vendor breach, misdirected email containing sensitive personal information, compromise of a personal email account containing material nonpublic company data, etc.). For this reason, regulators have encouraged companies to create, in addition to the general IRP, checklists or playbooks for different kinds of incidents. For example, in June 2021, the NYDFS released its Ransomware Guidance, which provided that regulated companies should have an IRP that explicitly addresses ransomware attacks, and "that plan should be tested, and the testing should include senior leadership—decision makers such as the CEO should not be testing the incident response plan for the first time during a ransomware incident."

- **Draft Communications**: Consider including draft internal and external communications (e.g., press releases, employee alerts, and customer notifications) for various types of incidents, so the company is not scrambling to draft those communications from scratch during an actual incident.

- **Outside Resources and Contacts**: Consider including a list of outside resources that are available to the company during an incident (e.g., cyber forensic firm, ransomware negotiator, crisis communications firm, document review vendor, outside legal counsel, etc.) along with the contact information for the relevant individuals. Also consider including the contact information for any insurers, auditors, law enforcement officers, and regulators who may need to be notified.

- **Disclosure and Notification Requirements**: Consider including the categories of likely notification obligations to individuals and regulators in the event of a data breach (including any contractual notification obligations), along with some of the more common requirements for notification. For incidents that may trigger tight notification deadlines (e.g., the new 36-hour rule for U.S. banks discussed further below), the IRP should also include protocols for quick evaluation, escalation, drafting, and approvals, so that the deadline can be met.

- **Data Management**: Consider including a section of the IRP on data preservation, issuing legal hold notices, chain of custody forms, and other aspects of evidence handling and data management that may be relevant to the incident.

- **Lessons Learned**: The IRP should provide that, following an incident, steps are taken to ensure that appropriate remediation measures are completed, the incident is properly documented, and that lessons learned from the incidents are used to update training and policies, including the IRP.

Modifying IRPs for the 36-Hour Breach Notification Final Rule for Banks

Under the Final Rule, starting on May 1, 2022, covered banking organizations must notify their primary federal regulator of any "computer-security incident" that rises to the level of a "notification incident" no later than 36 hours after determining that a notification incident has occurred. A "computer-security incident" is an event that results in actual harm to an information system or the information contained within it. A "notification incident" is a computer-security incident that is reasonably likely to materially disrupt or degrade a banking organization's operations (i) affecting a material portion of its customer base; (ii) resulting in a material loss of revenue, profit, or franchise value; or (iii) posing a threat to the financial stability of the United States.

Meeting this 36-hour deadline will be challenging because incidents that could trigger the 36-hour notification requirement will have to be almost immediately escalated to the individuals responsible for drafting, approving, and submitting the notification. Companies that are subject to the 36-hour deadline should consider the following preparations for implementation of the Final Rule, which may be memorialized in an updated IRP:

- **Scope of Rule's Application**: Determining which entities in their group are subject to the Final Rule and, if the Final Rule only applies to some entities, assessing which data, information systems, and employees are associated with the covered entities.

- **Agency to Notify**: Determining which of the federal banking agencies the financial institution should contact as its primary regulator in the event of a notification incident, along with the individual at that agency who would be contacted and that individual's up-to-date contact information.

- **Responsible Persons**: Determining who at the financial institution is the person responsible for making the notification, and who else, if anyone, must approve the notification before it is made. It may be prudent to designate more than one person for each of these roles, in case someone is unavailable.

- **Prompt Escalation**: Determining which incidents may trigger the 36-hour notification requirement and therefore should be escalated to the persons responsible for that notification, as well as who should be making that escalation.

- **Notification Template**: Companies should create a sample notification, so that the actual notification does not need to be drafted from scratch during an incident.

To subscribe to our Data Blog, please click here.

* * *

Please do not hesitate to contact us with any questions.

WASHINGTON, D.C.

Luke Dembosky
ldembosky@debevoise.com

NEW YORK

Avi Gesser
agesser@debevoise.com

Johanna N. Skrzypczyk
jnskrzypczyk@debevoise.com

Andres S. Gutierrez
asgutierrez@debevoise.com

Michelle Huang
mhuang1@debevoise.com

Michael R. Roberts
mrroberts@debevoise.com