JUNE 25, 2018

Legaltech® news

ONLINE

An ALM Publication

What to Consider When Developing or Refining Your Cyber Incident Response Plan

Recent events show that companies should consider instituting and strengthening plans for when—not if—they suffer a cybersecurity incident.

BY MICHAEL LEITER, JOE MOLOSKY AND MICHELLE WEINBAUM, SKADDEN

It is now commonplace to state that there are only two kinds of companies: those that have been the target of a cyberattack and those that will be. Another way to think about this statement is that regardless of how good an organization's cyber defenses may be, cyber breaches—whether caused by an external actor, insider threat, or otherwise—are almost certain to occur. From this perspective, it is imperative not only that organizations have world class defenses, but that they also have equally mature incident response plans to mitigate the effects of any breach.

Recent events underscore the importance of preparation in mitigating a cybersecurity incident. For example, when shipping firm Maersk suffered an attack during the major NotPetya malware events, the company contained the attack within approximately one day and restored normal operations in ten days—drastically limiting the overall cost of the incident to Maersk. On the other hand, other recent incidents, such as the data breach Equifax suffered, have demonstrated the negative outcomes from not having a thorough plan in place.

The likelihood of cyber preparedness having practical effects on companies is highlighted by reports that attacks are increasing from year to year. In 2017, companies publicly disclosed over 5,000 data breach incidents—an increase of over 850 incidents from 2016. Given this growing number of incidents, it is imperative that companies be familiar with industry standards and best practices to prepare effectively for and mitigate cybersecurity incidents. The following are several key areas for consideration when developing or refining a cybersecurity incident response plan.

Build a Truly Strategic Incident Response Team

A company should think strategically and include individuals with a wide range of competencies when forming an incident response team. The team should of course include individuals with technical responsibilities as well as individuals with legal, compliance, human resources, operations, and communications responsibilities.

More often overlooked, however, is the inclusion of treasury and finance, government relations teams, and other administrative support leads. Although not every office will be involved in every incident, disruptive cyber attacks may well require coordination amongst offices that are not traditionally thought of as core to security issues.

Moreover, companies should consider what service providers may be needed to assist their internal incident response team, such as outside counsel, forensics providers, public and government relations firms, and credit monitoring providers. It is also important for companies to consider establishing relationships with these providers in advance of a security incident to ensure responses are efficient and effective.

Inform Response Plans through Threat Profiles

Companies should identify the specific types of threats they face to guide the creation of well-tailored incident response plans. For example, the most common causes of cybersecurity incidents include phishing, hacking, malware, human error, and misuse of lost or stolen devices.

Preparing specific written plans for classifying and addressing each of these scenarios can enable companies to allocate resources and prioritize events. Such plans will also allow for a more uniform and complete response to cybersecurity incidents. In addition, companies should periodically update these preparations as cyber threats continue to evolve. For example, although many companies have long focused on denial of service attacks, many were caught less-than-fully-prepared in 2017 as ransomware became a more common occurrence.

Prepare Legal Notifications for Security Incidents

One of the most important tasks a legal department manages during a cybersecurity incident is the multitude of legally-required notifications to consumers, regulators, customers, and other third parties. Companies should have clear guidelines and document requirements for these communications in advance of security incidents, and given the rapidly evolving legal and regulatory landscape, such preparation should be regularly reviewed.

In general, company guidance should cover clearly what parties should be notified and in what situations notices should be sent. Preparing form documents and templates in advance can also be helpful for reducing costs and time for distributing notices to state regulators and consumers and preparing talking points and FAQs for use with customers, consumers, the media, and other third parties. The ability to address these requirements quickly and accurately is critical given the increased U.S. and international focus (e.g., the European Union's General Data Protection Regulation or GDPR) on rapid notice (e.g., 72 hours).

Test and Revise Plans

Companies should take the time to regularly test and assess their incident response plans to ensure that they include adequate policies and procedures to comply with constantly changing legal and business risk requirements. In many cases, conducting a tabletop exercise or other active training can be an effective way to test and refine technical functions of cybersecurity responses as well as company policies and procedures, such as recordkeeping requirements.

These exercises also provide an opportunity for company leadership and incident response team members to test communication including information coordination and sharing between team members, upward reporting, coordination with service providers and outside counsel, and the ease of accessing and using notification templates. Finally, given inevitable leadership turnover and changing technical capabilities, regular exercises are

valuable in making sure that the team that is in place for an actual incident has previously exercised plans together.

Connectivity with the Board

Oversight of a company's preparation for and mitigation of cybersecurity incidents ultimately resides—like other risks—with the Board, and members must be fully prepared to fulfill their fiduciary duties. Board members thus require briefings and appropriate training to help them stay abreast of their fiduciary duties and the company's legal and regulatory requirements related to cybersecurity and incident response.

Board members should receive cybersecurity-specific corporate governance training from their company's general counsel or their outside counsel, as well as an appropriate, high-level understanding of their company's incident response plans. Directors of public companies have added responsibilities to ensure their companies meet the Securities and Exchange Commission's enhanced disclosure requirements, as well as their personal responsibility to understand insider trading issues that have arisen in the context of cyber incidents.

Conduct Post-Incident Evaluations

Finally, following a security incident, companies should evaluate and document what occurred and the lessons learned from the incident. The lessons learned process should include answering questions that will help the organization to improve the incident response plan and other information security policies and procedures, such as:

- What caused the security incident and when did the incident occur?
- What was the impact on the company, its employees, its customers, and its service providers?
- How well did incident response team members and employees follow procedures?
- Did the policies and procedures adequately address the incident and conform to all legal requirements?
- How effectively was information collected and disseminated about the incident?
- Is the incident indicative of any cyber threat trends that require modification of the policies and procedures?
- Should contracts with vendors or customers be updated based on the lessons learned?

Equally critical, the management team should ensure that the company follows up with steps to mitigate any identified shortcomings. Absent doing so, the company will remain vulnerable or ill-prepared, as well as increasing the likelihood of adverse legal or regulatory action.

Key Takeaway

Recent events show that companies should consider instituting and strengthening plans for when—not if—they suffer a cybersecurity incident. Having a thorough, documented plan in place that incorporates these considerations can significantly improve a company's ability to adhere to legal and regulatory requirements when responding to security incidents. It can also improve a company's bottom line and protect its reputation.

Michael Leiter *represents clients in matters involving U.S. national security and cybersecurity, cross-border transactions and government investigations, with a focus on the defense, intelligence and technology sectors.* ***Joe Molosky*** *advises clients in a variety of transactional, regulatory and litigation matters, including cross-border transactions, regulatory proceedings, and privacy and cybersecurity issues. His practice focuses on national security reviews before the Committee on Foreign Investment in the United States (CFIUS), cybersecurity compliance and incident response, data privacy, national security, and consumer protection issues as well as internal and government investigations.* ***Michelle Weinbaum*** *is a CFIUS associate in Skadden's Washington, D.C. office.*