Bloomberg BNA

Corporate Law & Accountability Report™

CYBERSECURITY

Companies Should Heed DOJ's New Cybersecurity Guidance to Minimize Liability

BY KATHRYN ALLEN AND DANIEL FARRIS

The Department of Justice (DOJ) has released new guidance on cyber preparedness and incident response, becoming the latest federal agency to do so in recent months (13 CARE 1101, 5/22/15). Newly sworn-in Attorney General, Loretta Lynch, has indicated that the investigation and prosecution of cyber crimes will be one of the top priorities of her administration (13 CARE 921, 5/1/15). Although the Guidance sets forth only voluntary standards, companies wishing to minimize potential liability in enforcement actions and/or civil litigation should take notice.

In releasing its "*Best Practices for Victim Response and Reporting of Cyber Incidents*," the DOJ's Cybersecurity Unit called upon law enforcement and private industry to share in the effort to improve systems that protect consumer information (13 CARE 1086, 5/22/15). The Guidance sets forth detailed steps to improve cybersecurity and breach response at all stages within the breach lifecycle, ranging from preparation and deterrence to incident notification, response and, ultimately, remediation.

The DOJ standards are being viewed by many industry observers as the new benchmark against which corporate cyber-incident preparedness and response efforts may be measured. Although the proposed standards may not apply to all organizations in all instances, companies of all sizes would be ill-advised to ignore them. Failing to analyze the best practices and proactively implement applicable standards may leave companies open to accusations from regulators, class action plaintiffs and even shareholders for failing to satisfy this new standard of care as set forth by the DOJ.

Kathryn Allen is an attorney in the Data Center and Infrastructure Practice Group of Polsinelli and focuses her legal practice on the often-intersecting areas of information security/privacy, technology licensing/use, and intellectual property protection and monetization. Based in the firm's Kansas City office, Allen can be contacted at 816-572-4884 or at kallen@polsinelli.com.

Daniel Farris is a former software engineer and Co-Chair of Polsinelli's Privacy and Data Security Team, offering his clients real-world experience in fiber optic networking, data center operations, cloud computing, mobile app development, and data privacy and security matters. Farris, who is based in the firm's Chicago office, can be reached at 312-463-6323 or at dfarris@polsinelli.com.

Although the proposed standards may not apply to all organizations in all instances, companies of all sizes would be ill-advised to ignore them.

Implementation Issues

Implementing the standards, however, may prove more difficult and costly than some would expect. Many small-to-mid sized companies may lack the financial resources necessary to hire outside experts and invest in new technology that is not core to their business objectives. And while large companies likely have the financial wherewithal, their systems are large, sophisticated

 ISSN 2330-6300

and disparate, which can make consistent application of the standards more challenging. Still, failing to abide by the DOJ's step-by-step approach could leave companies that experience a breach open to new theories of liability and new claims of negligence.

The key for most organizations will be to focus on preparedness and breach prevention. Companies should not only harden their systems, but engage internal and external experts early, before a breach occurs. As some commentators have noted, there seems to be ''sort of a gold-rush mentality'' when it comes to privacy and data security. It is important for companies to not only make a plan, but to be sure to ask their outside lawyers, accountants and consultants to demonstrate their substantive knowledge and experience handling data preparedness and breach response efforts.

Managing Cybersecurity

Issues of privacy and data security, and how to manage cybersecurity effectively for an organization, can be confusing. Tailoring a cybersecurity and incident response plan to fit the organization's size, business climate, regulatory environment and, perhaps most importantly, budget is key.

Calculated Preparation

■ **Identify the organization's most prized assets.** Determine which of the data, assets and services warrants the most protection and how to protect each class of assets differently.

■ **Create a clear, concise and actionable response plan.** Identify the lead response people throughout the organization's key departments, such as legal, public communications, information technology and security, who will drive the response plan and work with those leads to craft a response plan that is unique to the organization's structure and needs.

■ **Prioritize mission-critical processes.** Work within the organization and with outside technical specialists to identify what data, networks or services are mission-critical to the organization's continued business, and prioritize those items within the response plan to ensure operational continuity during a time of crisis.

■ **Establish important relationships.** During any cyber incident, time is of the essence; therefore it is important to establish relationships with and identify contacts within law enforcement and governmental organizations as well as other computer incident reporting organizations before any incident. Establish these contacts and drafting a set procedure with each outside organization that will maximize them as a resource to the company in the event of a cyber incident.

Support During Crisis

■ **Keeping records and logs.** Things can get very hectic during a cyber incident, so it is very important to keep detailed records of whatever steps are taken and costs are incurred to mitigate damage. Determine what information will be important when recovering damages from responsible parties and for any criminal investigation that results.

■ **Communication with state and federal law enforcement.** Identify the appropriate law enforcement agencies, such as the Department of Homeland Security and the National Cybersecurity & Communications Integration Center, who need to be contacted in the event of a cyber incident, and work with those agencies to maximize their resources and knowhow for the company.

■ **Technical and operational specialists.** For smaller organizations that do not have robust information or technical security resources, find a partner to assist in the onboarding and management of third-party professional incident response experts that the company needs.

■ **Notification of affected parties.** As of January 2015, at least 47 states have laws that require companies to notify customers when their data has been compromised by an intrusion (13 CARE 895, 5/1/15). Determine the company's obligations under each of these laws as well as additional implications if in a regulated industry.

Post-Incident Audit

■ **On-site review.** It is important to ascertain from those that were ''in the mix'' during a cyber incident what worked and what did not. Conduct post-incident reviews of the organization's employees and stakeholders, third-party contractors and governmental agencies to assess the strengths and weaknesses of the organization's performance.

■ **Recommendation for the future.** Cyber incidents can be very disorienting. Get the business back on track fast by minimizing lingering operational and reputational risks, and providing guidance on how to mitigate the revealed weaknesses in the organization's security so that such an incident does not happen again.

   ISSN 2330-6300