New York Law Journal
A NEW YORK LAW JOURNAL SPECIAL SECTION
Internal Investigations
An ALM Publication
WWW.NYLJ.COM
MONDAY, NOVEMBER 10, 2014

Special Considerations and Challenges In **Data Security Investigations**

BY JOSEPH I. LIEBERMAN, DANIEL J. FETTERMAN AND BRIAN S. CHOI

Recent high-profile cyberattacks have shaken corporate America's confidence in safeguarding critical electronic information, including sensitive customer and intellectual property data. Consumers and retailers alike remember the devastating cyberattack on Target last December, in which approximately 40 million cardholders and 70 million other customers were affected, on Home Depot in September, in which information of 56 million cardholders was compromised and, most recently on JP Morgan, in which information of 76 million households and seven million small businesses was compromised. The magnitude of the consequences is hard to overstate. The former head of the NSA and U.S. Cyber Command, Gen. Keith Alexander, said in a speech in 2012 that cyber crime is the "greatest transfer of wealth in history," estimating that U.S. companies lose approximately $250 billion per year to theft of intellectual property and another $114 billion resulting from cyber crimes.[1]

Companies that have been or may be subjected to cyberattacks, and their counsel, face numerous potential legal challenges, including the prospect of government and regulatory investigations and actions, as well as private lawsuits, targeting whether their electronic data were properly protected, their security systems adequate, their monitoring and detection procedures appropriate and their remediation efforts timely and sufficient.[2]

To deal with these challenges, it usually makes sense for such companies to conduct their own internal investiga-

JOSEPH I. LIEBERMAN *is senior counsel,* DANIEL J. FETTERMAN *is a partner, and* BRIAN S. CHOI *is an associate at Kasowitz, Benson, Torres & Friedman.*

tions to ascertain the facts as quickly as possible. By the time a company discovers a cyberattack has occurred, it may be left with the daunting challenges of figuring out who hacked its systems or stole its data, how they did it, what information was taken, whether the system remains vulnerable, and if the company is obligated to report the breach under a myriad of complicated state and federal laws. This article identifies a number of special considerations companies and their counsel should be aware of in connection with cybersecurity.

Expect Investigations From Agencies

Given their sophisticated nature and the widespread financial harm they inflict on companies and their customers, cyberattacks have become a priority for many enforcement agencies. Companies with a significant data breach or cyber intrusion therefore should expect and prepare for investigations by regulatory and enforcement agencies. Recently, for example, following JP Morgan's disclosure of a cyberattack, government regulators and agencies, including the U.S. Attorney's Office for the Southern District of New York, the Federal Bureau of Investigation, and numerous state attorneys general, announced that they were investigating the case.[3] Other regulators, including the Federal Trade Commission,[4] New York's Department of Financial Services,[5] and the relatively new Consumer Financial Protection Bureau,[6] also are active in combating cyberattacks.

Challenges of Cyberattack Investigations

Plan for an Investigation. As companies face increasing threats, and the potential for after-the-fact reviews of their cybersecurity protocols by regulatory and enforcement agencies, it is incumbent on their technology, legal and compliance departments to work together to develop a plan for potential incidents, including a plan for conducting a thorough and complete investigation, which will be credible to government regulators, the media and customers. Apart from ensuring there is appropriate technology to prevent a cyberattack, such a plan should include methods for detecting and remedying data breaches as quickly as possible, for immediately preserving electronic data and ensuring that IT systems are safe. The plan should identify in advance the qualified professionals who can assist in the event of a problem, including outside counsel knowledgeable about cyber issues, IT vendors who have the sophistication and tools to assist in detecting and preventing further cyber intrusion without altering data or interfering with preservation efforts, and media and crisis management consultants.

Preservation of Data. Following a potential cyber or data breach incident, it is of paramount importance that a targeted company immediately preserve all relevant data in a forensically sound manner. Counsel should retain a trusted forensic consultant who is experienced in working with sophisticated data systems to ensure that all data, no matter how complex, will appropriately be preserved. Preserving the data in the condition that it was discovered—and saving a record of the back-up tapes containing such data—are typically crucial to establishing credibility with the regulators who may descend upon the company shortly after the first reports of a data breach. If the integrity of such data is not maintained, regulators may question every action taken by the company thereafter. Most importantly, failure to preserve data will foreclose a company from the best opportunity to determine how a hacker initially entered its system, what the system's vulnerabilities are, the duration of the cyberattack (and whether it is ongoing), and what, if any, data were actually taken.

Understanding the IT Enterprise Landscape. To ensure a complete and credible investigation, counsel and IT personnel must have an intimate understanding of the company's IT enterprise landscape. It is crucial for an internal investigation team to invest the time and resources in obtaining detailed knowledge of the network, learning about the nuances of the IT architecture and confirming that all information concerning the data, devices, and servers are current.

Risks to Compromising an Investigation. Depending on the size and sophistication of the company, its Chief Technology Officer or IT team already may have conducted an initial investigation of the company's system following the discovery of an attack or breach, but outside counsel should not rely entirely on its findings or proposed solutions. Among other things, it is possible that certain insiders, who are familiar with the IT infrastructure and have privileged access to the system, may have facilitated an intrusion and corrupted data. Before ruling out any potential causes, counsel should remain vigilant in comprehensively reviewing data from all potentially relevant custodians.

State Data Notification Obligations

As data breaches increase in frequency, more companies need to navigate the myriad of state-specific data notification laws. Forty-seven states have enacted laws obligating businesses and other entities to notify affected individuals when a data breach concerning their personally identifiable information (PII) occurs. Twenty states also require that the particular state's attorney general receive notification. Many companies will encounter challenges in complying with the current

patchwork of state notification laws because certain state laws vary and at times conflict with one another, including as to what constitutes PII and when a business legally is required to notify its customers of a breach. For example, in Colorado, disclosure is required unless the misuse of data is "not reasonably likely to occur."[7] But in Massachusetts, the standard appears to be more stringent—notification is mandatory if a business knows or has reason to know that the PII was acquired by an unauthorized party *or* used for an unauthorized purpose.[8] There also is an ongoing discussion of creating a uniform federal standard, which would bolster the security of consumer information, streamline the data notification process, and focus on the promptness with which a business would be required to notify its customers.[9]

In the context of an investigation, it is therefore not enough for counsel to understand why or how a breach affected a company's security network; counsel also must determine whether the breach triggered the company's obligation, pursuant to the various state notification laws, to notify its customers or clients of the breach. Thorny legal questions will invariably arise concerning whether a breach that constitutes a bona fide cybersecurity incident has occurred, but is sufficiently limited in scope, such that there is no evidence that PII or other customer information has actually been stolen or is likely to be misused. At the very least, counsel will be required to engage in a thorough review of the evidence, analyze any compromised data against the relevant state notification laws, and determine whether to report the breach to customers and the appropriate authorities.

Crisis Management And PR Considerations

A cyber intrusion or data breach, especially at a large corporation, undoubtedly will be reported by major news outlets. But beyond the initial publicity, companies also potentially will face the intense scrutiny of aggressive regulators, frustrated customers, and dissatisfied shareholders. Counsel therefore should take steps to adroitly address media inquiries while remaining sensitive to various stakeholders whose interests will inevitably be affected by the cyberattack.

One of the traps that companies should avoid is issuing an overbroad statement too quickly in the hopes of quelling a sense of crisis. Issuing such a statement prematurely ultimately may hurt the company. Early reports from a crisis are often inaccurate. Counsel should not give much credence to either good or bad news, and rather should focus on facilitating the investigation of the cyber incident on all fronts, including issuing a litigation hold, preserving relevant data, retaining experienced forensic consultants, coordinating with the proper IT personnel, and analyzing the company's reporting obligations under the various state data notification laws. Recent high profile incidents, such as the JP Morgan cyberattack, support the notion that initial reports often are riddled with inaccuracies—until just a few weeks before the bank formally disclosed the fact of the breach, it was reported that certain executives said they believed that only one million accounts were affected.[10] Target also revised its initial report of the number of customers whose personal information was stolen during last year's holiday data breach, nearly tripling its original estimate, and also disclosed that hackers had stolen a broader scope of data than originally reported.[11] If any communication must be issued at the outset of the investigation, it is best to keep it as short and concise as possible until a comprehensive and thorough investigation provides the company and counsel with a more accurate picture.

Conclusion

As the frequency and sophistication of cyber incidents increase, companies face new and significant challenges into protecting customer information and other valuable data and in responding to regulatory inquiries concerning a cyberattack. Accordingly, counsel representing such companies in investigations arising out of a data breach or cyberattack should proceed with the utmost caution in preserving data, implementing solutions, cooperating with regulatory authorities, and complying with various state notification laws.

1. Gen. Keith Alexander, Key Note Address, Cybersecurity and American Power, American Enterprise Institute, July 9, 2012, available at http://www.aei.org/events/2012/07/09/cybersecurity-and-american-power/.
2. One of the most troubling aspects of cyberattacks is that the victims—sophisticated entities with the resources and technology to protect themselves—often do not realize that their security systems had been breached when the intrusion occurred.
3. Michael Corkery, Jessica Silver-Greenberg and David E. Sanger, "Obama Had Security Fears on JPMorgan Data Breach," N.Y. Times, Oct. 8, 2014, available at http://dealbook.nytimes.com/2014/10/08/cyberattack-on-jpmorgan-raises-alarms-at-white-house-and-on-wall-street/.
4. FTC Release, "FTC Files Complaint Against Wyndham Hotels For Failure to Protect Consumers' Personal Information," June 26, 2012, available at http://www.ftc.gov/news-events/press-releases/2012/06/ftc-files-complaint-against-wyndham-hotels-failure-protect; see also *F.T.C. v. Wyndham Worldwide*, 2014 WL 1349019 (D.N.J. April 7, 2014).
5. Luciana Lopez and Karen Freifeld, "N.Y. financial regulator says to focus on cyber security," Reuters, Sept. 22, 2014, available at http://www.reuters.com/article/2014/09/22/us-regulator-cybersecurity-lawsky-idUSKCN0HH2J020140922.
6. Consumer Financial Protection Bureau, Strategic plan, budget, and performance plan and report, March 2014, available at http://files.consumerfinance.gov/f/strategic-plan-budget-and-performance-plan-and-report-FY2013-15.pdf.
7. Colo. Rev. Stat. §6-1-716.
8. Mass. Gen. Laws ch. 93H-1, §3.
9. DOJ Press Release, "Attorney General Holder Urges Congress to Create National Standard for Reporting Cyberattacks," Feb. 24, 2014, available at http://www.justice.gov/opa/pr/attorney-general-holder-urges-congress-create-national-standard-reporting-cyberattacks; Prepared Statement of then Acting Assistant Attorney General Mythili Raman, "Privacy in the Digital Age," to the Committee on the Judiciary, U.S. Senate, available at http://www.justice.gov/criminal/pr/speeches/2014/crm-speech-140204.html (Feb. 4, 2014).
10. Jessica Silver-Greenberg, Matthew Goldstein and Nicole Perlroth, "JP Morgan Chase Hacking Affects 76 Million Households," N.Y. Times, Oct. 2, 2014, available at http://dealbook.nytimes.com/2014/10/02/jpmorgan-discovers-further-cybersecurity-issues/.
11. Elizabeth A. Harris and Nicole Perlroth, "For Target, the Breach Numbers Grow," N.Y. Times, Jan. 10, 2014, available at http://www.nytimes.com/2014/01/11/business/target-breach-affected-70-million-customers.html.