Skadden

Cyberattacks 2014: How to Prepare Today and Respond Tomorrow

March 04, 2014

If you have any questions regarding the matters discussed in this memorandum, please contact the following attorneys or your regular Skadden contact.

John Beisner
Washington, D.C. / 202.371.7410
John.Beisner@skadden.com

Patrick Fitzgerald
Chicago / 312.407.0508
Patrick.Fitzgerald@skadden.com

Stuart Levi
New York / 212.735.2750
Stuart.Levi@skadden.com

4 Times Square
New York, NY 10036

On February 13, 2014, Skadden presented a webinar titled "Cyberattacks 2014: How to Prepare Today and Respond Tomorrow." Firm partners John Beisner, Patrick Fitzgerald and Stuart Levi presented an in-depth review of the cybersecurity issues companies face today. Topics included: key threats, steps every company should take to protect itself, how to best defend against data breach class actions and the issues related to working with the government in the event of a data breach.

Key Threats Companies Face Today

Where the Threats Are Coming From

Stuart Levi began the presentation with an overview of the reality that companies face today. Data breaches and cyberattacks are increasingly common, with companies in every industry being targeted. Attacks are no longer limited to the theft of personal information, even though those get the most press, but also can be motivated by theft of intellectual property or business information. In other cases, hackers merely look to launch denial-of-service attacks, which can shut a company's business down even if no information is taken. Stuart also noted that hackers no longer focus on the challenge of hacking the most difficult systems possible. Now, they attack easier targets that have larger financial awards. These factors have led a large segment of the security community to adopt an "assume you have been breached" mentality.

Response Times Have Accelerated

Stuart emphasized that rapid detection is as important as prevention, as the longer a threat goes undetected, the greater the potential loss and potential harm to the company. This detection is particularly important due to the fact that the response clock has accelerated. While some states have specific timelines in which companies have to notify the public (*e.g.* Florida requires notice within 45 days), many states merely require companies to provide notice "without reasonable delay." In the past, companies often delayed notice until full forensic analysis was completed. This provided companies with time to formulate a response and coordinate with public relations, communications and legal departments. However, various factors have combined to accelerate the timeline. First, privacy advocates and activists explore and discover breaches, threatening to go public if a company does not disclose the breach and, thus, requiring companies to move forward with less preparation. Second, insurance companies may require prompt notice in order to provide coverage under their policies. Finally, a recent complaint brought by the California attorney general against Kaiser Foundation Health Plan suggests that states may be defining an upper limit on what constitutes "reasonable delay" in providing notice. In this case, the company uncovered some of the breached data on December 11, 2011, and completed forensic testing in February 2012. Notification was provided on March 19, 2012. The complaint

alleges that this delay was too long and suggests that notices should have been sent on a rolling basis as soon as certain breach data was identified.

Key Legal Threats

The key legal threats companies face in relation to data beaches and cybersecurity attacks include FTC enforcement, shareholder litigation and data breach class action. Stuart emphasized that FTC enforcement can come from two separate angles: (a) companies misleading consumers by telling consumers that they have "robust" or "industry-standard" security policies and nevertheless getting hacked; and (b) companies having inadequate security protection. The second method for enforcement is less well-developed, but there is some indication that the FTC will view inadequate security protection as a type of unfair practice. However, plaintiffs' lawyers and the FTC need a "hook" in order to establish a valid claim — something that the company has done wrong. This could be failure to implement adequate security precautions; failure to follow internal security policies or vendor policies, misleading customers about the level of security; inadequate C-suite or board oversight; or excessively delayed notification. By eliminating as many of these "hooks" as possible, companies can minimize their risk.

Steps Every Company Should Take Today

Stuart identified six steps every company should take today in order to best protect themselves against cyberattacks:

- **Privacy audit and implementation**. Privacy audits, which are typically performed by a law firm or outside consultant, allow companies to identify potential privacy issues and pitfalls that may not be obvious to a company's employees. A privacy audit includes examination of how data is used, what security practices exist and how the company is communicating its policies with consumers. The entity conducting a privacy audit can identify areas of improvement and suggest best practices. An added benefit of conducing a privacy audit is that it is viewed favorably by regulators, and in the event of litigation can be a good fact to demonstrate the company's commitment to privacy. However, it is important that a company act on the recommendations generated by the audit, either by implementing them or documenting why they have opted not to do so.
- **Risk assessment**. A company should evaluate potential risks of a data breach, identifying what type of information can be compromised and the possible consequences, including lost business, regulatory scrutiny, fines and penalties.
- **Establishment of a rapid response team**. Given that companies may be forced to disclose data breaches sooner than they would like, it is important that companies think through in advance the issues they might confront and how they would respond. Creating a rapid response team comprised of stakeholders from different areas within the organization enables a company to design such a plan in advance.
- **Testing**. Companies should review and test their data response plan periodically, as the law may change or there may be company turnover or restructuring that necessitates an updated plan.
- **Privacy by design**. "Privacy by design" is a concept that has been touted as a best practice by the FTC. In essence, privacy by design means that companies should take privacy issues into account as they build products and services, and not merely consider those issues at the time the product or service is to be rolled out.

- **Evaluation of insurance coverage**. Cyber insurance is a growing area and covers many of the costs associated with a data breach (such as the cost of notification, business interruption, etc.). Companies should evaluate their own risk profiles and current insurance companies to determine if purchasing this type of insurance is a reasonable investment.

Data Security Class Actions

John Beisner continued the webinar by introducing various issues surrounding data security class actions, which have been the primary form of litigation so far. He also emphasized that other types of actions may develop, including state attorneys general invoking parens patriae powers to bring quasi class action suits; and he noted that, while there have not been significant numbers of class actions so far, they are expected to increase. Additionally, the class actions that have been filed so far provide lessons in how to best defend against these types of actions.

There are two key stages at which to challenge privacy class actions: motions to dismiss or class certification.

One defense against a consumer class action is to argue that plaintiffs lack standing. To defeat standing, defendants may argue that possible future harm resulting from a data breach is insufficient to qualify as concrete and particularized injury in fact. The law is somewhat unsettled in this area, with several courts having held that increased risk of personal data being misused is insufficient to create standing, with others courts holding that plaintiffs *do* have standing. John pointed to a recent U.S. Supreme Court case that held allegations of future injury insufficient in another context as evidence that courts may be moving toward denying standing based on increased risk of harm. Other potential defenses, depending on the nature of the underlying claims, might include: lack of cognizable injury, the economic loss doctrine, failure to quantify a loss, or lack of a private right of action.

With respect to class certification, John pointed to the denial of certification in *Hannaford Bros. Co. Customer Data Sec. Breach Litig.*, 293 F.R.D. 21, 24 (D.Me. 2013). In that case, the court refused to certify a class of consumers who claimed that they suffered out-of-pocket losses taking steps to mitigate a data breach that resulted in unauthorized access to their personal information. In denying class certification, the court noted that potential class members' claims likely would vary based on whether they actually incurred fraudulent charges and what precise mitigation steps they took. John noted that other data-security class actions may face similar predominance problems, especially those involving claims that require individualized proof of exposure to a misrepresentation, reliance or injury. In addition, John explained that proposed data security class actions will likely be subject to a host of other challenges arising from the potential difficulties in objectively ascertaining class membership and, with respect to proposed multistate classes, the need to apply the varying laws of multiple states.

Interacting With the Government

Patrick Fitzgerald concluded the webinar with some suggestions for companies. He focused on mitigating risks associated with internal controls, including both technical and management controls. He emphasized the importance of limiting access to confidential information and monitoring departing employees to ensure that the information is protected. He also

mentioned the importance of limiting exposure by minimizing the amount of information on laptops and other technology that employees carry with them while traveling, given the risk of loss. He also reiterated the importance of having a response chain and plan in effect in the event of a breach.

Patrick then shared some of his insights related to government communications. He began by explaining that sometimes the government will reach out to a company to tell the company that it has been breached, but the information does not get communicated internally to the appropriate level of management. In order to address these communication failures, companies should make cybersecurity part of overall risk enterprise management, including clarifying the reporting chain and obligations to report information about detected breaches (or government contacts) up the chain. Furthermore, once a company has been contacted by the government, it needs to determine the purpose of the communication and how to best respond.

Patrick concluded with a discussion of factors to consider when deciding whether to contact the government to inform it of a breach. This is a fact-specific inquiry that companies should conduct carefully. Reasons to contact the government include: the ability to learn additional information to which the company may not have access, access to the government's superior technical abilities and possible deterrence of future hackers. Being able to demonstrate that the company reached out proactively to the government also could be a helpful fact in any subsequent litigation. On the other hand, involving the government means that a company risks losing control over the situation, and the consequences of a possible future criminal prosecution of the wrongdoer, which may result in internal distraction or disruption. Furthermore, in certain industries, a perception that the company cooperates closely with the government could hurt a company's ties with customers. Ultimately, Patrick emphasized that a company's decision should be based on the specific facts of the case, the industry environment, the company's mission and an analysis of the risk/reward profile.

The panel concluded by taking questions from the audience over the web. In response to a question about board action, Stuart emphasized the importance of keeping cybersecurity a part of the discussion on the highest levels of a company. He emphasized that it is risky to leave these issues to the IT department. The board should remain apprised of major expenditures and measures that are being taken with regard to cybersecurity, as well as be informed of any cybersecurity or data breach issues that arise. Whether or not to form a separate security committee depends on the risk profile of the specific company.