Insights Conversations: Cybersecurity

Skadden

January 2015

This article is from Skadden's *2015 Insights* and is available at skadden.com/insights.

Contributing Partners

Cyrus Amir-Mokri
New York

Patrick Fitzgerald
Chicago

Marc S. Gerber
Washington, D.C.

Stuart D. Levi
New York

Timothy A. Miller
Palo Alto

This past year has been called the "year of the massive data breach," with many high-profile attacks on well-known companies. Skadden partners Cyrus Amir-Mokri, Patrick Fitzgerald, Marc S. Gerber, Stuart D. Levi and Timothy A. Miller discuss the issues businesses must consider, the litigation risks involved and the evolving role of governments in cybersecurity.

Cybersecurity attracts a lot of attention as one of the critical issues for businesses today. Is the problem overblown?

Pat: In a word: no. About four years ago, when I was a U.S. attorney, I was surprised when the FBI agent in charge of the Chicago office told me cybersecurity, not terrorism, was the issue that most kept him awake at night. As he briefed me on the issue, I understood why. The government has opened up more and more about its concerns in this area over the last few years, but I think many people wondered whether the threat was overstated. As things have played out, it is becoming more and more clear that the concerns were not overstated and that this is a real issue. What is less clear is how we will adapt. Companies need to address the nuts and bolts of cybersecurity, but they also need to consider how they wish to interact with the government in handling this common issue. Companies are concerned both about the risks of cooperating too closely with the government and the risks of not doing so. Fashioning policies that protect a company's intellectual property and the privacy of customers or employees, while not compromising national security and public safety, is not easy but it is important to do. The recalibration of how the public and private sectors interact in the cyber area is as important as any other legal and policy issue we face today.

Cyberattacks seem certain to increase in the near future. What steps should corporations and their boards take before a cyberattack occurs?

Stuart: The high-profile cyberattacks of 2014 serve as an important reminder that every company is vulnerable. At the end of 2013, too many companies decided that the Target attack did not apply to them because they were not retailers holding credit card information. Companies must not make the same mistake with the Sony attack and decide that this is not their issue because they do not engage in activity with geopolitical ramifications. The unfortunate reality is that every company is a potential target. For example, we have seen politically based hackers launch "ransomware" attacks on companies that are apolitical.

Companies therefore need to make cybersecurity a critical component of their risk assessment and business planning. The National Institute of Standards and Technology framework provides the best guidance for implementing such an assessment. In addition, companies must have a documented rapid response plan so they are prepared to address a cyberattack. In our experience, companies with such plans respond faster and are better able to contain their risk. Finally, the legal department should audit the company's privacy policies and procedures. It is a failure in these areas, more than failings on the technology front, that makes companies most susceptible to legal and regulatory challenges after a cyberattack.

Four Times Square
New York, NY 10036
212.735.3000

skadden.com

Marc: With that in mind, there are certain steps a board should take. As part of its oversight of a company's risk management, the board should understand how cyber incidents can impact the company's business, the company's experience with cyber incidents to date and the company's ongoing preparations for future cyber incidents. This includes asking questions to reach an informed view of whether management is considering the risks in a way that is consistent with the company's risk profile and whether it has employed appropriate resources to prevent and mitigate them. These are ultimately business judgments and, as with any business judgment, the board needs to be informed.

Cyrus: A key first step in that effort is to clarify accountability within senior management for cybersecurity issues, which should include a way for employees to escalate material cybersecurity issues promptly to senior management and, ultimately, the board. Senior managers responsible for cybersecurity should have direct access to the board. For example, boards should consider asking the chief information security officer to prepare regular reports to the board and present them in person at least annually so the board has the opportunity to ask follow-up questions.

More generally, companies should have a comprehensive cybersecurity policy, which should include performing a cybersecurity risk assessment, developing and continually updating a cyberattack crisis management protocol, maintaining robust lines of communication with relevant agencies of the U.S. government, adopting cyber hygiene best practices, participating in information-sharing platforms, evaluating all outside connections and discussing cyber readiness with business partners and vendors, and having a disaster recovery and business continuity plan.

What should companies think about in developing their rapid response teams? Are there considerations that are specific to particular industries?

Tim: Retail is an industry that faces a specific and significant set of security issues, with the cybersecurity of payment systems maintained by retailers being a focal point of plaintiffs and regulators. Retailers who suffer a security breach of credit card data can expect a fight on two fronts — from consumers impacted by the breach and from issuer banks — and rapid response teams can help minimize potential liability by allowing for a response at the first sign of a data breach.

Target is a good example. Computer hackers installed malware on Target's computer servers that read the data from 110 million customers' credit and debit cards when they were swiped in Target's stores over several weeks during the 2013 holiday season. In the ensuing multidistrict federal litigation in Minnesota (*In re Target Corporation Customer Data Security Breach Litigation*, MDL No. 14-2522 (D. Minn., Dec. 2, 2014)), the court recently allowed several claims to proceed against Target brought by the financial institutions that issued cards impacted by the breach and a separate putative class of Target consumers. The ruling on the claims by financial institutions hinged primarily on the allegation that Target turned off one of its security measures, thereby allegedly increasing the risk of a data security breach, and the claim that Target failed to respond swiftly enough to purported warning signs of an impending cyberattack. In upholding general negligence claims under Minnesota law, the court held that no special relationship was required between Target and the financial institutions to establish a duty, because the financial institutions were foreseeable victims of Target's allegedly negligent act of disabling a data security feature. In its separate ruling in the consumer class action, the court found Article III standing based on allegations of actual economic harm — for example, unauthorized credit card charges. The court found claims brought under dozens of state consumer protection and other statutes to be "plausible," allowing them to proceed absent compelling state law authority precluding the claims or supporting Target's interpretation of the various statutes at issue.

Cyrus: Another factor to consider with rapid response teams is how to address differences based on the unique characteristics of specific companies and industries. For example, because different government agencies act as principal cybersecurity contacts for particular industry sectors (*i.e.*, "sector-specific agencies"), rapid response teams will need to tailor crisis communications and information-sharing protocols to the relevant government agency for their sector. A similar tailoring of communications protocols would hold for relationships with ISACs (information sharing and analysis centers), which also are organized along industry sector lines.

The Target example also highlights the litigation risks involved with cyberattacks. How has the landscape for class actions evolved in this area, and what might we expect in the near future?

Tim: Actions seeking remedies for breaches in data security have followed practically every significant breach at retailers, banks and other businesses. Cases involving Target, Adobe and Sony (the PlayStation, not the movie studio) moved through the legal system in 2014. Standing continues to be the threshold battleground issue. Article III standing requires plaintiffs to allege injury in fact that is concrete and particularized and actual or imminent. The harm cannot be merely conjectural or hypothetical.

Plaintiffs continue to allege damages for risk of future harm, such as the increased risk of identity theft. So far courts have disagreed as to whether an increased risk of personal data being misused in the future is sufficient to constitute "concrete" and "imminent" injury necessary for Article III standing. Some courts have held that an increased risk of personal data being misused in the future is not sufficient, though the Ninth and Seventh Circuits have held the opposite. There was hope that the U.S. Supreme Court's decision in *Clapper v. Amnesty International*, 568 U.S. ___ (2013), would strengthen defendants' standing argument, because it seemed to suggest that a plaintiff must show that threatened future injury is “certainly impending.” But federal courts in California have held that *Clapper* did not change the law. Meanwhile, plaintiffs’ attempts to manufacture standing by making out-of-pocket expenditures on credit monitoring services have been rejected by most courts.

We anticipate that cases involving Article III standing will continue to favor class action plaintiffs. If so, look for plaintiffs to focus on state consumer protection statutes as a basis for liability. However, those statutes typically require a showing of “actual damages” that is higher than the Article III standing requirement of “concrete” injury. In 2014, courts continued to dismiss damage claims under such statutes.

Where does board oversight fit into the picture, and what are some of the key considerations for boards in this area?

Marc: The Target breach is an instructive example. Following the breach, shareholder lawsuits alleged that directors failed to take reasonable steps to oversee the company’s efforts to protect data and prevent breaches, in violation of their fiduciary duties. As I mentioned earlier, boards and those who advise boards need to build a record of being informed — understanding the company’s susceptibility to cyber incidents, the potential threats the company faces, the potential consequences of an incident, and the company’s rapid and longer-range response plans. To the extent industry standards or other external benchmarks are available, the board should understand why the company may or may not meet those standards and the business case for any decisions being made.

In December, the Senate Banking Committee held a hearing on ways to protect the financial sector from cyberattacks, with a particular focus on interagency cooperation. What did the public learn from the hearing? What can we expect from the government on cyber issues?

Cyrus: We know from the testimony of the government witnesses and from their agencies’ other efforts that they are hard at work within government and in collaboration with the private sector to help prevent attacks and to mitigate them when they occur. One important area in which they have made significant progress is information sharing. It is critical for the private sector to participate and make maximum use of government information-sharing and incident-management resources. Such information can enhance security efforts, for example, by providing insight into the signatures, penetration techniques and other exploits used by cyberattackers, or by identifying what IP addresses might be originating cyberattacks.

Government agencies also are more focused on cybersecurity now than they were a few years ago. In the financial services sector, for example, the banking regulators, market regulators and state regulators have taken significant steps to develop examination protocols and rules as part of their financial stability and safety and soundness missions.

Stuart: Another area to consider going forward is legislation. A couple of years ago, the Senate passed and the Obama administration supported comprehensive cybersecurity legislation, which the House rejected. Very little has been accomplished in the meantime. But this month, perhaps emboldened by Sony and the other recent high-profile breaches, President Obama proposed legislation to enhance online privacy and cybersecurity, including additional public-private information-sharing authorities, revisions to criminal laws related to computer crimes and a federal data breach notification law. The proposed legislation replicates many of the features of the 2011 initiative, though not some of its more controversial components, such as the establishment of a new cybersecurity regulatory authority permitting the Department of Homeland Security to review and approve critical infrastructure cybersecurity frameworks. These changes, along with a continuing stream of breaches, may be enough to convince Congress of the case for a federal role in private sector cybersecurity.

Recent reports have linked the governments of China, Iran and North Korea to major cyberattacks on public corporations. Do attacks launched by sovereign nations have different implications for corporations than those by "private" hackers?

Stuart: State-sponsored cyberattacks are particularly concerning because of the unprecedented resources a nation-state can bring to an attack. It's also far easier for hackers to conceal an attack if they enjoy the protection of the host state. It will be interesting to see whether, like in the case of Sony, state-sponsored attacks generate greater attention from the U.S. government and therefore stronger retaliatory measures. That said, law enforcement officials will tell you that the line between state-sponsored terrorism and criminal activity is beginning to blur, with countries relying on rogue actors to enhance their hacking capabilities.

Cyrus: Attacks by sovereign nations have at least three important implications. First, as Stuart noted, certain sovereign nations are very sophisticated and, therefore, may be able to inflict greater damage than other attackers. Second, the motives of sovereign nations vary, which means that the consequence of their intrusions will be different. Some sovereign nations may be interested only in exfiltrating sensitive information. Such actions do not cause destruction or embarrassment — as other sovereigns may wish to do — but they may enable competitors in other countries to use business and other secrets to better compete. Third, in the case of an attack by a sovereign, the response may be constrained by geopolitical, diplomatic or national security factors. In other words, law enforcement or private legal action may no longer be the focus.

In light of the cyber events of 2014, are all the old approaches to cybersecurity obsolete?

Pat: Not at all. The technical capabilities that have been deployed by rogue states, hackers and criminal enterprises are daunting and have rightly caught the attention of government agencies, companies and their boards, and now the plaintiffs' bar. But we should not forget the lower-tech threat from the insider that can do great damage as well. Many enterprises lose valuable intellectual property when employees — especially soon-to-be-former employees — walk out the door with trade secrets in low-cost thumb drives or log in from home to the company's secure network and download away. Companies need to do the basic blocking and tackling of limiting access to the most sensitive materials to those with a need to know, creating levels of security appropriate to the information, and changing levels of access as employees' positions change or as they leave the company. Paying attention to employees whose downloading activity is aberrational — either because of unusual volume or because the materials accessed are not related to the employee's responsibilities — is important, especially when the company learns an employee will be leaving the company.

Not all traditional insurance policies cover cyber losses. How has the "year of the massive breach" impacted the insurance industry? Do you expect to see a continued rise in specialty cyber policies or the emergence of other cyber-related coverage?

Cyrus: There is clearly greater interest in cyber insurance. Some insurers are beginning to underwrite cyber risk, although this is still a nascent market. Firms should evaluate whether their business-interruption policies cover cyberattacks. Some insurers have exclusions for cyber insurance in their business-interruption policies, making it a separate product. The development of cyber insurance is a subject to watch. Unlike other hazards, including severe weather and even terrorism, experience with cyberattacks is relatively new — accordingly, the market will continue to develop.

If 2014 was the year of the massive data breach, what are the big cybersecurity issues you expect to unfold in the near future?

Stuart: In many ways, 2014 laid the foundation for what are likely to be the key developments in 2015. There is no doubt that cybersecurity attacks will increase and spread, as companies and hackers engage in an "arms race" of cyber protection and cyberattack. We also are likely to see many more enforcement actions brought by the Federal Trade Commission as it looks to effectively impose minimum cybersecurity requirements on companies through Section 5 claims. 2015 also is likely to be the year that regulators in a variety of industries come down hard on their regulated companies to ensure that they are adhering to evolving industry standards in cyber protection. Finally, we expect to see greater cooperation between the government and the private sector as they combat this growing threat.

Cyrus: I agree — I think everyone agrees — that we should view the cyberattacks and breaches of 2014 as a harbinger of what's to come. Breaches and attacks occurred prior to 2014, including some very significant ones, so in a sense 2014 was simply a continuation of what was going on before. However, what we are seeing is increasing sophistication of attackers, together with the realization of the incredible capacity for disruption and destruction. Companies should become smarter in redesigning or reconfiguring their systems. It is no longer sufficient to design systems with a view of keeping attackers out. Companies should assume that penetration will occur. Their focus must shift from absolute prevention of penetration to making navigation and destruction by attackers more difficult to mitigating and managing damage once it occurs.

Overall, in addition to expecting more and more destructive cyberattacks, we should watch for the following trends: First, we should expect that non-sovereign nation actors will become more and more sophisticated. Second, as our connectivity through wireless media expands, we should watch for attacks on and through mobile technology. Third, although thus far we have not had instances of catastrophic data destruction, it is important for companies to continue to develop resilience in that respect.