Emerging Trends in Privacy and Cybersecurity

Skadden

January 2016

This article is from Skadden's *2016 Insights* and is available at skadden.com/insights/2016-insights.

Contributing Partner

Stuart D. Levi
New York

Four Times Square
New York, NY 10036
212.735.3000

skadden.com

Entering 2016, the relentless stream of cyberattacks continues unabated, having become a "business as usual" reality to which companies must adapt. All companies, regardless of size or industry, are potential targets, and the pool of attackers is expanding. Below is an overview of the key themes that emerged this year and what we expect to see in 2016.

Best Practices for Cybersecurity Preparedness

In 2015, a number of regulators, including the Securities and Exchange Commission's (SEC) Office of Compliance Inspections and Examinations (OCIE), issued guidance and alerts about cybersecurity preparedness. The good news for companies, whether regulated or not, is that consistent themes are emerging as to what constitutes best practices. They include:

- **Conducting a Risk Assessment.** Cybersecurity preparedness needs to start with assessing the company's risks and designing a plan that addresses those risks.
- **Strong Governance.** A cybersecurity plan must involve the active participation of senior management, and where applicable, the board.
- **Data Access.** Employees should be able to access only the data they require, with appropriate authentication steps.
- **Training.** Many attacks prey on employees who may unknowingly surrender their passwords or click on malware links. Regular employee training on cybersecurity is therefore critical.
- **Vendor Management.** Attacks are often launched through a third-party vendor that has access to the company's system for business purposes. Companies must have robust cybersecurity requirements for vendors.
- **Incident Response Plan.** All companies should have incident response plans to deal with cyberattacks and run tabletop exercises to walk through different scenarios.
- **Cyber Insurance.** Cyber insurance is emerging as an important component of any risk mitigation strategy.
- **Information Sharing.** Companies across multiple industries have begun to appreciate that sharing cyberthreat information and best practices with their competitors is a critical tool to reduce risks. The White House has been encouraging this practice, and in February 2015, President Barack Obama issued an executive order encouraging the development and formation of Information Sharing and Analysis Organizations. We expect these efforts to greatly expand in 2016, and all companies should consider joining an information-sharing group in their industry.

Outlook on Legislation

As in previous years over the past decade, Congress attempted to enact various privacy or cybersecurity legislation. These initiatives were expected to gain more traction following President Obama's release of a number of proposed bills in January 2015, including a federal data breach notification law and information-sharing legislation. However, the only piece of legislation that was enacted was the Cybersecurity Act of 2015, a bill that made it through Congress at the end of the year as part of the 2016 omnibus spending bill. The act creates a voluntary framework for real-time sharing of "cyber threat indicators" and "defensive measures" and provides liability protections and an antitrust exemption for such sharing.

We do not anticipate any other meaningful additional privacy or cybersecurity legislation being enacted in 2016. Indeed, state attorneys general responded to widespread calls for a federal data breach notification law by urging Congress to preserve state authority in this area. Such a federal law will probably continue to be discussed but is unlikely to pass in 2016.

The Role of the FTC

The Federal Trade Commission (FTC) has long been the most active regulator in the areas of privacy and cybersecurity. In 2015, the FTC won a significant victory when the U.S. Court of Appeals for the Third Circuit held in the *Wyndham* case that the agency has authority to deem a company's cybersecurity practices unfair under Section 5 the FTC Act, and that companies had fair notice as to what practices could violate that section. However, as the year drew to a close, the FTC was handed a defeat when its own administrative law judge held in the *LabMD* case that the FTC must show more than the mere "possibility" of harm from a cybersecurity incident in order to sustain a Section 5 case. Despite this setback, we anticipate that the FTC will remain highly active in this area, and that companies should be familiar with the types of cases the FTC is bringing in order to understand the issues on which the agency is focused.

EU Emerges as a Force to Be Reckoned With

Although the European Union has had a robust privacy regime for close to 20 years, the impact on U.S. companies has been relatively limited. A dramatic shift in this equation occurred this year. In December 2015, the EU announced completion of a new General Data Protection Regulation (GDPR), which will replace and significantly broaden the current EU Data Protection Directive. The GDPR is widely expected to be approved in early 2016 and go into effect two years later. The impact on any company doing business with European residents — even if not situated in Europe — will be significant.

The expanding impact of the EU was also felt two months earlier, when the Court of Justice of the European Union invalidated the U.S.-EU Safe Harbor framework on which thousands of companies had relied to send personal data from the EU to the U.S. The court also empowered local data protection authorities to decide for themselves whether personal information was being protected by international agreements. These developments suggest a far more activist European privacy regime than had been in place — one that could have a significant impact on global commerce in 2016 and beyond.

Class Action Lawsuits Must Remain Part of a Company's Risk Calculus

Most data breaches result in multiple class action lawsuits against the victim company. The gating issue has been whether the plaintiffs' alleged injury is sufficiently concrete and imminent to establish Article III standing, especially since these plaintiffs often have not suffered any monetary loss or other tangible injury. Cases from the past year offered little clarity on this issue. For example, in June 2015, in the *Zappos* litigation, a Nevada district court held, as have many other courts, that the possibility that a "credible threat may occur at some point in the future " is insufficient to confer standing. However, the U.S. Court of Appeals for the Seventh Circuit adopted a more lenient position, finding standing in the *Neiman Marcus* case because the presumed purpose of the theft of personal information was to make fraudulent charges or engage in identity theft, and plaintiffs should not be required to wait until such harm occurs. The decision by the Seventh Circuit and other courts that have found standing may further incentivize plaintiffs' counsel to bring class action lawsuits. The potential for such suits should therefore be part of the risk calculus of any company that collects or processes personal information.