JANUARY 16, 2018

Legaltech® news ONLINE

An ALM Publication

Targeted: Companies Face Emerging Regulatory and Cybersecurity Threats in 2018

Following a year where companies were targeted in breaches that compromised personal information of more than half of the U.S. population, regulators are moving away from voluntary cybersecurity compliance to comprehensive regulation and enforcement.

BY MICHELLE REED AND LAUREN YORK

Following a year where companies were targeted in breaches that compromised personal information of more than half of the U.S. population, regulators are moving away from voluntary cybersecurity compliance to comprehensive regulation and enforcement. Cybersecurity threats continue to escalate and evolve, and companies must prepare for the increased regulatory scrutiny and mandatory state, federal and international cybersecurity frameworks. This article explores key cybersecurity trends for 2018, provides an overview of changing regulatory frameworks, and outlines practical steps for companies to combat evolving cyber threats.

Key Cybersecurity Trends for 2018

Ransomware—the number of ransomware attacks exploded in 2017 nearly fourfold. Ransomware encrypts files with a private key that only the attacker possesses. Attacks became more sophisticated and were aimed at mobile phones as well as computers. Cryptocurrency, most notably Bitcoin, has provided ransomware attackers a difficult-to-trace way to collect from their targets. No industry has been spared from ransomware attacks,

which can occur through malicious emails or websites. The highly publicized and unprecedented "WannaCry" attack showed just how pervasive and quick-moving these attacks can be. In 2018, expect to see greater sophistication in both protection mechanisms and the attacks themselves, as perpetrators find innovative ways to exploit expanded technology and circumvent prior protective measures.

Sophisticated phishing—Phishing will likely continue to be one of the most effective cyberattack in 2018, as attackers have seen that even a slow-burning attack can yield a huge payout. Cybercriminals in 2017 perpetrated a Netflix phishing attack that thwarted many common protections currently used by spam filters, including mirroring html code from Netflix's own site and buying credible URLs to host its malicious pages. Other schemes targeted specific safety features embedded in well-known email clients, such as Office 365. Attackers are willing to take their time to social engineer the results they desire, and companies must respond with rigorous training for employees as well as consider implementing new digital safeguards with programs that detect impersonation and natural language processing that accompanies machines using Artificial Intelligence (AI) to enable their attacks.

Cyber destruction—In 2017, there was also a surge of attacks aimed not necessarily at monetary gain but for the sake of destruction alone. These attacks, sometimes cloaked under the guise of ransomware, have been used for political gain. Perpetrators of these destructive attacks have targeted not only companies, but key infrastructure players, including power plants and utility companies.

Overview of Changing Regulatory Frameworks

The much-discussed General Data Protection Regulation (GDPR) goes into effect May 25, 2018. The GDPR introduces a host of new regulations for data controllers and processors, aimed at giving individuals more control over their personal data. Although European companies (and those companies that handle data of EU citizens) have had two years to become GDPR-compliant, it is likely that many have not and non-compliant organizations may be used as an example. For the rest of 2018, the world will see what strong regulations look like in practice, and may begin to mirror their own regulations after those of the EU if the GDPR proves successful.

The United States still depends on a state-by-state framework for most cyber law. In March 2017, New York's Department of Financial Services (DFS) cybersecurity regulation, 23 NYCRR 500, went into effect, mandating minimum standards for all banking, insurance, and brokerage firms using a license to operate in New York. The DFS regulation requires, among other things, every entity to have a cybersecurity plan to protect users' data, have a senior security officer and training for employees, and submit a yearly statement of compliance. There are also tighter regulations related to third-party vendors. The DFS Regulation is thought to be the strictest of its kind in the United States. Other states, including Colorado with its Rule 51-4.8 Broker-Dealer Cybersecurity regulation, followed suit with their own regulations. It appears that the days of voluntary compliance with cybersecurity norms are slowly coming to an end.

On a national level, President Trump signed the 2018 National Defense Authorization Act in December 2017, which attempts to clarify the U.S.'s position on cyberattacks and cyber warfare, both offensive and defensive. We anticipate that President Trump will define what "cyber warfare" is and develop a plan to be approved by Congress (Sec. 1633), while the Defense Secretary is charged with streamlining current cyber initiatives. Other federal agencies are also raising the stakes. The FTC continues its strong enforcement and the SEC has signaled forthcoming Commission-level cybersecurity regulations. 2018 will likely be a seismic shift in the way that cybersecurity is addressed in the United States and the world.

Practical Steps to Implement Now

- Recognize and socialize the idea that no company is "completely safe" and it is better to be proactive and contain any breach. Conduct gap analyses and penetration testing to proactively identify weaknesses.
- Prepare an incident response plan for when you are the victim of an attack.
- Train your employees, including upper level management, through tabletop exercises and security training. Follow up on weaknesses to maintain competency.
- Ensure that your organization has a senior security officer. If a senior security officer in already in place, empower that individual in the workplace.

As the sophistication and damage from cyberattacks continue to rise, companies should expect that federal, state, and international cybersecurity regulations will become more rigorous. Preparing for the worst in advance can make the difference between a successful and unsuccessful breach response.

Michelle Reed *is a partner in the Dallas office and co-leader of Akin Gump Strauss Hauer & Feld's cybersecurity, privacy, and data protection practice.* ***Lauren York*** *is an associate in Akin Gump's Dallas office. They advise clients on data breach investigations, notifications, and subsequent litigation.*