Cybersecurity Law Report
An Acuris company

cslawreport.com

January 22, 2020

CYBER CRIME

Managing Legal Risks to U.S. Companies From Foreign Cyberattacks

By Amanda Lawrence, Sasha Leonhardt and James Chou, *Buckley*

Protecting online systems against individual hackers has been a top priority for companies for several years, but as we begin a new decade, a new threat has risen to the forefront: well-funded and sophisticated foreign governments seeking to wage a new kind of warfare on the United States.

In response to increasing tensions with Iran, the Department of Homeland Security warned at the beginning of the year that government-sponsored cyberattacks originating from the Middle East may be imminent. Days later, members of Congress urged the financial services industry to "be proactive" in preparing for "potential cyber attacks" from another country. On January 16, 2020, the FDIC and OCC issued a joint statement warning financial institutions about heightened cybersecurity risk and advising institutions to "review, update, and test incident response and business continuity plans," among other things. And state regulatory bodies, such as the New York Department of Financial Services, advised financial institutions to be wary of foreign cyberattacks in light of recent events. Separately, because this is an election year, cybersecurity is particularly critical for firms that offer electronic voting technology and support key public services.

State-sponsored cyber actors have stronger financial backing, better technology and more manpower than individual actors or small-scale syndicates, and their attacks have demonstrated significantly greater capacity to cause harm. Businesses face a unique set of challenges in defeating attackers motivated not by payoffs but by the intent to degrade, disrupt or destroy a company's operations with the overarching goal of harming the U.S. Companies should prepare for attacks designed not for limited financial gain, but to inflict major damage to their business in pursuit of a foreign political agenda.

Failure to anticipate and prepare for foreign state cyberattacks puts companies in legal peril. Federal laws create baseline obligations for businesses holding consumer data to manage cybersecurity risks; in sensitive industries like financial services and health care, the standards are even higher. State laws carry additional requirements, causes of action and enforcement liability. The General Data Protection Regulation creates yet another source of legal exposure for companies operating in Europe.

See CSLR's two-part series examining the CPPA close-up: "Review of Amendments and How to Prepare for Compliance" (Oct. 2, 2019);

and "The GLBA Carve-Out and How Financial Institutions Can Evaluate Applicability" (Oct. 9, 2019).

The Scope of Potential Cyberattacks from Nation-States

Many companies have taken steps to prevent cyber attackers from employing a suite of well-worn, but still effective, techniques:

- Social engineering: Tricking people into revealing sensitive information or performing certain actions through deception; these attacks accounted for more than 30 percent of all data breaches in 2018.
- Phishing: Posing as a trusted party to gain information from unsuspecting users.
- Spear-phishing: Phishing with personal information to create tailored messages that gain the user's trust.
- Distributed denial-of-service (DDoS) attacks: Deploying devices to push traffic to websites or online databases with the goal of overwhelming and crashing them.
- Man-in-the-middle attacks: Intercepting unencrypted internet traffic and exploiting it.
- Ransomware: Encrypting or threatening to delete data unless money is paid or some other action is taken.
- Malware: Installing hidden executable code on information systems to disrupt, damage or gain unauthorized access **to** them.

While many companies have fortified themselves against individual hackers' use of these techniques, foreign governments have greater resources and technological capabilities and can employ these same tactics with much greater precision and harm. In one case involving the Las Vegas Sands casino in 2014, a sophisticated foreign malware attack stole email addresses, Social Security numbers, banking information, tax information and driver's license numbers. Another malware attack in 2016 attributed to state-sponsors led to the theft of $81 million from a New York Federal Reserve Bank account.

The potential for damage is increasing as sovereign nations deploy newer, more sophisticated methods that may not be available to individual actors. Foreign governments can invest substantial resources to look for previously undiscovered weaknesses in computer systems in so-called "zero-day exploits" that companies struggle to defend against precisely because they are unaware of where they are vulnerable. Many zero-day exploits are quietly discovered, and in some instances can go unreported for years. Countries that lack the technical expertise to identify zero-day exploits on their own can purchase them on the black market and deploy them effectively.

The Legal Landscape for Victims of Hacking

The risks companies face stemming from a cyber attack are pervasive. One study puts the possibility of a business experiencing an attack within the next two years at nearly 30 percent, at an average cost of more than $8 million. Several federal laws allow consumers and enforcement agencies to sue companies that have suffered data breaches:

The Federal Trade Commission Act

The FTC Act protects consumers from unfair or deceptive acts or practices. The FTC has determined that maintaining poor cybersecurity practices can be an "unfair" practice under the FTC Act, and therefore may provide a basis for civil liability for data breaches or losses. The FTC has imposed liability on companies after a data breach caused by a lack of safeguards, to include unencrypted storage of payment card information, easily guessed passwords and the lack of firewalls. Similarly, if a company makes promises to consumers regarding its cybersecurity practices but fails to live up to these promises, that can be a "deceptive" act or practice which could result in liability under the FTC Act.

See "Eight Data Security Best Practices Revealed by Recent AG and FTC Enforcement Actions" (Jan. 8, 2020).

The Gramm-Leach-Bliley Act

The GLBA requires financial institutions in particular to "protect the security and confidentiality" of consumer information. Under its Safeguards Rule, regulators require financial institutions to establish policies and procedures for incident response, access control, third-party risk management and—in the event of a breach—consumer protection a nd notification. The FTC recently proposed to update the Safeguards Rule, expanding the de finition of "financial institution" to include co mpanies engaged in activities "incidental to fin ancial activities." The proposal also would req uire the adoption of incident-response plans and hold financial institutions more accountable for information security.

See "A Behind the Curtains View of FTC Security and Privacy Expectations" (Mar. 16, 2016).

The Health Insurance Portability and Accountability Act

Through rules promulgated by the Department of Health and Human Services, HIPAA requires most health care providers, health plans, healthcare clearinghouses and their business associates to protect patients' electronic health information. The HIPAA Security Rule requires covered entities to implement "administrative, physical and technical safeguards to ensure the confidentiality, integrity and security of electronic protected health information," or ePHI. They also must protect against reasonably anticipated threats to ePHI, perform both initial and ongoing risk assessments, and must implement a security awareness and training program for their workforce.

See "Lessons From the Continued Uptick in HIPAA Enforcements" (Feb. 8, 2017).

GDPR

Companies that provide services to E.U. residents also must comply with the GDPR, Article 5 of which requires that companies process all personal information "in a manner that ensures appropriate security." More specifically, Article 32 requires companies to implement a risk-based approach to data security, giving consideration to the availability, confidentiality, integrity and resilience of technical assets and information systems. Article 32 also recommends that companies collecting, processing, transmitting or storing personal information encrypt all personal information.

State Laws

States also are getting into the mix. For example, the California Consumer Privacy Act, which went into effect on January 1, 2020, provides for a private right of action and enforcement by the California Attorney General if personal information "is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices." And while the legislative season is just beginning, several state legislators – notably in Florida, Nebraska, New York and Washington – have already committed to making privacy and data security a priority.

See CSLR's two-part series on New York's new cybersecurity standards: "Expanding Definitions and Requirements" (Sep. 11, 2019); and "A Compliance Roadmap" (Sep. 18, 2019).

How to Protect Against (or Survive) a Cyber Attack

While no company can guarantee protection against sophisticated state actors, modest investments can significantly reduce the risks of a foreign cyberattack. Not only can these investments help limit reputational damage and civil liability, but also they can limit the harm to a company's business operations resulting from espionage, disruption and degradation.

With rising geopolitical tensions and evolving state-sponsored cyberthreats, companies should consider the following practices:

- Monitor existing and emerging laws to ensure compliance with federal, state and international cybersecurity requirements.
- Review and update information-security practices, analyzing both current and potential threats to an organization, and prepare an incident-response plan with clear instructions and responsibilities for relevant individuals.
- Provide employees and management regular information-security awareness training tailored to risks such as malware, phishing and spear phishing.
- Ensure that operating systems, software, servers and other applications are patched and updated in an appropriate, timely manner.
- Monitor internet traffic affecting key operational systems to detect attacks and the potential theft of company and consumer data.
- Perform due diligence on vendors to ensure that they have sufficient cybersecurity practices in place, especially cloud services or data service providers, and conduct regular audits or reviews of their cybersecurity practices.
- Consider additional technical safeguards —such as multi-factor authentication, password complexity and expiration rules, and encrypted/virtual private network connections—for remote-access and privileged/administrator accounts.
- Conduct periodic incident-response exercises involving appropriate information technology, management and legal staff.
- Establish relationships now with legal counsel, law enforcement and incident-response vendors so they are immediately available when an incident occurs.

Federal, state and foreign laws require companies to implement appropriate measures

to protect against cyber attacks, but the tools that foreign countries can bring to bear are different in scale and sophistication than what companies typically face from private actors. Unprepared businesses not only may suffer reputational or regulatory damage from the loss of consumer information, but also critical disruptions to their core business from state-sponsored attacks. While the goal of preventing any damage at all from a foreign cyber attack may not be realistic, companies can take several steps now to ensure that if an attack does occur they can identify it, protect their business and limit their legal exposure.

Amanda Lawrence is a partner in the Washington, D.C., office of Buckley LLP. She assists clients in managing cybersecurity, privacy, information security and vendor risks and compliance, as well as evaluating and addressing potential data security incidents, including drafting consumer and regulator notifications.

Sasha Leonhardt is a counsel in Buckley's Washington, D.C., office. He represents financial services industry clients in a broad range of enforcement, litigation and regulatory matters with a focus on privacy and data security issues. Mr. Leonhardt assists clients in resolving government investigations and enforcement actions before a wide variety of federal and state agencies.

James Chou is an associate in the firm's Washington, D.C., office. He assists clients in a broad range of transactional and regulatory matters with a focus on cybersecurity and privacy issues, which include security incident management and response. Previously, he was a Defense Analyst and Senior Operations Research Analyst for the U.S. Army.