Proskauer

Cybersecurity: Threats, Consequences, and the Regulatory Framework

Minding Your Business Blog on **May 20, 2020**

In today's world, cybersecurity breaches and threats are pervasive concerns for any business entity, without exception. Working from home arrangements due to COVID-19 constraints only magnify the risk and create further vulnerabilities for companies. Companies should be aware of (1) the key cyber threats they face, (2) the consequences of a breach, and (3) the statutory and regulatory framework governing cybersecurity. Cybersecurity breaches are unique in that an entity can both be the victim of the breach and still be found to have a degree of responsibility. Fortunately, there are precautionary measures that companies can implement to help prevent a breach and to mitigate the scope and damage of a breach if one were to occur. We will elaborate on the steps to take to guard against a breach and how to effectively respond to a breach in a forthcoming post.

Key Threats

In the United States alone in 2019, there were 467,361 complaints to the FBI of cybercrime, resulting in $3.5 million in losses. Globally, there were far more. In 2018, it is reported that there were 378 million victims of cybercrimes resulting in financial losses of $113 billion. There are many reasons for cyberattacks, including terrorism, hacktivism, and warfare; however, general crime is the most common reason that businesses suffer breaches. Attackers primarily utilize ransomware or a business email compromise scheme ("BEC scheme") to improperly gain access to money or valuable personal information. Both methods can result in serious damage to the breached entity.

In a ransomware attack, the hacker will lock and encrypt a client's computer data, then demand a ransom to restore access. In many cases, the victim must pay the cybercriminal within a set amount of time or risk losing access forever. However, as this is a criminal attack, paying the ransom does not ensure access will be restored. The risk to clients cannot be overstated: critical data can be forever damaged and lost.

BEC schemes are executed through phishing emails and also pose a material threat. An attacker will create an email that appears to be sent by a reliable and safe source such as a commonly used website like Netflix or Amazon, a government agency like the IRS or FBI, or even a high ranking person within the company like the CEO. The Financial Crimes Enforcement Network (FinCEN), an agency of the United States Department of the Treasury, published an alert warning of the emerging trend of such "imposter scams" related to COVID-19. Through such phishing emails, the email account of the target can be compromised resulting in the unauthorized transfer of funds, client or contact lists being stolen, or personal identifying information ("PII") being stolen. This stolen information is then typically sold on the Dark Web and is highly lucrative for these attackers.

Consequences of a Breach

To start, there are the obvious consequences of direct financial loss and the costs of responding to an attack. Responding to a successful attack is a very real and time consuming disruption to business operations. However, reputational harm is another impact that can also indirectly cause future difficulties and financial losses. The loss of investors', employees', or customers' trust in the company and its management can be hard to overcome. The attack can also lead to civil litigation, such as suits by individuals whose PII was compromised.

Additionally, a breach can trigger governmental and regulatory inquiries by the DOJ, SEC, FTC, FINRA, and even state attorney generals. The SEC has made it clear that cybersecurity is the "responsibility of every market participant" and that it will use its authority to bring cyber-related actions. Companies that suffer a breach can still be found to have a degree of responsibility for the breach.

Statutory and Regulatory Framework

The SEC's authority to require regulated entities, like investment advisers and broker-dealers, to implement policies procedures designed to protect against cyber-breaches is clear. Congress enacted the Graham Leach Bliley Act of 1999 which requires federal agencies to establish standards to safeguard security and confidentiality of customer records. The SEC complied with the Act by issuing the "Safeguard Rule" (Regulation S-P). This applies to registered broker-dealers, registered investment companies, and registered investment advisers. Regulation S-P requires such entities to have written policies and procedures reasonably designed to (a) ensure confidentiality of customer records and (b) protect against any anticipated threats or unauthorized access of customer information. Private funds and exempt reporting advisors should be aware of Regulation P issued by the Consumer Financial Protection Bureau, which mirrors Regulation S-P.

The SEC's authority to require public companies to prepare for and respond to cyber-breaches is less clear. There is no regulation analogous to Regulation S-P applicable to public companies. As a result, the SEC has had to find creative ways to require public companies to implement improved internal controls guarding against cyber-breaches. In October 2018, the SEC published a Section 21(a) Report of Investigation regarding cyber-breaches at several public companies. A 21(a) Report allows the SEC to publish findings from an investigation without charging any violations, but typically provides notice that (i) the SEC believes it could have charged a violation and (ii) it may charge violations in the future if it sees the same conduct again.

In the Report, the SEC explained that "Section 13(b)(2)(B)(i) and (iii) require certain issuers to 'devise and maintain a system of internal accounting controls sufficient to provide reasonable assurances that (i) transactions are executed in accordance with management's general or specific authorization,' and that '(iii) access to assets is permitted only in accordance with management's general or specific authorization.'" The SEC further explained that the public companies investigated each lost millions of dollars as a result of cyber-related frauds. While the SEC recognized that each company was a victim (which likely accounts for the SEC's decision to publish the Report rather than bringing enforcement actions), the SEC explained that the companies involved likely violated the internal accounting controls requirements under the Exchange Act.

Similarly, the SEC has taken somewhat extraordinary steps to explain the obligations of public companies to respond to and disclose significant cyber-breaches. In February 2018, the SEC issued clear guidance on disclosure obligations for public companies, explaining that public companies must disclose material cyber breaches and any material risks of cyber breaches in their periodic and other public SEC filings. The failure to disclose a breach can have sizeable financial consequences. For example, Altaba (formerly Yahoo!), paid a $35 million penalty to settle charges brought by the SEC relating to its failure to disclose a breach of personal data connected to user accounts.

The Federal Trade Commission ("FTC") has also been active in bring privacy and data security cases. The agency has successfully used Federal Trade Commission Act Section 5: Unfair or Deceptive Acts or Practices to pursue companies that have had breaches that exposed consumers' personal data. The FTC has applied the Act to cybersecurity breaches by stating that businesses operate deceptively when they fail to live up to their stated data security practices or when they fail to employ reasonable and appropriate measures to prevent unauthorized access to personal information. The FTC has also brought enforcement actions ensure that companies properly protect consumers' PII. Again, even when a company is the victim of a breach, it can still be held responsible for the breach by government agencies.

In addition to federal agency regulations, clients should be aware that almost all states require private entities to notify individuals of security breaches of information involving "personally identifiable information." These laws vary in terms of statutory structure and prosecutorial discretion. When an entity must notify individuals of a breach is also different from jurisdiction to jurisdiction. Some states only require that an entity notify the attorney general and only if the breach hits a particular threshold, while others require that entities notify individuals that a breach has occurred compromising their information no matter the significance. Regardless of these differences, states' attorney generals can impose penalties on companies for failure to protect PII.

Massachusetts' cybersecurity laws go beyond the Graham Leach Bliley Act and require that both employee and customer information are protected. The state has also issued a checklist to help entities comply with the law. At this time, Massachusetts has several additional pending bills relating to cybersecurity.

Notably, California now has a private right of action permitting victims of identity theft to bring a cause of action against a business for failure to protect their PII. The California Consumer Privacy Act of 2018 ("CCPA") became operative on January 1, 2020. This act generally requires that customers of qualifying businesses be able to know and control the information collected about them. Given the CCPA's broad definitions of consumers and businesses, investment funds and their managers may be considered "qualifying businesses" and information that they collect regarding their employees, job applicants, investors, and prospective investors residing in California could be subject to the CCPA.

Every state has its own laws and regulations making it vitally important to engage competent counsel to navigate the demands of the various jurisdictions that may be impacted by a breach.

* * *

Proskauer's cross-disciplinary, cross-jurisdictional Coronavirus Response Team is focused on supporting and addressing client concerns. Visit our Coronavirus Resource Center for guidance on risk management measures, practical steps businesses can take and resources to help manage ongoing operations.

View Original

Related Professionals

- **Margaret A. Dale**
  Partner