Proskauer

Private Equity and Cybersecurity: Threats, Consequences, and the Regulatory Framework

The Capital Commitment on **May 20, 2020**

Cybersecurity breaches and threats are pervasive concerns for any entity storing valuable data or managing large sums of money: private investment funds are no exception. Recently three private equity firms suffered breaches that compromised their email accounts and wire transfers, resulting in $1.3 million in losses. We have seen the SEC follow through on its 2019 priority of examining investment advisers about their cyber-security measures, as well as inquiring if they have suffered from a cyber-security breach. We expect that trend to continue. Fund sponsors 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. Fortunately, there are precautionary measures that fund sponsors can implement to help prevent a breach and to mitigate the scope and damage from a breach if one were to occur. We will elaborate on both 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. Through this phishing email, 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 such as 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' trust in the fund and its management can be hard to overcome and may create tensions between fund sponsors and investors. 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, FINRA, and even state attorney generals. 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. 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 that protect investors. If a fund or its manager have failed to take reasonable steps to protect investors' information, then the fund manager can be held accountable by the SEC.

Statutory and Regulatory Framework

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 this act by issuing the "Safeguard Rule" (Regulation S-P). This applies to registered broker-dealers, registered investment companies, and registered investment advisers. However, Regulation S-P does not specify what obligations a firm has in event of a cyber-breach in terms of disclosure and mitigation – in contrast to public companies, where there is clear guidance from the SEC on disclosure obligations.

The Consumer Financial Protection Bureau issued Regulation P. This regulation mirrors Regulation S-P and applies to exempt reporting advisers and private funds. It requires that these entities 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.

The SEC's Office of Compliance Inspections and Examinations ("OCIE") has repetitively identified cybersecurity as one of its priorities and the SEC has offered comments and guidance in how it will evaluate security breaches. In October 2018, the SEC issued a report explaining factors it would consider to determine whether businesses violated the federal securities laws by failing to have a sufficient system of internal controls to prevent losses from BEC and similar schemes. Failure to institute such internal controls or having insufficient internal controls could result in issues with the SEC, even when the fund sponsor is the victim of a cyber-attack. It is not uncommon for the SEC to request information about cyber controls or cyber breaches during an examination. In fact, up to now, the SEC has largely approached compliance with Regulation S-P through its examination program, rather than through enforcement actions. However, firms should be mindful that the SEC could bring an enforcement action in the case of a particularly large breach or become more aggressive under a new administration. We have seen the SEC remind private fund sponsors that they could also be held responsible for cyber breaches at a portfolio company if the company is a "control investment." Fund sponsors, particularly in the private equity buyout space, should make efforts to evaluate cyber risks and controls at such portfolio companies, particularly if they maintain or have access to any sort of PII.

In addition to federal agency regulations, fund sponsors 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 fund sponsors 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.

View Original

Related Professionals

- **Margaret A. Dale**
  Partner