Guidance on Cyber Threats to Private Equity and Hedge Funds

June 8, 2020

As the corporate world is evolving and becoming more accepting of working remotely, every company is facing the increased threat of cybercrimes. In 2019, the average cost of a data breach in the U.S. was more than $8 million, and the average time spent to identify and contain a breach was around 245 days. These numbers will continue to grow as cyber criminals become even more sophisticated.

Gone are the days where you could easily identify a phishing scam by an unrelated subject or misspelled words. Recently, three private equity firms suffered business email compromise ("BEC") schemes that resulted in over $1 million in losses. The hackers monitored employee email accounts for months in order to learn the specific workings of the company. They used email rules within Microsoft 365 to divert specific emails into a folder that they could monitor. They then used this knowledge to create a lookalike domain to send outbound messages requesting bank details, payments, transfers, etc. This attack, identified by CheckPoint®, involved the use of seven lookalike domains. However, they identified 29 others created by the hacking group since 2018. This suggests that the hackers will attack again.

The increased level of sophistication of cyberattacks make financial institutions more vulnerable. Most private equity firms and hedge funds lack the resources available to major banks or technology companies, and their cybersecurity measures suffer as a result. The SEC's recent guidance on best cybersecurity practices for financial service firms is a good place to start, but in many cases, makes recommendations that are simply outside of the realm of possibility for smaller companies.

The Financial Crimes Enforcement Network has recently issued an alert warning financial institutions to be vigilant in identifying fraudulent transactions similar to those that typically occur after a disaster, such as the COVID-19 outbreak. They urge these companies to come forward with concerns by reaching out to the Regulatory Support Section at 1-800-949-2732 or FRC@fincen.gov.

Consequences of Cybersecurity Breaches

Cybersecurity breaches can result in direct financial loss, reputational harm, loss of investors' trust, civil litigation, governmental and regulatory inquiries, and more. The Securities and Exchange Commission has deemed cybersecurity the "responsibility of every market participant" and has promised to use its authority to bring actions that protect investors. In 2019, they established a priority of examining investment advisers about their cybersecurity measures including asking if they have suffered a breach. Fund managers must take reasonable steps toward protecting investors' information at risk of being held directly accountable by the SEC. Until now, the SEC has usually approached compliance through examination rather than enforcement, but still reserves the right to bring an enforcement action in the case of a large breach.

What can you do?

The best way to prevent cybercrime and resulting litigation is to apply proper due diligence procedures, create a cultural awareness surrounding cybersecurity within the company, and take reasonable steps toward protecting confidential information.

Due Diligence

Capital One's March 2019 cybersecurity breach demonstrated that the security of your portfolio is crucial. A hacker gained access to Capital One credit card applications for consumers and small businesses from as early as 2005. Capital One detected the breach six months later. This particular breach was brought about through a misconfigured web application firewall.

With new data privacy laws both in the U.S. and the E.U., it is critical to review both cybersecurity and privacy mechanisms during due diligence on companies prior to any transaction. Review target companies for documentation related to previous or ongoing data breach investigations, policies and procedures in place in the event of a breach, and adherence to compliance standards and security frameworks where operational. In order to ensure proper privacy mechanisms, review how the company collects data, processes it, maintains it, and keeps it safe. Due diligence should also inquire into how data subjects are informed of data processing practices, rights and

obligations as well as how one could request a copy of their data and the turnaround time for that request. These compliance efforts, if missed, could have a material impact on the transaction due to heavy fines that are being levied by the regulatory bodies.

We would like to bring to your attention that 49% of M&A experts have seen deals derailed after due diligence brought an undisclosed breach to light, and 77% of experts had recommended that a particular company be acquired over another because of the strength of its cybersecurity program. It is good practice to do a test run on your cyber security due diligence procedures and inquiries by looking internally for vulnerabilities, before disclosing them in an acquisition situation.

Create Cultural Awareness around Cybersecurity

Starting with higher-level management, make sure that employees are following protocols when sending emails or posting on social media, as well as securing personal laptops and handheld devices. Undertake regular risk assessments and tests to make sure that cybersecurity practices are properly disseminated throughout the organization.

Take Reasonable Steps toward Cybersecurity – The Essential Eight

Our Redpoint Cybersecurity experts recommend companies follow eight essential and proactive steps that establish and define the basic tenets of cyber hygiene. They are:

1. Application control
2. Patch applications
3. User application hardening
4. Restriction of administrative privileges
5. Patch operating systems
6. Multi-factor authentication
7. Daily backups
8. Configuration of Microsoft Office® macro settings

For financial services firms, wire transfers are a particular vulnerability, specifically

through phishing attacks, so ensure that your wire transactions have a secondary verification route that bypasses the chance of compromised systems. Some more sophisticated options presented by the SEC are the use of systems that can detect and block data transmissions that contain sensitive information (such as Social Security or account numbers) and rigorous controls for system access (including randomly generated passcodes and immediate removal of access for employees who leave the company). If you're unsure on how to proceed, our team at Redpoint Cybersecurity is here to guide you. Requirements surrounding the necessary measures toward cybersecurity, and what to do when breached, vary state-to-state or country-to-country, so be sure to engage competent legal counsel to help you navigate the demands of various jurisdictions.

For more information and for help getting your fund secured against cyberattacks, please contact your Anchin Relationship Partner or Jeffrey Rosenthal at Jeffrey.Rosenthal@anchin.com, George Teixeira at George.Teixeira@anchin.com, or Tab Bradshaw at Tab@redpointcyber.com with any questions that you may have.