Private Equity: Prime Target For Cyberattacks

Why Your Risk May Be Higher Than You Realize

February 2022

LOCKTON®

AUTHOR

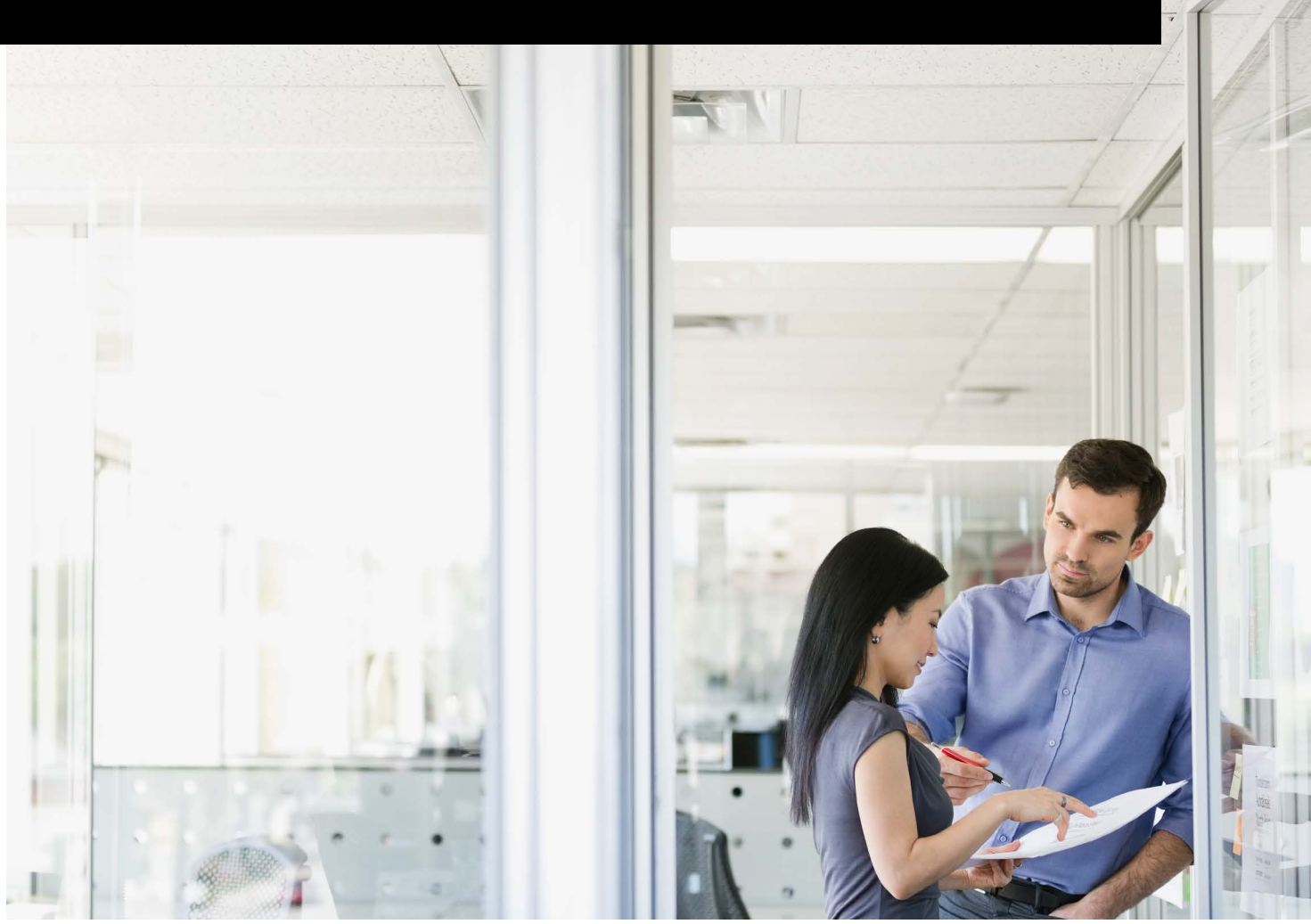
Elissa Doroff
Managing Director
Cyber Product Leader
Lockton Financial Services,
Pacific Series
O: 213.689.4278
M: 617.306.0520
edoroff@lockton.com

News about three British Private Equity (PE) firms that were scammed into transferring $1.3 million into fraudulent bank accounts[1] is just one example demonstrating Private Equity is not immune to cyberattacks.

IN FACT, PE FIRMS ARE BECOMING LUCRATIVE TARGETS for cybercrime, particularly as the volume of deals continues to draw public attention—and the interest of cyber criminals.

Bad actors are becoming increasingly sophisticated in their spoofing, targeted phishing, social engineering efforts and digital impersonation as seen in the case of the three British PE firms. In that attack, phishing emails targeted two staff members, one of which gave their credentials to the attacker. The attacks continued for several months in which four attempts were made to wire £1.1 million to fraudulent bank accounts in Hong Kong and the UK using bogus emails and registering look-alike domains. Ultimately, an emergency intervention salvaged £570,000 however, the rest of the money was permanently lost.

The substantial capital and sensitive client and market information at their disposal alone provide fertile ground for ransomware attacks. According to BitSight, a cyber risk analysis firm, financial services firms are 300 times as likely as other companies to be targeted by a cyberattack and "50% of these companies are at heightened risk of becoming a victim of ransomware." The FBI's warning on November 1, 2021[2] about the rise of ransomware attacks "...during significant financial events, such as mergers and acquisitions" is a timely reminder for private equity managers.



Stakes Even Higher for Private Equity

While cybersecurity is always a top priority for PE firms, the sheer increase in volume and velocity of transactions coupled with the shift to remote work in recent years presents additional threats and vulnerabilities for PE firms and their portfolio companies.

With expedited M&A timelines, many PE firms are only able to complete light IT security diligence. There are frequently comprehensive post-close initiatives to improve the portfolio company's posture, but this takes time to implement, which leads to vulnerabilities prior to completion. Even with improved controls, there is still the human risk element as well as a constant increase in the sophistication of cyberattacks that make prior best practices quickly outdated.

Since the onset of the pandemic, day-to-day operations for PE firms and their portfolio companies have been in a state of turbulence by remote work practices. PE firms managing multiple portfolios of companies with disparate security systems, controls and protocols only multiplies their exposure to cyber risk.

Financial services firms are 300 times as likely as other companies to be targeted by a cyberattack and "50% of these companies are at heightened risk of becoming a victim of ransomware."

Few would dispute that private equity firms are highly vulnerable to cyberattacks, and their most costly weaknesses may lie hidden within their portfolio companies, vendors, and third-party suppliers. Prominent data breaches in recent years have shown the far-reaching impact of cyberattacks on PE firms and the scale of impact on the value of a compromised portfolio company[3]. Investigation and remediation expenses of third-party breaches have proven exponentially more costly than the average individual breach[4]. Compounding these losses are the millions of dollars in potential legal fees, losses due to business interruption and reputational damage that often result from exposing sensitive client information.

Evolving and More Complex Regulation

The dynamic regulatory landscape further compounds the complexity of a private equity firm's cyber risk profile. Since private equity firms have portfolio companies operating in several jurisdictions, they are subject to an increasingly more onerous regulatory regime. With unique data and privacy rules in over 60 countries (and several states in the U.S. with similar measures) failing to comply with any of these regulations can result in regulatory fines and penalties, liability to third parties, including shareholder litigation and potential executive liability as well as damage to brand and reputation. Private equity firms that fail to do cybersecurity due diligence on their portfolio companies may fall outside the duty of care framework set forth by the US Securities and Exchange Commission (SEC) in 2018.

Furthermore, the US Federal Trade Commission (FTC) revised its Safeguards Rule to broaden the definition of "financial institutions" not subject to oversight by regulators such as the SEC. The revised rule[5], which will come into full effect in December 2022, will impose stricter cybersecurity requirements on private funds. The rule requires that companies involved in financial activities, even incidental activities, should thoroughly review their information security program and make sure it is compliant with the new Safeguards Rule. Specifically, the rule sets forth particular safeguards the information security program must include such as access controls, data inventory and classification, encryption, secure development practices, authentication, information disposal procedures, change management, and testing, and incident response.

The new Safeguards Rule requires financial institutions to implement the following policies to ensure effective employee training and oversight of service providers: (1) general employee training; (2) use of qualified information security personnel; (3) specific training for information security personnel; and (4) verification that security personnel are taking steps to maintain current knowledge on security issues.

Additionally, the new Safeguards Rule adds mechanisms designed to ensure employee training and oversight of service providers are effectual. This requires financial institutions to implement policies and procedures that include four main components: (1) general employee training; (2) use of qualified information security personnel; (3) specific training for information security personnel; and (4) verification that security personnel are taking steps to maintain current knowledge on security issues.

Also, in January of 2022, The Washington Post reported[6] that Congress may overhaul federal cybersecurity rules for the first time in eight years. If Congress acts, then any law enacted is certain to change, and potentially complicate, the regulatory environment faced by PE firms and their portfolio companies.

Regulators aren't the only ones motivated to act by the growth of cyber risks facing companies. The proliferation of cyber threats and need for more stringent network security has also contributed to a growing investor focus on environmental, social, and governance (ESG) issues, thus adding further pressure on private equity firms to consider the data and privacy strength of their portfolio companies.

Considering annual global cybercrime costs are estimated to reach $10.5 trillion USD[7], anticipating cyber threats and managing cyber risk throughout its ecosystem should be a top priority for private equity firms. Proactive measures to ensure compliance with evolving regulatory regimes along with sound cybersecurity systems, protocols and procedures will be vital to mitigating risk, reducing the impact of loss and safeguarding the profitability of portfolio companies.

Some Immediate Actions

What can a Private Equity firm do immediately? As a preliminary matter, it must determine the cybersecurity strength – or lack thereof – within its portfolio companies. Then it needs a consistent approach to give those companies a minimum threshold of cybersecurity proficiency and an adequate limit of insurance to properly protect the portfolio company's balance sheet and the PE firm's investment.

In November 2021, the Institutional Limited Partners Association (ILPA), a global organization dedicated to supporting the interests of limited partners, issued a new standardized due diligence questionnaire (DDQ) with added cybersecurity components. According to the ILPA website, the purpose of the revised DDQ is "to standardize the key areas of inquiry posed by investors during their diligence of managers."

According to ILPA, the best approach for managing cyber risk is to develop an informed perspective by way of a streamlined and manageable process that treats cyber risk equal to other types of risk, like market risk, counterparty risk, and legal risk.

Similarly, performing a comprehensive assessment of risks and threats in the target company's IT environment should be a standard protocol for those entities still in the due diligence process.

Private Equity firms just like any other industry, should have tools and procedures in place to detect threats as well as respond in the case of an incident. Confirmation of all the above protocols and procedures at the target entity should be paramount as part of the due diligence process.

Some additional best practices include:

- Make cybersecurity a regular board agenda item
- Ensure some board members have the appropriate technical background, experience and/or education to make informed decisions about the organization's cybersecurity risk and policies
- Regularly consider technological improvements, compliance assessments and implementations, and risk transfer mechanisms to improve the complete cyber risk posture
- Implement regular cybersecurity audit protocols for the organization and its supply chains
- Commit to and allocate sufficient resources for preventive measures, technological improvements and cyber insurance
- Establish adequate measures to take in the event of a supply chain cyberattack

As cybercrime grows, firms need to deploy enterprise cybersecurity strategies and systems that evolve with it. Lockton's Private Equity Practice provides made-to-measure, reliable risk transfer and insurance solutions for private equity firms and their portfolio companies.

[1]Woodman, Andrew. "Cybercriminals Scam Three UK PE Firms in £1.1m Heist." PitchBook, April 23, 2020

[2]Lloyd, Timothy, "FBI Warns of Ransomware Leveraging 'Significant Financial Events'." Private Funds CFO, November 8, 2021.

[3]Harragan, Paul. "Three Reasons Private Equity Firms Should Pay Attention to Cybersecurity." EY, October 16, 2020.

[4]"What's the Impact of a Third Party Data Breach?" SecurityScorecard.

[5]"Private Fund Cybersecurity Requirements Changing Significantly in 2022." Lexology. Ropes & Gray LLP, January 5, 2022.

[6]Marks, Joseph, and Aaron Schaffer. "Analysis | Congress to Update Government Cyber Rules, One Year after Solarwinds." *The Washington Post*. WP Company, January 12, 2022.

[7]Freeze, Di. "Cybercrime to Cost the World $10.5 Trillion Annually by 2025." *Cybercrime Magazine*, April 27, 2021.

UNCOMMONLY INDEPENDENT