TERRY MASON
DIRECTOR
HKA

Cybersecurity in private equity – time to take a closer look at portfolio companies

Cyber threats, along with related regulatory requirements, continue to evolve at a rapid pace, challenging even the most operationally mature firms to properly manage the risks. In 2021, we have seen gloomy headlines focused on ransomware, wire fraud and "supply chain" attacks, as well as run-of-the-mill data theft. As we move into 2022, these headlines may become even more prevalent, as firms' technology footprints continue to expand into the cloud and other digital platforms, along with risks of cyber-attacks within these technology environments.

It is difficult to overstate the ongoing impact of cyber-crime. Damages from cyber-crime are projected to reach $6 trillion in 2021 and continue rising to an estimated $10.5 trillion annually by 2025.

Regulators and lawmakers in the US and around the globe are being challenged to keep up with both technological advancements and related security risks, including insecure software, email phishing attacks and security issues surrounding internet-connected devices. Significant advances in legislation and oversight targeted at the appropriate management of cyber risks, both in the public and private sector, are emerging almost weekly. In addition, data privacy for individuals (e.g., customers and employees) has taken center stage due to frequent data breaches that spill personal information onto internet crime forums. Also in focus is how organizations manage response efforts in the event of a major cyber incident such as a successful ransomware attack. Some important recent legislative and regulatory advancements in cybersecurity in the US include:

- The Biden administration's executive order for federal agencies to better secure systems
- Data privacy laws such as the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA)
- Enforcement actions from the New York Department of Financial Services (NYDFS) and the US Securities and Exchange Commission (SEC) against companies in the brokerage, insurance and tech industries for insufficient cyber protections and the failure to properly disclose them

Cybersecurity in Private Equity

In the private equity (PE) space, cyber risk and threat awareness among General Partners (GPs) is on the rise. A strong driver of this shift is Limited Partners (LPs), who want a better understanding of how firms are securing their own environments and also how firms are addressing cyber risks with their portfolio companies.

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." A primary area of concern is PE firms' cybersecurity policies and procedures.

"Private equity firms that fail to do cybersecurity due diligence on their portfolio companies would fall under issues with the duty of care framework set forth by the SEC in 2018."

ILPA states on its website that the new questionnaire will help "ensure that the DDQ reflects emerging practices and norms, as well as transformation in technology, operating processes and industry best practices."

Such due diligence is crucial in the PE space. Igor Rozenblit, a former SEC official, shared his perspective on cyber due diligence while speaking at an HKA roundtable on SEC exam readiness in September 2021. While at the SEC, Rozenblit was founder and co-head of the SEC Division of Examinations' Private Funds Unit, and co-lead for the agency's inter-divisional Private Fund Specialized Working Group.

"Private equity firms that fail to do cybersecurity due diligence on their portfolio companies would fall under issues with the duty of care framework set forth by the SEC in 2018," Rozenblit said.

How should PE firms respond to these risks?
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 as equally as other types of risk, for example market risk, counterparty risk and legal risk.

Formal practices for managing cyber risk should align with other risk management approaches that are in place, where cyber risk is treated as just another risk. The SEC has encouraged developing a "reasonably" designed approach to managing cyber risk, such as one that reflects the following characteristics:

- *Informed* – supports and promotes an awareness of today's cyber risks, including regulatory and legal considerations
- *Manageable* – risk evaluation, if performed in a manner that is manageable, does not overwhelm the business and does not negatively impact day-to-day operations

- *Digestible* – reporting "in plain English" is generated that can easily be consumed by a firms' risk leads, including COOs, deal teams and boards of directors
- *Actionable* – reporting is clear and includes *reasonable* next steps to address key identified cyber risks

An effective approach to addressing cyber risk with portfolio companies

Should a PE firm or one of its portfolio companies be impacted by a serious cybersecurity event, the reputation of the firm among investors, regulators and other stakeholders may be on the line.

When planning a cybersecurity review of portfolio companies, consider one with the following attributes:

- *Efficient* – a summary review that is supported by at least one established cybersecurity control framework (e.g., NIST, ISO). A comprehensive security risk assessment likely is not required.
- *Measurable* – quantitative and baselined, with clear outputs from assessment activities
- *Repeatable* – can be executed periodically to capture potential changes in portfolio companies' cyber risk, such as changes in the technology environment (e.g., moving systems to the cloud)
- *Actionable* – clear reporting that includes *reasonable* next steps for portfolio companies to address any urgent identified cyber risks

Conclusion

As cyber threats continue to proliferate, anticipating and managing them at all organizational levels will remain vital during 2022 and beyond. As recent events have proved, PE firms are vulnerable on a variety of fronts, from their vendors and third-party suppliers to their portfolio companies. Taking steps now to ensure compliance with evolving protective regulations and leading practices can help reduce this risk and help ensure that portfolio companies generate profits—not headaches—for PE firms.

This article is courtesy of HKA Global, Inc., a leading global consultancy for multi-disciplinary expert and specialist services in risk mitigation and dispute resolution. We employ more than 1,000 consultants, experts and advisors in more than 40 offices across 17 countries. Our team has extensive experience advising clients on the economic impact of commercial and investment treaty disputes, forensic accounting matters and cybersecurity and privacy governance and compliance. We are experienced in working with PE firms, as well as with companies in business and consumer services; digital, technology and media; financial services; healthcare, medical technology and pharmaceuticals; and manufacturing and industrials. This breadth of experience affords HKA a unique

HKA

understanding of the potential cyber risk exposure of firms' portfolio companies.

The opinions expressed in this article are the views of the author alone and should not be attributed to any other individual or entity. The article is intended for general educational purposes only—it does not constitute legal, accounting, insurance, or other professional advice, and it should not be relied upon as the basis for your business decisions.

If you require any further information, please contact Terry Mason at terrymason@hka.com.