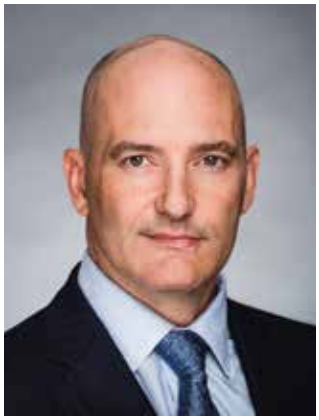
KEYNOTE INTERVIEW

How cyber-risk is reshaping private equity



The traditional PE approach to managing risk won't work with ever-evolving cybersecurity risks, says Jon Moore, Clearwater's chief risk officer and head of consulting services and customer success

In the ever-changing landscape of cybersecurity risks, private equity firms face a growing array of challenges. Clearwater's chief risk officer and head of consulting services and customer success, Jon Moore, discusses the emerging threats and shares insights on how PE firms can adapt their approach to cyber-risk management, moving beyond traditional approaches to protect their investments and portfolio companies better.

Q What do you see on the horizon for cybersecurity risks in the next year or two, especially the risks that private equity firms will encounter?

SPONSOR
CLEARWATER

Private equity firms' investments are only as secure as the companies in which they have invested. Today those companies face many cyber-risks.

One growing vulnerability is cloud misconfiguration. More companies are leveraging the cloud to host their solutions and infrastructure. Cloud-based solutions and infrastructure can be very powerful tools, but they're also very complex. With that complexity comes a high risk of misconfiguration that can, in turn, result in a breach. The classic cases are where data repositories or virtual servers are set up in the cloud, they've been misconfigured, and now they're publicly accessible. Basically, anyone with a browser can find them and access them. That can be particularly problematic when those resources contain proprietary or confidential client information or connect with other cloud assets that house this type of information.

There are other more subtle vulnerabilities that may be exploited in the cloud as well, such as misconfigured identity and access controls or stored secrets in places that are accessible to hackers.

Ransomware will likely continue to be an ongoing problem, particularly for

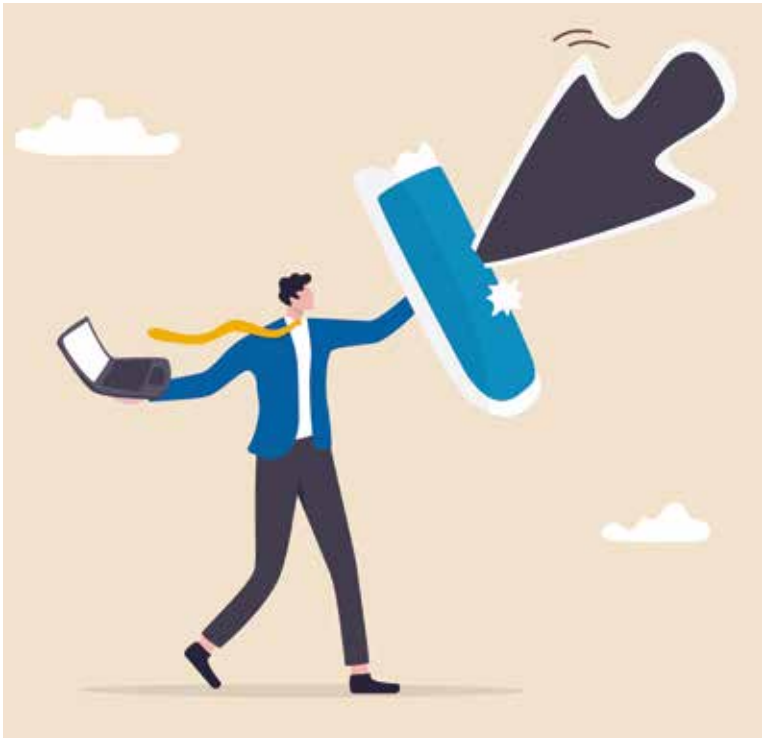
"We don't yet fully understand the risk to or from AI and machine learning-powered solutions"

the healthcare industry, which has been particularly hard hit. We know of portfolio companies that have been shut down due to ransomware attacks, and it's never a good feeling if you're a PE investor in one of those organizations.

I think there are going to be increasing federal and state-level compliance requirements, perhaps both at the PE level as well as at the portfolio level. Organizations must understand and manage their compliance with these potentially complex requirements.

There are also emerging technology risks around artificial intelligence and machine learning solutions. For example, there have been many discussions recently around the use of artificial intelligence tools and, in particular, ChatGPT. This language model allows attackers to craft better phishing emails and better business email compromise attacks.

We don't yet fully understand the risk to or from AI and machine learning-powered solutions. There are all the classic security risks to the confidentiality, integrity, and availability of the information. But beyond that, there are specialized attacks that allow attackers s to steal the AI or machine learning algorithms or poison the data that's been used to train these algorithms – either of which could have a significant impact from a business perspective.



Q How are you advising PE managers and their firms to adapt to evolving cyber-risks?

Traditionally, PE firms rely on their board representation to understand and manage risk at the investment level, and in most cases, with traditional business risks like financial risk, this is perfectly acceptable. Typically, the people serving in those board positions are well-qualified to understand and manage those business risks. However, those same folks are not typically familiar enough with cyber to be able to understand and manage cyber-risk; they don't have that experience and level of expertise.

To address this challenge, we typically work with PE firms to create a standard method of evaluating the cybersecurity programs at their portfolio companies. We help them understand if the programs are reasonable and appropriate for the companies and what if any investments the companies might consider to further strengthen their programs. We then assist the PE firm in monitoring their investments' cyber-programs over the life of their investment.

Another service we are often asked to deliver is educating the investment team on cybersecurity and compliance. We have found PE managers eager to become more knowledgeable to make better, more informed decisions.

Q What are the key criteria to keep in mind when implementing cyber-risk

management at the portfolio level and at the enterprise?

When implementing cyber-risk management at the enterprise level, there is a need to go deep. First, an organization must understand how it will frame risk. This means how it will define, evaluate, and manage its risk. Also, its leadership needs to determine the organization's risk threshold or how much risk it is willing to accept.

Next, the organization needs to assess its risk. This includes looking at each of its information assets and the safeguards in place to protect those assets, identifying all reasonably anticipated threats and vulnerabilities to the confidentiality, integrity and availability of the information processed by those assets, and determining how likely it is that a threat will exploit a vulnerability given the safeguards in place and the impact to the organization if that were to occur.

Once the risks are identified, the organization needs to make a treatment decision on what it will do with the risk. Risks below the organization's threshold are typically accepted, those above the threshold may be accepted, but typically the organization will look to avoid, transfer or mitigate the risk. The organization should document its treatment decisions and have a plan for any mitigation.

Finally, the organization needs to monitor its environment on an ongoing basis to make sure that the actions it has taken are sufficient to continue to keep its cyber-risk at an acceptable level.

Implementing cyber-risk management is a bit less complicated at the portfolio level. The goal is to understand the rigor of the cybersecurity programs in place at the portfolio companies and assess if the programs are reasonable and appropriate given the size and nature of the organization as well as the level of investment by the PE firm.

There is inevitably a desire by the PE firm to make the process not too burdensome on the portfolio companies, so much effort is placed on maximizing the information collected while minimizing the amount of time and inconvenience required of the portfolio companies' teams. In the end, the PE firms end up with an understanding of relative cyber-risk across their portfolio companies and where they might best spend their resources to minimize their risk and maximize their return on investment.

Q What are some common mistakes you see PE firms making with their cyber-risk management?

One mistake is relying too much on their representation on the boards of their portfolio companies to understand and manage their risk. Often, folks just don't have the experience and expertise necessary to do that effectively.

Another thing we hear is that each portfolio company is doing different kinds of assessments and looking at risk and their security programs in different ways. The PE firm can't make sense of any of it on a portfolio level because they're comparing apples and oranges, making it difficult to understand the relative risk between investments and the risk likelihood. It's easy for them to understand the potential impact because they know the size of their investments. But it's harder to know how likely any one of their portfolio companies is to suffer an incident that's going to have a financial impact on them. That lack of information for decision-making purposes is a common problem.

"Ransomware will likely continue to be an ongoing problem, particularly for the healthcare industry"

Q How can PE managers calculate what's at stake from cybersecurity risks, and the return on investment for cyber-risk management measures?

Ultimately you could lose it all. We've seen organizations go out of business from cyber-events. That is, of course, a worst-case scenario, but it's happened. What seems to work best is helping them think through the potential business impact of a breach. For example, we might ask PE managers: If the systems are down, how much would they lose each day? What's the impact?

We help them think through some of these scenarios. If it's a healthcare organization, we talk to them about how many records they have within their systems and how it will likely cost $400 or $500 per record if they have a breach. What does that look like from an organizational perspective, and what would be the impact on the portfolio company?

We also ask them to consider the different types of threats and how susceptible their organization is to each and compare the potential impact to the cost of mitigation. For example, on average a successful phishing email attack has an average impact—for a US manufacturer, of $4.35 million—while the cost of a phishing email education program and assessment will typically be less than 1 percent of that amount. ■