FUNDfire

Managers Face 'More Intense' Cyberthreats, Larger Losses

By Tom Stabile August 18, 2021

Private equity fund managers are increasingly aware of the risks from hacking attacks to their businesses and portfolio company investments, but many remain unprepared to adequately defend against or manage incidents – especially at their portfolio companies.

Managers have cybersecurity risks on their radar, but only some are prepared for the gut punch of today's threats with adequate technology defenses or insurance protection, says Robin Cohen, chair of Cohen Ziffer Frenchman & McKenna, a law firm specializing in insurance coverage.

"It's moving very quickly, and private equity firms are sensitized to it," she said. "But not a lot have been hit yet, and when it hits them, it hits hard."

Ransomware attacks in particular have escalated in technical complexity, frequency and damage, Cohen said.

"Hacking has been more intense, and they're accessing critical, confidential information, so the losses are larger," she said. "These groups are more sophisticated in the way they're hacking and more aggressive."

The past 12 months have featured several signature attacks impacting private funds, said Tari Schreider, senior analyst at Aite-Novarica Group, a strategic consultant. Those include Sequoia Capital telling investors of a hack in February, according to Axios, and major breaches against portfolio companies such as SolarWinds – a technology firm that Silver Lake and Thoma Bravo had stakes in – and FireEye, a cybersecurity firm in which Blackstone Group had invested.

"We put private equity firms in the same bucket as hospitals and government – historically lax in security," he said.

Managers are not only facing pressure from the risk of loss but also increasingly from regulators and their own investors, who are adding cybersecurity as part of the criteria under environmental, social and governance due diligence efforts, said Teresa Cutter,

head of ESG and impact at White Oak Global Advisors, an $8 billion private credit manager. There is significant and ongoing risk to portfolio company value from such attacks, she said.

“Equifax lost $700 million and had a 30% drop in share price after their [hacking attack],” she added. “Look at that kind of impact and pair it with increased digitization, more people working in hybrid environments or working from home, which bring more potential to be breached… It’s going to be a growing area of importance for limited partners to have managers that are focused on cyber-resilience for themselves and their borrowers and portfolio companies.”

The greatest point of exposure for private funds is typically through their portfolio companies, which can suffer actual money losses, but also business down time, remediation costs and reputation damage, Cohen said.

“Attacks can harm their investments in a big way,” she said.

The swirl of attacks and increased scrutiny have at least brought more private fund managers to the market looking for solutions, said Jason Elmer, CEO at Drawbridge, a cybersecurity provider. One of its latest tools is a private equity module that allows managers to monitor portfolio company cybersecurity controls, supply chain risk and policy compliance in real time.

“We’ve seen engagement over the last 18 months ticking up significantly,” he said. “There have been a lot of recent catalysts… A lot of people who had not taken it seriously have begun to take it seriously.”

But there is little consistency in how private fund managers approach preparing for such risks, Cohen said. Some are more focused on technology security, and others on insurance protection, she said.

Insurance coverage for cyberattacks spans across several potential areas of loss, Cohen said. The most common policies handle claims for the cost of investigations into a security breach; restoration of damaged digital assets and computer systems to their prior state; ransomware payments; and business interruption losses, such as profits forgone when services are down. Some policies also cover privacy breach liability protection against consumer class action and other third party lawsuits or – in certain states – reimburse the cost of regulatory fines and penalties, she said.

Few standard terms apply to cybersecurity coverage for private equity managers, with firms often negotiating custom features, Cohen said. Policies often have higher total policy coverage limits but stricter sub-limits for each individual claim type or narrow timeframes during which they will pay out claims, she said.

“Policyholders are more sophisticated now on what to request,” she said. “They’re hiring brokers to advise them.”

But even if they have coverage and systems protection, private equity firms that experience attacks have tough choices to make, Cohen said. For instance, in the case of ransomware, some managers agonize over the decision of whether to pay up but risk inviting hackers to make future intrusions, or to endure potential data loss and business interruption, she said.

“That’s an analysis the CEO or CFO has to do,” she said. “It’s important for each firm to make the right strategy call.”