Cyber Threats, Responses and Preventative Measures

With Schulte Roth & Zabel's Cybersecurity & Data Privacy Group

HAMLIN LOVELL

For an investment manager, the consequences of a cyberattack can be devastating. "It is not just about alerting investors to data breaches. If, due to a cyberattack, systems are completely shut down for a week or two, and fund managers cannot trade, they cannot fulfil their fiduciary duty to investors," says Edward Sadtler, head of the Intellectual Property, Sourcing & Technology group, and a member of the Cybersecurity & Data Privacy group, at Schulte Roth and Zabel.

Cyberattacks are hitting many parts of the financial industry, including hedge funds. In November 2020, reports surfaced of a potent attack against an Australian hedge fund initiated through a false Zoom invite that led to the loss of millions of dollars and ultimate closure of the fund. "The incident is just one example of increasingly sophisticated cyberattacks taking place all over the world. Hedge funds are particularly vulnerable, because they handle large amounts of money – but may have cybersecurity operations that are lean relative to large financial institutions," Sadtler points out.

"It's no surprise that CISA (the US Department of Homeland Security Cybersecurity and Infrastructure Security Agency) and other regulators, such as the SEC Division of Examinations (previously the Office of Compliance and Inspections (OCIE)) in the US, have repeatedly issued alerts urging companies to take the issue of cyberattacks seriously," says Sadtler.

Ransomware attacks

Cyberattacks might sometimes be a form of purely malicious vandalism but are more often motivated by the potential to extract ransoms from victims. "The size of ransoms could run into six, seven or even eight figure US dollar amounts, and we are seeing increased instances in which these are paid because the costs of systems being down for weeks could be much higher," Sadtler notes. "CISA's announcement on January 21 of a new public awareness program focused on ransomware underscores the continued threat presented by ransomware attacks," adds Sadtler.

However, advisories issued by the Department of Treasury at the end of 2020 create a quandary for fund managers faced with a ransomware attack. "Ransoms raise the age-old question of whether to negotiate with terrorists," says Kelly Koscuiszka, Special Counsel and a member of the Cybersecurity & Data Privacy group at Schulte Roth & Zabel LLP. "The guidance from Treasury warns that paying a ransom to Specially Designated Nationals could lead to sanctions. This has taken the option of paying ransom, which might otherwise be economically efficient, off the table in many cases," observes Koscuiszka.

Cyber risk insurance or cyber liability coverage (CLIC), which has existed since at least 1997, can provide a means to blunt the impact of a ransomware attack. "Ransoms can be covered by cyber insurance policies, though involving the insurance company in the response process can be critical to ensuring a payout," explains Ted Keyes, Special Counsel in the Insurance and Cybersecurity & Data Privacy groups at Schulte Roth & Zabel.

"Perpetrators of ransomware attacks often demand that ransoms be paid through cryptocurrencies such as bitcoin, rather than a traditional bank approach," adds Sadtler. "This is part of the great lengths cybercriminals often take to mask their identities. This makes planning for an attack all the more important."

As for the tax treatment of a ransom, Andi Mandell, a tax partner at Schulte Roth & Zabel points out "while there is no black letter law on the tax treatment of ransomware payments, there are two provisions of the tax code that provide justification for including them. First, there is a strong argument that a ransom payment is a deductible business expense under Section 162. These payments are becoming increasingly more commonplace for businesses and are certainly necessary if needed to regain control of a company's network or continue operations. Alternatively, a reasonable argument can be made that a ransom payment is a deductible theft loss under Section 165. The IRS has previously ruled a ransom payment was fully deductible under Section 165 when a key employee was kidnapped. Given that functioning systems and access to company data are essential to business continuity, it seems likely the IRS would find ransomware payments fully deductible as a theft loss as well".

However, the guidance from Treasury remains important to keep in mind. There is no payment that would be deductible if it was considered an illegal payment under either federal or state law," Mandell cautions.

Potential liability and investor disclosure

"Asset managers, fund directors, and third-party service providers could all potentially bear liability for cyberattacks, under their contracts and obligations to maintain data security. Laws relate to who owns or controls the data, and fund managers could be responsible for determining if data has been correctly accessed under US state laws," says Sadtler.

Many cyberattacks affect asset managers by infiltrating the systems of their service providers, such as fund administrators or IT service providers. "Even if it isn't your own systems that are attacked, you may be responsible for notifying investors whose personal data has been exposed or

compromised due to an attack on your service provider. Most state data breach notification laws create obligations on the entity who owns or controls the data, which is generally considered to be the fund in the case of information about its investors that is processed by a service provider," says Sadtler.

Even in situations where there is no statutory obligation to report a breach, interpretations of the concept of fiduciary duty might require asset managers to disclose a ransomware or other cyberattack to investors. "Fiduciary duty requires disclosure of all material matters, which is inherently very fact specific. There are suspicious emails and spear phishing attempts frequently, but they're not necessarily material. On the other hand, a ransomware attack that shuts down trading operations for a few days is likely going to be material to investors. We find that institutional investors are increasingly sophisticated on cyber risks and probe on these issues during initial and then periodic due diligence. Therefore, managers are formulating disclosures that provide transparency on material breaches," explains Koscuiszka.

Risk mitigation

"Conducting a tabletop exercise is a great way to pressure test a manager's preparedness for a cyberattack. An IT consultant walks IT team members and compliance officers through a simulated cybersecurity attack. I've found these exercises really drive home the importance of having a detailed, written response plan," says Sadtler. "A clear response tree, indicating internal and external persons who should be contacted and when, with contingency plans if someone is unavailable, should be part of that plan," he clarifies.

Due to COVID-19, personnel of many fund managers are working from home. This has heightened the risks of cyberattacks. "To mitigate these risks, firms should ensure they are updating software to ensure the most recent patches on an ongoing basis, and malware protection software is being utilized. Many firms are not updating it as often or as methodically as they could," says Sadtler. "Phishing attacks on emails are a key way in which security can be breached and may be catching people unawares in work from home situations. Periodic training for staff members to identify phishing attacks is essential," adds Sadtler.

Written policies and procedures for cybersecurity due diligence on service providers are also critical to cyber preparedness. "Regulators continue to exhort firms to develop policies for conducting cybersecurity due diligence on vendors, and rightfully so given the high incidence at which fund managers are impacted by cyber-attacks targeting their vendors," says Sadtler.

"Lawyers can help clients in conducting cybersecurity due diligence by ensuring clients are asking the right questions and documenting responses in the right way," Sadtler explains.

The new administration has already signalled that taking measures to address the cyberattacks threatening the nation's businesses will be a priority. "We're likely to see new regulations in this area. Monitoring developments, particularly changes that would impact fund managers, will be important," notes Koscuiszka. **THFJ**