Professional Perspective

Tips for Fund Managers Responding to Cyberattacks

Edward Sadtler, Kelly Koscuiszka, and Edward Nasti, Schulte Roth & Zabel

Bloomberg Law

Tips for Fund Managers Responding to Cyberattacks

Contributed by Edward Sadtler, Kelly Koscuiszka, and Edward Nasti, Schulte Roth & Zabel

In 2021, private fund managers faced a persistent wave of cyberattacks with potential to inflict devastating harm. In a ransomware attack—the fastest-growing type of cyberattack—perpetrators threaten to take action that would result in a wholesale inability to access critical systems if the ransom is not paid. Perpetrators often increase the pressure to pay the ransom by threatening to publicly expose the name of the victim or sensitive information about the victim's investors. Cyberattacks continue to grow in frequency and scope, as new reports claim that the group responsible for the SolarWinds attack targeted more than 600 organizations with nearly 23,000 attacks in its latest campaign.

The Securities and Exchange Commission has been increasingly aggressive in enforcing requirements for managers to maintain reasonable cybersecurity policies. In August 2021, the SEC announced three enforcement actions against fund managers and broker-dealers for cybersecurity deficiencies.

While many fund managers have stepped up their cybersecurity programs, cybercriminals continue to develop new ways to circumvent security measures. As fiduciaries that hold sensitive financial information, fund managers should be periodically evaluating and testing their preparedness for a cyber event.

This article provides fund managers with practical strategies for incident response.

Incident Response Plan

The foundation of an effective cybersecurity breach response is the development and maintenance of an incident response plan. An IRP can be included as part of, or attached to, the firm's information security policy. By establishing policies and identifying resources for responding to a cyberattack before it happens, an IRP frees up resources to focus on assessing the nature of the specific attack at hand and taking measures to remediate and contain it. In fact, SEC cybersecurity guidance advises registrants to have an IRP and offers recommendations on what an IRP should cover.

Cyberattack Response Checklist

Mobilize Your Internal Breach Response Team

Effective communication within a firm is critical for a successful cyberattack response. Precious time that could be spent evaluating and containing a breach can otherwise be lost figuring out who is responsible for what. An IRP that contains a detailed communications plan that the firm can put into motion as soon as it identifies an actual or potential breach can aid mobilization of an internal team.

For most fund managers, the cyber response team should include at a minimum:

- Chief compliance officer
- General counsel or other senior members of the legal team
- Senior IT staff
- IR team members

Depending on the breach and how the firm is organized, the team may also include persons such as:

- Chief information officer
- Chief operating officer
- Human resources representatives

Principals should be alerted to, and kept abreast of, the steps being taken to resolve any potentially serious breach. The SEC staff and the National Futures Association stress the importance of senior management playing an active role in cybersecurity matters. See, e.g., SEC Division of Examinations (formerly OCIE) Alert; NFA Interpretive Notice 9070, NFA Compliance Rules 2-9, 2-36 and 2-49: Information Systems Security Programs (eff. Mar. 1, 2016).

For each of the members of the internal breach response team, the IRP should identify:

- The member's name
- Contact information
- Contact information that can be used if IT or telephone systems are inoperable
- Alternate contact persons if a member of the team is unable to be reached

Assemble a Team of External Advisers

Once the internal breach response team has mobilized, it should engage with outside advisers to assist with identifying and implementing steps to thwart, contain, and otherwise remediate the breach. In most instances, outside advisers engaged include IT consultants—with specialized experience in breach response and conducting forensic investigations—and outside legal counsel.

Fund managers who have not yet established a slate of advisers should consider making those connections now and updating their IRP. In determining how they work with legal and other external advisers, fund managers should consider privilege issues. See generally, e.g., *In re Capital One Consumer Data Sec. Breach Litig.*, 488 F. Supp. 3d 374 (E.D. Va. 2020) (requiring disclosure of privileged documents when business or regulatory (rather than legal) concerns would have generated the same materials).

When selecting outside advisers, fund managers should be aware that certain mitigation service providers, such as entities that facilitate ransomware payments—for example, some digital forensics and incident response companies—could engage in activity that constitutes money transmission.

Entities engaged in money transmission are required to register as money services businesses with the U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) and are subject to reporting requirements under the Bank Secrecy Act, including filing suspicious activity reports (SARs). See 31 C.F.R. § 1022.320(a)(1). Therefore, fund managers should consider that some outside advisers, if engaged by the fund manager for mitigation services, may independently report the details of a fund's data breach to the U.S. government.

Notify Cyber-Insurance Carrier

Ideally, fund managers will have evaluated and secured appropriate cyber-insurance coverage before an incident. A fund manager should immediately notify its cyber-insurance carrier of a cyberattack. A delay in notice can potentially jeopardize the ability to recover under the insurance policy. Fund managers do not need to wait until they have complete details of the incident to contact the carrier.

Fund managers should open a dialogue with the carrier early to ensure the parties reach a consensus on the procedures that should be taken to address the cyberattack and minimize the risk of any gaps in coverage. Under many policies, certain expenses incurred in responding to a breach will not be covered unless they have been approved in advance by the carrier.

Communications between fund managers and carriers about breaches are generally ongoing, with fund managers providing updates to the carrier as more information becomes available. Often the insurance broker can help facilitate these communications.

> **Practice Tip:** Because cyber insurers see so many breaches, they can often serve as a helpful resource in identifying service providers to assist in remediation. Occasionally, carriers may require use of specific vendors or a selection of vendors from a pre-approved panel. Therefore, the insurer's preferences or requirements are one of the factors fund managers will want to consider in assembling their breach response team.

Fund managers should consider that cyber insurers that facilitate ransomware payments may be required to file SARs for certain ransomware events, which may involve disclosing to the U.S. government the details of the fund's data breach.

Engage With Law Enforcement

Engaging with the FBI and other law enforcement or regulators is often an important component of cyberattack response. Historically there has been a degree of reluctance to engage with law enforcement authorities where there isn't a legal requirement to do so.

Both the FBI and the Cybersecurity and Infrastructure Security Agency (CISA)—an agency whose mandate is to understand and manage cyber and physical risk to U.S. infrastructure—have increasingly called upon victims to promptly report cyber incidents, in particular ransomware attacks, regardless of whether a ransom has been paid. The FBI's recent actions and statements have aimed to clarify its role as an agency whose priority is to hold cybercriminals accountable and treat the targets of cyberattacks as victims. In its efforts to encourage reporting, the FBI has stated it ordinarily does not share information with agencies charged with enforcing cybersecurity regulations.

For example, the FBI's involvement in the highly-publicized Colonial Pipeline ransomware attack highlights the benefits in some circumstances of engaging the FBI in responding to a breach. Colonial Pipeline contacted the FBI when it became aware of the incident, and the FBI assisted Colonial Pipeline in navigating its response to the attack.

Colonial Pipeline paid a hefty ransom of approximately 75 bitcoins (then valued at $4.4M) in exchange for the decryption tool to unlock its systems. The FBI was later able to recoup and return to Colonial Pipeline 63.7 bitcoins of the ransom. The FBI took the bitcoin address where Colonial Pipeline paid the ransom, used software to trace it, and identified the specific digital wallet address belonging to the cybercriminal.

At a press conference announcing these developments, FBI Deputy Director Paul M. Abbate emphasized how critical it is for victims to report intrusions to the FBI as soon as possible. While the FBI's successful efforts to recoup a portion of the ransom in the Colonial Pipeline incident likely does not represent a new norm for future attacks—particularly less high-profile attacks—it shows that the FBI is not only interested in being notified of cyberattacks, but may be able to leverage the information it maintains on cybercrime perpetrators to provide decisive aid to victims.

Other U.S. government agencies that advise the public on the risks of ransomware and associated payments, such as FinCEN and the U.S. Department of the Treasury's Office of Foreign Assets Control, have issued statements encouraging companies to notify law enforcement immediately following the identification of a cyber-incident. For example, in a September 2021 advisory, OFAC reiterated that it "strongly encourages all victims and those involved with addressing ransomware attacks to report the incident to CISA, their local FBI field office, the FBI Internet Crime Complaint Center, or their local U.S. Secret Service office as soon as possible." Fund managers should be aware that facilitating a ransomware payment as a result of a cyber-incident could violate OFAC's regulations.

Develop an External Communication Strategy

For attacks where the cybercriminal obtains access to personal information, fund managers may have a legal obligation to notify the individual persons affected and, in some cases, certain authorities or credit bureaus. Fund managers will want to coordinate with their legal counsel and other advisers to determine whether any notice requirements or fiduciary obligations apply.

If so, the fund managers and legal counsel would need to coordinate to develop a timeline for sending notices that conform with the applicable legal requirements. In addition to providing any notices required by law, managers will want to work with their advisers to develop an overall PR strategy to assure investors that the incident is being handled responsibly, particularly if media coverage of the breach is inevitable.

> **Practice Tip:** All 50 states, Puerto Rico, and the District of Columbia maintain some form of data breach notification law. With respect to federal law, fund manager may have an obligation to provide notice in cases involving the unauthorized disclosure of healthcare information. Additionally, certain cyber events may require fund managers, as fiduciaries, to give notice to investors, particularly given that the SEC examination staff are increasingly focused on issues related to cybersecurity. Fund managers who trade in commodity interests should note that the National Futures Association imposes its own cybersecurity incident notification requirement.

Develop Action Items Based on a Post-Incident Review

Fund managers should coordinate with their outside legal and IT advisers to conduct a post-incident review, from which recommendations can be developed to mitigate the risks of a future breach. Action items for this type of review include:

- Implementing recommendations made by advisers for IT infrastructure updates and as otherwise commercially feasible
- Evaluating the effectiveness of the firm's IRP and other policies and procedures in responding to the breach and making updates to address identified gaps or weaknesses
- Testing the firm's IRP on a periodic basis to identify any additional gaps or weaknesses and take into account changes in technology; tabletop exercises are among the tools fund managers have found to be effective for pressure testing their IRP
- Conducting preemptive searches of systems and establishing alert systems to identify any unusual network traffic or other suspicious activities that could signal the presence of a threat actor or compromised system
- Training employees, as well as relevant independent contractors, on lessons learned from the specific incident and updating training curriculum and personnel manuals