Hot topic question

How can fund managers assess cyber security threats?

Mary Galligan
Director
Deloitte

Cary Stier
Global Investment Management Leader
Deloitte

The increased number of reported cyber attacks on businesses and the evolving nature of the breaches have led many fund managers to reevaluate their cyber security strategies, particularly with regard to preventive protocols and timely responses.

Mary Galligan, a director with the cyber risk services practice of Deloitte & Touche LLP, who previously served as special agent in charge of cyber and special operations in the Federal Bureau of Investigation's New York office, discusses what fund managers should be thinking about to strengthen their preventive cyber security measures. Mary is joined by other industry specialists who provide insights on how fund managers can help mitigate reputational risk and develop response protocols in the event of a cyber attack.

Mary Galligan

Investment managers should assess cyber security threats by asking simple questions, such as who would want our information and why do they want it. When making such evaluations, it is important for organisations to start with a clear understanding of their vulnerabilities to make risk management and mitigation more informed. Investment management firms may want to identify critical assets, 'treasures', as part of their cyber risk management plan, then prioritise threats to those assets and consider the assets and threats with business leaders.

The ability for investment managers to identify cyber security risks facing their organisation hinges on its ability to answer the following five questions:

1. Which cyber threats and vulnerabilities pose the greatest risk to our business and reputation?
2. What are the key assets that we need to protect?
3. Do we have the right talent—quantity and quality?
4. Do we have good cyber threat management practices, including protective, detective and response capabilities? Is it fully integrated with our business strategy and processes?
5. Do we have the right gauges to measure the success of our cyber threat management programme?

Investment managers should understand that the hacker community is smart, big, nimble and usually a step ahead of risk prevention measures. That makes monitoring the flow of information in and out of an organisation and blocking threats challenging, especially for investment management firms with offices around the world.

Cary Stier

With the level of cyber threats rising along with the proliferation of new technologies, more investment managers are looking to elevate their approach to cyber risk. Today, leading investment managers are using advanced forensic and analytic techniques to mine intelligence from both internal and external sources. The goal is to develop a deeper understanding of the origin of the attacks and track specific adversaries to enhance future risk analysis.

Although cyber threats are pervasive and often complex, the building blocks of a proactive approach to addressing them are similar to those for any well-planned business initiative. Investment managers need to understand what is at stake and the maturity level of their current efforts, and then make improvements by applying their existing capabilities whenever possible.

As investment managers expand their network of third-party providers, cyber risk should also be a key component of supplier risk reviews. For example, some investment managers are evaluating whether each vendor has adequate security controls in place and maintains an internal incident response team for cyber breaches.

Cyber risk management should run throughout an organisation to include the active involvement of the CEO and board, similar to the way senior management and employees think about an organisation's code of ethics.

Cyber risk management should run throughout an organisation to include the active involvement of the CEO and board, similar to the way senior management and employees think about an organisation's code of ethics

Investment management viewpoints

Perspectives from leading Chief Technology Officers

Leading chief technology officers at Deloitte's Alternative Investment Symposium emphasised that cyber risks do not need to be malicious to be considered serious threats, especially given the potential for systems to be infected by malware when employees bring personal technology into the workplace or engage in seemingly innocuous behavior such as clicking 'silly' links. Such inadvertent acts can be curtailed if investment managers develop education programmes for employees about cyber security risks and circumstances. With that said, several types of cyber threats were seen as especially worrisome according to the Chief Technology Officers, including:

1. Loss of control over Internet Protocol (IP) addresses, which are the binary sets of numbers that identify devices, such as servers, on a network
2. Loss of critical data or data leakage—whether related to an unintentional or deliberate act
3. Social engineering, in which users are manipulated into disclosing confidential information
4. Spear phishing, an email fraud scheme similar to phishing, but usually targeting specific organisations and coming from what seems to be a trusted source
5. A man-in-the-middle attack, in which a system is compromised and encrypted information is rerouted to a hacker's server and stolen before being sent back to legitimate users

Technology leaders also recognised that senior leadership cannot expect the technology team to stop every threat and attack. However, the technology team should be free to brief senior leadership about the risk and be comfortable doing so.

In addition, senior leadership should provide support to the technology team with respect to implementing the organisation's resiliency plan. Such a plan outlines the timeline and steps required for an organisation to recover from an attack and begin normal business operations. It also describes how the organisation should interact with law enforcement agencies.

To the **point**:

- The increased number of reported cyber attacks on businesses and the evolving nature of the breaches have led many investment managers to reevaluate their cyber security strategies, particularly with regard to preventive protocols and timely responses
- Cyber risk management is not just checking a box or passing a test. It requires understanding where the organisation's prized assets are and how criminals can come at them
- Investment management firms are looking to elevate their approach to cyber risk well beyond the walls of the IT department, a challenge that now requires active participation of senior leadership
- It can be important for investment management firms to create an education programme for clients and employees focused on cyber risk and prevention tactics that includes users to immediately report activity that they suspect may be related to a threat or an attack