PUBLICATIONS

Tips for Fund Managers Responding to Cyberattacks

December 2021

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.

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.

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.

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.

Related People

Kelly Koscuiszka

Partner

New York

Practices

INVESTMENT MANAGEMENT

REGULATORY AND COMPLIANCE

CYBERSECURITY AND DATA PRIVACY

Attachments

Download Article