ALERTS

Cybersecurity — Homeland Security Warns of Coronavirus-Related Cybersecurity Risks — Considerations for Private Fund Managers

March 16, 2020

On March 5, 2020, SRZ hosted a webinar on coronavirus preparedness during which we addressed certain cybersecurity and data risks that arise from working in a distributed workforce environment, as well as risks from cyber criminals exploiting the curiosity and fear surrounding the coronavirus outbreak.[1] On March 13, 2020, the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency ("CISA") issued a warning about these issues and encouraged organizations that move to a remote working environment "to adopt a heightened state of cybersecurity."

CISA Guidance. The March 13, 2020 CISA Alert lists a number of cybersecurity risks associated with telework, such as increased reliance on virtual private networks ("VPNs") that may not be updated with the latest security updates and patches or that do not utilize multi-factor authentication ("MFA") for remote access. CISA's Alert also recommends specific steps businesses can take to mitigate these increased risks:

- Update VPNs, network infrastructure devices and devices being used to remote into work environments with the latest software patches and security configurations;
- Alert employees to an expected increase in phishing attempts;
- Ensure IT security personnel are prepared to ramp up remote access cybersecurity tasks, including log review, attack detection and incident

response and recovery and document these tasks in the configuration management policy;

- Implement MFA on all VPN connections to increase security (or if MFA is not implemented, require teleworkers to use stronger passwords);
- Ensure IT security personnel test VPN limitations to prepare for mass usage and, if possible, implement modifications — such as rate limiting — to prioritize users that will require higher bandwidths; and
- Contact CISA to report incidents, phishing, malware and other cybersecurity concerns.

CISA and other government agencies have been warning for several weeks about the risks posed by cyber criminals and other scammers exploiting the pandemic.[2] While cybersecurity risks may be exacerbated in a telework environment, remember that they will continue to be heightened in traditional work settings and are not limited to the United States.

Implications for Private Fund Managers. The CISA Alert is not directed at any particular industry or sector, but it has obvious implications for private fund managers. At this point, most managers have tested their disaster recovery/business continuity plans and many have already shifted to a partial or complete "work-from-home" footing. However, the CISA Alert serves as a reminder that, in some ways, the cybersecurity risks, and need for vigilance, are just starting.

In particular, managers need to be reminding employees of the dangers posed by phishing emails, which are becoming more sophisticated and difficult to spot. Phishing attempts already reported during this crises include:

- Communications that look like they were sent by the World Health Organization[3] or another health or governmental organization;
- Fake purchase orders for face masks or other supplies;
- False "remote workplace testing" emails that request login or other authentication information; and
- Requests for donations that spoof legitimate relief organizations.

To succeed, a phishing attack only needs to convince one employee to click a link, open an attachment, or provide authentication information, which could compromise a manager's security or unleash malware that could render some or all of a company's systems inaccessible for an extended period of time. These threats pose significant harm and business interruptions under the best of circumstances but can be even more debilitating and difficult to address for offices that have moved partially or fully to remote work and reduced on-site IT monitoring and support.

Because employees are a major point of vulnerability, email alerts, trainings (which can be conducted via webinar or teleconference) and phishing tests (i.e., sending phishing simulation emails) can go a long way in mitigating the risks. Many managers have existing information security training programs and materials that can be leveraged for this purpose.

Additionally, while many managers already have a team and response plan in place for cyber incidents, adjustments should be considered to ensure the business is well-positioned to address cyber incidents in the current environment.

As before, should a cybersecurity incident occur, managers are reminded to consider any required notices to personnel or other affected individuals, as well as governmental authorities. For example, if investor information is accessed or extracted from the system, it could trigger reporting obligations under data breach notifications laws.

Authored by Brian T. Daly, Marc E. Elovitz, Edward H. Sadtler and Kelly Koscuiszka.

If you have any questions concerning this *Alert*, please contact your attorney at Schulte Roth & Zabel or one of the authors.

---

[1] Please contact events@srz.com if you would like the materials from that webinar.

[2] For example, CISA issued a March 6, 2020 Alert regarding cyber scams related to the coronavirus; the Federal Trade Commission issued a Feb. 10, 2020 Alert related to fake websites, emails and fundraising efforts related to the coronavirus, and the Securities and Exchange Commission's Office of Investor Education and Advocacy issued a Feb. 4, 2020 investor Alert warning investors about investment frauds involving

claims that a company's products or services will be used to help stop the coronavirus outbreak.

[3] The World Health Organization maintains a cybersecurity page with tips to assist organizations in validating communications and a link for reporting scams.

Related People

Marc Elovitz

Partner
New York

Kelly Koscuiszka

Partner
New York

Practices

INVESTMENT MANAGEMENT

Attachments

Download Alert