Schulte Roth&Zabel

Alert

Broker-Dealers: B-D Guidance on Increased Cybersecurity Risks Due to the COVID-19 Pandemic

March 20, 2020

As most broker-dealers move to a telework model and navigate the "new normal," it is critical that they take steps to mitigate the increased cybersecurity risks arising from the COVID-19 pandemic.

Guidance on Increased Cybersecurity Threats

On March 9, 2020, FINRA issued Regulatory Notice 20-08, advising members to review their business continuity plans and prepare themselves for heightened cybersecurity risks as they face significant business disruptions in the wake of the COVID-19 pandemic. FINRA reminds members that the pandemic has increased cybersecurity risks due to a combination of increased remote work and heightened anxiety and confusion about the virus among employees. The Regulatory Notice contains a number of steps that FINRA also recommends member firms take to mitigate those increased risks and vulnerabilities.

On March 13, 2020, the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency ("CISA") issued a similar alert that, although not specific to broker-dealers, provides additional information for organizations moving to a remote working environment and the steps they should take to adopt a heightened state of cybersecurity. In particular, CISA warns firms to anticipate sophisticated phishing attacks and to help employees to be on alert for these attacks.

Suggested cyber mitigation efforts include:

- Ensuring that virtual private networks ("VPNs") and other remote access systems are properly patched with the latest available security updates and configurations;
- Checking that system entitlements are current;
- Employing the use of multifactor authentication ("MFA") for associated persons who access systems remotely and implementing MFA on all VPN connections to increase security;
- Reminding associated persons of cyber risks through education and other exercises that promote heightened vigilance;
- Ensuring 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; and
- Ensuring 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.

Cyber SARs

As a reminder, broker-dealers and other financial institutions are required to file Suspicious Activity Reports ("SARs") with the U.S. Department of the Treasury's Financial Crimes Enforcement Network for certain cyber-events and cyber-enabled crime.[1] Filing a SAR does not relieve financial institutions of any other applicable notification requirements, and compliance with the Cybersecurity Information Sharing Act does not relieve financial institutions of any SAR reporting requirements for cyber-events or cyber-enabled crime.

The Biggest Cybersecurity Weakness May Be Your Employees

Both FINRA and CISA guidance emphasize the need for employees to practice heightened vigilance with respect to cybersecurity risks that will exploit human beings as a weak link. 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]

In particular, broker-dealers must regularly remind employees of the dangers posed by phishing emails. Phishing emails are becoming more sophisticated and difficult to spot, and are being designed to exploit uncertainty and anxiety about the pandemic. Reported phishing attempts already reported during this crisis 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 the firm's security or unleash malware that could render some or all firm systems inaccessible for an extended period of time. Under the best of circumstances, a successful phishing attack can cause significant harm and business interruptions. Where firms have moved partially or fully to remote work, or where on-site IT monitoring and support has been reduced, they can be even more debilitating and difficult to address.

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

[1] *See* FIN-2016-A005, issued Oct. 25, 2016, available at https://www.fincen.gov/sites/default/files/advisory/2016-10-25/Cyber%20Threats%20Advisory%20-%20FINAL%20508_2.pdf.

[2] For example, CISA issued a March 6 alert regarding cyber scams related to the coronavirus; the Federal Trade Commission issued a Feb. 10 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 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.

long way in mitigating the risks. Existing information security training programs and materials can and should be leveraged for this purpose, and tailored to the extent possible to current COVID-19 situation.

Have a Plan for Responding to a Cybersecurity Incident

Finally, firms should prepare for the potential eventuality of a cybersecurity incident. Firms should evaluate any team and response plan currently in place to ensure that it is capable of responding in the current environment. Should a cybersecurity incident occur, firms must consider whether any notices are required to personnel, other affected individuals (e.g., customers or clients) or, governmental authorities. For example, if client information is accessed or extracted from a firm's systems, it could trigger reporting obligations under various data breach notifications laws.

Authored by Craig S. Warkol, Edward H. Sadtler, Derek N. Lacarrubba, Kelly Koscuiszka, David S. Sieradzki, Katherine M. Sullivan and Amanda C. Wichot.

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

Schulte Roth & Zabel
New York | Washington DC | London
www.srz.com