Cybersecurity Attacks Could Derail At-Home Advisors, Experts Warn

April 7, 2020

Cyberthieves are pouncing on advisors working remotely during the coronavirus crisis, taking advantage of at-home systems and necessarily weaker compliance oversight, according to lawyers and compliance consultants.

Brokers, advisors and their firms are particularly vulnerable to phishing attacks, in which thieves posing as clients gain access to usernames, passwords and account details via seemingly innocuous emails and attachments, said Wes Stillman, chief executive of RightSize Solutions.
“Over the past two weeks, we have seen a huge rise in the number of their clients’ email accounts being hacked,” Stillman said, citing incident reports pouring into his outsourced information technology firm.

The biggest concern is that once the hackers get access to client accounts, they will initiate wire transfers that could slip by normal vetting procedures when firms are fully staffed and working from centralized locations. Most larger firms require follow-up phone calls by advisors or client associates when transfers are requested, but experts fear the procedures are not being rigorously followed.

“It makes sense to start thinking about a firm’s procedures on authorizing the distribution of checks and of wire requests” said Max Schatzow, a securities lawyer at Stark & Stark in Lawrenceville, New Jersey.

Most of Schatzow's advisor clients are using virtual private networks accessed through firm-issued authentication devices, he said, but firms need to increase approval processes and supervision through souped-up reviews of advisor-to-client emails and video conferencing.

The compliance issue is exacerbated because many advisors and brokers are using personal cellphones, tablets and home computers that firms cannot monitor, not to mention falling back on unsecure texting and Twitter communications to check up on clients. Firms should consider requiring advisors to register their devices under the corporate domain while layering in more conditional access policies, Stillman said.

They also must remind brokers to be vigilant about memorializing conversations and action advice with clients through client relationship management software that may not be readily available if they don't have direct and reliable access to their workstations.

"Any communication needs to be retained and reviewed by advisors and broker dealers," said Jeff Groves, chief executive of ComplianceWorks. "Those communications need to be presented to regulators upon demand in an audit situation."

Companies must also reevaluate and strengthen their wire-approval processes, the consultants said.

"I certainly would recommend that if it's a one-person approval process, involve a second person in that process now," Schatzow said. "Everyone's remote and the risks are so high."

The Securities and Exchange Commission and the Financial Industry Regulatory Authority are not making allowances for advisors and brokers working from home, according to Amy Lynch, founder and president of Rockville, MD-based consulting firm FrontLine Compliance.

"Examinations that started before the shutdown occurred…are still ongoing and they're even starting to ask follow-up questions about firm cybersecurity and business continuity plans," she said. "They are taking a look at what firms are doing right now."

Many firms are holding compliance review sessions for advisors and their staff who are working remotely. They should cover a range of issues, from the basics of how to access workstations remotely to reminders about being super-cautious about fielding e-mails, according to Lynch.

"Use a WebEx or GoToMeeting or some form of an online platform to conduct training for your employees to remind them of what the firm policies and procedures are," she said.