Bloomberg Law

Securities Law News

INSIGHT: Protecting Broker Dealers From Cyber Threats

By Frances Floriano Goins and Michael Davis Hoenig Posted Feb. 19, 2019, 4:01 AM

FINRA recently issued a report providing broker dealers with best practices for effective cybersecurity, including a list of telltale signs of a phishing attack. Two Ulmer & Berne LLP attorneys examine the report, and warn that with the risk of cyberattacks growing, it is imperative to implement controls tailored to each firm's situation.

The risks of cybersecurity attacks are particularly acute for securities firms and broker dealers because they control not only their own business data, but also clients' financial information.

To educate firms on cyber-best practices, the Financial Industry Regulatory Authority (FINRA) recently published its *Report on Selected Cybersecurity Practices - 2018,* discussing effective procedures broker dealers have implemented for the five areas firms struggle with most:

- branch office control,
- phishing attacks,
- insider threats,
- penetration testing, and
- employees' use of mobile devices.

Importantly, the report "does not create any new legal requirements or change any existing regulatory obligations."

Recommended Branch Office Controls

Branch office control is particularly challenging for many broker dealers, and with many firms employing agents who work offsite, cybersecurity becomes even more difficult. FINRA suggests security controls including:

- comprehensive, easily referenced Written Supervisory Procedures (WSP) to formalize minimum oversight practices;
- inventorying branch data, software, and hardware assets;
- designating individual branch managers or other supervisors to be responsible for cybersecurity;
- maintaining technical controls; and
- implementing branch cybersecurity examination programs.

Recommended hardware and software options and settings, and use of approved vendors can also tighten branch security.

Phishing Scams

The FINRA report also addresses methods of limiting phishing and insider attacks that may expose firm and customer information to hackers.

To understand phishing, consider the classic *Saturday Night Live* sketch where a character dressed as a shark tries to enter a house. The shark knocks on the door pretending to be someone else—a candygram, plumber, mailman, etc. The person inside isn't fooled at first—"it's not my birthday. I didn't call a plumber. Mail isn't delivered on Sunday." But the shark persists and eventually convinces the person inside to open the door—"I'm not a shark, I promise, I'm just a dolphin. … A Dolphin? OK, come on in. … Chomp!"

Today's sharks try to enter otherwise secure networks through phishing email scams. In a phishing attack a cybercriminal sends an email pretending to be someone familiar—a friend, family member, or coworker—and asks the recipient to relay personal information, click on a malicious link, or open an infected attachment. If the email recipient takes the bait, the cybercriminal may be able to access the entire system and take firm and personal information such as social security and drivers' license numbers and financial information.

Phishing is one of the top cybersecurity problems for financial firms. One reason for this is because the "growing sophistication and quality of phishing (especially spear [targeted] phishing and whaling [emails purporting to come from a company executive]) attacks makes it challenging for recipients to distinguish them from legitimate communications."

In a common scam, a cybercriminal sends an urgent email appearing to come from management asking an employee to provide information or wire funds immediately, usually at an odd hour like late Friday or just before a holiday. The intent is to get the employee to react quickly to a demand by a superior. This can be effective and devastating. Just imagine a broker quickly responding to a seemingly urgent request from a manager asking him to provide information on his top clients only to discover later the request was a scam.

Don't Become Shark Bait

So how do firms protect themselves and their customers from becoming shark bait? The first step is recognizing a phishing email.

FINRA has provided a useful list of telltale signs of a phishing attack:

Once employees know what to look for, they will be less likely to fall for these schemes.

Insider Threats

With additional offices come additional employees, some of whom may themselves become threats. Inside threats from bad actors—rogue employees purposefully disclosing sensitive information—or inadvertent disclosures by well-meaning employees can wreak havoc on security because insiders already have access to company networks.

FINRA reports that one way firms mitigate insider risk is by implementing strong data loss prevention procedures that will "typically identify sensitive customer and firm data based on rules and then block or quarantine the transmission of the data whether by email, data upload or download, file transfer or other method." Such programs can prevent, or at least minimize, the inadvertent or malicious transmission of confidential data.

System Tests

Frequent penetration testing is another cybersecurity best practice. In these tests, cybersecurity vendors attempt to break into the firm's network. Their results can help management determine how to allocate resources to improve the firm's cybersecurity.

Employees' Use of Mobile Devices

FINRA also shares ways firms can mitigate risks arising from the use of personal computers, smart phones, and tablets, ranging from completely prohibiting employees from conducting business on personal devices to ensuring that personal devices are equipped with protections like updated antivirus software and an encrypted mobile device management application.

Recognizing that "[t]here is no one-size-fits-all approach to cybersecurity," FINRA "has made a priority of providing firms with reports and other tools to help them determine the right set of practices for their individual business." It is up to each firm, however, to implement controls that are effective for its particular situation.

Author Information

Frances Floriano Goins is a parter at Ulmer & Berne LLP in Cleveland and co-chair of the firm's Financial Services & Securities Litigation practice and Cybersecurity & Privacy practice. She is skilled in resolving complex business disputes for public and private companies, including matters involving securities, corporate governance, cybersecurity, consumer, and contract law.

Michael Davis Hoenig is an associate at Ulmer & Berne in Cleveland who represents broker-dealers in FINRA arbitrations and regulatory proceedings.

© 2019 The Bureau of National Affairs, Inc. All Rights Reserved