"Only the Paranoid Survive"

FACING CYBER THREATS, FIRMS NEED "A CULTURE OF SECURITY"

By Ed McCarthy

Financial advisers understand the importance of cybersecurity. According to a 2016 survey report by the Financial Planning Association Research and Practice Institute ("Is Your Data Safe?"), 81% of respondents indicated cybersecurity was a high or very high priority. However, only 26% of respondents completely agreed that they are aware of all the cybersecurity requirements issued by the Securities and Exchange Commission's Office of Compliance Inspections and Examinations (OCIE), and only 18% of respondents were very confident they would pass an OCIE examination at the time of the survey.

KEY POINTS

Cybersecurity has become a top concern for the SEC and FINRA, and noncompliance fines are on the rise.

Data theft, insufficient credential management, ransomware, and phishing are among the most common security gaps facing financial firms.

Smaller advisory firms usually rely more heavily on third parties for software and to provide their IT infrastructure.

In fairness to the respondents, cybersecurity threats and compliance measures are complex and evolving. Not too long ago, the primary information technology (IT) threat facing most firms was willful or unintentional employee misbehavior; a departing employee downloaded the client list, for example, or someone lost a company laptop. Firewalls and antivirus software were adequate protection for online threats because data thieves were more likely to break in and steal computer hardware from your office than to penetrate your network.

Those activities are still threats, but the range of exposures has expanded. A 2014 Financial Institutions Regulatory Authority (FINRA) bulletin listed numerous IT vulnerabilities that advisory firms face, including mobile devices, employee theft, malware and phishing emails, third-party vendors, software and hardware, and hackers posing as clients. Nation-states, hacktivists (computer hackers seeking to advance a social or political cause), criminals, and insiders exploit these vulnerabilities and constantly seek new ones, so advisory firms must devote more time and money than ever to cybersecurity.

Firms and regulators often have to play catch-up with the bad guys, but FINRA and the SEC have stepped up their cybersecurity compliance efforts. The OCIE's National Exam Program Examination Priorities have highlighted cybersecurity since 2014, as did a 2015 SEC Compliance Outreach Program. An April 2014 OCIE Risk Alert discussed a planned sweep of registered investment advisers' cybersecurity programs for 2014, with another round in late 2015. The agencies' industry education efforts and compliance emphasis have continued since then. "I would say cybersecurity has become one of the SEC's and FINRA's top concerns, as security incidents, breaches, and just security practices continue to place customer records at risk," says Kimberly Peretti, co-chair of law firm Alston & Bird's cybersecurity preparedness and response team in Washington, DC.

The cost of noncompliance is increasing, too. In May 2014, when one firm's IT employee left an unencrypted laptop in a restroom, placing over 352,000 customers' personal and confidential information at risk, FINRA imposed multiple sanctions, including a $225,000 fine. In September 2015, the SEC sanctioned an investment adviser for $75,000 under the "safeguards rule" because clients' personal data were stored on a third-party server that was compromised, despite a lack of evidence the data were accessed inappropriately.

RISK ASSESSMENT

In its 15 September 2015 Risk Alert, the OCIE served notice it will focus on six areas to assess procedures and controls: governance and risk assessment; access rights and controls; data loss prevention; vendor management; training; and incident response.

It's a comprehensive list, but one way for firms to address the multiple themes simultaneously is to start with a cybersecurity risk assessment. FINRA's February 2015 "Report on Cybersecurity Practices" defines an assessment as "a systematic process firms complete to identify and analyze potential dangers or risks to a firm's business that could arise through its information technology systems." The assessment should include "external and internal threats and asset vulnerabilities" and "prioritized and time-bound recommendations to remediate identified risks."

The agency cites six sets of risk assessment activities or outcomes developed in the National Institute of Standards and Technology (NIST) Framework that are applicable to financial firms: identify and document asset vulnerabilities; review threat and vulnerability information from information-sharing forums and sources; identify and document internal and external threats; identify potential business impacts and likelihoods; use threats, vulnerabilities, likelihoods, and impacts to determine risk; and identify and prioritize risk responses.

The NIST Framework allows assessments to be customized, which is essential because each advisory firm has unique cyber risks, Peretti observes. "Cyber risk can be built based on the number of systems you have, the number of inner connections, the number of vendors, your global footprint,

how big you are, how small you are, how you manage your systems," she says.

For example, smaller advisory firms usually rely more heavily on third parties for software and to provide their IT infrastructure, says Kennet Westby, president of cyber risk management and consulting firm Coalfire Systems in Seattle, Washington. In those instances, an assessment involves greater review of external providers' policies and controls, because a larger organization is more likely to develop and control its IT assets internally.

Assessments start with a "scoping call," says Ryan Castle, vice president of technology with security consultant TraceSecurity in Baton Rouge, Louisiana. The goal is to identify potentially vulnerable assets, which are defined as systems that can interact with sensitive business data. The initial discussion will review the firm's use of a client access portal, its record-keeping systems, and cybersecurity protocols, among other topics. Another purpose of the call is to determine the adviser's expectations for the assessment.

After the scoping call, TraceSecurity's analysts complete a risk template based on the NIST Framework. The template focuses on three primary criteria: identifying the assets (i.e., a firm's systems that have access to sensitive information); determining the threats against those assets—how the data can be lost or compromised; and evaluating the controls in place to mitigate the threats.

"The concept behind the risk assessment is to understand at the end of it where you have very critical assets that have very severe threats against them and you are not adequately controlling those threats," says Castle. In turn, the assessment should influence how a firm allocates its cybersecurity resources, according to Castle: "If you have a limited budget, limited personnel, we want to use them in the most effective manner possible."

AUDITS AND PENETRATION TESTS

Risk assessments are often conducted remotely and use information provided by the advisory firm. In a cybersecurity audit, the IT security consultants verify policies and procedures reported during the risk assessment to seek proof that the firm is doing what it claims in the areas covered by the engagement. It's not necessary to conduct the assessment and audit sequentially, says Castle, but it is a logical work flow.

Penetration testing is a controlled hacking procedure to check the firm's protective measures. Castle describes it as analogous to a burglar walking around a home's exterior to test locks and look for open windows and keys under doormats. The goal is to find an exploitable security weakness. "We do this in prioritized fashion, to say, 'Here are some things that are pretty glaring problems for you,' or, 'This is particularly critical' and [to provide] some ways to go about fixing those things," says Castle.

COMMON SECURITY GAPS

Westby cites several weaknesses among advisers. The risk of data theft, either when they reside in a system or are in transit between systems, is one risk. Insufficient attention to credential management is another area (multifactor authentication is a good practice to adopt in response, he notes). Ransomware—malicious software designed to block access to a computer system until a sum of money is paid—is another exposure, and one that's becoming more prevalent and sophisticated. A recent report from Symantec, "Ransomware and Businesses 2016," notes that ransomware groups are exhibiting a level of expertise in their attacks that "is similar to that seen in many cyberespionage attacks. Attackers have managed to gain a foothold on networks by exploiting vulnerabilities in public-facing web servers and then traversing the network using legitimate tools before identifying and infecting hundreds of computers."

Phishing remains a widely exploited weakness. "We've seen more and more hackers find ways to acquire credentials and then use legitimate credentials to access systems, because then it doesn't require them to hack it all," says Peretti. "And the number one way that they do that is through phishing to get individuals to click on a link and provide their credentials. In some cases, it's just clicking on the link that compromises the system and allows hackers in the front door."

STAFF AND CLIENTS ON THE FRONT LINE

The phishing exposure can result from staff members' errors, says Castle, and the likelihood of making such an error increases with inadequate security training. Advisory firms' training efforts are mixed, he says, with some firms addressing the need while others don't know how to go about it.

David Damiani, CFA, chief financial officer with wealth management firm Balentine in Atlanta, Georgia, says that his business has undergone a cybersecurity audit and penetration testing. The firm also extensively trains its 30 employees on security. "We spend a lot of time getting our folks aware of what can happen, and I think a lot of this starts with creating a culture of security, a culture of risk management," he says. "Understanding that every piece of data that we touch is critical and it needs to be protected, and so we do a lot of internal training creating a culture of 'only the paranoid survive.'"

Security isn't just a technology issue; it's a human issue as well, Damiani emphasizes. "It's about user training and education. Making sure that the culture of your firm really buys into this and fully understands and appreciates that it's not just a technology issue. I would say that's the key piece, which I think a lot of folks may not fully appreciate: It's not just about technology."

Clients are another potential weak link in the security chain. Published incidents have reported how criminals gained access to clients' personal email accounts, monitored messages, and then used those accounts to request funds from the victims' financial advisers. When advisers implement stricter security controls, however—such as requiring telephone confirmation of requests—some clients don't appreciate the added security. The extra steps can create a strain between clients and the staff with whom they work, making it necessary for a firm's management to support the security efforts, according to Jennifer Papadopolo, chief

operating officer with Morristown, New Jersey–based wealth managers RegentAtlantic Capital. "Once they understand it, they're willing to do it and are willing to work with the client on why we're doing this," she says.

COORDINATED RESPONSE PLAN

Other areas regulators want to see addressed are the development of detailed response plans for handling a data breach and tests of those plans. It's a form of crisis management that shows the organization can react and respond quickly to incidents, says Peretti: "Some of them end up being [a] false positive. Some end up being smaller incidents. But it's the big ones that you want to be able to catch early and plan for and know the company can respond to. What's as important as having the plan is making sure the plan is effective, and the only way you'll identify that is if you go through scenarios, walk through scenarios, have the right people at the table and talk through how you would respond to a particular incident."

KEEP GOING

"Cybersecurity: Don't Become the Hacker's Next Victim," *Enterprising Investor* (22 June 2016) [blogs.cfainstitute.org]

"Securing Client Data," *CFA Institute Magazine* (November/December 2013) [www.cfapubs.org]

EXPERT HELP

In theory, an advisory firm could conduct its own risk assessment, but working with an external vendor is likely to provide a broader perspective, greater expertise, and carry more weight with regulators. Kevin Witt, chief technology officer at Kestra Financial in Austin, Texas, suggests that an IT consultant under consideration should be conversant with FINRA and SEC regulatory expectations. The IT firm also should be able to provide a comprehensive review that includes the physical security of the facility, computer network devices, data-access administration, and how the firm exchanges information with clients. If the advisory firm deals with insurance, HIPAA-compliance expertise might also be required.

An assessment, perhaps combined with an audit and penetration test, is a good first step, but firms can't relax, says Damiani: "You have to adhere to the standards that you have just tested yourself for, because it's not going to be a silver bullet."

Ed McCarthy is a freelance financial writer in Pascoag, Rhode Island.