Reg-Room

Reg-Watch

Regulators Say Firms Need to Constantly Update Cyber Defenses

By Fanni Koszeg, for Reg-Room LLC March 8, 2018

Cybersecurity is now a top priority, from Fortune 500 companies and major financial firms, to politicians and financial regulators. However, the wide range of threats, new technology, and the steep learning curve faced by regulators, means that the response is not always effective.

These were among the conclusions of a FINRA cybersecurity conference held in New York on February 22. Attendees included about 400 information security and operations professionals at financial industry firms (including broker-dealers, banks and buy-side firms). Topics covered evolution of cyberattacks, internal and third-party risks, and best practices for preventing and responding to attacks.

Participants heard from representatives of the US Treasury Department and the Securities and Exchange Commission (SEC). Speakers concluded that threats are evolving and will not go away, so firms need to focus on training and prevention as much as incident response planning. They stressed the need for cyber mitigation to be treated as a top-level business risk, rather than merely an operational function.

Senior executives and company boards must focus on this risk and ensure adequate resources for professionals designated to deal with them. Many attendees would prefer if evolving cyber requirements and supervisory expectations were more coordinated and harmonized. Fed Vice-Chair for Supervision, Randall Quarles, also agreed with the need for coordination in a recent speech on cyber risks, for details see: Reg-Track#40751.

Types of Cyber Risks

Cyber risks can be external or from inside a firm, ranging from phishing to account takeovers, ransomware, wire fraud, theft and disclosure of confidential information, and any combination of these. Panelists agreed that phishing and spear phishing attacks are still the most common types, especially given that technological cybersecurity protections have been improving.

Spear fishing is a targeted form of phishing in which fraudulent emails target many employees at an organization. At a large firm, it may be enough to trick one or two from amongst hundreds of employees into opening an attachment or clicking on a malicious embedded link to cause harm. 98% of the audience present said they had experienced phishing attacks. An increasingly prevalent category of phishing is CEO fraud, where an attacker spoofs top executives and tricks employees into wiring funds to fraudulent accounts or disclosing protected information. Panelists predicted CEO fraud will be on the rise in the coming year.

A newer and increasing source of risk is the more widespread adoption of cloud-based data storage. Among financial entities, FINRA was an early adapter of storing data in the cloud and of perfecting corresponding defenses embedded in it. For FINRA's take on cloud security, see: Reg-Track #40843.

In the not too distant future, as artificial intelligence keeps improving, AI will be used by criminals to crack passwords and engage in other forms of attacks. According to presenters, a unique problem for responding to AI-driven attacks is that existing detection software is tailored to respond to machine behavior and will not detect good AI that is successfully simulating human behavior. A portion of firms' internal resources will increasingly explore how firm-developed AI and machine learning tools can prevent these types of attacks.

Minimizing Internal Threats from Employees

In addition to ever smarter and more sophisticated outside attackers, every firm needs to focus on risks presented by its own employees and third-party providers. JP Morgan's representative reminded the audience that employees present risks in a number of ways in addition to cyber. Insider risk is synonymous with the people you employ, which is why firms must take a holistic approach, he said. Some risks can be prevented during the hiring process by running good background checks on potential employees especially if they will handle sensitive information.

Once employees are hired, the best approach is to collect and analyze a range of data on them to assess risk potential and promote early intervention. JP Morgan calls its program Workforce Risk Analytics and Prevention. Notably, its employee communications and training emphasize "safety" rather than "internal threats". The use of more hostile language is not conducive to learning and enthusiastic compliance by employees. Each employee is assigned a probabilistic risk score based upon large amounts of data and the type of job they perform.

The program focuses on intentional breaches rather than accidental ones, which are often successfully stopped by technology tools. The biggest risk of unauthorized disclosure or theft of confidential information is during the last 30 days of employment before a person departs.

Early warning indicators include out-of-the-ordinary online behaviors and excess downloading of files. Some warnings will trigger a review by cybersecurity experts followed by escalation to legal, HR and compliance departments. Those units typically jointly assess and determine if further investigation or disciplinary proceedings should proceed (up to and including termination). In response to a poll, 71 percent of the audience said they regularly conduct internal risk monitoring.

Third Party Risks Harder to Control

According to several participants, third-party risk is one of the biggest concerns for information security professionals. Third parties may be external application providers, contractors or providers of administrative services. Many of these are located in foreign jurisdictions with different levels of cyber and legal protections. A representative of Raymond James explained that his firm recently moved several of their application development suppliers from Russia to Poland and other Eastern European countries. After careful analysis, the firm decided that keeping their exposure to providers in countries notorious for cyber fraud would not be prudent, especially given uncertain intellectual property laws.

To establish a good third-party program is a long-term endeavor and could take several years to develop. A crucial first step is to analyze what the intellectual property (IP) laws and cyber rules are within a given country and establish priorities. Educating partners on the firm's priorities is key and if compliance is difficult to check, site visits are recommended. 90 percent of participants indicated that they use a formal program on third party oversight for cyber risks. 40 percent would describe the program as nascent, and 25 percent said theirs qualifies as established.

How to protect yourself and your customers?

Panelists emphasized the most important step a firm can take is to fully integrate its security operations within business decision-making. Understanding and appropriately ranking threats, so the firm can prepare accordingly, is also important. Even if there are no real attacks, "war gaming" and cybersecurity tabletop exercises to identify areas to improve resilience is good strategy. Once a cyber incident is confirmed, it is important to follow established processes and procedures "as you would in the military," said one of the panelists. Deviating from well-designed processes can worsen the situation and following those on all communication levels and steps will ensure a uniform response.

Panelists agreed that sharing information and trends with the Financial Services Information Sharing and Analysis Center (FS-ISAC) helps firms learn from each other and develop effective strategies. It is important to not only focus on protecting the firm's information but also focus on protecting consumers. A breach such as at Equifax, see: Reg-Track. 35387 could mean huge reputational and litigation risks for firms. A participant said consumer protection is one of his main concerns but did not think regulators were focused enough on that aspect of cyber security.

What can regulators do?

Both the legislative and executive branch as well as federal and state regulators have been increasingly focused on cybersecurity. Representatives of the Treasury Department and the SEC both stressed the importance of collaborating with the financial industry. The SEC recently updated its cyber guidance (for details see: Reg-track 40613) and its cyber unit will focus on assisting firms with compliance. The SEC OCIE conducts examinations based on business type and tailors those to a firms' risk profiles. It also plans to publish anonymized findings from those examinations, to inform regulated entities of typical deficiencies, areas for improvement.

For Treasury, the number one focus is engaging with and listening to the industry. The department also plans to be more proactive assisting firms with preventing incidents. Treasury's recently published strategic plan (see: Reg-Track 40339) contains cybersecurity as one of the top-level risks for the industry. Instead of "checkbox" compliance requirements, the administration wants to focus on harmonizing requirements among regulators and working with law enforcement, if necessary.

Treasury and the SEC both argued that it was a positive sign that cybersecurity is being taken seriously at all levels of government. These include the CFTC and State regulators like the NY Department of Financial Services (DFS), whose one of a kind cyber regulations recently came into effect, see: Reg-Track 34737.

However, both are keenly aware of a need for harmonization of rules focusing on terminology in particular. As some participants we spoke to pointed out, many of the regulators are asking the same questions using different phrases and requiring firms to duplicate efforts. If regulators are able to live up to their promises to coordinate efforts domestically and internationally, that would be a welcome development.

"These conferences are useful, because at least regulators are talking with us about cybersecurity," said a private wealth management firm's executive we spoke to.