FINRA's 2016 Regulatory and Examination Priorities Letter – Part 2

SR Hello and welcome. I'm Sarah Razaq.

SP And I'm Steve Polansky.

SR This is the second podcast in a three-part series about FINRA's 2016 Regulatory and Examination Priorities Letter. In this series, we talk about some highlights from the letter, but the letter has even more. So, be sure to read it for topics relevant to your business. Here, we focus on technology management and cybersecurity, and we bring back some key concepts from FINRA's cybersecurity report to elaborate on what the letter says.

SP Let's begin with a note about technology management. FINRA has seen shortcomings in this area at many firms. For instance, an error while changing a firm's systems or the applications they use can cause problems that range from adverse customer effects to market disrupting orders. As a result, FINRA's reviews focus on firms' changed management practices in different areas such as algorithms as well as back office and vendor system changes. FINRA is also seeing deficiencies in written procedures, insufficient segregation of duties for people involved in developing and deploying technology changes and the lack of user acceptance testing and quality assurance, and FINRA is seeing significant operational breakdowns at firms when they change from legacy to new compliance systems.

SR On a related note, FINRA is examining firms' data governance, quality controls and reporting practices to make sure they are accurate, complete, consistent and timely.

FINRA has seen operational problems at firms often come up from data quality and integrity issues. These can undermine a firm's ability to monitor key details needed to manage its risk and business activities.

SP Turning now to cybersecurity, FINRA remains focused on firms' preparedness for cyber threats. While many firms have improved their defenses and plans, many still have not, or the changes have not been enough. FINRA is reviewing firms' approaches to cybersecurity risk management. As part of these reviews, FINRA is examining firms' abilities to protect the confidentiality, integrity and availability of sensitive customer and firm information.

SR There are seven key cybersecurity areas FINRA is examining, depending on the firm's business and risk profile. They are:

- governance
- risk assessment
- technical controls
- incident response
- vendor management
- data loss prevention and
- staff training

All of these are important, but in this podcast we will draw on FINRA's report on cybersecurity practices to dive deeper into a few of them.

SP Let's start with governance. Firms should set up and implement a cybersecurity governance framework that supports informed decision-making and escalation in organization to identify and manage cybersecurity risks. The framework should include

defined risk-management policies, processes and structures, coupled with relevant controls tailored to that firm's risks and resources.

SR Active executive involvement in governance is also important whether it's a firm's senior management or executive board, if applicable. Without their involvement, firms are unlikely to achieve their cybersecurity goals. The National Association of Corporate Directors and the Internet Security Alliance released a publication called *Cyber Risk Oversight* that provided five cybersecurity principles for boards. The first one is they should approach cybersecurity as an enterprise-wide risk-management issue, not an IT issue. The second is they should understand legal implications of cyber risks for their company. And third, boards should have access to cybersecurity expertise and give regular and adequate time to these issues on the board meeting agenda. The fourth principle is that boards should set the expectation that management will set up an enterprise-wide cyber risk management framework with adequate staffing and budget. And the last one, board and management discussions of cyber risk should include identifying what risks to avoid, accept, mitigate or transfer through insurance as well as specific plans for each approach.

SP To reinforce why these principles are so important, let's look at an example of a real-life enforcement action that shows governance failures. In this case, hackers attacked a firm's database server to get confidential information about more than 200,000 customers. This included names, account numbers and even Social Security numbers. The data was stored on a computer with an internet connection, but lacked encryption, and the firm only became aware of the breach when the hackers tried to extort money from the firm, even though the breaches had been visible on the firm's server logs.

SR The firm failed to put safeguards in place to protect customer information. The firm did perform penetration testing, but it did not include an asset with sensitive customer information as part of that test. The firm also lacked procedures to review the server logs that would have revealed the theft. The firm did not respond to an earlier auditor recommendation that it get an intrusion detection system. And, the firm failed to have written procedures in place for its information security program designed to protect confidential customer information. This case shows some of the pitfalls to avoid when it comes to cybersecurity governance.

SP Now let's touch on the role of frameworks and standards. One effective practice is for firms to evaluate such frameworks and standards as reference points for their own approaches to cybersecurity. There are a number of standards available. One of the most prevalent comes from the National Institute of Standards and Technology called NIST. It provides a thorough yet flexible risk-based approach to think through a firm's approach to cybersecurity. It also helps a firm figure out what to change to achieve its cybersecurity risk management priorities and those priorities are defined by the firm's goals, legal and regulatory requirements, and industry best practices.

SR And there are other frameworks firms can consider like the International Organization for Standardization and International Electrotechnical Commission, commonly called the ISO Frameworks, and another called COBIT-5, and still another is the Payment Card Industry Data Security Standard.

SP Another useful resource is what's called the Sands 20. It lists the top 20 cybersecurity controls that are "effective against the latest advanced targeted threats with a strong

emphasis on what works." This means things that are in use and have demonstrated real-world effectiveness. For each control, the Top 20 explains why it's important, how to implement it, and what procedures and tools are necessary to make the control effective. And it gives implementation effectiveness and automation metrics.

SR Now let's move on to another important cybersecurity area, risk assessment. Firms should do regular assessments to identify cybersecurity risks associated with firm assets and vendors, and prioritize their remediation. One effective practice is to identify and maintain an inventory of assets authorized to access the firm's network and critical assets that should have prioritized protection. Another is to conduct a comprehensive cybersecurity risk assessment. It should include looking at external and internal threats and asset vulnerabilities, and it should include a prioritized and time-bound set of recommendations to deal with those risks.

SP FINRA views the risk assessment process as a key driver in a firm's risk-management based cybersecurity program, and it should lead to changes in a firm's controls to remediate identified risks. Some examples include adding antivirus or email content analysis software and setting up system restore processes.

SR And planning in light of risk assessment leads us to our third cybersecurity area, incident response. Its goal is to provide a framework to manage a cybersecurity event in a way that limits damage, increases stakeholder confidence, and reduces recovery time and costs. A firm's response plan should address different attack scenarios since they can come from many different directions. Firms cannot prepare response plans for every possible incident, but they should at least have plans for the most common attacks.

Based on details firms provide to FINRA, common events include distributed denial of service attacks, malware infections, insider threats, and cyber-enabled fraudulent wire transfers.

SP Incident response plans generally include five broad steps. First is containment and mitigation. This is important to stop an incident from causing more damage or overwhelming the firm's resources. Depending on the attack, responses might include things like shutting down a system or disconnecting it from the network. The next step is eradication and recovery. After the incident is contained, firms may need to get rid of the problem. As part of this, they may need to find and close exploited vulnerabilities, then administrators can recover by restoring systems and confirming they're functioning normally.

SR Once recovery is complete, a timely investigation should determine what was lost and the root causes. That's why it's important for firms to develop a log-retention policy. Some firms do not save log information in an effort to reduce costs and that has impeded investigations.

SP The fourth incident response step is notification. The plan should lay out who should be notified and what should be reported and when. Firms should determine whether they have notification obligations under SEC identity theft regulation SID, state reporting requirements or FINRA rules, and FINRA urges firms to report incidents that do not trigger a reporting obligation through their regulatory coordinator.

SR And the fifth step is making clients whole. If clients lost money or had their personal identifying information exposed, it can lead both to material loss and loss of investor

confidence in broker-dealers as a whole, so firms should take steps to address this. For instance, they should provide free credit monitoring services to customers whose information has been compromised. And they should reimburse clients who have lost money through direct attacks like account takeovers or through a cyber-enabled attack like a phishing attack that leads to a fraudulent wire transfer.

SP The topics we talked about represent just a portion of the technology and cybersecurity priorities in the 2016 Regulatory and Examination Priorities Letter, as well as FINRA's cybersecurity report. So, be sure to check out both of them for more information.

SR We hope you found this podcast helpful, and that you'll share it with your colleagues. And stay tuned for the next episode in the series where we will highlight even more exam priorities like sales practice and market integrity.

SP Until then, for all of us at FINRA, thanks for listening.