CYBERSECURITY: FINRA GUIDANCE THROUGH 2018 PRIORITIES AND RECENT EXAM FINDINGS INCLUDING SDDCO REGULATORY SERVICES, LLC ELEMENTS

The Financial Industry Regulatory Authority (FINRA) is ramping up on their commitment to assist the industry in its cybersecurity compliance efforts. Recent guidance to the industry from FINRA includes:

1. Examination Findings Report, detailing observations from recent broker-dealer examinations with the goal of assisting broker-dealers in enhancing their compliance programs and better anticipating potential areas of concern (FINRA included compliance areas to highlight based on the frequency of deficiencies and the potential impact on investors and markets); and
2. The 2018 Regulatory and Examination Priorities, in which, notably, FINRA instructed firms to review the priorities in conjunction with the Examination Findings Report.

FINRA called out cybersecurity, in its Examination Findings Report, as one of the "principal operational risks facing broker-dealers." While acknowledging the increased threats today, FINRA noted that firms have generally increased their focus on cybersecurity issues and some firms examined are at the forefront of developing "cutting-edge cybersecurity programs."

FINRA detailed areas in which they observed in the examinations that firms' cybersecurity programs were either effective or deficient. Reviewing the positives and negatives provides valuable information for firms looking to shore up their cybersecurity programs.

EXAMPLES OF EFFECTIVE PRACTICES INCLUDE:

- **Escalation Protocols:** Have an escalation process that ensures appropriate level at the firm is apprised of issues to ensure attention and resolution.
- SDDco Regulatory Services, LLC trains and educates personnel to recognize exposure incidents and provides incident reporting from within the client dashboard.
- **Plans to Resolve Issues:** Implement detailed resolution steps and timeframes for completion.
- Upon determination of an exposure event SDDco Regulatory Services, LLC activates full response management including containment, planning, investigations and determination of state, federal, notifications and corrective actions.
- **Routine Risk Assessments:** Conduct regular risk assessments, including vulnerability and penetration tests.
- SDDco Regulatory Services, LLC coverage includes cybersecurity risk assessments, data handling assessments, email vulnerability testing, and infrastructure testing including endpoints and full external penetration tests.
- **Routine Training:** Conduct training for firm employees, including training tailored to different functions, in addition to generic cross-firm training.
- SDDco Regulatory Services, LLC customizes and provides multiple actively managed and ongoing data security training and testing for all designated individuals.
- **Branch Office Reviews:** Include cybersecurity focused branch exams to assess risks and identify issues.
- SDDco Regulatory Services, LLC coverage includes data handling assessment and guidance.

CYBERSECURITY: FINRA GUIDANCE THROUGH 2018 PRIORITIES AND RECENT EXAM FINDINGS INCLUDING SDDCO REGULATORY SERVICES, LLC ELEMENTS

- **Additional Practices:** Implement security information and event management practices, use system usage analytics, and adopt data loss prevention tools.
- SDDco Regulatory Services, LLC provides electronic endpoint diagnostics along with other tools to identify vulnerabilities.

EXAMPLES OF DEFICIENT PRACTICES INCLUDE:

- **Failure to Follow Access Management Steps:**
  - Not immediately terminating access of departing employees.
  - Failing to have processes to monitor or supervise "privileged users" to identify unusual activity (e.g., assigning extra access rights, unauthorized work outside business hours, or logging in from different geographical locations at or about the same time).
  - SDDco Regulatory Services, LLC develops full policies and procedures including data access privileges.
  - SDDco Regulatory Services, LLC provides electronic endpoint diagnostics along with other tools to ensure compliance with policies and procedures.
- **Infrequent or No Risk Assessments:**
  - No formal risk assessment practices.
  - Unable to identify critical assets or potential risks.
  - SDDco Regulatory Services, LLC provides and includes multiple electronic and human risk and diagnostic assessments ranging from cybersecurity to infrastructure diagnostics.
- **Informal Processes for or Lack of Vendor Management:**
  - Failed to have formal processes to assess vendor's cybersecurity preparedness;
  - Failed to include required notification of breaches involving customer information in vendor contracts.
  - SDDco Regulatory Services, LLC provides and produces full third party rostering and vendor due diligence along with vendor agreements.
- **Noncompliant Branch Offices:**
  - Failed to manage passwords.
  - Failed to implement security patches and software updates.
  - Failed to update anti-virus software.
  - Lacked control of employee use of removable storage devices.
  - Use of unencrypted data and devices.
  - Failed to report incidents.
  - SDDco Regulatory Services, LLC develops full policies and procedures including cybersecurity controls.
  - SDDco Regulatory Services, LLC technology provides hub and spoke deployment which retains home office requirements while allowing for branch individuality.
- **Segregation of Duties:**
  - Failed to segregate duties for requesting, implementing, and approving cyber-security rules and systems changes.
  - SDDco Regulatory Services, LLC develops full policies and procedures including identification or roles and responsibilities as related to cybersecurity.

- **Data Loss Prevention:**
  - Lack of rules to ensure all customer sensitive information is covered.
  - Permitted or failed to block large file transfers to outside or untrusted recipients.
  - Failed to implement formal change-management processes for data loss prevention systems changes.
  - SDDco Regulatory Services, LLC develops full policies and procedures including data handling controls.
  - SDDco Regulatory Services, LLC provides electronic endpoint diagnostics along with other tools to ensure compliance with policies and procedures.

FINRA's *2018 Examination and Regulatory Priorities* also include cybersecurity as a priority area. In addition to the areas noted above, which FINRA also calls out in the Priority Letter, FINRA noted two additional themes. One, they will evaluate the effectiveness of firms' cybersecurity programs in protecting sensitive information. Two, FINRA also reminds firms that they need policies and procedures to determine when a Suspicious Activity Report should be filed regarding a cybersecurity event. (See, FinCEN's *Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime*, Oct. 25, 2016.)

CONCLUSION

FINRA reminds firms that, while exam deficiencies must be addressed, firms often benefit from "proactively" remediating issues before the exam is completed. Acting proactively strengthens firms' programs and enhances regulatory protections. Our observation, as outside counsel, is that when firms take proactive steps to get ahead of issues, it demonstrates to the regulators that the firm has a commitment to a strong compliance program and, in the right circumstances, may have a material impact on how FINRA decides to resolve an issue.

The information FINRA provides in the Examination Report and Priorities Letter provides roadmaps to enhancing overall compliance, supervisory, and risk management programs. With regard to the focus on cybersecurity, by using this resource, firms can effectively prepare for examinations and potentially prevent program gaps and avoid cybersecurity incidents.