FINRA GUIDANCE

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

- Examination Findings Report, detailing observations from recent broker-dealer examinations with the goal of assisting broker-dealers in enhancing their compliance programs and better.

- The 2018 Regulatory and Examination Priorities, in which, notably, FINRA instructed firms to review the priorities in conjunction with the Examination Findings Report.

EXAMPLES OF EFFECTIVE PRACTICES

Routine Risk Assessments: Firms should conduct assessments of cybersecurity risks, data handling processes, and overall business security vulnerabilities. Assessments should include vulnerability and penetration tests.

Escalation Protocols: Have an escalation process that ensures appropriate level at the firm is apprised of issues to ensure attention and resolution.

Plans to Resolve Issues: Implement detailed resolution steps and timeframes for completion.

Routine Training: Conduct training for firm employees, including training tailored to different functions, in addition to generic cross-firm training.

Branch Office Reviews: Include cybersecurity focused branch exams to assess risks and identify issues.

RECOMMENDATIONS

(This Example is from a recent FINRA exam)

During the review of the firm's cybersecurity program, Staff noted areas of improvement opportunities in the firm's existing systems and controls and as a result, staff recommends that the firm implement the enhancements listed below.

a) Governance – The firm should conduct regularly scheduled cybersecurity meetings at least twice a year as stated in its Written Supervisory Procedures, or even more frequently in line with industry best practices.

b) Data Protection:
   i. The firm should require encryption of desktop and laptop computer hard drives in both the home office and branch locations. Confidential data could be downloaded using spreadsheets before being transmitted to customers or to the clearing firm;
   ii. Establish a data classification policy that clearly identifies sensitive data and protect them as needed; and
   iii. Evaluate implementation of a data loss prevention solution to monitor and encrypt sensitive data before being sent outside the network.

c) Business Continuity and Disaster Recovery – The firm should test the Business Continuity and Disaster Recovery plan at least once a year in order to ensure that the plan in place will function properly in case of a disaster.

d) Secure Configuration – The firm should implement a process that confirms proper application of updates as part of its patch management process. The process should include a follow up step to ensure application of needed updates in a timely manner.