Cybersecurity Regulations and the Financial Services Sector: Be Prepared

By Jonathan Hard
Jonathan.Hard@h2lsolutions.com

Cybersecurity Regulations and the Financial Services Sector: Be Prepared

EXECUTIVE SUMMARY

It is commonly known that cybersecurity has become a major point of discussion in the past few years. With US organizations experiencing major security hits, such as those that occurred at JPMorgan, Bank of America, and Citigroup, as well as the onslaught of serious Ransomware and DDoS attacks, regulatory organizations have begun to take notice and act on establishing security standards meant to help guide companies on how to protect their organizations from being compromised. In 2013, President Obama signed Executive Order (EO) 13636 for "Improving Critical Infrastructure Cybersecurity" where the National Institute for Standards and Technology (NIST) was tasked to work with the private sector on developing industry best practices that would be incorporated into an overarching Cybersecurity Framework[1]. The EO effectively jumpstarted a broad movement across industries to being implementing sound cybersecurity measures within organizations. This progression has also moved into the Financial Industry.

Starting in 2014, the Securities and Exchange Commission (SEC) has gradually been moving cybersecurity into the forefront of their attention. The SEC has charged its Office of Compliance Inspections and Examinations (OCIE) with developing examinations that focus on how organizations are effectively implementing cybersecurity measures within their infrastructure. The first cybersecurity sweep initiative was issued in April of 2014[2], with the goal of assessing where the industry was in addressing cybersecurity and determining which cyber threats were have the most impact on organizations. In 2015, the Cybersecurity Examination Initiative[3] was further refined into a set list of categories that were to be assessed during examinations, with focus on how companies are protecting client information. In 2016, the SEC continued to build upon the established Cybersecurity Examinations with a specific focus on testing and assessing exactly how firms are implementing security procedures and controls[4]. For 2017, the organization prioritized three (3) main areas which included protecting retail investors, determining risks to retiring, and elderly investors and assessing market-wide risk.

After examining 75 firms, the OCIE noted that Broker-Dealers and Advisers showed an increased awareness of and had implemented controls to mitigate cybersecurity risk such as:

- Periodic risk assessments of critical systems to identify cybersecurity threats, vulnerabilities, and the potential business consequences of a cyber incident.
- Penetration tests and vulnerability scans on critical systems
- Some form of system, utility, or tool for data loss prevention as it relates to personally identifiable information.
- A process in place for ensuring regular system maintenance, including the installation of software patches to address security vulnerabilities.

- Cyber-related business continuity planning and response plans for addressing security incidents including denial of service incidents and unauthorized intrusions.
- A cybersecurity organization with identified cybersecurity roles and responsibilities.
- Vendor risk assessments or requirements that vendors provide the firms with risk management and performance reports and security reviews or certification reports[6].

CURRENT REQUIREMENTS

While the examinations conducted in 2016 focused on ensuring that firms were "doing what they say they are doing" within their organizations, the assessments for 2017 involved monitoring automated investment advice, bundled fees for advisory and brokerage services, exchange-traded funds (ETFs), and review requirements for investment advisers.

Along with these, the SEC continued its multi-year examination of the ReTIRE initiative which focused on retirement accounts services provided by investment advisers and broker-dealers. Public pension advisers were also included in the examinations as they handle pension plans and retirement assets for states and other government entities. The SEC also investigated how firms managed their interactions with senior investors.

Reforms made to Money Market Fund management in 2014 became effective in October of 2016 and the SEC continued its investigation to assess how a company handles oversight, risk and reporting as well as compliance with the changes. Payment processing, clearing agencies, and any specific areas of risk such as money laundering and terrorist financing were also being closely investigated.

Along with cybersecurity, another key area of concern is having appropriate policies and procedures in place. The OCIE examines cybersecurity compliance procedures and controls and verifies that those controls were being tested. Additionally, a firm's policies and procedures were assessed based on whether the documents were maintained and enforced. The OCIE reviewed controls related to recording time transactions, how they synchronized with other systems, and how market data was collected and analyzed. Further, the investigations cover how a company handles risk management for their main office as well as any off-site locations[5].

At this time, the SEC is focusing on reviewing company operations for IT governance and risk assessments, access rights and controls, sensitive data loss prevention, management of all vendors in use, proper awareness training for employees and a tested, incident response program. A more granular breakdown of the requirements is shown below.

The SEC is requiring firms to conduct periodic assessments and are expecting to see proof of the following:

- Nature, sensitivity, and location of information collected, processed and stored by firms.
- Existing threats and vulnerabilities of individual firms.
- Security controls and processes currently in place.
- The impact of a specific technology or system being compromised.
- The effectiveness of the IT governance structure for the management of cybersecurity risk.
- Robust policies and procedures including classifications of risk, business consequences, acceptable

use, mobile device management, vetting of vendors, and employee access.

The SEC expects the firms to create a strategy that is designed to prevent, detect, and respond to cybersecurity threats, such strategies include:

- Control access via management of user credentials, authentication and authorization, firewalls, tiered access to sensitive information and network resources, network segregation and system hardening
- Data encryption at rest and in motion
- Protect data loss or exfiltration via removable media by deploying software that monitors for exfiltration, unauthorized extraction, or other unusual events
- Perform frequent data backups and test the retrieval process
- Development of incident response plan which is one of the major focus points of the SEC and should be tested frequently
- Continuous monitoring and system maintenance includes vulnerability scans and patch management
- Detailed cybersecurity related policies and procedures for penetration testing, security monitoring and auditing, access rights, and incident reporting
- Mandatory employee security training and verification of senior management engagement[6]

RECOMMENDATIONS

As many firms are beginning to understand, the SEC is not taking cybersecurity lightly; however, there are many possible solutions that can help organizations meet, or even exceed, these requirements.

With the results of the past year's examination, it is critical that firms develop strong policies and procedures as the initial building blocks of a strong cybersecurity program. Providing proper security, and specifically, cybersecurity, training for employees is an excellent way to incorporate security into the work environment. This aids in developing company-wide awareness of everyday threats.

Aside from the compliance requirements flowed down from the SEC, firms can also benefit from referencing Federal security policies and procedures such as identity theft, data protection, fraud, or business continuity. Cybersecurity regulations often have overlapping general security measures listed in their documents. Therefore, by becoming compliant with one Federal security regulation, a firm can jumpstart their compliance process with another regulation.

Firms may also mitigate exposure to technical threats and risks by performing frequent vulnerability assessments, penetration tests, actively monitoring the existing IT environment, testing the validity of the backup systems and the incident response programs in place. In addition to the robust policies and procedures, a firm needs to conduct ongoing risk assessments and have a written and actionable process to remediate any findings[6].

CONCLUSION

The requirements and initiatives for cybersecurity that are being pushed by the SEC may seem like a daunting task for a team that does not have a dedicated IT security staff, but tackling the cybersecurity initiatives will, in the end, create a safer and more efficient work place, as well as provide a stronger protection of employee and client data. In the upcoming SEC audits, firms can expect to be analyzed at the policy and procedure level as well as the technical level.

H2L prides itself on helping organizations become compliant with cybersecurity regulations. If your organization has any questions concerning the new SEC requirements, please contact us at info@h2lsolutions.com.

REFERENCES

[1]Cybersecurity – Executive Order 13636. https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/eo-13636

[2]OCIE Cybersecurity Initiative. https://www.sec.gov/ocie/announcement/Cybersecurity-Risk-Alert--Appendix---4.15.14.pdf

[3]OCIE's 2015 Cybersecurity Examination Initiative. https://www.sec.gov/ocie/announcement/ocie-2015-cybersecurity-examination-initiative.pdf

[4]Examination Priorities for 2016. https://www.sec.gov/about/offices/ocie/national-examination-program-priorities-2016.pdf

[5]Examination Priorities for 2017. https://www.sec.gov/about/offices/ocie/national-examination-program-priorities-2017.pdf

[6]Observations from Cybersecurity Examinations. https://www.sec.gov/files/observations-from-cybersecurity-examinations.pdf