How to Prepare for an SEC Cybersecurity Exam

By Adam Stutz, edited by James Smith

About the Authors:
Adam Stutz is a Compliance Consultant at Core Compliance & Legal Services ("CCLS"). He can be reached at adam.stutz@corecls.com.
James Smith is a Sr. Compliance Consultant at Core Compliance & Legal Services ("CCLS"). He can be reached at james.smith@corecls.com.

This article was originally published by Core Compliance & Legal Services, Inc. in October 2020.

Cybersecurity continues to be a top priority for the Securities and Exchange Commission's ("SEC") Office of Compliance Inspections and Examinations' ("OCIE"), especially as the bulk of firms have had to shift to working remotely in light of COVID-19. Just in the past few months, OCIE has issued risk alerts reminding firms to remain vigilant and to proactively address cyber risks.[1] [2]

Despite the changes in workplace dynamics due to the pandemic, OCIE shows no signs of slowing its examinations of investment advisers and broker-dealers, and it is vital that firms prepare for the possibility of a cybersecurity focused exam.

SEC exams are daunting enough, and a focused cybersecurity exam can give any seasoned Chief Compliance Officer ("CCO") and/or Information Security Officer ("ISO") pause. Many CCOs and ISOs might be asking themselves: what parts of the firm's cybersecurity program will be scrutinized by the SEC? What areas should the CCO and/or ISO review in preparation for the exam? How should the firm test its current controls? How should the firm respond to gaps in controls? What kind of documentation does the SEC expect the firm to have when it comes to cybersecurity? How does the firm prepare employees for a cybersecurity sweep exam?

In this article, we discuss the steps you can take to prepare for and thrive during a cybersecurity sweep exam.

The Risk Assessment

The risk assessment is one of the most important tools in any firm's compliance arsenal, and especially so when used to evaluate the strengths of the different domains of your cybersecurity program.

By evaluating and classifying the high, medium, and low levels of risk associated with you program's governance, access rights, data loss prevention, vendor management and incident response domains, you can build a road map to determine which controls require the most immediate attention and proceed to implement, strengthen or add controls in order to address the risk and threat levels within the relevant domain.

When thinking about how to conduct your risk assessment, an important consideration is whether the firm should conduct the assessment internally or if an independent third-party should conduct an external assessment. As the firm evaluates its options, your firm's stakeholders should contemplate an approach that is going to yield an independent and thorough evaluation of the firm's cybersecurity controls and identified risk levels in order to best address possible gaps and enhance controls.

As your firm goes through the process of conducting a risk assessment, it is important to consider one of the most important pillars of any cybersecurity program - strong policies and procedures.

Cybersecurity Policies and Procedures

A firm's policies and procedures ("P&Ps") are the framework upon which any compliance program is built, and it is no different for cybersecurity. When thinking about preparation for a

1. https://www.sec.gov/ocie/announcement/risk-alert-covid19-compliance.
2. https://www.sec.gov/ocie/announcement/risk-alert-credential-compromise.

cybersecurity exam, it is important to consider your P&Ps as your foundation. When assessing your P&Ps, think about whether they contemplate the domains listed above (governance, access rights, data loss, etc.) and do they acknowledge specific controls within those domains, including:

- Identification of an ISO or principal responsible for oversight of cybersecurity
- Controls for the protection of client records containing client personal identifying information
- Vulnerability assessments and penetration tests
- Patch management controls
- Verification of client fund transfer requests
- Identity theft and privacy regulations
- Access management
- Vendor management and due diligence
- Change management including new hires, transfers, and terminations
- Data exfiltration and loss prevention
- Login failures, lockouts, and password resets
- Personal devices and removable storage
- Business continuity and disaster recovery
- Training of employees and independent contractors
- Incident response plans and tests

The list is substantial, but it is important to bear in mind that your P&Ps need to address these domains ***and*** be customized specifically for your firm's business model. Scalability is important to think about as you review your policies and procedures. There is no one-size-fits-all solution for firms so it will be important for the CCO, ISO, and senior management to work together to review and address gaps in the policies and procedures. Which brings us to another important topic: governance.

Governance

Buy-in from senior management on the firm's cybersecurity program in preparation for a cybersecurity focused exam is important because it affects the "tone from the top." Your senior managers need to understand the different risk levels associated with the different domains of your cybersecurity program in order to both address issues as they arise but also to provide an example for the firm's rank and file on the importance of cybersecurity. Often the level of involvement by senior management can be evidenced by the level of documentation provided to senior managers including periodic reports, training, presentations, and continuing education. By engaging the firm's senior management, it will also aid the CCO and/or ISO in allocating time and resources to be able to maintain strong controls and address gaps that will be crucial during a sweep exam.

Inventories and Reports

Inventories and reports are also essential tools to evaluate the controls at your firm. Often when we think of inventories, we focus on the identification of a firm's hardware and software and keeping lists that identify attributes such as makes, models, and serial numbers. But inventories should go beyond equipment and applications and focus on other areas including:

- Contracts, terms of service, and audit reports
- Patch management schedules
- Anti-malware, anti-virus, and intrusion detection applications
- Service-provider and vendor lists

- Access Management and change management logs documenting network credentials and permissions for firm employees as well as independent contractors and vendors
- Login, lock-out, and unauthorized attempt logins

Inventories should not only be helpful in tracking the type of information that you are retaining for your cybersecurity program but should also be helpful in identifying where you are maintaining this information as part of your books and records. Inventories can also serve as a good source for outlining the types of reports your firm should maintain for their processes. Much like other areas of compliance, reports are great tools for conducting periodic tests of the cybersecurity program to practice pattern detection and show potential weaknesses. Examples of periodic reports include:

- Vulnerability and threat reports
- Penetration test results
- Anti-malware and anti-virus scans
- Patch management reports

These reports can provide valuable information not only to the CCO and ISO, but also to senior management to outline threat vectors, malefactors, and provide a holistic view on the state of the firm's cybersecurity program to determine if things are working or if additional controls and resources are necessary.

Incident Response Plan Testing

An incident response plan ("IRP") is an important tool to help a firm prepare for cybersecurity incidents. A good incident response plan will address how the firm identifies cybersecurity incidents; contains affected systems; eradicates the threat; recovers and rebuilds systems; and lays out the firm's post-incident response procedures. In order to ensure that your firm's IRP remains effective, periodic IRP testing should be conducted regularly to evaluate the strength of your IRP and address any gaps in controls. IRP testing can also help to prepare your firm for a cybersecurity focused exam.

When thinking about testing your incident response plan, consider how your firm will respond to and remediate any cyberattacks that occur within your firm's cybersecurity framework. Before beginning the test, we would suggest seeking out the services of a reputable third-party vendor to simulate a cyberattack. Prior to the simulation, sit down with your staff and discuss the incident response plan and review the firm's steps for identification, containment, eradication, recovery, and post-incident procedures. Posit different outcomes and discuss running different scenarios to engage not just your IT staff but also your senior management and other firm employees to practice the steps addressed in the IRP.

Once the test is complete, make sure to document and discuss the results and determine if updates to and the addition of controls are necessary, and then commit to a schedule of implementing those updates.

Training

Training is another important area that the SEC will want to examine when conducting a cybersecurity exam. We believe that training shouldn't be relegated to an annual exercise where employees are forced to gather in a conference room to learn about cybersecurity, but rather, training should be a year-long exercise that is engaging, thoughtful and customized to the needs of the firm.

For example, some firms might utilize the use of phishing tests to simulate a phishing email campaign. By engaging employees in the phishing email tests, CCOs and/or ISOs can determine if there are trends that indicate that employees need more training and to target training for those individuals that might need a leg-up on their cybersecurity knowledge.

Another way to raise awareness and educate the firm on cybersecurity topics is to share OCIE's risk alerts and SEC enforcement cases. The risk alerts provide valuable outlines on best practices for the firm and the enforcement cases can supply examples of real-world consequences for firms that do not implement suitable controls for their cybersecurity programs.

Lastly, you should make sure to document and maintain all of the various training methods that have been utilized, presentations, phishing tests, training exercises, reading materials, and training attendee lists as part of your books and records.

Cybersecurity Mock Audit

We feel that the cybersecurity mock audit is going to be one of the most effective tools to prepare your firm for a cybersecurity focused exam. We suggest engaging an independent consultant to conduct the mock audit to provide objective and unvarnished recommendations. When sitting down with the consultant, make sure to discuss the goals of the mock audit and communicate the importance of covering all your different risk domains. The service provider or consultant conducting the mock audit should also provide you with the following documents and activities when conducting the mock audit:

- A request for specific books and records related to the firm's cybersecurity program including policies and procedures, inventories, risk assessments, audit reports, IRPs, test results, and training materials
- Engaging in practice interviews with the CCO, ISO or principal responsible for cybersecurity, and senior management
- Tests of certain controls and requests for demonstrations of certain systems
- Furnishing a report with findings and recommendations based on the results of the mock audit.

Much like the risk assessment, we believe that having an experienced consultant present to conduct a thorough mock audit of the firm that closely simulates of an actual SEC exam will only serve to strengthen your firm in preparation for the real thing.

Conclusion

As outlined above, preparation for a cybersecurity focused exam is an involved process and as a CCOs and/or ISO, you need to confirm that you have the right controls in place in order to confidently demonstrate that your firms' cybersecurity programs can withstand regulatory inspection. However, we believe if you firm has the right tools and takes steps to perform risk assessments, review your policies and procedures, assemble inventories and reports, conduct testing and training, and engage in mock audits, you will be well-prepared for a cybersecurity focused exam. ■