THIS MONTH'S RESOURCE
SEC/State Cybersecurity Sweep Exams

AUGUST FOCUS: **CYBERSECURITY SWEEP EXAMS**

This year, the SEC has focused its efforts on examining firms regarding their cybersecurity programs. It's not a matter of **"if"** firms experience an attempted breach but **"when."** The SEC and State regulatory agencies want to know firms have protocols to mitigate risk for client data exposure. This month we address a **sampling of request items directly from an SEC Exam Item Request List**, as well as recently published information from the DOL. With these resources, we'll outline some **"think-through"** items to assist firms in getting prepared for an exam and/or possible future breach.

➢ HAVE A FORMAL, WELL DOCUMENTED CYBERSECURITY PROGRAM

1. **Sample Sec Exam Item Request:**
   Provide compliance and operational policies and procedures in effect during the Review Period for the Adviser and its affiliates. Please be sure to include policies and procedures addressing the protection of customer/client records and information; including those that are designed to secure customer/client documents and information, protect against anticipated threats to customer/client information, and protect against unauthorized access to customer/client accounts or information for the review period.

   Firm Think-Through Items:
   - ☐ Does your Firm have tailored cybersecurity policies or procedures?
     DATE OF LAST REVIEW: _____

➢ HAVE STRONG ACCESS CONTROL PROCEDURES

2. **Sample SEC Exam Item Request:**
   Provide a list of the systems or applications for which Registrant uses multi-factor authentication for employee, contractor/vendor, other third parties, and client access. Please include the type of multi-factor authentication employed for each system or application. Also, provide a list of the systems or applications for which the Registrant does not use multi-factor authentication.

   Firm Think-Through Items:
   - ☐ Does the Firm require multi-factor authentication for mission-critical systems and email domains?

➢ CLEARLY DEFINE AND ASSIGN INFORMATION SECURITY ROLES AND RESPONSIBILITIES

3. **Sample SEC Exam Item Request:**
   Identify the Chief Information Security Officer or equivalent position. If the role does not exist, explain where the principal responsibility for overseeing cybersecurity resides within the Registrant.

4. **Sample SEC Exam Item Request:**
   If the Registrant conducts reviews of users (i.e., employee, IAR, contractor/vendors, other third parties) access rights and restrictions concerning professional roles or job-specific resources within the network, provide a list of reviews conducted during the Examination Period with a brief description of each. If the Registrant maintains documentation related to these reviews, provide a copy of the most recent report for each type of review.

   Firm Think-Through Items:
   - ☐ Who in the Firm is accountable for security policies and procedures?
   - ☐ Review individuals, third-party vendors responsible for assigned IT roles.
     DATE OF REVIEW: _____

➢ CONDUCT PRUDENT ANNUAL RISK ASSESSMENTS

5. **Sample SEC Exam Item Request:**
   Provide a copy of the Registrant's policies and procedures relating to risk assessment and data risk classification. Please include a list of the risk level classification (e.g., low, medium, or high) associated with each data classification

(email, cloud, client files, etc.) and a description of how the factors and risks are considered when determining where data fits within each classification.

6. **Sample SEC Exam Item Request:**
   Provide information regarding the Firm's periodic risk assessments to identify cybersecurity threats, vulnerabilities, and potential business and compliance consequences. If applicable, note the date of the most recent risk assessment, any related high or medium criticality findings, and responsive remediation efforts taken by the Firm.

   Firm Think-Through Item:
   - ☐ Is there a third-party vendor with direct access to Firm systems and is involved in the design, implementation, and ongoing maintenance of security controls? *Note: Third-party vendors assist with audits and security assessments and hold much of the knowledge needed to complete the audits and exams.*

➢ ENSURE THAT ANY ASSETS OR DATA STORED IN A CLOUD OR MANAGED BY A THIRD-PARTY SERVICE PROVIDER ARE SUBJECT TO APPROPRIATE SECURITY REVIEWS AND INDEPENDENT SECURITY ASSESSMENTS

7. **Sample SEC Exam Item Request:**
   Provide a list of all third-party vendors with access to the Registrant's network, systems, or data. Would you please indicate whether the vendor is a web or cloud-based service provider or a cybersecurity-related vendor?

8. **Sample SEC Exam Item Request:**
   Provide a copy of the Registrant's policies, procedures, and standards for contracting with third-party vendors, including cloud service providers. If no written policies or procedures exist, please describe the Registrant's vendor selection, management, and oversight processes.

9. **Sample SEC Exam Item Request:**
   Provide a list of terminated vendors during the Examination Period.

   Firm Think-Through Item:
   - ☐ Last date of the due diligence conducted on new and existing vendors.
     DATE OF REVIEW: _____
   - ☐ Does the Firm routinely (annually) review the vendor's compliance with agreements and any third-party assessments/audits on the third-party vendor?

➢ CONDUCT PERIODIC CYBERSECURITY AWARENESS TRAINING

10. **Sample SEC Exam Item Request:**
    Please provide a list of any training offered by the Registrant and/or third-party vendors to its employees, contractor/vendors during the examination period related to cybersecurity and risks (e.g., the Registrant's cybersecurity policies and procedures, acceptable use of mobile devices, anti-phishing, ransomware, denial of service, etc.). For each training, please identify the date(s) offered, topics, nature of the training method (e.g., in person, computer-based learning, or email alerts), and groups of participants.

    Firm Think-Through Item:
    - ☐ Date of last employee training on cybersecurity. DATE OF REVIEW: _____
    - ☐ Does the Firm conduct initial (upon hire) and ongoing access to online training?
      (Vendor Resource: www.knowbe4.com)

➢ HAVE AN EFFECTIVE BUSINESS RESILIENCY PROGRAM ADDRESSING BUSINESS CONTINUITY, DISASTER RECOVERY, AND INCIDENT RESPONSE.

11. **Sample SEC Exam Item Request:**
Provide a copy of the Registrant's written plan that addresses mitigation of the effects of a cybersecurity incident and/or recovery from such an incident if such a plan exists. If the Registrant maintains separate written cybersecurity incident response policies and procedures, please provide a copy.

12. **Sample SEC Exam Item Request:**
Provide a copy of the Registrant's policies and procedures for conducting tests or exercises of its incident response plan, including the frequency of such testing, if applicable.

Firm Think-Through Item:

- ☐ Has the Firm designed, implemented, maintained, monitored, and tested backup and disaster recovery solutions as part of business continuity and disaster recovery plans?

➢ ENCRYPT SENSITIVE DATA STORED AND IN TRANSIT

13. **Sample SEC Exam Item Request:**
Provide a copy of the Registrant's policies and procedures relating to the encryption of data "in motion" both internally and externally and data "at rest" on all systems and servers, including both on-premises and off-premises.

14. **Sample SEC Exam Item Request:**
Provide a copy of the Registrant's policies, procedures, and standards regarding any devices (i.e., Registrant-issued, and personal devices) used by employees, contractors/vendors, and/or other third parties to access the Registrant's system externally, including any written policies or procedures addressing the encryption of such devices and the Registrant's ability to monitor, track, and deactivate remote devices remotely.

Firm Think-Through Items:

- ☐ What system and controls are in place within the Firm to encrypt Firm data (1) at rest and (2) data in transit?
- ☐ Create an inventory of all employees, contractors/vendors, and/or other third-party devices that access firm systems. DATE OF REVIEW: _____

➢ APPROPRIATELY RESPOND TO ANY PAST CYBERSECURITY INCIDENTS

15. **Sample SEC Exam Item Request:**
Provide a list of all cybersecurity incidents or breaches that occurred during the Examination Period.

Firm Think-Through Items:

- ☐ Who is responsible to reviewing cybersecurity incidents? NAME: _____
- ☐ Are they adequately investigated, responded to, and documented? ☐ YES ☐ NO
- ☐ If required, is there proper notification to those affected? ☐ YES ☐ NO
- ☐ Was there follow-up per regulatory requirements and data privacy laws? ☐ YES ☐ NO

CRP has included a CCO Technology Review Checklist to assist with the review of additional policies and procedure considerations relating to a Firm's Cyber-Tech Program.