October 2015

Regulatory brief

A publication of PwC's financial services regulatory practice

Cybersecurity: SEC round two

Overview

On September 15th, the Securities and Exchange Commission (SEC) issued a risk alert, announcing the agency's 2015 cybersecurity examination priorities. The issuance makes it clear that this year's examinations will cover more areas of cybersecurity and will go deeper into each area than last year's first round did. Most notably, the bar has been raised for requirements around data loss prevention, access controls, and cybersecurity governance.

The SEC's Office of Compliance Inspections and Examinations (OCIE) launched its cybersecurity examinations last year, as part of the broader regulatory response to the recent wave of high-profile cybersecurity breaches.[1] Given the continuing rise of cyber threats facing financial institutions and identified gaps in the industry's defensive measures, it comes as no surprise that this year OCIE expects broker-dealers and investment advisors to demonstrate more mature cybersecurity programs.

To meet this expectation, entities will need to prove (with adequate documentation) that their cybersecurity controls are sufficient and operate consistently. This includes robust cyber risk oversight by the Board and senior management,[2] strong authentication mechanisms, and enhanced controls over data transmission by employees and third party vendors,[3] among other measures.

Accordingly, firms should focus on (i) developing a complete asset inventory which includes all types of critical data and systems, (ii) conducting a cyber risk assessment which identifies risks inherent in the environment, (iii) establishing controls to mitigate identified risks, (iv) enhancing controls such as multi-factor authentication and data loss prevention (DLP), and (v) assessing adequacy of controls used by vendors.

In our view developing a complete asset inventory of critical data is the most often misunderstood part of the process. These assets should not just include customer-related data that is collected, stored, or processed (e.g., personally identifiable information, protected health information, or bank account data), but in order to be done effectively must also include information that cuts across the business. This type of information would include investment strategies (e.g., pending trades, investment logic, trading algorithms), research information (e.g., analytics models, signals), financial information (e.g., account balances, executive compensation), market information (e.g., external data feeds, market analytics), and payments processing data (e.g., wire transfers, accounts payable).

This **Regulatory brief** discusses (a) new expectations resulting from OCIE's 2015 priorities document with our suggestions for meeting them, and (b) our general guidance on best practices for preparing for OCIE examinations.

pwc

What has the SEC changed?

The table below outlines OCIE's additional examination requirements that were introduced last month and provides our assessment of what firms should do in order to prepare for them. The most significant update to the examination procedures has been in the area of DLP, so most firms will have the most additional work to do in this area.

	What is new?	What should firms do?
Governance and risk assessment	OCIE's examination will include an assessment of senior management's and the Board's oversight of cybersecurity. The assessment must focus on reports that are presented to senior management and the Board, and how key decisions are made and communicated throughout the organization. Additionally, OCIE will examine an organization's cyber risk assessment process to ensure that it identifies cyber risks inherent in the environment and assesses controls that are used to mitigate risk.	• Formalize senior management and Board responsibilities for cybersecurity. • Establish regular cybersecurity reporting to senior management and the Board. Reporting should include key metrics, control weaknesses, and remediation initiatives. • Translate cyber risks to business risks so that information can be easily understood by senior management and the Board. • Obtain management and Board's review and approval for key cybersecurity governance activities (e.g., major changes to policies, compliance exceptions, and risk acceptance). • Conduct a cyber risk assessment that identifies the risks associated with data and systems, and assesses the adequacy and operating effectiveness of controls that are used to mitigate risk.
Access rights and controls	OCIE's examination will assess the following related to access rights and controls: • Authentication mechanisms, including multi-factor authentication. • Access levels of employees, vendors, and customers for compliance with institutional policies. • Network segmentation practices and remote access controls. • Authentication of fund transfer requests and prevention of fraudulent requests.	• Enhance authentication mechanisms (e.g., multi-factor authentication) and ensure that strong authentication mechanisms have been implemented before execution of high impact transactions (e.g., funds transfers). • Implement an entitlements management program which includes all systems and applications containing critical data. Perform entitlement reviews for in-scope systems. • Segment the network to ensure that critical systems are not exposed to systems with lower control levels.
DLP	OCIE's examination will include data inventorying, data classification, and monitoring of unauthorized transfer of confidential information to external parties.	• Implement a DLP program including technology and processes to (a) inventory and classify structured (e.g., databases) and unstructured data (e.g., spreadsheets), (b) implement control levels based on data classification levels, (c) monitor for unauthorized or insecure transmissions of confidential data to external networks, and (d) respond to data loss incidents and enhance controls to mitigate risk.

	What is new?	What should firms do?
Incident response	OCIE will examine incident response procedures and practices to identify critical assets (data, systems, and services) and how control levels are defined based on asset criticality.	• Document an incident response procedure and train employees to follow it. • Identify critical systems and processes and ensure that control levels and incident response times are defined based on criticality.[4] • Conduct practice exercises to assess readiness to respond to cyber incidents.
Vendor management	OCIE will examine services provided by vendors who help firms mitigate cybersecurity risks (e.g., access control and DLP), and the business contingency plan when any critical vendor is unable to provide services.	• Assess the impact of service providers providing critical services, including cybersecurity controls management, and ensure adequate controls are in place to mitigate risk to systems and data. • Enhance the business contingency plan to include country risk and a contingency mechanism in case a critical vendor is unable to provide services (e.g., conflict of interest or going out of business).

Preparing for OCIE cybersecurity examinations

Preparing for a cybersecurity examination could be an intense and time-consuming exercise. In addition to the steps provided in the table above that firms should take to meet the additional requirements for this year's examinations, we recommend that firms continue to take the following steps to ensure preparedness:

1. Establish cybersecurity program

- Define enterprise-wide roles and responsibilities across the three lines of defense.
- Develop cybersecurity policies and procedures.
- Establish governance committees.

2. Perform risk assessment

- Develop asset inventory and identify critical assets
- Execute a cyber risk assessment to identify and understand risks inherent in technology and operations.
- Determine whether controls are commensurate with the identified risk levels.

3. Test effectiveness of controls

- Implement an independent controls testing function to assess the operating effectiveness of cybersecurity controls.
- Ensure that the controls testing program is sustainable.

4. Remediate control weaknesses

- Develop remediation plans for identified control weaknesses.
- Document instances of compliance exceptions and risk acceptances and present to management for approval.

5. Report to management and Board

- Present to senior management and the Board (a) results of the risk assessment and controls testing activities, (b) remediation plans, and (c) any proposed changes to cybersecurity program.

6. Prepare examination documentation

- Prepare documentation for the examination including (a) policies and procedures, (b) results of risk assessment and controls testing, (c) remediation plans, and (d) management and Board oversight (reports, communications, meeting minutes).

Endnotes

1. See PwC's *Whitepaper, Understanding and preparing for OCIE cybersecurity exams* (May 2014). For a broader discussion of regulators' actions, see PwC's *A closer look, Cyber: Think risk, not IT* (April 2015).
2. See PwC's *Viewpoint, Threat smart: Building a cyber resilient financial institution* (October 2014).
3. See PwC's *A closer look, Outsourcing: How cyber resilient are you?* (June 2015).
4. The NIST Cyber Security Framework is a useful tool to define cybersecurity control levels.

Additional information

For additional information about this **Regulatory brief** or PwC's Financial Services Regulatory Practice, please contact:

Dan Ryan
Financial Services Advisory Leader
646 471 8488
daniel.ryan@pwc.com

Adam Gilbert
Financial Services Global Regulatory Leader
646 471 5806
adam.gilbert@pwc.com

Sean Joyce
Financial Crimes Leader
703 918 3528
sean.joyce@pwc.com

Joseph Nocera
Financial Crimes Cybersecurity Leader
312 298 2745
joseph.nocera@pwc.com

Armen Meyer
Director of Regulatory Strategy
646 531 4519
armen.meyer@pwc.com

Contributor: Harish Siripurapu.

To learn more about financial services regulation from your iPad or iPhone, click here to download PwC's new Regulatory Navigator App from the Apple App Store.

Follow us on Twitter @PwC_US_FinSrvcs

© 2015 PricewaterhouseCoopers LLP, a Delaware limited liability partnership. All rights reserved. PwC refers to the US member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.

This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors. PwC US helps organizations and individuals create the value they're looking for. We're a member of the PwC network of firms in 158 countries with more than 180,000 people. We're committed to delivering quality in assurance, tax and advisory services. Tell us what matters to you and find out more by visiting us at www.pwc.com/us.