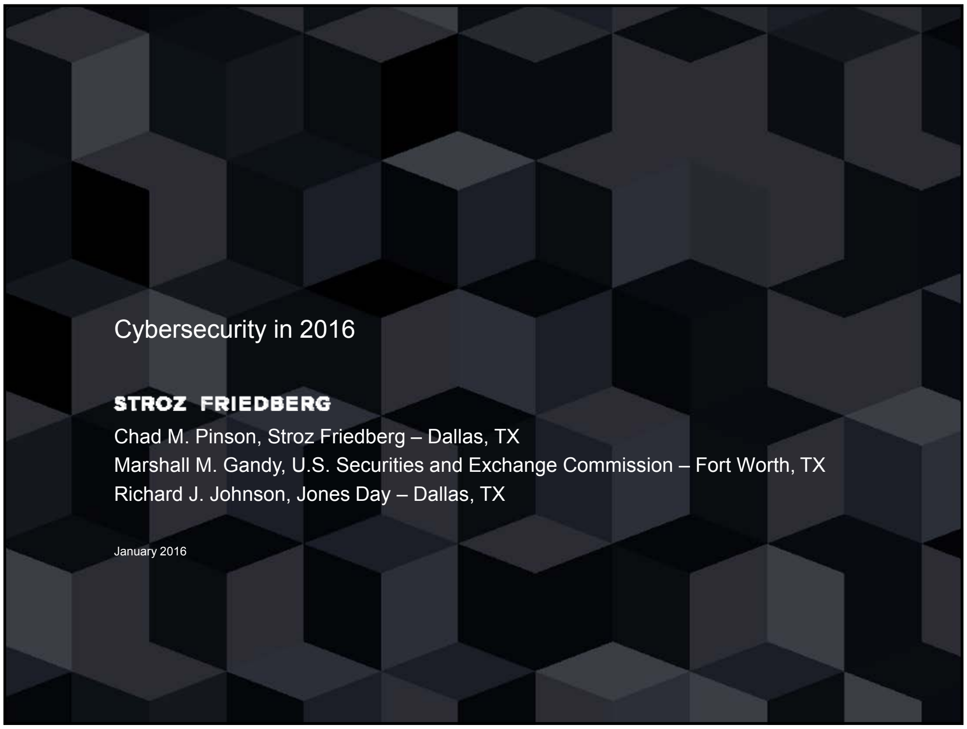
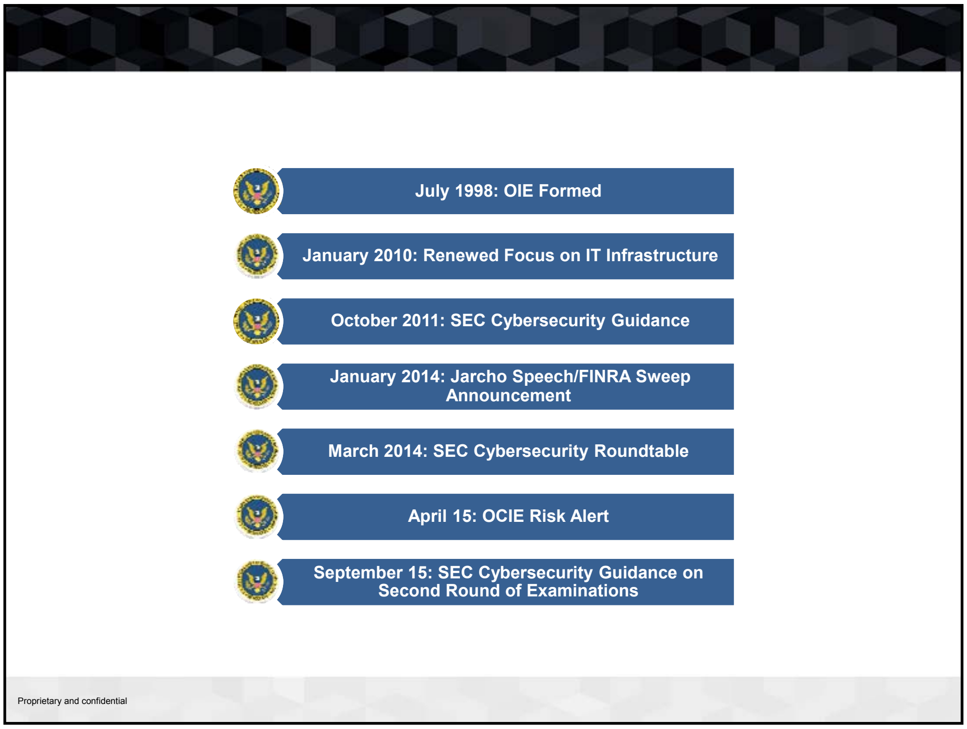


Cybersecurity in 2016

STROZ FRIEDBERG

Chad M. Pinson, Stroz Friedberg – Dallas, TX
Marshall M. Gandy, U.S. Securities and Exchange Commission – Fort Worth, TX
Richard J. Johnson, Jones Day – Dallas, TX

January 2016

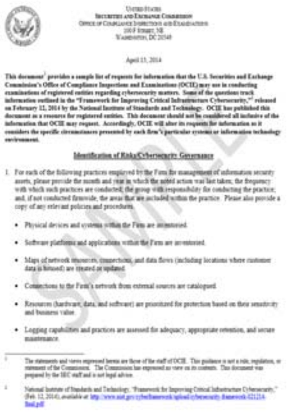


- July 1998: OIE Formed
- January 2010: Renewed Focus on IT Infrastructure
- October 2011: SEC Cybersecurity Guidance
- January 2014: Jarcho Speech/FINRA Sweep Announcement
- March 2014: SEC Cybersecurity Roundtable
- April 15: OCIE Risk Alert
- September 15: SEC Cybersecurity Guidance on Second Round of Examinations

REGULATION S-P “The Safeguard Rule”

- Applies To SEC Registered Broker-dealers And Investment Advisers
- Ensure The Security And Confidentiality Of Customer Records And Information
- Protect Against Any Anticipated Threats Or Hazards To The Security Or Integrity Of Customer Re- cords And Information; And
- Protect Against Unauthorized Access To Or Use Of Customer Records Or Information That Could Result In Substantial Harm Or Inconvenience To Any Customer

Compliance Inspection



United States
Securities and Exchange Commission
Office of Compliance Inspections and Examinations
100 F Street, NE
Washington, DC 20549

April 15, 2014

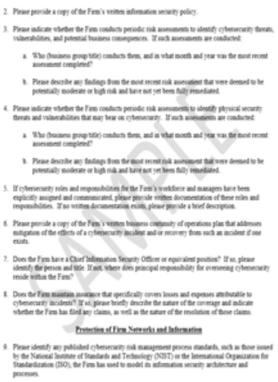
This document[1] provides a sample list of requests for information that the U.S. Securities and Exchange Commission's Office of Compliance Inspections and Examinations (OCIE) may use in conducting examinations of registered entities regarding cybersecurity matters. Some of the questions track information outlined in the "Framework for Improving Critical Infrastructure Cybersecurity,"[2] released on February 12, 2014 by the National Institute of Standards and Technology. OCIE has published this document as a resource for registered entities. This document should not be considered all inclusive of the information that OCIE may request. Accordingly, OCIE will alter its requests for information as it considers the specific circumstances presented by each firm's particular systems or information technology environment.

Identification of Risks/Cybersecurity Governance

1. For each of the following practices employed by the Firm for management of information security assets, please provide the month and year in which the noted action was last taken; the frequency with which such practices are conducted; the group with responsibility for conducting the practice; and, if not conducted firmwide, the areas that are included within the practice. Please also provide a copy of any relevant policies and procedures.
   - Physical devices and systems within the Firm are inventoried.
   - Software platforms and applications within the Firm are inventoried.
   - Maps of network resources, connections, and data flows (including locations where customer data is housed) are created or updated.
   - Connections to the Firm's network from external sources are catalogued.
   - Resources (hardware, data, and software) are prioritized for protection based on their sensitivity and business value.
   - Logging capabilities and practices are assessed for adequacy, appropriate retention, and secure maintenance.

[1] The statements and views expressed herein are those of the staff of OCIE. This guidance is not a rule, regulation, or statement of the Commission. The Commission has expressed no view on its contents. This document was prepared by the SEC staff and is not legal advice.

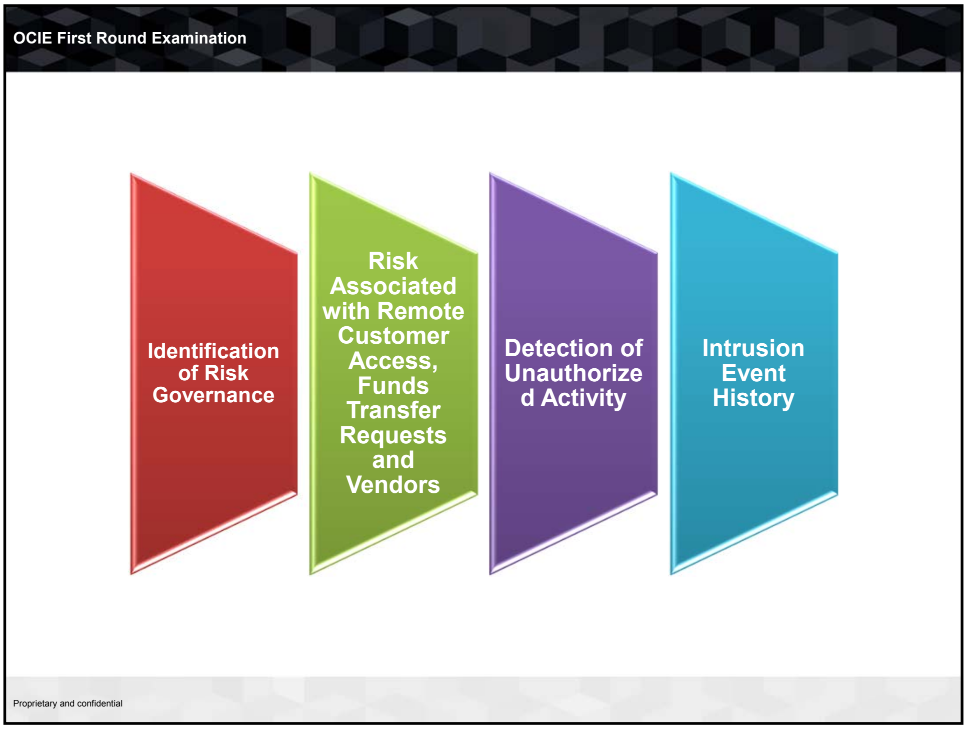
[2] National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity," (Feb. 12, 2014), available at http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf



2. Please provide a copy of the Firm's written information security policy.
3. Please indicate whether the Firm conducts periodic risk assessments to identify cybersecurity threats, vulnerabilities, and potential business consequences. If such assessments are conducted:
   a. Who (business group/title) conducts them, and in what month and year was the most recent assessment completed?
   b. Please describe any findings from the most recent risk assessment that were deemed to be potentially moderate or high risk and have not yet been fully remediated.
4. Please indicate whether the Firm conducts periodic risk assessments to identify physical security threats and vulnerabilities that may bear on cybersecurity. If such assessments are conducted:
   a. Who (business group/title) conducts them, and in what month and year was the most recent assessment completed?
   b. Please describe any findings from the most recent risk assessment that were deemed to be potentially moderate or high risk and have not yet been fully remediated.
5. If cybersecurity roles and responsibilities for the Firm's workforce and managers have been explicitly assigned and communicated, please provide written documentation of these roles and responsibilities. If no written documentation exists, please provide a brief description.
6. Please provide a copy of the Firm's written business continuity of operations plan that addresses mitigation of the effects of a cybersecurity incident and/or recovery from such an incident if one exists.
7. Does the Firm have a Chief Information Security Officer or equivalent position? If so, please identify the person and title. If not, where does principal responsibility for overseeing cybersecurity reside within the Firm?
8. Does the Firm maintain insurance that specifically covers losses and expenses attributable to cybersecurity incidents? If so, please briefly describe the nature of the coverage and indicate whether the Firm has filed any claims, as well as the nature of the resolution of those claims.

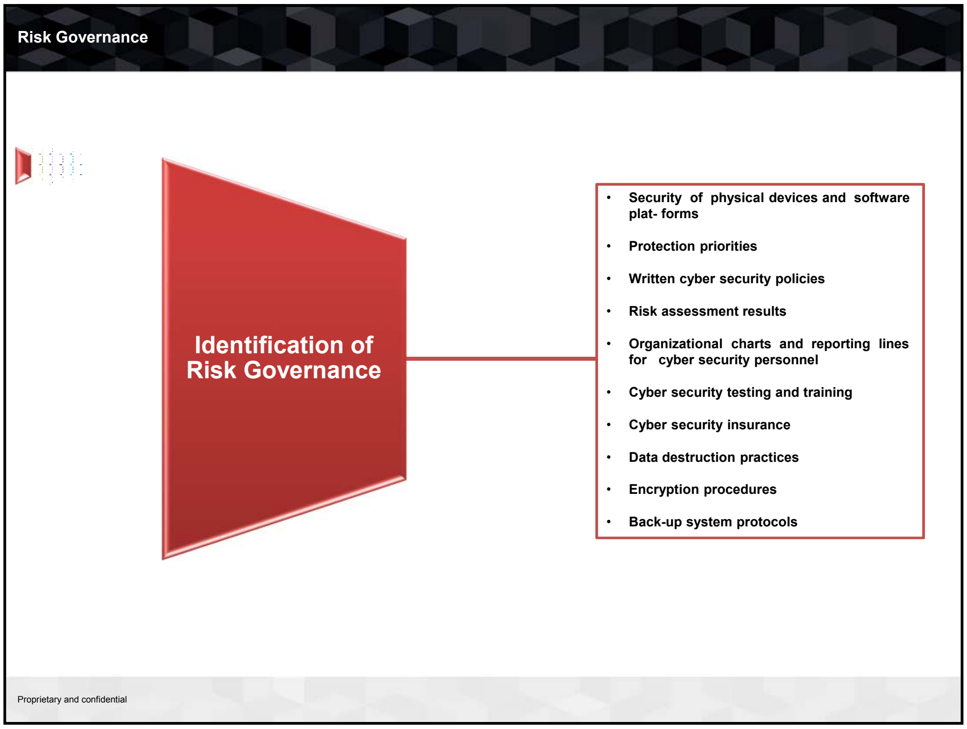
Protection of Firm Networks and Information

9. Please identify any published cybersecurity risk management process standards, such as those issued by the National Institute of Standards and Technology (NIST) or the International Organization for Standardization (ISO), the Firm has used to model its information security architecture and processes.



OCIE First Round Examination

- Identification of Risk Governance
- Risk Associated with Remote Customer Access, Funds Transfer Requests and Vendors
- Detection of Unauthorized Activity
- Intrusion Event History



Risk Governance

Identification of Risk Governance

- Security of physical devices and software plat- forms
- Protection priorities
- Written cyber security policies
- Risk assessment results
- Organizational charts and reporting lines for cyber security personnel
- Cyber security testing and training
- Cyber security insurance
- Data destruction practices
- Encryption procedures
- Back-up system protocols