RECENT REGULATORY DEVELOPMENTS REGARDING CYBERSECURITY:

WHAT FINANCIAL INSTITUTIONS NEED TO KNOW

Presented to the:

Cyber Security Council

Association of Institutional Investors

February 23, 2016

Dechert LLP

Today’s Presenter

Hilary Bonaccorsi
Associate, Dechert LLP

Boston

hilary.bonaccorsi@dechert.com

+1 617 728 7153

Overview

- Regulatory Updates:
  - Securities and Exchange Commission (“SEC”)
    - Registered Advisers, Broker-Dealers and Investment Companies
    - Federal Trade Commission (“FTC”) has authority over non-registered entities
    - What Will the SEC Really Want to Know in an Examination?
  - National Futures Association (“NFA”)
    - CPOs, CTAs, introducing brokers, future commission merchants, swap dealers
  - Financial Industry Regulation Authority (“FINRA”)
    - Broker-Dealers
- Industry Considerations:
  - Vendor Management
  - Incident Response Plans
  - Data Breach Reporting

Regulatory Updates: SEC

SEC: Recent Developments - Overview

- April 2014: SEC Issues Risk Alert – Staff to Inspect 50 Registered Entities with Regard to Cybersecurity Practices
- February 2015: SEC Issues Cybersecurity Examination Sweep Summary
- April 2015: SEC Division of Investment Management Issues Cybersecurity Guidance
- September 2015: SEC Issues Risk Alert – OCIE's 2015 Cybersecurity Examination Initiative
- September 2015: SEC Charges Investment Adviser with Failing to Adopt Proper Cybersecurity Policies and Procedures Prior to Breach

April 2014: SEC Risk Alert: Staff To Inspect 50 Registered Entities With Regard to Cybersecurity Practices

- OCIE's sample set of examination inquiries focused on a firm's ability to:

  (i) identify its own cybersecurity risks;

  (ii) protect its networks;

  (iii) ensure secure remote access and transfer requests;

  (iv) safeguard client information from third parties (including those who have been granted access, such as vendors and business partners);

  (v) detect unauthorized activity;

  (vi) recover from an adverse cybersecurity event;

  (vii) appropriately monitor and respond to new cybersecurity regulations; and

  (viii) adapt to the evolving cybersecurity landscape by determining its own set of best practices.

February 2015: SEC Summarizes Results of First Cybersecurity Examination Sweep

- The Alert summarizes the results of OCIE's 2014 Cybersecurity Examination Sweep

- Key Takeaway: Broker-dealers are significantly more prepared to deal with a cyber-incident than investment advisers

  - Vast majority of firms had adopted ***written information security programs***, but 82% of broker-dealers discussed how to mitigate the effects of a cyber-incident, compared to 51% of investment advisers

  - 72% of broker-dealers incorporate cyber-risk requirements into their ***contracts with vendors***, versus only 24% of investment advisers

  - 68% of broker-dealers had appointed a ***Chief Information Security Officer*** ("CISO") as compared to 30% of investment advisers

April 2015: SEC Division of Investment Management Issues Cybersecurity Guidance

- The May 2015 IM Guidance sets forth a step-by-step process for firms to use when addressing their cybersecurity risks, which includes:
  - ***Conducting a periodic assessment*** of vulnerabilities and current practices
  - ***Creating a strategy*** to prevent, detect and respond to cyber threats
  - ***Implementing the strategy*** developed via self-assessments
- The Division of Investment Management touched on "new" areas in the 2015 Guidance, which included:
  - An emphasis on "periodic testing" of strategies
  - A recommendation to consider the entity's entire corporate network during an assessment

September 2015: OCIE Issues 2015 Cybersecurity Examination Initiative Risk Alert

- **Key Takeaway:** Unlike OCIE's 2014 Cybersecurity Examination Initiative, OCIE's 2015 Cybersecurity Examination Initiative will focus on whether firms are actually implementing the policies and procedures they have adopted.

  - "The staff's document reviews and questions were designed to discern basic distinctions among the level of preparedness of the examined firms. ***The staff conducted limited testing of the accuracy of the responses and the extent to which firms' policies and procedures were implemented***. The examinations did not include reviews of technical sufficiency of the firms' programs."

    OCIE's Cybersecurity Examination Sweep Summary – February 2015

  - "OCIE is issuing this Risk Alert to provide additional information on the areas of focus for OCIE's second round of cybersecurity examinations, which will ***involve more testing to assess implementation of firm procedures and controls***."

    OCIE's 2015 Cybersecurity Examination Initiative – September 2015

September 2015: OCIE Issues 2015 Cybersecurity Examination Initiative Risk Alert

- **Key Takeaway:** OCIE has indicated that in its 2015 Cybersecurity Examination Initiative, it will drill-down on the specific technical controls firms have in place to protect customer information.
  - "Firms may be particularly ***at risk of a data breach from a failure to implement basic controls*** to prevent unauthorized access to systems or information, such as multifactor authentication or updating access rights based on personnel or system changes."

    OCIE's 2015 Cybersecurity Examination Initiative – September 2015

  - "Examiners may review how firms control access to various systems and data via management of user credentials, authentication and authorization methods. This may include a ***review of controls associated with remote access, customer logins, passwords, firm protocols to address customer login problems, network segmentation, and tiered access***."

    OCIE's 2015 Cybersecurity Examination Initiative – September 2015

  - OCIE may ***request firms' policies and procedures relating to "patch management practices***, including those regarding the prompt installation of critical patches and the documentation evidencing such actions."

    OCIE's 2015 Cybersecurity Examination Initiative – September 2015

September 2015: OCIE Issues 2015 Cybersecurity Examination Initiative Risk Alert

- **Key Takeaway:** OCIE's 2015 Cybersecurity Examination Initiative Risk Alert demonstrates an increased focus on "Vendor Management"

- "Some of the largest data breaches over the last few years may have resulted from the hacking of third party vendor platforms. As a result, examiners may focus on firm practices and controls related to vendor management, such as due diligence with regard to vendor selection, monitoring and oversight of vendors, and contract terms. Examiners may assess how vendor relationships are considered as part of the firm's ongoing risk assessment process as well as how the firm determines the appropriate level of due diligence to conduct on a vendor."

  OCIE's 2015 Cybersecurity Examination Initiative – September 2015

- This focus on vendor management is particularly interesting due to the following findings reported by OCIE in February 2015:

  - "The vast majority of examined firms conduct periodic risk assessments, on a firm-wide basis, to identify cybersecurity threats, vulnerabilities and potential business consequences***. Fewer firms apply these requirements to their vendors***. A majority of broker-dealers (84%) and ***a third of the advisers (32%) require cybersecurity risk assessments of vendors with access to their firms' networks***."

    OCIE's Cybersecurity Examination Sweep Summary – February 2015

September 2015: SEC Charges Investment Adviser with Failing to Adopt Proper Cybersecurity Policies and Procedures Prior to Breach

- SEC released an Order regarding a $75K settlement with R. T. Jones in connection with its alleged violation of Rule 30(a) of Regulation S-P (the “Safeguards Rule”).
- **Alleged Facts:**
  - For approximately 4 years, R. T. Jones—an SEC-registered investment adviser with 8,400 client accounts and $480 million in assets under management–stored sensitive personally identifiable information (“PII”) of clients and other persons on its third party-hosted web server.
  - R.T. Jones did not adopt written policies and procedures regarding the security and confidentiality of that information and the protection of that information from anticipated threats or unauthorized access.
  - In July 2013, the firm’s web server was hacked and the PII over more than 100,000 individuals, including thousands of R.T. Jones’s clients, was left vulnerable to theft.
  - R.T Jones retained more than one cybersecurity consulting firm to confirm and assess the attack. Neither could confirm whether the PII stored on the server had been accessed or compromised.
  - R.T. Jones notified the affected individuals and provided free identity monitoring.
  - At the time of the Order, there was no indication that any client has suffered actual financial harm as a result of the breach.
- **SEC Findings:**
  - R.T. Jones failed to adopt any written policies and procedures reasonably designed to safeguard its clients’ PII as required by the Safeguards Rule. R. T. Jones’s policies and procedures did not include, for example:
    - Conducting periodic risk assessments;
    - Employing a firewall to protect the web server containing client PII;
    - Establishing procedures to respond to a cybersecurity incident; or
    - Encrypting client PII.

What Will the SEC Really Want to Know in an Examination of Asset Managers, Investment Advisers, Custodian Banks, or Broker Dealers?

1. Do you truly understand your firm's cybersecurity infrastructure?

2. Have you enacted policies and internal procedures specifically tailored to your risks?

3. Can you prove - - with documents - - that you adhere to and enforce your own policies?

4. Can you detect - - in real time - - any unlawful access to your firm's data networks?

5. Are you actively monitoring and minimizing the risks associated with your third party vendors and service providers?

Regulatory Updates: FINRA

February 2015: FINRA Issues Report on Cyber Practices

- Provides a detailed account of its observations as well as tools to assist firms in preparing for a cyber attack.

- Key Points:
  - Have a strong governance framework with board & senior-level engagement
  - Conduct risk assessments
  - Understand your data flows and having tailored technical controls
  - Develop, implement and test incident response plans
  - Conduct vendor due diligence and manage threats posed by vendors
  - Train your staff effectively and frequently
  - Take advantage of intelligence-sharing opportunities

Regulatory Updates: NFA

October 2015: NFA Issues Cybersecurity Guidance

- NFA adopted an "Interpretive Notice to NFA Compliance Rules 2-9, 2-36 and 2-49: "Information Systems Security Programs," requiring each NFA Member to adopt an ISSP by March 1, 2016.

- **NFA's Five Guidelines for Information Systems Security Program**
  - **1: Adopt and Enforce a Written Program**
    - Approved by an executive-level official
    - Use a formal process to develop an appropriately tailored ISSP
  - **2: Security and Risk Analysis**
    - Assess and prioritize the risks associated with the use of IT systems
    - Inventory information, estimate the severity of threats, consider past incidents
  - **3: Deployment of Protective Measures Against Identified Threats & Vulnerabilities**
    - Document and describe safeguards deployed to meet threats
  - **4: Response and Recovery from Events That Threaten the Security of Electronic Systems**
    - Create an Incident Response Plan
  - **5: Employee Training**
    - Implement ongoing education and training throughout employment

Industry Considerations: Incident Response Plans

Industry Considerations: Incident Response Plans

- An incident response plan details, in writing, a concrete plan for what a company will do if it faces a suspected or actual data breach or cyber-attack. The plan should, at a minimum:
  - Identify the company's most vulnerable data;
  - Assign responsibility for each element of the response plan and provide 24-hour contact information for all personnel and back-up personnel, including a rapid response team
  - Explain how to determine whether an incident is actually a breach and whether and how it should be escalated;
  - Indicate that data should be preserved so a forensic investigation can be conducted;
  - Identify who will keep logs and records of all information relating to the incident; and
  - Include procedures for notifying law enforcement and criteria for whether customers or third-parties need to be notified.
- Incident response plans should be tested
  - Personnel need to be trained and know how to respond to a data breach or cyber-attack.

Industry Considerations: Vendor Management

Industry Considerations: Vendor Management

- Conduct due diligence with regard to vendor selection
- Hold vendors and service providers to the same legal standard
- Require vendors and service providers to provide notice of information security breaches
- Supervise and monitor vendors' and service providers' compliance

Industry Considerations: Vendor Management

Holding Service Providers to the Same Legal Standard

- Consider that service providers may not be subject to the relevant laws

- Contractor acknowledges that (1) Bank is subject to the consumer and customer privacy provisions of the Gramm Leach Bliley Act and Federal regulations that implement the Act (the "Regulation"); (2) the Confidential Information covered by this Agreement may include Non-Public Personal Information as defined in the Regulation; and (3) that Bank has certain obligations to protect the Confidential Information from unauthorized disclosure to third parties. Contractor understands that Contractor's willingness and ability to cooperate with and assist Bank in this regard is a material factor in Bank's willingness to enter into this Agreement, and such other agreements as Bank may enter into, or have entered into, with Contractor, through which agreements Confidential Information will be released from Bank to Contractor

- Contractor acknowledges receipt from Bank of a copy of the Gramm-Leach-Bliley Act and acknowledges that it has access to all applicable rules and regulations promulgated thereunder, and warrants that its procedures with regard to preventing release of Confidential Information are such as to be fully compliant with the Regulation as if Contractor were fully subject to the Regulation to the same extent as Bank

Industry Considerations: Vendor Management
Establishing Information Security Standards

- Service provider may have different security standards

- Specifically, and not by way of limitation, Contractor shall: (1) maintain Confidential Information of Bank in physical and electronically secure media and facilities, subject to commercially reasonable security procedures; (2) not use, nor permit its employees, agents, subcontractors or affiliates to use, such Confidential Information for any purpose whatsoever except strictly in connection with performance of its contractual duties to Bank; (3) neither use, nor permit use of, such data for any sales or marketing purposes; (4) make and enforce policies and procedures in hiring, training, supervision and monitoring of its staff, agents and subcontractors in proper handling and protection of Confidential Information, including, at a minimum and not by way of limitation, written agreements for confidentiality to be signed personally by all such parties, training, and provision for disciplinary action where appropriate; and (5) not copy, nor permit copying of, the Confidential Information, in any manner, or in any medium, whatsoever, and return all such data immediately upon completion of the task for which it was received, or with Bank's prior written approval, certify destruction of such data in writing

Industry Considerations: Vendor Management
Requiring Notice of Data Breaches

- Require service providers to provide notice of data breaches

- **Notice of Security Breach.** If a party to this Agreement becomes aware of any actual or suspected loss of, unauthorized access to, or unauthorized use or disclosure of any Confidential Information of the other party, including any Personal Information covered by this Agreement, such party promptly shall, at its expense: (a) notify the other party in writing; (b) investigate the circumstances relating to such actual or suspected loss or unauthorized access, use or disclosure; (c) take commercially reasonable steps to mitigate the effects of such loss or unauthorized access, use or disclosure and to prevent any reoccurrence; (d) provide to the Owner such information regarding such loss or unauthorized access, use or disclosure as is reasonably required for the Owner to evaluate the likely consequences and any regulatory or legal requirements arising out of such loss or unauthorized access, use or disclosure; and (e) cooperate with the Owner to further comply with all relevant laws, rules and regulations

Industry Considerations: Data Breach Reporting

Industry Considerations: Data Breach Reporting

- 46 states + D.C. have data breach notification laws.
- Generally, a company must notify the affected consumer when there is a “breach of security.”
- A “breach of security” is ordinarily defined as “an unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information.”
- Each state law is different, and therefore you must analyze each statute to ensure compliance.

Industry Considerations: Data Breach Reporting

Differences in State Data Breach Notification Laws

1. Definition of “Personal Information”
2. What is a “triggering event” (numerical thresholds, risk calculation)
3. Timing of notice (“following discovery”, no later than “10 days”, “as soon as practical”)
4. Content of notice
5. Recipients of notice (agencies, individuals, data “owners”)
6. Means of notice (who sends?)
7. Penalties, private right of action

Industry Considerations: Data Breach Reporting

- Faced with a patchwork of 47 state data breach notification laws (plus the District of Columbia) members of Congress have put forth at least 10 federal data breach reporting bills to streamline the process.

- The bills that have received the most attention include:
  - The Data Security and Breach Notification Act of 2015 (“Blackburn Bill”)
    - Introduced by House Representative Marsha Blackburn April 2015
    - Referred to the Subcommittee on Commerce, Manufacturing, and Trade April 2015
  - The Personal Data Notification and Protection Act of 2015 (“Obama Bill”)
    - Proposed by the White House, introduced by Representative James Langevin March 2015
    - Referred to the Subcommittee on the Constitution and Civil Justice April 2015
  - Consumer Privacy Protection Act (“Leahy Bill”)
    - Introduced by Senator Patrick Leahy April 2015
    - Referred to the Committee on the Judiciary April 2015
  - The Data Security Act (“Neugebauer Bill”)
    - Introduced by House Representative Randy Neugebauer
    - Approved by the Committee on Financial Services December 2015

Industry Considerations: Data Breach Reporting

- How are the proposed bills similar?
  - All contemplate a single federal statute to govern data breach reporting
- How are the proposed bills different?
  - The Blackburn Bill would:
    - Trigger a notification requirement for fewer types of personal information than most existing state laws (and would preempt state law)
    - Require companies to notify consumers only if they determine there is a "reasonable risk" of "identity theft, economic loss or economic harm, or financial fraud"
  - The Obama Bill would:
    - Target only businesses that work with the personal information of over 10,000 customers over a 12-month timeframe
    - Define "personal information" more broadly to include, for example, unique biometric data and account identifiers
  - The Leahy Bill would:
    - Require disclosure for breaches that impact social networks and cloud email services
    - Create seven new categories of "protected information," including health information, geolocation data, and password-protected private videos and photos
  - The Neugebauer Bill would:
    - Create a single, consistent minimum standard for data security as well as for breach notification
    - Only require notification if the breach was reasonably likely to cause substantial harm
    - Contemplate what to do in case of a third-party service provider breach