Thunder and lightning in those i-clouds!
Today's "storm" forecast

- Cybersecurity risks
- Related regulations
  - Privacy and safeguarding rules
  - Identity theft "red flags" rules
  - State breach notification laws
  - Business continuity preparedness
  - Books and records - insider trading
- Readiness - resources
  - Getting started
  - NIST framework
Cybersecurity risks

- Threats come in all sizes - "CHEW"
  - Criminals - organized and petty
  - "Hacktivists" - "Occupy Wall Street"
  - Espionage - foreign governments
  - War - terrorists - foreign governments
- Payment systems - credit card theft
- Data theft => Identity theft =>
  - Unauthorized account access
  - Unauthorized account orders
  - Email "impersonations"
Cybersecurity risks

Staples, J.P. Morgan Chase, Home Depot, Target - 500+ million records YTD in 2014 alone

Verizon report - top cyber risks -
- Point-of-sale intrusions
- Card "skimmers"
- Web app attacks
- Insider and privilege misuse
- Crimeware
- Denial of service
- Cyber-espionage
Cybersecurity risks

Electronic devices -
- Computers, laptops, tablets, wireless
- Smartphones

Electronic data storage -
- "i-Clouds"
- Archives and back-ups
- Flash drives

Electronic data transmission -
- Internet connectivity
- Wireless connectivity
Cybersecurity risks

- Potential "participants" -
  - Unwitting or disgruntled clients
  - Unwitting/disgruntled employees/reps
  - Eees/reps with "issues" (drugs, alcohol, gambling)
  - Former/competing Eees/reps
  - Dishonest family members - all "camps"
  - Disgruntled - dishonest service vendors
  - Flawed third-party's software/systems
  - Cyber criminals - domestic and foreign
Cybersecurity risks

- Symantec (anti-virus software vendor)
  - 30% attacks <= 250 Employees (2013)
  - 31% attacks <= 250 Employees (2012)

- Symantec's "Top 10 Targets"
  - Real names, birth dates, email addresses
  - Home address, telephone numbers
  - User names and passwords
  - Government ID - Social Security #s
  - Medical records
  - Financial information
  - Insurance
Cybersecurity risks

- Symantec 2013 data highlights -
  - 91% increase in targeted campaigns
  - 62% increase the number of breaches
  - 552M+ identities exposed
  - 23 "zero-day" software vulnerabilities
  - A software hole unknown to the vendor and exploited by hackers until discovered
  - E.g., the "Heartbleed Bug"
  - 38% of mobile users experienced mobile cybercrime in past 12 months
Cybersecurity risks

- Symantec 2013 data highlights -
  - Spam volume - 66% of all email traffic
  - 1 in 392 emails are phishing attacks
  - Targeted "spear phishing" attacks
    - Spurious internal-appearing emails targeted to employees requesting info
  - Web-based attacks are up 23%
  - 1 in 8 legitimate websites have a critical vulnerability
Cybersecurity risks

- NASAA 2014 study (440 state-registered IAs)
  - 47% had <= $25 million in AUM
  - 4.1% had a cybersecurity "incident"
  - 1.1% had theft, loss, exposure, access
  - 50% use unsecured email
  - 43% accept email instructions but lacked ID verification procedures
  - 23% lacked cyber/tech policies/training
Cybersecurity risks

- SEC 2014 Cybersecurity Roundtable
- OCIE and FINRA cyber sweeps
- SEC case example (2014 OCIE Bowden speech)
  - Good client service - weak controls
  - Permitted pre-signed transfer LoA's
  - Retained client logins and passwords
  - Hacker gained control client’s email
  - Hacker emailed wire instructions
  - Firm failed to verify authenticity
  - Money gone
Related regulations

- Privacy and safeguarding rules
  - SEC's Regulation S-P, *Privacy of Consumer Financial Information*
    - Applies to SEC registrants
  - FTC's *Privacy of Consumer Financial Information* rules
    - Applies to state-registered IAs
  - State insurance privacy law and rules
Related regulations

SEC's "safeguarding rule" requires

- Written policies and procedures “reasonably designed” to:
  - Insure the security and confidentiality of customer records and information
  - Protect against any anticipated threats or hazards to the security or integrity of customer records and information
  - Protect against unauthorized access or use of customer records or information

SEC 2008 proposed amendments never adopted - less rigorous than FTC's rule
Related regulations

- FTC's "safeguarding" rule requires
  - An "information security program"
  - Program must be "comprehensive"
    - Designate an employee coordinator(s)
    - Identify reasonably foreseeable internal and external risks affecting -
      - Data security, confidentiality, and integrity
      - Unauthorized disclosure, misuse, alteration, destruction or compromise
  - Sufficiency of your safeguards
Related regulations

- FTC's program must address -
  - Employee training and management;
  - Information systems, including network and software design, as well as information processing, storage, transmission and disposal
  - Detecting, preventing and responding to attacks, intrusions, or systems failures
- FTC has enforcement power but does not examine for compliance
- States could make referrals to FTC
Related regulations

- State safeguarding laws -
  - Insurance companies and producers
    - Model state privacy/safeguarding rule
  - Massachusetts rule - any MA clients
- Specialty state privacy-related laws -
  - E.g., truncating Social Security numbers
Related regulations

- Identity theft "red flags" rules
  - SEC Regulation S-ID, *Duties Regarding the Detection, Prevention, and Mitigation of Identity Theft*
    - Applies to SEC registrants
    - Broad interpretation about its application
  - FTC's rule is comparable but generic
    - Applies to all other "financial institutions" not regulated by SEC, CFTC, or federal bank regulators
    - Application to state-RIAs is less clear
Related regulations

- Red Flags rules require an identity theft prevention program -
  - Written policies and procedures -
  - Tailored to size, complexity, activities
  - Designed to detect, prevent, and mitigate identity theft relating to
    - Opening, maintaining, or holding a "covered account" (deposits/withdrawals)
  - SEC includes power to initiate transfers to third-parties (e.g., direct a custodian)
  - FTC guidance is silent on this point
Related regulations

- Program elements - "reasonable" policies/procedures to:
  - Identify relevant red flags
  - Detect those red flags
  - Respond - protect against and mitigate
  - Periodically update program

- Red Flags Rules' appendices have helpful guidance and examples
Related regulations

- "Reasonableness" standards evolving
- SEC/OCIE - FINRA sweep reports coming
  - The "good", "bad", and "ugly"
- SEC/OCIE and FINRA exam experience
  - Exam alerts are likely to be issued
- State exam experience - NASAA reports
  - Standards will be driven by -
    - Government - industry collaborations
    - National experience with cyber-disasters
    - More federal and state legislation
    - SEC-FINRA-FTC enforcement cases
Related regulations

- State breach notification laws
  - 47 state laws - requirements vary
    - Not specific to financial services industry
    - Home state and each client's state
    - No SEC rule - no federal preemption
    - Notify all affected clients in each state
    - Notify each state's designated authority

- State "security freeze" laws
  - 47 state laws - requirements vary
    - Consumers "freeze" their credit reports
    - Credit reporting companies charge fees
Related regulations

- Business continuity preparedness
- SEC Compliance Program Rule 206(4)-7
- State business continuity program rules
  - NASAA is developing a model BCP rule
- Address risks from cyber attacks -
  - Firm's own operations
  - Reliance on third-party operations
- Other relevant rules -
  - Books and records to be preserved
  - Steps to prevent "insider trading"
Readiness - self-assessment

Getting started -
- Muster an internal team - include
  - IT, operations, and compliance staff
  - Front-line and back-office staff
  - Senior management
- Identify gaps to fill (e.g., tech support)
- Assign responsibilities to learn more
- Identify a team coordinator
- Set realistic and attainable goals
- Keep good records of steps taken
Readiness - game planning

Cybersecurity planning
- Develop target timelines
- Set and update priorities
- Check out the NIST "Framework"
- Review the SEC/OCIE’s cybersecurity sweep document request list

Identity theft prevention planning
- See FINRA’s “red flags” template
- See the Red Flags Rules appendices
Readiness - internal threats

Start with some basics
- Budget more $$$$$ for cybersecurity
- Encrypt and password protect computers, laptops, wireless routers, mobile devices
- Encrypt emails, attachments, file transfers
- Control installation of new software
- Cover office, home, and mobile devices
- Install and update antivirus software
- Train employees on password practices
- Require ID verification for transfers and address changes - confirm changes
- Train employees about phishing scams
## Readiness - Internal Threats

### SIFMA Small Firm's Checklist

<table>
<thead>
<tr>
<th>Function</th>
<th>Summary Description</th>
</tr>
</thead>
</table>
| **Username and Password Protection** | Strictly enforce robust password security per NIST standards that include:  
- Upper and lower case letters, numbers, and symbols  
- A minimum of 8 characters, avoiding common words and dates  
- Password is not used for any other credential  
- Changing passwords regularly  
- Deploy multi-factor authentication |
| **Control Administrative and Privileged Access** | Restrict administrative and privileged access to systems and data through preventative and detective controls to prevent unauthorized access or alteration of systems and/or data. |
| **Application Whitelisting** | Allow only trusted software to execute on operating systems. Prevent the execution of all other software through the use of application whitelists. |
| **Anti-Virus, Email and Website Filters** | Updated anti-virus software, in addition to web security software, greatly reduces the risk of unintentional and intentional computer infection. Additionally, personal vigilance against suspicious emails and attachments greatly reduces cyber threats. |
### Readiness - internal threats

**SIFMA small firm's checklist**

<table>
<thead>
<tr>
<th>Secure Standard Operating Systems</th>
<th>Standardize on trusted operating systems that meet Common Criteria. Using unsupported or outdated operating systems, such as Windows XP, presents risks to the network and critical data.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automated Patching Tools and Processes</td>
<td>Utilize automatic software updates and spot-check that updates are applied frequently to ensure software currency and reduce the risks associated with out-of-date, vulnerable software.</td>
</tr>
<tr>
<td>Back Up Data Regularly</td>
<td>Investing in and using cloud or physical external hard-drive backup systems provides an additional level of security for important data in the event that information is destroyed.</td>
</tr>
<tr>
<td>Mobile Device Security and Encryption of Data</td>
<td>Ensure that mobile devices are secure with passwords and the data is encrypted in the event of loss.</td>
</tr>
</tbody>
</table>
Readiness - external threats

- Assess third-party providers
- Request their business continuity plans
- Request cybersecurity information
- Request CPA-issued SSAE 16 and service organization control reports
- Check vendor service contracts -
  - Your obligations - client obligations
  - Vendor warranty disclaimers
  - Vendor limitations of liability
Readiness - clients

- Educate clients -
  - Explain the risks and protective steps
    - Common types of cyber-crime
    - Management of passwords and user IDs
    - Installing anti-virus software and updates
  - Explain why ID verification is critical
  - Create a client ID theft response plan
Readiness - resources

National Institute of Standards and Technology (NIST)
  Framework for Improving Critical Infrastructure Cybersecurity
  Small Business Information Security: The Fundamentals

Securities Industry and Financial Markets Association (SIFMA)
  Guidance for Small Firms
  Small Firm Cybersecurity Checklist
Readiness - next steps

- Four important take-aways -
  - Read the WN&J cybersecurity article
  - Check out the related exhibits
  - Then . . .
    - Do something
    - Do it in writing
    - Do it now
Cybersecurity Risks, Regulation, and Resources

By: Shane B. Hansen, Partner
Carly Zagaroli, Associate
Warner Norcross & Judd LLP

Financial Planning Association of Michigan
2014 Fall Symposium
October 23, 2014

I. Overview

There is “thunder and lightning” in those “clouds”. The storm of cybersecurity attacks is rapidly intensifying and the forecasted impact on clients and the financial services firms who serve them is alarming. Stealing money is the ultimate objective, but these criminal enterprises have become more sophisticated and often involve domestic or foreign organized crime syndicates, foreign nationals and even foreign governments—no longer just techno-geeks and petty thieves. The lucrative black market in illegally stolen cyber data from “mass attacks” such as reported by J.P. Morgan Chase, Home Depot, and Target feeds the criminal activities of identity thieves around the globe. Entrepreneuring criminals buy and then use the stolen cyber data to prey upon other targets, such as smaller, “softer” financial services firms through unauthorized account access and client impersonations. Key areas of cyber vulnerability include remote access to client information, remote customer access to accounts, fund transfer requests, risks associated with third-party vendors, and detection of unauthorized activity.
Readiness - exhibits

By the Office of Compliance Inspections and Examinations

Volume IV, Issue 2

April 15, 2014

OCIE CYBERSECURITY INITIATIVE

I. Introduction

The U.S. Securities and Exchange Commission’s Office of Compliance Inspections and Examinations (OCIE) previously announced that its 2014 Examination Priorities included a focus on technology, including cybersecurity preparedness. OCIE is issuing this Risk Alert to provide additional information concerning its initiative to assess cybersecurity preparedness in the securities industry.

II. Background

On March 26, 2014, the SEC sponsored a Cybersecurity Roundtable. In opening the Roundtable, Chair Mary Jo White underscored the importance of this area to the integrity of our market system and customer data protection. Chair White also emphasized the “compelling need for stronger partnerships between the government and private sector” to address cyber threats. Commissioner Aguilar, who recommended holding a Cybersecurity Roundtable, emphasized the importance for the Commission to gather information and “consider what additional steps the Commission should take to address cyber-threats.”
Appendix

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

April 15, 2014

This document 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,” 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.
Compilation of Results of a Pilot Survey of Cybersecurity Practices of Small and Mid-Sized Investment Adviser Firms
Readiness - exhibits

SMALL FIRMS CYBERSECURITY GUIDANCE
HOW SMALL FIRMS CAN BETTER PROTECT THEIR BUSINESS
JULY 2014
Small Business Information Security: The Fundamentals

Richard Kissel
Framework for Improving Critical Infrastructure Cybersecurity

Version 1.0

National Institute of Standards and Technology

February 12, 2014
Readiness - exhibits

SEC Regulation S-ID, *Duties Regarding the Detection, Prevention, and Mitigation of Identity Theft*, Section 248.201

Click to open document in a browser.

(a) **Scope.** This section applies to a financial institution or creditor, as defined in the Fair Credit Reporting Act (15 U.S.C. 1681), that is:

1. A broker, dealer or any other person that is registered or required to be registered under the Securities Exchange Act of 1934;
2. An investment company that is registered or required to be registered under the Investment Company Act of 1940, that has elected to be regulated as a business development company under that Act, or that operates as an employees' securities company under that Act; or
3. An investment adviser that is registered or required to be registered under the Investment Advisers Act of 1940.

(b) **Definitions.** For purposes of this subpart, and Appendix A of this subpart, the following definitions apply:

1. **Account** means a continuing relationship established by a person with a financial institution or creditor to obtain a product or service for personal, family, household or business purposes. Account includes a brokerage account, a mutual fund account (i.e., an account with an open-end investment company), and an investment advisory account.

2. The term **board of directors** includes:
   
   (i) In the case of a branch or agency of a foreign financial institution or creditor, the managing official of that branch or agency; and
   
   (ii) In the case of a financial institution or creditor that does not have a board of directors, a designated employee at the level of senior management.
Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation

Section 248.201 requires each financial institution and creditor that offers or maintains one or more covered accounts, as defined in §248.201(b)(3), to develop and provide for the continued administration of a written Program to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account. These guidelines are intended to assist financial institutions and creditors in the formulation and maintenance of a Program that satisfies the requirements of §248.201.

I. The Program

In designing its Program, a financial institution or creditor may incorporate, as appropriate, its existing policies, procedures, and other arrangements that control reasonably foreseeable risks to customers or to the safety and soundness of the financial institution or creditor from identity theft.

II. Identifying Relevant Red Flags

(a) **Risk Factors.** A financial institution or creditor should consider the following factors in identifying relevant Red Flags for covered accounts, as appropriate:

1. The types of covered accounts it offers or maintains;
2. The methods it provides to open its covered accounts;
3. The methods it provides to access its covered accounts; and
4. Its previous experiences with identity theft.
Identity Theft Red Flags Rule Template

Important: If you choose to use this template as a guide, you must adapt it to reflect your individual firm. Without the analysis and modification required to fit your firm’s situation, your Identity Theft Prevention Program (ITPP) will not comply with regulatory requirements.

This template is an optional guide for firms to assist them in fulfilling their requirements under Securities and Exchange Commission (“SEC”) Regulation S-ID: Identity Theft Red Flags (“Red Flags Rule”), which requires specified firms to create a written Identity Theft Prevention Program (“ITPP”) designed to identify, detect and respond to “red flags”—patterns, practices or specific activities—that could indicate identity theft. Identity theft is a fraud committed or attempted using the identifying information of another person without authority.
I. Firm Policy

State your firm’s objectives for your ITPP.

TEXT EXAMPLE: Our firm’s policy is to protect our customers and their accounts from identity theft and to comply with the SEC’s Red Flags Rule. We will do this by developing and implementing this written ITPP, which is appropriate to our size and complexity, as well as the nature and scope of our activities. This ITPP addresses (1) identifying relevant identity theft red flags for our firm, (2) detecting those red flags, (3) responding appropriately to any that are detected to prevent and mitigate identity theft, and (4) updating our ITPP periodically to reflect changes in risks.

Our identity theft policies, procedures and internal controls will be reviewed and updated periodically to ensure they account for changes both in regulations and in our business.

Rule: 17 C.F.R. § 248.201(d)(1) and Appendix A, Section I.
Readiness - exhibits

SSEA 16 and the New Reporting Options

Janet P. Knaus, Kenneth A. Coleman

The Statement on Auditing Standards No. 70 (SAS 70) has been around for nearly 20 years. First released in 1992, it was the gold standard for assuring data center users that their data center was secure and operating under proper control systems. The problem with SAS 70, according to the American Institute of CPAs (AICPA), was that it focused only on internal controls over financial reporting. It was never designed to be used by service organizations that offer co-location, managed servers or cloud hosting services.

New Reporting Options

SOC 1 Reports: Under the new AICPA reporting standards, an audit conducted under SSAE 16 results in a SOC 1 report. This report, however, will still focus on internal controls over financial reporting. Overall, SOC 1 will be the basic form of reporting for SSAE 16 audits.

As with the old SAS 70, SOC 1 reports will be available as Type 1 or Type 2 reports:
Questions?