Small Firm Focus: A Practical Approach to Cybersecurity
Friday, May 29
9:00 a.m. – 10:15 a.m.

Topics:
- Explain why it is important for firms of all sizes to address cybersecurity risk.
- Demonstrate awareness of cybersecurity-related laws and regulations governing broker-dealers.
- Have knowledge of relevant cybersecurity risk management frameworks and standards.
- Know how to structure and implement a cybersecurity risk management program.
- Address critical risk items directly with proven control techniques.

Speakers:

John Brady (moderator)
Vice President and Chief Information Security Officer
FINRA Technology Administration

Allan Goldstein
Chief Compliance Officer, Chief Operating Officer and Chief Financial Officer
Trade Informatics LLC

Lisa Roth
President
Monahan & Roth, LLC

Hardeep Walia
Co-Founder & Chief Executive Officer
Motif Investing
Small Firm Focus: A Practical Approach to Cybersecurity

FINRA Annual Conference
May 29, 2015 • Washington, DC
Panelists

Moderator:
• John Brady, Vice President and Chief Information Security Officer, FINRA Technology Administration

Panelists:
• Allan Goldstein, Chief Compliance Officer, Chief Operating Officer and Chief Financial Officer, Trade Informatics LLC
• Lisa Roth, President, Monahan & Roth, LLC
• Hardeep Walia, Co-Founder & Chief Executive Officer, Motif Investing
Cyber Security – A Serious Matter

- Member firms (of all sizes) need to take cybersecurity seriously and address the threat.

- Headline events have captured the attention of our Customers and our Regulators:
  - Target, Home Depot, JP Morgan Chase, EBay, etc…
  - FINRA and SEC Enforcement Actions and Surveys
  - Wall Street Journal, Local and Regional Press

- $3.5 million / company*
  - 37% due to insufficient funding for IT**
  - 20% due to improper vetting of vendors
  - 44% involving malware
  - 24% involving compromised passwords

* Ponemon Institute, May 5th 2014
** Wall Street Journal, April 20th 2015
# Cyber Security Regulations and Laws

## Laws Directly Related to Cybersecurity
- Regulation S-P
- Fact Act
- State Laws

## Regulations Cited by Regulators in Cybersecurity Guidance, Examination Findings and Enforcement (in addition to the above)
- Supervision and Control
- Business Continuity
- Books and Records
- Written Procedures
Cyber Risk Framework and Standards

All Firms

- National Institute of Standards and Technology (“NIST”) Framework for Improving Critical Infrastructure Cybersecurity Version 1.0
- International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) Information Framework
- ISACA’s Control Objectives for Information and Related Technology (COBIT)

Small Firms

- NIST Small Business Corner
- FCC Cybersecurity for Small Business
- Trade Associations (SIFMA, FS-ISAC)
# NIST CSF & SANS Critical Controls

<table>
<thead>
<tr>
<th>NIST Cyber Security Framework</th>
<th>SANS Institute “Top 20” Critical Security Controls</th>
<th>Other Sound Practices</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Identify</strong></td>
<td>Inventory of Devices</td>
<td><strong>Identify high-risk business processes (e.g. outbound wire transfers)</strong></td>
</tr>
<tr>
<td>Asset Management</td>
<td>Inventory of Software</td>
<td></td>
</tr>
<tr>
<td>Business Environment</td>
<td>Vulnerability Assessment and Remediation</td>
<td></td>
</tr>
<tr>
<td>Governance</td>
<td>Application Software Security</td>
<td></td>
</tr>
<tr>
<td>Risk Assessment</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk Management Strategy</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Protect</strong></td>
<td>Secure Computer Configurations</td>
<td><strong>Add fraud detection steps to high-risk business processes</strong></td>
</tr>
<tr>
<td>Access Control</td>
<td>Secure Network Configurations</td>
<td></td>
</tr>
<tr>
<td>Awareness and Training</td>
<td>Malware Defenses</td>
<td></td>
</tr>
<tr>
<td>Data Security</td>
<td>Wireless Access Control</td>
<td></td>
</tr>
<tr>
<td>Information Protection</td>
<td>Security Skills Training</td>
<td></td>
</tr>
<tr>
<td>Processes and Procedures</td>
<td>Firewalling of Ports, Protocols, and Services</td>
<td></td>
</tr>
<tr>
<td>Maintenance</td>
<td>Controlled use of Administrator Privileges</td>
<td></td>
</tr>
<tr>
<td>Protective Technology</td>
<td>Boundary Defense</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Controlled Access Based on Need to Know</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Data Protection</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Secure Network Engineering</td>
<td></td>
</tr>
</tbody>
</table>

2015 FINRA Annual Conference • © 2015 FINRA. All rights reserved.
# NIST CSF & SANS Critical Controls

<table>
<thead>
<tr>
<th>NIST Cyber Security Framework</th>
<th>SANS Institute “Top 20” Critical Security Controls</th>
<th>Other Sound Practices</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Detect</strong></td>
<td>Anomalies and Events Security Continuous Monitoring Detection Processes</td>
<td>Maintenance, Monitoring and Analysis of Audit Logs <strong>Account Monitoring and Control</strong></td>
</tr>
<tr>
<td><strong>Respond</strong></td>
<td>Response Planning Communications Analysis Mitigation Improvements</td>
<td>Incident Response and Management <strong>Penetration Tests and Red Team Exercises</strong></td>
</tr>
<tr>
<td><strong>Recover</strong></td>
<td>Recovery Planning Improvements Communications</td>
<td><strong>Data Recovery Capability</strong></td>
</tr>
</tbody>
</table>
Recommendations

Build a Cybersecurity program patterned after FINRA’s Cybersecurity Report and NIST’s CSF:

- **Identify**
  - Establish a Cyber Security Officer or Designee
  - Conduct a Threat/Risk Assessment
    - External Vendor Assessment
    - Internal access control, BYOD, email
    - Client expectations
  - Create Policies & Procedures
    - Escalation & reporting
    - “Need to Have” access policy
    - Change of employment status
  - Staff Training

- **Protect**
  - Firewall (upgrade and patch)
  - Anti-virus, Anti-Spyware/malware
  - Webfilter Appliance
  - Laptop/portable device protections
  - Conduct 3rd party intrusion testing
  - Patch Management
  - Remote Desktop vs VPN
  - Clean screen/clean desk
  - Restrict workstation admin privileges
  - Cloud back-up
Recommendations (cont’d)

- **Detect**
  - Logging
  - Whistleblower program
  - Automated reporting
  - Email review
  - Awareness

- **Respond**
  - Classification of threats
  - Law enforcement, client notification, legal counsel, senior management, IT Security Team
  - Periodic review and test of response program

- **Recover**
  - Cyber insurance
  - Data restoration
  - Hardware restoration
WHERE TO START?
Physical Steps to “Just Go Do…”

- **Secure Electronic Equipment from Unauthorized Access:** Determine who and how by assessing the premises
- **Inventory Electronic Devices:** BYOD policies, Record type of equipment and % business/personal use
- **Identify Workable Contingency Operations:** leverage your business continuity plan for processes
- **Implement Temporary Guest Policies:** Badges, Log book, temporary pass keys
- **Establish Disposal Policies:** Understand and implement appropriate paper and electronic destruction methods
Technical Steps to “Just Go Do…”

- **Backup your data**: Best approach: a secure, cloud-based backup service
- **Install Anti-Virus**: You can start with free tools, however paid products have more features and capabilities
- **Apply Security Patches and Software Updates**: Most malware/viruses take advantage of missing patches to infect systems
- **Use Strong Passwords or Two Factor Authentication**: Best: two-factor authentication; 2nd best: a strong password generator and vault; change default passwords on devices and software; change passwords periodically
- **Secure your WiFi**: Enable encryption with an un-guessable passphrase
- **Use a Firewall**: Prevents unauthorized access to internal computers
- **Encrypt Laptops and Portable Storage Media**: Windows has built-in capability (called BitLocker)
Administrative Steps to “Just Go Do…”

- **Designate a Security POC:** And instruct all staff to report incidents and concerns to that person.

- **Guard High Risk Business Processes:** Identify risky business processes (e.g., outbound money transfers, customer service calls/email) and safeguard with fraud detection and verification steps.

- **Create Security Policies:** For Passwords, Use of Mobile Devices, etc.

- **Train Staff on Security Principles and your Policies:** Teach staff how to choose strong passwords, where customer data can and cannot be copied (e.g., prohibit putting sensitive data on mobile devices), etc.

- **Hire a Consultant To Test Your Security:** Penetration testing, vulnerability mapping, phishing testing/training.

- **Use Email and Web Security Services:** To reduce the volume of spam and lower the risk of viruses arriving via email or web browsing; Web Security services can also block access to inappropriate web content.
Resources

Resources, References, & Enforcement Actions
Regulatory Guidance

- **FINRA Report on Cybersecurity Practices (February 3, 2015)**

- **NIST Cyber Security Framework and Roadmap**

- **SEC National Exam Program Risk Alert (OCIE Cyber Security Initiative)**

- **SEC Cybersecurity Guidance Update (April 2015)**
Tips and Templates

- **FCC 10 Cyber Security Tips for Small Business**

- **FCC Small Biz Cyber Planner**
  - [http://www.fcc.gov/cyberplanner](http://www.fcc.gov/cyberplanner)

- **SIFMA Cybersecurity Guidance for Small Firms**

- **National Cyber Security Alliance – Mobile Tip Sheet**

- **Cyber Security in the Golden State (see “Practical Steps”)**
  - [https://oag.ca.gov/cybersecurity](https://oag.ca.gov/cybersecurity)

- **Verizon Data Breach Investigations Report**
SEC & FINRA Enforcement Actions

- **Re: Next Financial: Regulation SP violations related to RR recruiting**
  - Read more at: https://www.financialservices.org/uploadedFiles/FSI/Events/Web_Conferences/03NEXT_Financial_Summary.pdf

- **Re: Commonwealth Equity Services: Regarding mandatory anti-virus software on computers, computer audits, recordkeeping**
  - Read more at: https://www.sec.gov/litigation/admin/2009/34-60733.pdf

- **Re: Wells Investment Securities: A firm’s periodic audits were inadequate because they did not review laptops for security (FINRA case # 2009019893801)**
  - Read more at: http://disciplinaryactions.finra.org/

- **Re: Failure to Encrypt Sensitive Customer Data: Encryption failures including laptops (FINRA case # 2008015299801)**
  - Read more at: http://disciplinaryactions.finra.org/
SEC & FINRA Enforcement Actions

Regarding Security Policies and Procedures

- Recommendations or suggestions, rather than mandates.

- Inadequate controls to prevent account takeover and fraudulent ACH transfers. (FINRA case # 2012034190001)
  - Found at: http://disciplinaryactions.finra.org/

- Reviews of RR computer security measures.

- Response to cybersecurity issues detected through branch audits.
QUESTIONS?

THANK YOU!
Small Firm Focus: A Practical Approach to Cybersecurity
Friday, May 29
9:00 a.m. – 10:15 a.m.

Resources

Regulatory Guidance


- NIST Cyber Security Framework and Roadmap

- SEC National Exam Program Risk Alert (OCIE Cyber Security Initiative)

- SEC Cybersecurity Guidance Update (April 2015)

Tips and Templates

- FCC 10 Cyber Security Tips for Small Business

- FCC Small Biz Cyber Planner
  www.fcc.gov/cyberplanner

- SIFMA Cybersecurity Guidance for Small Firms

- National Cyber Security Alliance – Mobile Tip Sheet
  http://staysafeonline.org/stay-safe-online/resources/stc-mobile-tip-sheet
Cyber Security in the Golden State (see “Practical Steps”)
https://oag.ca.gov/cybersecurity

Verizon Data Breach Investigations Report
www.verizonenterprise.com/DBIR/

SEC and FINRA Enforcement Actions

- Next Financial: Regulation SP violations related to RR recruiting
  www.financialservices.org/uploadedFiles/FSI/Events/Web_Conferences/03NEXT_Financial_Summary.pdf

- Commonwealth Equity Services: Regarding mandatory anti-virus software on computers, computer audits, recordkeeping

- Wells Investment Securities: A firm’s periodic audits were inadequate because they did not review laptops for security (FINRA case # 2009019893801)
  http://disciplinaryactions.finra.org/Search/ViewDocument/25628

- Failure to Encrypt Sensitive Customer Data: Encryption failures including laptops (FINRA case # 2008015299801)
  http://disciplinaryactions.finra.org/Search/ViewDocument/37555

Securities Policies and Procedures

- Recommendations or suggestions, rather than mandates.
  www.sec.gov/litigation/admin/2008/34-58515.pdf

- Inadequate controls to prevent account takeover and fraudulent ACH transfers. (FINRA case # 2012034190001)
  http://disciplinaryactions.finra.org/Search/ViewDocument/38882

- Reviews of RR computer security measures.

- Response to cybersecurity issues detected through branch audits.