Financial Industry Regulatory Authority

South Region Compliance Seminar

New Orleans, LA | December 2 – 3, 2015

Cybersecurity: Understanding the Exposure
Thursday, December 3
11:00 a.m. – 12:00 p.m.

This session provides an overview of the latest cybersecurity threats firms' face and provides preventative measures firms can take to protect their business. Industry panelists and FINRA staff share effective practices to develop a cyber-risk program and steps to take to address cyber weaknesses. Panelists discuss real-life examples of cyber breaches and lessons learned from them.

Moderator:

David Kelley
Surveillance Director
FINRA Kansas City District Office

Panelists:

Mark Grosvenor
Chief Technology Officer
NFP Securities, Inc.

Christopher Longobucco
Regulatory Principal, Technology Control
FINRA Chicago District Office

Thomas Shaw
Vice President – Enterprise Financial Crimes Management
USAA

Cybersecurity: Understanding the Exposure Panelist Bios:

Moderator:

Dave Kelley is the Surveillance Director based out of their Kansas City District office, and has been with FINRA for more than five years. Mr. Kelley also leads FINRA's Regulatory Specialist team for Cyber Security, IT Controls and Privacy. Prior to joining FINRA, he worked for more than 19 years at American Century Investments in various positions, including Chief Privacy Officer, Director of IT Audit and Director of Electronic Commerce Controls. He led the development of website controls, including customer application security, ethical hacking programs and application controls. Mr. Kelley is a CPA and Certified Internal Auditor, and previously held the Series 7 and 24 licenses.

Panelists:

Mark Grosvenor joined NFP in January 2006 as Senior Vice President and advanced into his current role as Chief Technology Officer. Prior to joining NFP, he served as Vice President of Professional Services and Support at ResolutionEBS and Program Manager and Regional Delivery Lead at GTECH. Mr. Grosvenor holds a B.A. in Operations Management and Management Information Systems from Texas A&M University.

Chris Longobucco is presently Regulatory Principal, Technology Control from the FINRA Chicago District office where he is a member of a team of Technology professionals responsible for the continued development and implementation of the firm's Cybersecurity exam program over member firms. Mr. Longobucco has over twenty years of experience working with global financial service companies on Wall Street as a strategic business leader with a broad range of skills in Technology Operations, Governance, Risk, and Finance. While working in the financial services sector, he provided the strategic direction in leading large Technology and Finance operations' groups in delivering complex projects for global financial organizations; Investment Banking, Private Banking, Asset Management, Credit, Risk/Compliance, and Commodities. While in leading Technology positions he worked closely with the firm's regulators domestically and abroad. Prior to joining FINRA, he was with Morgan Stanley, as their Chief Operating Officer and Business Manager for their global Technology Risk and Enterprise Data Security organizations. Mr. Longobucco was responsible for developing and implementing best practices relating to operational and technology risk controls enterprise wide. Also, he spent a considerable amount of time leading the New York Mercantile Exchange's Technology operations group, and assisting the Exchange in going public in 2006, and instrumental in leading the development and implementation of three new exchanges, in Dubai, Dublin, and London. From 2009 to 2010, Mr. Longobucco worked with the company's newly merged entity, the Chicago Mercantile Exchange and was an integral participant in leading the integration of the two entity's systems operations and implementing an enterprise Technology governance program. Other financial firm experience was with Deutsche Bank and American Express where he lead enterprise wide re-organizations of the both the firm's Technology and IT Finance groups. Mr. Longobucco began his career with Arthur Andersen. Mr. Longobucco holds an undergraduate degree in Accounting and a master degree in Finance from Southern Methodist University.

Tom Shaw, Vice President of Enterprise Financial Crimes Management for USAA, has overall responsibility for fraud prevention, detection, recovery and investigations. He is also the Identity Theft Officer for USAA. Mr. Shaw has over 25 years' experience in the financial services industry with 16 years of this time at Bank of America. He currently serves as Chairman of the Board for the Association of Certified Fraud Examiner's Financial Foundation. He is a member of the MasterCard US Fraud Advisory Council and a member of the Visa North America Risk Executive Council. Mr. Shaw is a Certified Fraud Examiner (CFE) and a Certified Anti-Money Laundering Specialist (CAMS). He earned his MBA from Our Lady of the Lake University and his BS in International Economics from Texas Tech University.

South Region Compliance Seminar
December 2-3, 2015 | New Orleans, LA

Cybersecurity: Understanding the Exposure

FINRA

Panelists

Moderator:

- David Kelley, Surveillance Director, FINRA Kansas City District Office

Panelists:

- Mark Grosvenor, Chief Technology Officer, NFP Securities, Inc.
- Christopher Longobucco, Regulatory Principal, Technology Control, FINRA Chicago District Office
- Thomas Shaw, Vice President – Enterprise Financial Crimes Management, USAA

Outline

- FINRA's Definition of Cybersecurity
- Governance
- Risk Assessment
- Access Control
- Vendor Management
- Incident Response Plan
- Training
- Branch Controls
- Technical Measures
- Information Sharing

What do we mean by “Cybersecurity”?

- **In broad terms we mean the protection of investor and firm information from compromise through the use – in whole or in part – of electronic media (e.g., computers, cell phones, IP-based telephony systems).**
  - **“Compromise” refers to a loss of data confidentiality, integrity or availability**
  - **Protection of customer information and PII (Personal Identifiable Information)**
  - **Protection of firm confidential information**

Governance

- **Principle: Firms should establish Information Security governance frameworks that support informed decision-making and escalation at appropriate levels within the organization. This would include:**
  - **Active senior management and, as appropriate, board level oversight of cybersecurity**
  - **Articulated risk appetite that guides firm decision-making with respect to the acceptance, mitigation, avoidance or transfer of risks**
  - **Defined accountabilities, structures, policies and procedures to support decision-making based on risk appetite and industry effective practices**
  - **Use of appropriate metrics and thresholds**

Risk Assessment

- **Principle: Firms should conduct regular risk assessments to identify vulnerabilities and prioritize risk remediation activities.**
  - **What is a risk assessment?**
    - As defined by the International Organization for Standardization (ISO), risk assessment is a systematic approach to estimating the magnitude of risks (risk analysis) and comparing risk to risk criteria (risk evaluation). It is an ongoing process, not a single point-in-time review
  - **Scope of a risk assessment**
    - Critical asset inventory
    - Threat evaluation – both external and internal
    - Vulnerability assessment of assets
    - Risk evaluation and prioritization – governance
    - Technical Controls
    - Vendors and their Affiliates

Access Control

- **Principle: Physical and logical – Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.**
  - **Access permissions are managed, incorporating the principles of least privilege and separation of duties**
  - **Identities and credentials are managed for authorized devices and users**
  - **Physical access to assets is managed and protected**
  - **Remote access is managed**
  - **Password rules are appropriate**

Vendor Management

- **Principle: Firms should address cybersecurity risks that arise from vendor relationships.**
  - **Vendor management should cover the lifecycle of the relationship, from initiation through termination, and should be risk-based, i.e., there is greater due diligence and oversight on vendors who have access to sensitive data or processes.**
  - **Appropriate initial and ongoing due diligence**
  - **Incorporation of appropriate contractual requirements**
  - **Include vendors and vendor systems as part of the overall risk assessment process**
  - **Cloud Computing applications – understanding segregation of data and controls around access**
  - **Firms should conduct ongoing vendor re-assessments**

Incident/Breach Response Planning

- **Principle: Firms should develop plans to respond to cybersecurity incidents. Key elements include:**
  - **Event/Alert Management**
  - **Established policies and procedures – as well as roles and responsibilities – for escalating cybersecurity incidents**
  - **Media**
  - **Prepared communications plan for outreach to relevant stakeholders, e.g., customers, regulators, industry information-sharing bodies, law enforcement, and intelligence agencies, as appropriate**
  - **External Sources**
  - **Involvement in industry-wide exercises as appropriate to the role and scale of a firm's business in the securities markets, e.g. BCP/DR**
  - **Testing of the Plan**

Training

- **Principle: Firms should provide cybersecurity training to their staff and provide additional training based on staff's role.**
  - **Appropriate types of training are driven by:**
  - **Staffs' functional responsibilities:**
  - **Training on fraudulent money transfer schemes for account reps**
  - **Training on secure coding practices for developers**
  - **Firm's experience with cybersecurity incidents, such as loss incidents**
  - **Risk assessment**
  - **Awareness and intelligence about threats firm may face**
  - **In addition, firms should also consider providing resources to customers that will help them enhance their own cybersecurity practices**

Branch Office Controls

- **Firms with an Independent Contractor branch model may have more risk due to the nature of the branch technology infrastructure. Control Areas would include:**
  - **The use of passwords**
  - **Physical security of assets and data**
  - **Encryption of computers**
  - **Use and storage of email**
  - **Transmission of data**
  - **Incident reporting of lost or stolen data and hardware**
  - **Patch and virus protection processes**
  - **Firm branch exams**
  - **RR training and certification**

Technical Measures

There are a number of technical measures firms take to enhance their cybersecurity controls.

Anti-virus software	Anti-malware software
Application firewalls	Identity, access and privilege management
Data encryption	DDOS tools
Patch and software updates	Email content filtering
Web/URL filtering	Use of removable media
Penetration (PIN) testing	WiFi protection
BYOD	Online Access Management

Information Sharing

- **Principle: Firms should monitor the cybersecurity landscape and use information about current and evolving threats to enhance their ability to protect customer and firm information.**
  - **Information sharing can help firms prevent incidents or respond to incidents more quickly and can help protect the industry as a whole**
  - **A firm's infrastructure in this area should be scaled to the size of the firm and its degree of exposure to cybersecurity threats**
  - **Firms should participate in industry information-sharing bodies such as the FS-ISAC, NCFTA, 3rd Party Security Vendors and local law enforcement authorities**

Supplemental Guidance

- FINRA Report on Cybersecurity: *http://finranet.finra.org/news-events/employee-news/announcements/FINRA-Releases-Report-on-Cybersecurity-Practices*
- NIST: *www.nist.gov/cyberframework/index.cfm*.
- COBIT 5 - *www.isaca.org/COBIT/Pages/COBIT-5-Framework-product-page.aspx*
- ISO 27001/27002: *www.iso.org/iso/home/standards/management-standards/iso27001.htm*
- SIFMA Cybersecurity Resource Center: *www.sifma.org/issues/operations-and-technology/cybersecurity/overview/*
- FFIEC cybersecurity resources for banking organizations: *www.ffiec.gov/cybersecurity.htm* AND *www.ffiec.gov/cybersecurity.htm*
- *www.sec.gov/rules/final/34-42974.htm*
- *www.sec.gov/rules/final/2013/34-69359.pdf*
- *www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx*
- *www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx*
- *www.sec.gov/rules/final/34-44992.htm*
- *www.fsisac.com/*
- *www.ncfta.net/*

Financial Industry Regulatory Authority

South Region Compliance Seminar

New Orleans, LA | December 2 – 3, 2015

Cybersecurity: Understanding the Exposure
Thursday, December 3
11:00 a.m. – 12:00 p.m.

Resources

FINRA Resources

- *FINRA Report on Cybersecurity*

  http://finranet.finra.org/news-events/employee-news/announcements/FINRA-Releases-Report-on-Cybersecurity-Practices

SEC Resources

- *Identity Theft Red Flags Rules* (April 2013)

  www.sec.gov/rules/final/2013/34-69359.pdf

- *Books and Records Requirements for Brokers and Dealers Under the Securities Exchange Act of 1934* (May 2003)

  www.sec.gov/rules/final/34-44992.htm

- *Privacy of Consumer Financial Information (Regulation S-P)* (November 2000)

  www.*sec.gov/rules/final/34-42974.htm*

Federal Financial Institutions Examination Council (FFIEC) Cybersecurity Resources

- Cybersecurity Awareness

  www.ffiec.gov/cybersecurity.htm

NIST Resources

- Cybersecurity Framework

  www.nist.gov/cyberframework/index.cfm

National Conference of State Legislatures Resources

- State Laws Related to Internet Privacy

  www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx

- Security Breach Notification Laws

  www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx

SIFMA Resources

- Cybersecurity Resource Center

  www.sifma.org/issues/operations-and-technology/cybersecurity/overview/

Information Systems Audit and Control Association

- COBIT 5 Framework

  www.isaca.org/COBIT/Pages/COBIT-5-Framework-product-page.aspx

International Organization for Standardization

- ISO/IEC 27001 - Information Security Management

  www.iso.org/iso/home/standards/management-standards/iso27001.htm

Financial Services Information Sharing and Analysis Center

- FSISAC main webpage

  www.fsisac.com/

National Cyber-Forensics & Training Alliance

- Cracking Down on Cyber Crime

  www.ncfta.net/

