Cyber Security

Clint Johnson, Surveillance Director, FINRA, Atlanta District Office

Clint Johnson is Surveillance Director of FINRA's Atlanta District Office. In this role, he is responsible for the district's financial and sales practice risk surveillance programs. Prior to his current role, Mr. Johnson spent nearly 13 years conducting and managing examinations of FINRA member firms within the district's cycle, cause and membership application programs. Mr. Johnson has earned a bachelor's of business administration degree from the University of Georgia, and M.P.A. from Georgia State University.

Kevin Carreno, Principal, International Assets Advisory, LLC

Kevin A. Carreno is currently part owner and a principal of International Assets Advisory, LLC based in Orlando, FL. IAA is a small FINRA member firm involved in investment banking, institutional and retail business. Mr. Carreno has more than 25 years of experience as a lawyer in private practice, in-house counsel and in a variety of senior management positions, including Chief Compliance Officer, Chief Operating Officer and Chief Executive Officer with several brokerage firms. He has represented individuals and small firms in FINRA enforcement proceedings, new and continuing membership applications, examinations and investigations. Mr. Carreno has been appointed as an independent consultant in SEC, FINRA and various state enforcement matters. Mr. Carreno has served on the Board of the Florida Securities Dealers Association and as a member of the State Legislation and Regulation Committee of the Securities Industry Association (nka SIFMA). Mr. Carreno is a graduate of the United States Air Force Academy in Colorado Springs with an engineering degree. He is also a graduate of the University of Denver College of Law with a Juris Doctor. He currently holds the Series 4, 7, 24 and 53 licenses, and is a member of the Colorado and Florida Bars. Mr. Carreno was commissioned as a Second Lieutenant in the U.S. Air Force after graduation from the Academy. He served for five years on active duty and 18 years in the AF Reserve before retiring as a Lieutenant Colonel.

Dave Kelley, Surveillance Director, FINRA, Kansas City District Office

Dave Kelley is Surveillance Director of FINRA's Kansas City District Office, and has more than 20 years' experience dealing with cyber security, IT controls, and the privacy of customer and company information. He has been with FINRA for more than two years at the Kansas City District office as a regulatory coordinator and now the Surveillance Director, and leads FINRA's Regulatory Specialist team for Cyber Security, IT Controls and Privacy. Prior to joining FINRA, Mr. Kelley worked for 20 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 CIA, and holds the Series 7 and 24 securities registrations.

Tom Shaw, VP of Enterprise Financial Crimes Management and the Identity Theft Officer, USAA

Tom Shaw is the Vice President of Enterprise Financial Crimes Management and the Identity Theft Officer for USAA. He has direct overall responsibility for financial crimes prevention, detection, investigations and recovery. Mr. Shaw has more than 25 years of experience in the financial services industry, with over 16 years of this time at Bank of America. He has held leadership and direct contributor roles in fraud management, anti-money laundering, bank operations, credit/debit card operations, project management, consumer banking, ecommerce, call center management, small business lending and

private banking. Mr. Shaw participates in various working groups for financial crimes mitigation, such as the American Bankers Association, BITS and MasterCard US Fraud Advisory Council. He serves on the Board of Directors of the Identity Theft Assistance Center, which is a non-profit organization that educates consumers on ways to prevent and detect identity theft and helps consumers restore their identities when identity theft occurs. Mr. Shaw is also 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. Mr. Shaw earned his bachelor's degree in international economics from Texas Tech University and a M.B.A. from Our Lady of the Lake University. He is a Certified Anti-Money Laundering Specialist (CAMS) and a Certified Fraud Examiner (CFE).

Cybersecurity

South Region Compliance Seminar
November 20, 2014

Introduction – Moderator and Panelists

Moderator - Clint Johnson, Surveillance Director, FINRA Atlanta District Office

Panelist - Dave Kelley, Surveillance Director, FINRA Kansas City District Office

Panelist - Kevin Carreno, General Counsel and Chief Risk Officer, International Assets Advisory, LLC

Agenda

- Discussion Topics
  - FINRA's Cybersecurity Sweep
    - Background
    - Governance
    - Risk Assessment
    - Monitoring
    - Training
    - Incident Response
    - Insurance
  - Member Firm Perspective on Cybersecurity
  - Resources
  - Q&A

FINRA's Cybersecurity Sweep

Financial Industry Regulatory Authority

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
  - Availability
- **We are focused first and foremost on the protection of customer information, and PII in particular**
- **We are also concerned with the protection of firm information**
- **And, we are concerned about the potential impact of cyber incidents on the financial sector as a whole**

FINRA proposes a two-fold Cybersecurity approach

A principles-based approach provides the necessary flexibility for firms to develop an approach that best protects customer and firm information

- **There is no single right approach to cybersecurity**
- **The approach a firm takes is a function of both internal and external factors**
  - Internal factors include business model, technology architecture, and size
  - External factors: threat environment
- **A prescriptive approach that works for one firm may be entirely inappropriate for another**

Risk management-based approach to cybersecurity

A risk management-based approach enables firms to identify risks and prioritize actions based on their individual needs

- Again, there is no single right approach to cybersecurity
- A risk management-based approach is (or should be) holistic
- Given this broad approach, we necessarily focus on a variety of topics such as governance, risk management, and information sharing. We do not limit our review to technical measures such as anti-virus and anti-malware software
- Tools are available for firms that are more prescriptive, *e.g.*, the recent SIFMA Small Firms Cybersecurity Guidance document – July 2014
- Review and identification of appropriate frameworks – *e.g.*, NIST, ISO, COBIT – to inform firms' thinking about their approach to cybersecurity

Governance

Principle: Firms should establish governance frameworks that support informed decision-making and escalation at appropriate levels within the organization. This includes:

- 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 risks
- Defined accountabilities, structures, policies, and procedures to support decision-making based on risk appetite
- Use of appropriate metrics and thresholds
- Firms' governance structures support informed decision-making and escalation at appropriate levels within the organization

Risk assessment

Principle: Firms should conduct regular risk assessments to identify vulnerabilities and prioritize risk remediation activities

- **What is a risk assessment?**
  - ISO: a systematic approach to estimating the magnitude of risks (risk analysis) and comparing risk to risk criteria (risk evaluation)
- **Key features of a risk assessment**
  - Ongoing process, not a single point-in-time review
  - Critical asset inventory (done either as part of the risk assessment or separately to inform the risk assessment). This is essential to the firm understanding what it needs to protect and potential avenues for attack
  - Threat evaluation – both external and internal
  - Vulnerability assessment of assets
  - Risk evaluation and prioritization – governance

Risk assessment – continued

We observed a variety of different models firms use to perform their risk assessment

- **Primarily in-sourced with certain tasks**
  - Observed this more at large, sophisticated firms
- **Largely outsourced**
  - Observed this more at mid-sized firms and firms just getting started with the process

Critical asset inventory

Principle: Firms should develop and maintain a critical asset inventory

- **The inventory enables firms to understand what they need to protect and potential avenues for attack**
  - The development and maintenance of this inventory may be done either as part of the risk assessment or separately to inform the risk assessment
  - As part of creating the inventory, firms need to think through the criteria they use to define "critical asset"
  - There needs to be governance around the critical asset identification process (on both an initial and ongoing basis) to approve, monitor and update the asset risk rankings as appropriate.

Vendor management

Principle: Firms should address cybersecurity risks that arise from their 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 the more sensitive the data or processes to which the vendor has access**
  - Appropriate initial and ongoing due diligence
  - Incorporation of appropriate contractual requirements safeguard, *e.g.*, regarding:
    - Data protection
    - On-site visits
  - Include vendors and vendor systems as part of the overall risk assessment process
  - Cloud Computing applications

Training

Principle: Firms should provide cybersecurity training to their staff appropriate to the staff's role

- **Appropriate types of training are driven by:**
  - Staff's functional responsibilities, *e.g.*,
    - Training on fraudulent money transfer schemes for account reps
    - Training on secure coding practices for developers
  - Firm's experience with cybersecurity incidents, *e.g.*, loss incidents
  - Risk assessment
  - 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**

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 and NCFTA**
- **We observed that firms take a variety of approaches to managing threat intelligence**

Incident response planning

Principle: Firms should develop plans to respond to cybersecurity incidents on an individual basis as well as in an industry-wide context. Key elements of an incident response plan include:

- **Established policies and procedures – as well as roles and responsibilities – for escalating cybersecurity incidents**
- **Prepared communications plan for outreach to relevant stakeholders, *e.g.*, customers, regulators, industry information-sharing bodies, law enforcement and intelligence agencies, as appropriate**
- **Involvement in industry-wide exercises as appropriate to the role and scale of a firm's business in the securities markets**

Insurance

Principle: As part of the risk management process, firms should evaluate the level of cybersecurity risk the firm should transfer, if any, and purchase appropriate coverage, if available

- **The market for cybersecurity insurance is evolving, providing more rider and coverage choices that allow firms the option to transfer specific risks**
- **Firms should conduct a periodic analysis of the coverage provided to determine if it adequately covers those cybersecurity risks (as identified in the risk assessment process) the firm wishes to transfer**
- **As part of this review, firms should compare the coverage of cyber security insurance to other coverage (*i.e.*, fidelity bond or E&O)**

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 testing	WiFi protection
BYOD	

Cybersecurity – Member Firm Perspective

Financial Industry Regulatory Authority

Member Firm Perspective

Implementing Cyber Security Plan

- **Delegate Responsibility for Cybersecurity to appropriate staff**
- **Conduct a Risk Assessment**
- **Periodically Test Adequacy of Cybersecurity Controls**
- **Evaluate the Adequacy of Controls**

Member Firm Perspective

Risk Assessment

- **What are the Firm's Vulnerabilities**
  - Network Security
  - Account Access/Client Data
  - Critical Financial Data
  - Vendors (Clearing Firm, Email archive, external IT and cloud data services)
  - Website
  - Email

Member Firm Perspective

Network Security

- **Coordinate Cybersecurity Program with IT vendor**
  - Plan drafting tool http://www.fcc.gov/cyberplanner
- **Schedule intrusion events and results to test network security**
- **Implement Password protocol**
- **Secure Wi-Fi access**
- **Establish Protocol for Remote Access**
- **Establish policy for updating applications and web browsers**
- **Test Firewall security policies**

Member Firm Perspective

Client Data Security

- **Coordinate with Clearing Firm on access to client data, on-line access and security policies of Clearing Firm.**
- **Delegate responsibility for approving/removal of entitlements**
- **Reinforce policy that client data (financial information, positions, etc.) should only be maintained on clearing firm platform**

Member Firm Perspective

Firm Data

- Segregate Critical Data
- Manage Entitlements
- Password protect Financial Data
- Establish password protocol with banks and other financial institutions

Member Firm Perspective

Vendors

- Inventory Key Vendors
- Review Vendor Contracts
- Obtain Verification of Data Policies
- Results of Testing by Vendors

Member Firm Perspective

Web Security

- Security of Content of Public Websites
- Include Web Hosting vendor as key vendor
- Content and access filtering policy

Member Firm Perspective

Email Security

- Establish Email Use Policy
- Implement Spam Filtering
- Data Encryption

Member Firm Perspective

Staff Training

- **Include Cybersecurity in Annual Compliance Training**
- **Conduct periodic training on cybersecurity for all network users**

Resources

- **FINRA**
  - FINRA Cybersecurity Webinar - http://www.finra.org/Industry/Education/OnlineLearning/Webinars/P601394
  - FINRA Cybersecurity Webinar: Additional Resources & Organizations http://www.finra.org/web/groups/industry/@ip/@edu/documents/education/p601396.pdf
  - Industry Issues page – Customer Information Protection http://www.finra.org/Industry/Issues/CustomerInformationProtection/
  - Regulatory Notice 12-05 Verification of Emailed Instructions to Transmit or Withdraw Assets From Customer Accounts
  - Firm Checklist for Compromised Accounts - http://www.finra.org/Industry/Issues/CustomerInformationProtection/p117443
- **SEC**
  - National Exam Program Risk Alert – OCIE Cybersecurity Initiative http://www.sec.gov/ocie/announcement/Cybersecurity+Risk+Alert++%2526+Appendix+-+4.15.14.pdf
  - Cybersecurity Roundtable - http://www.sec.gov/spotlight/cybersecurity-roundtable.shtml

Resources

- **Other Resources**
  - NIST (National Institute of Standards and Technology) Cybersecurity Framework was created as a result of the President's executive order in Feb 2013 to develop a voluntary framework for reducing cyber risks to critical infrastructures. http://www.nist.gov/cyberframework/index.cfm
  - COBIT 5 - Developed by the Information Security Audit and Control Association (ISACA) (IT Auditors and Security Professionals). COBIT 5 is a framework for the governance and management of enterprise information technology. http://www.isaca.org/cobit/pages/default.aspx
  - ISO – International Organization for Standards – An independent, non-governmental organization that publishes standards that organizations and governments use for the operation and protection of information technology systems. Their Cybersecurity management standard is often referred to ISO/IEC 27001 (Information Security Management). http://www.iso.org/iso/home/standards/management-standards/iso27001.htm
  - FS-ISAC – Information Sharing and Analysis Center: A financial industry forum for collaboration on critical security threats. https://www.fsisac.com/

Questions ?

Session Notes