Financial Industry Regulatory Authority

Cybersecurity Conference

New York, NY | February 11, 2016

Identifying High-Risk Business Processes and Programs
Thursday, February 11
1:15 p.m. – 2:15 p.m.

Each firm has a unique threat landscape that is distinct from others; therefore, identifying your firm's areas of highest risk for security threats is critical. During this session, panelists discuss measures firms can take to determine their risk profile and risk tolerance.

Moderator:

David Kelley
Surveillance Director
FINRA Kansas City District Office

Panelists:

Jose Dominguez
Chief Information Security Officer
TD Ameritrade, Inc.

Lisa Roth
President
Monahan & Roth, LLC

Andy Zolper
Senior Vice President and Chief Information Security Officer
Raymond James Financial, Inc.

Identifying High Risk Business Processes and Programs Panelist Bios:

Moderator:

David 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:

Jose Dominguez is the Chief Information Security Officer at TD Ameritrade. He joined TD Ameritrade Holding Corporation (Nasdaq: AMTD) in 1997. He has been responsible for the development, maintenance and implementation of the enterprise security program and policies since 2013. Previous to his CISO role, Jose was in various management positions within technology leading Infrastructure and Application Development teams. Prior to joining TD Ameritrade, Jose spent 10 years with the brokerage firm Gruntal & Co. in various application development roles supporting front and back-office functions. He currently sits on the SIFMA Board Subcommittee on Cybersecurity and is a member of the NJ CISO Summit Governing Body.

Lisa Roth is a registered principal with Keystone Capital Corporation; a FINRA member firm headquartered in San Diego, CA. Ms. Roth holds FINRA Series 4, 7, 24, 53 and 65 licenses. Ms. Roth is also the President of Monahan & Roth, LLC, a professional consulting firm offering regulatory compliance consulting, expert witness and litigation support services. Previously, Ms. Roth was the founder and CEO of ComplianceMAX Financial Corp., a regulatory compliance company offering technology and consulting services to more than 1,000 broker-dealers and investment advisers. Ms. Roth's leadership at CMAX led to the development of audit and compliance workflow technologies now in use by some of the United States largest (and smallest) broker-dealers and investment advisers. Ms. Roth has also served in various executive capacities with Royal Alliance Associates, First Affiliated Securities, and other brokerage and advisory firms. Ms. Roth has served on the FINRA Small Firm Advisory Board, including one year as its chair. She is the past chairman of the National Association of Independent Broker-Dealer (NAIBD), and has served on the Board of the Third Party Marketers' Association. Ms. Roth has recently completed a two-year term as a member of the PCAOB Standing Advisory Group. She is an active participant in industry forums, including FINRA committees and trade associations. Ms. Roth is a frequent speaker at industry and regulatory conferences, and serves on ad hoc committees as necessary to promote a culture of continuous improvement for compliance and operations among investment services firms. Ms. Roth resides in CA, but is a native of Pennsylvania, where she attained a bachelor's degree and was awarded the History Prize from Moravian College.

Andy Zolper is Chief Information Security Officer for Raymond James Financial, Inc., a diversified financial services provider with subsidiaries engaged in investment and financial planning, investment banking and asset management. Through its three broker-dealer subsidiaries, Raymond James Financial has more than 6,300 financial advisers, serving more than 2.5 million accounts in more than 2,500 locations throughout the United States, Canada and overseas. As CISO, Mr. Zolper provides strategic direction to identify appropriate security measures, sponsors implementation of security solutions, manages daily security operations and provides governance to manage technology risk—all in order to help Raymond James achieve its business objectives. Mr. Zolper was previously at UBS as CISO of its Wealth Management Americas division, and later as global head of IT Risk Management. Prior to joining UBS, he led teams in IT risk management, global program management and business process reengineering at JPMorgan Chase. Before working at JPMC, Mr. Zolper was responsible for application development at Sterling Resources Inc., and developed the company's process reengineering, e-learning and knowledge management software products. Before joining Sterling Resources, he served in various management roles at Verizon, ranging from staff director of competitive intelligence analysis to field management of "fiber to the curb" deployment. Mr. Zolper graduated from the Virginia Military Institute. He is a U.S. Marine Corps veteran, having served as a communications

and signals intelligence officer. He is a graduate of SIFMA's Securities Industry Institute at The Wharton School, a Registered Operations Professional (Series 99), a certified Six Sigma Black Belt and a Certified Information Security Manager (CISM). He represents Raymond James on the Advisory Council of BITS, the technology policy division of The Financial Services Roundtable, and is a member of SIFMA's Cyber Security Working Group.

Cybersecurity Conference

February 11, 2016 • New York, NY

Identifying High-Risk Business Processes and Programs

FINRA

Panelists

- **Moderator:**
  - David Kelley, Surveillance Director, FINRA Kansas City District Office
- **Panelists:**
  - Jose Dominguez, Chief Information Security Officer, TD Ameritrade, Inc.
  - Lisa Roth, President, Monahan & Roth, LLC
  - Andy Zolper, Senior Vice President and Chief Information Security Officer, Raymond James Financial, Inc.

Risk Assessment Report

Purpose/Scope
Description of the system components, elements, users, sites considered (branches, home office, clearing firm)

Risk Assessment Approach
List participants, techniques used (questionnaires, templates), risk scale employed (numerical range, criteria)

System Characterization:
Description of critical assets.

Hardware:

Software:

Data:

Risk Assessment Report

Users:

☐ Attach connectivity diagram or system input and output flowchart to delineate the scope of this risk assessment effort.

Risk Assessment Results
Compilation of potential threat-sources and associated threat actions applicable to the system assessed, scored according to likelihood ("L"), impact ("I") and rating ("R").

Risk ID	Description	Source of Risk (Internal, External, User, etc)	Existing Mitigating Controls	L	I	R (sum)	Critical Risk (Yes or No)	Recommended Controls

Risk Assessment Report

Risk ID	Description	Source of Risk (Internal, External, User, etc)	Existing Mitigating Controls	L	I	R (sum)	Critical Risk (Yes or No)	Recommended Controls

Risk Assessment Report

Summary and Acknowledgement:
At minimum, discuss mitigation of critical risks including time frame if applicable.

Reviewed by (Name): _____ **Initials:** _____ **Date:** _____

Reviewed by (Name): _____ **Initials:** _____ **Date:** _____

Reviewed by (Name): _____ **Initials:** _____ **Date:** _____

Bring Your Own Device ("BYOD")

Policy Development and Implementation Outline

- **Secure Mobile Devices**
  - **Authentication (passcode/PIN) requirements**
  - **Storage/transmission encryption requirements**
  - **Requirements to automatically wipe devices after a number of failed login attempts**
  - **Usage restrictions for mobile devices**
  - **Company rights to monitor, manage and wipe**
    Invest in a mobile device management (MDM) solution to enforce policies and monitor usage and access.
  - **Enforce industry standard security policies as a minimum: whole-device encryption, PIN code, failed login attempt actions, remotely wiping, etc.**
  - **Set a security baseline: certify hardware/operating systems for enterprise use using this baseline.**
  - **Differentiate trusted and untrusted devise access: layer infrastructure accordingly.**
  - **Introduce more stringent authentication and access controls for critical business apps.**
  - **Add mobile device risk to the organization's awareness program.**

- **Address App Risk**
  - **Use mobile anti-virus programs to protect company- issued and BYOD malware-prone mobile operating systems with mobile anti-virus.**
  - **Ensure security processes cover mobile app development and leverage tools, and vendors to bridge assessment skill gaps.**
  - **Manage apps through a mobile app management product.**
  - **Introduce services that enable data sharing between BYOD devices.**
  - **To increase productivity and security, continually assess the need for new apps.**

- **Manage the Mobile Environment**
  - **Create and enforce an appropriate BYOD support and usage policy.**
  - **Revamp support provisioning and de-provisioning (wipe) of devices, and an increased level of self-help.**
  - **Create a patch education process to encourage users to update their mobile devices.**
  - **Introduce a social support mechanism to augment the existing IT support team.**
  - **Implement a wiki/knowledge base employee self-service support solution.**

- **Test and Verify the Security of the Implementation**
  - **Perform security testing and review of the implemented solution**
  - **Use an integrated testing approach combining automated tools**
  - **Perform manual penetration testing**

- **Test Infrastructural Changes Affecting Mobile Connections to the Enterprise Network**
  - **Wi-Fi deployments**
  - **VPN endpoints**

Cyber Security Incident Report

Complete the following form when any of the following events has occurred. Include incidents resulting from an accident or negligence, as well as those resulting from deliberate wrongdoing.

1. *Malware was detected on one or more Firm devices.*
2. *Access to a web site or network resource was blocked or impaired by a denial of service attack.*
3. *The availability of a critical web or network resource was impaired by a software or hardware malfunction.*
4. *An unauthorized user breached the network.*
5. *The compromise of a customer's or vendor's computer was used to remotely access the Firm's network resulted in fraudulent activity, such as efforts to fraudulently transfer funds from a customer account or the submission of fraudulent payment requests purportedly on behalf of a vendor.*
6. *The Firm received fraudulent emails, purportedly from customers, seeking to direct transfers of customer funds of securities.*
7. *The Firm was the subject of an extortion attempt by an individual or group threatening to impair access to or damage the Firm's data, devices, network, or web services.*
8. *An employee or other authorized user of the Firm's network engaged in misconduct resulting in the misappropriation of funds, securities, sensitive customer or Firm information or damage to the Firm's network or data.*
9. *The Firm, either directly or as a result of an incident involving a vendor, experienced the theft, loss, unauthorized exposure, or unauthorized use of or access to customer information.*
10. *Any other security breach event.*

Which of the above best describes the incident: (No.#): __

If (other) please describe:

Date detected: _____ Date Remediated: _____

How was the incident detected? ☐ Internally ☐ Externally ☐Not Known
What was the source of the incident? ☐ Internal ☐ External ☐Not Known
Please identify the cause of the incident. ☐ Deliberate wrongdoing ☐ Error, accident

Was client non-public data compromised? ☐ Yes ☐ No

Please describe the nature, duration, and consequences of the breach, how it was detected and how it was remediated:

Please provide any additional notes and/or details regarding this event, including the name(s) of any regulatory authorities to which the incident was reported.

Report Submitted by: _____ Date: _____

Report Reviewed by: _____ Date: _____

Electronic Devices and Communications Inspection Form

Electronic Device Review:

Device Name	Description	% Business Use	% Personal Use

□ Yes □ No Anti-malware software is installed on this device.

□ Yes □ No Anti-virus software is installed on this device.

□ Yes □ No Software auto-update is set to "ON" on this device.

□ Yes □ No Log in privileges to this device are password protected.

□ Yes □ No This device 'times out' after 15 minutes or less time of non-use.

□ Yes □ No ONLY approved (company) email is received on this device.

□ Yes □ No This device 'times out' after 15 minutes or less time of non-use.

□ Yes □ No ONLY associated personnel have access to this device.

Please explain any "NO" answer in the space provided below:

Exceptions, Notes:

Electronic Device Review:

Device Name	Description	% Business Use	% Personal Use

□ Yes □ No Anti-malware software is installed on this device.

□ Yes □ No Anti-virus software is installed on this device.

□ Yes □ No Software auto-update is set to "ON" on this device.

□ Yes □ No Log in privileges to this device are password protected.

□ Yes □ No This device 'times out' after 15 minutes or less time of non-use.

□ Yes □ No ONLY approved (company) email is received on this device.

□ Yes □ No This device 'times out' after 15 minutes or less time of non-use.

□ Yes □ No ONLY associated personnel have access to this device.

Please explain any "NO" answer in the space provided below:

Exceptions, Notes:

ONLINE RESOURCES CYBERSECURITY

Ten Cyber Security Tips for Small Business (FCC)
https://apps.fcc.gov/edocs_public/attachmatch/DOC-306595A1.pdf

US SEC National Exam Program Risk Alert (OCIE Cyber Security Initiative)
https://www.sec.gov/ocie/announcement/ocie-2015-cybersecurity-examination-initiative.pdf

2015 Verizon Data Breach Investigations Report
http://www.verizonenterprise.com/DBIR/2015/

FCC Cyber Security Policy Planning Guide Template
http://www.fcc.gov/cyberplanner

National Cyber Security Alliance – Mobile Tip Sheet (for personnel and customers)
http://staysafeonline.org/stay-safe-online/resources/stay-cyberaware-while-on-the-go-safety-tips-for-mobile-devices

Cyber Security in the Golden State (see "Practical Steps")
https://oag.ca.gov/cybersecurity

Boards of Directors, Corporate Governance and Cyber---Risks: Sharpening the Focus (a speech by SEC Commissioner Luis A. Aguilar)
http://www.sec.gov/News/Speech/Detail/Speech/1370542057946#.VMviuMZh1B w

National Institute of Standards and Technology – Cyber Security Framework
http://www.nist.gov/cyberframework/index.cfm

National Institute of Standards and Technology – Cyber Security Roadmap
http://www.nist.gov/cyberframework/upload/roadmap-021214.pdf