2020 FINRA Cybersecurity Conference

January 14, 2020 | New York, NY

Protect: Measures and Controls
Tuesday, January 14, 2020
11:15 a.m. – 12:15 p.m.

Attend this session to learn about preventive measures firms can take to control access to their systems, protect data on those systems, and educate and train contractors and staff about sound cybersecurity practices. As part of this discussion, panelists address some of the common areas where failures may occur (e.g., malware downloads, phishing attacks and wire transfers) and measures to prevent them.

Moderator:

John Brady
Vice President and Chief Information Security Officer
FINRA Technology, Cyber & Information Security

Speakers:

Joseph Copeland
Chief Information Security Officer
SFA Partners, Inc.

Allen Eickelberg
Vice President and Director of Operations
Spire Investment Partners, LLC

Jason Lish
Chief Security, Privacy and Data Officer
Advisor Group

Barry Suskind
Senior Director, Technology
FINRA Information Security Architecture

Protect: Measures and Controls Panelist Bios:

Moderator:

John Brady is Vice President in Technology for Cyber and Information Security for FINRA, and is the organization's Chief Information Security Officer (CISO). In this capacity, he is responsible for all aspects of FINRA's information and cyber security programs, as well as ensures compliance with related laws and regulations. He oversees staff focused in four primary information security areas: security architecture and controls, security management tools, application security, and identity management. Mr. Brady, along with counterparts in FINRA's Data Privacy Office, establishes policy and technical controls to ensure information is appropriately protected throughout its lifecycle. He began his career with FINRA more than 10 years ago as the Director of Networks and Firewalls. He then broadened and deepened his technical knowledge by taking on responsibility for server and storage infrastructure, where he led system engineering efforts to expand capacity and performance of Market Regulation systems in response to data volumes growing more than 40 percent year over year. Mr. Brady recently led the establishment, design, and implementation of FINRA's new data centers and the seamless migration of more than 175 applications from an outsourcer to those new data centers. Prior to the commencement of his work with FINRA in October 2002, Mr. Brady was Director of Networks at VeriSign from 2000 to 2002 and Network Solutions from 1998 to 2000. From 1995 to 1998, he built and operated Citibank's Internet Web and email services as Vice President, Internet Services. From 1993 to 1995, Mr. Brady worked for Sun Microsystems as Senior Consultant, where he built integrated network systems for prominent customers. Mr. Brady began his professional career as a member of technical staff at The Aerospace Corporation from 1987 to 1993, designing satellite systems and command and control networks for the Air Force Space Command. Mr. Brady holds a bachelor's degree in Computer and Electrical Engineering from Purdue University of West Lafayette in Indiana, and a master's degree in Industrial Engineering and Operations Research from the University of California at Berkeley. He also is an $(ISC)^2$ Certified Information Systems Security Professional (CISSP).

Speakers:

Jay Copeland is Vice President, Information Systems and Technology for The Strategic Financial Alliance, Inc. and Strategic Blueprint, LLC. and the Chief Information Security Officer for SFA Partners, Inc. and The SFA, Inc. Mr. Copeland is responsible for all aspects of IT, including systems, servers, network administration and cybersecurity for the broker dealer. Prior to The SFA, Mr. Copeland spent four years as the IT Manager for the marine electronics division of Johnson Outdoors, Inc. overseeing IT systems and technology in Georgia, Alabama and Canada. Prior to Johnson Outdoors, Mr. Copeland was Director, Information Technology of TSYS, an international credit card processing company for six years. As head of Service Delivery for TSYS Distribution Technologies, Mr. Copeland was responsible for IT project management and PCI compliance for all client facing, revenue generating systems. Mr. Copeland was also the Information Technology Manager of Tom's Foods, Inc., a nationally recognized snack food manufacturer, for 16 years prior to joining TSYS.

Allen Eickelberg, CFP® is Director of Operations for Spire Investment Partners, LLC; the parent of both a SEC RIA and a FINRA member BD. In this role, he oversees the operations and supervision of Spire's brokerage & advisory services, its IT infrastructure, and cyber security programs. Mr. Eickelberg has excelled at taking an entrepreneurial approach to introducing new technologies, streamlining operations processes, and improving Spires' cyber security programs. Previously, Mr. Eickelberg has held a number of positions with increasing responsibilities in both operations and administration at Spire working directly with Spires' executive leadership, compliance and wealth management teams. A graduate of Virginia Tech; Mr. Eickelberg spends his free time volunteering at a local ceramics studio and home-brewing a variety of styles of beer.

Jason Lish is currently the Chief Security, Privacy, and Data Officer for Advisor Solutions where he is developing a comprehensive and proactive strategy to drive business decisions and protect value creation on behalf of Advisor Group and its affiliated Advisors. Prior to Advisor Group, Mr. Lish served as Alight's Chief Information Officer. In this role, Mr. Lish was responsible for Alight's overall digital, technology, enterprise risk and security strategy and execution. Before joining Alight, Mr. Lish was the Senior Vice President of Security Technology and Operations for Charles Schwab and held senior roles in cyber security at Honeywell. Mr. Lish began his career in the United States Air Force as a telecommunication specialist where he administered large network, communication, and cryptographic

systems. He serves on several advisory boards related to systems security. Mr. Lish degrees include a B.S. in Business Information Systems and an M.B.A.

Barry Suskind, CISSP is a senior director and has been a member of the Cyber Security community for almost 30 years. He is a well-respected member of the Cyber Security community and regularly attends premiere Security Conferences like BlackHat and Defcon. As an early adopter of the Internet, Mr. Suskind built firewalls and secured the companies where he worked, sharing his experiences and knowledge with other divisions and staff. He came to FINRA in 2000, when it was still NASD and NASDAQ was still a part of the company. During his first week he was instrumental in stopping one of the worst email computer viruses, "I Love You". He worked with NASDAQ providing security expertise when they looked to create markets in Europe and Asia. Since then, he has diligently protected FINRA from security breaches both from external attacks and from computer viruses. His persistence in 2003-2004 prevented several computer viruses from causing any harm at FINRA but had adversely affected many other Financial Services companies. This earned him an "Excellence in Service Award." Mr. Suskind has deployed many of the security tools helping to keep FINRA safe, such as Spam Blockers, Intrusion Prevention, Data Loss Prevention and Vulnerability scanning. He has built a team of highly skilled staff that monitor and stop attacks from effecting our users or systems. When FINRA began its migration to the AWS Cloud, Mr. Suskind was there to ensure our enterprise was configured to be more secure than in the data center. He was an early adaptor of "Micro-segmentation" where hosts instead of networks are isolated, which further secures systems by preventing any attack from spreading. His current work includes working with enterprise architects to ensure the security of all FINRA's applications, including CAT. He's also working with his team to utilize Splunk to provide high level metrics so senior management and executives can see at a glance our security posture.

Protect:

Measures and Controls

Panelists

- Moderator
  - John Brady, Vice President and Chief Information Security Officer, FINRA Technology, Cyber & Information Security
- Panelists
  - Joseph Copeland, Chief Information Security Officer, SFA Partners, Inc.
  - Allen Eickelberg, Vice President and Director of Operations, Spire Investment Partners, LLC
  - Jason Lish, Chief Security, Privacy and Data Officer, Advisor Group
  - Barry Suskind, Senior Director, Technology, FINRA Information Security Architecture

To Access Polling

- Under the “Schedule” icon on the home screen,
- Select the day,
- Choose the Protect: Measures and Controls session,
- Click on the polling icon: 

AGENDA

1. NIST Cybersecurity Framework (CSF)
2. Protect Function Overview
3. Discussion Topics
4. Panel Discussion
5. Resources
6. Further Details on the Protect Function

1 | NIST Cybersecurity Framework (CSF)

NIST Cybersecurity Framework (CSF)

- Common and accessible language
- Adaptable to many technologies, lifecycle phases, sectors and uses
- Risk-based
- Based on international standards
- Living document
- Guided by many perspectives – private sector, academia, public sector

2 | Protect Function Overview

Protect Function Overview

1. Protect
   I. Develop and implement appropriate safeguards to ensure delivery of critical infrastructure services
   II. Supports the ability to limit or contain the impact of a potential cybersecurity event. Examples of outcome Categories within this Function include:
      a. Identity Management, Authentication and Access Control
      b. Awareness and Training
      c. Data Security
      d. Information Protection Processes and Procedures
      e. Maintenance
      f. Protective Technology

3 | Discussion Topics

Potential Discussion Topics – Polling Question 1

1. What do you consider to be your firm's most challenging cybersecurity concern?
   a. Phishing emails / Business Email Compromise (BEC)
   b. Malware / Ransomware
   c. Managing user identities across vendor systems
   d. Insider threats and risks
   e. Avoiding loss or theft of valuable data files
   f. Securing privileged access
   g. Account takeover / fraudulent wire transfers

4 | Panel Discussion

Phishing Emails / BEC

- Add a warning banner to emails originating from external domains
  Example:
  ****** EXTERNAL EMAIL ******
- Require Multi-Factor Authentication (MFA)
- Conduct phishing simulation exercises that train on how to spot and report suspicious emails
- Sophisticated SPAM filtering (Domain, IP, country origin)
- Strong email password length, complexity, and change frequency requirements
- Annual cybersecurity awareness training
- Extra training for staff that repeatedly fall for simulated or real phishes
- Regular cybersecurity awareness training
- Periodic IT and cybersecurity tips and tricks
- Detect and quarantine likely “impostor” emails
- Provide a method for user reporting of suspected phishing emails to Security (e.g., a “Phish Report” button in Outlook)

Malware / Ransomware

- Centralized anti-virus logging with analytics and automated electronic notifications and search tools to support threat hunting
- Highly segregated data storage and role level security to minimize information exposure
- Multiple backup schemes (offsite to cloud, offsite to remote facility, daily data replication to remote facility) and monthly recovery testing
- Layered anti-malware defenses – email & web filtering, intrusion prevention, endpoint detection and response (EDR) on workstations and servers
- Use advanced Endpoint Detection and Response tools
- Utilize the MITRE ATT&CK framework to guide design of protective and detective controls
- Scan for vulnerabilities and missing patches on a frequent basis and apply security patches in a timely manner
- Network segmentation – the more you can segment the harder it is for malware to spread
- Authenticate web browsing sessions
- Limit use of local admin rights

Managing User Identities Across Vendor Systems

- Best approach: Single Sign On (SSO) with federated identities leveraging your existing identity store (e.g. Active Directory)
- Defined on-boarding and off-boarding processes with checklists or automated identity management tools
- Periodic review of accounts and entitlements in each vendor system with manager attestation
- Utilize MFA to prevent unauthorized login to vendor systems even if passwords have been stolen or guessed
- Vendor or third-party risk management program to identify risks and drive informed vendor or partner selection
- Have a strong password policy for all accounts (especially administrators) – longer passwords are always better

Insider Threats and Risks

- Routinely review all employee entitlements to ensure only “business need” entitlements are granted
- Baseline normal activity for various job roles and deploy monitoring and tools to identify abnormal employee activity
- Gate moderate and higher risk activities with an “ask first” entitlement process by which requests are approved by an administrator and logged before they are executed
- Flag high-risk staff, such as those resigning, for additional monitoring and reduced entitlements
- Extensive employee background checks
- Electronic physical access control system logging
- Segregate and lock down valuable data (i.e., no open shares)
- Email supervision review with DLP (for acct #’s, SSNs, etc.)
- Educate staff as “human sensors”
- Monthly Cybersecurity Task Force (CTF) meetings
- Quarterly Cybersecurity Executive Committee meetings

Avoiding Loss or Theft of Valuable Data Files

- Data Loss Prevention tools for email, web uploads, and other network activity
- Invest in end-point device control systems to secure desktops, laptops and mobile devices and prevent writes to portable storage
- Tightly control access to sensitive and valuable data / files
- Limited laptop / remote access distribution and system access from office only (or remotely using VPN)
- Use containerized solutions for BYOD smartphones to segregate and secure company data
- Comprehensive cybersecurity awareness / training program
- Consider Information Rights Management (IRM) tools for your most sensitive docs – IRM puts a secure envelope around your data files and controls reading, sharing, editing, copying, or printing
- Control access to file upload websites
- User awareness training to ensure policies are known and adhered to

Securing Privileged Access

- All privileged access should have an audit trail, even super-admin users should be accountable and have their activities reviewed by the right people
- No privileged access allowed except by IT and only when needed for system / software administration
- No business functions performed using elevated privileges
- Separate credentials for all administrator users
- Require MFA for privileged access to prevent malware or hackers from taking administrative control of your network and servers
- Tightly control access between end-user and production environments to thwart phishing malware (e.g. “jump servers” w/ MFA or a server admin VPN)
- Periodically review privileged access and remove any unnecessary entitlements

Account Takeover / Fraudulent Wire Transfers

- Educate staff to recognize the tell-tale signs of account takeovers and social engineering (phishing, vishing, etc.)
- Authentication of the caller is essential – verbal passcodes or challenge questions are advisable
- Do not communicate passwords or usernames electronically
- Use adaptive login which detects a change of user device and challenges the user with extra authentication (such as random code to registered mobile #)
- Correlate anomalous events (e.g., password change followed by banking info update or outbound wire)
- Set appropriate $ thresholds for unverified wires; all transactions above the threshold should be verified by contacting (and authenticating) the account holder
- Analyze your incidents for opportunities to improve processes
- Look for trends or patterns in account takeover attempts to make sure they aren't connected and part of a larger breach effort
- Offer MFA as an option
- Utilize and integrate credential and PII theft monitoring services

5 | Resources

Resources

1. FINRA's Cybersecurity Page :
   I. 2018 Report on Selected Cybersecurity Practices
   II. 2015 Report on Cybersecurity Practices
   III. Small Firm Cybersecurity Checklist
   IV. Cybersecurity related Information Notices:
      a. Cloud-Based Email Account Takeovers – 10/2/2019
      b. Imposter Websites Impacting Member Firms – 4/29/2019

2. FINRA's listing of non-FINRA resources:
   I. Security news sites and reports
   II. Industry effective practices and guidance
      a. NIST, FBI, OWASP, SANS, and SIFMA
   III. Diagnostic Tools
   IV. Other Resources – MITRE ATT&CK Framework

6 Further Details on the Protect Function

Identity Management, Authentication and Access Control

- Identity Management, Authentication and Access Control
  - Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes
  - Physical access to assets is managed and protected
  - Remote access is managed
  - Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties
  - Network integrity is protected (e.g., network segregation, network segmentation)
  - Identities are proofed and bound to credentials and asserted in interactions
  - Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)

Awareness and Training

Awareness and Training

- All users are informed and trained
- Privileged users understand their roles and responsibilities
- Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities
- Senior executives understand their roles and responsibilities
- Physical and cybersecurity personnel understand their roles and responsibilities

Data Security

Data Security:

- Data-at-rest is protected
- Data-in-transit is protected
- Assets are formally managed throughout removal, transfers, and disposition
- Adequate capacity to ensure availability is maintained
- Protections against data leaks are implemented
- Integrity checking mechanisms are used to verify software, firmware, and information integrity
- The development and testing environment(s) are separate from the production environment
- Integrity checking mechanisms are used to verify hardware integrity

Information Protection

Information Protection Processes and Procedures:

- Baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g., concept of least functionality)
- System Development Life Cycle to manage systems is implemented
- Configuration change control processes are in place
- Backups of information are conducted, maintained, and tested
- Policy and regulations regarding the physical operating environment for organizational assets are met
- Data is destroyed according to policy
- Protection processes are improved
- Effectiveness of protection technologies is shared
- Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed
- Response and recovery plans are tested
- Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)
- Vulnerability management plan is developed and implemented

Maintenance

- Maintenance:
  - Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools
  - Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access

Protective Technology

- Protective Technology:
  - Audit/log records are determined, documented, implemented, and reviewed in accordance with policy
  - Removable media is protected and its use restricted according to policy
  - The principle of least functionality is incorporated by configuring systems to provide only essential capabilities
  - Communications and control networks are protected
  - Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations

2020 FINRA Cybersecurity Conference

January 14, 2020 | New York, NY

Protect: Measures and Controls
Tuesday, January 14, 2020
11:15 a.m. – 12:15 p.m.

Resources

FINRA Resources

- FINRA's Cybersecurity Webpage

  www.finra.org/industry/cybersecurity

- 2018 Report on Selected Cybersecurity Practices

  www.finra.org/sites/default/files/Cybersecurity_Report_2018.pdf

- 2015 Report on Cybersecurity Practices

  www.finra.org/sites/default/files/p602363%20Report%20on%20Cybersecurity%20Practices_0.pdf

- Small Firm Cybersecurity Checklist

  www.finra.org/sites/default/files/smallfirm_cybersecurity_checklist.xlsx

- Cybersecurity Alert: Cloud-Based Email Account Takeovers – 10/2/2019

  www.finra.org/rules-guidance/notices/information-notice-100219

- Imposter Websites Impacting Member Firms – 4/29/2019

  www.finra.org/rules-guidance/notices/information-notice-042919

- Non-FINRA Cybersecurity Resources Webpage

  www.finra.org/rules-guidance/key-topics/cybersecurity/non-finra-cybersecurity-resources

Other Resources

- MITRA ATT&CK Webpage

  https://attack.mitre.org/

