2020 FINRA Cybersecurity Conference

January 14, 2020 | New York, NY

Welcome Remarks
Tuesday, January 14, 2020
9:00 a.m. – 9:05 a.m.

Speaker: Steven Randich
Executive Vice President, Chief Information Officer
FINRA Office of the Chief Information Officer

Speaker Biography:

Steven J. Randich, Executive Vice President and Chief Information Officer (CIO), oversees all technology at FINRA. Previously, Mr. Randich served as Co-CIO at Citigroup, and CIO and Global Head of Technology for Citigroup's Institutional Clients Group. Prior to joining Citigroup, he was Executive Vice President of Operations and Technology and CIO at NASDAQ, where he was responsible for all aspects of NASDAQ technology, including applications development and technology infrastructure. From 1996 to 2000, Mr. Randich served as Executive Vice President and CIO for the Chicago Stock Exchange. He was responsible for all technology, trading-floor and back-office operations, and business product planning and development. Prior to joining the Chicago Stock Exchange, Mr. Randich was a Managing Principal at IBM Global Services and a Manager at KPMG. Mr. Randich has an undergraduate degree in computer science from Northern Illinois University and an M.B.A. from the University of Chicago.

2020 FINRA Cybersecurity Conference

January 14, 2020 | New York, NY

Welcome Remarks

FINRA®

Speaker

- Speaker
  - Steven Randich, Executive Vice President, Chief Information Officer, FINRA Office of the Chief Information Officer

Keynote Address
Tuesday, January 14, 2020
9:05 a.m. – 9:45 a.m.

Speaker: Michael Driscoll
Special Agent in Charge
Federal Bureau of Investigation (FBI)

Speaker Biography:

In June 2019, Director Christopher Wray named **Michael J. Driscoll** as a Special Agent in Charge in the New York Office where he currently oversees the Counterintelligence/Cyber Division. SAC Driscoll previously recently served as a Section Chief in the Criminal Investigative Division at FBI Headquarters in Washington, D.C. SAC Driscoll began his career as an FBI Special Agent in 1996, when he was assigned to the New York Office to work counterterrorism matters. He was part of the team that investigated al Qaeda conspirators, including those responsible for the 1998 bombings of United States Embassies in Kenya and Tanzania and the attacks on 9/11. SAC Driscoll was transferred to FBI Headquarters in 2003 to work as the FBI's representative to the al Qaeda Department of the CIA's Counterterrorism Center. In 2005, SAC Driscoll was promoted to Supervisor and returned to the New York Office, where he was in charge of the squad responsible for extraterritorial investigations in Africa. He also led the FBI's counterterrorism efforts in the New York Hudson Valley region and was later promoted to the Coordinating Supervisory Special Agent for New York's Counterterrorism Program. SAC Driscoll was named Assistant Legal Attaché for London in 2013, overseeing the Cyber Program and working closely with United Kingdom law enforcement and intelligence services. In 2016, he was appointed Assistant Special Agent in Charge of the Philadelphia Field Office's Cyber and Counterintelligence Programs. He returned to FBI Headquarters in 2018 as the chief of the Violent Crime Section, which leads the FBI's Crimes Against Children Program, as well as efforts to reduce violent crime and gang-related violence. Prior to joining the FBI, SAC Driscoll was an attorney working in commercial litigation. He graduated from the State University of New York in Albany and received his law degree from Hofstra University School of Law in Hempstead, New York. He earned an Attorney General's Award for Distinguished Service in 2002 for his work investigating al Qaeda and the 1998 embassy bombings.

Cyber DIVISION
FEDERAL BUREAU OF INVESTIGATION

Cyber Threats, Response, and Collaboration

Michael J. Driscoll
Special Agent in Charge
Cyber and Counterintelligence Division
New York Office

UNCLASSIFIED

Hello

Me

What we are concerned about?

National Priorities

Tools

2 Requests

National Priorities

- Counterterrorism
- Counterintelligence
- Cyber
- Criminal

- Hybrid Threats
- Universal Threats
- Common Modus Operandi

The changing threat of Hostile Nation States

Spies

Economic espionage now dominates our counterintelligence program.

Non-traditional collectors

Investors

Business partners

University Professors and Staff

Students

Researchers

Consultants

RUSSIA

Fifteen largest companies in each country, according to Forbes Global 2000 list (2018):

	China	Russia	USA
1	Industrial & Commercial Bank of China	Gazprom	Berkshire Hathaway
2	China Construction Bank	Sberbank	JPMorgan Chase
3	Agricultural Bank of China	Rosneft	Wells Fargo
4	Bank of China	Lukoil	Bank of America
5	Ping An Insurance Group	Surgutneftegas	Apple
6	Sinopec	VTB Bank	AT&T
7	Bank of Communications	Novatek	Citigroup
8	China Merchants Bank	Norilsk Nickel	ExxonMobil
9	China Life Insurance	Transneft	General Electric
10	Postal Savings Bank of China	Tatneft	Wal-Mart
11	Industrial Bank	Rosseti	Verizon
12	Shanghai Pudong Development Bank	Magnit	Microsoft
13	China State Construction Engineering	Rusal	Alphabet
14	China Minsheng Banking	Novolipetsk Steel	Comcast
15	China CITIC Bank	Severstal	Johnson & Johnson

- IRAN
- NORTH KOREA
- Others?

Hostile Nation States are our most serious source of Cyber related threats.

They will target your network, your people, and your supply chain.

Criminal Threats

DDOS and the IOT

Ransomware

- More focused attacks on companies or parts of companies
- Increasing focus on State and Local government offices

BEC

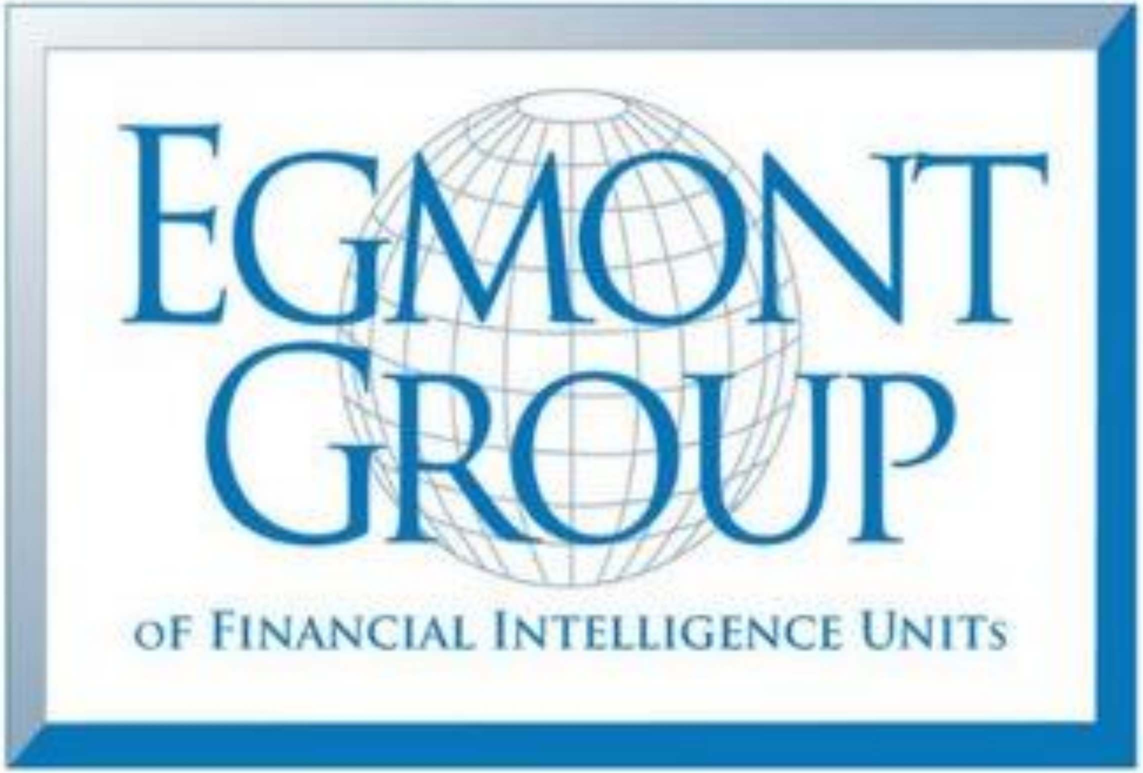
- Attackers are getting better at targeting the right people in your organization.

- Other Cyber Threats, like Malware, are being used to better understand your business processes.

Once you have been the victim of a BEC….

…the clock is ticking.

Financial Intelligence Units



EGMONT
GROUP
oF FINANCIAL INTELLIGENCE UNITs

155

Members

FINANCIAL CRIMES
ENFORCEMENT NETWORK

Bank Secrecy Act information

7

- CTR
- 8300
- CMIR
- DoEP
- FBAR
- RMSB
- SAR

- SARs

Identifying Criminal Actors

Low-level Structures

Facilitators

Serial Fraudsters

Typology Frequency

SARs tell a story !

Details are important…but what is your story?

Accuracy is important…

particularly with names !!

Outside the norm??

Fraud

Terrorist Financing

Human Trafficking

Your reporting can also help identify Cyber threats!

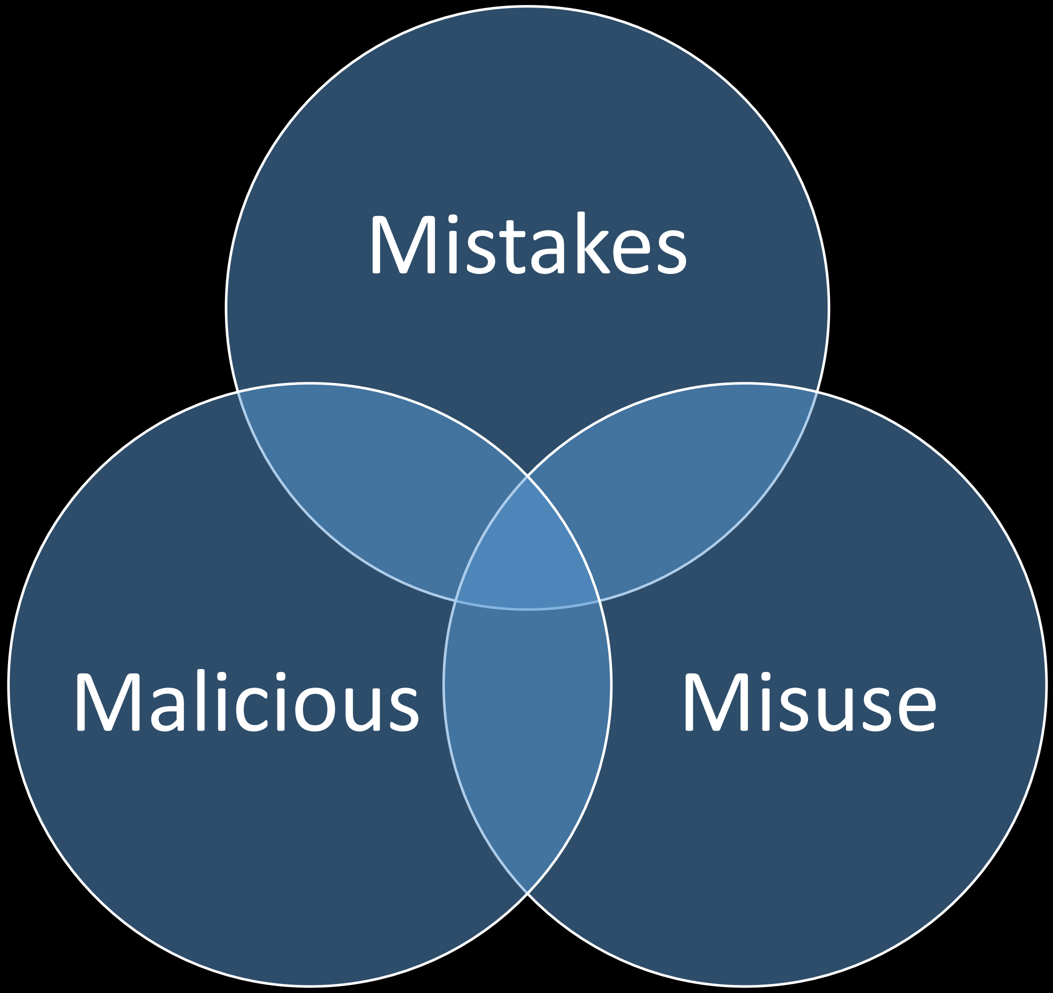
Elder Fraud

Elder Fraud Task Force

Early Adopters of Dark Web Tools

The Insider Threat

THREE TYPES OF INSIDER THREATS



Indicators

- Irregular Work Hours
- Accessing more that the position requires
- Repeated policy violations
- Financial difficulty or unexplained wealth
- Undisclosed foreign contacts
- Undisclosed foreign travel
- Destructive behaviors
- Ego

Indicators of Insiders for the Financial Sector

- Unexplained affluence
- Attempts to access information or accounts…The Dormant Account!!
- Avoids vacations
- Repeated policy violations

The Insider Threat can lead to serious Cyber vulnerabilities!

What happens when you leave the door open??

Consider how your efforts to combat money laundering, identify cyber threats, or address issues of fraud might also be used to identify the insider threat for your organization.

Best Practices for Individuals

- Remember: The Internet was not designed for security
- Limit personal information you post on the web and social media
- Manage your privacy/security settings on social media
- Do not use easy-to-guess passwords or reuse passwords. Consider using a password manager.
- Use two-factor authentication when possible
- Be suspicious of any e-mails you did not expect, especially those containing links or attachments
- Never provide personal information after clicking on a link
- Avoid public Wi-Fi spots and never conduct personal or sensitive business using public Wi-Fi
- Use secure browsing (HTTPS) when possible https://
- Keep antivirus tools up to date
- Only install software from trusted sources
- Do not ignore software update warnings, updates often include critical security fixes
- Remove software you do not use

Best Practices for the Enterprise

- Utilize legal banners
- Establish enforceable security policies and an employee handbook
- Implement employee training and awareness programs
- Maintain network topography maps
- Maintain lists of internal and external IP addresses and hosts
- Maintain inventory of network devices (switches, routers, etc)
- Maintain adequate incident logs
- Archive network traffic
- Perform regular backups of critical systems and data
- Ensure all patches and anti-virus software are up-to-date
- Obtain forensic images of compromised hosts (live memory captures)
- Maintain physical access logs (video cameras, key cards, etc)
- Contact the FBI as soon as possible following an incident

Good Logs!!

Patching!!

What are you protecting??

Don’t trust email!!

Cyber Security Frameworks

www.IC3.gov

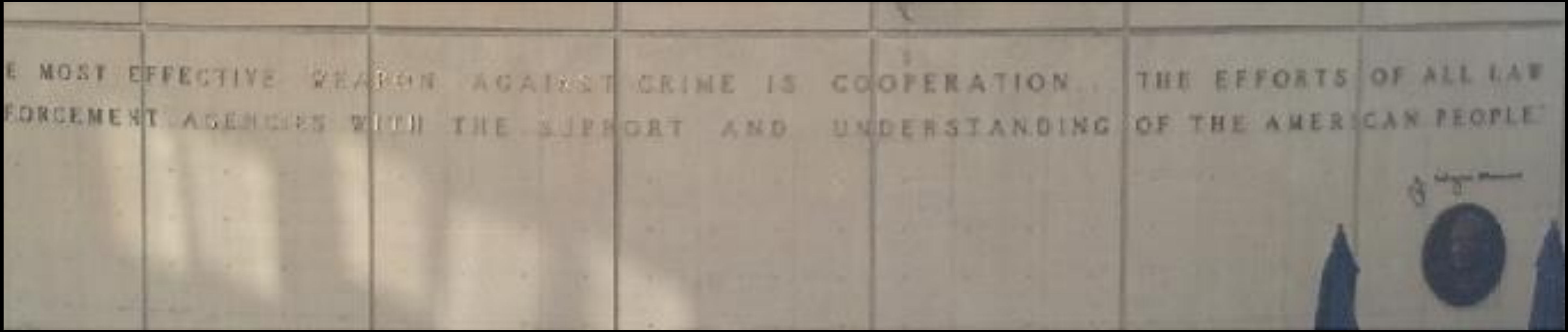
FEDERAL BUREAU OF INVESTIGATION
IC3
INTERNET CRIME COMPLAINT CENTER

https://www.ncfta.net/

www.ncfta.net

www.infragardnational.org

2nd Request



E MOST EFFECTIVE WEAPON AGAINST CRIME IS COOPERATION ... THE EFFORTS OF ALL LAW
FORCEMENT AGENCIES WITH THE SUPPORT AND UNDERSTANDING OF THE AMERICAN PEOPLE"

“The most effective weapon against crime is cooperation… the efforts of all law enforcement agencies with the support and understanding of the American people.”

2020 FINRA Cybersecurity Conference

January 14, 2020 | New York, NY

Identify: Cybersecurity Threats
Tuesday, January 14, 2020
10:00 a.m. – 11:00 a.m.

Join FINRA staff and industry panelists as they discuss the benefit of the National Institute of Standards and Technology (NIST) Cybersecurity Framework in developing a strong cybersecurity program. During the session, panelists discuss using a risk-management-based approach to cybersecurity, cybersecurity governance, assessments, including vendor due diligence, and the identification and inventorying of critical assets. Panelists discuss how firms with different business models conduct assessments and how the results inform a firm's cybersecurity program.

Moderator: John Kines
Director, Technology
FINRA Cyber & Information Security

Speakers: Michael Bouley
Chief Compliance Officer
Stockpile Investments, Inc.

Dwayne Roberts
Executive Director of IT Security and Risk
Grosvenor Capital

Lisa Roth
President
Tessera Capital Partners, LLC

Identify: Cybersecurity Threats Panelist Bios:

Moderator:

John Kines is Director of Technology for Cyber and Information Security for FINRA. In this capacity he is responsible for leading the Risk and Compliance Management team whose focus is on Enterprise Risk Management, Third Party Vendor Management, and maintaining FINRA's FISMA/FedRAMP and PCS-DSS Compliance. In prior positions at FINRA, he was a Technical Project Manager responsible for development and delivery of web application projects including the Nationwide Mortgage Licensing System (NMLS) and FINRA's Proctor applications. Mr. Kines holds a master's degree in Computer Science from Johns Hopkins University along with an MBA from Loyola University Maryland. He also holds numerous professional certifications including: ISACA's Certified Information Security Manager (CISM), Certified in Risk and Information Systems Control (CRISC) and Certified Information Systems Auditor (CISA) along with the Project Management Professional (PMP) certification.

Speakers:

Michael Bouley has more than 19 years of experience in the financial services industry working with various traditional and online FINRA member broker-dealer firms. His background includes serving as Chief Compliance Officer (CCO) for Stockpile Investments, Inc., a FINRA member broker-dealer, overseeing the firm's operations and compliance functions. Prior to Stockpile, some of his other work experience includes serving as Senior Manager Service at Zecco Trading, Inc., Brokerage and Offshore Delivery Manager at E*Trade Securities LLC, and as a Brokerage Manager at Brown & Co. LLC. Mr. Bouley received his B.S. from the Rhode Island College (RI). He currently maintains the Series 4, 6, 7, 9/10, 24, 63, 57 licenses.

Dwayne Roberts, Executive Director, Technology, specializes in cybersecurity and risk. Prior to joining GCM Grosvenor, Mr. Roberts spent three years at the Tribune Publishing Company as Digital Security Manager, and two years as Security Architect for TransUnion credit bureau. Previously, Mr. Roberts served 12 years in Japan performing multiple cybersecurity roles: Information Assurance Technical Lead for United States Forces Japan, Lead IT Security Engineer for Marine Corps Community Services, Security Operations Center (SOC) Analyst for the United States Navy and Information Protection Specialist for the United States Air Force. He has achieved several industry certifications throughout his 20 year cybersecurity career, such as, Certified Information Systems Security Professional (CISSP), Certified HIPAA Security Specialist (CHSS) and Payment Card Industry Professional (PCI-P). Mr. Roberts earned his degree in Information Systems Technology while on active duty in the Unites States Air Force.

Lisa Roth is the president of Monahan & Roth, LLC, a professional consulting firm offering compliance guidance, expert witness and related services on financial and investment services topics including securities and financial services industry compliance, investment product due diligence, investor suitability, management and supervision, information security and related topics. Ms. Roth is also the President, AML Compliance Officer and Chief Information Security Officer of Tessera Capital Partners. Tessera is a limited purpose broker dealer offering new business development, financial intermediary relations, client services and marketing support to investment managers and financial services firms. Ms. Roth holds FINRA Series 7, 24, 53, 4, 65, 99 Licenses, and has served in various executive capacities with Keystone Capital Corporation, Royal Alliance Associates, First Affiliated (now Allied) Securities, and other brokerage and advisory firms. In 2003, Ms. Roth founded ComplianceMAX Financial Corp. acquired by NRS in 2007), a regulatory compliance company offering technology and consulting services to more than 1000 broker-dealers and investment advisers. Ms. Roth's leadership at ComplianceMAX led to the development of revolutionary audit and compliance workflow technologies now in use by some of the United States' largest (and smallest) broker-dealers, investment advisors and other financial services companies. Ms. Roth has been engaged as an expert witness on more than 100 occasions, including FINRA, JAMS and AAA arbitrations, Superior Court and other litigations, providing research, analysis, expert reports, damages calculations and/or testimony at deposition, hearing and trial. Ms. Roth is a member of FINRA DR's National Arbitration and Mediation Committee, and FINRA's Series 14 Item Writing Committee. Ms. Roth was unanimously selected by her peers to serve as the Chairman of FINRA's Small Firm Advisory Board for one of a total of four years of service on the Board from 2008-2012. She has also served as a member of the PCAOB Standing Advisory Group, and is an active participant in other industry forums, including speaking engagements and trade associations. Ms. Roth resides in CA, but is a native of Pennsylvania, where she attained a Bachelors of Arts Degree and was awarded the History Prize from Moravian College in Bethlehem, PA.

Identify:

Cybersecurity Threats

Panelists

- Moderator
  - John Kines, Director, Technology, FINRA Cyber & Information Security
- Panelists
  - Michael Bouley, Chief Compliance Officer, Stockpile Investments, Inc.
  - Dwayne Roberts, Executive Director of IT Security and Risk, Grosvenor Capital
  - Lisa Roth, President, Tessera Capital Partners, LLC

To Access Polling

○ Under the “Schedule” icon on the home screen,

○ Select the day,

○ Choose the Identify: Cybersecurity Threats session,

○ Click on the polling icon: 📋

AGENDA

01 | Goals

02 | Polling Questions

03 | NIST Cybersecurity Framework (CSF)

04 | Identify Function

05 | Real World Insights On Vendor Management, Risk Assessments and Asset Management

06 | Resources

Panel Goals

- At the completion of session panel attendees should:
  - Understand the rationale for a risk based approach to Cybersecurity
  - Gain perspective on NIST Cybersecurity Framework (CSF)
  - Recognize the importance of vendor management, risk assessments and identification of critical assets
  - Walk away with key insights from real world experiences and have actionable next steps for your own firm

Polling Question #1

1. Does your firm work with a standard Cybersecurity Framework?
   a. Yes – NIST based framework
   b. Yes – Another framework
   c. No or not sure

Polling Question #2

2. Does your firm have an established inventory of critical assets?
    a. Yes
    b. No
    c. Not sure

Polling Question #3

3. How frequently does your firm perform a risk assessment that includes cybersecurity?
   a. Annually
   b. Every 2-3 years
   c. Not Yet

Polling Question #4

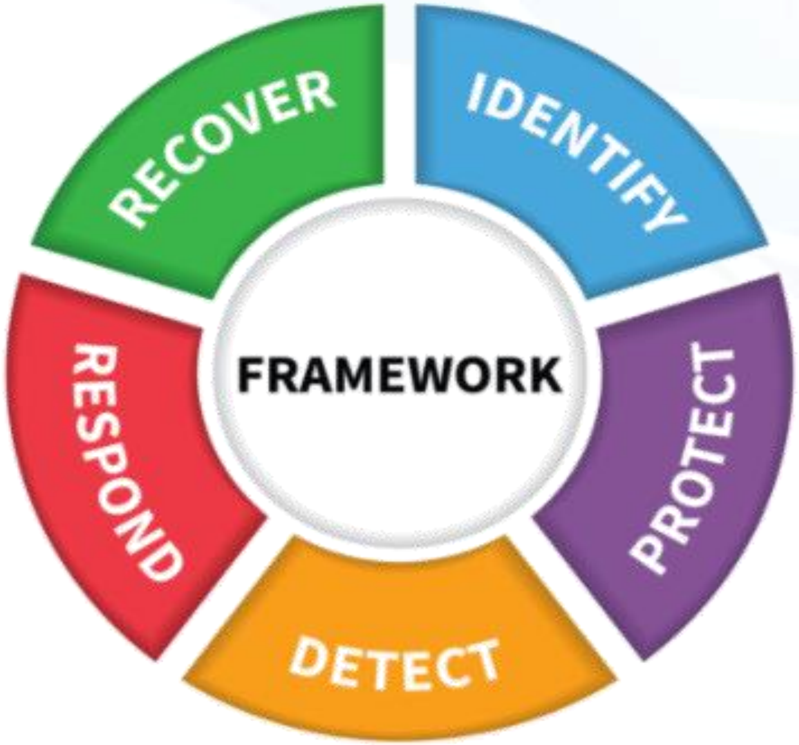
4. Does your firm outsource cybersecurity tasks to third party vendors?
    a. Yes – 50% or more
    b. Yes, but less than 50%
    c. No

Risk Based Approach to Cybersecurity

- Risks require both an existing vulnerability and identified threat
- Risk levels are organization specific
- Attempts to address all risks invariably outstrips mitigation resources
- Risk tolerance is the foundation of a risk based approach
- Goal is meaningful risk reduction, not 100% security
- Adopting a Cybersecurity Framework will help an organization align and prioritize its cybersecurity activities with:
  - Business/Mission requirements
  - Risk tolerances
  - Available resources

NIST Cybersecurity Framework (CSF) (Dwayne)

- 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



Identify Function (Lisa)

1. Identify -
   I. First of Five Framework Functions – core to the CSF
   II. Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities
   III. Framework Core – Foundational for effective use of the CSF
   IV. Key is to understand the business context, the resources that support critical functions, and the related cybersecurity risks
   V. Examples of outcome Categories within this Function include:
      a. Asset Management
      b. Business Environment
      c. Governance
      d. Risk Assessment
      e. Risk Management Strategy

Discussion Topic – Vendor Management (Michael)

1. Complete Due Diligence Checklist
2. IT and Compliance work hand and hand during the due diligence process
3. Consider the type of vendor/contractor and level of service
4. Consider Experience & Reputation of Vendor
5. Capability of vendor to provide required reporting information to fulfill potential compliance requirements
6. Is the potential vendor/contractor subject to previous regulatory reportable events
7. Some examples of requested information from vendor prior to engagement:
   - I. Privacy Policy
   - II. Cybersecurity/Information Security Policy
   - III. Business Continuity Plan
8. At minimum, perform an annual review of current vendors/contractors

Discussion Topic – Risk Assessments (Lisa)

1. Determine the Scope
   I. What needs to be protected (assets, systems, applications)?
   II. Who is the audience? (internal or external)
2. Collect Data
   I. Evaluate the current state of the assets in scope
   II. Review policies and procedures
   III. Conduct interviews
3. Analyze the vulnerabilities and threats
   I. Penetration vs vulnerability testing
   II. Human versus non-human; Consider leveraging:
      a. Internal Firm risk assessment tools
      b. Automated and manual account activity review
      c. Utilize internal exception reports
      d. Leverage clearing firm resources
4. Propose mitigation
   I. Quantify the value to the firm
   II. Remedy gaps in procedures, training

Discussion Topic – Asset Management (Dwayne)

1. Organizational assets go well beyond physical hardware and encompass: systems, devices, software, licenses, data and facilities that support business processes
2. A crucial step in Asset Management to perform asset inventory discovery scans:
   I. ICMP vs port scans
   II. Use of a vulnerability scanner
   III. If you don't know what you have you can't protect it!
3. Next, the criticality of each asset should be determined based on their relative importance to organizational objectives and risk strategy
4. Assets are then prioritized based on their classification, criticality, and business value and should be recorded in a gold source location (i.e., CMDB)
5. Major benefit of the inventory of all assets is that it helps:
   I. Combat shadow IT
   II. Ensure that effective controls are in place to protect critical assets
   III. Improve operational efficiency in terms of patching and maintenance

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, SIFMA
    III. Diagnostic Tools
    IV. Other Resources

Q
A

Identify: Cybersecurity Threats
Tuesday, January 14, 2020
10:00 a.m. – 11:00 a.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

FIRM NAME

Cyber Security Policies and Procedures

As of January, 2020

Table of Contents

Overview

FIRM NAME, LLC ("[FIRM]") has implemented this program, designed to maintain the privacy and confidentiality of all ***Confidential Information*** that [FIRM] obtains from current, past and prospective customers. Its goal is to also monitor and maintain [FIRM]'s information technology systems which include any discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic information.

A full definition of ***Confidential Information*** is available in ***Privacy and Confidentiality section, subsection A, of [FIRM]'s WSPs***. ***Exclusions from Confidential Information*** is available in ***Privacy and Confidentiality section, subsection B, of [FIRM]'s WSPs***.

The goal of this program is to:

(1) identify internal and external cyber risks by, at a minimum, identifying the Confidential Information stored by [FIRM], the sensitivity of such Confidential Information, and how and by whom such Confidential information may be accessed;
(2) use defensive infrastructure and the implementation of policies and procedures to protect [FIRM], its information systems and the Confidential Information stored on those the Firm's Information Systems, from unauthorized access, use or other malicious acts;
(3) detect Cybersecurity incidents;
(4) respond to identified or detected Cybersecurity incidents to mitigate any negative effects;
(5) recover from Cybersecurity incidents and restore normal operations and services; and
(6) fulfill all regulatory reporting obligations.

[DESIGNATED PRINCIPAL] has been designated as the Chief Information Security Officer ("CISO") and has primary oversight, maintenance, and execution of this Cyber Security Program (the "Program") which includes both technology and information security. The CISO is authorized to delegate physical, technical, and administrative components of this program to qualified third parties as and whenever appropriate.

[FIRM]'s CCO, [EXECUTIVE OFFICER], bears overall responsibility for the Firm's Business Continuity ("BCP") and Disaster Recovery ("DRP") planning, Privacy and Confidentiality, information protection, and including the integration of security processes and procedures tailored to the firm's size and resources.

Together, the CISO and CCO have identified the following core functions to guide this Program. These functions will be evaluated and updated by the CISO as indicated below to adjust for technological, business and/or operational changes at the firm that may have a material impact on the Program. The CISO will also report any exceptions to the CCO, CEO or other management as appropriate.

The CISO will be responsible for preparing a report, at least annually that addresses the following, to the extent they are relevant:

(1) assesses the confidentiality, integrity and availability of [FIRM]'s Information Systems;
(2) details exceptions to [FIRM]'s cybersecurity policies and procedures;
(3) identifies cyber risks to [FIRM];
(4) assesses the effectiveness of [FIRM]'s cybersecurity program;
(5) proposes steps to remediate any inadequacies identified therein; and
(6) includes a summary of all material Cybersecurity incidents that affected [FIRM] during the time period addressed by the report.

The CISO shall present the report to [FIRM]'s senior management as applicable.

Function	Designated Person	Frequency of Activity
Access management: password and technology access	CCO / CISO	Periodically
Access management: physical access	CCO	Periodically
End-user: desktop, web, network and server security	CISO	Annually
End-user: mobile devices and application security	CISO	Annually
Collaboration sites and storage networks	CCO	Annually
Security risk assessment	CISO	Annually
Cyber security testing and summary report to CCO	CISO	Annually
Network vulnerability scan	CISO	Annually
Employee security awareness training	CISO	Annually
Vendor selection and maintenance	CCO	Annually
Technology asset inventory	CCO	Annually
Technology end-of-life process	CISO	Annually
Implementation of Employee termination procedures	CCO	Annually
Disaster recovery and backup testing	CCO	Annually
Cybersecurity insurance	CISO	Optional, considered annually
Information Security	CCO	Annually
Vendor and third party service provider management	CCO	Annually
Cyber incident response	CCO / CISO	As needed
Penetration testing	CCO / CISO	Optional, considered annually

Function	Designated Person	Frequency of Activity
CISO Report to Senior Management	CISO	Annually

Audit Trail

The CISO, with the assistance of the CCO shall reasonably rely on document retention systems, including [SYSTEMS], for purposes of audit trail. These systems shall generally provide:

(1) tracking and maintenance data that allows for the complete and accurate reconstruction of all financial transactions and accounting necessary to enable [FIRM] to detect and respond to a Cybersecurity incident;
(2) Administrator and user management controls
(3) protection of the integrity of data stored and maintained as part of any audit trail from alteration or tampering (WORM storage through third party vendors);
(4) maintenance of the company's records as required by SEC Rule 17a-4.

Access Management

[FIRM] has an approach to entitlement management that helps establish controls around access activities. The goal of this program is focused on the following:

- Protect remote, mobile, cloud and social access on electronic devices in use by [FIRM] personnel including Associated Persons conducting business in branch offices.

- Provide transparency and up-to-date information on entitlements

- Provide centralized administration for permissions ([SYSTEM] and Email)

- Ensure that employees have access only relevant to their job functions

- Protect against insider threats and unauthorized escalation of user privileges

Each employee's profile will be managed in a central directory on [SYSTEM] that will be used to create, delete and modify employee access data. The CCO is the primary owner of the central directory.

Authorization: [FIRM] manages authorization information that defines what functions an employee can perform in the context of a specific application. The CCO may maintain a record of the authorizations, in any manner she deems appropriate. For instance, a record in the system provider shall be acceptable.

Information Sharing: Associated Persons are prohibited from sharing any Confidential Information with anyone without the express written approval of the CCO. If Confidential Information may be shared, the following guidelines apply:

- Associated Persons will obtain a NDA from those who are given access to non-public or Confidential Information.

- Confidential Information for business purposed may only be sent through email when using a [FIRM] email address or one that I am authorized by [FIRM] to utilize (dbas).

- Any Confidential Information being sent that contains an attachment such as PPMs, Offering Documents, Subscription, presentation, proposal, letter or other must be sent in an inalterable format such as PDF. Further, any legal documents or other non-public information such as an offering document or ppm should be sent in a password protected or encrypted format – a PDF file that has been password protected is an acceptable format. Alternatively, Associated Persons may send files using a link in [SYSTEM] which encrypts data and emails.

In addition, third parties with which Confidential Information is shared, must fall within regulatory guidelines for sharing information. Associated Persons are encouraged to contact the CISO or CCO with any questions regarding [FIRM]'s requirements and restrictions relative to Confidential Information.

Passwords: For accessing the company's books and records on [SYSTEM] the following password protocol applies:

Passwords must not contain username.
Password cannot include username.
Last 4 passwords cannot be reused.
Password must contain characters from 3 of the following categories:
English uppercase characters (A-Z)

- English lowercase characters (a-z)
- Numbers (0-9)
- Special characters (e.g., ! $ # %)

Each administrator will have a unique login account and password.

Associated Persons are prohibited from sharing passwords or posting them openly in their work areas.

Any person or person's employees (employees of a consultant or other party delegated responsibility for [FIRM]'s program, on an as needed basis, will each have a unique login and password to access the firm's password management list.

Physical access: [FIRM] will secure the firm's physical premises with locks and inventory keys issued to authorized persons on an ongoing basis.

Employees working from remote locations are required to store all Confidential Information in filing cabinets that prevent access to unauthorized persons and/or on protected systems ([SYSTEM]).

Associated Person may not allow anyone, non-related to [FIRM], to use the computer they conduct [FIRM] business on.

End-user: desktop, web, network and server security:

A. **[FIRM] responsibilities:**

[FIRM] has developed practices to protect the sensitivity of all the firm's information by implementing the following processes:

- Implement the use of password protection for all sensitive data, applications, and collaboration tools

- Educate end-users on appropriate use of desktops and web browsing for business purposes

- Maintain an inventory of all hardware, software and devices used by Associated Persons of [FIRM]

- Reconcile the inventory of hardware, software and devices

- Assist Associated Persons with the secure destruction of devices no longer in use

- Monitor access by Associated Persons of all emails and other Confidential Information maintained on [SYSTEM] (or [SYSTEM])

- Monitor Associated Person behaviors to detect potentially malicious insiders, including but not limited to work patterns, disclosure of unlawful activity or securities violations, decline in performance, significant debt or recurring financial irresponsibility, attempts to bypass securities system(s), falsifying reports or other such behaviors

B. Associated Persons responsibilities:

Associated Person will ensure:

- Each electronic device, including but not limited to a desk-top-computer, laptop, notebook, tablet (i-pad or other) or smart phone (i-Phone, Blackberry, Android or other) used by Associated Persons has been reported to [FIRM] for purposes of maintaining a device inventory.

- Access to the physical office space occupied by the Associated Person is secure from unauthorized access, including but not limited to file cabinets and electronic devices.

- Each electronic device, including but not limited to a desk-top-computer, laptop, notebook, tablet (i-pad or other) or smart phone (i-Phone, Blackberry, Android or other) used by Associated Persons has the appropriate safeguards such as encryption, firewalls and password protection.

- All email sent using personal devices must be configured so that they will be captured by [FIRM]'s electronic storage media. Associated Persons are strictly prohibited from the use of personal email or communication accounts for the business communications.

- All electronic devices including computers, tablets, or smart-phones are set to conduct automatic downloads of security patches as well as application and operating system software updates.

- Spam filters and other email gateways are employed and continuously updated by auto-update. [FIRM] is currently providing Proofpoint to all Associated Persons of the firm for purposes of implementing this requirement.

- Employ up-to-date, anti-malware, anti-virus and anti-spyware software (continuously updated by auto-update plus quarterly reviews) installed on their computers. Employees that are using devices that are not provided by [FIRM] are required to maintain this protection on any electronic device they utilize. These programs must also be set to Auto-Update to ensure continuous protections.

- Associated Persons using Wi-Fi must ensure that their connections are password protected.

- [FIRM] records required to be maintained under SEC Rules 17a-3 and 17a-4 must be saved to the company's secure archive system ([SYSTEM] offered by [SYSTEM]).

- Report lost, stolen or retired devices.

- Implement a "time out" protocol that ensures each electronic device requires a restart (including PW access) after a period of inactivity of 15 minutes or less.

- Removing software, services or applications that violate [FIRM]'s security policies.

- Comply with [FIRM]'s reporting requirements, including electronic device inventory, breaches/losses when detected or suspected, software including operating systems upon request.

C. End-user: mobile device and application security

Firm-owned devices include, but are not limited to, laptops, tablets, cellular phones, and smartphones provided by [FIRM]. Personal devices may utilize mobile access if they are password-encrypted and firm-approved.

At the time of hiring, and annually thereafter, [FIRM] requests disclosure of all electronic devices, including the % business and personal use for purposes of maintaining an up-to-date inventory.

Employees are advised to report any lost, stolen, or compromised electronic device used for business purposes to the CISO or CCO immediately. Upon such notice, the

CISO and/or CCO shall take reasonable steps to protect unauthorized access from the device.

The CISO and/or CCO reserve the right to inspect Associated Persons' computers or other electronic devices for purposes of ensuring that applications or software might compromise the security of Confidential Information stored by the firm.

Firm personnel will receive training on the secure use of mobile devices and removable media on an as-needed basis including during the annual compliance meeting.

D. Collaboration sites and end-user data storage

The CISO will be primarily responsible for vetting any collaboration site and data storage along with the CCO. Each site must have identified "data owners," who manage, control, and review access. Only firm approved collaboration sites listed below will be utilized.

The following collaborations sites are permitted for [FIRM] information:

- [SYSTEM]

Protecting firm data includes the proper use of collaboration sites and data storage sites. The following are requirements for collaboration sites and storing data:

Desktop, laptop, remote desktop and tablets

- Ensure storage of [FIRM] records on its approved archive systems;

- Only use applications approved by [FIRM]. Associated Persons are encouraged to seek CISO or CCO approval prior to use/installation of any new application used for business purposes or otherwise related to [FIRM]'s business and records.

Mobile devices (smart phones and tablets)

- Only store data within firm-approved applications
- Report all existing and new mobile devices, including % business versus personal use, as requested by [FIRM].

Records retention

- Certain types of data have retention periods

- All records including digital should be stored in an approved records repository

- Collaboration sites are not approved repositories
- Employees are responsible for preventing inappropriate use of or access to data by:
  - Only accessing information needed for your job function
  - Preparing, handling, using and releasing data
  - Using correct storage locations

- Following appropriate use or restrictions of electronic communications, including but not limited to email, instant messaging, text, chat, audio/video conferencing and social media

Security Risk Assessment

[FIRM]'s CISO and CCO will perform an annual assessment reasonably incorporating the following, as applicable and practical relevant to its size, resources and overall risk assessment:

Category	Subcategory
Network Security	Network Infrastructure Firewalls Network Diagram Frequency of Documentation Wireless
Data Security	Data Classification Backup and Restoration Encryption Mobile Security Disposal Protection of Transmission
Access Control	Active Directory Authentication Network Access Control Account/Password Management Application Access
System Development	Systems Installation Software Development Maintenance and Patching Decommissioning Change Control Management
Protection	Antivirus software Updates and patches Web Filter and traffic
Testing and Monitoring	Server Monitoring Network Monitoring Penetration Testing Vulnerability Testing Alerting
Vendors	Vendor Assessment Client Data
Employees	Termination / Role Transfer
Physical Premise Security	Data Center Building Security and Staff Building and Office Access Server Room
Information Security Program	Info Security Policy
Cybersecurity Insurance	Coverage Review

Employee Security Awareness Training

To assist firm employees in understanding their obligations regarding sensitive firm information, the CISO will provide each employee with a copy of this Program upon commencement of employment and whenever changes are made. In addition, the CISO and/or CCO will implement programs to perform training functions on an as-needed basis.

At the discretion of the CCO and CISO, employee security awareness training may include any of the following:

- Instruct employees to take basic steps to maintain the security, confidentiality and integrity of client and investor information, including:
  - Secure all files, notes, and correspondence
  - Change passwords periodically and do not post passwords near computers
  - Recognize and report any actual or perceived fraudulent attempts to obtain client or investor information and report to appropriate management personnel
  - Access firm, client, or investor information on removable and mobile devices with care and on an as-needed basis using firm protocols (passwords, etc.)
- Instruct employees to close out of files that hold protected client and investor information, investments, investment strategies, and other confidential information when they are not at their desks
- Educate employees about the types of cybersecurity attacks and appropriate responses

Vendor Selection and Management

For vendors interacting with [FIRM]'s systems, network and data, the firm will perform the following activities to protect sensitive information:

- Evaluate vendors before working with them including a reasonable cyber-security risk assessment
- Review third-party vendor contract language to establish each party's responsibility with respect to cyber-security procedures
- Segregate sensitive firm systems from third-party vendor access and monitor remote maintenance performed by third-party contractors (note third party vendors are utilized to store, and therefore have access to firm information. These vendors are subject to stricter due diligence checks than those vendors who do not have access to firm information.)
- the use of encryption to protect all Nonpublic Information in transit and at rest;
- prompt notice to be provided to the CCO or CISO in the event of a Cybersecurity incident affecting the third-party service provider;
- identity protection services to be provided for any customers materially impacted by a cybersecurity incident that results from the third-party service provider's negligence or willful misconduct;
- representations and warranties from the third-party service provider that the service or product provided to [FIRM] is free of viruses, trap doors, time bombs and other mechanisms that would impair the security of [FIRM]'s Information Systems or Nonpublic Information; and
- the right of [FIRM] or its agents to perform cybersecurity audits of the third-party service provider.

Furthermore, Associated Persons of [FIRM] must follow the following procedures:

- Alert [FIRM]'s CCO if any third-party service providers have access to my computer and indirectly or directly to [FIRM]'s network.

- No third-party provider that has access to Confidential Information of [FIRM] may be used without the express written permission of the CCO.

- Ensure that any service providers used have established, implemented and tested their data security procedures.

- At least annually, review each service provider to determine whether they monitor and defend against common vulnerabilities as part of their regular safeguards program and report findings to Senior Management.

Technology Asset Inventory, Classification and Tracking

[FIRM] Capital has a process in place to identify, classify, and track all technology assets (“assets”):

- [FIRM] will maintain an inventory of all assets as well as an identified owner.

- [FIRM] will track assets and their attributes throughout their lifecycle.

- [FIRM] will establish and enforce a process of assessing and classifying assets based on their sensitivity to attack and business value.

- [FIRM] shall take reasonable steps to protect its assets from unauthorized use.

Electronic Device - End-of-life Process

While the disposal of sensitive information that is kept in hard copy form is much easier to address, the firm has also become aware of its need to protect non-public and sensitive information that is stored on electronic devices (hard drives, CDs, flash drives, floppy disks, laptops and PDAs) if they are discarded by the firm. All Associated Persons of the firm must notify the CCO before any electronic devices, that are property of [FIRM] or are used for business purposes, are discarded.

[FIRM] has developed and will follow processes for securely disposing of assets once they are no longer being used by the firm or have reached the end of their usable life (the "end-of-life process").

Depending on the device, the CCO may choose from a number end-of-life-options to dispose of the electronic device. [FIRM] may use any of the following methods:

- Employ a certified end-of-life management vendor ("EMV") that will properly recycle any old hardware.
- Instruct Associated Persons how to "clean" the electronic device:
  - using Media Wiper or another appropriate software which has been approved by the CCO and is designed to permanently remove all information stored on the device.
  - Use of a magnet to demagnetize the electronic device, which will also permanently clear all information off the device.
  - Use of Device-Vendor technical support personnel to clear the device.

Once a device has been cleaned, the electronic device may be discarded.

The CCO may as applicable document the disposal process by writing a note to the file detailing the type of electronic device, the name of person that submitted the device for disposal, the type of information kept on that device and the methods used to permanently erase the information contained in it.

Employee Termination

The firm is dedicated to protecting the network and proprietary data at risk upon termination of employees. To prevent any issues of former employees leaking information, [FIRM] has adopted an approach towards access controls and entitlement management.

The CCO shall employ the use of a checklist or other summary document to track change in status generally including the following:

- Network access
- Desktop access
- Mobile device access
- Internal and external applications
- Vendor relationships

Business Continuity and Disaster Recovery Plans

Please see [FIRM]'s separate Business Continuity and Disaster Recovery Plans (BCP and DRP) for detailed documentation on the Firm's programs and testing of these programs. Updates to these policies will be represented in the separate plans and employees will be notified as to such changes.

The CCO, in consultation with the CISO, will update the firm's BCP and DRPs on an as-needed basis, but no less frequently than annually, to ensure that it is consistent with this Program and the [FIRM]'s activities.

Cybersecurity Insurance

On an annual basis, the CISO will review the firm's insurance coverage related to cybersecurity threats and decide as to its adequacy in conjunction with the CCO and COO.

[It is anticipated that cybersecurity insurance will not be attained unless or until the firm's risk profile substantially increases, because currently most sensitive data, including that of clients, is password protected.]

Cybersecurity Breach Framework

The firm has implemented a framework to identify, prepare, prevent, detect, respond, and recover from cybersecurity incidents, any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt or misuse an Information System or information stored on such Information System.

For purposes of the section, personally identifiable information (PII) shall be defined as any of the following in combination with the client's full name:

- Full birth date
- Passport ID numbers
- Online login credentials, such as usernames, passwords, and security questions
- Private encryption keys used for electronic signature
- Social Security numbers,
- driver's license numbers,
- credit and debit card information in combination with any required security or access code
- any other account holder identifying information in combination with any password or security question and answer that would permit access to an online account.

In the event of a cybersecurity incident, the firm's information technology personnel (or anyone detecting the incident) shall immediately notify the CISO or CCO who will work with appropriate personnel to perform any of the following as deemed appropriate:

- Assess the nature and scope of any such incident and maintain a written record of the systems and information involved

- Take appropriate steps to contain and control the incident to prevent further unauthorized access, disclosure or use, and maintain a written record of steps taken

- Promptly conduct a reasonable investigation, determine the likelihood that personal information has or will be misused, and maintain a written record of such determination.

- Discuss the issue with outside counsel, or other qualified resource and decide whether to disclose the issue to regulatory authorities, law enforcement and/or individuals whose information may have been affected

- Evaluate the need for changes to the firm's policies and procedures considering the breach

- The firm will work with outside resources and/or outside counsel as necessary to determine appropriate next steps including addressing any weaknesses identified in the process

- A record of the response to the incident shall be recorded and retained among the firm's central records.

If it is determined that a breach has occurred involving any of the PII or combinations of PII, then the CCO and CISO shall coordinate efforts to notify affected clients and appropriate state or other governmental agencies.

The notice to affected consumers and to applicable agencies must occur within 30 days from discovery of the breach unless law enforcement has indicated to the firm that notification to the public should be withheld while a criminal investigation is ongoing.

To address the common situation in which an entity whose data has been compromised may discover the problem only long after the breach began and, in some cases, only after active exfiltration of data has ceased, the notice must include the time frame of exposure, if known, including the date of the breach and the date of the discovery of the breach.

If applicable to comply with state governmental or other agency laws, rules or regulations, the contents of the firm's notice to the applicable agencies shall take the form and include the data required by that agency. This may include the timing-related data noted above, as well as a list of the types of personal information affected by the breach; a summary of the steps taken to contain the breach; and a sample of the notice to be provided to consumers. If applicable, the firm shall provide updates to the agency(ies) according to their requirements.

If the breach involves a compromise of a client's login credentials (username, password, security questions) of an email account provided by the breached entity itself, the entity cannot use consumers' compromised email accounts to provide them with notice.

A record of the communications to the incident shall be recorded and retained among the firm's central records.

Senior Manager Approval

I have approved these Cyber Security Policies and Procedures as reasonably designed to enable [FIRM] to maintain the privacy and confidentiality of all ***Confidential Information*** that [FIRM] obtains and to monitor [FIRM]'s information technology systems.

[EXECUTIVE OFFICER], CEO and CCO

Signed: ________________________________

Title: ________________________________

Date: ________________________________

[DESIGNATED PRINCIPAL], CISO and AML CO

Signed: ________________________________

Title: ________________________________

Date: ________________________________

Cyber Security Risk Assessment

Date:

Cybersecurity Program Document Version or Date: ________________________

Scope of Review:

Cybersecurity Insurance Coverage Date:
Cybersecurity Insurance Coverage Review:

Category: Network Security

Network Security	**Vulnerability**	**Impact to Organization**	**Likelihood of Occurrence**
Network Infrastructure			
Firewalls			
Network Diagram			
Frequency of Documentation			
Wireless			

Proposed Mitigation:

Category: Data Security

Data Security	**Vulnerability**	**Impact to Organization**	**Likelihood of Occurrence**
Data Classification			
Firewalls			
Backup and Restoration			
Encryption			
Mobile Security			
Disposal			
Protection of Transmission			

Proposed Mitigation:

Cyber Security Risk Assessment

Category: Access Control

Access Control	Vulnerability	Impact to Organization	Likelihood of Occurrence
Active Directory			
Authentication			
Network Access Control			
Account/Password Management			
Application Access			

Proposed Mitigation:

Category: System Development

System Development	Vulnerability	Impact to Organization	Likelihood of Occurrence
Systems Installation			
Software Development			
Maintenance and Patching			
Decommissioning			
Change Control Management			

Proposed Mitigation:

Category: Protection

Protection	Vulnerability	Impact to Organization	Likelihood of Occurrence
Antivirus software			
Updates and patches			
Web filter and traffic			

Proposed Mitigation:

Prepared for FINRA Cybersecurity Conference 1.14.2020
Courtesy of Monahan & Roth, LLC

Cyber Security Risk Assessment

Category: Testing and Monitoring

Testing and Monitoring	**Vulnerability**	**Impact to Organization**	**Likelihood of Occurrence**
Server Monitoring			
Network Monitoring			
Penetration Testing			
Vulnerability Testing			

Proposed Mitigation:

Category: Vendors

Vendors	**Vulnerability**	**Impact to Organization**	**Likelihood of Occurrence**
Vendor Assessment			
Client Data			
Vendor Reports, Breaches			

Proposed Mitigation:

Category: Employees

Employees	**Vulnerability**	**Impact to Organization**	**Likelihood of Occurrence**
New Employees			
Terminated Employees			
Independent Contractors			
Training			

Proposed Mitigation:

Prepared for FINRA Cybersecurity Conference 1.14.2020
Courtesy of Monahan & Roth, LLC

Cyber Security Risk Assessment

Category: Physical Premises Security

Physical Premises Security	**Vulnerability**	**Impact to Organization**	**Likelihood of Occurrence**
Data Center			
Building Security and Staff			
Building and Office Access			
Server Room			
Branch Locations			

Proposed Mitigation:

Review Performed by:

Review Reviewed by:

Prepared for FINRA Cybersecurity Conference 1.14.2020
Courtesy of Monahan & Roth, LLC

Electronic Device Inspection Template

Broker Name	
Supervisor Name	
Date of Inspection	
Electronic Means Used (laptop, desktop, etc)	
Inspection Performed by	

Electronic Device Description

□ Primary Business Device □ Secondary Business Device

Description (PC/Mac; desktop/laptop/other; approximate age)

This device connects to the internet via:

□ Secure Wifi □ Ethernet/Cable □ Other ___________________________

Device Review

Identify Device User(s)

Name	**Primary User**	**Secondary User**	**User Role (NRF, RR, DP, Other)**	**If Other, Describe**
	□	□		
	□	□		
	□	□		

Are company related folders/files found:

□ Yes □ No

Electronic Device Inspection Template

Description:

Are approved OBA related folders/files found:

□ Yes □ No

Description:

Are email accounts found (if yes, complete the table):

□ Yes □ No

Name	**Business, Personal, OBA; include % use if applicable**	**Subject to Company Archive/ Surveillance (Y or N)**	**Notes (Contents, nature of communications, sampling reviewed)**

Please complete the following for this device:

Password Protection is "ON"	**Software Auto Update is "ON"**	**Anti-Malware is "ON"**	**Anti-Spam is "ON"**	**Archive is "ON"**
	□	□	□	□

General Notes

Electronic Device Inspection Template

Reviewed by (signature)____ Date: ________

Reviewed by: (printed name): __________________________________

Reviewed by (signature)____ Date: ________

Reviewed by: (printed name): __________________________________

Comments:

FINRA

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

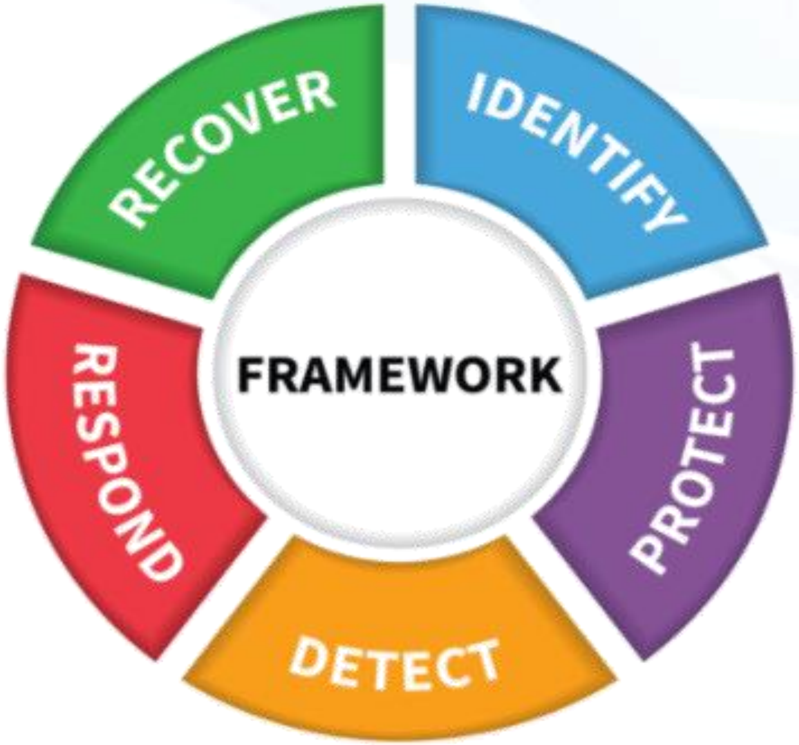
6 | Further Details on the Protect Function

FINRA

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

FINRA®

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

FINRA

- 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

FINRA

- 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

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/

Detect: Detecting Threats in a Timely Manner
Tuesday, January 14, 2020
1:15 p.m. – 2:15 p.m.

During this session, panelists discuss monitoring for cybersecurity threats and detecting cyber events or attacks and security breaches. Panelist discuss the types of monitoring that firms perform; the policies, processes and tools that support that monitoring; and the challenges of maintaining strong detective controls and making effective use of data and alerts.

Moderator: Gregory Markovich
Regulatory Principal, Chicago District Office
FINRA Member Supervision

Speakers: Matthew Beals
Chief Operating Officer and Chief Information Officer
Bolton Global Capital

Nicole Olivo
Compliance Liaison and Information Security Officer
TFS Securities, Inc.

Len Smuglin
IT Examination Manager
FINRA Member Supervision

Detect: Detecting Threats in a Timely Manner Panelist Bios:

Moderator:

Greg Markovich joined FINRA on February 1, 2016, as Regulatory Principal and he is currently responsible for leading cybersecurity examinations and providing security consultation and training for other staff. Prior to joining FINRA, Mr. Markovich has 30 years of information technology (IT) and security experience working at two investment management firms including Capital Group – American Funds, and American Century Investments. His leadership roles at these firms included responsibility for information security, risk management, identity access management, and disaster recovery. Mr. Markovich also has experience leading applications development and infrastructure support teams. In addition to having an MBA degree from the University of Missouri, Mr. Markovich has several security certifications including a certified Information Systems Security Professional (CISSP) and a Certified Information Security Manager (CISM) certification.

Speakers:

Matthew Beals is Chief Operating Officer and Chief Information Officer at Bolton Global Capital. In this role, Mr. Beals oversees back office operations, platform development, infrastructure expansion, information systems, and cybersecurity. He also works closely with Bolton's executive team on business development and company strategy. Prior to his current role, Mr. Beals was Manager of Technology and Business Development for Bolton Global Capital, where he managed information systems, cybersecurity, and supported new advisor acquisition. Mr. Beals holds a BS in Mathematics and Statistics and an MBA, both from the University of Massachusetts at Amherst. He also holds FINRA Series 7 and 24 licenses.

Nicole Olivo is Compliance Liaison and Information Security Officer at TFS Securities, Inc. As part of her responsibilities, Ms. Olivo spearheads cybersecurity efforts across the firm's securities, advisory, insurance, and mortgage divisions. Ms. Olivo developed the program with a focus on cybersecurity strategy and network architecture, internal and external threat assessments, and incorporating a "defense in depth" philosophy. Ms. Olivo developed and currently oversees cyber auditing process and procedures, WISPs, SIEM monitoring, DR/BCP programs, and continues to maintain and enhance open and effective dialogue with senior management, vendors, and advisors. Ms. Olivo serves as one of the firm's primary liaisons during SEC and FINRA Compliance Exams, as well as New York Department of Finance (23 NYCRR 500) Audits. Ms. Olivo has 20 years' experience in the financial services industry; holding positions at several specialist, investment banking, and broker-dealer firms in the areas of operations, compliance, risk management, regulatory research and examinations, supervisory structures and procedures, internal and external audits, innovative systems development, and project management.

Len Smuglin is an IT Exam Manager at FINRA. Prior to joining FINRA more than five years ago, Mr. Smuglin worked in the financial services industry for more than 20 years for several large New York area institutions. His roles and responsibilities were in the following areas: IT Audit, Technology Risk and Systems Quality Assurance. He is a University of Wisconsin (at Milwaukee) graduate where he majored in MIS (Management Information Systems) and completed Advanced Certificate Program in Systems Auditing at New York University. Mr. Smuglin holds a CISA certification (Certified Information Systems Auditor).

2020 FINRA Cybersecurity Conference

January 14, 2020 | New York, NY

Detect:

Detecting Threats in a Timely Manner

Panelists

- Moderator
  - Gregory Markovich, Regulatory Principal, Chicago District Office, FINRA Member Supervision
- Panelists
  - Matthew Beals, Chief Operating Officer and Chief Information Officer, Bolton Global Capital
  - Nicole Olivo, Compliance Liaison and Information Security Officer, TFS Securities, Inc.
  - Len Smuglin, IT Examination Manager, FINRA Member Supervision

To Access Polling

- Under the “Schedule” icon on the home screen,
- Select the day,
- Choose the Detect: Detecting Threats in a Timely Manner session,
- Click on the polling icon: 📋

AGENDA

01 | NIST Cybersecurity Framework (CSF)

02 | Detect Function

03 | Baselines

04 | Continuous Security Monitoring
(Vulnerability Scanning, Log Data Management, Internal Communications, Third Parties, Threat Intelligence)

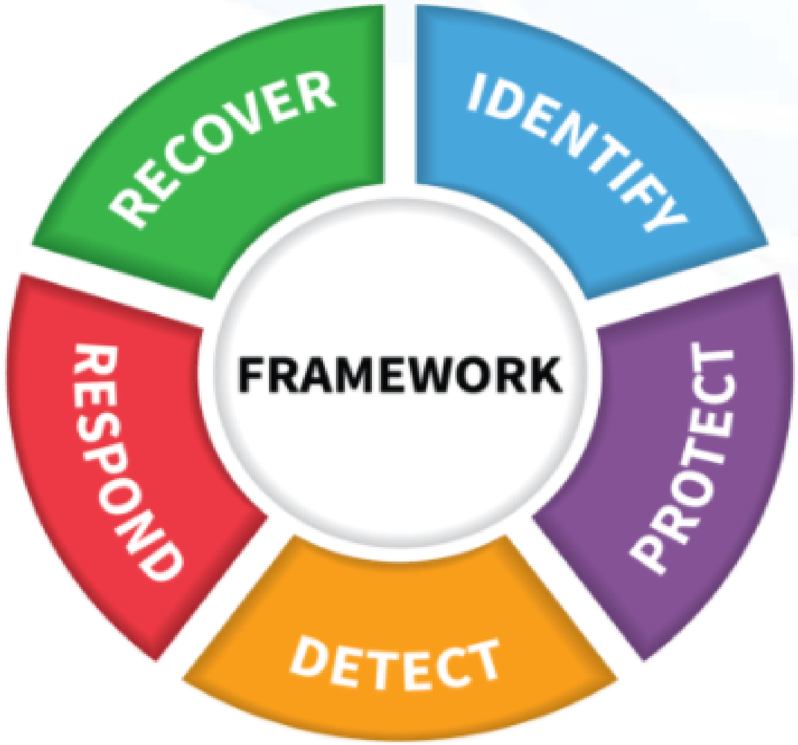
05 | Insider Risk

06 | Resources

07 | Q&A

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



Detect Function Defined

- Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.
- Enables timely discovery of cybersecurity events.
- Examples of outcome Categories within this Function include:
  I. Anomalies and Events
  II. Security Continuous Monitoring
  III. Detection Processes

Detect – Anomalies and Events

- Baseline of network operations and data flows for users / systems is established
- Detected events are analyzed to understand attack targets and methods
- Event data are collected and correlated from multiple sources and sensors
- Impact of events is determined
- Incident alert thresholds are established

Detect – Anomalies and Events: Baselines

1. Network Baseline:
   I. Inventory the hardware, software, and configuration of your network environment.
   II. Measure and record the key performance indictors of your network during normal operations on a typical business day.
      a. Metrics include network utilization, number of attached devices, protocol usage, peak utilization, and average throughput.
2. Data location and flows:
   I. Maintain an inventory of the location of critical databases in your environment and held at third party providers.
   II. Ensure an accurate data flow diagram is available for use in monitoring systems.
3. Users and systems:
   I. Maintain an inventory of all authorized systems in your environments and through third party providers including the cloud.
   II. Authorized users should only have access to the systems they need and this access should be monitored.

Poll Question 1: Baselines

1. Has your firm established baselines for your network, data, users, and/or application systems?
   a. Yes, we have most of these baselines in place
   b. Yes, we have some of these baselines established
   c. No, but we plan to establish baselines in the next 12 months
   d. No, we have not discussed establishing baselines
   e. What is a baseline?

Detect – Monitoring

- Physical environment is monitored to detect potential cybersecurity events.
- Personnel activity is monitored to detect potential cybersecurity events.
- Malicious code is detected
- Unauthorized mobile code is detected
- External service provider activity is monitored to detect potential cybersecurity events.
- Monitoring for unauthorized personnel, connections, devices, and software is performed.
- Vulnerability scans are performed.

Detect – Supporting Processes

- Roles and responsibilities for detection are well defined to ensure accountability.
- Detection activities comply with all applicable requirements.
- Detection processes are tested.
- Event detection information is communicated.
- Detection processes are continuously improved.

Poll Question 2: Monitoring

2. Does your firm monitor your network, servers, or desktop / laptop devices to detect potential cyber events or attacks?
    a. Yes, we have monitoring processes and tools in place
    b. Yes, we use a third party to monitor our environment
    c. No, but we plan to implement monitoring in the next 12 months
    d. No, we are not currently monitoring our environment

Considerations for Continuous Security Monitoring

1. Attacks from the outside (external)
2. Attacks from the inside (internal)
3. Third Party Provider system attacks (supply-chain)

Components of Continuous Security Monitoring

- Process to manage log data from multiple sources
- Network and End Point Monitoring tool(s) and process
- Intrusion Detection and Prevention (IDS and IPS)
- Security Incident and Event Management (SIEM)
- Knowledgeable staff / resources to analyze monitoring data and alerts
- Vulnerability identification/scanning tool(s) and process
- Monitor the security posture of your third party providers

Poll Question 3: Third Party Providers

3. Which of the following best describes how does your firm monitors the risks and activities of your critical third party providers who have access to client information and/or critical processes (e.g., trading, etc.)?
   a. We conduct regular oversight and monitoring of our vendor(s)
   b. We conduct an annual review of critical vendor security controls
   c. We rely on service levels and contract terms and conditions
   d. We rely on the reputation of the vendor (e.g., large industry provider)
   e. None of the above

Security Monitoring of Third Party Providers

- Annual assessment of third party providers processes and controls
- Use of a third party security rating service that maintains a “score-card” for your critical vendors with frequent updates
- Service level agreements and contractual terms related to confidentiality, personnel practices, security controls, and breach notification

Poll Question 4: Insider Risk Detection

4. Does your firm actively monitor your environment, either with internal or third party resources, to detect internal risk such as loss of client data or other proprietary information?
   a. Yes, we have processes and tools that monitor internal use of critical information and that provide alerts when anomalies are detected
   b. Yes, we have established basic monitoring to detect internal threats
   c. We rely on manual reviews of various reports/systems to uncover potential insider risks
   d. We do not currently monitor our systems/data to identify internal risk

Insider Risk – Common Types[1]

- Careless Worker –
  - Ignores business or technical processes or makes a legitimate mistake.
- Inside Agent –
  - Recruited by an external party to steal or corrupt company data.
- Disgruntled Employees –
  - Unhappy or angry worker seeking revenge.
- Malicious Insider –
  - deliberate misuse of corporate data or resources for personal gain.
- Third Party User –
  - compromise of data or systems because of negligence, data misuse, malicious intent, or accidentally.

[1] – 2019 Verizon Data Breach Report

Insider Risk – Monitoring Tools

- Identity Management –
  - Verify the identity of individuals access critical data and systems.
- Access Management –
  - Provide limited and granular access to sensitive data and systems.
- User Activity –
  - Identify abnormal user behavior through user analytics.
- Data Loss Prevention (DLP) –
  - Monitor use and transmission of sensitive data.

[1] – 2019 Verizon Data Breach Report

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, SIFMA
   III. Diagnostic Tools
   IV. Other Resources

Q
A

Detect: Detecting Threats in a Timely Manner
Tuesday, January 14, 2020
1:15 p.m. – 2:15 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

Respond and Recover: Recovery Plan – Minimizing the Damage
Tuesday, January 14, 2020
2:30 p.m. – 3:30 p.m.

This session evaluates how to respond to and recover from a cyber-attack or security breach. Panelists address incident response planning, restoring systems, process improvements, and communications with clients and regulators when breaches occur.

Moderator:

Kevin Bogue
Regulatory Principal, Chicago District Office
FINRA Member Supervision

Speakers:

Greg Lockwood
Chief Technology Officer and Chief Information Security Officer
USA Financial Securities Corp.

Paul Nickelson
Director, Cyber Fusion Center
TD Ameritrade

Jennifer Szaro
Chief Compliance Officer
Lara, May & Associates, LLC

Respond and Recover: Recovery Plan – Minimizing the Damage Panelist Bios:

Moderator:

Kevin Bogue joined FINRA in January 2017 as Regulatory Principal in the Chicago Office. Mr. Bogue is a member of the Member Supervision Cybersecurity team responsible for examining firms' controls over their protection of sensitive client and firm information. Prior to joining FINRA, Mr. Bogue has more than 18 years of information technology (IT) and information security experience working as a technology consultant with Accenture, as an internal Global IT auditor, IT Compliance Manager and SOX Program Manager with Abbott Laboratories, as an IT Compliance Manager with Brunswick and as an internal IT Audit Manager with CDW. Mr. Bogue earned an MS in Information Systems from DePaul University in Chicago, IL and a BS in Psychology from Iowa State University in Ames, IA.

Speakers:

Greg Lockwood is the chief technology officer and chief information security officer for USA Financial. His responsibilities include leading the internal technical staff and external consultants to deliver software, hardware, network, telecom and other technical services that support those connected to USA Financial. As CISO, Mr. Lockwood leads the organization's enterprise security program. Since joining the firm in 2007, he's played a vital role in the continued success of USA Financial by implementing processes and systems to address the needs of its staff, advisors, and clients. Through his technology leadership, Mr. Lockwood has improved the efficiencies and security posture of the internal staff, as well as the advisors and clients who are affected daily by the technology systems employed by the firm. Mr. Lockwood is a 20+ year veteran of the Information Technology field and holds a B.S. in communications from Grand Valley State University in Grand Rapids, Michigan.

Jennifer Szaro is Chief Compliance Officer for Lara, May & Associates, LLC ("LMA") a fully disclosed introducing broker/dealer and its affiliated investment advisory firm, XML Financial Group. Ms. Szaro is responsible for managing both firms' compliance infrastructures. Ms. Szaro joined the securities industry in 2000. She previously worked in the internet technology sector where she had experience in ecommerce, hosting and product development. As the securities industry went through significant changes with higher regulatory demands she took on more compliance and marketing related roles. In 2011, she became a senior level executive and LMA's Chief Compliance Officer. In addition to her role as the CCO, she is the AMLCO, and alternative FINOP. She's obtained the following FINRA series 6, 7, 14, 24, 28, 53, 63, 65 and 99. In 2012, she completed FINRA's Certified Regulatory and Compliance Professional Program (CRCP)® previously through the FINRA Institute at Wharton. In 2018, she became a non-public FINRA Dispute Resolution Arbitrator, having qualified through the National Arbitration and Mediation Committee. In 2019, she was appointed by FINRA to serve out a two-year term on the Small Firm Advisory Committee (SFAC) and is the 2020 Chair. Ms. Szaro is a graduate from the University of Rhode Island with a Bachelor of Science.

2020 FINRA Cybersecurity Conference

January 14, 2020 | New York, NY

Respond and Recover:

Recovery Plan – Minimizing the Damage

FINRA®

Panelists

- Moderator
  - Kevin Bogue, Regulatory Principal, Chicago District Office, FINRA Member Supervision
- Panelists
  - Greg Lockwood, Chief Technology Officer and Chief Information Security Officer, USA Financial Securities Corp.
  - Paul Nickelson, Director, Cyber Fusion Center, TD Ameritrade
  - Jennifer Szaro, Chief Compliance Officer, Lara, May & Associates, LLC

To Access Polling

- Under the “Schedule” icon on the home screen,
- Select the day,
- Choose the Respond and Recover: Recovery Plan – Minimizing the Damage session,
- Click on the polling icon: 📋

AGENDA

01 | NIST Cybersecurity Framework (CSF)

02 | Respond Function

03 | Respond Categories

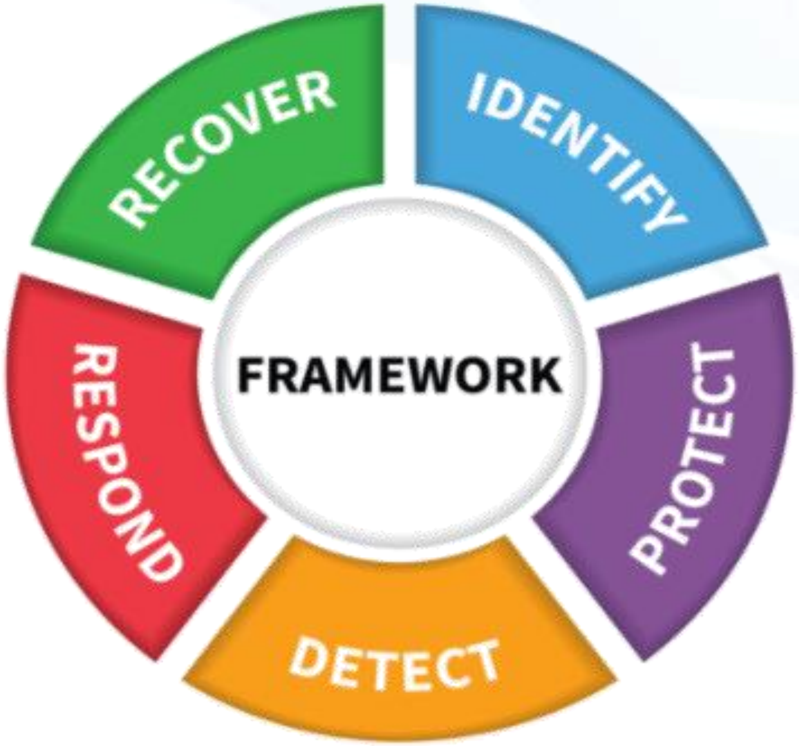
04 | Recover Function

05 | Recover Categories

06 | Resources

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



Poll Question 1: Incident Response Plan

1. Has your firm established a formal Incident Response plan?
   a. Yes, we are testing at least annually
   b. Yes, we have not tested the plan yet
   c. No, but we plan to establish a plan in the next 12 months
   d. No, we have not discussed establishing a plan

Respond Function Defined

1. Respond
   I. Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.
   II. Supports the ability to contain the impact of a potential cybersecurity incident. Examples of outcome Categories within this Function include:
      a. Response Planning;
      b. Communications;
      c. Analysis;
      d. Mitigation; and
      e. Improvements.

Respond – Response Planning

Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.

- Response plan is executed during or after an incident

Respond – Communications

Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).

- Personnel know their roles and order of operations when a response is needed
- Incidents are reported consistent with established criteria
- Information is shared consistent with response plans
- Coordination with stakeholders occurs consistent with response plans
- Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness

Respond – Analysis

- Analysis is conducted to ensure effective response and support recovery activities.
- Notifications from detection systems are investigated
- The impact of the incident is understood
- Forensics are performed
- Incidents are categorized consistent with response plans
- Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)

Respond – Mitigation

Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.

- Incidents are contained
- Incidents are mitigated
- Newly identified vulnerabilities are mitigated or documented as accepted risks

Respond – Improvements

Organizational response activities are improved by incorporating lessons learned from current and previous detection / response activities.

- Response plans incorporate lessons learned
- Response strategies are updated

Poll Question 2: Recovery Plan

1. Has your firm established a formal Recovery Plan?
   a. Yes, we are testing at least annually
   b. Yes, we have not tested the plan yet
   c. No, but we plan to establish a plan in the next 12 months
   d. No, we have not discussed establishing a plan

Recover Function Defined

1. Recover
   - I. Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.
   - II. Supports timely recovery to normal operations to reduce the impact from a cybersecurity incident. Examples of outcome Categories within this Function include:
     - a. Recovery Planning;
     - b. Improvements; and
     - c. Communications.

Recover – Recovery Planning

Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.

- Recovery plan is executed during or after a cybersecurity incident

Recover – Improvements

Recovery planning and processes are improved by incorporating lessons learned into future activities.

- Recovery plans incorporate lessons learned
- Recovery strategies are updated

Recover – Communications

Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).

- Public relations are managed
- Reputation is repaired after an incident
- Recovery activities are communicated to internal and external stakeholders as well as executive and management teams

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, SIFMA
   III. Diagnostic Tools
   IV. Other Resources

Q
A

Respond and Recover: Recovery Plan – Minimizing the Damage
Tuesday, January 14, 2020
2:30 p.m. – 3:30 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

2020 FINRA Cybersecurity Conference

January 14, 2020 | New York, NY

Cybersecurity the Current Regulatory Environment: Insight from Regulators and Industry Experts
Tuesday, January 14, 2020
3:45 p.m. – 4:40 p.m.

During this session, hear insight from regulators and industry experts. Panelists answer your questions related to the cybersecurity regulatory landscape, what they are seeing during examinations and other important issues. You will hear their perspectives on effective practices and helpful tips they have identified.

Moderator: David Kelley
Surveillance Director, Kansas City District Office
FINRA Member Supervision

Speakers: Gregory Markovich
Regulatory Principal, Chicago District Office
FINRA Member Supervision

Salvatore Montemarano
Senior Specialized Examiner - Information Technology, Technology Controls Program, Office of Compliance Inspections and Examination (OCIE)
U.S. Securities and Exchange Commission (SEC)

Dale Spoljaric
Managing Director, Compliance
National Futures Association (NFA)

Cybersecurity the Current Regulatory Environment: Insight from Regulators and Industry Experts Panelist Bios:

Moderator:

Dave Kelley is Surveillance Director based out of FINRA's Kansas City office. He has been with FINRA for nine years and leads the regulatory surveillance team based in Kansas City. Mr. Kelley also leads FINRA's Sales Practice exam program for cybersecurity and the 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.

Speakers:

Greg Markovich joined FINRA on February 1, 2016, as Regulatory Principal and he is currently responsible for leading cybersecurity examinations and providing security consultation and training for other staff. Prior to joining FINRA, Mr. Markovich has 30 years of information technology (IT) and security experience working at two investment management firms including Capital Group – American Funds, and American Century Investments. His leadership roles at these firms included responsibility for information security, risk management, identity access management, and disaster recovery. Mr. Markovich also has experience leading applications development and infrastructure support teams. In addition to having an MBA degree from the University of Missouri, Mr. Markovich has several security certifications including a certified Information Systems Security Professional (CISSP) and a Certified Information Security Manager (CISM) certification.

Salvatore Montemarano has been an examiner within the SEC's Office of Compliance Inspections and Examinations for three years. Prior to joining the Commission, he was the Chief Information Security Officer for the Overseas Private Investment Corporation (OPIC). Mr. Montemarano has worked in the information technology field for more than 20 years, 12 years focused on cybersecurity. Mr. Montemarano has a degree from George Mason University and a Masters in Information Security from the University of Maryland University College.

Dale Spoljaric currently is Managing Director with the National Futures Association, where he helps oversee the compliance department's examination, investigation, financial surveillance, and risk management programs. Prior to his current role, Mr. Spoljaric was US Head of Agency Derivative Services Compliance at Barclays Capital Inc. where he led a team of compliance professionals covering futures, cleared swaps, and FX prime brokerage. He also spent time as a Control Officer with JP Morgan Securities in the F&O and Cleared OTC Operations group. He began his career in the futures industry with Chicago Mercantile Exchange where he conducted audits of clearing member FCMs. Mr. Spoljaric earned a Bachelor of Science degree with a double major in Accounting and Information Technology from Marquette University in Milwaukee, Wisconsin. He's also a registered CPA in Illinois and Certified Fraud Examiner.

2020 FINRA Cybersecurity Conference

January 14, 2020 | New York, NY

Cybersecurity the Current Regulatory Environment:

Insight from Regulators and Industry Experts

FINRA®

Panelists

- Moderator
  - David Kelley, Surveillance Director, Kansas City Office, FINRA Member Supervision
- Panelists
  - Gregory Markovich, Regulatory Principal, Chicago District Office, FINRA Member Supervision
  - Salvatore Montemarano, Senior Specialized Examiner - Information Technology, Technology Controls Program, Office of Compliance Inspections and Examination (OCIE), U.S. Securities and Exchange Commission (SEC)
  - Dale Spoljaric, Managing Director, Compliance, National Futures Association (NFA)

FINRA

2020 FINRA Cybersecurity Conference

January 14, 2020 | New York, NY

Closing Remarks
Tuesday, January 14, 2020
4:40 p.m. – 4:45 p.m.

Speaker: Steven Randich
Executive Vice President, Chief Information Officer
FINRA Office of the Chief Information Officer

Speaker Biography:

Steven J. Randich, Executive Vice President and Chief Information Officer (CIO), oversees all technology at FINRA. Previously, Mr. Randich served as Co-CIO at Citigroup, and CIO and Global Head of Technology for Citigroup's Institutional Clients Group. Prior to joining Citigroup, he was Executive Vice President of Operations and Technology and CIO at NASDAQ, where he was responsible for all aspects of NASDAQ technology, including applications development and technology infrastructure. From 1996 to 2000, Mr. Randich served as Executive Vice President and CIO for the Chicago Stock Exchange. He was responsible for all technology, trading-floor and back-office operations, and business product planning and development. Prior to joining the Chicago Stock Exchange, Mr. Randich was a Managing Principal at IBM Global Services and a Manager at KPMG. Mr. Randich has an undergraduate degree in computer science from Northern Illinois University and an M.B.A. from the University of Chicago.

Closing Remarks

Speaker

- Speaker
  - Steven Randich, Executive Vice President, Chief Information Officer, FINRA Office of the Chief Information Officer