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

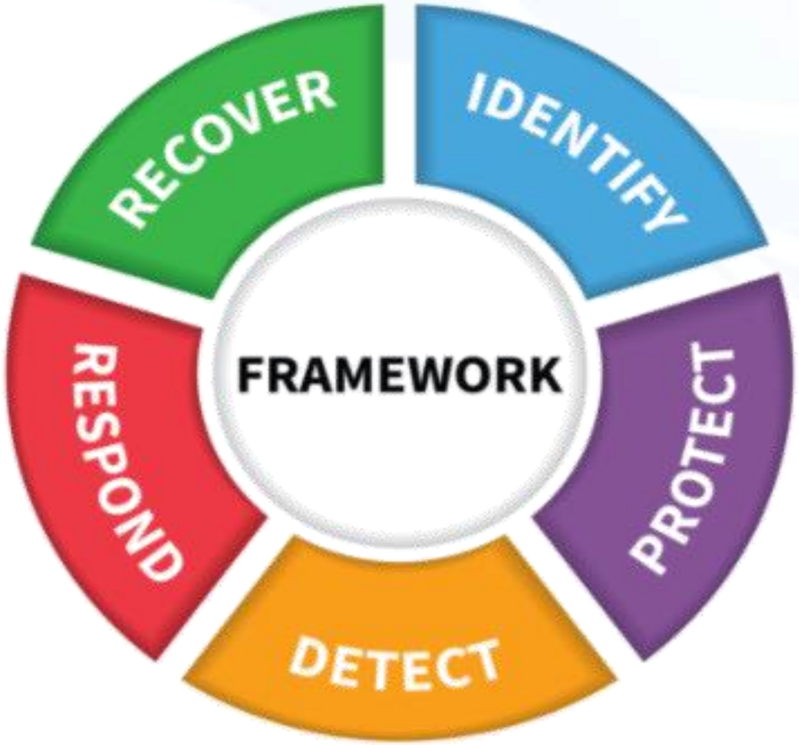
Risk Based Approach to Cybersecurity

- 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

Copyright 2020 FINRA Cybersecurity Conference

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

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.

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:

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

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:

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:

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:

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

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

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:
