Financial Industry Regulatory Authority

Small Firm Conference

Santa Monica, CA | November 11 – 12, 2015

Decode Cyber Risks and Security
Thursday, November 12
1:45 p.m. – 2:45 p.m.

This session provides an overview of the latest cybersecurity threats that small firms face, and provides preventative measures firms can take to protect their practice. Join industry panelists and FINRA staff as they share effective practices to protect your firm's data. Panelists discuss real-life examples of cyber breaches and lessons learned.

Moderator:
David Kelley
Surveillance Director
FINRA Kansas City District Office

Panelists:
Joe Romano
President
Romano Brothers & Co.

Lisa Roth
President
Monahan & Roth, LLC

Decode Cyber Risks and Security Panelist Bios:

Moderator:

David Kelley is the Surveillance Director based out of their Kansas City District office, and has been with FINRA for more than five years. Mr. Kelley also leads FINRA's Regulatory Specialist team for Cyber Security, IT Controls and Privacy. Prior to joining FINRA, he worked for more than 19 years at American Century Investments in various positions, including Chief Privacy Officer, Director of IT Audit and Director of Electronic Commerce Controls. He led the development of website controls, including customer application security, ethical hacking programs and application controls. Mr. Kelley is a CPA and Certified Internal Auditor, and previously held the Series 7 and 24 licenses.

Panelists:

Joe Romano is President of Romano Brothers & Co., a dually registered RIA/BD founded by his father Richard Romano in 1962, which now manages $1 billion in client assets. In addition to administering the firm, Mr. Romano heads its Investment Committee and acts as a portfolio manager, creating customized portfolios for private clients using individual stocks and bonds. He began his career in 1995 earning his Series 7 General Securities and Series 55 Equity Trading licenses. He later obtained the Series 24 General Securities Principal and Series 4 Registered Options Principal licenses. He served for several years until 2007 as the firm's Chief Compliance Officer (CCO). Mr. Romano is a past President of the Illinois Securities Industry Association and a former member of the FINRA District 8 (Midwest) Committee from 2009-2012. He then became a member of the FINRA Small Firm Advisory Board and served as its Chair in 2015. Most recently in August of 2015 he was elected by his constituency to serve a three year term as a Small Firm representative on the FINRA Board of Governors. Mr. Romano graduated with honors in economics from Wesleyan University, Middletown, CT, in 1992.

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

Small Firm Conference

November 11-12, 2015 | Santa Monica, CA

Decode Cyber Risks and Security

FINRA

Panelists

Moderator:

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

Panelists:

- Joe Romano, President, Romano Brothers and Company
- Lisa Roth, President, Monahan & Roth, LLC

Outline

I. FINRA's Definition of Cybersecurity
II. Governance
III. Risk Assessment
IV. Access Control
V. Vendor Management
VI. Incident Response Plan
VII. Training
VIII. Branch Controls
IX. Technical Measures

What do we mean by “Cybersecurity”?

- **In broad terms we mean the protection of investor and firm information from compromise through the use – in whole or in part – of electronic media (e.g., computers, cell phones, IP-based telephony systems).**
  - **“Compromise” refers to a loss of data confidentiality, integrity or availability**
  - **Protection of customer information and PII (Personal Identifiable Information)**
  - **Protection of firm confidential information**

Governance

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

- **Active senior management and, as appropriate, board level oversight of cybersecurity**
- **Articulated risk appetite that guides firm decision-making with respect to the acceptance, mitigation, avoidance or transfer of risks**
- **Defined accountabilities, structures, policies and procedures to support decision-making based on risk appetite and industry effective practices**
- **Use of appropriate metrics and thresholds**

Risk Assessment

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

- **What is a risk assessment?**
  - As defined by the International Organization for Standardization (ISO), risk assessment is a systematic approach to estimating the magnitude of risks (risk analysis) and comparing risk to risk criteria (risk evaluation). It is an ongoing process, not a single point-in-time review
- **Scope of a risk assessment**
  - Critical asset inventory
  - Threat evaluation – both external and internal
  - Vulnerability assessment of assets
  - Risk evaluation and prioritization – governance
  - Technical Controls
  - Vendors and their Affiliates

Access Control

Principle: Physical and logical - Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.

- **Access permissions are managed, incorporating the principles of least privilege and separation of duties**
- **Identities and credentials are managed for authorized devices and users**
- **Physical access to assets is managed and protected**
- **Remote access is managed**
- **Password rules are appropriate**

Vendor Management

Principle: Firms should address cybersecurity risks that arise from vendor relationships.

- **Vendor management should cover the lifecycle of the relationship, from initiation through termination, and should be risk-based, i.e., there is greater due diligence and oversight on vendors who have access to sensitive data or processes.**
- **Appropriate initial and ongoing due diligence**
- **Incorporation of appropriate contractual requirements**
- **Include vendors and vendor systems as part of the overall risk assessment process**
- **Cloud Computing applications – understanding segregation of data and controls around access**
- **Firms should conduct ongoing vendor re-assessments**

Incident / Breach Response Planning

Principle: Firms should develop plans to respond to cybersecurity incidents. Key elements include:

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

Training

Principle: Firms should provide cybersecurity training to their staff and provide additional training based on staff's role.

- **Appropriate types of training are driven by:**
  - Staffs' functional responsibilities:
    - Training on fraudulent money transfer schemes for account reps
    - Training on secure coding practices for developers
  - Firm's experience with cybersecurity incidents, such as loss incidents
  - Risk assessment
  - Awareness and intelligence about threats firm may face
- **In addition, firms should also consider providing resources to customers that will help them enhance their own cybersecurity practices**

Branch Office Controls

Firms with an Independent Contractor branch model may have more risk due to the nature of the branch technology infrastructure.

- **Control Areas would include:**
  - The use of passwords
  - Physical security of assets and data
  - Encryption of computers
  - Use and storage of email
  - Transmission of data
  - Incident reporting of lost or stolen data and hardware
  - Patch and virus protection processes
  - Firm branch exams
  - RR training and certification

Technical Measures

There are a number of technical measures firms take to enhance their cybersecurity controls.

Anti-virus software	Anti-malware software
Application firewalls	Identity, access and privilege management
Data encryption	DDOS tools
Patch and software updates	Email content filtering
Web/URL filtering	Use of removable media
Penetration (PIN) testing	WiFi protection
BYOD	Online Access Management

Handouts

- Outsourcing Due Diligence Form
- Electronic Devices and Communications Inspection Form
- Cyber Security Incident Report
- Bring Your Own Device Policy Development and Implementation Outline
- Cybersecurity Terminology

Supplemental Guidance

- FINRA Report on Cybersecurity - *http://finranet.finra.org/news-events/employee-news/announcements/FINRA-Releases-Report-on-Cybersecurity-Practices*
- NIST - *www.nist.gov/cyberframework/index.cfm*.
- COBIT 5 - *www.isaca.org/COBIT/Pages/COBIT-5-Framework-product-page.aspx*
- ISO 27001/27002 - *www.iso.org/iso/home/standards/management-standards/iso27001.htm*
- SIFMA Cybersecurity Resource Center: *www.sifma.org/issues/operations-and-technology/cybersecurity/overview/*
- FFIEC cybersecurity resources for banking organizations: *http://www.ffiec.gov/cybersecurity.htm* AND *http://www.ffiec.gov/cybersecurity.htm*
- *www.sec.gov/rules/final/34-42974.htm*
- *www.sec.gov/rules/final/2013/34-69359.pdf*
- *www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx*
- *www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx*
- *www.sec.gov/rules/final/34-44992.htm*
- *www.fsisac.com/*
- *www.ncfta.net/*

OUTSOURCING DUE DILIGENCE FORM

SERVICE TO BE OUTSOURCED

1. **Type of service to be outsourced:**
   - ☐ Accounting/Finance: _____ ☐ Compliance Consulting: _____
   - ☐ Legal Services: _____ ☐ Administrative Functions: _____
   - ☐ Information Technology: _____ ☐ Operations/Support Functions: _____
   - ☐ Other: _____

2. Is this service essential to the operation of the Firm (i.e. transaction order entry; custody and prime brokerage; service designed to promote rapid recovery of operations etc.)? ☐ Yes ☐ No

APPROPRIATENESS OF OUTSOURCING

1. **Potential impact on Firm if service provider fails to perform:**

Financial Impact:	☐ High	☐ Medium	☐ Low	☐ N/A
Reputational Impact:	☐ High	☐ Medium	☐ Low	☐ N/A
Operational Impact:	☐ High	☐ Medium	☐ Low	☐ N/A
Customer Service Impact:	☐ High	☐ Medium	☐ Low	☐ N/A
Potential Losses to Customers:	☐ High	☐ Medium	☐ Low	☐ N/A
Comply with Regulatory Requirements:	☐ High	☐ Medium	☐ Low	☐ N/A
Costs to Firm:	☐ High	☐ Medium	☐ Low	☐ N/A
Degree of Difficulty Replacing Service Provider:	☐ High	☐ Medium	☐ Low	☐ N/A

Comments:

2. Is there an affiliation or other relationship between the Firm and the service provider? ☐ Yes ☐ No
   If yes, please describe the relationship and any potential conflicts of interest:

3. Is the service provider a regulated entity subject to independent supervision or jurisdiction? ☐ Yes ☐ No
   If yes, name of regulator: _____

SERVICE PROVIDER INFORMATION

1. **General Information**
   Vendor Name:
   _____

   Vendor Address:
   _____

   _____

   Contact Name(s): _____ CRD # (if applicable): _____
   Phone: _____ Fax: _____ Website: _____

2. Is the service provider owned/controlled by a Parent Co.? ☐ Yes ☐ No Name: _____

3. **Personnel:**
   Approximate # of employees:_____
   Does the service provider hire independent contractors? ☐ Yes ☐ No

4. **Background Information:**
   How many years has the service provider been in business? _____
   How many years has the service provider provided the outsourced function? _____

   Is the service provider known to the Firm or employees of the Firm? ☐ Yes ☐ No
   If yes, please name the individual(s) and describe any prior experience each had with the service provider:
   _____
   _____

DUE DILIGENCE

1. What methods did the Firm use to verify the service provider's information? (Choose all that apply.)

☐ FINRA Public Disclosure	☐ Internet Research	☐ Entity Formation Documents
☐ SEC Public Disclosure	☐ Credit/Background Check	☐ Independent Research
☐ Form BD/ADV	☐ Media/News Reports	☐ Personal Referral
☐ Business Plan	☐ 10K	☐ RFP
☐ Policies Manual(s)	☐ Personal Interviews	☐ Marketing Materials
☐ Financials	☐ Onsite Inspection	☐ Sales Materials
☐ Other:		

_____

Identify where this evidence is maintained of the above methods used to verify the service provider's information (i.e. copies of documents reviewed; notes from personal interviews and onsite inspections; printouts from public disclosure sites etc.)?

2. Please list one or more qualified references; firms that use this service (if contacted personally, identify the name of the contact and the result of the contact):

1.
2.
3.

3. Please describe the background and experience of individuals who will be performing the services:

4. Based on your review of reference and background information, has/have the service provider and/or its principals been subject to any regulatory, criminal or civil disciplinary issues? ☐ Yes ☐ No
   If yes, please describe:

5. Based on your review of reference and background information, please describe the service provider's ability and capacity to perform the outsourced activities effectively, reliably, and to a high standard (include in your description relevant technical, financial, human resources, and/or other assets of the service provider):

6. Confirm that the service provider has an adequate information security plan in effect. ☐ Yes ☐ No

   If yes, review a copy of the plan and comment on its adequacy including at minimum standards for compliance (NIST or other) and method(s) for breach reporting and mitigation:

7. Will the service provider have access to non-public information? ☐ Yes ☐ No

If yes, comment on the adequacy of the service provider's for safeguarding non-public information:

8. After reviewing the information, are there any questionable issues or potential conflicts of interest?
   ☐ Yes ☐ No
   If yes, please describe:

CONTRACTS AND AGREEMENTS

1. Has (or will) the Firm entered into a written agreement with the service provider? ☐ Yes ☐ No
   If yes, please identify the relevant provisions and disclosures in the contract (choose all that apply).

   ☐ Provides for Firm and regulator access to records
   ☐ Limitations on service provider's ability to sub-contract
   ☐ Defines responsibilities of all parties subject to contract
   ☐ Defines how responsibilities will be monitored
   ☐ Liability for unsatisfactory performance or other breach
   ☐ Requirement to maintain a disaster recovery plan
   ☐ Time Commitment (Termination Date):
   _____
   ☐ Other relevant provision(s):
   _____
   ☐ Firm and client confidentiality
   ☐ Payment arrangements
   ☐ Provide quality services measures
   ☐ Guarantees and indemnities
   ☐ Information security provisions
   ☐ Disclosure of breaches in security

2. Was the written agreement reviewed by the Firm's legal counsel? ☐ Yes ☐ No ☐ N/A
   If yes, name of legal counsel: _____
   Date of Review: _____

3. Was the written agreement reviewed by the principal responsible for outsourcing functions?
   ☐ Yes ☐ No
   If yes, name of principal: _____ Date of Review: _____

OVERSIGHT AND PERIODIC REVIEW

1. List the name and title of the Firm Principal who is responsible for the periodic oversight and review of the outsourced service? _____

2. Please identify the individual(s) who will monitor the outsourced service if different from above.
_____

3. Please identify the tools that will be used to monitor the outsourced service:

☐ Service delivery reports prepared internally
☐ Publicly available resources
☐ Internal auditor
☐ External auditor
☐ Other
☐ Service delivery reports supplied by the service provider
☐ Performance levels established in written agreement
☐ Onsite inspection
☐ Attestations by service provider

_____

4. Frequency of monitoring: ☐ Daily ☐ Weekly ☐ Monthly ☐ Quarterly ☐ Annually
☐ Other
_____

5. If deficiencies are found, are there procedures in place to respond to such deficiencies (i.e. communicate with the service provider; terminate the contract)? ☐ Yes ☐ No

DOCUMENTATION REVIEW AND APPROVAL

1. Individual(s) responsible for completing this due diligence review:
   a. _____
   b. _____
   c. _____

Firm Principal: I have reviewed the information contained in this Outsourcing Due Diligence Form and:

☐ The Firm has elected to use the service provider above.

☐ The Firm will not use the service provider above.

_____ _____ _____
Principal Signature Date Printed Name of Principal

Electronic Devices and Communications Inspection Form

Electronic Device Review:

Device Name	Description	% Business Use	% Personal Use

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

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

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

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

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

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

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

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

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

Exceptions, Notes:

Electronic Device Review:

Device Name	Description	% Business Use	% Personal Use

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

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

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

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

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

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

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

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

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

Exceptions, Notes:

Cyber Security Incident Report

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

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

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

If (other) please describe:

Date detected: _____ Date Remediated: _____

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

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

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

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

Report Submitted by: _____ Date: _____

Report Reviewed by: _____ Date: _____

Bring Your Own Device ("BYOD")

Policy Development and Implementation Outline

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

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

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

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

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

Financial Industry Regulatory Authority

Small Firm Conference

Santa Monica, CA | November 11 – 12, 2015

Cybersecurity Terminology Defined

- Access controls (including employees): controls to certain assets based on least privilege, and is limited to authorized users, processes, or devices, and to authorized activities and transactions.
- Application Software Security: measures taken throughout the code's life-cycle to prevent gaps in the security policy of an application or the underlying system through flaws in the design, development, deployment, upgrade, or maintenance of the application.
- Assets, including inventory process: Identify PII of employees, customers, or other individuals that may be impacted by or connected to cybersecurity procedures, including systems, applications; e.g. define the firms "Crown Jewels"
- Authorized v. Unauthorized Devices: authorized devices can be laptops, mobile phones, tablets which are configured within firm policy. Unauthorized devices might be USB, removable storage devices.
- Availability of the website: Websites can go down due to website defacement attacks.
- Boundary Defense: protection of configuration and architectural frameworks; the perimeter systems, network devices, and Internet-facing client machines.
- Breach: system has been compromised; loss of data, confidential firm and/or client information
- Change Management: – is the management of technical security solutions to ensure the security and resilience of systems and assets are consistent with related policies and procedures and agreements.
- Cybersecurity architectures and industry models include NIST, COBIT 5, OSO/IEC 27001/2. Refer to the references section for hyperlinks to additional resources.
- Cybersecurity Governance: The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental and operational requirements are understood and inform the management of cybersecurity risk.
- Data recovery capability: defined backup and restore services
- Data security programs: policies and procedures that outline protection of PII and other confidential firm data.
- Distributed denial of services attacks/incidents
- Hack of wireless network: This is usually caused by poor configuration and those caused by weak encryption.
- Incident response planning and recovery: This is the process of capturing, classifying, and remediating events. Depending on the nature and severity, might be updated in a firm's BCP/DR plans.

- Information Sharing: sharing known threats/attacks with various organizations; e.g. FS-ISAC, NCFTA, local Law Enforcement Authorities
- Limitation and Control of network ports, protocols and services: secure socket layers (SSL) are cryptographic protocols designed to provide communications security over a computer network.
- Malware defined and defenses: malicious software that may be blocked with tools such as McAfee, Kaspersky, Norton, TrendMicro, etc.
- Password sniffing: software application that scans and records passwords that are used or broadcasted on a computer.
- Patch Management: the process to deploy updates from vendor applications, and systems addressing known deficiencies in code, networks, devices.
- Penetration Tests: is an attack on a computer system with the intention of finding security weaknesses, potentially gaining access to it, its functionality and data. The process involves identifying the target systems and the goal, then reviewing the information available and undertaking available means to attain the goal. A penetration test target may be a white box or black box. A penetration test can help determine whether a system is vulnerable to attack, if the defenses were sufficient and which defenses were defeated in the penetration test.
- Personally Identifiable Information ("PII") – any information about an individual maintained by an agency, including any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, etc.
- Phishing: is the attempt to acquire sensitive information such as usernames, passwords, and other PII details by masquerading as a trustworthy entity in an electronic communication.
- Red team exercises: finding network threats before hackers do.
- Secure Configurations for hardware and software: appropriate safeguards are in place at all stages of PII's lifecycle within the organization
- Secure Network Engineering: Threats and vulnerabilities are assessed and monitoring and control processes in place to ensure protection of PII.
- Social engineering or social hacking: manipulation of people into performing actions or divulging confidential information.
- SSAE 15: certification that controls are in place and are designed and operating effectively.
- System Development Lifecycle: the process workflow of a change to the technology environment; Scope through Implementation.
- System Penetration: attack on a computer system with the intention of finding security weaknesses, potentially gaining access to it.
- Table-top exercise: A discussion-based exercise where personnel meet in a room or breakout groups and are presented with a scenario to validate the content of plans, procedures, policies, cooperative agreements or other information for managing an incident.
- Technology Framework: depending on the business model, the platform in which technology monitors and controls the firm's assets; e.g. applications, systems, data, servers, network, workstations, other devices
- Vendor management process, including controls, audit and termination clauses: process for selecting, monitoring, and terminating relationships with vendors who have access to customer PII or company confidential information.

- Vulnerability Assessment and Remediation: regularly evaluate the effectiveness of procedures detecting vulnerabilities in applications and systems, and remediate known deficiencies
- Website defacement: an attack on a website that changes the visual appearance of the site or a webpage. These are typically the work of system crackers, who break into a web server and replace the hosted website with one of their own.
- Wireless access controls: access controls that might require a fob – such as an RSA fob.

[Firm Name]
Cyber Security Policies and Procedures
September 2015

CONTENTS

OVERVIEW 2

ACCESS MANAGEMENT 3

END-USER: MOBILE DEVICE AND APPLICATION SECURITY 5

COLLABORATION SITES AND END-USER DATA STORAGE 6

SECURITY RISK ASSESSMENT 7

EMPLOYEE SECURITY AWARENESS TRAINING 8

VENDOR SELECTION AND MANAGEMENT 9

TECHNOLOGY ASSET INVENTORY, CLASSIFICATION AND TRACKING 9

TECHNOLOGY END-OF-LIFE PROCESS 10

EMPLOYEE TERMINATION 10

DISASTER RECOVERY AND BACKUP TESTING 11

CYBERSECURITY INSURANCE 11

CYBERSECURITY BREACH FRAMEWORK 11

Overview

[Firm Name] has a holistic, systematic and risk-based approach to technology and information security. At a high level, the goal of this program is to:

- Provide that the business takes action relevant to the firm's technology assets and related events
- Provide for the safety and protection of information
- Prevent inappropriate use or access to data that can lead to an information security incident, where any firm computer, device or data is lost, stolen, misused or left unsecured
- Minimize the impact of adverse information security events to the portfolio, and therefore the investors of the fund

[Name] has been designated as the Chief Information Security Officer ("CISO") and has primary oversight, maintenance, and execution of this Technology and Information Security Program (the "Program"). The CISO is authorized to delegate physical, technical, and administrative components of this program to qualified third parties as and whenever appropriate.

The [Firm Name] CCO bears overall responsibility for Business Continuity Plan ("BCP") / Disaster Recovery ("DR") planning, information protection, and creating agile security processes and procedures. The CCO has identified the following core functions to guide the Program. These functions will be evaluated and updated by the CISO as indicated below to adjust to technological, business and/or operational changes at the firm that may have a material impact on the Program. The CISO will also be reporting any exceptions to the COO, CEO or other management as appropriate.

Functions	Designated Person	Frequency of Document Review	Frequency of Execution
Access management: password and technology access	CISO	Quarterly	As needed
Access management: physical access	CISO	Quarterly	As needed
End-user: desktop, web, network and server security	CISO	Quarterly	As needed
End-user: mobile devices and application security	CISO	Quarterly	As needed

Collaboration sites and storage networks	CISO	Quarterly	Quarterly with 3rd Party
Security risk assessment	CISO	Annually	Annually with RSI Technologies
Cybersecurity testing and audit	CISO	Annually or as needed	Annually or as needed with RSI Technologies
Network intrusion scan	CISO	Annually	Ongoing with 3rd Party
Employee security awareness training	CISO	Annually	Annually (CCO during ACM)
Vendor selection and maintenance	COO	As needed	Ongoing with 3rd Party
Technology asset inventory	CISO	Annually	Annually
Technology end-of-life process	CISO	Annually	As needed with 3rd Party
Employee termination	COO	Annually	As needed with CCO
Disaster recovery and backup testing	COO	See BCP/DR Manual	See BCP/DR Manual
Cybersecurity insurance	CISO	Upon renewal	N/A as of 9.2015

Access Management

We have a rigorous 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
- Provide transparency and up-to-date information on entitlements
- Provide centralized administration for permissions
- 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 that will be used to create, delete and modify employee access data. The CCO is the primary owner of the central directory.

Authorization: We will manage authorization information that defines what functions an employee can perform in the context of a specific application. Please consult the CCO for the complete directory of employees and associated applications.

Passwords: For accessing any firm desktop or device, employees will use unique passwords, requiring the following characteristics:

- Contains at least 8 characters
- Uses a combination of lower and uppercase letters
- Uses at least one number and one symbol
- Expires every 180 days (the reuse of any previous password is disallowed)
- After 10 failed login attempts within 15 minutes, the user account will be locked until released by the CISO or 3rd Party.

Each administrator will have a unique login account and password

3rd Party's employees, on an as needed basis, will each have a unique login and password to access the firm's password management list.

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

End-user: desktop, web, network and server security
We have developed practices in our firm to protect the sensitivity of all information by implementing the following processes:

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

• Reconcile the inventory of hardware, software and devices with 3rd Party

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

• Track and log USB portable flash drive uses that access the firm's desktop to detect any unauthorized use

• Maintain white-list of desktop approved applications and blacklist policy for websites (i.e. adult content, social media, gambling, etc.)

Working closely with the CISO, 3rd Party will proactively manage the following items:

• Maintain inventory of hardware, software and devices

• Closely monitor application and systems log activity (i.e. control the execution of code with an application white-listing policy)

• Deploy critical operating system security patches within 48 hours of release

• Non-critical patches are delivered monthly

• Implement appropriate protections for electronic systems, including anti-virus software and firewalls

• Anti-virus software is set to auto-update and firewalls are updated at least quarterly by 3rd Party

• To combat social engineering, the 3rd Party will do the following:

– Employ up-to-date anti-malware systems (continuously updated by auto-update plus quarterly reviews)

– Employ spam filters and other email gateways (continuously updated by auto-update and periodically reviewed by 3rd Party)

End-user: mobile device and application security

Firm-owned devices include, but are not limited to, laptops, tablets, cellular phones, and smartphones. Personal devices may utilize mobile access as long as they are password-encrypted and firm-approved. At the time of hiring, and annually thereafter, we request 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 to the CISO or CCO immediately. The CISO or CCO will update the firm inventory and shut off inbound and outbound access to the device as necessary. 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.

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:
[NO APPROVED SITES CURRENTLY IN USE]

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 only in an approved, sandboxed or otherwise encrypted location instead of the desktop

• Save information to be shared to an access-controlled network location such as a network shared drive

• Store data and information with retention requirements in a records management repository

• Only use applications obtained through firm-approved channels

Mobile devices (smart phones and tablets)

• Only store data within firm-approved applications

• [Firm Name] intends to have remote-wipe capability for all employee devices

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

The firm will use an independent 3rd party to perform a comprehensive enterprise risk assessment. The 3rd party will assess any potential or existing cyber-security threats to identify potential risks and business impacts. The following items under review include, but are not limited to:

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.

Employee security awareness training will include, but is not limited to:

• 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

– Avoid the use of speaker phones and discourage discussions in public areas

– Recognize any 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 our systems, network and data, the firm will perform the following activities to protect sensitive information:

• Assess vendors before working with them including a 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

Technology asset inventory, classification and tracking

[Firm Name] has a process in place to identify, classify, and track all technology assets ("assets"):

• To ensure accurate classification and tracking, we will procure/vet all assets through 3rd Party

• We will maintain an inventory of all assets as well as an identified owner

• We will cross-reference the list of internal assets with 3rd Party

• Asset identification and classification process will be scalable to accommodate growth and acquisition

• We will track assets and their attributes throughout their lifecycle

• Automated processes will be used periodically to perform discovery of unknown assets

• We will create a map of network resources, including data flows, internal connections and external connections

We will establish and enforce a process of assessing and classifying assets based on their sensitivity to attack and business value.

3rd Party will auto-alert [Firm Name] if a new device is discovered on the network

Technology end-of-life process

We have 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").
Working closely with the CISO, 3rd Party will closely monitor the firm hardware and recommend a refresh every 3-5 years per individual hardware equipment. A certified end-of-life management vendor ("EMV") will properly recycle any old hardware.

Notification: The end-of-life process will notify all necessary and relevant parties to initiate a coordinated execution:

- CISO
- Asset owner
- End user(s)
- Relevant vendor(s)

Hard Drives: Any decommissioned hard drive will be securely stored for a minimum of 6 years since decommission date. When disposing the hard drive, the EMV will do the following:

- Erase all data on the drive
- Physically destroy the hard drive
- Produce documentation of proper disposal

Employee termination

The firm is highly focused on protecting the network and proprietary data at risk upon termination of employees. To prevent any issues of former employees leaking information, we have a strict approach towards access controls and entitlement management.
Please refer to the 3rd Party checklist for employee on/off-boarding. We will continuously maintain this list as new applications, drives, systems, and vendors are incorporated. The following items will be monitored:

- Network access
- Desktop access
- Mobile device access

• Internal and external applications

• Vendors, such as prime brokers, executing brokers, etc.

Disaster recovery and backup testing

Please see the original Business Continuity Procedures / Disaster Recovery Plan ("BCP") for detailed documentation. Any changes can be represented in that BCP / DR plan.

The CCO in connection with the CISO will update the firm's BCP on an as-needed basis to ensure that it is consistent with the Program.

Cybersecurity insurance

On an annual basis the CISO will review the firm's insurance coverage related to cybersecurity threats and make a determination 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 the majority of client sensitive data are retained by competent third party vendors primarily including its clearing firm.

Cybersecurity breach framework

The firm has implemented a framework to identify, prepare, prevent, detect, respond, and recover from cybersecurity incidents.

In the event of a cybersecurity incident, the firm's information technology personnel (or anyone detecting the incident) will immediately notify the CISO (or 3rd Party Fishell) who will work with appropriate personnel to:

• 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 and make a determination regarding disclosing 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 in light of the breach

• The firm will work with 3rd Party and outside counsel as necessary to determine appropriate next steps

Financial Industry Regulatory Authority

Small Firm Conference

Santa Monica, CA | November 11 – 12, 2015

Decoded Cyber Risks and Security
Thursday, November 12
11:30 a.m. – 12:30 p.m.

Resources

FINRA Resources

- *FINRA Report on Cybersecurity*

  http://finranet.finra.org/news-events/employee-news/announcements/FINRA-Releases-Report-on-Cybersecurity-Practices

SEC Resources

- *Identity Theft Red Flags Rules* (April 2013)

  http://www.sec.gov/rules/final/2013/34-69359.pdf

- *Books and Records Requirements for Brokers and Dealers Under the Securities Exchange Act of 1934* (May 2003)

  http://www.sec.gov/rules/final/34-44992.htm

- *Privacy of Consumer Financial Information (Regulation S-P)* (November 2000)

  http://www.sec.gov/rules/final/34-42974.htm

Other Resources

Federal Financial Institutions Examination Council (FFIEC) Cybersecurity Resources

- Cybersecurity Awareness

  http://www.ffiec.gov/cybersecurity.htm

NIST Resources

- Cybersecurity Framework

  http://www.nist.gov/cyberframework/index.cfm

National Conference of State Legislatures Resources

- State Laws Related to Internet Privacy

  http://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx

- Security Breach Notification Laws

  http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx

SIFMA Resources

- Cybersecurity Resource Center

  http://www.sifma.org/issues/operations-and-technology/cybersecurity/overview/

Information Systems Audit and Control Association

- COBIT 5 Framework

  http://www.isaca.org/COBIT/Pages/COBIT-5-Framework-product-page.aspx

International Organization for Standardization

- ISO/IEC 27001 - Information Security Management

  http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

Financial Services Information Sharing and Analysis Center

- FSISAC main webpage

  http://www.fsisac.com/

National Cyber-Forensics & Training Alliance

- Cracking Down on Cyber Crime

  http://www.ncfta.net/

