2020 FINRA Cybersecurity Conference
January 14, 2020 | New York, NY

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

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

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

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

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

Len Smuglin
IT Examination Manager
FINRA Member Supervision

Detect: Detecting Threats in a Timely Manner Panelist Bios:

Moderator:

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

Speakers:

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

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

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

2020 FINRA Cybersecurity Conference

January 14, 2020 | New York, NY

Detect:

Detecting Threats in a Timely Manner

Panelists

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

To Access Polling

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

AGENDA

01 | NIST Cybersecurity Framework (CSF)

02 | Detect Function

03 | Baselines

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

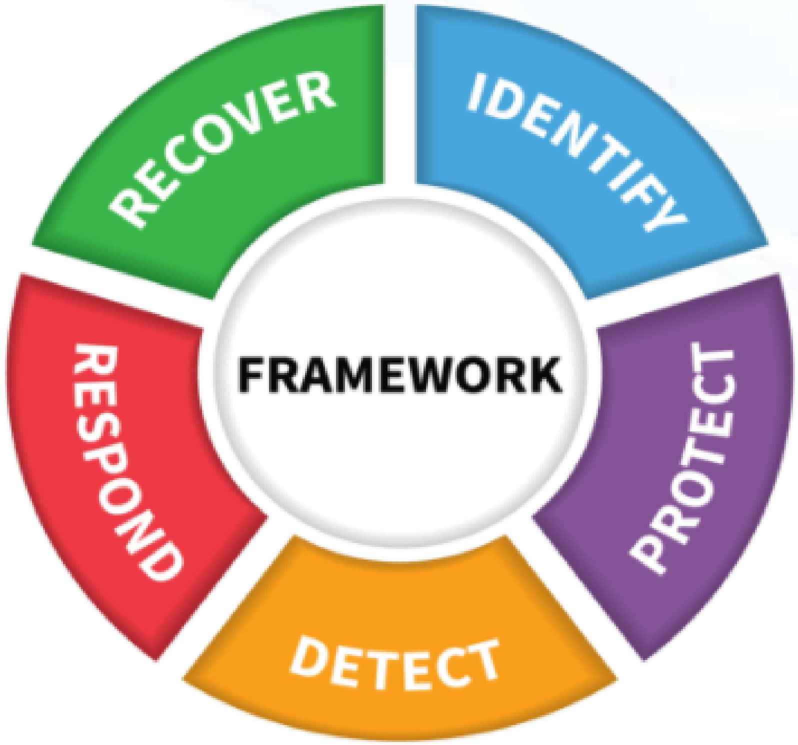
05 | Insider Risk

06 | Resources

07 | Q&A

NIST Cybersecurity Framework (CSF)

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



Detect Function Defined

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

Detect – Anomalies and Events

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

Detect – Anomalies and Events: Baselines

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

Poll Question 1: Baselines

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

Detect – Monitoring

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

Detect – Supporting Processes

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

Poll Question 2: Monitoring

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

Considerations for Continuous Security Monitoring

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

Components of Continuous Security Monitoring

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

Poll Question 3: Third Party Providers

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

Security Monitoring of Third Party Providers

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

Poll Question 4: Insider Risk Detection

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

Insider Risk – Common Types[1]

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

[1] – 2019 Verizon Data Breach Report

Insider Risk – Monitoring Tools

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

[1] – 2019 Verizon Data Breach Report

Resources

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

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

Q
A

FINRA®

2020 FINRA Cybersecurity Conference

January 14, 2020 | New York, NY

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

Resources

FINRA Resources

- FINRA's Cybersecurity Webpage

  www.finra.org/industry/cybersecurity

- 2018 Report on Selected Cybersecurity Practices

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

- 2015 Report on Cybersecurity Practices

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

- Small Firm Cybersecurity Checklist

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

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

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

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

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

- Non-FINRA Cybersecurity Resources Webpage

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