2020 FINRA Cybersecurity Conference

January 14, 2020 | New York, NY

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

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

Moderator:

Kevin Bogue
Regulatory Principal, Chicago District Office
FINRA Member Supervision

Speakers:

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

Paul Nickelson
Director, Cyber Fusion Center
TD Ameritrade

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

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

Moderator:

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

Speakers:

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

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

2020 FINRA Cybersecurity Conference

January 14, 2020 | New York, NY

Respond and Recover:

Recovery Plan – Minimizing the Damage

Panelists

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

To Access Polling

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

AGENDA

01 | NIST Cybersecurity Framework (CSF)

02 | Respond Function

03 | Respond Categories

04 | Recover Function

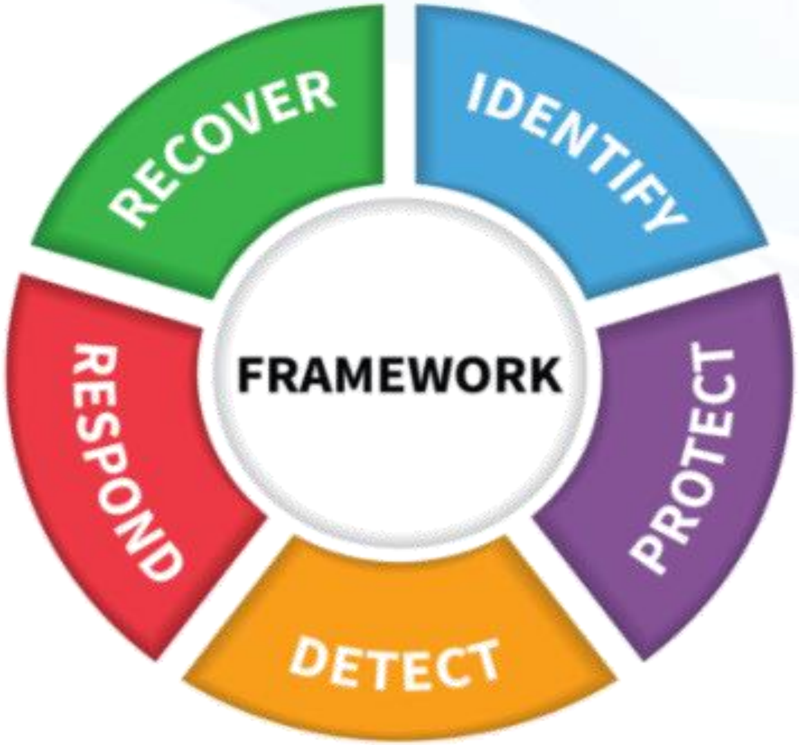
05 | Recover Categories

06 | Resources

Copyright 2020 FINRA Cybersecurity Conference

NIST Cybersecurity Framework (CSF)

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



Poll Question 1: Incident Response Plan

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

Respond Function Defined

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

Respond – Response Planning

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

- Response plan is executed during or after an incident

Respond – Communications

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

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

Respond – Analysis

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

Respond – Mitigation

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

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

Respond – Improvements

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

- Response plans incorporate lessons learned
- Response strategies are updated

Poll Question 2: Recovery Plan

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

Recover Function Defined

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

Recover – Recovery Planning

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

- Recovery plan is executed during or after a cybersecurity incident

Recover – Improvements

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

- Recovery plans incorporate lessons learned
- Recovery strategies are updated

Recover – Communications

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

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

Resources

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

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

Q
A

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

Resources

FINRA Resources

- FINRA's Cybersecurity Webpage

  www.finra.org/industry/cybersecurity

- 2018 Report on Selected Cybersecurity Practices

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

- 2015 Report on Cybersecurity Practices

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

- Small Firm Cybersecurity Checklist

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

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

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

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

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

- Non-FINRA Cybersecurity Resources Webpage

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