EXCHANGE ANALYTICS
Regulatory Compliance Solutions

Cybersecurity - Refresher Course 2025

Course Outline and Provider Qualifications

The Exchange Analytics Cybersecurity - Refresher Course is designed to enhance understanding of cybersecurity risks, emerging trends, regulatory requirements, and best practices. Tailored for staff at U.S.-based financial firms with prior cybersecurity fundamentals training, this course introduces role-based learning to optimize the user experience. **Content is customized for three distinct role types**, ensuring a focus on the cybersecurity issues most relevant to each role. Select **Option 1** if you work in the front office and/or first line of defense, such as: traders, brokers, advisors, sales, operations, marketing, finance and accounting, software developers. Select **Option 2** if you are a mid- and senior level supervisor, or control functions and back office support teams, such as: managers, compliance, legal, internal audit, government relations. Select **Option 3** if you are information security department staff; those in IT with privileged access to networks, systems, applications, etc.

Option 1: Front Office and/or First Line of Defense

I. Exercise: Cyber Threats & Techniques – Drag and Drop
   a. Credential Recycling
   b. Phishing
   c. Social Engineering
   d. Trojan Horse
   e. Whaling

II. Best Practices
   a. Phishing Attacks
      i. Basic Tips
      ii. Exercise: Phishing Email – Legit Email
      iii. Exercise: Malicious Spear – Phishing Email
   b. Password Guidance
   c. Policies & Procedures
   d. Mobile Devices
   e. Social Media
   f. Artificial Intelligence Risks
      i. AI Risks
      ii. AI Risks – Associated with AI Used by Cyber-Criminals
      iii. AI Risks – Associated with AI Used by Financial Firms
   g. Internet Security

h. Transmitting Sensitive Information
i. Working Remotely

III. Regulatory Enforcement Cases
a. FINRA
b. CFTC

IV. Quiz

Option 2: Mid- and Senior-Level Supervisors and/or Back Office Staff

I. Exercise: Cyber Threats & Techniques – Drag and Drop
a. Credential Recycling
b. Phishing
c. Social Engineering
d. Trojan Horse
e. Whaling

II. Best Practices
a. Phishing Attacks
i. Basic Tips
ii. Exercise: Phishing Email – Legit Email
iii. Exercise Malicious Spear – Phishing Email
b. Password Guidance
c. Mobile Devices
d. Social Media
e. Artificial Intelligence Risks
i. AI Risks
ii. AI Risks – Associated with AI Used by Cyber-Criminals
iii. AI Risks – Associated with AI Used by Financial Firms
f. Internet Security
g. Transmitting Sensitive Information
h. Working Remotely
i. Implementing Non-Technical Controls – Acceptable Use Policy
j. Supervisory & Control Responsibilities
i. Implementing Policies & Procedures
ii. Escalation & Modeling
k. Social Media
l. Password Guidance
m. Mobile Devices
n. Artificial Intelligence Risks
i. AI Risks
ii. AI Risks – Associated with AI Used by Cyber-Criminals
iii. AI Risk – Associated with AI Used by Financial Firms

III. Regulatory Priorities

a. Regulatory Updates
    i. CFTC
    ii. SEC
    iii. EU (DORA)
    iv. New York Department of Financial Services
b. Regulatory Enforcement Cases
    iii. FINRA
    iv. CFTC

IV. Quiz

Option 3: IT & Information Security System Admins

I. Best Practices
a. Phishing Attacks
b. Poor Privileged Access Practices
c. Social Media
d. Password Guidance
e. Mobile Devices
f. Artificial Intelligence Risks
    i. Overview
    ii. AI Risks – Associated with AI Used by Cyber-Criminals
    iii. AI Risks – Associated with AI Used by Financial Firms
g. Internet Security
h. Transmitting Sensitive Information
i. Mitigating Remote Work Risks
j. Implementing Non-Technical Controls – Acceptable Use Policy
k. Escalation & Modeling Good Behavior
l. Insider Threats
    i. Overview
    ii. Insider Threats – Vulnerabilities
    iii. Insider Threats – Risks
    iv. Insider Threats – Monitoring and Mitigation
m. System Administration & Role Segregation
n. Implementing Technical Controls – Data Back-Up
o. Additional Risk Considerations
    i. Poor Patch Management
    ii. Unrestricted Code Execution
    iii. Cloud Security Misconfiguration
    iv. Insufficient Network Segregation
    v. Inadequate Monitoring & Logging
    vi. Default Configurations & Credentials

II. Regulatory Enforcement Cases
   a. FINRA
   b. CFTC
III. Quiz

Provider Qualifications - About the Authors

Joseph Adamczyk served as the author. Prior to his affiliation with Exchange Analytics, he served as the Chief Compliance Officer for Options Clearing Corporation (OCC). Mr. Adamczyk oversaw the firm's compliance risk monitoring and governance programs, advised the board of directors and staff on compliance and regulatory requirements, and interacted with federal regulators on compliance, risk, and examination matters. Before joining OCC, Mr. Adamczyk worked at CME Group where he served as the Managing Director & Associate General Counsel overseeing the company's non-U.S. legal staff and activities. In this role, he interacted with regulators from around the globe. He also handled CME Group's interactions with U.S. regulators and other authorities on cybersecurity and technology controls, requirements, cyber incident response, and examinations. At CME Group, Mr. Adamczyk also served as the Global Head of Investigations and Enforcement in the Market Regulation Department. In that role, he oversaw teams responsible for monitoring, investigating, and enforcing the CME Group exchanges' trade practice rules and other requirements. Mr. Adamczyk received his MBA from the University of Chicago, law degree from Loyola University Chicago School of Law, and undergraduate degree from DePaul University. He has no regulatory actions or other disciplinary history.

Cyber Advisory Group

This course was reviewed by the Cyber Advisory Group. The Exchange Analytics (XA) Cyber Advisory Group assists management of XA with regard to its cybersecurity risk management and privacy practices, advising on: (1) the practices, procedures and controls that XA management uses to identify, manage and mitigate risks related to cybersecurity, privacy and disaster recovery and respond to incidents with respect thereto; and (2) advise on cybersecurity risk and privacy courses and other regulatory compliance solutions that XA offers to its clients. XA's Cyber Advisory Group consists of leading cybersecurity practitioners with decades of government and private industry experience, including a former Chief Information Security Officer for the U.S. Central Intelligence Agency, and a former Chief Information Security Officer for the U.S. Defense Intelligence Agency. For more information on the CAG, click here.