EXCHANGE | ANALYTICS

Cybersecurity Refresher Training 2026

Course Outline

The Exchange Analytics Cybersecurity Refresher Training 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.

I. Introduction
   a. Cybersecurity Overview
   b. Importance of Robust Cyber Practices
   c. Importance for Financial Firms
   d. Expanding Regulatory Requirements
   e. Managing the Risks
   f. Participation by Everyone
   g. Role-Based Learning Selection

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
   b. Basic Tips
      i. Exercise: Phishing Email – Legit Email
      ii. Exercise: Malicious Spear-Phishing Email
   c. Password Guidance

d. Following Policies & Procedures
e. Mobile Devices
f. Social Media
g. Artificial Intelligence
    i. AI Risks
    ii. Using AI – Regulator Expectations
    iii. AI Risks – Associated with AI Used by Cyber-Criminals
    iv. AI Risks – Associated with AI Used by Financial Firms
h. Internet Security
i. Transmitting Sensitive Information
j. Working Remotely
k. Regulatory Priorities

III. 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. Using AI – Regulator Expectations
        iii. AI Risks – Associated with AI Used by Cyber-Criminals
        iv. 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. Regulatory Priorities

l. SEC Regulation S-P Compliance Deadlines
m. NYSDFS Guidance on Managing Third-Party Risks

III. 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. Using AI – Regulator Expectations
      iii. AI Risks – Associated with AI Used by Cyber-Criminals
      iv. 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. System Administration & Role Segregation
   m. Implementing Technical Controls – Data Back-Up
   n. Insider Threats
      i. Vulnerabilities
      ii. Risks
      iii. Monitoring & Mitigation
   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 Priorities
III. NYSDFS Guidance on Managing Third-Party Risks
IV. Quiz