EXCHANGE ANALYTICS
Regulatory Compliance Solutions

2021 Cybersecurity (21.2)

Course Outline and Provider Qualifications

I. Course Content

a. Cybersecurity Training Goals
b. Incidents in the Headlines
c. What is Cybersecurity?
d. Enterprise Risk Management
e. The Importance of Participation by Management and Employees
f. The Benefits of a Strong Cybersecurity Program
g. Types of Cybersecurity Threats
    i. Insecure passwords
    ii. Malware
    iii. Viruses, Worms, Trojans
    iv. Spyware
    v. Lost, Stolen or Obsolete Hardware
    vi. Spoofing
    vii. Physical Access to Systems
    viii. Unauthorized Visitors
    ix. Social Engineering
    x. Remote Access
    xi. Internet of Things (IoT) Breaches
h. Types of Cybersecurity Attacks
    i. Hacking
    ii. Ransomware and Cybersecurity Extortion
    iii. Website Hacking
    iv. Theft of Information
    v. Automated Password Attacks
    vi. Credential Recycling
    vii. Watering Hole Techniques
    viii. Phishing
    ix. Spear Phishing
    x. Business Email Compromise
    xi. Denial of Service Attacks
    xii. A Distributed Denial of Service
    xiii. Cyber Extortion
    xiv. Social Engineering
i. Critical Cybersecurity Threats
    i. Cyber Terrorism
    ii. Cyber Espionage
j. Procedures for Reporting and Responding to Security Incidents

k. Defense Against Hackers
l. Mobile Protection
m. SIM Card Swapping
n. Social Network Risks
o. Safe Use of Social Networks
p. Compliance Requirements
q. Regulatory Requirements
r. Best Practices for Employees
s. Best Practices for Firms
t. Specific Requirements for Financial Services

II. Case Studies

III. Conclusion and Acknowledgment

About the Course Authors

Arnold Feist served as author. He is the President of Executive Compliance International, an independent financial services consulting firm. Mr. Feist has held board memberships and director positions and managed the compliance functions at several major clearing brokers and futures commission merchants in institutional and retail securities, commodities, forex, brokerage operations and prime brokerage. He has been an expert witness in securities litigation, a speaker and moderator at industry seminars, a guest lecturer at New York University School of Continuing and Professional Studies and at the New York Institute of Finance.

Joseph Adamczyk served as a co-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.