EXCHANGE ANALYTICS INC.

# 2019 Cybersecurity Training Course Outline

## I. Introduction

a. Guidance from NFA, SEC, FINRA
b. The Enterprise Risk Management Program

## II. The Firm's Responsibility

a. Regulatory Background
    i. Gramm-Leach-Bliley Act
    ii. Fair Credit Reporting Act
    iii. Bank Secrecy Act
b. CFTC Best Practices
c. FINRA Report on Cybersecurity Practices
d. Frameworks and Resources
    i. SANS
    ii. NIST
e. Security and Risk Analysis
f. Deployment of Protective Measures
g. Response and Recovery/Response Team
h. Outside Experts and Counsel
i. Assessment of a Cyber Event
j. Securing the Network
k. Record, Collect, Preserve
l. Voluntary & Mandatory Notifications/Timing
m. Information Sharing with Law Enforcement/Industry
n. Employee Training
o. Review of the Cybersecurity Program
p. Third-Party Service Providers
q. The Cloud
r. Recordkeeping
s. Cyber Insurance
t. Information Security

## III. The Individual's Responsibility

a. Physical Security
b. Lost or Stolen
c. Encryption
d. Away from the Office
e. Network Security/External Threats
f. Hacking Techniques
    i. Ransomware
    ii. Website Takeover
    iii. Denial of Service
    iv. Theft of Information
g. Defining a Breach
h. Internal Threats
i. Cyber Hygiene
j. Perimeter Defenses
k. The Crown Jewels
l. Personal Identifying Information
m. Securing Data
n. Control Access
o. Protecting the Network
p. Access Anomalies
q. Encryption
r. Email Take Over
s. Business Email Compromise and Other Email Ploys
t. Passwords
u. Two-Factor Authentication
v. The "Internet of Things"
w. Social Engineering/Techniques
x. Best Practices
y. DNS

## IV. Noteworthy Regulatory Cases

## V. Case Study: The Broker and the Help Desk

## VI. Quiz