

# **EXCHANGE ANALYTICS INC.**

## **Cybersecurity Training 2018 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. FINRA Report on Cybersecurity Practices
- c. CFTC Best 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
- m. Information Sharing
- n. Employee Training
- o. Review of the Cybersecurity Program
- p. Third-Party Service Providers
- q. The Cloud
- r. Recordkeeping
- s. Cyber Insurance and Information Security

### **III. The Individual's Responsibility**

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

### **IV. Noteworthy Regulatory Cases**

### **V. Case Study: The Emergency Wire Request**

### **VI. Quiz**