CYBER-ENABLED CRIME

Course Syllabus

Audience

The primary target is the frontline analyst, teaching skills that benefit new and experienced employees, especially as regulator and market expectations increase. This course assumes the employer has already introduced that organization's unique roles, processes, systems, and common cases, and this course will not conflict with those. To bring all learners to a shared baseline of terminology, concepts, and processes, the course starts with the "*Essentials*" video and then builds from there.

The course is written and presented by subject matter experts working around the world. It pulls examples from many countries, and is globally appropriate. The lessons and examples are relevant to any industry. A primary focus is "financial institutions," including banks, credit unions, asset managers, insurance, MSB, securities broker-dealers, credit card issuers, alternate payment systems, etc.

Course Structure

ACAMS allows you 4 calendar weeks to complete **4 hours of coursework**, including a final assessment. You will be guided using a learning path on ACAMS' learning management system (LMS). Follow carefully all instructions. Live virtual classroom events are pre-scheduled before you purchase the course. 4 weeks from the course start date your access expires.

	Assignment	Format	Download from LMS
Week 1	30 mins – VIDEO *"Essentials"*	Video: Self-paced, available anytime	PDF quick reference
Week 2	90 mins – VIRTUAL CLASSROOM	Live event: See LMS for date/time. Later a recording will be on the LMS.	PDF slides
Week 3	90 mins – VIRTUAL CLASSROOM	Live event: See LMS for date/time. Later a recording will be on the LMS.	PDF slides
Week 4	15 mins – HOMEWORK 15 mins – ONLINE ASSESSMENT	Self-paced, available anytime. Self-paced, available anytime.	PDF Assignment PDF ACAMS Certificate

To earn the certificate you must pass the assessment within the 4 weeks. The assessment has 20 questions. The minimum passing score is 80%. Multiple attempts are allowed. When you pass, your ACAMS Certificate will be available in the learning path itself. Click to download a PDF. ACAMS will automatically add 4 CAMS Credits to your profile.

Technical Requirements:

The course is compatible with most operating systems and browsers to make it easy to participate. The video, homework, and final assessment are mobile-friendly. The virtual classroom uses Webex Event Center which currently does not support mobile devices. The ACAMS Learning Management System (LMS) is https://lms.acams.com. Contact your organization's IT department for assistance.

Harden your organization's defenses to protect data and financial assets.

Behavioral outcomes of this course:

1. Describe the tremendous threat that cyber-enabled crime poses to your organization and identify the most common attack methods
2. Identify the "soft spots" where your organization is the most vulnerable to cyber-attackers
3. Create an effective cyber-attack preparation and response plan to protect your organization, your clients and your reputation from being exploited
4. Collect, analyze and report intelligence information to aid law enforcement in the identification and capture of cyber criminals

Course content

1. Introduction
   a. Definition: FinCEN defines "Cyber-Enabled Crime" as illegal activities (e.g., fraud, money laundering, identity theft,) carried out or facilitated by electronic systems and devices, such as networks and computers.
   b. Relationship with AML-CTF
      i. How BSA reporting helps US authorities combat cyber-events and cyber-enabled crime
      ii. Requires an additional, technical, skillset
      iii. Many learners will be victims
   c. Benefits of combatting cyber-enabled crime
      i. To you, personally
      ii. To the organization
      iii. To Law Enforcement
      iv. To society
   d. Learning Objectives: Upon completion of this learning activity, you will be able to:
      i. Know the hunters: Describe the tremendous threat that cyber-enabled crime poses to your organization and identify the most common attack methods
      ii. Avoid being the prey: Identify the "soft spots" where your organization is the most vulnerable to cyber-attackers
      iii. Defend yourself: Create an effective cyber-attack preparation and response plan to protect your organization, your clients and your reputation from being exploited

iv. Be proactive vs. reactive: Collect, analyze and report intelligence information to aid law enforcement in the identification and capture of cyber criminals

2. Know the hunters: Describe the tremendous threat that cyber-enabled crime poses to your organization and identify the most common attack methods
    a. Cyber-enabled crime is growing
    b. Cyber-criminal are getting better
    c. The high cost of cybercrime
        i. From a financial standpoint
        ii. From your customer's standpoint
        iii. Cybercrime is extremely damaging to your company's reputation
    d. The most common typologies
        i. Traditional AML types repackaged as cybercrime
            1. Attacks directly on the financial institution or money managed by the government
                a. Unauthorized access to funds, data, lines of credit:
                    i. Phishing (includes Spear Phishing)
                    ii. Spoofing
                    iii. Malware
                    iv. Social Engineering (such as elder abuse)
                        1. Includes social media such as job changes announced through LinkedIn
                    v. Hacking using vulnerabilities
                b. Ransomware
                c. DDoS
                d. Counterfeit virtual funds (e.g. credit/debit/gift cards, wire transfers, etc.)
                e. Falsified transaction information to disguise routes or histories in order to enable money-laundering, terrorist financing, sanctions evasion
                    i. Data manipulation
                    ii. Virtual account opening/access
                    iii. Data or funds rerouting
                    iv. Currency conversion
        ii. Attacks against individual account holders
            1. Unauthorized access to funds, data, or lines of credit managed by the individual and/or financial institution (identity theft)
                a. Phishing
                b. Malware

c. Social engineering
d. Hacking

2. Ransomware
3. Counterfeit virtual funds (credit/debit/gift cards, ACH, etc.)

iii. Examples

1. Bank of Bangladesh, February, 2016
    a. i$81 million theft
    b. As of 1/2017, still unsolved
2. Tesco Bank, November 2016
    a. One of the largest-ever cyberattacks on a UK bank
    b. Nearly one-third of depository accounts were compromised
    c. £2.5 million stolen
3. Other(s)

e. Red Flags
f. Sanction

3. Avoid being the prey: Identify the "soft spots" where your organization is the most vulnerable to cyber-attackers
    a. This is how the attackers will likely get in
        i. Hackers are sophisticated yet most get in by tricking a gullible employee
        ii. Wall Street Journal article, "Cyber Soft Spots: Hackers Exploit Staffers at Banks"
    b. How employees are tricked
        i. Thumb drives
        ii. Via links in emails
            1. Phishing, Spear phishing
        iii. Attachments
        iv. Malware
            1. Disguised as free games or pornography
            2. Malware from 2007, 2010, 2011, 2012, 2013 still in use
        v. SWIFT scams
        vi. Hackers
            1. Coveted account credentials
            2. Often in unprotected files such as spreadsheets

3. Social Media gives hackers valuable intelligence
    a. New job or promotion
    b. Business travel—out of office messages alert hackers when computer is not monitored
4. Hackers sell data
    a. Social Security numbers, phone numbers, addresses, credit card numbers

vii. Money Mules
1. Funnel accounts
2. Many users but one underlying identity

viii. Examples
1. US
2. UK or global

ix. Evaluate your organization and where the weaknesses are

4. Defend yourself: Create an effective cyber-attack preparation and response plan to protect your organization, your clients and your reputation from being exploited
    a. Tabletop simulations
    b. Work jointly with systems team
    c. Create a plan
        i. Policies blessed by Board of Directors
        ii. Reporting
        iii. Do things ahead of time to prepare
        iv. Prioritize based on the impact to your organization's reputation and loss levels
    d. Need to practice your plan
        i. Instant Response team should establish relationships with Law Enforcement in advance. (Don't pick your team on game day!)
        ii. Example from bank of Bangladesh
    e. Best practices
        i. Two factor authentication
        ii. Patch management
        iii. Identify and protect your organizations most valuable assets
5. Be proactive vs. reactive: Collect, analyze and report intelligence information to aid law enforcement in the identification and capture of cyber criminals
    a. Related SAR filing requirements
        i. Include relevant and available cyber-related information
            1. IP addresses with timestamps

2. Virtual wallet information
3. Device identifiers
4. Methodologies used
5. Etc.

b. Engaging your organization's network security team
    i. Need to collaborate with in-house cybersecurity units
        1. Information provided by cybersecurity units would reveal additional patterns of suspicious behavior and identify suspects not previously known to BSA/AML units
        2. Likewise, cybersecurity personnel can use information provided by BSA/AML to guard against cyber-events/cyber-related crime
c. Share information among other Financial Institutions to guard against and report:
    i. Money laundering
    ii. Terrorist Financing
    iii. Cyber-enabled crime
    iv. Under Section 314(b), participating FI's may exchange information, including cyber-related information, regarding:
        1. Individuals
        2. Entities
        3. Organizations
        4. Countries
    v. Industry collaboration
        1. National Cyber Forensic Training Alliance (NCFTA)
            a. Public-Private partnership
        2. Others
d. Future Trends in Cyber-security
    i. How to stay several steps ahead
    ii. Proactive vs. Reactive