Cyber Intelligence 4U

Cybersecurity Sales Associate Program 2022-2023 Syllabus

CYBER
INTELLIGENCE 4U

Cybersecurity Sales Associate Program 2022-2023

Program Overview

Cybersecurity is a complex topic. Most salespeople don't really understand cybersecurity. The Cybersecurity Sales Associate Program ensures these teams can confidently assess customer needs, present your cybersecurity solutions in context to decision makers, and sell products successfully to your clients.

CISOs and cyber buyers want to have a return on their investment. The digital asset approach allows salespeople to calculate ROIs for cybersecurity tools. Building the business case is one of the key aspects of enabling your customer to say yes.

This course will enable you to elevate the conversation and establish yourself as a trusted advisor with the client. Start by building foundational knowledge, covering terminology, breaches, trends, and other cyber related information.

Different companies have different cybersecurity needs based on their maturity. Cybersecurity sales teams are most effective when they can position a solution that meets the client's most urgent need. This course allows them the ability to "meet the client where they are."

Through customized product role play, students can practice and prepare a practical approach when dealing with clients that ensures sales close. You'll gain confidence in speaking with sophisticated buyers about their cybersecurity needs and solutions based on customer cyber maturity. Most clients see a 10% increase in sales within a few months.

In this course, you will be empowered to:

- Have the ability to upsell and cross sell your cybersecurity offerings.
- Acquire an in-depth understanding of cybersecurity, maturity levels, and selling products and services effectively.
- Utilize tools to determine prospect cybersecurity maturity and cyber tool ROI.
- Engage with hands-on learning with the VRisk cybersecurity platform, using live or dummy data to risk model, inventory digital assets, quantify exposures, and calculate tool ROI.
- Earn a premier certificate from Pace University's Seidenberg School of Computer Science and Information Systems as validation of your newfound cybersecurity knowledge and skills
- Have access to a global network of likeminded cybersecurity professionals.

Required Text

Managing Cyber Risk - Strategies for Surviving and Thriving in the age of Interconnectivity and Innovation, Evans; 1st Edition, ISBN-13: 978-0367177737.

Prerequisites

No prior knowledge of IT or cyber is required

Module 1: Evolution of Cybersecurity and Cybersecurity Basics

Module Description

This module provides an introduction to cybersecurity from a business point of view based on research with the Fortune 1000 and cyber insurance industry using a digital asset methodology. In 2001, 10% of a business was digital, today 85% of an organization's value is digital. The module focuses on building student understanding of cybersecurity from how cyber evolved out of information technology, addresses key cyber-related business and technical roles, demonstrates the consequences of poor cyber hygiene and reviews cybersecurity trends.

In addition to the evolution of cyber, students learn to communicate in the language of cybersecurity, study data breaches, attack surfaces, enterprise threats of today and enterprise cybersecurity programs components.

Each student is required to conduct a data breach case study and do an online lab. The lab assignment is an inventory of digital assets of their organization or a fictious or public organization. The lab uses the VRisk platform.

Digital Asset Inventories contain about a dozen attributes needed for cyber risk quantification and scoring that will be performed in later modules. The digital asset inventory aims at identifying crown jewel assets and validating the key attributes used in cyber risk scoring related to the asset behavioral and user behavioral analytics.

Here are the main digital asset objectives found in organizations:

Systems – Sets of technologies purchased or developed by organizations for specific business purposes. Relates to data exfiltration metrics.

Technologies - computer related components that typically consist of hardware and software, databases, messaging and devices. Relates to technology risks, assessments and systems.

Processes - a set of digital rules that are utilized by one or more systems to take inputs, transform them and produce outputs that are reported or utilized by other systems. Relates to business interruption exposures and risks.

Data Types - information that is processed and stored. Data can be classified into different types including privacy, credit card, intellectual property, customer data, supply chain data, etc. and relates to regulatory exposures.

Module Grade

Each student is expected to satisfy the following
requirements: Quizzes (30%)
Data Breach Case Study Assignment (20%)
Digital Asset Lab (50%)

Module 2: Cybersecurity Regulations and Frameworks

Module Description

This module provides an introduction to cybersecurity regulation based on industry, geography, government and data type. It explores standards and frameworks aligning them to security control tests. Regulations covered at the Federal level are the Healthcare Information Portability and Accounting Act (HIPAA), Securities Exchange Commission (SEC), Graham Leach Bliley Act (GLBA), and the Fair Practices Act. Regulations at the state level focus on new privacy laws including the California Consumer Protection Act (CCPA), State privacy acts in Maine, Nevada, Colorado and the New York State Department of Financial Services Part 500 (NY CRR 500) and the Insurance Data Security Act. The module covers both organizational and third-party requirements.

The module explores each control test, their use, and how to conduct the tests in a lab environment. Each student is required to do an online lab. The lab assignment is a security assessment of a system at their organization or a fictious or public organization. Security Assessments can be prescriptive or not. Controls can be mapped across frameworks.

Here are the main objectives found in this module are to map control assessment requirements to the following laws:

Federal Regulations – Including FTC, FCC, OCIE, HHS and GLBA Laws

State Regulations – Including CCPA, NYS DFS, State Privacy Laws, and the Insurance Data Security Act

Industry Standards – Including PCI

European Regulations – Including GDPR

Frameworks – Including ISO27001, PCI-DSS, NIST 800-53, NIST CSF, COBIT, CIS Top 20 Controls, etc.

Module Grade

Each student is expected to satisfy the following requirements:

Quizzes (50%)

Security Assessment Lab (50%)

Module 3: Cybersecurity Tools and ROI

Module Description

This module provides an introduction to cybersecurity tools. Many companies use layered tools to identify, protect, detect, respond or recover to cybersecurity events. We explore the many types of cybersecurity tools, their purpose, how they work, what they do and where they are used. Each cybersecurity tool provides risk reduction in terms of data exfiltration, business interruption or regulatory loss. We will map the cybersecurity tools to the types of risk reductions.

In this module, students will understand how to quantify digital asset cybersecurity exposures in terms of data exfiltration, business interruption or regulatory loss. Students will define risk reduction models and associate them to the cybersecurity tools. A cost benefit analysis is taught to demonstrate how to calculate the return on investment of each cybersecurity tool. There is a lab where students calculate return on investment using the VRisk product.

Here are the main objectives of the cyber quantification lab:

- Determine the Risk Modelling for data exfiltration, business interruption or regulatory loss.
- Determine the Calculation of the Digital Asset Risk.
- Determine the Calculation of the Return on Investment of the Cybersecurity Tool.

Module Grade

Each student is expected to satisfy the following requirements:

Quizzes (30%)
ROI Lab (70%)

Module 4: Cybersecurity Maturity = Cybersecurity Selling

Module Description

This module provides a deep dive into over 25 corporate attributes that can be used to determine the maturity of an organization. Based on three years of research with the Fortune 1000 and cyber insurance industry, each attribute is mapped to one of five categories: unaware, tactical, focused, strategic or pervasive. The company is scored based on the information and a overall cybersecurity maturity is determined.

Students will select a prospect for a maturity assignment. Students will ascertain the data needed to identify the maturities across the organization attributes and determine an overall maturity for the company.

Based on the maturity analysis the student will identify prospects for their cybersecurity offerings. This is a custom course and an initial mapping by Cyber Intelligence 4U is required.

Students will role play by creating an introductory email with the goal of getting up a meeting with a decision maker.

Module Grade

Each student is expected to satisfy the following requirements:

Quizzes (30%)
Maturity Assignment (35%)
Role Playing Email Assignment (35%)