Cyber Intelligence 4U

Enterprise Cybersecurity Certificate
Basic Course Syllabus

 66 West Flagler St. Miami FL 33103 info@yberintelu.com

CYBER
INTELLIGENCE 4U

Table of Contents

Enterprise Cybersecurity Certificate Program

Program Overview

Cyber is a business issue. This is a program about business impacts. The best cyber, privacy, compliance and risk managers have a good foundational cyber understanding and need to have a well-rounded solid skill set of core business acumen in terms of analytical skills, and critical thinking focused on cyber risks. This program is about creating thought leaders and critical thinkers who can bridge these gaps. This program is holistic and starts with the basics, covering terminology, breach case studies, cyber program roles, processes and tools.

The Enterprise Cybersecurity Program is a rigorous 2-day in person or self-paced online curriculum led by prominent cybersecurity experts, many of whom advise governments, agencies, and industry bodies around the world. The program brings together executives, experts, innovators, and regulators to address cybersecurity from a digital point of view and leaves the student empowered.

This program is ideal for the following roles and departments: CISO, CRO, DPO, Board of Directors, Compliance, Audit, Security Manager, Security Team, IT Team, Vendor Team

Students will be empowered by:

- The ability to understand cyber holistically from a business perspective across regulation, compliance, security standards and risk. Students will be able to strategize how to lower cyber risk and work with stakeholders to increase cyber resilience.
- An in-depth understanding of cyber exposures and scores that determine show crown jewel exposures, identify hidden exposures, determine cyber insurance needs, and identify gaps in the programs across security, compliance and privacy.
- Hands on learning with the VRisk product that allows students to use live or dummy data to risk model, quantify exposures, perform a privacy impact assessment and deliver board reports with KPIs and metrics that empower the board.
- A premier certificate from Seton Hall University, as validation of newfound cybersecurity knowledge and skills, as well as 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

Note: This syllabus is subject to change based on the needs of the class.

CYBER
INTELLIGENCE 4U

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%)

CYBER
INTELLIGENCE 4U

Module 2: Regulations, Standards 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%)