Cyber Intelligence 4U

Enterprise Cybersecurity Certificate
Advanced Course Syllabus

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

CYBER
INTELLIGENCE 4U

Table of Contents

CYBER
INTELLIGENCE 4U

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. It moves deeper into the integrated cyber risk perspective while exploring the newest regulations, security assessment frameworks, forensics and auditing techniques, cyber risk management and cyber strategy using hands on learning to inventory digital assets, perform privacy assessments, quantify exposures and risk model.

The Enterprise Cybersecurity Program is a rigorous 5-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 Unviersity, 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%)

CYBER
INTELLIGENCE 4U

Module 3: Cyber Insurance

Module Description

This module provides an introduction to cybersecurity insurance. Many companies are now required to have cyber insurance to work with the federal government, their contractors and other commercial entities. Digital asset quantification aligns exactly to how a cyber insurance claim will be paid. Having the right amounts and steering clear of exceptions is critical to ensuring an investment.

Ransomware is rising exponentially over the past few years and more so with the Corona Virus pandemic. The course provides students with a method to create an effective ransomware strategy and gauge their preparedness for a ransomware attack.

In this module, students will understand how to quantify cyber insurance and calculate the aggregate limit, and sub-limits including cyber extortion, business interruption and privacy sub-limits. The module explores first and third-party cyber risks and identifies gaps in current property and casualty insurance policies where claims would not be paid. A cyber insurance case study is required that explores a data breach or ransomware attack. Students learn trends and statistics and gaps in cybersecurity programs that might result in unpaid claims and how to avoid them.

Here are the main objectives of the cyber quantification lab:

- Aggregate limit calculation
- Cyber Extortion Sub-limit calculation
- Business Interruption Sublimit Calculation
- Privacy Sub-limit Calculation

Module Grade

Each student is expected to satisfy the following requirements:

- Quizzes (20%)
- Cyber Insurance Case Study (30%)
- Cyber Insurance Quantification Lab (50%)

CYBER
INTELLIGENCE 4U

Module 4: New York State Department of Financial Services Part 500

Module Description

This module provides a deep dive into the New York State Department of Financial Services Part 500 cybersecurity regulation. The New York State Department of Financial Services has been closely monitoring the ever-growing threat posed to information and financial systems by nation-states, terrorist organizations and independent criminal actors. Recently, cybercriminals have sought to exploit technological vulnerabilities to gain access to sensitive electronic data. Cybercriminals can cause significant financial losses for DFS regulated entities as well as for New York consumers whose private information may be revealed and/or stolen for illicit purposes.

In this module, students will understand who is in scope, exceptions to the regulation and how to comply with each section of the regulation. Students learn the requirements and which control tests are required. Students are required to do a vendor cyber risk assessment lab.

Here are the main objectives covered in the module:

- Section 500.02: Cybersecurity Program
- Section 500.03: Cybersecurity Policy
- Section 500.04: Chief Information Security Officer
- Section 500.05: Penetration Testing and Vulnerability Assessments
- Section 500.06: Audit Trail
- Section 500.07: Access Privileges
- Section 500.08: Application Security
- Section 500.09: Risk Assessment
- Section 500.10: Cybersecurity Personnel and Intelligence
- Section 500.11: Third-Party Service Provider Security Policy
- Section 500.12: Multi-Factor Authentication
- Section 500.13: Limitations on Data Retention
- Section 500.14: Training and Monitoring
- Section 500.15: Encryption of non-public Information
- Section 500.16: Incident Response Plan
- Section 500.17: Notices to Superintendent

Module Grade

Each student is expected to satisfy the following requirements:

- Quizzes (30%)
- Vendor Risk Assessment Lab (70%)

CYBER
INTELLIGENCE 4U

Module 5: General Data Protection Regulations (GDPR)

Module Description

40% of American companies are in scope for the GDPR. This new privacy regulation is the most stringent and new privacy laws in the United States are adopting many of its requirements.

This module provides a deep dive into the General Data Protection Regulation. Students learn about scope, enforcement and how to meet all the requirements for each article. The module focuses on the policies, procedures, forms and assessments needed to be compliant. Students will learn how to demonstrate the needed cybersecurity controls are designed properly and function effectively in protecting the privacy of the internal and external stakeholders.

Policy, procedure and form templates are provided to students. A policy assignment is required by students. Students pick a policy relevant to their organization and create it.

Risk modeling is taught to measure confidentiality and integrity of data and is based on the digital asset approach. Students are required to do a privacy impact assessment lab using the VRisk product on their firms' data or fictious data.

The module covers the main objectives of GDPR including:

- Article 1: Identifying all EU privacy data
- Article 5: Ensuring data has adequate integrity and confidentiality
- Article 15: The Right to Access Personal Data
- Article 16: The Right to Rectification
- Article 17: The Right to Erasure
- Article 18: The Right to Restrict Processing
- Article 19: The Right to be Notified
- Article 20: The Right to Data Portability
- Article 21: The Right to Object
- Article 22: The Right to Reject Automated Decision Making

Module Grade

Each student is expected to satisfy the following requirements:

- Quizzes (30%)
- Policy Assignment (20%)
- Privacy Impact Assessment (50%)

CYBER
INTELLIGENCE 4U

Module 6: Audit and Forensics

Module Description

This module provides a high-level overview of IT auditing and cyber forensics. The module focuses on the role of the IT auditor and how audits are performed, the four phases of an audit and challenges from the cybersecurity landscape. Students will learn how to demonstrate the businesses cybersecurity controls are designed properly and function effectively in protecting the information assets, protecting the privacy of the internal and external stakeholders, protecting the reputation of the organization, complying with laws, regulations and contracts while preventing litigation fees and regulatory fines. Real world examples are referenced to anchor the students understanding. Students will be introduced to cloud auditing.

The module covers the main objectives of auditing:

- Planning
- Fieldwork
- Reporting
- Follow Up

In this module, students will allow be provided a high-level understanding of the cyber forensics world. Students will review a child pornography case study and its ramifications.

The module covers the main objectives of cyber forensics:

- Evidence Gathering
- Goal Setting
- Investigative Plan
- Privileged Information
- Counsels Role
- Covert and Overt Investigation Techniques
- Chain of Custody

Module Grade

Each student is expected to satisfy the following requirements:

- Quizzes (100%)

CYBER
INTELLIGENCE 4U

Module 7: Cyber Risk Management

Module Description

Cyber risk has mystified organizations for the past decade. Many companies do a vulnerability assessment and call it a risk assessment. A vulnerability assessment is an assessment of weaknesses in systems, it is not a risk assessment. Insurance companies gather lawsuit data and call that risk. Lawsuit data is based on incidents. Incidents have a 100% probability and are not risk. Some look at data from the deep and dark web and call spam propagation and botnets risk. They are threats.

This course is based on three years of research with the Fortune 1000 and cyber insurance industry to understand why companies struggle to be cyber resilient. They are looking at the wrong data to make strategic decisions with long term consequences regarding budget, insurance, and cyber tools. Cyber risk is measured with two metrics – exposures and scores using impact and likelihood data. This module provides students that ability to quantify cyber exposures and measure cyber risk scores. It demonstrates the use cases for cyber exposures including crown jewel asset strategies, identification of hidden exposures, vendor exposures, calculation cyber insurance limits and sub-limits, and M&A due diligence.

Students learn how to measure inherent cyber risk, residual cyber risk and the effectiveness of cybersecurity controls and its relationship to risk mitigation. Demonstration of use cases including identifying gaps in the organizations' cybersecurity program and their vendors programs.

Risk modeling is taught to quantify:

- Data Exfiltration
- Business Interruption from Ransomware
- Business Interruption from DoS
- Regulatory Exposures

This course examines the relationships between inherent risk, security assessments and residual risk and offers strategies to prioritize remediation work. Risk modeling techniques are taught to measure inherent and residual cyber risks based on the digital asset characteristics, how it is used and protected.

Module Grade

Each student is expected to satisfy the following requirements:

- Quizzes (30%)
- Policy Assignment (20%)
- Risk Modeling Assignment (50%)

CYBER
INTELLIGENCE 4U

Module 8: Cyber in the Boardroom and Cybersecurity Strategies

Module Description

Cybersecurity has been treated as an IT issue with dismal results. Cyber risk is owned by the board of directors and senior executives. They have the fiduciary duty to protect the digital assets. Effective strategies require the understanding of cyber maturity and useful metrics that are digestible to the risk owners. This module provides students the ability to measure cybersecurity maturity across over 20 different organizational attributes and map them to five categories: Unaware, Tactical, Focused, Strategic and Pervasive.

The module focuses students on how to create an effective and resilient strategy using people, process and tools. Students learn how to translate cyber risk metrics into actionable boardroom strategies to optimize cyber resilience. These include four major areas:

- **Protecting the digital assets**
  - What are our most valuable digital assets? Which ones are crown jewels?
  - How much financial exposure do we have related to a data breach, ransomware, business interruption and regulatory loss?
  - How much hidden exposure do we have?
  - How do the digital assets compare in terms of their cyber risk?
  - Which digital assets are above their risk thresholds? By how much and why?
  - How effective is our cyber program?
  - What are the gaps in our cyber program?
  - What initiatives should we prioritize to lower risk?
  - Do we have enough cyber budget?
  - Do we have enough resources and how do we prioritize them?
- **Cyber Risk Transference**
  - Do we have enough cyber insurance?
  - How much to we need exactly?
  - Are our sub-limits on ransomware, business interruption and regulatory loss enough?
  - What is our ransomware strategy?
- **Vendor Cyber Risk**
  - What relationships do we have with vendors associated to our digital assets?
  - How much financial exposure and cyber risk do we have with these third-parties? How can we reduce it?
  - How effective are the vendors' cyber controls?
- **M&A Cyber Risk**
  - We are planning to sell the company-how does our cyber resiliency impact our acquisition price?
  - We are planning to buy a company-what financial exposure will we inherit? How effective is their cyber program?

Module Grade

Each student is expected to satisfy the following requirements:

- Quizzes (50%)
- Maturity Assignment (50%)