Cyber Intelligence 4U and Seton Hall University

Certified Cybersecurity Risk Management for Executives

Certificate Program

2024 Syllabus

CYBER
INTELLIGENCE 4U

Table of Contents

Certified Cybersecurity Risk Management for Executives 3
Module 1: Evolution of Cybersecurity and Cybersecurity Basics (1h) 4
Module 2: Cybersecurity Regulations (2h) 5
Module 3: Cyber Insurance (1.5h) 6
Module 4: Financial Quantification of Cyber Risk (1.5h) 7
Module 5: Third Party Risk Management (1h) 8
Module 6: Cyber Risk Strategy and Board Reporting (1.5h) 9

CYBER
INTELLIGENCE 4U

Certified Cybersecurity Risk Management for Executives

The 2022 U.S. Security Exchange Commission (SEC) proposed a new rule on "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure." The SEC proposes some significant changes that the board of directors must note. This proposal, which is likely to go into effect in 2023 addresses changes meant to better inform investors about a company's risk management, strategy, and governance and to give investors prompt notice of a significant cybersecurity incident. The following are two key highlights from the proposal:

I. Board members should "consider cybersecurity risks as part of its business strategy, risk management, and financial oversight" as a shared responsibility; they must also rely on IT and legal departments to understand their cyber risks, and board members can't delegate their supervisory function.

II. The board has oversight responsibility of cybersecurity risk, and it requires them to:

- Inform investors about their role in cybersecurity risk management.
- Understand the economic drivers and impact of cyber risk.
- Informed about the financial impact of significant cybersecurity risks and incidents promptly. Incident reporting should now "include quantitative and qualitative factors."
- Incorporate cybersecurity expertise into board governance.

This is the first time the SEC explicitly raises the need to view cyber risk by financially quantifying it.

Nonpublic companies and small and medium enterprises face similar requirements from new privacy regulations. In most cases, data breaches can lead to unsustainability of small and medium companies.

Program Overview

The Seton Hall Certified Cybersecurity Risk Management for Executives is a one-day program offering an unrivaled course with labs that provide hands-on learning. This program provides new and relevant content on oversight responsibilities related to financial impacts that your board and executives must understand to comply with the SEC's new rule on "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure clearly.” Come to this program to learn the best “next practices” to lead your executive team and board through periods of rapid change.

This program will center on required issues in cybersecurity. How much financial exposure does your firm have? Are your organization’s most critical data protected? How much budget is needed to ensure your organization can lower financial risk to acceptable levels? How does visibility into your digital assets mitigate operating risk? How can you get the right information from your CISO? The course Certified Cybersecurity Risk Management for Executives will discuss these questions and many others.

Courses include courseware on learning management systems and hands-on learning with the ValuRisQ cyber risk platform in our state-of-the-art labs. Weekly “Chat with the Chair” sessions are held for 30 minutes for Q&A.

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 class's needs.

CYBER
INTELLIGENCE 4U

Module 1: Cybersecurity Basics (1h)

Module Description

This module introduces cybersecurity from a business point of view based on research with the Fortune 1000 and cyber insurance industry. In 2001, 10% of a business was digital, today over 85% of an organization's value is digital. The module focuses on building student understanding of cybersecurity, starting with how cyber evolved out of information technology, addresses key cyber-related business use cases, 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, learn about attack surfaces, today's enterprise threats, and enterprise cybersecurity program components.

Module Grade

Each student is expected to satisfy the following requirements:

- Quizzes (100%)

CYBER
INTELLIGENCE 4U

Module 2: Cybersecurity Regulations (2h)

Module Description

This module introduces cybersecurity regulation based on industry, geography, technology, and data type. It touches on standards and frameworks, aligning them to security control tests.

The federal regulations covered are the Healthcare Information Portability and Accounting Act (HIPAA), Securities Exchange Commission (SEC), Graham Leach Bliley Act (GLBA), and Fair Practices Act.

Regulations at the state level focus on new privacy laws, including the California Consumer Protection Act (CCPA), Virginia Consumer Data Protection Act (VCDPA), and other state privacy acts in Maine, Nevada, and Colorado. A deep dive into the New York State Department of Financial Services Part 500 (NY CRR 500) and the Insurance Data Security Act.

The GDRP will be reviewed and studied regarding privacy impact assessments and data subject access rights.

This module covers both organizational and third-party requirements.

Pending privacy regulations and regulatory velocity are included.

The main objectives of 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

Module Grade

Each student is expected to satisfy the following requirements:

- Quizzes (100%)

CYBER
INTELLIGENCE 4U

Module 3: Cyber Insurance (1.5h)

Module Description

This module introduces 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.

Ransomware has risen exponentially over the past few years. 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. Students learn trends, statistics, and gaps in cybersecurity programs that might result in unpaid claims and how to avoid them. Students do a case study of a cyber insurance policy.

Here are the main objectives of the cyber quantification lab:

- Aggregate limit calculation
- Cyber extortion sub-limit calculation
- Business interruption sub-limit 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: Financial Quantification of Cyber Risk (1.5h)

Module Description

Cyber risk has mystified organizations for the past decade. This course helps answer the question: How much investment is needed to mitigate cyber risk to acceptable levels?

This course is based on five years of research with the Fortune 1000 and cyber insurance industry to tie financial exposures to cybersecurity. This data is used to make strategic decisions with long-term consequences regarding budget, insurance, and cyber tools. Cyber risk is measured with two metrics – impact and likelihood data. This module allows students to quantify cyber exposures and understand cyber risk likelihood. It demonstrates the use cases for cyber exposures, including crown jewel asset strategies, hidden and vendor exposures identification.

Risk modeling is taught to quantify:

- Data Loss from a Data Breach
- Business Interruption Loss from Ransomware
- Business Interruption Loss from DoS
- Regulatory Financial Exposures

This course examines the relationship between cybersecurity and financial loss. It teaches risk modeling techniques to measure inherent and residual cyber risks based on the characteristics of digital assets and how they are used and protected.

Module Grade

Each student is expected to satisfy the following requirements:

- Quizzes (50%)
- Risk Modeling Assignment (50%)

CYBER
INTELLIGENCE 4U

Module 5: Third Party Cyber Risk (1h)

A third-party risk management program is essential for compliance with regulations. Vendors are responsible for 63% of reported data breaches. Each second, third, and fourth party becomes a part of your digital ecosystem, which multiplies your cyber risk exponentially. Measuring these non-first-party cyber risks is crucial to avoid data breaches. Most recently, regulators have provided detailed guidance on requirements for risk assessments and monitoring of third-party cyber risk.

A recent survey by the Ponemon Institute reveals that 53% of organizations had one or more data breaches caused by a third party, which cost an average of $7.5 million to remediate. Third-party data breaches are twice as costly as internally caused data breaches and are devastating to small businesses.

In this module, students will learn about the types of third parties in your supply chain, vendor inventories, their associated risks, how to measure them, and how to begin a third-party vendor management program.

Module Grade

Each student is expected to satisfy the following requirements:

- Quizzes (50%)
- Cloud Risk Modeling Assignment (50%)