PACE UNIVERSITY

Seidenberg School of Computer Science and Information Systems

Cyber Intelligence 4U
and Pace University

Certified Cybersecurity Risk Management for Executives

Certificate Program

2023 Syllabus

CYBER
INTELLIGENCE 4U

Table of Contents

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 clearly." The SEC proposes some significant changes that the board of directors must take note of. This proposal, which is likely to go into effect in 2023, addresses changes that are 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 all need to rely also 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 medium enterprises are facing similar requirements from new privacy regulations. In most cases, data breaches can lead to unsustainability of small and medium companies.

Program Overview

The Pace 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 need to understand for compliance with the SEC proposed a 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 that your organization can lower financial risk down to acceptable levels? How does visibility into your digital assets mitigate operating risk? How can you get the right information from your CISO? These questions and many others will be discussed in the course Certified Cybersecurity Risk Management for Executives.

Courses include courseware on the 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 needs of the class.

Module 1: Evolution of Cybersecurity and 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, 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 ValuRisQ 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 quantification related to how the cybercriminal attacks the business and causes financial losses.

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 FAsset Lab (50%)

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.

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), Virginia Consumer Data Protection Act (VCDPA) and other state privacy acts in Maine, Nevada, 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 in terms of 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 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

Module Grade

Each student is expected to satisfy the following requirements:

- Quizzes (100%)

Module 3: Cyber Insurance (1.5h)

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.

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 and statistics and gaps in cybersecurity programs that might result in unpaid claims and how to avoid them. Students do a case study on 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 to answer the question: how much investment do we need to mitigate cyber risk down 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 provides students with the ability to quantify cyber exposures and understand cyber risk likelihood. It demonstrates the use cases for cyber exposures including crown jewel asset strategies, identification of hidden exposures, and vendor exposures.

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

CYBER
INTELLIGENCE 4U

Module 5: Third Party Risk Management (1h)

Module Description

A third-party risk management program is an essential part of being compliant with regulations. Vendors are responsible for 63% of reported data breaches. Each second, third and fourth party becomes a part of your digital ecosystem. Your digital ecosystem 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 conducted 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. Data breaches caused by third parties 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, the specific risks associated with them, 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%)

CYBER
INTELLIGENCE 4U

Module 6: Cyber Risk Strategy and Board Reporting (1.5h)

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. Risk owners have the fiduciary duty to protect the digital assets. Effective strategies require the understanding of financial metrics that are digestible to the risk owners. Using the learnings from module 4 students learn how to create effective and useful board reports. This data is put into actionable boardroom strategies to optimize cyber resilience. These include four major areas:

- **Protecting the digital assets**
  - o What are our most valuable digital assets? Which ones are crown jewels?
  - o How much investment is needed to lower cyber risk to acceptable thresholds?
  - How much financial exposure do we have related to a data breach, ransomware, business interruption and regulatory loss?
  - o How much hidden exposure do we have?
  - o How do digital assets compare in terms of cyber risk?
  - o Which digital assets are above their risk thresholds? By how much and why?
  - How effective is our cyber program?
  - o What are the gaps in our cyber program?
  - o What initiatives should we prioritize to lower risk?
  - o Do we have enough cyber budget?
  - o Do we have enough resources and how do we prioritize them?
- **Cyber Risk Transference**
  - o Do we have enough cyber insurance?
  - o How much do we need exactly?
  - o Are our sub-limits on ransomware, business interruption and regulatory loss enough?
  - o What is our ransomware strategy?
- **Vendor Cyber Risk**
  - o What relationships do we have with vendors associated with our digital assets?
  - o How much financial exposure and cyber risk do we have with these third parties? How can we reduce it?
  - o How effective are the vendors' cyber controls?
- **M&A Cyber Risk**
  - o We are planning to sell the company-how does our cyber resiliency impact our acquisition price?
  - o 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%)
- Labs (50%)