CYBER
INTELLIGENCE 4U

PACE
UNIVERSITY

Seidenberg School of Computer
Science and Information Systems

Cyber Intelligence 4U Pace Seidenberg

Cybersecurity Insurance In Digital Business Course
2022-2023 Syllabus

CYBER
INTELLIGENCE 4U

Table of Contents

CYBER
INTELLIGENCE 4U

Cybersecurity Insurance In Digital Business Course 2022-2023

Program Overview
The Cyber Insurance in Digital Business Course is a certification program which provides agents, reinsurance experts and brokers with a deeper understanding of industry best practices in cyber security risk management, governance, privacy, compliance and operations.

Students will learn what high-performing agents and brokers need to know in order to thrive in their roles, including how to interact with executive leadership of potential customers, how to provide analysis and support in effective cyber risk management, and how to build and maintain strong relationships with prospective cyber risk insurance clients.

Cyber is a business issue. This is a program about business impacts. The best cyber insurance professionals understand the intersection of privacy, compliance and risk and have a good foundational cyber understanding. This course provides them with a well-rounded solid skill set of core cyber business acumen in terms of analytical skills, and critical thinking focused on cyber risks and their relationship to cyber insurance.

This course is about creating thought leaders and critical thinkers who can bridge these gaps. This course is holistic and starts with the basics, covering terminology, breach case studies, cyber programs, 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 quantify cyber risk exposures and score the risk of the digital assets that demonstrate gaps in the asset themselves, the controls and how threats, vulnerates and incidents impact cyber risk.

The Cybersecurity Insurance in Digital Business Course is a rigorous 5-day in person or self-paced online curriculum led by prominent cybersecurity experts, many of whom advise governments, insurance firms, and industry bodies around the world. The course 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: Carriers, Cyber Insurance Broker, Reinsurance Specialist and Business Development Professions in Cyber Insurance.

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 crown jewel exposures, identify hidden exposures, determine cyber insurance adequacy, risk accumulation metrics and actuarial analysis using digital assets.
- 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 metrics and that empower the cyber insurance company.
-

- A premier certificate from Pace Seidenberg's School of Computer Science and Information Systems, 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: The Evolution of Cybersecurity & Cybersecurity Basics

Module Description

This module introduces 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 insurance evolved out of property and casualty into a true digital asset-based program. It addresses key cyber-related business consequences and demonstrates the consequences of poor cyber hygiene and reviews cybersecurity trends that impact the insurance industry.

In addition to the evolution of cyber from an insurance perspective, students learn to communicate in the language of cybersecurity, study data breaches and business interruptions and their impact on the firm from a financial and insurance outlook, 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 introduces 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.
- **Technology Regulations** – Including BIPA 740 ILCS/14 and Public Act 095-994 Biometric Information Privacy Act and California IoT Security Act

Module Grade
Each student is expected to satisfy the following requirements:

- Quizzes (50%)
- Security Assessment Lab (50%)

CYBER
INTELLIGENCE 4U

Module 3: Cyber Insurance Overview

Module Description

This module includes Cyber incident response trends and statistics, Cyber threat environment Hot Topics, Cyber risk management 101, Traditional cyber insurance coverage, Gap analysis discussion (Cyber/ Other P&C Products) and compares cyber insurance stand-alone policy attributes to property and casualty policy attributes and identities the typical gaps in the coverage. Covers TPRM aspects of shared responsibility model for control effectiveness.

The module also explores the hardening cyber market causes and conditions in a post covid world.

Here are the main objectives found in this module are understand cyber independently and interdependently with Casualty and Property covering:

- Coverage Types
- First Party Coverage
- Third Party Coverage
- Gaps and Overlaps

Module Grade

Each student is expected to satisfy the following requirements:

- Quizzes (100%)

CYBER
INTELLIGENCE 4U

Module 4: Digital Asset Quantification

Module Description
This module provides cyber risk metric quantification for financial exposures aligned to how the carrier will pay a cyber insurance claim. Each metric has been vetted with the cyber insurance industry, academic and analyst community. Financial quantification is the beginning of understanding limits adequacy, risk accumulation metrics and actuarial analysis.

The main objectives found in this module are to learn how to calculate cyber financial exposures including:

- Data Exfiltration Exposure
- Ransomware Exposure
- Business Interruption Exposure
- Regulatory Exposures
    - GDPR
    - CCPA
    - NYS DFS
    - HIPAA
    - Privacy State Regs
    - International Regs

Module Grade
Each student is expected to satisfy the following requirements:

- Quizzes (30%)
- Security Assessment Lab (70%)

CYBER
INTELLIGENCE 4U

Module 5: Cyber Insurance Limits Adequacy

Module Description
This module uses the digital asset approach to quantify accurate limits and identify hidden exposures that are greater than the cyber insurance limit with mitigating recommendations to reduce that risk.

The main objectives found in this module are to learn how to calculate cyber insurance limits and sublimits including:

- Data Exfiltration Limit
- Ransomware Dependent Sublimit
- Ransomware Non-Dependent Sublimit
- Business Interruption Dependent Sublimit
- Business Interruption Non-Dependent Sublimit
- Regulatory Sublimits
    - GDRP
    - US Privacy
    - PCI
    - Healthcare

Module Grade
Each student is expected to satisfy the following requirements:

- Quizzes (30%)
- Security Assessment Lab (70%)

CYBER
INTELLIGENCE 4U

Module 6: Cyber Insurance Risk Scoring

Module Description
This module uses the digital asset approach to score the inherent cyber risk. Inherent cyber risk can be used understand the likelihood that a company will have specific cyber events or incidents based on their digital asset behavioral and user behavior. Mitigating recommendations can be made to lower these risks.

The main objectives found in this module are to learn how to attributes related to the likelihood calculations associated with inherent cyber risk including:

- PAM Risk
- IDAM Risk
- Technology Risk
- Location Risk
- Access Risk
- Interface Risk
- User Risk
- Privacy Risk
- Confidentiality Risk
- Integrity Risk
- Availability Risk
- Dozens of Others

Module Grade
Each student is expected to satisfy the following requirements:

- Quizzes (30%)
- Security Assessment Lab (70%)

CYBER
INTELLIGENCE 4U

Module 7: Cyber Controls

Module Description
This module allows students to understand cybersecurity controls across multiple frameworks and to align the risk mitigation effectiveness to the controls.

The main objectives found in this module include understanding cyber controls from a likelihood perspective. Controls covered include:

- Access Controls
- Encryption Controls
- IDAM Controls
- PAM Controls
- Vulnerability Controls
- Patch Management Controls
- User Awareness Controls
- End Point Security Controls
- Application Security Controls
- Dozens of Others

Module Grade
Each student is expected to satisfy the following requirements:

- Quizzes (30%)
- Security Assessment Lab (70%)

CYBER
INTELLIGENCE 4U

Module 8: Continuous Control Monitoring

Module Description
This module allows for the continuous monitoring of cyber controls. Inherent cyber risk can be used understand the likelihood that a company will have specific cyber events or incidents based on their digital asset behavioral and user behavior. Mitigating recommendations can be made to lower these risks.

The main objectives found in this module are to learn how to attributes related to the likelihood calculations associated with inherent cyber risk including:

- PAM Risk
- IDAM Risk
- Technology Risk
- Location Risk
- Access Risk
- Interface Risk
- User Risk
- Privacy Risk
- Confidentiality Risk
- Integrity Risk
- Availability Risk
- Dozens of others

Module Grade
Each student is expected to satisfy the following requirements:

- Quizzes (30%)
- Security Assessment Lab (70%)

CYBER
INTELLIGENCE 4U

Module 9: Risk Accumulation Metrics

Module Description

This module provides the student with the means to understand risk accumulation metrics in cyber insurance. Using the digital asset approach allows for aggregation of risk across the portfolio from a digital perspective.

The main objectives found in this module are to understand the different types of risk accumulation and to calculation them including:

- Cloud Risk
- IoT Risk
- Technology Risk
- Location Risk
- Access Risk
- Interface Risk
- User Risk
- Privacy Risk
- Confidentiality Risk
- Integrity Risk
- Availability Risk
- Dozens of others

Module Grade

Each student is expected to satisfy the following requirements:

- Quizzes (30%)
- Security Assessment Lab (70%)

CYBER
INTELLIGENCE 4U

Module 10: Good Cyber Hygiene Discounts

Module Description
This module provides the student with the means to understand how to provide a cyber discount program based on good cyber hygiene. Each student will be able to utilize the cyber controls to determine how to discount policies based on risk mitigation.

The main objectives found in this module include the ability to map behavior to control mitigation and create discount models based on the following:

- Access Controls
- Encryption Controls
- IDAM Controls
- PAM Controls
- Vulnerability Controls
- Patch Management Controls
- User Awareness Controls
- End Point Security Controls
- Application Security Controls
- Dozens of Others

Module Grade
Each student is expected to satisfy the following requirements:

- Quizzes (30%)
- Security Assessment Lab (70%)