CYBER
INTELLIGENCE 4U

Cyber Intelligence 4U
Seton Hall University

Fast Track Enterprise Cybersecurity in Digital Business
Basic Certificate Program
2024 Syllabus

CYBER
INTELLIGENCE 4U

Table of Contents

CYBER
INTELLIGENCE 4U

Fast Track Enterprise Cybersecurity in Digital Business Basic Certificate Program 2024

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 a well-rounded, solid skill set of core business acumen in terms of analytical skills and critical thinking focused on cyber risks. This program creates thought leaders and critical thinkers who can bridge these gaps. This holistic program 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 models.

The Fast Track Enterprise Cybersecurity in Digital Business Basic Certificate Program is a self-paced online curriculum led by prominent cybersecurity experts, many of whom advise governments, agencies, and industry bodies worldwide. 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, and 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 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 ValuRisQ 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 and access to a global network of like-minded 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 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 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 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 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, endpoints, 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), the Securities Exchange Commission (SEC), the 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, and 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 fictitious 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 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 Top20 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 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 system weaknesses, 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 deep and dark web data and call spam propagation and botnet 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 regarding budget, insurance, and cyber tools with long-term consequences. Cyber risk is measured with two metrics – exposures and scores using impact and likelihood data. This module allows students to quantify cyber exposures and measure cyber risk scores. It demonstrates the use cases for cyber exposures, including crown jewel asset strategies, identifying hidden exposures and vendor exposures, calculating cyber insurance limits and sub-limits, and M&A due diligence.

Students learn how to measure inherent cyber risk, residual cyber risk, the effectiveness of cybersecurity controls, and its relationship to risk mitigation. Demonstration of use cases, including identifying gaps in the organization's cybersecurity program and their vendor's 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 characteristics of digital assets and how they are 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 4: 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 digital assets. Effective strategies require an understanding of cyber maturity and useful metrics that are digestible to risk owners. This module provides students with 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, processes, and tools. Students learn to translate cyber risk metrics into actionable boardroom strategies to optimize cyber resilience. These include four major areas:

1. **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?

2. **Cyber Risk Transference**

- Do we have enough cyber insurance?
- How much do we need exactly?
- Are our sub-limits on ransomware, business interruption, and regulatory loss enough?
- What is our ransomware strategy?

3. **Vendor Cyber Risk**

- What relationships do we have with vendors associated with our digital assets?
- How much financial exposure and cyber risk do we have with these third parties? How can we reduce it?
- How adequate are the vendors' cyber controls?

4. **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?

CYBER
INTELLIGENCE 4U

Module Grade

Each student is expected to satisfy the following requirements:

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