Cyber Intelligence 4U

Cyber Risk Management Cybersecurity Certificate Program 2022-2023 Syllabus

CYBER
INTELLIGENCE 4U

Table of Contents

Program Overview

Cyber is a business issue. 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. The course is based on three years of research with the Fortune 1000 and cyber insurance industry to understand why businesses cannot be cyber resilient and how to get the business and cyber team to speak the same language. In 2001, 10% of a business was digital, today 85% of an organization's value is digital.

This program is about creating thought leaders and critical thinkers who can bridge these gaps. This program is based on digital asset risk. Cyber criminals attack your digital assets. They steal your data, interrupt your business processes with ransomware or denial of service and cause regulatory penalties and fines based on the type of data you store and process in your systems. In additional to quantifying exposures, it moves deeper into the integrated cyber risk perspective while exploring the newest regulations, security assessment frameworks, cybersecurity tool data and cyber strategy using hands on learning to inventory digital assets, perform privacy assessments, quantify exposures and risk model among others.

The Cyber Risk Management 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, and Vendor Team Members.

Students will be empowered by:
The ability to quantity cyber risk and score cyber risk based on the digital asset methodology. The digital asset methodology is used by the Israeli Prime Minister's Office and other governments. Students will understand cyber holistically from a business perspective across regulation, compliance, security standards and risk. Students will be able to measure cyber resiliency and strategize how to lower cyber risk and work with stakeholders to increase cyber resilience.

Lab work includes 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. This 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 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.

Module 1: Introduction to Digital Assets

Module Description

This module provides an introduction to the digital asset approach to cyber risk management. Digital asset metrics can be used by boards and CISOs to show cybersecurity from a business point of view. The course is based on three years of research with the Fortune 1000 and cyber insurance industry to understand why businesses cannot be cyber resilient and how to get the business and cyber team to speak the same language. 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 do a lab assignment, which 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, 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%)
Digital Asset Lab (70%)

Module 2: Cyber Risk Exposures - Quantification

Module Description

Cyber risk exposures are quantified amounts of financial impacts from a data breach, business interruption or regulator. This module provides an introduction to the design of cybersecurity risk algorithms and their usage in privacy, compliance, cyber risk management and cyber insurance. Modeling includes data exfiltration due to malware or misconfiguration, business interruption due to ransomware or denial of service attacks and regulatory exposures. Regulatory exposures covered are those that can be levied by the Department of Health and Human Services for the Healthcare Information Portability and Accounting Act (HIPAA), the Payment Card Security Council for the Payment Card Industry Data Security Standard (PCI-DSS), the European Union Supervisory Authority for the General Data Protection Regulation (GDPR), the Attorney General of California for the California Consumer Protection Act (CCPA) and more. Students learn how to associate the quantification metrics to use cases for monitoring digital asset risk, identifying hidden exposures and cyber insurance limits and sub-limits used in the board reporting. Students are required to do a cyber risk exposure lab using the VRisk product.

Module Grade

Each student is expected to satisfy the following requirements:

Quizzes (30%)
Risk Modeling Exposure Lab (70%)

Module 3: Inherent Cyber Risk Scoring

Module Description

Inherent cyber risk is the risk without the controls in place. It is raw risk, or as if there is zero percent effectiveness of controls. We also call this cybergeddon risk. This module provides an introduction to the theory, and algorithms to measure inherent cyber risk. Students learn how to measure user and asset behavioral analytics to provide insight into the inherent riskiness of a digital asset. In this module, students will understand how digital assets, protection mechanisms and user behaviors work in concert to measure likelihood. Over 20 different asset and user behavior attributes and protection mechanisms are introduced.

Students will explore the attributes related to data privacy and understand how to measure integrity and confidentiality of data. Students are required to do a cyber risk scoring lab using the VRisk product.

Module Grade

Each student is expected to satisfy the following requirements:
Quizzes (30%)
Inherent Cyber Risk Lab (70%)

Module 4: Security Control Assessments

Module Description

Security Control Assessments are not risk assessments. They are a test of the security controls required to be in place for the company. This module provides a deep dive into cybersecurity control frameworks and their relationship to inherent cyber risk. Students will learn all the security controls that are required to be in place to ensure integrity, confidentiality and availability. Students will learn the means to demonstrate the effectiveness of the cybersecurity controls and to identify the trends and gaps across the digital assets.

In this module, students will learn the requirements and which control tests that are required and how to map these requirements across frameworks. Students create algorithms to show the effectiveness of the cybersecurity controls and their relationship to inherent cyber risk. Students are required to do a control assessment lab using the VRisk product.

Here are the main control assessment frameworks covered in the module:

- NIST Cybersecurity Framework
- NIST 800-53
- ISO 27001
- COBIT 5
- ITIL 4
- PCI-DSS

Module Grade

Each student is expected to satisfy the following requirements:

- Quizzes (30%)
- NIST Cybersecurity Framework Lab (70%)

Module 5: Residual Cyber Risk Scoring

Module Description

Cyber risk increases when there is a weakness in a system, incident or threat to the data. Residual cyber risk is the risk with cyber controls in place and uses data that is ingested from cybersecurity tools such as vulnerabilities from a vulnerability management scanner (VMS), security incident event management (SIEM) system, or advanced persistent threat (APT) technologies.

This module provides a deep dive into the digital asset relationships of technologies and their weaknesses, data breaches, business interruptions, and attackers malicious acts. Students create residual risk algorithms based on the type of data that the cybersecurity tool provides.

Residual cyber risk modeling is taught to demonstrate when cyber risk rises above thresholds based on the cyber risk tolerances and asset classifications. Students are required to do a residual risk lab using the VRisk product.

The module covers the main cybersecurity tool data types including:

- Vulnerability management scanner (VMS)
- Security incident event management (SIEM) system
- Advanced persistent threat (APT) technologies

Module Grade

Each student is expected to satisfy the following requirements:

Quizzes (30%)
Residual Cyber Risk Lab (70%)

CYBER
INTELLIGENCE 4U

Module 6: Board Reporting

Module Description

Providing metrics to the hoard that are digestible and actionable is the job of the cyber risk manager. Without tone at the top there is not enough support to have an effective cybersecurity program. This module provides a board reporting metrics that are based on the data that the student developed in the previous five modules.

The module focuses on the key elements of board reporting including:

- Demonstration of protection of the digital assets – Cyber Program Effectiveness
- Vendor cyber risk exposures and cyber program gaps
- M&A due diligence
- Cyber insurance limit and sublimit needs

In this module, students will utilize the VRisk platform to create a board report that includes:

Digital Asset Cyber Risk Program Effectiveness

- 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?
- What is our cyber resiliency and how do we increase it?
- 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?
- How can we continuously monitor a risky vendor?

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 (30%)
Board Report (70%)