CYBER
INTELLIGENCE 4U

Cybersecurity Risk Management for Executives Syllabus

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 builds students' understanding of cybersecurity, starting with cybersecurity terminology. It addresses critical cyber-related case studies, demonstrates the consequences of poor cyber hygiene, and reviews cybersecurity trends.

Students learn to communicate in the language of cybersecurity, study data breaches, and 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%)

 66 West Flagler St. Miami FL 33130 info@cyberintelu.com

Module 2: Cybersecurity Regulations (1h)

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.

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%)

Module 3: Cybersecurity Insurance (1h)

Module Description

This module introduces cybersecurity insurance. Many companies must now have cyber insurance to work with the federal government, its contractors, and other commercial entities. Digital asset quantification aligns with how a cyber insurance claim will be paid.

Ransomware has increased exponentially over the past few years. The course provides students with a method for creating an effective ransomware strategy and gauging their preparedness for an 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, gaps in cybersecurity programs that might result in unpaid claims, and how to avoid them. Students also 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 (100%)

Module 4: Cyber Risk Metrics (1hr)

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 and 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 (100%)

Module 5: Third-Party Risk Management (1h)

Module Description

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 part of your digital ecosystem, exponentially multiplying your cyber risk. 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 internal 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 (100%)

Module 6: Summing it all up (.5h)

Module Description

This module summarizes the critical points for executive learning. These include:

- **Protecting the digital assets**

What are our most valuable digital assets? Which ones are crown jewels?

How much investment is needed to lower cyber risk to acceptable thresholds?

How much financial exposure do we have to a data breach, ransomware, business interruption, and regulatory loss?

How much hidden exposure do we have?

How do digital assets compare in terms of cyber risk?

Which digital assets are above their risk thresholds? By how much and why? How effective is our cyber program?

What are the control 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?

- **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?

- **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?