

Course No. 1925

# Cyber Risk Quantification for Insurance Training Course

---

**CYBER INSURANCE  
INSURANCE & RISK MANAGEMENT**

---

DURATION

**5 Days**

DELIVERY

**Classroom**



## Course Overview

---

The Cyber Risk Quantification for Insurance Training Course provides a practical and analytical framework for measuring cyber risk in financial and insurance terms. The course enables insurance professionals to move beyond qualitative descriptions of cyber exposure and develop structured approaches for estimating potential financial losses, evaluating risk severity, supporting underwriting decisions, and improving portfolio management.

Participants will explore the relationship between cyber threats, vulnerabilities, business dependencies, security controls, and financial consequences. The program examines how cyber events such as ransomware, data breaches, business interruption, technology failures, cloud outages, social engineering, and third-party incidents can be translated into measurable loss scenarios for insurance purposes.

The course addresses quantitative risk assessment methodologies, including frequency and severity analysis, scenario-based quantification, loss distributions, probability assessment, financial impact modeling, sensitivity analysis, stress testing, and aggregation analysis. Particular attention is given to the challenges of limited historical data, rapidly evolving threats, correlated events, systemic cyber risk, and uncertainty in cyber loss estimates.

Participants will also learn how quantified cyber risk can support insurance underwriting, pricing, policy limits, deductibles, reinsurance decisions, capital planning, portfolio optimization, and risk appetite. Through practical exercises, simulated datasets, loss scenarios, and insurance case studies, participants will develop a structured methodology for quantifying cyber risk and translating analytical results into actionable insurance decisions.

## Objectives

---

- By the end of the course, participants will be able to:
- Analyze the principles and applications of cyber risk quantification in insurance.
- Identify key cyber risk drivers and their potential financial consequences.
- Translate cyber threats and vulnerabilities into measurable loss scenarios.
- Assess cyber loss frequency and severity using quantitative approaches.
- Develop financial impact models for major cyber events.

- Apply scenario analysis to ransomware, data breach, and business interruption risks.
- Evaluate the financial impact of third-party and cloud-related cyber incidents.
- Apply probability, uncertainty, and sensitivity analysis to cyber risk estimates.
- Develop loss distributions and estimate potential loss ranges.
- Quantify cyber accumulation, aggregation, and systemic risk exposures.
- Use quantified risk information to support underwriting and pricing decisions.
- Assess appropriate policy limits, deductibles, and risk transfer structures.
- Integrate cyber risk quantification into portfolio and reinsurance decisions.
- Apply stress testing to assess severe but plausible cyber scenarios.
- Communicate quantitative cyber risk results effectively to executives and decision-makers.

## Who Should Attend

---

This course is designed for insurance executives, underwriting managers, senior underwriters, actuarial professionals, risk managers, cyber insurance specialists, portfolio managers, and professionals involved in the financial assessment of cyber risks.

It is also suitable for claims professionals, pricing teams, reinsurance specialists, enterprise risk professionals, cybersecurity and technology risk specialists, data analysts, financial risk professionals, compliance and governance teams, and professionals responsible for evaluating cyber exposure and potential losses.

The program is particularly valuable for insurance organizations seeking to strengthen quantitative cyber risk capabilities, improve risk-based underwriting and pricing, evaluate portfolio accumulation, support reinsurance decisions, and provide management with clearer financial perspectives on cyber exposure.

## Learning Outcomes

---

- By the end of the course, participants will be able to:
- Explain the role of quantitative cyber risk assessment in insurance.
- Identify the data required to quantify cyber risk.
- Develop structured cyber loss scenarios.

- Estimate potential financial losses from cyber events.
- Analyze loss frequency and severity.
- Evaluate direct and indirect cyber-related financial impacts.
- Quantify business interruption and technology dependency losses.
- Assess third-party and cloud concentration risks.
- Apply probability and uncertainty techniques to cyber risk estimates.
- Conduct sensitivity analysis on key loss assumptions.
- Develop quantitative views of cyber aggregation and systemic risk.
- Use stress testing to evaluate severe cyber scenarios.
- Apply quantified risk insights to underwriting and pricing decisions.
- Support decisions regarding limits, deductibles, reinsurance, and risk transfer.
- Interpret quantitative cyber risk outputs for management and decision-makers.
- Develop a practical cyber risk quantification framework for insurance applications.

## Course Outline

---

### DAY 01

## Foundations of Cyber Risk Quantification for Insurance

- Principles and objectives of cyber risk quantification.
- Qualitative versus quantitative cyber risk assessment.
- Cyber threats, vulnerabilities, controls, and financial exposure.
- Identifying critical assets, systems, processes, and dependencies.
- Ransomware, data breach, business interruption, and technology failure scenarios.
- Direct and indirect financial consequences of cyber events.
- Cyber risk drivers across different industries and business models.
- Data requirements for quantitative cyber risk analysis.
- Challenges associated with incomplete and rapidly changing cyber data.
- Establishing assumptions and boundaries for cyber risk models.

## DAY 01 — CONTINUED

**PRACTICAL APPLICATION**

Develop a structured cyber risk profile and identify the key variables required to quantify potential insurance losses.

## DAY 02

## Cyber Loss Frequency, Severity and Financial Impact Modeling

- Principles of cyber loss frequency and severity analysis.
- Identifying loss events and relevant exposure variables.
- Estimating frequency of cyber incidents.
- Assessing potential loss severity.
- Modeling ransomware and extortion losses.
- Quantifying data breach and privacy-related losses.
- Modeling cyber business interruption losses.
- Assessing technology recovery and additional expense losses.
- Evaluating third-party and dependent business interruption losses.
- Developing financial loss assumptions and scenarios.

**PRACTICAL APPLICATION**

Build a simulated cyber loss model covering frequency, severity, direct losses, business interruption, and additional expenses.

## DAY 03

## Scenario Analysis, Probability and Uncertainty

- Scenario-based cyber risk quantification.
- Developing severe but plausible cyber scenarios.
- Probability assessment and loss estimation.
- Understanding uncertainty in cyber risk models.
- Sensitivity analysis and key model assumptions.
- Scenario analysis for major ransomware events.

## DAY 03 — CONTINUED

- Modeling cloud service and technology provider outages.
- Evaluating supply-chain and interconnected cyber risks.
- Stress testing cyber insurance exposures.
- Interpreting ranges of potential losses and confidence levels.

**PRACTICAL APPLICATION**

Quantify a major cyber incident using multiple scenarios and assess how changes in key assumptions affect expected losses.

## DAY 04

## Aggregation, Systemic Risk and Insurance Portfolio Quantification

- Cyber accumulation and aggregation risk.
- Correlated and interconnected cyber events.
- Systemic cyber risk and widespread technology failures.
- Portfolio-level exposure analysis.
- Common technology providers and concentration risk.
- Estimating aggregate losses across multiple insureds.
- Scenario-based portfolio stress testing.
- Assessing potential large-loss events.
- Applying quantitative risk insights to reinsurance and risk transfer.
- Supporting capital planning and risk appetite decisions.
- Portfolio optimization using quantified cyber exposures.

**PRACTICAL APPLICATION**

Analyze a simulated portfolio exposed to a systemic cyber event and quantify the potential aggregate financial impact.

**DAY 05**

## Applying Cyber Risk Quantification to Underwriting, Pricing and Strategic Decisions

- Using quantitative cyber risk information in underwriting.
- Linking quantified exposure to pricing decisions.
- Supporting policy limits and deductible decisions.
- Integrating cyber risk quantification into portfolio management.
- Applying quantitative insights to reinsurance strategy.
- Monitoring changes in cyber exposure throughout the policy lifecycle.
- Model governance, validation, limitations, and documentation.
- Managing uncertainty and avoiding overreliance on model outputs.
- Communicating quantitative cyber risk to senior management.
- Developing cyber risk indicators and quantitative reporting.
- Establishing a sustainable cyber risk quantification framework.

**FINAL WORKSHOP**

Develop an integrated cyber risk quantification framework for an insurance portfolio, including exposure assessment, loss scenarios, frequency and severity analysis, financial impact modeling, uncertainty, stress testing, aggregation, underwriting and pricing applications, reinsurance considerations, and executive reporting.

### Register or Request More Information

Course page: <https://quest-training.com/courses/cyber-risk-quantification-for-insurance-training-course>

Website: <https://quest-training.com>

Email: [info@quest-training.com](mailto:info@quest-training.com)

Phone: +905016771440