QUEST
Professional Center

PROFESSIONAL TRAINING COURSE

Course No. 1923

Cyber Insurance Claims Management Training Course

CYBER INSURANCE
INSURANCE & RISK MANAGEMENT

DURATION
5 Days

DELIVERY
Classroom

Course Overview

The Cyber Insurance Claims Management Training Course provides a comprehensive and practical framework for managing cyber insurance claims from first notification of loss through investigation, coverage assessment, loss quantification, settlement, recovery, and post-claim analysis. The course is designed to strengthen the ability of insurance professionals to manage complex cyber claims while balancing policyholder support, coverage obligations, fraud controls, regulatory requirements, and portfolio profitability.

Participants will explore the characteristics of cyber insurance claims arising from ransomware, data breaches, business interruption, cyber extortion, privacy incidents, technology failures, social engineering, network security events, and third-party cyber incidents. The program focuses on understanding how these events translate into insured losses and how claims professionals can establish a structured and defensible claims-handling process.

The course addresses the end-to-end cyber claims lifecycle, including first notification of loss, triage, coverage analysis, incident investigation, forensic coordination, documentation, loss measurement, business interruption assessment, legal and regulatory considerations, policy interpretation, reserve setting, settlement negotiations, and claims closure. Particular emphasis is placed on managing multiple stakeholders during high-severity cyber incidents.

Participants will also examine emerging challenges such as systemic cyber events, third-party dependencies, cloud outages, ransomware negotiations, privacy obligations, fraud, claims aggregation, and complex causation issues. Through practical case studies, simulations, claims file exercises, and incident scenarios, the course enables participants to develop consistent, efficient, and risk-sensitive approaches to cyber insurance claims management.

Objectives

- By the end of the course, participants will be able to:
- Analyze the characteristics and complexity of cyber insurance claims.
- Apply structured procedures for receiving and triaging cyber claims.
- Assess initial coverage considerations following a cyber incident.
- Identify key information and documentation required for claims investigation.

- Coordinate effectively with forensic specialists, legal advisers, cybersecurity experts, and other stakeholders.
- Evaluate losses arising from ransomware, data breaches, business interruption, and technology failures.
- Assess cyber business interruption and dependent business interruption losses.
- Apply appropriate approaches to loss quantification and claims reserving.
- Identify potential fraud indicators and inconsistencies within cyber claims.
- Evaluate causation, policy triggers, exclusions, sublimits, deductibles, and coverage conditions.
- Manage complex and high-severity cyber claims involving multiple parties.
- Assess systemic, aggregation, and accumulation issues affecting cyber claims.
- Strengthen claims negotiation and settlement practices.
- Improve regulatory, legal, privacy, and documentation compliance throughout the claims lifecycle.
- Develop an effective framework for cyber claims governance, quality assurance, and continuous improvement.

Who Should Attend

This course is designed for claims managers, senior claims professionals, cyber claims specialists, insurance executives, and professionals responsible for managing and evaluating cyber insurance claims. It is particularly relevant to professionals working in commercial insurance, specialty insurance, cyber insurance, claims operations, loss assessment, and complex claims management.

The course is also suitable for underwriters, risk managers, insurance brokers, reinsurance professionals, legal and compliance teams, fraud investigators, internal auditors, cybersecurity professionals, business continuity specialists, and professionals involved in coordinating responses to major cyber incidents.

It is especially valuable for organizations seeking to strengthen cyber claims governance, improve claims handling consistency, enhance loss assessment capabilities, reduce claims leakage, manage complex stakeholder relationships, and improve the overall policyholder experience during cyber incidents.

Learning Outcomes

- By the end of the course, participants will be able to:
- Explain the complete cyber insurance claims management lifecycle.
- Triage cyber claims according to severity, urgency, and potential financial impact.
- Evaluate initial coverage and policy response considerations.
- Identify the information required to investigate cyber incidents and resulting losses.
- Establish appropriate claims investigation strategies.
- Coordinate multidisciplinary teams during major cyber incidents.
- Evaluate ransomware and cyber extortion claims.
- Assess data breach and privacy-related claims.
- Quantify cyber business interruption losses.
- Evaluate dependent business interruption and technology service interruption losses.
- Identify potential fraud, exaggeration, and misrepresentation within cyber claims.
- Assess causation and the relationship between cyber events and insured losses.
- Evaluate policy limits, deductibles, exclusions, sublimits, and coverage conditions.
- Establish appropriate claims reserves based on available evidence and expected exposure.
- Manage settlement negotiations and claims resolution effectively.
- Develop a robust cyber claims governance and quality assurance framework.

Course Outline

DAY 01

Cyber Insurance Claims Landscape and Claims Triage

- Fundamentals of cyber insurance claims management.
- Characteristics of cyber claims compared with traditional insurance claims.
- Major sources of cyber insurance losses.
- Ransomware, data breaches, cyber extortion, and network security incidents.
- Business interruption and technology dependency claims.
- Social engineering and fraudulent transfer claims.
- Third-party cyber liability claims.

DAY 01 — CONTINUED

- First notification of loss and immediate response requirements.
- Cyber claims triage, severity assessment, and escalation.
- Identifying urgent operational, legal, financial, and reputational considerations.

PRACTICAL APPLICATION

Analyze a simulated cyber incident and perform an initial claims notification, triage, severity assessment, and escalation decision.

DAY 02

Coverage Assessment and Cyber Claims Investigation

- Understanding cyber policy structures and coverage triggers.
- Reviewing policy limits, deductibles, sublimits, exclusions, and conditions.
- Determining coverage applicability following a cyber incident.
- Identifying key facts and documentation required for investigation.
- Establishing the claims investigation plan.
- Coordination with cybersecurity specialists and forensic investigators.
- Digital evidence and incident documentation considerations.
- Assessing causation and establishing the connection between the incident and insured loss.
- Legal, regulatory, privacy, and notification considerations.
- Managing communication between the insurer, insured, brokers, advisers, and service providers.

PRACTICAL APPLICATION

Review a simulated cyber claims file and determine the initial coverage position, information requirements, investigation priorities, and stakeholder responsibilities.

DAY 03

Loss Assessment, Business Interruption and Claims Reserving

- Principles of cyber loss measurement and quantification.
- Assessing direct and indirect financial losses.

DAY 03 — CONTINUED

- Cyber business interruption claims.
- Dependent business interruption and third-party service disruption.
- Additional expenses and mitigation costs.
- Data restoration and technology recovery costs.
- Ransom payments and associated response expenses.
- Privacy breach response and notification costs.
- Evaluating financial documentation and loss calculations.
- Establishing and updating claims reserves.
- Identifying uncertainty and potential development in complex cyber claims.

> **PRACTICAL APPLICATION**
>
> Calculate and assess a simulated cyber business interruption claim and develop an appropriate initial claims reserve.

DAY 04

Complex Cyber Claims, Fraud and Settlement Management

- Managing high-severity and complex cyber insurance claims.
- Systemic cyber events and claims aggregation.
- Cloud service provider and technology concentration losses.
- Multiple insureds and interconnected claims.
- Third-party claims and liability considerations.
- Identifying fraud, exaggeration, misrepresentation, and suspicious claim patterns.
- Investigating inconsistencies and validating supporting documentation.
- Claims negotiation strategies and settlement considerations.
- Managing disputes and coverage disagreements.
- Claims leakage prevention and financial control.
- Maintaining the policyholder relationship during difficult claims.

DAY 04 — CONTINUED

PRACTICAL APPLICATION

Conduct a complex cyber claims simulation involving multiple stakeholders, disputed coverage, significant business interruption, and potential fraud indicators.

DAY 05

Cyber Claims Governance, Performance and Strategic Improvement

- Cyber claims governance and accountability.
- Standardizing claims handling procedures and decision-making.
- Claims quality assurance and file review.
- Claims performance indicators and management reporting.
- Monitoring claims frequency, severity, development, and leakage.
- Lessons learned from major cyber incidents.
- Integrating claims insights into underwriting and risk selection.
- Strengthening collaboration between claims, underwriting, risk, cybersecurity, legal, and reinsurance teams.
- Developing cyber claims escalation and incident response protocols.
- Improving claims processes, policyholder experience, and operational resilience.
- Building a continuous improvement framework for cyber claims management.

FINAL WORKSHOP

Develop an integrated cyber insurance claims management framework covering notification, triage, coverage assessment, investigation, forensic coordination, loss quantification, reserving, fraud assessment, settlement, governance, reporting, and post-claim improvement.

QUEST
Professional Center

Register or Request More Information

Course page: https://quest-training.com/courses/cyber-insurance-claims-management-training-course
Website: https://quest-training.com
Email: info@quest-training.com
Phone: +905016771440