



Cyber Insurance Course: Underwriting, Ransomware Cover, Accumulation and Claims



Cyber Insurance Course: Underwriting, Ransomware Cover, Accumulation and Claims

Introduction:

Cyber insurance underwriting, ransomware cover, accumulation and claims are taught in this 5-day course for cyber underwriters, brokers, claims handlers and corporate insurance buyers, who finish with a Cyber Underwriting File and Insurance Programme Design for a case company. Carriers and buyers lose money when security questionnaires are accepted at face value, extortion sublimits are guessed and correlated outage losses are never modelled. Nominees already handle insurance submissions, placements or claims and work through case study on proposal forms, scan evidence and incident cost data. CoreConcept Training Center designed this cyber insurance course.

Course Objectives:

- Profile a company's digital exposure by records held, revenue dependency on systems and reliance on cloud and technology suppliers
- Interpret first-party, third-party, network business interruption and extortion insuring agreements and the exclusions that limit them
- Evaluate underwriting questionnaires, outside-in scan findings and security control evidence to accept, condition or decline a cyber risk
- Set premium, limits, sublimits and retentions for a cyber policy using a rating worksheet and loss scenarios
- Measure accumulation exposure across a cyber book and select reinsurance structures that protect capital
- Activate incident response panels and quantify forensic, restoration, extortion and income loss elements of a cyber claim

Target Audience:

- Cyber and specialty underwriting functions that select, price and set terms for cyber risks
 - Broking and placement functions that prepare cyber submissions and negotiate wordings for clients
 - Claims and loss adjusting functions that handle breach, extortion and outage notifications
 - Corporate risk and insurance functions that buy cyber cover and choose limits and retentions
 - Portfolio, exposure management and reinsurance functions that monitor cyber accumulation
 - Product development functions that design cyber wordings and endorsements
-

Course Outline:

Day 1: Cyber Loss Landscape and Exposure Assessment for Insurers

- Cyber Loss Event Taxonomy for Breach, Extortion and Outage
- Ransomware Extortion Patterns Including Double Extortion and Leak Sites
- Silent Cyber Review of Property and Liability Wordings
- Digital Exposure Profile of Records, Revenue and Dependencies
- Cyber Market Cycle Indicators for Capacity and Rate Movement

Day 2: Cyber Policy Architecture and Coverage Triggers

- First-Party Insuring Agreements for Breach Response and Data Restoration
- Third-Party Insuring Agreements for Privacy and Network Security Liability
- Network Business Interruption Waiting Period and Indemnity Period Design
- Ransomware Extortion Cover and Ransom Payment Conditions
- War, Infrastructure and Prior Acts Exclusions in General Terms

Day 3: Cyber Underwriting, Pricing and Limit Setting

- Cyber Underwriting Questionnaire Review and Follow-Up Question Design
- Security Control Expectations for MFA, Backups and Endpoint Detection
- Outside-In Scan Evidence and Vulnerability Findings in Risk Selection
- Cyber Rating Worksheet with Revenue Bands, Sector Loads and Credits
- Limits, Sublimits, Retentions and Coinsurance for Extortion Cover

Day 4: Accumulation, Reinsurance and Cyber Claims Handling

- Cyber Accumulation Scenarios for Cloud Outage and Widespread Malware
- Aggregate Exposure Monitoring by Shared Technology Dependency
- Cyber Reinsurance Structures Including Quota Share and Event Excess
- Breach Notification Hotline and Incident Response Panel Activation
- Cyber Claims Quantification of Forensics, Restoration and Income Loss

Day 5: Case Study on Cyber Underwriting and Programme Design

- Case Company Submission Pack and Security Questionnaire Responses
 - Case Company Risk Selection Decision and Pricing Rationale
 - Corporate Buyer Limit Benchmarking and Cyber Retention Choice
 - Simulated Ransomware Claim Walkthrough Against the Proposed Wording
 - Cyber Underwriting File and Insurance Programme Design Completion
-

Skills You Will Gain:

- Digital Exposure Profiling
- Cyber Wording Analysis
- Security Control Evaluation
- Cyber Premium Rating
- Extortion Sublimit Setting
- Cyber Accumulation Monitoring
- Incident Response Panel Coordination
- Cyber Loss Quantification

Why Attend This Course:

- Deliver a Cyber Underwriting File and Insurance Programme Design to the head of underwriting, the placing broker or the corporate insurance committee
- Decide whether a cyber risk should be accepted, conditioned on security improvements or declined, and at what limit and retention
- Avoid unpriced silent cyber, guessed extortion sublimits and disputed business interruption claims that erode underwriting results
- Share the rating worksheet, questionnaire follow-up list and claims quantification template with underwriting, broking and claims colleagues

Conclusion:

Back at work, the participant presents the Cyber Underwriting File and Insurance Programme Design to the head of underwriting, the placing broker or the corporate insurance committee. Carriers use it to agree acceptance terms, security conditions and the rate for the next cyber submission, while buyers use it to choose limits, retentions and extortion cover before renewal. After the first notified incident or renewal, the team should compare actual response costs and downtime with the quantified scenarios and adjust sublimits, waiting periods and accumulation assumptions.

Frequently Asked Questions FAQ:

What should participants know before the cyber insurance underwriting, ransomware cover and claims course?

Participants should already handle insurance submissions, placements, claims or a company insurance programme and understand basic policy terms. No technical security skill is needed. An anonymised cyber proposal form, wording or incident report helps them apply the case work.

How does a cyber insurance underwriting and claims course differ from a cyber risk governance course?

It treats cyber risk as an insurable exposure: wordings, questionnaires, rating, sublimits, accumulation, reinsurance and claims quantification. Governance courses address board oversight, risk appetite and security frameworks, and mention insurance only as one risk transfer option.

Why does cyber insurance accumulation matter to insurers and reinsurers?

A single cloud outage or widespread malware event can trigger many cyber policies at once, unlike most property losses. Insurers therefore track shared technology dependencies, model accumulation scenarios and buy reinsurance so one event cannot exhaust capital.

What do participants take back from the cyber insurance underwriting, ransomware cover and claims course?

Participants take back a Cyber Underwriting File and Insurance Programme Design with an exposure profile, questionnaire follow-up list, rating worksheet, limit and retention structure, accumulation note and a claims quantification template.
