Training Course on Cyber Insurance and Incident Response Readiness

Professional Development Training Course Outline

Category	Digital Forensics	**Duration**	10 Days
Base Fee	$3,000 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

In today’s hyperconnected digital world, cybersecurity threats are no longer a possibility—they are an inevitability. With ransomware attacks, data breaches, and supply chain vulnerabilities on the rise, organizations must not only prepare to respond to cyber incidents but also mitigate financial loss through robust cyber insurance coverage. Training Course on Cyber Insurance and Incident Response Readiness equips participants with critical insights into incident response planning, cyber risk assessment, insurance policy evaluation, and legal compliance frameworks. It ensures participants are ready to face modern threats with confidence.

This course is ideal for professionals looking to enhance their organization's incident response posture, reduce downtime during breaches, and understand the nuances of cyber insurance underwriting. Learners will gain practical knowledge through hands-on modules, real-world case studies, and expert-guided sessions that align with global standards such as NIST, ISO 27001, and GDPR. Whether you're an IT manager, legal counsel, risk officer, or business leader, this course positions you to proactively defend, respond, and recover from cyber incidents while optimizing your insurance strategy.

Programme Curriculum

Training Course on Cyber Insurance and Incident Response Readiness

Introduction

In today’s hyperconnected digital world, cybersecurity threats are no longer a possibility—they are an inevitability. With ransomware attacks, data breaches, and supply chain vulnerabilities on the rise, organizations must not only prepare to respond to cyber incidents but also mitigate financial loss through robust cyber insurance coverage. Training Course on Cyber Insurance and Incident Response Readiness equips participants with critical insights into incident response planning, cyber risk assessment, insurance policy evaluation, and legal compliance frameworks. It ensures participants are ready to face modern threats with confidence.

This course is ideal for professionals looking to enhance their organization's incident response posture, reduce downtime during breaches, and understand the nuances of cyber insurance underwriting. Learners will gain practical knowledge through hands-on modules, real-world case studies, and expert-guided sessions that align with global standards such as NIST, ISO 27001, and GDPR. Whether you're an IT manager, legal counsel, risk officer, or business leader, this course positions you to proactively defend, respond, and recover from cyber incidents while optimizing your insurance strategy.

Course Objectives

By the end of this course, participants will be able to:

1. Understand core principles of cyber insurance policies and coverage models
2. Evaluate cyber risk exposure and map it to relevant insurance solutions
3. Design an incident response plan (IRP) based on NIST and ISO best practices
4. Conduct cyber risk assessments to identify potential threats and vulnerabilities
5. Analyze policy exclusions and hidden clauses in insurance contracts
6. Integrate regulatory compliance (GDPR, HIPAA, CCPA) into insurance planning
7. Simulate data breach response workflows and chain-of-command strategies
8. Assess the financial implications of ransomware and data extortion
9. Understand the cyber insurance claims process from filing to settlement
10. Collaborate with legal, risk, and IT teams to align response and coverage
11. Prepare for insurance audits and security hygiene reviews
12. Leverage cybersecurity frameworks to improve insurability
13. Examine case studies of real-world attacks and insurance impact

Target Audiences

1. Chief Information Security Officers (CISOs)
2. IT Security Managers
3. Risk Management Officers
4. Compliance and Legal Advisors
5. Insurance Brokers and Underwriters
6. Incident Response Team Members
7. Business Continuity Planners
8. Cybersecurity Consultants

Course Duration: 10 days

Course Modules

Module 1: Introduction to Cyber Insurance

- What is cyber insurance?
- Market trends and evolution
- Policy types and coverage tiers
- Common exclusions and limitations
- Role of insurers in incident recovery
- **Case Study:** Capital One breach and insurance implications

Module 2: Understanding Cyber Risk

- Categories of cyber threats
- Risk quantification and exposure
- Cybersecurity frameworks overview
- Mapping threats to policy needs
- Internal vs. external threat models

- **Case Study:** Equifax breach risk assessment

Module 3: Regulatory and Compliance Landscape

- Overview of global data privacy laws
- GDPR, HIPAA, CCPA, and their impact
- Cyber insurance compliance challenges
- Legal liabilities and enforcement
- Compliance as a risk control factor
- **Case Study:** Marriott GDPR violation

Module 4: Incident Response Planning

- Building an incident response team
- Phases of incident response (NIST model)
- Roles and responsibilities
- Communication plans and escalation
- Documentation and evidence handling
- **Case Study:** Norsk Hydro's IR strategy

Module 5: Cybersecurity Frameworks and Readiness

- NIST CSF and ISO 27001
- Framework mapping to insurance
- Security control implementation
- Maturity assessments
- Continuous monitoring tools
- **Case Study:** Small business ISO alignment

Module 6: Insurance Underwriting Process

- What underwriters look for
- Security posture evaluation
- Insurance application process
- Third-party vendor risk considerations
- Underwriting questionnaires
- **Case Study:** Retail company underwriting rejection

Module 7: Cyber Insurance Policy Analysis

- Policy components
- Deductibles and limits
- Business interruption coverage
- Legal and forensic costs
- Subrogation clauses
- **Case Study:** Hospital chain policy payout

Module 8: Claims Process and Incident Reporting

- Steps to initiate a claim
- Insurer response time expectations
- Documentation requirements
- Working with forensic investigators
- Post-incident insurer review
- **Case Study:** Manufacturing firm ransomware claim

Module 9: Business Continuity & Disaster Recovery

- Linking BCP/DR to insurance
- Data backup and recovery best practices
- Role of insurance in DR plans
- Crisis communication
- Operational resilience metrics
- **Case Study:** COVID-era BCP failures

Module 10: Financial Impact of Cyber Incidents

- Estimating financial losses
- Loss of revenue vs. reputational damage
- Forensic cost breakdown
- Regulatory fines and penalties
- Role of insurance in cost mitigation
- **Case Study:** Sony Pictures breach fallout

Module 11: Ransomware & Extortion Coverage

- Common ransomware attack vectors
- Negotiation and ransom payment
- Insurance position on payment
- Role of law enforcement
- Crypto tracing and recovery
- **Case Study:** Colonial Pipeline attack

Module 12: Third-Party and Vendor Risk

- Importance of supply chain security
- Insurance requirements for vendors
- Shared responsibility in breaches
- Due diligence best practices
- Legal implications in third-party coverage
- **Case Study:** Target breach via HVAC vendor

Module 13: Security Hygiene and Insurability

- Importance of patching and updates
- MFA and endpoint protection
- Employee training
- Security audits and scoring
- Improving insurability through controls
- **Case Study:** SMB insurance denial due to weak hygiene

Module 14: Legal and Ethical Considerations

- Ethics in ransomware negotiation
- Data privacy and human rights
- Legal defenses in insurance litigation
- Attorney-client privilege during IR
- Ethical guidelines for CISOs
- **Case Study:** Uber breach cover-up case

Module 15: Simulation and Crisis Drill

- Live response simulation setup
- Role-playing and war-gaming

- Decision tree modeling
- Media and legal response testing
- Debrief and lessons learned
- **Case Study:** Simulated healthcare ransomware drill

Training Methodology

- Instructor-led sessions with cybersecurity insurance experts
- Real-world case study analysis for applied learning
- Interactive simulations of breaches and claims processes
- Group discussions and team exercises
- Quizzes and hands-on policy reviews

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call *+254769199797*

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
23 Nov 2026	04 Dec 2026	Online	$2,000
23 Nov 2026	04 Dec 2026	Physical	$3,000
23 Nov 2026	04 Dec 2026	Physical	$6,000

Start Date	End Date	Location	Price
23 Nov 2026	04 Dec 2026	Physical	$6,000
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 2026	Physical	$9,000
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 2026	Physical	$12,000

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com