Cybersecurity in Supply Chains Training Course

Professional Development Training Course Outline

Category	Logistics and Supply Chain Management	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

The modern supply chain is increasingly dependent on digital technologies, making cybersecurity a critical concern for organizations worldwide. With the integration of cloud computing, IoT devices, and real-time data analytics, supply chains are exposed to evolving cyber threats, including ransomware, phishing attacks, and insider threats. Cybersecurity in Supply Chains Training Course equips participants with the knowledge and practical skills necessary to safeguard supply chain operations, protect sensitive data, and ensure business continuity. Participants will gain a deep understanding of cybersecurity frameworks, risk management strategies, and proactive measures to mitigate vulnerabilities within the supply chain ecosystem.

This course emphasizes a practical approach, combining theoretical knowledge with real-world case studies, enabling participants to apply cybersecurity best practices in operational settings. Through interactive sessions, hands-on exercises, and industry-relevant examples, learners will develop the ability to identify threats, implement security controls, and respond effectively to cyber incidents. By the end of the course, participants will be prepared to strengthen the cybersecurity posture of their organizations, ensuring resilience against emerging cyber risks in global supply chains.

Programme Curriculum

Cybersecurity in Supply Chains Training Course

Introduction

The modern supply chain is increasingly dependent on digital technologies, making cybersecurity a critical concern for organizations worldwide. With the integration of cloud computing, IoT devices, and real-time data analytics, supply chains are exposed to evolving cyber threats, including ransomware, phishing attacks, and insider threats. Cybersecurity in Supply Chains Training Course equips participants with the knowledge and

practical skills necessary to safeguard supply chain operations, protect sensitive data, and ensure business continuity. Participants will gain a deep understanding of cybersecurity frameworks, risk management strategies, and proactive measures to mitigate vulnerabilities within the supply chain ecosystem.

This course emphasizes a practical approach, combining theoretical knowledge with real-world case studies, enabling participants to apply cybersecurity best practices in operational settings. Through interactive sessions, hands-on exercises, and industry-relevant examples, learners will develop the ability to identify threats, implement security controls, and respond effectively to cyber incidents. By the end of the course, participants will be prepared to strengthen the cybersecurity posture of their organizations, ensuring resilience against emerging cyber risks in global supply chains.

Course Objectives

1. Understand the fundamentals of cybersecurity in supply chain management.
2. Identify and assess risks and vulnerabilities in supply chain networks.
3. Apply cybersecurity frameworks and standards to supply chain operations.
4. Develop incident response strategies for cyber threats in supply chains.
5. Implement secure communication protocols and data protection measures.
6. Analyze real-world cyber attack case studies in supply chain contexts.
7. Explore emerging technologies and their cybersecurity implications.
8. Integrate risk management practices into procurement and logistics processes.
9. Evaluate third-party supplier security and compliance requirements.
10. Develop policies for secure digital collaboration across supply chain partners.
11. Understand regulatory requirements and compliance standards for supply chains.
12. Enhance organizational resilience through proactive cybersecurity strategies.
13. Foster a culture of cybersecurity awareness among supply chain personnel.

Organizational Benefits

- Strengthened protection against cyber threats and data breaches.
- Reduced operational downtime due to improved incident response.
- Enhanced compliance with global cybersecurity standards.
- Increased trust among partners and clients.
- Optimized supply chain risk management practices.
- Improved monitoring and detection of cyber vulnerabilities.
- Minimized financial losses from cyber attacks.
- Enhanced employee cybersecurity awareness and engagement.
- Streamlined secure collaboration across the supply chain ecosystem.
- Better preparedness for emerging cybersecurity challenges.

Target Audiences

1. Supply chain managers and coordinators
2. IT security professionals and analysts
3. Procurement officers and logistics managers
4. Risk management and compliance officers

5. Operations managers in manufacturing and distribution
6. Cybersecurity consultants
7. Business continuity and disaster recovery planners
8. Organizational leaders responsible for digital transformation

Course Duration: 5 days

Course Modules

Module 1: Introduction to Cybersecurity in Supply Chains

- Overview of cybersecurity challenges in supply chains
- Key components of digital supply chain security
- Threat landscape analysis for global supply chains
- Security policies and frameworks for supply chains
- Case study: Cyber attack on a global logistics provider
- Hands-on exercise: Risk assessment of a supply chain network

Module 2: Risk Assessment and Vulnerability Management

- Identifying and evaluating supply chain vulnerabilities
- Tools for cyber risk assessment
- Prioritizing critical assets and data protection
- Supplier risk evaluation techniques
- Case study: Breach in supplier network
- Practical activity: Risk scoring and mitigation planning

Module 3: Cybersecurity Frameworks and Standards

- NIST Cybersecurity Framework application in supply chains
- ISO 27001 and supply chain security compliance
- Industry-specific cybersecurity standards
- Best practices for implementing frameworks
- Case study: Compliance failure in a manufacturing supply chain
- Group exercise: Framework implementation simulation

Module 4: Incident Response and Recovery

- Developing effective incident response plans
- Cyber attack detection and reporting protocols
- Business continuity and disaster recovery integration
- Crisis communication strategies
- Case study: Ransomware attack on a distribution network

- Simulation exercise: Incident response drill

Module 5: Data Protection and Secure Communication

- Encryption and secure data transfer methods
- Protecting intellectual property in supply chains
- Cloud security for supply chain operations
- Secure collaboration tools and platforms
- Case study: Data leak from third-party vendor
- Hands-on activity: Implementing secure communication channels

Module 6: Emerging Technologies and Cybersecurity

- IoT and AI in supply chains: security implications
- Blockchain applications for secure supply chains
- Predictive analytics and cyber threat detection
- Cybersecurity in autonomous logistics systems
- Case study: AI-enabled supply chain attack scenario
- Practical demonstration: IoT device vulnerability testing

Module 7: Supplier and Third-Party Risk Management

- Supplier vetting and cybersecurity assessments
- Contractual requirements for cybersecurity
- Continuous monitoring of supplier networks
- Incident management with third parties
- Case study: Supplier data compromise
- Group exercise: Supplier cybersecurity audit

Module 8: Building a Cybersecurity Culture in Supply Chains

- Training and awareness programs for employees
- Developing a cybersecurity-first mindset
- Reporting mechanisms for internal threats
- Leadership and accountability in cybersecurity
- Case study: Organizational culture affecting security posture
- Workshop: Designing an internal awareness campaign

Training Methodology

- Interactive lectures and expert presentations

- Hands-on practical exercises and simulations
- Real-world case study analyses and discussions
- Group activities and scenario-based workshops
- Risk assessment and mitigation exercises
- Evaluation through quizzes, assignments, and simulations

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	27 Nov 2026	Online	$1,000
23 Nov 2026	27 Nov 2026	Physical	$1,500
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$3,000

Start Date	End Date	Location	Price
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$4,500
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$6,000

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

Register Online Now

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