Cyber Threats in Logistics 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 rapid advancement of technology in logistics and supply chain operations has created new opportunities for efficiency, transparency, and real-time tracking. However, this digital transformation has also exposed logistics organizations to a growing number of cyber threats, including ransomware attacks, phishing schemes, data breaches, and industrial espionage. Protecting sensitive operational data, maintaining system integrity, and ensuring uninterrupted supply chain operations have become critical priorities for logistics managers, IT professionals, and organizational leadership. Cyber Threats in Logistics Training Course equips participants with the knowledge, skills, and strategies to proactively identify, mitigate, and respond to cyber threats, ensuring the resilience and security of logistics operations in an increasingly digital environment.

Participants will gain hands-on insights into cybersecurity frameworks, risk assessment methodologies, and real-world threat simulations specific to logistics environments. The course emphasizes both technical and managerial approaches, enabling participants to develop comprehensive cyber defense strategies, implement robust security protocols, and foster a culture of security awareness within their organizations. By the end of the course, participants will be capable of safeguarding supply chain networks, protecting sensitive data, and minimizing operational disruptions caused by cyber incidents.

Programme Curriculum

Cyber Threats in Logistics Training Course

Introduction

The rapid advancement of technology in logistics and supply chain operations has created new opportunities for efficiency, transparency, and real-time tracking. However, this digital transformation has also exposed logistics organizations to a growing number of cyber threats, including ransomware attacks, phishing schemes, data

breaches, and industrial espionage. Protecting sensitive operational data, maintaining system integrity, and ensuring uninterrupted supply chain operations have become critical priorities for logistics managers, IT professionals, and organizational leadership. Cyber Threats in Logistics Training Course equips participants with the knowledge, skills, and strategies to proactively identify, mitigate, and respond to cyber threats, ensuring the resilience and security of logistics operations in an increasingly digital environment.

Participants will gain hands-on insights into cybersecurity frameworks, risk assessment methodologies, and real-world threat simulations specific to logistics environments. The course emphasizes both technical and managerial approaches, enabling participants to develop comprehensive cyber defense strategies, implement robust security protocols, and foster a culture of security awareness within their organizations. By the end of the course, participants will be capable of safeguarding supply chain networks, protecting sensitive data, and minimizing operational disruptions caused by cyber incidents.

Course Objectives

1. Understand the evolving landscape of cyber threats in logistics and supply chain management
2. Identify common attack vectors targeting logistics operations
3. Analyze vulnerabilities in transportation management systems (TMS) and warehouse management systems (WMS)
4. Implement cybersecurity best practices for logistics networks
5. Develop incident response plans for cyber attacks
6. Evaluate cybersecurity frameworks such as NIST and ISO 27001 in logistics contexts
7. Utilize risk assessment tools to prioritize security investments
8. Apply encryption, access controls, and monitoring solutions effectively
9. Conduct penetration testing and vulnerability scanning in logistics environments
10. Integrate cybersecurity awareness programs for logistics staff
11. Examine legal and regulatory compliance requirements related to logistics cybersecurity
12. Assess emerging threats such as IoT and AI-based logistics attacks
13. Enhance organizational resilience against supply chain disruptions due to cyber incidents

Organizational Benefits

1. Strengthened protection of sensitive logistics and supply chain data
2. Reduced risk of operational disruption due to cyber attacks
3. Improved regulatory compliance and risk mitigation
4. Enhanced employee awareness and cybersecurity culture
5. Increased trust among clients and business partners
6. Optimized incident response and business continuity planning

7. Reduced financial losses from cyber-related incidents
8. Improved integration of technology and security in logistics operations
9. Strategic alignment of IT and logistics departments
10. Competitive advantage through proactive cybersecurity management

Target Audiences

1. Logistics managers and supply chain coordinators
2. IT security professionals in logistics companies
3. Operations managers
4. Risk and compliance officers
5. Warehouse managers and supervisors
6. Transportation and fleet managers
7. Business continuity and disaster recovery specialists
8. Consulting firms serving the logistics industry

Course Duration: 5 days

Course Modules

Module 1: Introduction to Cybersecurity in Logistics

- Overview of logistics cybersecurity landscape
- Key terminology and concepts
- Common cyber threats in logistics
- Importance of cybersecurity awareness
- Case Study: Cyber attack on a global shipping company
- Hands-on exercise: Identifying system vulnerabilities

Module 2: Threat Analysis and Risk Assessment

- Types of cyber threats in logistics networks
- Assessing risk levels and vulnerabilities
- Threat modeling and scenario planning
- Tools for cyber risk assessment
- Case Study: Ransomware targeting warehouse management systems
- Group activity: Risk assessment simulation

Module 3: Cybersecurity Frameworks and Standards

- NIST Cybersecurity Framework for logistics
- ISO 27001 and compliance standards
- Security policies and governance
- Regulatory considerations in logistics cybersecurity
- Case Study: Compliance failure in a transportation company
- Hands-on activity: Developing a security policy template

Module 4: Network and System Security

- Securing TMS, WMS, and IoT devices
- Firewall configuration and intrusion detection
- Access controls and authentication
- Encryption techniques for sensitive data
- Case Study: Data breach in IoT-enabled fleet
- Lab exercise: Securing a logistics network

Module 5: Incident Response and Recovery

- Cyber incident response planning
- Communication and reporting procedures
- Containment and eradication of threats
- Post-incident analysis and improvement
- Case Study: Logistics company recovering from cyber attack
- Simulation: Incident response drill

Module 6: Emerging Cyber Threats in Logistics

- AI and machine learning-based attacks
- Phishing and social engineering risks
- Insider threats and human factor risks
- Advanced persistent threats (APTs)
- Case Study: Insider attack in a regional warehouse
- Discussion: Emerging threat mitigation strategies

Module 7: Employee Awareness and Training

- Importance of security culture
- Designing awareness programs
- Phishing simulations and social engineering tests
- Cybersecurity training for logistics staff
- Case Study: Training reduces breach incidents
- Workshop: Developing an awareness campaign

Module 8: Future Trends and Strategic Cybersecurity Planning

- Integrating cybersecurity in digital logistics transformation
- Cloud security in supply chains
- Predictive analytics for threat prevention
- Aligning IT and logistics for resilience
- Case Study: Strategic planning prevents cyber disruption
- Group project: Cybersecurity strategic roadmap

Training Methodology

- Interactive lectures with real-world examples
- Hands-on lab exercises for practical experience
- Case studies for contextual learning
- Group discussions and collaborative projects
- Threat simulation exercises for scenario-based learning
- Continuous feedback and assessment

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
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