

Cybersecurity in Industry 4.0

One-Week Training Program

Objective: Equip participants with a comprehensive understanding of cybersecurity challenges and solutions in Industry 4.0, focusing on legal regulations in Kenya, risk mitigation strategies, and practical implementation to secure industrial systems.

Day 1: Foundations of Cybersecurity and Industry 4.0

Morning Session:

- Welcome and Course Introduction
 - Icebreaker and introductions
 - Overview of Industry 4.0 and cybersecurity challenges
- Fundamentals of Cybersecurity
 - Definitions, history, and evolution of cybersecurity
 - Key concepts: encryption, authentication, access control

Afternoon Session:

- Industry 4.0 Cybersecurity Ecosystem
 - Cyber-physical systems, IoT, big data, and cloud security
 - Threats and vulnerabilities in smart factories
 - Case Studies: Cybersecurity Incidents in Industry
 - Analysis of real-world cyber threats
 - Discussion on challenges and lessons learned
-

Day 2: Risk Assessment and Threat Mitigation

Morning Session:

- Cyber Risk Management
 - Identifying risks in industrial networks
 - Risk assessment frameworks and best practices
- Common Threats in Industry 4.0
 - Ransomware, phishing, insider threats
 - Case studies of major cyber attacks

Afternoon Session:

- Hands-on Workshop: Conducting a Risk Assessment
 - Introduction to tools and frameworks
 - Risk identification and mitigation planning
 - Group Discussion: Implementing Risk-Based Cybersecurity Strategies
-

Day 3: Network Security and Endpoint Protection

Morning Session:

- Securing Industrial Networks
 - Firewalls, IDS/IPS, network segmentation
 - Best practices for OT and IT security convergence
- Endpoint Protection Strategies
 - Securing connected devices and industrial control systems
 - Role of AI and automation in cybersecurity

Afternoon Session:

- Hands-on Workshop: Implementing Network Security Measures
 - Configuring firewalls and intrusion detection systems
 - Simulating and mitigating cyber attacks
 - Panel Discussion: Future Trends in Industrial Cybersecurity
-

Day 4: Data Protection, Incident Response, and Legal Compliance in Kenya

Morning Session:

- Data Security in Industry 4.0
 - Importance of encryption and secure data storage
 - Data privacy and regulatory compliance
- Incident Response Planning
 - Creating an effective incident response plan
 - Cyber threat intelligence and forensics

Afternoon Session:

- Overview of Cybersecurity Laws and Regulations in Kenya
 - The Data Protection Act
 - Computer Misuse and Cybercrimes Act
 - Regulatory bodies and their roles
 - Hands-on Workshop: Compliance and Risk Assessment
 - Evaluating an organization's cybersecurity policies
 - Aligning with legal and regulatory frameworks
-

Day 5: Capstone Project and Presentations

Morning Session:

- Capstone Project Introduction
 - Participants work in teams to design a cybersecurity solution for an industry-specific problem
 - Mentors provide guidance and feedback

Afternoon Session:

- Team Presentations
 - Project pitches with Q&A sessions
 - Peer and instructor evaluations
 - Closing Remarks and Feedback Session
-

Course Deliverables:

- Comprehensive course materials and datasets
- Access to cybersecurity tools and resources
- Certification of completion