Cybersecurity in Public Sector Training Course

Professional Development Training Course Outline

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

Course Introduction

Cybersecurity in the public sector is critical for safeguarding sensitive government data, protecting citizen information, and ensuring the continuity of essential services. As governments increasingly rely on digital infrastructure, cloud services, and interconnected systems, the risk of cyberattacks—including data breaches, ransomware, and state-sponsored threats—has grown exponentially. Cybersecurity in Public Sector Training Course provides public sector professionals with a comprehensive understanding of cybersecurity principles, risk management strategies, and compliance frameworks, enabling them to protect critical infrastructure and sensitive data while maintaining operational resilience.

The training equips participants with practical skills for threat detection, incident response, vulnerability management, network security, and policy enforcement. Participants will explore real-world scenarios, emerging threats, and advanced security technologies. Through hands-on exercises, case studies, and strategic frameworks, learners will be able to implement robust cybersecurity programs, establish governance structures, and promote a culture of security awareness across public sector organizations. The course emphasizes proactive defense, regulatory compliance, and secure digital transformation to strengthen trust and resilience in government operations.

Programme Curriculum

Cybersecurity in Public Sector Training Course

Introduction

Cybersecurity in the public sector is critical for safeguarding sensitive government data, protecting citizen information, and ensuring the continuity of essential services. As governments increasingly rely on digital infrastructure, cloud services, and interconnected systems, the risk of cyberattacks—including data breaches, ransomware, and state-sponsored threats—has grown exponentially. Cybersecurity in Public Sector Training

Course provides public sector professionals with a comprehensive understanding of cybersecurity principles, risk management strategies, and compliance frameworks, enabling them to protect critical infrastructure and sensitive data while maintaining operational resilience.

The training equips participants with practical skills for threat detection, incident response, vulnerability management, network security, and policy enforcement. Participants will explore real-world scenarios, emerging threats, and advanced security technologies. Through hands-on exercises, case studies, and strategic frameworks, learners will be able to implement robust cybersecurity programs, establish governance structures, and promote a culture of security awareness across public sector organizations. The course emphasizes proactive defense, regulatory compliance, and secure digital transformation to strengthen trust and resilience in government operations.

Course Objectives

1. Understand cybersecurity fundamentals and their application in public sector environments.
2. Identify and assess cyber threats targeting public sector systems.
3. Implement risk management frameworks for government networks and data.
4. Develop policies and procedures for compliance with national and international regulations.
5. Apply security measures including encryption, firewalls, and access controls.
6. Detect, respond to, and recover from cyber incidents effectively.
7. Strengthen network security and protect critical infrastructure.
8. Deploy security monitoring tools and threat intelligence platforms.
9. Integrate cybersecurity into public sector digital transformation initiatives.
10. Promote organizational awareness and staff training for cyber hygiene.
11. Evaluate emerging technologies and their security implications.
12. Conduct audits and continuous improvement of cybersecurity programs.
13. Build a culture of resilience and governance in public sector cybersecurity.

Organizational Benefits

- Strengthened protection of sensitive citizen and government data
- Reduced risk of cyberattacks, data breaches, and ransomware incidents
- Improved compliance with national and international regulations
- Enhanced operational resilience for critical government services
- Streamlined incident response and disaster recovery procedures
- Increased employee awareness and adoption of cyber hygiene practices
- Better integration of cybersecurity into digital initiatives
- Reduced financial and reputational losses from cyber incidents
- Improved governance, risk assessment, and reporting frameworks
- Proactive identification of vulnerabilities and mitigation strategies

Target Audiences

- Public sector IT and security officers
- Government cybersecurity managers and analysts
- Policy makers and regulatory compliance officers

- Public sector risk management teams
- Network administrators and system engineers
- Incident response and forensic teams
- Auditors and internal control professionals
- Digital transformation and e-government program managers

Course Duration: 10 days

Course Modules

Module 1: Introduction to Public Sector Cybersecurity

- Overview of cybersecurity in government and public institutions
- Key threats and vulnerabilities affecting public sector systems
- Importance of cybersecurity in digital governance
- Legal and regulatory context for public sector cybersecurity
- Cybersecurity frameworks and standards for government organizations
- Case Study: Cyberattack on a municipal government database

Module 2: Cyber Threat Landscape and Intelligence

- Types of cyber threats: malware, phishing, ransomware, insider threats
- Threat actor profiles: hacktivists, cybercriminals, nation-states
- Intelligence gathering and threat assessment techniques
- Use of open-source intelligence (OSINT) in public sector security
- Prioritizing threats based on criticality and risk impact
- Case Study: Ransomware attack on a government healthcare system

Module 3: Risk Assessment and Management

- Cyber risk identification and assessment methodologies
- Risk prioritization and mitigation strategies
- Integrating cybersecurity risk management into governance
- Establishing a risk register and monitoring processes
- Scenario-based risk modeling and stress testing
- Case Study: Risk assessment for a national identity system

Module 4: Cybersecurity Governance and Policy

- Developing policies, standards, and procedures for public sector cybersecurity
- Role of governance in enforcing security compliance
- Aligning cybersecurity policy with national frameworks and regulations
- Establishing accountability and reporting structures

- Auditing policy adherence and continuous improvement
- Case Study: Implementation of a government-wide cybersecurity policy

Module 5: Network Security and Infrastructure Protection

- Securing government networks and critical infrastructure
- Firewalls, VPNs, intrusion detection and prevention systems
- Network segmentation, monitoring, and access control
- Cloud infrastructure security best practices
- Protecting Internet-of-Things (IoT) and SCADA systems
- Case Study: Securing a city-wide e-governance network

Module 6: Endpoint and Application Security

- Securing endpoints, servers, and workstations
- Application-level vulnerabilities and secure development practices
- Patch management and software update protocols
- Mobile device and remote access security measures
- Security monitoring and automated endpoint defenses
- Case Study: Exploitation of web application vulnerabilities in a public agency

Module 7: Identity, Access Management, and Authentication

- Implementing role-based access control (RBAC)
- Multi-factor authentication and password policies
- Identity lifecycle management in government systems
- Monitoring privileged user access
- Preventing unauthorized access and insider threats
- Case Study: Insider breach through privileged account misuse

Module 8: Incident Response and Crisis Management

- Developing an incident response plan for public sector organizations
- Incident detection, reporting, and escalation protocols
- Forensic investigation techniques and evidence preservation
- Crisis communication and stakeholder management
- Post-incident analysis and lessons learned
- Case Study: Response to a cyber breach in a national tax agency

Module 9: Data Privacy and Protection

- Principles of data privacy and compliance with GDPR and national laws
- Sensitive data classification and handling procedures
- Encryption, anonymization, and secure storage methods
- Protecting citizen data in digital services
- Data sharing protocols and third-party management
- Case Study: Data breach in a government health registry

Module 10: Security Awareness and Training

- Building a culture of cybersecurity within public institutions
- Staff training and awareness campaigns
- Phishing simulations and social engineering awareness
- Security policies communication strategies
- Monitoring training effectiveness and engagement
- Case Study: Organization-wide security awareness program success

Module 11: Cloud Security in Public Sector

- Cloud adoption trends and risks in government services
- Cloud security architecture and best practices
- Governance of cloud service providers
- Secure data migration and cloud monitoring
- Compliance requirements for public sector cloud environments
- Case Study: Cloud migration and incident response planning for a government portal

Module 12: Emerging Technologies and Cybersecurity

- Security implications of AI, blockchain, IoT, and smart cities
- Managing risks from emerging technologies in public sector operations
- Integrating cybersecurity considerations in technology adoption
- Threat modeling for new digital initiatives
- Cybersecurity assessment for government innovation projects
- Case Study: Securing an AI-powered public service system

Module 13: Auditing, Compliance, and Regulatory Oversight

- Conducting cybersecurity audits in public organizations
- Compliance assessment and reporting
- Managing regulatory inspections and findings
- Continuous monitoring for policy adherence
- Integrating audit results into risk and governance programs
- Case Study: Compliance audit of a municipal digital services department

Module 14: Cybersecurity Metrics and Performance Measurement

- Developing KPIs and performance indicators for cybersecurity programs
- Measuring incident response effectiveness
- Monitoring network, system, and policy compliance
- Reporting metrics to management and regulators
- Continuous improvement based on data-driven insights
- Case Study: Performance dashboard implementation for a government IT department

Module 15: Strategic Cybersecurity Program Implementation

- Developing institution-wide cybersecurity strategies
- Resource planning, budget, and investment prioritization
- Scaling cybersecurity initiatives across departments
- Aligning cybersecurity strategy with digital government transformation
- Leadership roles in sustaining a secure public sector ecosystem
- Case Study: National cybersecurity program rollout and lessons learned

Training Methodology

- Instructor-led presentations and conceptual briefings
- Hands-on practical exercises and simulated incident response scenarios
- Group discussions and peer-learning activities
- Case study analysis and real-world application exercises
- Demonstrations of security monitoring tools and compliance checklists
- Continuous assessment, interactive feedback, and action plan development

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
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