Training Course on Cybersecurity Incident Response for Schools

Professional Development Training Course Outline

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

Course Introduction

In today's digital-first learning environments, educational institutions face a rising tide of cyber threats targeting sensitive student data, internal communications, and operational systems. Training Course on Cybersecurity Incident Response for Schools is meticulously designed to empower school administrators, IT staff, and educators with the strategic knowledge, trending practices, and actionable frameworks necessary to detect, respond to, and mitigate cyber incidents. Leveraging cutting-edge cybersecurity frameworks and aligned with compliance standards like FERPA, COPPA, and CISA directives, this course emphasizes readiness, resilience, and recovery in educational settings.

With the rapid digital transformation in K–12 and higher education, schools are more vulnerable than ever to ransomware, phishing attacks, data breaches, and internal security lapses. This course equips school personnel with incident response protocols, real-time threat detection skills, digital forensic techniques, and communication playbooks for effective crisis management. Through real-world case studies, simulations, and evidence-based practices, learners will become key defenders of digital safety in education.

Programme Curriculum

Training Course on Cybersecurity Incident Response for Schools

Introduction

In today's digital-first learning environments, educational institutions face a rising tide of cyber threats targeting sensitive student data, internal communications, and operational systems. Training Course on Cybersecurity Incident Response for Schools is meticulously designed to empower school administrators, IT staff, and educators with the strategic knowledge, trending practices, and actionable frameworks necessary to detect, respond to, and mitigate cyber incidents. Leveraging cutting-edge cybersecurity frameworks and aligned with compliance standards like FERPA, COPPA, and CISA directives, this course emphasizes readiness, resilience, and recovery in educational settings.

With the rapid digital transformation in K–12 and higher education, schools are more vulnerable than ever to ransomware, phishing attacks, data breaches, and internal security lapses. This course equips school personnel with incident response protocols, real-time threat detection skills, digital forensic techniques, and communication playbooks for effective crisis management. Through real-world case studies, simulations, and evidence-based practices, learners will become key defenders of digital safety in education.

Course Objectives

1. Identify and evaluate cybersecurity threats in educational ecosystems
2. Understand cyber risk management and threat intelligence principles
3. Apply best practices for detecting and reporting cyber incidents
4. Implement incident response policies aligned with NIST and CISA guidelines
5. Perform digital forensics and malware analysis in school systems
6. Utilize SIEM tools for real-time monitoring and alerting
7. Build secure remote learning infrastructures
8. Create actionable school cybersecurity incident response plans
9. Train staff and students on digital hygiene and phishing awareness
10. Coordinate with law enforcement and cybersecurity agencies during crises
11. Conduct post-incident analysis for future threat mitigation
12. Comply with educational data privacy regulations (FERPA, COPPA, etc.)
13. Leverage AI-driven tools for proactive threat prevention

Target Audiences

1. K-12 School IT Administrators
2. District Technology Directors
3. Higher Education CIOs and CTOs
4. School Principals and Vice Principals
5. Cybersecurity Educators
6. Curriculum Designers & EdTech Consultants
7. School Board Members & Policy Makers
8. School-based Law Enforcement (SROs)

Course Duration: 5 days

Course Modules

Module 1: Understanding the Threat Landscape in Schools

- Types of cyber threats targeting schools
- Real-world attacks: ransomware, phishing, and DDoS
- Emerging trends in educational cybersecurity
- Internal vs external vulnerabilities
- Threat modeling using MITRE ATT&CK
- **Case Study: The ransomware attack on Los Angeles Unified School District**

Module 2: Establishing an Incident Response Team (IRT)

- Roles and responsibilities within IRT
- Staffing needs and skill sets
- Creating an incident response policy
- Communication flowcharts and escalation paths
- Cross-functional collaboration in crises
- **Case Study: How Baltimore County Public Schools formed a rapid response team**

Module 3: Detection and Monitoring Tools

- Introduction to SIEM (Security Information and Event Management)
- Log analysis and anomaly detection
- Setting up alerts and thresholds
- Real-time threat intelligence integration
- Selecting affordable tools for schools
- **Case Study: Using Splunk to identify anomalies in login activity**

Module 4: Incident Handling and Containment

- First-response protocols for cyber incidents
- Isolating affected systems and users
- Backup recovery and continuity planning
- Managing third-party vendor breaches
- Ensuring minimal learning disruption
- **Case Study: Containment strategies during the Miami-Dade Schools breach**

Module 5: Digital Forensics and Evidence Preservation

- Basics of data preservation and chain of custody
- Tools for collecting and analyzing evidence
- Tracking attacker movement
- Malware reverse engineering
- Reporting evidence to authorities
- **Case Study: Forensic timeline from a school network intrusion**

Module 6: Recovery and Post-Incident Review

- System restoration best practices
- Evaluating impact and risk exposure
- Updating security controls post-breach
- Conducting after-action reviews (AAR)
- Updating policies and staff training
- **Case Study: Lessons learned from the Chicago Public Schools breach**

Module 7: Student and Staff Awareness Training

- Cyber hygiene essentials for students
- Creating a culture of security
- Gamified phishing simulations
- Regular threat drills and tabletop exercises
- Integrating cybersecurity into curriculum
- **Case Study: Anti-phishing campaign success in a Texas high school**

Module 8: Legal and Regulatory Compliance

- FERPA, COPPA, CIPA: What schools need to know
- State breach notification laws
- Working with legal counsel
- Insurance and liability considerations
- Preparing compliance documentation
- **Case Study: Legal fallout after a data leak in a Florida school district**

Training Methodology

- Interactive webinars with subject matter experts

- Scenario-based simulations and tabletop exercises
- Hands-on labs with incident response tools
- Group projects and action plan development
- Real-world case study evaluations
- Continuous assessments and feedback loops

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

Start Date	End Date	Location	Price
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