Training Course on Cyber Crisis Preparedness and Incident Management

Professional Development Training Course Outline

Category	CEOs and Directors	**Duration**	10 Days
Base Fee	$3,000 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

In today's interconnected digital landscape, **cyber threats** are evolving rapidly, posing significant **risks** to organizations across all sectors. A robust **Cyber Crisis Preparedness and Incident Management** framework is no longer a luxury but a critical necessity for **organizational resilience** and **business continuity**. Training Course on Cyber Crisis Preparedness and Incident Management is designed to equip professionals with the **knowledge, skills, and strategic frameworks** essential to effectively **detect, respond to, and recover** from **cyber incidents** and full-blown **cyber crises**, minimizing **damage** and protecting **critical assets** and **reputation**.

This program delves into the entire **cyber incident lifecycle**, from proactive **threat intelligence** and **risk assessment** to immediate **incident response**, **digital forensics**, **crisis communication**, and post-incident **recovery strategies**. Participants will gain practical expertise in developing **resilient incident response plans**, establishing effective **communication protocols**, and conducting realistic **cyberattack simulations**. By integrating **industry best practices** and aligning with **international standards**, this course empowers organizations to **mitigate cyber risk**, enhance their **security posture**, and safeguard their **digital infrastructure** against the ever-present and sophisticated **cyber landscape**.

Programme Curriculum

Training Course on Cyber Crisis Preparedness and Incident Management

Introduction

In today's interconnected digital landscape, **cyber threats** are evolving rapidly, posing significant **risks** to organizations across all sectors. A robust **Cyber Crisis Preparedness and Incident Management** framework is no longer a luxury but a critical necessity for **organizational resilience** and **business continuity**. Training Course on Cyber Crisis Preparedness and Incident Management

is designed to equip professionals with the **knowledge, skills, and strategic frameworks** essential to effectively **detect, respond to, and recover** from **cyber incidents** and full-blown **cyber crises**, minimizing **damage** and protecting **critical assets** and **reputation**.

This program delves into the entire **cyber incident lifecycle**, from proactive **threat intelligence** and **risk assessment** to immediate **incident response**, **digital forensics**, **crisis communication**, and post-incident **recovery strategies**. Participants will gain practical expertise in developing **resilient incident response plans**, establishing effective **communication protocols**, and conducting realistic **cyberattack simulations**. By integrating **industry best practices** and aligning with **international standards**, this course empowers organizations to **mitigate cyber risk**, enhance their **security posture**, and safeguard their **digital infrastructure** against the ever-present and sophisticated **cyber landscape**.

Course Duration

10 days

Course Objectives

1. Master foundational cybersecurity concepts and the evolving threat landscape.
2. Develop robust incident response plans (IRP) aligned with NIST CSF and ISO 27035.
3. Implement advanced threat detection and real-time monitoring strategies using SIEM and SOAR.
4. Execute effective containment, eradication, and recovery procedures during live cyberattacks.
5. Conduct meticulous digital forensics and root cause analysis for post-incident learning.
6. Formulate impactful crisis communication strategies and manage stakeholder engagement during breaches.
7. Integrate cyber risk management into comprehensive business continuity (BCP) and disaster recovery (DRP) plans.
8. Leverage threat intelligence to proactively anticipate and mitigate emerging cyber threats.
9. Lead and coordinate cross-functional teams under high-pressure cyber crisis scenarios.
10. Comply with relevant cybersecurity regulations (e.g., GDPR, NIS2, DORA) and legal implications.
11. Design and facilitate realistic cyber crisis simulations and tabletop exercises.
12. Establish a culture of continuous improvement and organizational resilience in cybersecurity.
13. Protect critical infrastructure and sensitive data through proactive and reactive measures.

Organizational Benefits

- A workforce better equipped to withstand and recover from cyberattacks, minimizing downtime and operational disruption.
- Swift and effective incident response limits the financial impact of breaches, including remediation costs, legal fees, and reputational damage.
- Adherence to regulatory requirements (GDPR, NIS2, DORA, etc.) mitigates legal penalties and reputational fallout.
- Demonstrating a proactive approach to cybersecurity fosters confidence among customers, partners, and stakeholders.
- Optimized incident response and recovery plans lead to quicker restoration of services and business operations.
- Better understanding of the threat landscape and intelligence integration allows for pre-emptive measures.
- Clear processes, roles, and responsibilities ensure efficient and coordinated responses.

- Increased awareness and preparedness across the organization, transforming employees into a strong line of defense.
- Efficient use of security tools, technologies, and personnel during incidents.
- Organizations with superior cyber resilience are viewed as more reliable and trustworthy partners.

Target Audience

1. IT and Cybersecurity Professionals
2. Crisis Management and Risk Management Professionals
3. Senior Management and Executives
4. Business Continuity and Disaster Recovery Planners
5. Legal and Compliance Officers
6. Network and System Administrators
7. Audit and Governance Professionals
8. Operations Managers

Course Outline

Module 1: Understanding the Cyber Threat Landscape and Crisis Fundamentals

- Defining cyber crisis vs. cyber incident: Understanding scope and impact.
- Current global cyber threat trends: Ransomware, supply chain attacks, nation-state threats.
- Impact of cyber crises on business operations, reputation, and financial stability.
- Legal and regulatory implications of major cyber incidents (GDPR, NIS2, DORA).
- **Case Study:** The Colonial Pipeline Ransomware Attack – Analyzing operational disruption and crisis response.

Module 2: Cybersecurity Risk Assessment and Vulnerability Management

- Identifying critical assets and their inherent vulnerabilities.
- Conducting comprehensive cyber risk assessments (quantitative and qualitative).
- Prioritizing risks and developing mitigation strategies.
- Introduction to vulnerability scanning and penetration testing.
- **Case Study:** Equifax Data Breach – Examining the impact of unpatched vulnerabilities and inadequate risk management.

Module 3: Building a Robust Incident Response Plan (IRP)

- Components of an effective IRP: Preparation, Detection & Analysis, Containment, Eradication, Recovery, Post-incident Activity.
- Defining roles, responsibilities, and the Incident Response Team (IRT) structure.
- Developing clear escalation pathways and communication trees.
- Establishing essential policies, procedures, and runbooks.
- **Case Study:** Maersk NotPetya Attack – How a strong, albeit challenged, IRP helped in recovery.

Module 4: Incident Detection, Monitoring, and Alerting

- Leveraging SIEM solutions for centralized log management and correlation.
- Implementing EDR and network traffic analysis for anomaly detection.
- Integrating threat intelligence feeds for proactive identification of indicators of compromise (IOCs).

- Configuring effective alerting mechanisms and thresholds.
- **Case Study:** Target Data Breach – Analysis of missed alerts and the importance of timely detection.

Module 5: Incident Triage and Analysis

- Techniques for rapid incident classification and prioritization.
- Collecting and preserving digital evidence: Chain of custody.
- Initial analysis of attack vectors and threat actor motives.
- Understanding the Kill Chain and MITRE ATT&CK Framework.
- **Case Study:** Sony Pictures Entertainment Hack – Deciphering attack methods and initial impact assessment.

Module 6: Incident Containment and Eradication Strategies

- Implementing isolation techniques to prevent further spread (network segmentation, host isolation).
- Eradicating malware and malicious access points from infected systems.
- Applying security patches and configuration changes to close vulnerabilities.
- Strategies for managing active threats and disrupting attacker operations.
- **Case Study:** WannaCry Ransomware – Examining effective and ineffective containment efforts globally.

Module 7: Incident Recovery and Post-Incident Activities

- Restoring affected systems and data from secure backups.
- Validating system integrity and ensuring security post-recovery.
- Conducting comprehensive post-mortem analysis and lessons learned.
- Developing and implementing continuous improvement plans for the IRP.
- **Case Study:** CD Projekt Red Cyberattack – Assessing the complexities of data recovery and post-incident public relations.

Module 8: Digital Forensics Fundamentals

- Principles of digital forensics: Volatile vs. non-volatile data.
- Tools and techniques for collecting and analyzing forensic evidence (memory dumps, disk images).
- Identifying malicious artifacts and understanding attacker methodologies.
- Reporting forensic findings for legal, compliance, and internal purposes.
- **Case Study:** Stuxnet Malware – Understanding how forensic analysis revealed a sophisticated cyberweapon.

Module 9: Cyber Crisis Communication and Stakeholder Management

- Developing a comprehensive crisis communication plan (internal and external).
- Crafting clear, concise, and empathetic messaging during a crisis.
- Managing media relations, social media, and public perception.
- Engaging with regulatory bodies, law enforcement, and legal counsel.
- **Case Study:** Facebook (Meta) Outage – Analyzing communication failures and public reaction to system downtime.

Module 10: Business Continuity and Disaster Recovery Integration

- Aligning cyber incident response with BCP and DRP.

- Identifying critical business functions and their dependencies.
- Developing recovery time objectives (RTO) and recovery point objectives (RPO).
- Strategies for maintaining operations during and after a significant cyber crisis.
- **Case Study:** Hurricane Sandy Impact on Data Centers – Learning from natural disaster recovery for cyber resilience.

Module 11: Legal, Regulatory, and Ethical Considerations

- Understanding data breach notification laws and reporting requirements.
- Navigating privacy regulations (GDPR, CCPA) in incident response.
- Ethical dilemmas in cyber crisis management and information sharing.
- Engaging with legal counsel and law enforcement during investigations.
- **Case Study:** British Airways Data Breach – Examining the regulatory fines and legal consequences of non-compliance.

Module 12: Cybersecurity Frameworks and Standards

- Overview of NIST Cybersecurity Framework (CSF) for improving critical infrastructure cybersecurity.
- Implementing ISO/IEC 27035 (Information security incident management).
- Understanding other relevant standards: CIS Controls, MITRE D3FEND.
- Mapping organizational practices to industry best practices.
- **Case Study:** Adherence to HIPAA in Healthcare Sector Breaches – The importance of industry-specific compliance.

Module 13: Cyber Crisis Simulation and Tabletop Exercises

- Designing realistic cyberattack scenarios for exercises.
- Conducting tabletop exercises to test IRPs and crisis communication.
- Facilitating full-scale simulation drills to practice technical and executive response.
- Evaluating exercise outcomes and identifying areas for improvement.
- **Case Study:** Large-Scale Financial Institution Cyber Drill – Lessons learned from a multi-agency simulation.

Module 14: Threat Intelligence and Proactive Defense

- Sources and types of threat intelligence (OSINT, commercial, government).
- Integrating threat intelligence into security operations.
- Proactive hunting for threats within the organizational environment.
- Developing a continuous threat monitoring and assessment program.
- **Case Study:** The SolarWinds Supply Chain Attack – Highlighting the need for advanced threat intelligence and supply chain security.

Module 15: Building a Culture of Cyber Resilience

- Importance of leadership commitment and employee training.
- Developing security awareness programs and phishing simulations.
- Fostering a proactive and adaptive security mindset.
- Promoting collaboration between technical and non-technical teams.
- **Case Study:** Microsoft’s Security Transformation – How large organizations build and maintain a strong security culture.

Training Methodology

This course employs a **blended learning approach** designed for maximum engagement and practical skill development:

- **Interactive Lectures and Discussions:** Expert-led sessions providing theoretical foundations and industry insights.
- **Real-World Case Studies Analysis:** In-depth examination of past cyber crises to derive practical lessons.
- **Hands-on Exercises and Labs:** Practical application of tools and techniques for incident detection, analysis, and containment.
- **Scenario-Based Tabletop Exercises:** Facilitated discussions and decision-making simulations for strategic crisis response.
- **Live Cyberattack Simulations (Optional/Advanced):** Immersive, realistic drills to test technical and organizational response capabilities under pressure.
- **Group Activities and Collaborative Problem-Solving:** Fostering teamwork and shared learning experiences.
- **Expert Q&A Sessions:** Opportunities for direct engagement with experienced cybersecurity professionals.
- **Best Practice Frameworks and Templates:** Provision of actionable resources for immediate implementation.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.com or call *+254769199797*

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
07 Sep 2026	18 Sep 2026	Physical	$3,000
14 Sep 2026	25 Sep 2026	Physical	$3,000
21 Sep 2026	02 Oct 2026	Physical	$3,000
28 Sep 2026	09 Oct 2026	Physical	$3,000
05 Oct 2026	16 Oct 2026	Physical	$3,000
12 Oct 2026	23 Oct 2026	Physical	$3,000
19 Oct 2026	30 Oct 2026	Physical	$3,000
26 Oct 2026	06 Nov 2026	Physical	$3,000

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

Register Online Now

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