Training Course on Cybersecurity Incident Response for Executives

Professional Development Training Course Outline

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

Course Introduction

In today's hyper-connected world, **cyber threats** are not just IT issues; they are critical **business risks** that can severely impact an organization's **reputation, financial stability, and operational continuity**. Training Course on Cybersecurity Incident Response for Executives is meticulously designed for senior leaders and executives, providing them with the **strategic insights** and **actionable frameworks** necessary to navigate the complexities of a **cybersecurity incident** effectively. Participants will gain a deep understanding of **proactive cybersecurity strategies**, **crisis communication protocols**, and **post-incident recovery**, transforming them from passive observers into **resilient cyber leaders** ready to protect their enterprise from evolving digital dangers.

The program emphasizes a **holistic approach** to **cyber incident management**, moving beyond technical jargon to focus on the **executive decision-making** and **governance structures** crucial for minimizing damage and ensuring swift **business recovery**. Through **real-world case studies**, **interactive simulations**, and expert-led discussions, executives will develop the confidence and capabilities to lead their organizations through a **cyber-crisis**, upholding **stakeholder trust** and safeguarding critical assets. This course is an essential investment for any organization committed to building a robust **cyber resilience framework** and maintaining a competitive edge in an increasingly volatile digital landscape.

Programme Curriculum

Training Course on Cybersecurity Incident Response for Executives

Introduction

In today's hyper-connected world, **cyber threats** are not just IT issues; they are critical **business risks** that can severely impact an organization's **reputation, financial stability, and operational**

continuity. Training Course on Cybersecurity Incident Response for Executives is meticulously designed for senior leaders and executives, providing them with the **strategic insights** and **actionable frameworks** necessary to navigate the complexities of a **cybersecurity incident** effectively. Participants will gain a deep understanding of **proactive cybersecurity strategies**, **crisis communication protocols**, and **post-incident recovery**, transforming them from passive observers into **resilient cyber leaders** ready to protect their enterprise from evolving digital dangers.

The program emphasizes a **holistic approach** to **cyber incident management**, moving beyond technical jargon to focus on the **executive decision-making** and **governance structures** crucial for minimizing damage and ensuring swift **business recovery**. Through **real-world case studies**, **interactive simulations**, and expert-led discussions, executives will develop the confidence and capabilities to lead their organizations through a **cyber-crisis**, upholding **stakeholder trust** and safeguarding critical assets. This course is an essential investment for any organization committed to building a robust **cyber resilience framework** and maintaining a competitive edge in an increasingly volatile digital landscape.

Course Duration

5 days

Course Objectives

1. Understand and implement effective cybersecurity governance frameworks to align with organizational risk appetite.
2. Leverage threat intelligence to proactively identify and mitigate emerging cyber threats and vulnerabilities.
3. Master the creation and implementation of robust incident response playbooks tailored to diverse attack vectors.
4. Establish and execute transparent crisis communication strategies for internal and external stakeholders during a cyber-breach.
5. Implement techniques to contain cyber incidents swiftly and reduce business downtime and financial impact.
6. Navigate complex cybersecurity regulations (e.g., GDPR, NIST, ISO 27001) and data breach notification requirements.
7. Build a culture of cyber resilience across all business functions.
8. Guide effective post-incident analysis and recovery operations, including digital forensics and system restoration.
9. Assess the organization's current security posture and identify critical security gaps.
10. Develop strategies to detect, prevent, and respond to insider threats and privileged access misuse.
11. Understand and mitigate supply chain cybersecurity risks impacting the broader ecosystem.
12. Seamlessly integrate cyber risk management into the overall Enterprise Risk Management (ERM) framework.
13. Champion cybersecurity awareness and best practices across the executive team and the entire organization.

Organizational Benefits

- Minimize the monetary losses associated with **data breaches**, system downtime, and regulatory fines.

- Protect the organization's **reputation** and **customer trust** by demonstrating strong **cybersecurity leadership** during incidents.
- Ensure swift **recovery** and **operational continuity** in the face of **cyber attacks**, safeguarding critical business functions.
- Avoid legal penalties and reputational damage by adhering to **data protection laws** and industry standards.
- Shift from a reactive to a **proactive cybersecurity posture**, identifying and mitigating risks before they escalate.
- Instill confidence among investors, partners, and customers through demonstrable **cyber resilience**.
- Efficiently allocate resources for **cybersecurity investments** based on identified risks and priorities.
- Foster a pervasive **security-aware culture** from the top down, empowering all employees.

Target Audience

1. C-Suite Executives.
2. Board Members.
3. Senior Management.
4. Risk Management Professionals.
5. Legal and Compliance Officers.
6. Business Continuity and Disaster Recovery Managers
7. Public Relations and Communications Leads.
8. Audit Committee Members

Course Outline

Module 1: The Evolving Cyber Threat Landscape & Executive Imperatives

- Understanding Advanced Persistent Threats (APTs), ransomware, phishing, and supply chain attacks.
- The business impact of cyber breaches: financial, reputational, legal, and operational.
- Current global cyber trends and their implications for executive decision-making.
- Key cybersecurity terminology translated for executive understanding.
- The executive's role in establishing a cyber-aware culture and security posture.
- **Case Study:** The Colonial Pipeline Ransomware Attack: Analyzing the operational shutdown, economic impact, and executive response.

Module 2: Cybersecurity Governance and Risk Management for Leaders

- Developing a robust cybersecurity governance framework aligned with organizational objectives.
- Integrating cyber risk assessment into enterprise risk management (ERM).
- Establishing clear roles and responsibilities for cybersecurity oversight at the executive level.
- Budgeting for cybersecurity investments: Strategic allocation for defense and incident response capabilities.
- Metrics and reporting: Understanding key performance indicators (KPIs) for cybersecurity effectiveness.
- **Case Study:** Equifax Data Breach: Examining governance failures, board oversight, and the long-term impact on trust and regulatory fines.

Module 3: Incident Response Planning & Preparation: Building Your Playbook

- Components of an effective Cybersecurity Incident Response Plan (CIRP).
- Defining the Incident Response Team (IRT) and its cross-functional activation.
- Proactive measures: threat hunting, vulnerability management, and security awareness programs.
- Developing incident response playbooks for various scenarios (e.g., data exfiltration, system compromise).
- Establishing communication protocols and escalation paths for rapid response.
- **Case Study:** Target Data Breach: Analyzing the failure of early detection and the importance of a well-rehearsed incident response plan.

Module 4: Detection, Analysis, and Containment Strategies

- Understanding incident detection mechanisms: SIEM, EDR, network monitoring.
- Triage and initial analysis of security alerts: distinguishing real threats from false positives.
- Containment strategies: isolating compromised systems and preventing further damage.
- Evidence preservation and the importance of a chain of custody for legal proceedings.
- Working effectively with technical teams during the incident's critical early stages.
- **Case Study:** Maersk NotPetya Attack: Illustrating the rapid spread of malware, the challenges of containment, and the massive financial toll.

Module 5: Eradication, Recovery, and Post-Incident Activities

- Eradication: Removing the root cause of the incident and eliminating the threat.
- System recovery and restoration: Restoring affected systems and data from secure backups.
- Post-incident analysis (Lessons Learned): Identifying gaps and improving future response capabilities.
- Communication during recovery: Managing expectations and providing updates to stakeholders.
- Implementing preventative measures to avoid recurrence.
- **Case Study:** Sony Pictures Entertainment Hack: Examining the challenges of system rebuilding, data recovery, and managing long-term reputational damage.

Module 6: Legal, Regulatory, and Compliance Considerations

- Data breach notification laws (e.g., GDPR, CCPA, specific industry regulations).
- Understanding legal liabilities and forensic investigations.
- Working with legal counsel and law enforcement agencies.
- Compliance frameworks: NIST Cybersecurity Framework, ISO 27001, NIS2.
- The role of cyber insurance in mitigating financial risks.
- **Case Study:** Marriott International Data Breach: Focusing on the implications of delayed disclosure and the resulting regulatory fines and class-action lawsuits under GDPR.

Module 7: Crisis Communication and Stakeholder Management

- Developing a crisis communication plan for internal and external audiences.
- Crafting effective messaging for media, customers, employees, and regulators.
- Managing reputational damage and restoring public trust post-incident.
- The role of the executive in public statements and press conferences.
- Simulated press conferences and stakeholder engagement exercises.
- **Case Study:** British Airways Data Breach: Analyzing the impact of public perception, the speed and clarity of communication, and the ultimate financial penalties.

Module 8: Executive Cyber Simulation & Leadership Masterclass

- Full-scale tabletop exercises simulating complex cyber crisis scenarios.
- Real-time executive decision-making under pressure.
- Cross-functional team coordination and communication during the simulation.
- Leadership lessons from real-world cyber incidents.
- Developing a personal executive action plan for enhanced cyber resilience.
- **Case Study:** Simulated supply chain attack on a critical infrastructure company, requiring executive decisions on system shutdowns, regulatory reporting, and public safety communications. This will be an interactive, scenario-based exercise.

Training Methodology

This training course will employ a highly interactive and practical methodology designed for executive-level learning. It will include:

- **Interactive Lectures and Discussions**: Expert-led sessions with ample opportunity for Q&A and peer-to-peer exchange.
- **Real-World Case Studies Analysis**: Deep dives into significant cyber incidents, focusing on executive decision-making, organizational impact, and lessons learned.
- **Tabletop Exercises and Simulations**: Hands-on, scenario-based exercises to practice incident response planning, crisis communication, and executive leadership under pressure.
- **Guest Speakers**: Insights from industry CISOs, legal experts, and incident response practitioners.
- **Group Activities and Workshops**: Collaborative problem-solving and development of practical frameworks.
- **Post-Training Action Planning**: Facilitated sessions to help executives translate course learnings into actionable strategies for their organizations.

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
21 Sep 2026	25 Sep 2026	Online	$1,000
21 Sep 2026	25 Sep 2026	Physical	$1,500
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0

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

Register Online Now

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