Training Course on Developing a Cyber Incident Disclosure Strategy

Professional Development Training Course Outline

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

Course Introduction

In an era of escalating cyber threats and stringent regulatory landscapes, a robust and strategic approach to cyber incident disclosure is no longer a matter of choice but a critical component of organizational resilience and brand trust. Proactive, transparent, and legally sound communication following a security breach can significantly mitigate financial and reputational damage, turning a potential crisis into a demonstration of accountability and strength. Training Course on Developing a Cyber Incident Disclosure Strategy is meticulously designed to empower organizations to navigate the complexities of incident disclosure, ensuring compliance with evolving regulations, fostering stakeholder confidence, and maintaining a security-first posture in a volatile digital world.

This course moves beyond theoretical frameworks, offering pragmatic and actionable guidance on creating a comprehensive cyber incident disclosure strategy. Participants will delve into the critical interplay between legal obligations, public relations, and technical incident response, equipping them with the skills to craft clear, concise, and timely communications. By analyzing real-world case studies and engaging in practical exercises, attendees will learn to manage the narrative, control the flow of information, and ultimately, build a more cyber-resilient organization prepared to face the inevitable challenges of the modern threat landscape.

Programme Curriculum

Training Course on Developing a Cyber Incident Disclosure Strategy

Introduction

In an era of escalating cyber threats and stringent regulatory landscapes, a robust and strategic approach to cyber incident disclosure is no longer a matter of choice but a critical component of organizational resilience and brand trust. Proactive, transparent, and legally sound communication following a security breach can significantly mitigate financial and reputational damage, turning a

potential crisis into a demonstration of accountability and strength. Training Course on Developing a Cyber Incident Disclosure Strategy is meticulously designed to empower organizations to navigate the complexities of incident disclosure, ensuring compliance with evolving regulations, fostering stakeholder confidence, and maintaining a security-first posture in a volatile digital world.

This course moves beyond theoretical frameworks, offering pragmatic and actionable guidance on creating a comprehensive cyber incident disclosure strategy. Participants will delve into the critical interplay between legal obligations, public relations, and technical incident response, equipping them with the skills to craft clear, concise, and timely communications. By analyzing real-world case studies and engaging in practical exercises, attendees will learn to manage the narrative, control the flow of information, and ultimately, build a more cyber-resilient organization prepared to face the inevitable challenges of the modern threat landscape.

Course Duration

5 days

Course Objectives

Upon completion of this training, participants will be able to:

1. Understand and apply industry-standard frameworks like NIST and ISO/IEC 27001 to incident disclosure.
2. Interpret and comply with key data breach notification laws, including GDPR, CCPA, and emerging federal mandates.
3. Formulate a proactive communication strategy to manage stakeholder expectations and protect brand reputation.
4. Leverage threat intelligence to anticipate and prepare for various incident scenarios.
5. Orchestrate a seamless response across legal, technical, and communication teams.
6. Craft targeted and transparent messaging for customers, employees, investors, and regulators.
7. Engage with the media effectively to ensure accurate and responsible reporting.
8. Conduct thorough post-mortem analyses to identify lessons learned and enhance future responses.
9. Understand the role of digital forensics in shaping the disclosure narrative and legal defensibility.
10. Quantify and proactively manage the reputational fallout from a cyber-incident.
11. Understand the role and limitations of cyber insurance in the disclosure process.
12. Participate in realistic tabletop exercises to test and refine disclosure strategies.
13. Champion a security-first culture to minimize the likelihood and impact of future incidents.

Organizational Benefits

- **Enhanced Regulatory Compliance:** Avoid hefty fines and legal penalties by ensuring timely and accurate incident reporting.
- **Reduced Reputational Damage:** Protect brand value and customer trust through transparent and strategic communication.
- **Improved Incident Response Time:** Streamline the disclosure process for a more efficient and effective response.
- **Increased Stakeholder Confidence:** Foster trust with customers, investors, and partners through proactive engagement.
- **Mitigated Financial Loss:** Minimize the financial impact of a breach through a well-executed disclosure strategy.

- **Strengthened Cybersecurity Posture:** Identify and remediate vulnerabilities highlighted during incident response and disclosure planning.

Target Participants

1. Chief Information Security Officers (CISOs) and IT Security Managers
2. Legal Counsel and Compliance Officers
3. Public Relations and Corporate Communications Teams
4. Incident Response Team Members
5. Risk Management Professionals
6. Executive Leadership (CEOs, CFOs, COOs)
7. Data Privacy Officers (DPOs)
8. IT Auditors

Course Modules

Module 1: The Imperative of a Cyber Incident Disclosure Strategy

- Understanding the Modern Threat Landscape and Attack Vectors
- The Financial and Reputational Costs of a Poor Disclosure
- Legal and Regulatory Drivers for Incident Disclosure
- The Intersection of Incident Response, Legal, and Public Relations
- **Case Study:** The Equifax data breach and its lasting impact on disclosure regulations.

Module 2: Building Your Incident Disclosure Framework

- Aligning with NIST, ISO/IEC 27001, and other relevant standards
- Defining Roles and Responsibilities: The Disclosure Team
- Establishing Communication Channels and Protocols
- Developing a Tiered Approach to Incident Classification
- **Case Study:** Analyzing the coordinated disclosure of the SolarWinds supply chain attack.

Module 3: Navigating the Legal and Regulatory Maze

- A Deep Dive into GDPR, CCPA, and other key regulations
- Understanding Contractual Obligations for Disclosure
- Attorney-Client Privilege in the Context of a Breach
- Reporting to Law Enforcement and Government Agencies
- **Case Study:** Marriott's Starwood data breach and the complexities of international data protection laws.

Module 4: Crafting the Narrative: Crisis Communication and Media Management

- Developing a Proactive Crisis Communication Plan
- Writing Clear, Concise, and Empathetic Notifications
- Managing Media Inquiries and Press Conferences
- Leveraging Social Media for Timely Updates
- **Case Study:** The Colonial Pipeline ransomware attack and the public-private response coordination.

Module 5: The Role of Digital Forensics in Disclosure

- Understanding the Digital Forensics Investigation Process
- How Forensic Findings Shape the Disclosure Timeline and Content

- Preserving Evidence for Legal and Regulatory Scrutiny
- Communicating Technical Details to a Non-Technical Audience
- **Case Study:** The investigation and disclosure of the MOVEit Transfer vulnerability.

Module 6: Internal Communications and Stakeholder Management

- Keeping Employees Informed and Engaged
- Communicating with the Board of Directors and Executive Leadership
- Managing Investor Relations During a Crisis
- Notifying and Supporting Affected Customers
- **Case Study:** Target's 2013 data breach and the evolution of customer notification strategies.

Module 7: Tabletop Exercises and Simulation

- Planning and Executing Realistic Incident Disclosure Scenarios
- Testing the Effectiveness of Your Communication Plan
- Identifying Gaps and Weaknesses in Your Strategy
- Refining Your Response in a Controlled Environment
- **Case Study:** A simulated ransomware attack on a financial institution and the subsequent disclosure decisions.

Module 8: Post-Incident Review and Continuous Improvement

- Conducting a Thorough Post-Mortem Analysis
- Identifying Lessons Learned and Areas for Improvement
- Updating and Refining Your Disclosure Strategy
- Building a Culture of Transparency and Resilience
- **Case Study:** How the lessons from past breaches have shaped current industry best practices.

Training Methodology

This course will employ a blended learning approach, combining expert-led instruction with interactive, hands-on activities. The methodology includes:

- **Interactive Lectures and Discussions:** Engaging presentations by seasoned cybersecurity and communication professionals.
- **Real-World Case Study Analysis:** In-depth examination of significant cyber incidents and their disclosure strategies.
- **Practical Workshops and Group Exercises:** Collaborative sessions to develop key components of a disclosure plan.
- **Tabletop Simulations:** Realistic role-playing exercises to test decision-making and communication skills in a crisis.
- **Peer-to-Peer Learning:** Opportunities for participants to share experiences and best practices.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.com 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
07 Sep 2026	11 Sep 2026	Physical	$1,500
14 Sep 2026	18 Sep 2026	Physical	$1,500
21 Sep 2026	25 Sep 2026	Physical	$1,500
28 Sep 2026	02 Oct 2026	Physical	$1,500
05 Oct 2026	09 Oct 2026	Physical	$1,500
12 Oct 2026	16 Oct 2026	Physical	$1,500
19 Oct 2026	23 Oct 2026	Physical	$1,500
26 Oct 2026	30 Oct 2026	Physical	$1,500

Register Online Now

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