Training Course on Data Breach Management and Incident Response

Professional Development Training Course Outline

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

Course Introduction

In today’s hyper-connected digital ecosystem, data breach management and incident response strategies have become critical components of every organization’s cybersecurity framework. With rising threats from ransomware, phishing attacks, and insider threats, a single vulnerability can lead to catastrophic damage to a brand’s reputation, legal standing, and financial stability. Training Course on Data Breach Management and Incident Response is designed to empower IT professionals, legal advisors, and compliance officers with real-time incident response techniques, regulatory compliance knowledge, and advanced risk mitigation tools to effectively handle and prevent data breaches.

By leveraging hands-on simulations, real-world case studies, and risk assessment models, participants will develop the ability to detect, contain, and recover from cyber incidents efficiently. With the integration of globally accepted standards such as NIST, GDPR, HIPAA, and ISO/IEC 27035, this course delivers a 360-degree approach to safeguarding data assets and maintaining business continuity.

Programme Curriculum

Training Course on Data Breach Management and Incident Response

Introduction

In today’s hyper-connected digital ecosystem, data breach management and incident response strategies have become critical components of every organization’s cybersecurity framework. With rising threats from ransomware, phishing attacks, and insider threats, a single vulnerability can lead to catastrophic damage to a brand’s reputation, legal standing, and financial stability. Training Course on Data Breach Management and Incident Response is designed to empower IT professionals, legal advisors, and compliance officers with real-time incident response techniques, regulatory compliance knowledge, and advanced risk mitigation tools to effectively handle and prevent data breaches.

By leveraging hands-on simulations, real-world case studies, and risk assessment models, participants will develop the ability to detect, contain, and recover from cyber incidents efficiently. With the integration of globally accepted standards such as NIST, GDPR, HIPAA, and ISO/IEC 27035, this course delivers a 360-degree approach to safeguarding data assets and maintaining business continuity.

Course Objectives

1. Understand the fundamentals of data breach lifecycle and cybersecurity incident response.
2. Implement threat detection and analysis using advanced monitoring tools.
3. Build an incident response plan aligned with NIST guidelines.
4. Establish incident triage procedures and response team protocols.
5. Develop a communication strategy for stakeholders post-breach.
6. Execute data breach notification procedures under legal mandates (GDPR, CCPA).
7. Perform root cause analysis to prevent future breaches.
8. Integrate SIEM systems for real-time incident monitoring.
9. Evaluate the effectiveness of response strategies through forensic investigation.
10. Align response planning with data governance and compliance frameworks.
11. Use cyber threat intelligence to predict and mitigate emerging risks.
12. Create a post-incident recovery roadmap to restore operational integrity.
13. Apply business continuity planning (BCP) for sustained resilience.

Target Audience

1. Chief Information Security Officers (CISOs)
2. IT and Network Security Professionals
3. Risk and Compliance Managers
4. Cybersecurity Analysts
5. Legal and Regulatory Advisors
6. Data Privacy Officers
7. Business Continuity Planners
8. Government and Law Enforcement Cyber Units

Course Duration: 5 days

Course Modules

Module 1: Introduction to Data Breach Management

- Definition and classification of data breaches
- Breach lifecycle overview
- Key legal and financial implications
- Data sensitivity and risk assessment
- Common causes and entry points
- **Case Study:** Target Data Breach – What Went Wrong?

Module 2: Building an Effective Incident Response Team (IRT)

- Roles and responsibilities within IRT
- Creating incident escalation paths
- Internal and external communication channels
- Integrating IT, legal, and HR departments
- Tabletop exercises for team readiness
- **Case Study:** Capital One IRT Analysis

Module 3: Threat Detection and Monitoring Systems

- SIEM tools and best practices
- Real-time monitoring with SOC integration
- Log analysis and anomaly detection
- Network traffic analysis
- Integrating threat intelligence platforms
- **Case Study:** Equifax’s Failure in Threat Detection

Module 4: Legal and Regulatory Compliance

- Overview of GDPR, HIPAA, CCPA
- Legal consequences of data breach
- Data breach notification laws
- Cross-border data breach challenges
- Third-party compliance management
- **Case Study:** Facebook GDPR Violation Analysis

Module 5: Forensic Investigation and Evidence Handling

- Introduction to digital forensics
- Capturing volatile and non-volatile data
- Chain of custody protocols
- Memory and disk analysis
- Preserving evidence for litigation
- **Case Study:** Uber's Concealed Breach and DOJ Investigation

Module 6: Containment, Eradication, and Recovery

- Breach containment strategies
- Malware and ransomware removal
- System restoration and patching
- Backup validation and recovery testing
- Preventive maintenance plans
- **Case Study:** Maersk’s Global IT Recovery After NotPetya

Module 7: Communication and Notification Protocols

- Internal staff notification procedures
- External communication: customers, media, regulators
- Crisis management communication plan
- Drafting breach notification letters
- Managing public trust and reputation
- **Case Study:** Marriott International’s Breach Notification Strategy

Module 8: Post-Incident Review and Business Continuity

- Conducting post-mortem breach reviews
- Updating incident response policies
- Metrics for incident response performance
- Enhancing security culture
- Business continuity and disaster recovery planning
- **Case Study:** Sony Pictures Entertainment – Lessons in Resilience

Training Methodology

- Interactive virtual or in-person workshops
- Hands-on cybersecurity lab exercises

- Real-world case study analysis
- Simulated breach scenarios and tabletop exercises
- Group discussions and expert panels

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
23 Nov 2026	27 Nov 2026	Physical	$6,000

Start Date	End Date	Location	Price
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