Training Course on Crisis Communication and Public Relations for Cyber Incidents

Professional Development Training Course Outline

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

Course Introduction

In today’s hyper-connected digital ecosystem, cyber incidents such as data breaches, ransomware attacks, and system infiltrations can significantly damage an organization's reputation, stakeholder trust, and public image. Effective crisis communication and strategic public relations management have become non-negotiable skills in managing the aftermath of such events. Training Course on Crisis Communication and Public Relations for Cyber Incidents is designed to equip professionals with real-world skills, tools, and frameworks needed to control narratives, minimize reputation damage, and restore organizational trust in a post-breach environment.

This course blends cutting-edge PR strategies, real-time incident response communication frameworks, and cybersecurity crisis simulation case studies to empower teams and individuals. With a growing emphasis on digital resilience, reputation management, and cybersecurity governance, this training aligns with global best practices and prepares participants to handle modern digital crises with confidence and clarity.

Programme Curriculum

Training Course on Crisis Communication and Public Relations for Cyber Incidents

Introduction

In today’s hyper-connected digital ecosystem, cyber incidents such as data breaches, ransomware attacks, and system infiltrations can significantly damage an organization's reputation, stakeholder trust, and public image. Effective crisis communication and strategic public relations management have become non-negotiable skills in managing the aftermath of such events. Training Course on Crisis Communication and Public Relations for Cyber Incidents is designed to equip professionals with real-world skills, tools, and frameworks needed to control narratives, minimize reputation damage, and restore organizational trust in a post-breach environment.

This course blends cutting-edge PR strategies, real-time incident response communication frameworks, and cybersecurity crisis simulation case studies to empower teams and individuals. With a growing emphasis on digital resilience, reputation management, and cybersecurity governance, this training aligns with global best practices and prepares participants to handle modern digital crises with confidence and clarity.

Course Objectives

1. Master crisis communication planning for cybersecurity incidents.
2. Develop a real-time incident response communication strategy.
3. Understand regulatory and legal aspects of data breach disclosure.
4. Build a proactive public relations risk mitigation framework.
5. Manage internal and external stakeholder engagement post-breach.
6. Learn media handling and press release writing for cyber crises.
7. Use social media response strategies during digital attacks.
8. Conduct crisis simulation exercises for communication preparedness.
9. Monitor and measure online sentiment and reputation analytics.
10. Integrate cybersecurity messaging into corporate communications.
11. Identify best practices for transparent communication ethics.
12. Coordinate with technical teams on technical PR explanations.
13. Analyze real-world cyber incident case studies and response tactics.

Target Audience

1. Corporate communication professionals
2. PR and media relations managers
3. Chief Information Security Officers (CISOs)
4. Cybersecurity managers and analysts
5. Public affairs officers
6. Crisis and risk management consultants
7. Legal and compliance officers
8. Government and NGO communication teams

Course Duration: 10 days

Course Modules

Module 1: Introduction to Crisis Communication in Cybersecurity

- Definitions and scope of crisis communication
- Key challenges in cyber incident communication
- PR vs. technical response timelines
- Stakeholder sensitivity in digital crises
- Role of communication in cyber resilience
- **Case Study:** Target’s 2013 data breach response

Module 2: Anatomy of a Cybersecurity Crisis

- Types of cyber threats and their impacts
- Stages of a cyber crisis
- Psychological impacts on stakeholders
- Real-time data flow during an attack
- Legal and compliance pressures
- **Case Study:** Equifax data breach and its PR implications

Module 3: Developing a Cyber Crisis Communication Plan

- Building a response communication checklist
- Identifying key spokespersons
- Chain of communication in crisis
- Internal vs. external communication lines
- Pre-drafted response templates
- **Case Study:** Sony Pictures hack response plan

Module 4: Legal Considerations in Crisis PR

- Understanding data breach notification laws
- Legal vs. reputational considerations
- Regulatory reporting requirements
- Coordination with legal counsel
- Communicating under legal review
- **Case Study:** Marriott breach and GDPR implications

Module 5: Social Media Management in Real-Time Crises

- Monitoring social media for signals
- Real-time social media response plans
- Handling misinformation and panic
- Platform-specific response techniques
- Activating influencer or ambassador networks
- **Case Study:** Zoom’s response to “Zoombombing”

Module 6: Building Spokesperson Confidence

- Media training for IT/security spokespeople
- Crafting key messages and soundbites
- Dealing with hostile press interviews
- Maintaining calm and authority under pressure
- Coordinating with PR advisors and legal
- **Case Study:** Facebook’s executive communication post-Cambridge Analytica

Module 7: Managing Internal Communications Post-Attack

- Communicating with staff after an incident
- Internal FAQs and rumor control
- Leadership visibility and reassurance
- Rebuilding employee confidence
- Staff training on post-crisis behavior
- **Case Study:** Twitter's insider breach – internal handling

Module 8: Crisis Communication Simulation and Roleplay

- Simulation planning and logistics
- Role assignments and briefing
- Evaluating performance under pressure
- Debriefing and feedback loops
- Improvement planning post-simulation
- **Case Study:** Cyber crisis simulation at NATO

Module 9: Crafting the Right Messaging

- Messaging frameworks: clarity, empathy, authority
- Choosing the right tone and language

- Addressing public fears
- Aligning messages across channels
- Avoiding over-disclosure vs. under-disclosure
- **Case Study:** Capital One's incident messaging audit

Module 10: Engaging with Traditional and Digital Media

- Preparing press releases post-breach
- Hosting digital press briefings
- Coordinating with media outlets
- Using blogs and official statements
- Crisis communication across time zones
- **Case Study:** Uber’s data breach delayed disclosure

Module 11: Working with Third Parties

- Engaging cybersecurity vendors in PR
- Collaborating with law enforcement
- Coordinating with industry associations
- Partner and client communications
- Insurance and crisis communication integration
- **Case Study:** Colonial Pipeline and federal coordination

Module 12: Reputation Management and Recovery

- Long-term damage control techniques
- Rebuilding stakeholder trust
- Rebranding post-cyber crisis
- Monitoring sentiment recovery metrics
- Building future-proof resilience plans
- **Case Study:** Yahoo's breach and brand recovery process

Module 13: Crisis Communication Metrics and KPIs

- Key metrics to track during a crisis
- Evaluating communication effectiveness
- Sentiment analysis tools
- PR attribution to recovery
- Lessons learned documentation
- **Case Study:** Deloitte’s cyber incident KPI dashboard

Module 14: Cross-Functional Crisis Team Integration

- IT, PR, legal, and HR coordination
- Creating communication SOPs
- Integrating response plans
- Pre-incident drills and cross-training
- Escalation protocols
- **Case Study:** Microsoft's unified breach response protocol

Module 15: Future Trends in Cyber Crisis Communication

- AI in real-time crisis communication
- Predictive reputation analytics
- Emerging platforms and audience shifts
- New regulatory trends

- Post-pandemic crisis models
- **Case Study:** Case study on emerging threats in healthcare PR (ransomware)

Training Methodology

- Instructor-led presentations with live Q&A
- Interactive group simulations and tabletop exercises
- Role-based communication drills
- Real-world case analysis and discussions
- Access to templates, checklists, and response toolkits
- Online collaborative assessments and feedback

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	04 Dec 2026	Online	$2,000
23 Nov 2026	04 Dec 2026	Physical	$3,000
23 Nov 2026	04 Dec 2026	Physical	$6,000
23 Nov 2026	04 Dec 2026	Physical	$6,000

Start Date	End Date	Location	Price
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 2026	Physical	$9,000
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 2026	Physical	$12,000

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

Register Online Now

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