Executive-Level Crisis Communications for Security Incidents Training Course

Professional Development Training Course Outline

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

Course Introduction

Navigating a security incident in today's digital-first landscape is arguably the ultimate test of executive leadership and corporate resilience. Executive-Level Crisis Communications for Security Incidents Training Course is specifically designed for high-level leaders who must take immediate, decisive, and communicative action when a cybersecurity breach or major physical security event threatens the organization's reputation, financial stability, and stakeholder trust. Modern crises demand more than technical response; they require strategic communication that projects credibility, transparency, and calm under extreme pressure. Silence or mixed messages can be as damaging as the incident itself, turning an operational failure into a catastrophic reputational crisis.

This intensive, scenario-based program provides the C-Suite and senior management with a crisis playbook for the digital age. Participants will master the critical skills of stakeholder engagement, media relations in a crisis, and internal communication during high-stakes security events like ransomware attacks, data breaches, or critical infrastructure failure. We focus on the non-technical, strategic response that secures the narrative, mitigates long-term brand damage, and positions the organization for a swift, credible post-crisis recovery. The goal is to transform a high-impact security incident from a potential disaster into a demonstration of organizational preparedness and leadership strength.

Programme Curriculum

Executive-Level Crisis Communications for Security Incidents Training Course

Introduction

Navigating a security incident in today's digital-first landscape is arguably the ultimate test of executive leadership and corporate resilience. Executive-Level Crisis Communications for Security Incidents Training Course is specifically designed for high-level leaders who must take immediate, decisive, and communicative

action when a cybersecurity breach or major physical security event threatens the organization's reputation, financial stability, and stakeholder trust. Modern crises demand more than technical response; they require strategic communication that projects credibility, transparency, and calm under extreme pressure. Silence or mixed messages can be as damaging as the incident itself, turning an operational failure into a catastrophic reputational crisis.

This intensive, scenario-based program provides the C-Suite and senior management with a crisis playbook for the digital age. Participants will master the critical skills of stakeholder engagement, media relations in a crisis, and internal communication during high-stakes security events like ransomware attacks, data breaches, or critical infrastructure failure. We focus on the non-technical, strategic response that secures the narrative, mitigates long-term brand damage, and positions the organization for a swift, credible post-crisis recovery. The goal is to transform a high-impact security incident from a potential disaster into a demonstration of organizational preparedness and leadership strength.

Course Duration

5 days

Course Objectives

This program aims to equip executive leaders with the skills to achieve the following:

1. Define and embed the executive role in the Security Incident Response Plan (SIRP).
2. Proactively reduce the long-term impact of a data breach or security failure on brand integrity and market valuation.
3. Develop and deploy a single, consistent, and empathetic communication strategy across all channels.
4. Maintain and rebuild investor confidence and regulatory relationships through structured, transparent reporting.
5. Effectively handle aggressive crisis media relations, live interviews, and press conferences with message discipline.
6. Master the use of social media monitoring and rapid response to manage the spread of misinformation and rumor.
7. Institute CEO communication practices that maintain employee morale, safety, and operational continuity.
8. Align communication strategies with legal counsel to ensure adherence to compliance without sacrificing organizational credibility.
9. Conduct pre-crisis communication audits to identify and close potential security and communication gaps.
10. Participate in real-time crisis simulations to stress-test communication plans and executive decision-making under duress.
11. Design and execute a robust reputation recovery and "lessons learned" program to enhance organizational resilience.
12. Understand and comply with evolving global data privacy regulations and mandatory disclosure requirements.
13. Train and coach executive spokespersons for high-stakes, high-pressure interviews with gravitas and clarity.

Target Audience

1. Chief Executive Officer (CEO)
2. Chief Information Security Officer (CISO)

3. Chief Communications Officer (CCO) / VP of PR
4. Chief Operating Officer (COO)
5. Chief Legal Officer (CLO) / General Counsel
6. Board Members and Non-Executive Directors
7. Chief Risk Officer (CRO)
8. Senior Executive Team members

Course Modules

Module 1: The Executive Mandate in a Security Crisis

- Defining the "Right of Boom" leadership role: transitioning from incident detection to strategic crisis oversight.
- Establishing the Executive Crisis Response Team.
- Integrating the executive-level communication strategy with the technical Incident Response (IR) playbook.
- Case Study: Analyzing the Tylenol Scare and the Equifax Data Breach.
- Understanding the CEO's first 60 minutes during a major event: what to say, what not to say, and the initial audience hierarchy.

Module 2: Strategic Stakeholder Mapping and Engagement

- Identifying and prioritizing key audiences.
- Developing bespoke messaging platforms for critical groups to address their specific concerns and information needs.
- Managing investor relations during a crisis.
- Case Study: The Colonial Pipeline Ransomware Attack analyzing communication with government/critical infrastructure stakeholders and the public.
- Techniques for maintaining regulatory transparency while managing privileged and sensitive information.

Module 3: High-Stakes Media Relations and Message Discipline

- Preparing for the Media Feeding Frenzy.
- Spokesperson selection and training.
- The "Three R's" of Crisis Communication.
- Case Study: The Target Data Breach response.
- Conducting effective on-camera mock interviews and "ambush" media drills with immediate, actionable feedback.

Module 4: Managing the Digital Crisis and Misinformation

- Developing a Dark Site for rapid deployment of official statements and continuous updates.
- Social media triage and monitoring.
- Strategies for rapid and decisive action to counter rumors and stop the spread of fake news or unverified facts.
- Case Study: The Sony Pictures Hack examining the role of leaked internal communications and social media damage.
- Leveraging third-party validation to enhance organizational credibility.

Module 5: Internal Communication for Trust and Continuity

- Crafting immediate and consistent messaging for employees to prevent internal confusion and external leaks.
- The vital role of middle management and internal channels as trusted messengers during a crisis.
- Addressing employee safety, operational impact, and the psychological effects of a security incident.
- Case Study: Examining best-practice internal communication during an operational security incident to maintain Business Continuity.
- Utilizing "All-Hands" meetings and executive video messages to demonstrate strong, reassuring leadership.

Module 6: Legal, Compliance, and Ethical Communication

- Understanding the tension between Legal Hold and Transparency: how to communicate openly without compromising legal standing.
- Adhering to global breach notification laws.
- Working effectively with external counsel and forensic investigators to streamline the flow of verified information.
- Case Study: Regulatory fines and communication failures following a major data exposure event in a highly regulated industry.
- Embedding ethical communication principles as the cornerstone of the crisis response philosophy.

Module 7: Crisis Simulation and Tabletop Exercise (TTX)

- Introduction to advanced Scenario-Based Learning and the pressure-cooker environment of a live TTX.
- A simulated Ransomware Attack on Critical Systems: participants execute their communication plan in real-time.
- Testing decision-making pathways.
- Case Study: Post-TTX debrief of a recent large-scale Cyber Espionage scenario, focusing on leadership clarity and decision logs.
- Identifying "single points of failure" in the communication chain and immediate actions for remediation.

Module 8: Post-Crisis Recovery and Organizational Resilience

- Executing the Reputation Repair Plan.
- Conducting a formal After-Action Review to institutionalize communication lessons learned.
- Developing and communicating material changes to security posture and governance to the Board and public.
- Case Study: The prolonged Brand Recovery efforts following a major security incident and quantifying the Return on Crisis Preparedness.
- Shifting the narrative from "incident response" to proactive Organizational Resilience and future-proofing.

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.

- Continuous feedback and personalized guidance.

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