

Cybersecurity Crisis Management

Professional Training Course

Skillslab Training Provider

Skills for Tomorrow's World 



Course Description

Introduction

Cybersecurity Crisis Management is an advanced professional training program designed to help organizations prepare for, manage, and recover from high-impact cyber incidents. The course equips executives, cybersecurity leaders, risk professionals, operational managers, and public sector decision-makers with the strategic, technical, and governance capabilities required to respond effectively to ransomware, data breaches, service disruptions, insider threats, supply chain attacks, and other cyber emergencies.

The executive-level value of this program lies in its ability to transform cyber incident response from a purely technical activity into a coordinated organizational crisis management capability. Participants learn how to protect critical operations, make timely decisions under pressure, maintain stakeholder confidence, meet regulatory obligations, and restore essential services while controlling financial, legal, operational, and reputational damage.

Through realistic simulations, crisis scenarios, decision exercises, and implementation workshops, participants will examine cyber incident command structures, executive response protocols, digital forensics coordination, business continuity, crisis communication, regulatory reporting, third-party risk, recovery planning, and post-incident improvement. The program is particularly suitable for government entities, ministries, public sector institutions, critical infrastructure operators, and large corporations seeking to strengthen cyber resilience and organizational readiness.

Course Objectives

By the end of the Cybersecurity Crisis Management training course, participants will be able to:

- Understand the strategic, operational, legal, and reputational dimensions of cyber crises.
- Distinguish cyber incidents from major organizational cybersecurity emergencies.
- Establish effective cyber crisis governance and incident command structures.

- Define roles, responsibilities, escalation thresholds, and executive decision authorities.
- Coordinate cybersecurity, technology, legal, risk, communication, and operational teams.
- Assess the business impact of ransomware, breaches, disruption, and data loss.
- Make evidence-based decisions under uncertainty and severe time pressure.
- Develop effective internal, external, regulatory, and media communication strategies.
- Integrate cyber incident response with business continuity and disaster recovery.
- Manage third-party, supplier, and critical infrastructure dependencies during crises.
- Conduct structured post-incident reviews and identify resilience improvements.
- Develop a practical cybersecurity crisis management and response roadmap.

Course Content

Day 1: Cyber Crisis Governance and Organizational Preparedness

- Understanding the nature and lifecycle of cybersecurity crises.
- Differentiating incidents, emergencies, disruptions, and enterprise-level crises.
- Identifying major cyber threats and organizational impact scenarios.
- Defining cyber crisis governance and executive accountability.
- Establishing crisis leadership, command, and coordination structures.
- Assigning responsibilities across technical and non-technical teams.
- Creating escalation thresholds and crisis activation criteria.
- Assessing organizational readiness and cyber resilience maturity.
- Developing crisis management policies, plans, and response procedures.
- Aligning cybersecurity response with enterprise risk management.

Day 2: Incident Command, Decision-Making, and Operational Coordination

- Establishing a cyber incident command and control framework.
- Managing incomplete, conflicting, and rapidly changing information.
- Prioritizing people, critical services, systems, data, and assets.

- Coordinating security operations, technology, legal, risk, and business teams.
- Developing executive situation reports and decision briefings.
- Managing crisis meetings, action tracking, and accountability.
- Evaluating containment, isolation, shutdown, and continuity decisions.
- Maintaining evidence integrity and supporting digital investigations.
- Coordinating with law enforcement and external specialists.
- Managing prolonged cyber incidents and leadership fatigue.

Day 3: Ransomware, Data Breaches, and Critical Service Disruption

- Understanding ransomware attack patterns and business impact.
- Evaluating encryption, data theft, extortion, and service disruption scenarios.
- Assessing legal, ethical, financial, and operational response options.
- Managing data breach identification, containment, and notification.
- Determining the scope of compromised systems and sensitive information.
- Protecting critical services and maintaining essential operations.
- Evaluating backup reliability and restoration priorities.
- Coordinating forensic, recovery, and business continuity activities.
- Managing insider threats and privileged account compromise.
- Addressing third-party and supply chain cyber incidents.

Day 4: Crisis Communication, Stakeholder Management, and Compliance

- Developing clear internal cybersecurity crisis communication.
- Briefing executives, boards, regulators, employees, and operational teams.
- Communicating with customers, citizens, partners, and suppliers.
- Managing media interest, public statements, and reputational risk.
- Avoiding speculation, inconsistency, and premature disclosure.
- Coordinating communication with legal and regulatory requirements.
- Preparing notification messages for affected stakeholders.

- Managing misinformation, rumors, and social media pressure.
- Maintaining stakeholder trust during prolonged disruptions.
- Documenting decisions, approvals, communications, and regulatory actions.

Day 5: Recovery, Resilience, and Crisis Simulation

- Establishing safe system restoration and service recovery priorities.
- Validating systems, data integrity, access controls, and security measures.
- Managing phased recovery and return-to-operation decisions.
- Monitoring for reinfection, persistence, and secondary attacks.
- Conducting structured post-incident reviews and lessons learned.
- Identifying control failures, process gaps, and capability weaknesses.
- Updating response plans, policies, training, and technical controls.
- Measuring cyber resilience and crisis management performance.
- Conducting an executive-level cybersecurity crisis simulation.
- Developing an organizational cyber crisis improvement roadmap.

Target Audience

This Cybersecurity Crisis Management course is designed for:

- Senior executives responsible for organizational resilience and strategic risk.
- Chief information security officers and cybersecurity leaders.
- Chief information officers and technology executives.
- Government and ministry officials overseeing digital security and continuity.
- Cyber incident response and security operations professionals.
- Enterprise risk, governance, and compliance managers.
- Business continuity and disaster recovery professionals.
- Legal, regulatory, privacy, and data protection specialists.
- Corporate communication and public affairs leaders.
- Critical infrastructure and operational technology managers.

- Internal auditors and assurance professionals.
- Crisis management and emergency response teams.
- Technology vendors and third-party risk managers.
- Consultants supporting cyber resilience and incident response programs.

Course Requirements

No advanced programming knowledge is required. Participants should have a general understanding of cybersecurity, organizational risk, information technology, crisis management, business continuity, compliance, or executive decision-making.

Attendees are encouraged to bring examples of current incident response plans, crisis structures, business continuity arrangements, escalation procedures, or cyber risk scenarios for selected exercises. A laptop is recommended for crisis planning, scenario analysis, response mapping, communication development, and implementation activities.

Training Methodology

The training methodology combines executive education, crisis simulation, practical planning, and collaborative decision-making. The course is designed to help participants develop the confidence and discipline required to manage cyber emergencies in realistic organizational environments.

The program includes:

- Expert-led presentations based on current cybersecurity practices.
- Real-world cyber crisis case studies.
- Ransomware and data breach response scenarios.
- Executive decision-making exercises under pressure.
- Cyber incident command and coordination workshops.
- Crisis communication and stakeholder briefing activities.
- Business continuity and recovery planning exercises.
- Regulatory notification and documentation scenarios.

- Tabletop simulations involving multidisciplinary response teams.
- Post-incident review and improvement workshops.
- Individual and organizational action planning.

This applied methodology enables participants to test their response capabilities, identify gaps, and develop practical improvements that can be implemented within their organizations.

Learning Outcomes

Upon successful completion of the program, participants will be able to:

- Recognize when a cyber incident requires enterprise crisis activation.
- Establish effective leadership, governance, and coordination arrangements.
- Manage cybersecurity decisions under uncertainty and operational pressure.
- Prioritize critical services, systems, information, and stakeholder needs.
- Coordinate technical response with business continuity and recovery.
- Respond effectively to ransomware, breaches, and digital disruption.
- Communicate clearly with executives, employees, regulators, and the public.
- Manage legal, compliance, privacy, and reputational considerations.
- Evaluate supplier and third-party risks during cyber emergencies.
- Lead structured recovery and post-incident improvement activities.
- Strengthen organizational cyber resilience and crisis preparedness.
- Develop a practical cybersecurity crisis management implementation plan.

Instructor Profile

The program is delivered by an internationally certified expert with extensive practical and consulting experience. The instructor possesses broad expertise in cybersecurity crisis management, cyber incident response, digital risk, business continuity, ransomware response, data breach management, crisis communication, governance, regulatory compliance, and organizational resilience.

The instructor uses realistic case studies, executive simulations, facilitated discussions, decision exercises, and implementation-focused workshops to ensure participants can apply the learning directly within their

organizations. The delivery approach is suitable for executives, government representatives, cybersecurity professionals, technology leaders, risk managers, legal specialists, and multidisciplinary crisis teams.

Contact Us

For registration inquiries, upcoming dates, or group pricing, please contact us:

Website

www.skillslab-training.com

Email

info@skillslab-training.com

WhatsApp

+966 559 653 447

Generated by Skillslab Training

info@skillslab-training.com | WhatsApp: +966 559 653 447

www.skillslab-training.com