QUEST
Professional Center

PROFESSIONAL TRAINING COURSE

Course No. 1983

Incident Response Planning, Playbooks & Cyber Crisis Management Training Course

SECURITY OPERATIONS & INCIDENT RESPONSE
INFORMATION TECHNOLOGY & CYBERSECURITY

DURATION
5 Days

DELIVERY
Classroom

Course Overview

The Incident Response Planning, Playbooks & Cyber Crisis Management Training Course provides a practical and strategic framework for preparing organizations to detect, respond to, contain, and recover from cybersecurity incidents. The program focuses on building structured incident response capabilities that enable security, IT, risk, compliance, and executive teams to coordinate effectively when facing cyber threats and disruptive security events.

Participants will examine the complete incident response lifecycle, from preparation and detection through analysis, containment, eradication, recovery, and post-incident improvement. The course addresses incident classification, escalation criteria, roles and responsibilities, communication protocols, evidence handling, decision-making, business continuity considerations, and coordination between technical and non-technical stakeholders.

A major focus of the program is the development and effective use of incident response playbooks. Participants will learn how to translate organizational risks and common attack scenarios into actionable response procedures covering events such as ransomware, phishing, compromised accounts, malware infections, data breaches, denial-of-service attacks, insider threats, and third-party security incidents. Emphasis is placed on creating clear decision points, response actions, escalation paths, and communication requirements.

The course also addresses cyber crisis management at the organizational and executive levels. Participants will explore how to manage high-impact incidents involving business disruption, sensitive information, regulatory obligations, reputational exposure, and critical services. Through simulations, tabletop exercises, scenario analysis, and response planning workshops, participants will develop practical capabilities to improve organizational readiness and resilience.

Objectives

- By the end of the course, participants will be able to:
- Explain the principles and lifecycle of cybersecurity incident response.
- Assess organizational readiness for cybersecurity incidents and crisis situations.
- Develop structured incident response plans aligned with organizational risks.
- Define incident severity levels, escalation criteria, and response priorities.

- Establish clear roles and responsibilities across incident response teams.
- Design practical playbooks for common cybersecurity incident scenarios.
- Apply structured procedures for incident detection, analysis, containment, and recovery.
- Strengthen coordination between cybersecurity, IT, risk, legal, compliance, communications, and executive teams.
- Develop effective internal and external communication procedures during cyber incidents.
- Evaluate business and operational impacts when responding to major security incidents.
- Apply appropriate principles for evidence preservation and incident documentation.
- Manage decision-making under pressure during high-impact cyber events.
- Develop cyber crisis escalation and executive notification processes.
- Conduct tabletop exercises to test incident response capabilities.
- Identify weaknesses in existing response plans and playbooks.
- Establish post-incident review and continuous improvement mechanisms.

Who Should Attend

This course is designed for cybersecurity managers, security operations professionals, incident response specialists, information security professionals, IT managers, security engineers, threat and vulnerability management professionals, and professionals responsible for developing or operating organizational incident response capabilities.

It is also suitable for risk and compliance professionals, business continuity specialists, internal control teams, legal and privacy professionals, communications managers, technology leaders, crisis management teams, and executives who may participate in cyber incident decision-making or organizational crisis response.

The program is particularly relevant to government entities, ministries, banks and financial institutions, oil and gas organizations, critical infrastructure operators, telecommunications companies, technology organizations, multinational corporations, and large enterprises seeking to strengthen cybersecurity preparedness, incident response maturity, and cyber resilience.

Learning Outcomes

- Upon completion of the course, participants will be able to:
- Assess the maturity of an organization's incident response capability.
- Map critical systems, stakeholders, dependencies, and response requirements.
- Build an incident response plan with defined phases and responsibilities.
- Classify cybersecurity incidents according to severity, impact, and urgency.
- Establish escalation thresholds and decision-making authorities.
- Develop actionable playbooks for priority cybersecurity scenarios.
- Coordinate technical response activities with business and executive requirements.
- Structure incident communications for internal and external stakeholders.
- Support evidence preservation and accurate incident documentation.
- Evaluate operational, financial, regulatory, and reputational impacts during a cyber crisis.
- Coordinate containment, eradication, and recovery activities.
- Conduct structured tabletop exercises and evaluate response performance.
- Identify gaps in response plans, procedures, roles, and capabilities.
- Develop corrective actions following cybersecurity incidents.
- Establish measurable indicators for incident response readiness and performance.
- Create a practical roadmap for improving cyber crisis management and organizational resilience.

Course Outline

DAY 01

Foundations of Incident Response and Cybersecurity Readiness

- Cybersecurity incident response principles and objectives.
- The incident response lifecycle.
- Incident types, categories, and severity levels.
- Threat identification and incident recognition.
- Incident response readiness assessment.
- Roles of security operations and incident response teams.

DAY 01 — CONTINUED

- Responsibilities of IT, risk, compliance, legal, communications, and management.
- Incident classification and prioritization.
- Escalation criteria and notification thresholds.
- Incident response policies and governance.
- Integration with business continuity and disaster recovery.
- Building organizational incident response readiness.

PRACTICAL APPLICATION

Conduct an incident response readiness assessment and develop an initial incident classification and escalation framework.

DAY 02

Incident Response Planning and Playbook Development

- Structure and components of an incident response plan.
- Defining response roles and decision authorities.
- Incident response procedures and workflows.
- Designing actionable cybersecurity playbooks.
- Playbook structure, triggers, decision points, and response actions.
- Ransomware incident response.
- Phishing and credential compromise response.
- Malware and endpoint compromise response.
- Data breach and unauthorized data access response.
- Denial-of-service incident response.
- Insider threat and third-party incident response.
- Playbook testing, maintenance, and version control.

PRACTICAL APPLICATION

Develop a complete incident response playbook for a selected cyber incident scenario, including triggers, roles, actions, escalation, communications, and recovery requirements.

DAY 03

Incident Investigation, Containment and Recovery

- Incident detection, validation, and initial analysis.
- Establishing incident timelines.
- Evidence identification and preservation.
- Documentation and incident records.
- Containment strategies and response priorities.
- Short-term and long-term containment.
- Threat eradication and root cause analysis.
- System recovery and service restoration.
- Coordination with technology and business teams.
- Managing dependencies during recovery.
- Validating system security after recovery.
- Lessons learned and post-incident analysis.

PRACTICAL APPLICATION

Analyze a simulated cybersecurity incident from detection through containment and recovery, documenting key decisions, evidence, actions, and outcomes.

DAY 04

Cyber Crisis Management and Executive Response

- From cybersecurity incident to organizational crisis.
- Cyber crisis identification and escalation.
- Executive decision-making during major cyber incidents.
- Crisis management structures and responsibilities.
- Business impact assessment.
- Protecting critical services and business operations.
- Internal and external crisis communications.
- Stakeholder, customer, partner, and supplier communications.
- Regulatory, legal, privacy, and compliance considerations.

DAY 04 — CONTINUED

- Media and reputational risk management.
- Managing uncertainty and conflicting information.
- Executive briefings and crisis decision logs.

PRACTICAL APPLICATION

Conduct an executive-level cyber crisis simulation involving business disruption, sensitive information exposure, stakeholder communications, and competing response priorities.

DAY 05

Tabletop Exercises, Response Testing and Continuous Improvement

- Principles of effective incident response exercises.
- Designing cybersecurity tabletop scenarios.
- Testing incident response plans and playbooks.
- Evaluating team coordination and decision-making.
- Measuring response effectiveness and readiness.
- Identifying gaps in people, processes, technology, and governance.
- Incident response performance indicators.
- Post-exercise reporting and corrective actions.
- Updating playbooks based on lessons learned.
- Continuous improvement and response maturity.
- Building a sustainable cyber crisis management capability.
- Developing an incident response improvement roadmap.

FINAL WORKSHOP

Conduct an integrated cyber crisis tabletop exercise from initial detection through executive escalation, incident containment, crisis communication, recovery, and post-incident review, followed by development of a prioritized improvement roadmap.

QUEST
Professional Center

Register or Request More Information

Course page: https://quest-training.com/courses/incident-response-planning-playbooks-cyber-crisis-management-training-course
Website: https://quest-training.com
Email: info@quest-training.com
Phone: +905016771440