CONCEPT

Cyber Crisis Leadership and Incident Response Governance



Cyber Crisis Leadership and Incident Response Governance

Introduction

Catastrophic network intrusions, data exfiltration and extortion threats increasingly paralyse critical digital infrastructure, presenting organisations with high-velocity dilemmas that conventional business continuity runbooks fail to resolve. Navigating these adversarial incidents requires disciplined command protocols to decipher intrusion telemetry, enforce immediate containment boundaries, and meet each regulator's notification deadline, from immediate notification to SAMA to 72 hours for personal-data breaches under the PDPL. Participants leave with a tested Cyber Incident Response Runbook for their organisation. This one-week advanced programme in Cyber Crisis Leadership and Incident Response Governance is delivered by Core Concept.

Course Objectives

- Direct enterprise breach response across technical remediation, corporate communications, and statutory legal reporting lines.
- Calibrate escalation thresholds for critical digital infrastructure disruption using threat actor profiling and compromise telemetry.
- Command high-stakes ransomware extortion response deliberations, weighing data recovery probabilities against legal liabilities.
- Establish compliance workflows that meet the mandatory incident-reporting obligations of NCA, SAMA and SDAIA.
- Deploy cyber incident command structures using rapid triage cycles, forensic evidence preservation, and defensible rationale logs.
- Formulate an enterprise-specific digital disruption runbook establishing command hierarchy, technical containment triggers, and stakeholder holding statements.

Target Audience

- Executives accountable for enterprise security strategy, breach defence and the decision to escalate a cyber incident to crisis level
- Legal, privacy and compliance leads accountable for mandatory regulatory disclosure workflows and the defensibility of incident evidence
- Incident command and security operations leads responsible for directing triage, containment and threat intelligence during a breach
- Communications leads responsible for protecting reputation and briefing media, customers and partners during major security outages
- Resilience and infrastructure owners responsible for coordinating recovery steering groups and restoring critical digital services

Course Outline

Day 1: Threat Landscape, Incident Triage and Escalation Triggers

- Adversary Tradecraft Evolution: Data Exfiltration, Double Extortion Schemes, and Critical System Sabotage
- Cyber Threat Severity Classification: Distinguishing Routine Malware Alerts from Catastrophic Enterprise Breaches
- Initial Triage Telemetry Analysis: Interpreting Endpoint Detection, Network Anomalies, and Initial Access Indicators
- Escalation Trigger Matrix Design: Thresholds Separating Localised Containment from Enterprise-Wide Emergency Activation
- Baseline Readiness Assessment against International Cybersecurity Incident Handling Standards

Day 2: Incident Command Structure and Regulatory Reporting Mandates

- Unified Incident Command Architecture: Roles, Responsibilities, and Delegated Containment Authority
- Statutory Disclosure Protocols: Mapping and Meeting NCA, SAMA and PDPL Notification Requirements
- Legal Liability and Evidentiary Defensibility: Chain-of-Custody Preservation and Forensic Log Retention
- Cross-Functional Coordination Workflows: Bridging CISO Technical Findings with Legal Counsel and Board Oversight
- Steering Committee Battle Rhythms: Briefing Cadences, Situation Report Templates, and Stakeholder Update Channels

Day 3: Ransomware Extortion Handling and Critical Containment

- Threat Actor Engagement Dilemmas: Legal Prohibitions, Sanctioned Entity Screening, and Negotiation Posture Options
- Technical Containment Measures: Network Segmentation, Identity Revocation, and Operational Technology Isolation
- Business Interruption Mitigation: Critical Digital Infrastructure Disruption Handling and Core Service Recovery Tiers
- Stakeholder Salience and Communication: Managing Third-Party Vendor Alerts, Customer Disclosures, and Press Inquiries
- Countering Cognitive Stress Traps: Mitigating Analysis Paralysis and Alarm Fatigue during Fast-Moving Breach Events

Day 4: Forensics, Business Restoration and Systemic Renewal

- Forensic Investigation Oversight: Coordinating External Incident Response Retainers and Digital Investigators
- Safe Restoration Workflows: Clean Room Validation, Golden Image Redeployment, and Active Directory Rebuilding
- Enterprise Recovery Milestones: Service Restitution Priorities, Integrity Verification, and Formal Incident De-Escalation
- Regulatory Post-Incident Filings: Compiling Comprehensive Root-Cause Documentation and Supervisory Remediation Reports
- Post-Incident Review Methodology: Conducting Blameless Technical Post-Mortems and Institutionalising Defense Adaptations

Day 5: High-Stakes Cyber Attack Simulation and Playbook Synthesis

- Advanced Tabletop Simulation: Responding to a Catastrophic Ransomware Extortion Response Scenario across Distributed Systems
- Real-Time Regulatory Challenge: Executing Mandatory Regulatory Disclosure under Tight Statutory Deadlines
- Technical Press Conference Practicum: Delivering Adversarial Media Briefings and Customer-Facing Transparency Reports
- Assembly of the Cyber Incident Response Runbook: Defining Containment Authorities, Contact Rosters, and Notification Workflows
- Expert Review Panel: Defensive Runbook Stress-Testing and Operational Readiness Validation

Skills You Will Gain

- Cyber incident command
- Ransomware extortion response
- Mandatory regulatory disclosure
- Breach containment protocols
- Forensic log governance
- Threat telemetry interpretation
- Critical infrastructure restoration
- Post-breach evidentiary reporting

Why Attend This Course

- Equip your steering group with proven breach containment protocols designed to withstand high-velocity cyber extortion events.
- Master compliant notification workflows to confidently satisfy strict mandatory regulatory disclosure obligations without risking supervisory penalties.
- Bridge the communication barrier between deep technical digital forensics, corporate legal obligations, and senior oversight boards.
- Leave with an enterprise-ready Cyber Incident Response Runbook tailored to defend your critical digital infrastructure assets against disruption.

Frequently Asked Questions

What technical background is required for this programme?

This course is designed for senior professionals, security directors, and legal leads; while a high-level comprehension of enterprise IT architecture is beneficial, deep programming or hands-on penetration testing skills are not required.

How does this programme address statutory reporting requirements?

The curriculum details the compliance workflows needed to meet supervisory disclosure deadlines, which range from immediate notification SAMA to 72 hours for personal-data breaches SDAIA, PDPL, during critical infrastructure disruption and data compromise events.

What deliverable do participants complete during the course?

Participants construct and validate an enterprise Cyber Incident Response Runbook, integrating containment authority matrices, extortion negotiation parameters, and regulatory reporting procedures.

Conclusion

Sustaining digital operational resilience during severe cyber attacks demands decisive breach command, precise threat evaluation, and strict adherence to supervisory disclosure obligations. By mastering threat containment protocols, forensic preservation, and statutory reporting under intense operational pressure, enterprise steering teams protect their networks, reputations, and corporate viability. Senior professionals return to their organisations prepared to lead through digital hostility with technical clarity and defensible governance.