Qualifi Level 5 Diploma in Cyber Security

Communications and Incident Management

Level 5: Diploma in Cyber Security
UeCampus Study Guide

Academic Module Study Guide Online Learning

Unit Overview: Three Chapters

Chapter 1

Managing Major Cyber Incidents

CERT teams, site set-up, staffing, Gold–Silver–Bronze command, equipment and technology

Chapter 2

BCM, DR, and Crisis Management

Business continuity, disaster recovery, crisis management, integration with incident response

Chapter 3

Crisis Comms & Cyber Resilience

Communications strategy, isomorphic lessons, breach case studies, building cyber resilience

The Nature and Impact of Major Cyber Incidents

What Is a Major Incident?

An event that significantly disrupts operations, compromises critical systems/data, and requires coordinated cross-functional response

NCSC classifies: Category 6 (localised) to Category 1 (national cyber emergency)

Examples: ransomware, data breaches, DDoS, supply chain compromise, insider threats

$4.88M

Global average cost per data breach (IBM, 2024)

£3.58M

UK average cost per data breach (IBM, 2024)

50% of UK businesses reported a cyber breach in the past 12 months (UK Gov Cyber Security Breaches Survey 2024)

Computer Emergency Response Teams (CERTs)

National CERTs

Country-wide coordination.
UK: NCSC (part of GCHQ)

Sectoral CERTs

Industry-specific.
e.g. Financial Sector (FSCCC)

Organisational CSIRTs

Internal teams detecting, responding, recovering

Vendor CERTs

Product vulnerability management (e.g. MSRC)

Building an Organisational CSIRT Requires:

- Clear mandate & authority from senior management
- Defined scope, SOPs, and escalation procedures
- Skilled staff (handlers, forensic analysts, threat intel)
- Secure communication channels and established external relationships (NCSC, law enforcement, ISACs)

Site Set-Up and Staffing for Major Incidents

Incident Response Facility (War Room)

- Secure room with restricted, logged access
- Multiple display screens for dashboards
- Dedicated phone lines, encrypted messaging
- Secondary out-of-band communications
- Dedicated scribe for real-time documentation
- Welfare: food, rest areas, shift rotation

Key Incident Response Roles

Incident Commander	Strategic decisions, external liaison
Technical Lead	Investigation, containment, eradication
Communications Lead	Internal/external comms, media, PR
Legal Advisor	GDPR notification, law enforcement
Forensic Analyst(s)	Evidence acquisition and analysis
Threat Intel Analyst	IOCs, attacker research, context
Scribe/Recorder	Maintains real-time incident log

Gold–Silver–Bronze Command Structure

GOLD

Strategic

Senior management / board level
Sets strategic objectives
‘Protect customer data’, ‘Restore in 24hrs’

SILVER

Tactical

Incident Commander & leads
Translates strategy into tactical plans
Coordinates all response activities

BRONZE

Operational

Technical staff executing response
Forensic analysts, sysadmins, engineers
Containment, investigation, remediation

Mirrors UK emergency services command structure — recommended by the NCSC for major cyber incident management

Business Continuity Management (BCM)

Business Impact Analysis (BIA)

Identify critical processes,
RTO, RPO, MTPD

Risk Assessment

Threats, vulnerabilities, likelihood, impact

Strategy Development

Alternative locations, IT recovery, supply chain

Plan Development

Documented BCPs with roles and procedures

Exercise & Testing

Tabletop, simulation, full-scale drills

RTO (Recovery Time Objective): Max acceptable downtime **RPO** (Recovery Point Objective): Max acceptable data loss
MTPD (Max Tolerable Period of Disruption): Point of irreversible damage

Disaster Recovery Strategies

Cold Site

Days–weeks

Lowest cost

Basic infrastructure only, no pre-installed equipment

Warm Site

Hours–days

Medium cost

Hardware installed, not fully synchronised

Hot Site

Minutes–hours

Highest cost

Full replica with real-time data replication

Cloud DRaaS

Minutes–hours

Flexible cost

Cloud-based DR (AWS, Azure, GCP). Scalable

3-2-1 Backup Rule:

3 copies • 2 different media types • 1 offsite/cloud • + 1 offline/air-gapped (ransomware protection) • 0 errors (verified restores)

Crisis Management Principles

Crisis Management Team (CMT)

- CEO / Managing Director
- CISO / CTO
- Head of Communications / PR
- General Counsel / Legal
- Chief Operations Officer
- HR Director
- External advisors as required

Core Principles

Speed of response: First hours are critical

Transparency: Concealment always worsens outcomes

Empathy: Acknowledge impact on individuals

Accountability: Accept responsibility, show actions

Consistency: Single source of messaging

Compliance: ICO within 72hrs for data breaches

Integrating BCM, DR, CM, and Incident Response

Incident Response	Technical detection, containment, eradication	**Attacker evicted; systems cleaned**
Disaster Recovery	IT systems and data restoration	**Systems restored within RTO/RPO**
Business Continuity	Maintaining critical business operations	**Business continues operating**
Crisis Management	Strategic coordination and reputation	**Stakeholder confidence maintained**

All four disciplines must operate in concert — the CMT provides direction, IR feeds intelligence, BCM maintains operations, DR restores systems

The Role of Communications in Incident Management

Internal Communications

- Staff notification – what happened, what to do
- Management briefings – structured updates
- Cross-functional coordination – consistent messaging across all departments

External Communications

- Customer notification – GDPR: high-risk breaches
- Regulatory – ICO within 72 hours
- Media – proactive engagement, holding statements
- Law enforcement – Action Fraud, NCA, NCSC
- Supply chain – partner notification and collaboration

What an organisation says — and when and how it says it — can determine whether an incident results in a manageable disruption or an existential crisis

Isomorphic Lessons from Major Cyber Breaches

TalkTalk (2015)

£400K fine, £60M cost,
100K+ customers lost

Lesson:

Verify facts before public statements. Implement basics.

BA (2018)

£20M ICO fine
(initially £183M proposed)

Lesson:

Swift notification mitigates but doesn't eliminate penalties.

Maersk (2017)

$300M cost, 49K laptops,
3,500 servers destroyed

Lesson:

Offline backups essential. Geographic diversity saves.

SolarWinds (2020)

18,000 orgs affected,
9 months undetected

Lesson:

Supply chain security critical. Zero Trust reduces blast radius.

Isomorphic learning: drawing lessons from other organisations' incidents and applying them to your own context

Building Cyber Resilience: The Five Pillars

Identify	Protect	Detect	Respond	Recover
Assets, risks, threat landscape analysis	Access mgmt, encryption, segmentation, training	SIEM, EDR, IDS/IPS, threat hunting	IR plans, trained teams, communications	DR, BCM, immutable backups, rebuild

Organisational Culture for Resilience:

- Board-level engagement as a standing agenda item
- Security awareness training with phishing simulations
- Just culture – encourage reporting without blame
- Post-incident reviews and continuous improvement

Future-Proofing and Disruptive Technology

AI-Powered Attacks	Sophisticated phishing, deepfakes, automated exploitation — but also enhanced defensive AI
Quantum Computing	Could break current public key cryptography; organisations must plan post-quantum migration
Supply Chain Complexity	Cloud services, SaaS, third-party integrations expanding the attack surface dramatically
IoT & OT Convergence	Industrial control systems integrating with IT creates new vectors with physical consequences
Regulatory Evolution	DUA Act 2025, NIS2, sector-specific rules demand ongoing compliance monitoring

Key Takeaways

- Major cyber incidents require coordinated cross-functional response — CERT/CSIRT teams with clear mandates, authority, and skilled personnel
- Gold–Silver–Bronze command structure provides clear strategic, tactical, and operational decision-making layers
- BCM, DR, and Crisis Management are distinct but interdependent disciplines that must operate in concert with incident response
- Business Impact Analysis (BIA) establishes RTO, RPO, and MTPD — the foundation of all recovery and continuity planning
- The 3-2-1 backup rule with immutable, air-gapped backups is critical defence against ransomware
- Crisis communications must be fast, accurate, empathetic, and consistent — poor communications can be more damaging than the breach itself
- Isomorphic learning from TalkTalk, BA, Maersk, and SolarWinds provides transferable lessons for all organisations
- Cyber resilience spans five pillars: Identify, Protect, Detect, Respond, Recover — supported by board engagement and just culture