Communications and Incident Management

First published in 2026 by UE Campus

Unit specifications can be found on the UE Campus Portal: https://uecampus.com/

Contents

Using your Study Guide

Welcome to the study guide, designed to support you in completing your Level 5 Diploma in Cyber Security.

This study guide follows the order of the syllabus, which is the basis for your studies. Each chapter starts by listing the syllabus learning outcomes covered and the assessment criteria.

Level 5 Units

The study guide includes a number of features to enhance your studies:

📝	'Over to you:' activities for you to apply what you have learned.
🌍	'Industry Insights:' discover up-to-date trends, expert opinions, and real-world examples from incident management practice.
🧭	'Did you know?' highlights interesting facts or surprising information to deepen your understanding.
💼	'Case studies:' realistic scenarios to reinforce and test your understanding.
📱	'Revision on the go:' use your phone camera to capture key pieces of learning and save them as revision notes.
❗	'Need to know:' key pieces of information highlighted in the text.
💡	'Examples:' illustrating points made in the text to show how it works in practice.

Note: Website addresses current as of March 2026.

Level 5 Communications and Incident Management

About this unit

The professional and lawful response to managing an incident can be the difference between company survival or otherwise. Poor responses to major incidents, including mega data breaches, have significantly damaged organisational reputations and financial performance. Significantly mismanaging a cyber incident can result in catastrophic personal and organisational consequences.

In this unit you will explore the types of site, personnel, and equipment required in relation to planning for incident management and forming an organisational CERT team (Computer Emergency Response Team). You will then explore the core sub-disciplines of cyber incident management: Disaster Recovery, Business Continuity Management, and Crisis Management. You will discuss the importance of the organisational requirement for skilled and planned communications to operate in combination with advanced management responses and strategy.

You will develop an understanding of security technical and generic management and leadership teaching. Much of this teaching will be particularly relevant to learners wishing to move into more advanced Information Security Management technical qualifications, including the CompTIA Security+ accreditation and the Cyber Security industry gold standard: the Certified Information Systems Security Professional (CISSP).

Chapter One – Managing Major Cyber Security Incidents

Introduction

This chapter examines the physical and human resources required to manage a major suspected cyber security incident. You will analyse the nature and impact of major cyber incidents, study the structure and function of Computer Emergency Response Teams, evaluate site set-up and staffing requirements, assess organisational arrangements and command structures, and examine the equipment and technology needs for effective incident management.

Learning Outcomes

On completing this chapter, you will be able to:

- Understand the physical and human resources required to manage a major suspected cyber security incident.

Assessment Criteria

1.1 Explain site set-up, staffing and organisational arrangements for major suspected cyber-related incidents.

1.1 The nature and impact of major cyber incidents

Over to you – Video Watch: Incident Response

Watch this YouTube video:

Title: Incident Response

Link: https://www.youtube.com/watch?v=YZSM3YPn998

After watching, describe the NIST incident response lifecycle and explain why preparation is the most important phase of incident management.

Defining a Major Cyber Incident

A major cyber incident is an event that significantly disrupts an organisation's operations, compromises the confidentiality, integrity, or availability of critical systems or data, and requires a coordinated, cross-functional response beyond normal IT operations. The UK National Cyber Security Centre (NCSC) classifies incidents from Category 6 (localised) to Category 1 (national cyber emergency).

Major incidents may include: ransomware attacks that encrypt critical systems and halt operations; large-scale data breaches exposing personal, financial, or intellectual property data; distributed denial-of-service (DDoS) attacks that overwhelm public-facing services; supply chain compromises that cascade across multiple organisations; and insider threats involving deliberate sabotage or data theft.

The Business Impact of Major Incidents

The impact of a major cyber incident extends far beyond the immediate technical disruption:

- **Financial impact** – direct costs include incident response, forensic investigation, system restoration, legal fees, regulatory fines, and customer notification. IBM's 2024 Cost of a Data Breach Report found the global average cost was $4.88 million per breach, with the UK average at £3.58 million.
- **Reputational damage** – loss of customer trust, negative media coverage, and long-term brand erosion. Research consistently shows that customers abandon organisations following significant breaches.
- **Operational disruption** – system downtime, loss of productivity, inability to deliver services, and supply chain disruption.
- **Regulatory consequences** – fines under UK GDPR (up to £17.5 million or 4% of global turnover), NIS Regulations penalties, and mandatory breach notifications within 72 hours.
- **Legal liability** – class action lawsuits, regulatory enforcement actions, and contractual penalties.
- **Human impact** – stress and burnout on incident response teams, impact on employees whose personal data may be compromised, and potential physical safety risks.

Did you know?

According to the UK Government's Cyber Security Breaches Survey 2024, 50% of businesses and 32% of charities reported experiencing some form of cyber security breach or attack in the previous 12 months. Among medium and large businesses, the figure rose to 70–74%. The average cost of the single most disruptive breach for

medium and large businesses was approximately £10,830. These figures underscore that cyber incidents are not exceptional events but a routine threat that every organisation must be prepared to manage.

1.2 Computer Emergency Response Teams (CERTs)

What Is a CERT/CSIRT?

A Computer Emergency Response Team (CERT), also known as a Computer Security Incident Response Team (CSIRT), is a dedicated team of specialists responsible for receiving, reviewing, and responding to computer security incident reports and activity. CERTs may operate at national, sectoral, or organisational levels.

Types of CERT/CSIRT

- **National CERTs** – provide incident response coordination for an entire country. The UK's national CERT function is delivered by the NCSC (part of GCHQ). CERT-UK was its predecessor before being absorbed into the NCSC in 2016.
- **Sectoral CERTs** – serve specific sectors such as financial services, healthcare, or government. For example, the Financial Sector Cyber Collaboration Centre (FSCCC) supports UK financial institutions.
- **Organisational CERTs/CSIRTs** – internal teams within individual organisations responsible for detecting, responding to, and recovering from security incidents.
- **Vendor CERTs** – operated by technology vendors to handle vulnerabilities and incidents affecting their products (e.g. Microsoft Security Response Center, Apple Product Security).

Building an Organisational CSIRT

An effective organisational CSIRT requires:

- **Clear mandate and authority** – senior management must formally establish the team with defined authority to investigate incidents, isolate systems, and coordinate response activities.
- **Defined scope and constituency** – which systems, networks, and business units the CSIRT serves.
- **Staffing and skills** – roles include CSIRT manager, incident handlers, forensic analysts, threat intelligence analysts, malware analysts, and communications liaison. The team size depends on the organisation but should provide adequate coverage including out-of-hours.
- **Standard Operating Procedures (SOPs)** – documented procedures for incident classification, triage, escalation, investigation, containment, eradication, recovery, and post-incident review.
- **Communication channels** – secure communication mechanisms for internal coordination and external reporting (encrypted email, secure messaging, dedicated phone lines).
- **Tooling** – SIEM, EDR, forensic tools, ticketing systems, threat intelligence platforms, and collaboration tools.
- **Relationships** – established relationships with law enforcement, the NCSC, sector regulators, external forensic providers, and peer organisations for information sharing (e.g. through ISACs – Information Sharing and Analysis Centres).

Over to you – CSIRT Design

Design the structure for a CSIRT for a UK-based e-commerce company with 300 employees and 50,000 daily transactions. Define: (1) the team's mandate and reporting line, (2) roles and responsibilities for each team member, (3) required skills and certifications, (4) operating model (in-house, hybrid, or outsourced), (5) escalation

procedures, and (6) external relationships. Present as a structured report of approximately 500 words.

1.3 Site set-up and staffing for major incidents

Incident Response Facility (War Room)

When a major incident is declared, a dedicated incident response facility (often called a 'war room' or 'bridge') should be activated. This provides a centralised location for the incident management team to coordinate the response:

- **Physical requirements** – a secure room with restricted access, sufficient desk space for the core team, multiple display screens for dashboards and monitoring, whiteboards or digital collaboration boards, reliable power supply with UPS, and dedicated network connectivity (isolated from the compromised network if necessary).
- **Communications infrastructure** – dedicated phone lines, secure video conferencing, encrypted messaging, and a secondary communication channel in case primary systems are compromised.
- **Documentation** – incident log (chronological record of all actions and decisions), evidence log, communications log, and decision log. A dedicated scribe should be assigned to maintain real-time documentation.
- **Welfare provisions** – major incidents may last days or weeks. Provisions for food, rest areas, and shift rotation are essential to maintain team effectiveness and prevent burnout.

Virtual and Hybrid Incident Response

In a post-pandemic world, many organisations operate with distributed teams. Virtual incident response capabilities are essential:

- Secure collaboration platforms (Microsoft Teams, Slack with enterprise security, or dedicated incident management platforms such as PagerDuty or Jira Service Management).
- Cloud-based forensic and analysis tools that can be accessed remotely.
- Pre-established secure VPN access for all CSIRT members.
- Regular exercises that test virtual response capabilities, not just co-located scenarios.

Staffing a Major Incident Response

Role	Responsibilities
Incident Commander	Overall authority for the response; makes strategic decisions; interfaces with senior management and external stakeholders.
Technical Lead	Directs technical investigation and remediation; coordinates forensic analysis; manages containment and eradication.
Communications Lead	Manages all internal and external communications; coordinates with PR/media; drafts customer notifications.
Legal Advisor	Provides guidance on regulatory obligations (GDPR notification), law enforcement engagement, and legal privilege.
Business Liaison	Interfaces between IT response and business units; assesses and communicates business impact.

Forensic Analyst(s)	Conducts evidence acquisition, preservation, and analysis. Maintains chain of custody.
Threat Intelligence Analyst	Researches the threat actor, attack vectors, and indicators of compromise; provides context for the investigation.
Scribe/Recorder	Maintains the real-time incident log documenting all actions, decisions, and communications.

1.4 Organisational arrangements and command structures

Incident Classification and Escalation

Incidents should be classified by severity to trigger appropriate response levels:

Severity	Description	Response Level
P1 – Critical	Complete loss of critical services; active data breach; ransomware encrypting production systems	Full CSIRT activation; senior management notification; potential external support; regulatory notification assessment
P2 – High	Significant degradation of services; confirmed unauthorised access; potential data exposure	Core CSIRT activation; management notification; enhanced monitoring
P3 – Medium	Limited impact; contained malware infection; suspicious but unconfirmed activity	Assigned incident handler(s); standard investigation; routine management reporting
P4 – Low	Minor security events; policy violations; single-user issues	Handled by IT operations or SOC; logged and monitored

Command Structures

For major incidents, a clear command structure prevents confusion and ensures effective coordination:

- **Gold (Strategic)** – senior management/board level. Sets the strategic objectives for the response (e.g. ‘protect customer data’, ‘restore operations within 24 hours’, ‘comply with all regulatory obligations’). Does not manage the tactical details.
- **Silver (Tactical)** – the Incident Commander and leads. Translates strategic objectives into tactical plans and coordinates the response activities across all teams.
- **Bronze (Operational)** – the technical staff executing the response: forensic analysts, system administrators, network engineers, and security analysts performing containment, investigation, and remediation tasks.

This Gold–Silver–Bronze framework mirrors the emergency services command structure widely used in the UK and is recommended by the NCSC for major cyber incident management.

1.5 Equipment and technology requirements

Core Technology Stack for Incident Response

- **SIEM (Security Information and Event Management)** – centralised log collection, correlation, and alerting. Essential for detection and investigation. Examples: Splunk, Microsoft Sentinel, IBM QRadar, Elastic Security.
- **EDR (Endpoint Detection and Response)** – real-time monitoring and response on endpoints. Enables remote isolation, memory capture, and artefact collection. Examples: CrowdStrike Falcon, Microsoft Defender for Endpoint, SentinelOne.
- **Forensic tools** – imaging (FTK Imager, Guymager), analysis (EnCase, Autopsy, Magnet AXIOM), memory forensics (Volatility), and network forensics (Wireshark, Zeek).
- **Threat intelligence platforms** – aggregation and analysis of threat data. Examples: MISP, Recorded Future, Mandiant Advantage.
- **Ticketing and case management** – tracking incidents through their lifecycle. Examples: ServiceNow, TheHive, Jira Service Management.
- **Secure communications** – encrypted messaging (Signal), secure email, and out-of-band communication channels in case primary systems are compromised.
- **Incident response 'go bags'** – pre-prepared kits containing: forensic laptops with imaging software, hardware write blockers, external storage, evidence bags, documentation forms, network cables, and portable power supplies.

Network Monitoring and Detection

- **IDS/IPS** – intrusion detection and prevention systems for network-based threat detection (Snort, Suricata).
- **Network traffic analysis** – full packet capture and NetFlow/sFlow analysis for identifying data exfiltration and lateral movement.
- **DNS monitoring** – detecting command-and-control communications and DNS tunnelling.
- **Deception technology** – honeypots and honeynets that detect attackers who have breached the perimeter.

Reading List

- Cichonski, P. et al. (2022) *Computer security incident handling guide. NIST SP 800-61 Rev. 2. Gaithersburg, MD: National Institute of Standards and Technology*.
- Johansen, G. (2022) *Digital forensics and incident response: incident response tools and techniques for effective cyber threat response*. 3rd edn. Birmingham: Packt Publishing.
- Kral, P. (2022) *The incident handler's handbook. Updated edn. Bethesda, MD: SANS Institute.* Available at: https://www.sans.org/white-papers/33901/ (Accessed: 15 March 2026).
- NCSC (2024) *Incident management.* Available at: https://www.ncsc.gov.uk/collection/incident-management (Accessed: 15 March 2026).
- Murdoch, D. (2023) *Blue team handbook: SOC, SIEM, and threat hunting use cases.* 3rd edn. Self-published.
- Anson, S. (2023) *Applied incident response.* 2nd edn. Indianapolis: Wiley.

Summary

In this chapter, you have examined the physical and human resources required to manage a major suspected cyber security incident. You have analysed the nature and business impact of major incidents. You have studied CERT/CSIRT structures at national, sectoral, and organisational levels.

You have evaluated site set-up requirements including incident response facilities, virtual capabilities, and staffing roles. You have assessed organisational command structures using the Gold–Silver–Bronze framework. You have examined the technology and equipment required for effective incident detection, investigation, and response.

Chapter Two – Business Continuity, Disaster Recovery, and Crisis Management

Introduction

This chapter explores the three critical disciplines that support organisational resilience during and after major cyber incidents: Business Continuity Management (BCM), Disaster Recovery (DR), and Crisis Management (CM). You will analyse how each discipline operates independently and how they integrate to provide a comprehensive response to cyber-enabled incidents.

Learning Outcomes

On completing this chapter, you will be able to:

- Apply Business Continuity Management to major incident planning and response.
- Understand how Disaster Recovery and Crisis Management are integrated into a suspected major cyber-enabled incident.

Assessment Criteria

2.1 Assess how Business Continuity Management can be aligned and integrated into a suspected cyber-enabled incident.

2.2 Explain the people, assets and processes required within a Business Continuity Plan.

2.3 Assess how DR and CM strategies and tactics relate to a suspected major cyber-enabled incident.

2.4 Explain the components of good practice in DR and CM plans.

2.1 Business Continuity Management (BCM)

Over to you – Video Watch: Business Continuity Planning

Watch this YouTube video:

Title: Business Continuity Planning

Channel: Professor Messer

Duration: 4:41

Link: https://www.youtube.com/watch?v=B4APySh4JL0

After watching, explain the relationship between Business Impact Analysis, Recovery Time Objective, and Recovery Point Objective. Why are these critical for cyber incident planning?

Defining Business Continuity Management

Business Continuity Management (BCM) is the holistic management process that identifies potential threats to an organisation and the impacts those threats, if realised, might cause to business operations. It provides a framework for building organisational resilience with the capability of an effective response that safeguards the interests of key stakeholders, reputation, brand, and value-creating activities.

The international standard for BCM is ISO 22301:2019 (Security and resilience – Business continuity management systems – Requirements). In the UK, the Business Continuity Institute (BCI) provides professional guidance and certification.

The BCM Lifecycle

- **Business Impact Analysis (BIA)** – the foundational step. Identifies critical business processes, assesses the impact of their disruption over time, and determines recovery priorities. The BIA establishes two critical metrics:
- **Recovery Time Objective (RTO)** – the maximum acceptable time to restore a business process after a disruption. A 4-hour RTO for email means email must be restored within 4 hours.
- **Recovery Point Objective (RPO)** – the maximum acceptable amount of data loss, measured in time. An RPO of 1 hour means data must be recoverable to within 1 hour of the disruption.
- **Maximum Tolerable Period of Disruption (MTPD)** – the absolute maximum time a business process can be unavailable before the organisation suffers irreversible damage.
- **Risk assessment** – identifying threats and vulnerabilities that could cause disruption, assessing their likelihood and impact.
- **Strategy development** – developing continuity strategies for critical processes, including alternative work locations, IT recovery solutions, supply chain alternatives, and communication plans.
- **Plan development** – documenting detailed Business Continuity Plans (BCPs) with activation criteria, roles and responsibilities, procedures, contact lists, and resource requirements.
- **Exercise and testing** – regular testing of plans through tabletop exercises, simulation exercises, and full-scale drills.
- **Maintenance and review** – continuous improvement through regular review, updating, and lessons learned from exercises and real incidents.

The Business Continuity Plan (BCP)

A BCP should include:

- Scope and objectives – which processes and systems are covered.
- Activation criteria and escalation procedures.
- Roles, responsibilities, and contact information for the BCM team.
- Continuity strategies for each critical process (manual workarounds, alternative systems, relocation plans).
- IT recovery procedures (linked to the Disaster Recovery Plan).
- Communication plans (internal staff, customers, suppliers, regulators, media).
- Resource requirements (people, facilities, equipment, third-party services).
- Recovery procedures and return-to-normal processes.

! Need to know

The UK Civil Contingencies Act 2004 places statutory duties on Category 1 responders (including local authorities, emergency services, and NHS bodies) to maintain business continuity plans. While private sector organisations are not directly subject to this Act, the principles it establishes inform best practice across all sectors. The NCSC strongly recommends that all UK organisations maintain business continuity plans that address cyber incidents.

2.2 Disaster Recovery planning and strategies

Defining Disaster Recovery

Disaster Recovery (DR) focuses specifically on the recovery of IT systems, data, and infrastructure following a disruptive event. While BCM addresses the broader business continuity, DR is the technical component that ensures IT services can be restored within the required timeframes (RTO/RPO).

DR Strategies for Cyber Incidents

- **Cold site** – a facility with basic infrastructure (power, networking, space) but no pre-installed IT equipment. Lowest cost but longest recovery time (days to weeks).
- **Warm site** – a facility with pre-installed hardware and network connectivity, but not fully configured or synchronised with live data. Recovery time: hours to days.
- **Hot site** – a fully operational replica of the primary environment with real-time or near-real-time data replication. Enables rapid failover (minutes to hours). Highest cost but lowest RTO.
- **Cloud-based DR (DRaaS)** – Disaster Recovery as a Service using cloud infrastructure (AWS, Azure, GCP). Provides flexible, scalable recovery without maintaining a physical secondary site. Increasingly the preferred approach for organisations of all sizes.

Backup Strategies

- **3-2-1 rule** – maintain 3 copies of data, on 2 different media types, with 1 copy offsite. Modern best practice adds: 1 copy offline or air-gapped (protection against ransomware) and 0 errors (verified through regular restore testing).
- **Immutable backups** – backups that cannot be modified or deleted for a defined retention period. Critical defence against ransomware that attempts to encrypt or destroy backups.
- **Backup testing** – regular restore tests to verify backup integrity. A backup that cannot be restored is worthless. Schedule quarterly restore tests at minimum.

Components of a Disaster Recovery Plan (DRP)

- Scope – which systems, applications, and data are covered, prioritised by BIA results.
- Recovery procedures – step-by-step instructions for recovering each system, including dependencies and sequencing.
- RTO and RPO targets for each system – aligned with the BIA.
- Roles and responsibilities – who leads the DR effort and who is responsible for each system.
- Communication procedures – notification chains, status updates, and escalation.
- Testing schedule – regular DR exercises (tabletop, simulation, full failover).
- Vendor and supplier contacts – including SLAs for third-party services and cloud providers.

💼 Case Study – Ransomware and Disaster Recovery

In May 2021, the Colonial Pipeline company in the US was hit by a DarkSide ransomware attack that shut down the largest fuel pipeline on the US East Coast for six days. The company paid a $4.4 million ransom. Post-incident analysis revealed that

while the company had backups, the recovery process was so slow that paying the ransom was considered faster.

Task: Research this case and analyse: (1) what DR weaknesses were exposed, (2) why backup restoration was too slow, (3) what changes to the DR plan could have avoided the ransom payment, and (4) the broader implications for organisations' DR strategies regarding ransomware. Write approximately 500 words.

2.3 Crisis Management principles and practice

Defining Crisis Management

Crisis Management (CM) is the overall coordination of an organisation's response to a crisis, with the aim of protecting life, minimising damage, and restoring normal operations. While incident management focuses on the technical response and BCM ensures business processes continue, crisis management addresses the strategic, reputational, and stakeholder dimensions.

A crisis differs from an incident in its scale, complexity, and potential for catastrophic consequences. Not every incident becomes a crisis, but every crisis began as an incident that escalated.

The Crisis Management Team (CMT)

The Crisis Management Team operates at the strategic (Gold) level and typically includes:

- Chief Executive Officer or Managing Director (ultimate decision-maker).
- Chief Information Security Officer (CISO) or Chief Technology Officer.
- Chief Communications Officer or Head of PR/Corporate Communications.
- General Counsel or Head of Legal.
- Chief Operations Officer.
- Human Resources Director.
- External advisors (legal, PR, forensic) as required.

Crisis Management Principles

- **Speed of response** – the first hours are critical. Delayed response amplifies damage, erodes stakeholder confidence, and allows the narrative to be controlled by external parties.
- **Transparency and honesty** – attempting to conceal or minimise a breach almost always results in worse outcomes when the truth emerges.
- **Empathy** – acknowledging the impact on affected individuals and demonstrating genuine concern.
- **Accountability** – accepting responsibility and demonstrating concrete remedial actions.
- **Consistent messaging** – all communications must be coordinated through a single source to prevent conflicting messages.
- **Regulatory compliance** – meeting all notification obligations (ICO within 72 hours for personal data breaches, sector regulators, affected individuals where there is a high risk to their rights and freedoms).

Components of a Crisis Management Plan

- Activation criteria – what triggers the crisis management process.
- Crisis Management Team composition, roles, and contact details.
- Decision-making authority and escalation framework.
- Communication strategy – pre-prepared holding statements, media response templates, customer notification templates.
- Stakeholder management – identifying all stakeholders and their communication needs.
- Legal and regulatory checklist – notification obligations, legal privilege considerations.

- Post-crisis review and lessons learned process.

2.4 Integrating BCM, DR, and CM into cyber incident response

BCM, DR, and CM are distinct but interdependent disciplines that must operate in concert during a major cyber incident:

Discipline	Focus	Key Output
Incident Response	Technical detection, containment, eradication, and recovery	Incident resolved; attacker evicted; systems cleaned
Disaster Recovery	IT systems and data restoration	Systems restored to operational state within RTO/RPO
Business Continuity	Maintaining critical business operations	Business continues to operate during and after the incident
Crisis Management	Strategic coordination, stakeholder management, reputation	Stakeholder confidence maintained; regulatory compliance achieved

The integration points are critical:

- The incident response team feeds technical intelligence to the CMT to inform strategic decisions.
- The CMT provides strategic direction and resource authorisation to the technical teams.
- The BCM team activates continuity procedures for affected business processes based on BIA priorities.
- The DR team executes system recovery in alignment with the incident response timeline (systems must be clean before recovery).
- Communications flow in both directions: the CMT needs accurate technical information to communicate externally, while the technical teams need to understand strategic priorities.

Industry Insight – The NCSC's Cyber Incident Response Framework

The UK National Cyber Security Centre provides a comprehensive incident response framework that integrates technical response with business continuity and crisis management. The NCSC recommends that organisations: (1) prepare a cyber incident response plan that aligns with their BCP and DR plans, (2) establish clear escalation criteria, (3) practise their response through regular exercises, and (4) build relationships with the NCSC, law enforcement, and sector peers before incidents occur. The NCSC also offers the Cyber Assessment Framework (CAF) and Exercise in a Box – a free online tool that helps organisations test their response to a range of cyber attack scenarios. Explore: https://www.ncsc.gov.uk/section/exercises

Reading List

- BCI (2023) Good practice guidelines 2023. Reading: Business Continuity Institute.
- Drinkwater, D. and Sherwood, T. (2022) Business continuity management: a practical guide to organisational resilience and ISO 22301. 2nd edn. London: IT Governance Publishing.

- Hiles, A. (2022) *Business continuity management: global best practices*. 5th edn. Brookfield, CT: Rothstein Publishing.
- ISO (2019) ISO 22301:2019 *Security and resilience – Business continuity management systems – Requirements.* Geneva: International Organization for Standardization.
- NCSC (2024) *Incident management collection.* Available at: https://www.ncsc.gov.uk/collection/incident-management (Accessed: 15 March 2026).
- Whitman, M.E. and Mattord, H.J. (2022) *Management of information security*. 7th edn. Boston: Cengage Learning.

Summary

In this chapter, you have explored the three critical disciplines underpinning organisational resilience. You have analysed Business Continuity Management including the BIA, RTO/RPO, and the BCM lifecycle. You have evaluated Disaster Recovery strategies from cold sites to cloud-based DRaaS, backup strategies, and DRP components.

You have studied Crisis Management principles, the role of the Crisis Management Team, and the components of an effective crisis management plan. You have assessed how BCM, DR, and CM integrate with incident response to provide a comprehensive organisational response to major cyber incidents.

Chapter Three – Crisis Communications and Cyber Resilience

Introduction

This chapter evaluates the role of communications in incident management, analyses the isomorphic lessons from major cyber breaches, examines communications failures that have led to catastrophic business outcomes, and develops the principles of cyber resilience and future-proofing.

Learning Outcomes

On completing this chapter, you will be able to:

- Evaluate the potential impact of NOT planning crisis communications and incident response.

Assessment Criteria

4.1 Evaluate the isomorphic lessons from major cyber breaches and company shutdowns.

4.2 Analyse communications approaches and perceived failures in cases of catastrophic business loss related to IT systems failure or attack.

4.3 Justify recommendations that would support a cyber-resilient approach.

3.1 The role of communications in incident management

Why Communications Matter

During a major cyber incident, what an organisation says – and when and how it says it – can determine whether the incident results in a manageable disruption or an existential crisis. Poor communication amplifies reputational damage, erodes customer trust, invites regulatory scrutiny, and can lead to legal liability.

Internal Communications

- **Staff notification** – employees need to know what has happened, what actions they should take (e.g. change passwords, avoid clicking links), and who to contact with concerns. Uninformed staff may inadvertently worsen the situation or share inaccurate information externally.
- **Management briefings** – regular, structured updates to senior management and the board, providing situational awareness without overwhelming them with technical detail.
- **Cross-functional coordination** – ensuring all departments (legal, HR, operations, customer service, PR) receive consistent, timely information and understand their roles in the response.

External Communications

- **Customer notification** – under UK GDPR, individuals must be notified without undue delay if a breach results in a high risk to their rights and freedoms. Notifications must be clear, specific, and include advice on protective measures (e.g. changing passwords, monitoring bank statements).
- **Regulatory notification** – the ICO must be notified within 72 hours of becoming aware of a personal data breach (unless the breach is unlikely to result in a risk to individuals). Sector-specific regulators (FCA, Ofcom, NHS Digital) may have additional requirements.
- **Media management** – proactive media engagement is generally more effective than reactive damage control. Pre-prepared holding statements allow rapid initial response while detailed information is confirmed.
- **Law enforcement liaison** – engaging with Action Fraud (for cybercrime reporting), the National Crime Agency (for serious organised crime), and the NCSC (for technical assistance and national coordination).
- **Supply chain and partner communication** – suppliers and partners may be affected by the incident or may be required to support the response. Timely, honest communication maintains trust and enables collaborative remediation.

Communication Principles During Incidents

- Speed – be first to tell your own story. Delays create a vacuum filled by speculation.
- Accuracy – only communicate what is confirmed. Retracting statements destroys credibility.
- Empathy – acknowledge impact on affected individuals. Lead with concern, not corporate language.
- Consistency – single spokesperson, approved messaging, unified across all channels.
- Regularity – commit to regular updates, even if only to confirm that the investigation is ongoing.

3.2 Isomorphic lessons from major cyber breaches

Isomorphic learning involves drawing lessons from incidents in other organisations or sectors and applying them to your own context. Major cyber breaches provide a rich source of lessons that are transferable across all organisations.

Case Study 1: TalkTalk (2015)

The UK telecommunications company TalkTalk suffered a data breach affecting approximately 157,000 customers, including bank account details. The response was widely criticised:

- The CEO gave media interviews before the full extent of the breach was understood, initially overstating the number of affected customers.
- Customer communications were delayed and unclear.
- The ICO fined TalkTalk £400,000 for failing to implement basic security measures.
- The company lost over 100,000 customers and reported costs of £60 million.

Lesson: Verify facts before public statements. Designate trained spokespeople. Implement basic security controls as a foundation.

Case Study 2: British Airways (2018)

A Magecart attack on the BA website and mobile app compromised the payment card details of approximately 380,000 customers over a two-week period:

- BA's response was relatively swift once the breach was discovered, notifying affected customers within two days.
- However, the ICO initially proposed a £183 million fine (reduced to £20 million) for inadequate security measures, specifically for failing to protect data in transit.

Lesson: Swift notification mitigates but does not eliminate regulatory action. Prevention is always better than response.

Case Study 3: Maersk/NotPetya (2017)

The NotPetya malware attack devastated the world's largest container shipping company, destroying 49,000 laptops, 3,500 servers, and 1,200 applications across 600 sites in 130 countries. Maersk had to reinstall its entire IT infrastructure in 10 days:

- Total cost estimated at $300 million.
- Business continuity was maintained through manual processes and extraordinary staff effort.
- Recovery was aided by a single surviving Active Directory domain controller in Ghana that was offline during the attack due to a power outage.

Lesson: Maintain offline/isolated backups. Test DR procedures. Have manual fallback processes. Geographic diversity of IT infrastructure provides resilience.

Case Study 4: SolarWinds (2020)

A sophisticated supply chain attack compromised SolarWinds' Orion software update mechanism, affecting approximately 18,000 organisations globally including US government agencies and major corporations:

- The attack went undetected for approximately 9 months.
- Detection came from an external security firm (FireEye), not internal monitoring.
- The scale and sophistication of the attack (attributed to Russian state actors) demonstrated the limitations of perimeter-based security.

Lesson: Supply chain security is critical. Zero Trust architecture reduces blast radius. Advanced persistent threats require advanced detection capabilities.

Over to you – Isomorphic Analysis

Choose two major cyber breaches from the past five years (not listed above). For each breach, research and document: (1) what happened, (2) how the organisation responded (technical and communications), (3) the consequences (financial, regulatory, reputational), and (4) the isomorphic lessons that other organisations can apply. Identify at least three common themes across all breaches studied. Present as a 600-word comparative analysis.

3.3 Communications failures and catastrophic business loss

Several high-profile cases demonstrate that poor crisis communications can be more damaging than the underlying incident itself:

Equifax (2017)

The Equifax data breach exposed personal data of 147 million people. The company's communications response was widely regarded as one of the worst in corporate history:

- Notification was delayed by six weeks after discovery.
- The breach notification website was built on a different domain, leading many to believe it was a phishing site.
- The website initially required customers to waive their right to legal action to use the credit monitoring service (later reversed after public outcry).
- Senior executives sold shares before the breach was publicly disclosed.
- The CEO, CIO, and CISO all departed within weeks.
- Total cost estimated at over $1.4 billion.

Key Communications Failures Across Cases

Failure Pattern	Consequence
Delayed notification	Loss of trust; regulatory penalties; speculation fills the information vacuum
Inaccurate initial statements	Credibility destroyed when corrections are needed; fuels media criticism
Lack of empathy	Perceived as prioritising corporate interests over affected individuals
Inconsistent messaging	Confusion among stakeholders; contradictory information undermines trust
Insufficient remedial measures	Perceived as not taking the breach seriously; increases regulatory action
Attempting to conceal or minimise	Massively amplifies reputational damage when truth emerges; potential criminal liability

3.4 Building cyber resilience

Defining Cyber Resilience

Cyber resilience is the ability of an organisation to continuously deliver the intended outcome despite adverse cyber events. It goes beyond cybersecurity (prevention) to encompass the ability to anticipate, withstand, recover from, and adapt to cyber threats. The NCSC defines cyber resilience as the ability to prepare for, respond to, and recover from cyber attacks and security breaches.

The Five Pillars of Cyber Resilience

- **Identify** – understand the organisation's assets, risks, and threat landscape. Conduct regular risk assessments, maintain asset inventories, and perform threat intelligence analysis.
- **Protect** – implement preventive controls: access management, encryption, network segmentation, endpoint protection, security awareness training, and vulnerability management.
- **Detect** – deploy monitoring and detection capabilities: SIEM, EDR, IDS/IPS, threat hunting, and anomaly detection. The mean time to detect (MTTD) a breach remains a critical metric.
- **Respond** – have tested incident response plans, trained response teams, established communication procedures, and relationships with external support (NCSC, law enforcement, forensic providers).
- **Recover** – maintain robust DR and BCM capabilities. Ensure backups are immutable and regularly tested. Plan for full infrastructure rebuild scenarios (as demonstrated by Maersk).

Organisational Culture and Resilience

Cyber resilience is not solely a technical challenge – it requires a cultural transformation:

- Board-level engagement – cybersecurity must be a standing board agenda item with regular reporting on risk posture, incidents, and resilience metrics.
- Security awareness training – all staff must understand their role in preventing and reporting incidents. Regular phishing simulations and training reinforce awareness.
- Just culture – encouraging staff to report security incidents and near-misses without fear of blame. Organisations with a blame culture experience delayed incident reporting and worse outcomes.
- Lessons learned – conducting thorough post-incident reviews and implementing improvements. Sharing lessons (anonymised) across the sector through ISACs and the CiSP platform.

3.5 Future-proofing and disruptive technology considerations

- **AI-powered attacks** – artificial intelligence is enabling more sophisticated phishing, deepfake social engineering, automated vulnerability exploitation, and adaptive malware. Conversely, AI also enhances defensive capabilities through automated threat detection, anomaly identification, and incident triage.
- **Quantum computing threats** – quantum computers could break current public key cryptography. Organisations must begin planning for post-quantum migration (covered in detail in the Cryptography unit).
- **Supply chain complexity** – increasing reliance on cloud services, SaaS applications, and third-party integrations creates expanding attack surfaces. Supply chain risk management must be a core component of resilience planning.
- **IoT and OT convergence** – the integration of operational technology (industrial control systems, building management, medical devices) with IT networks creates new attack vectors and potential for physical consequences.
- **Regulatory evolution** – the UK's evolving regulatory landscape (Data Use and Access Act 2025, NIS Regulations, sector-specific requirements) demands ongoing compliance monitoring and adaptation.
- **Cyber insurance** – the cyber insurance market continues to evolve, with insurers increasingly requiring evidence of cybersecurity maturity (including incident response plans, BCPs, and regular testing) as conditions for coverage.

3.6 Recommending a cyber-resilient approach

Over to you – Cyber Resilience Strategy

Design a comprehensive cyber resilience strategy for the following organisation:

Scenario: A UK-based healthcare trust operating 3 hospitals, 12 community clinics, and employing 8,000 staff. The trust handles highly sensitive patient data (special category under UK GDPR), operates critical medical systems (including networked medical devices), and has experienced a ransomware attack in the past 12 months that forced some services to revert to paper-based processes for 5 days.

Your strategy should address: (1) governance and leadership arrangements, (2) CSIRT structure and capabilities, (3) incident response plan aligned with BCM and DR, (4) crisis communications plan including regulatory notification procedures, (5) specific ransomware resilience measures, (6) staff training and awareness programme, (7) supply chain and third-party risk management, (8) future-proofing considerations (AI, IoT medical devices, cloud), and (9) metrics and KPIs for measuring resilience maturity. Present as a formal strategy document of approximately 2,000 words.

Reading List

- Coombs, W.T. (2022) Ongoing crisis communication: planning, managing, and responding. 6th edn. Thousand Oaks, CA: SAGE Publications.
- Grimes, R.A. (2022) Ransomware protection playbook. Indianapolis: Wiley.
- NCSC (2024) 10 steps to cyber security. Available at: https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security (Accessed: 15 March 2026).
- NHS England (2023) Data security and protection toolkit. Available at: https://www.dsptoolkit.nhs.uk/ (Accessed: 15 March 2026).
- Sanger, D.E. (2021) The perfect weapon: war, sabotage, and fear in the cyber age. Updated edn. New York: Broadway Books.
- Whitman, M.E. and Mattord, H.J. (2022) Management of information security. 7th edn. Boston: Cengage Learning.

Summary

In this chapter, you have evaluated the critical role of communications in incident management, including internal and external communication principles. You have analysed isomorphic lessons from major cyber breaches including TalkTalk, British Airways, Maersk, and SolarWinds, extracting transferable learning.

You have examined communications failures that contributed to catastrophic business outcomes. You have developed the principles of cyber resilience across the five pillars of Identify, Protect, Detect, Respond, and Recover. You have assessed future challenges including AI, quantum computing, and supply chain risk. Finally, you have developed recommendations for a cyber-resilient approach.

Glossary

Word / Term	Explanation
BCM	Business Continuity Management – the holistic process of building organisational resilience.
BCP	Business Continuity Plan – documented procedures for maintaining operations during disruption.
BIA	Business Impact Analysis – identifies critical processes and the impact of their disruption.
CERT	Computer Emergency Response Team – a team that responds to computer security incidents.
CM	Crisis Management – strategic coordination of an organisation's response to a crisis.
CMT	Crisis Management Team – the senior leadership team that manages a crisis.
CSIRT	Computer Security Incident Response Team – synonymous with CERT.
Cyber Resilience	The ability to anticipate, withstand, recover from, and adapt to cyber threats.
DR	Disaster Recovery – the recovery of IT systems and data following a disruptive event.
DRaaS	Disaster Recovery as a Service – cloud-based disaster recovery.
DRP	Disaster Recovery Plan – documented procedures for recovering IT systems.
EDR	Endpoint Detection and Response – security tool for real-time endpoint monitoring and response.
Gold-Silver-Bronze	UK command structure for major incident management (Strategic-Tactical-Operational).
ICO	Information Commissioner's Office – the UK's data protection regulator.
Immutable Backup	A backup that cannot be modified or deleted for a defined retention period.
Incident Commander	The person with overall authority for managing an incident response.
ISAC	Information Sharing and Analysis Centre – a sector-specific body for sharing threat intelligence.
Isomorphic Learning	Drawing lessons from incidents in other organisations and applying them to your own context.
MTPD	Maximum Tolerable Period of Disruption – the longest a process can be unavailable.

NCSC	National Cyber Security Centre – the UK's technical authority for cyber security.
NIS Regulations	Network and Information Systems Regulations – UK regulations for essential services.
RPO	Recovery Point Objective – the maximum acceptable amount of data loss, measured in time.
RTO	Recovery Time Objective – the maximum acceptable time to restore a service.
SIEM	Security Information and Event Management – centralised log collection and analysis platform.
SOC	Security Operations Centre – the facility where security monitoring is conducted.
Tabletop Exercise	A discussion-based exercise where participants walk through a simulated scenario.
War Room	A dedicated facility for coordinating major incident response.

MCQs and True & False Questions (self-assessment)

True or False Questions

1. A CERT and a CSIRT are essentially the same type of team.
2. The Gold command level in UK incident management handles operational tasks.
3. A Business Impact Analysis identifies critical processes and recovery priorities.
4. RPO measures the maximum acceptable downtime after a disruption.
5. ISO 22301 is the international standard for Business Continuity Management.
6. A cold site provides the fastest disaster recovery.
7. Under UK GDPR, personal data breaches must be reported to the ICO within 72 hours.
8. Immutable backups protect against ransomware that targets backup systems.
9. The Crisis Management Team operates at the Bronze (operational) level.
10. Isomorphic learning involves applying lessons from one organisation to another.
11. The NCSC is part of GCHQ.
12. A warm site has pre-installed hardware but is not fully synchronised with live data.
13. EDR stands for Enterprise Data Recovery.
14. The 3-2-1 backup rule recommends 3 copies, 2 media types, 1 offsite.
15. Crisis communications should prioritise speed over accuracy.
16. The TalkTalk breach demonstrated the importance of verifying facts before public statements.
17. DRaaS uses cloud infrastructure for disaster recovery.
18. A SIEM platform provides centralised log collection and correlation.
19. The Maersk NotPetya attack cost an estimated $300 million.
20. Cyber resilience only refers to preventing cyber attacks.

Multiple Choice Questions

1. What does BIA stand for?

A. Business Intelligence Assessment B. Business Impact Analysis C. Breach Investigation Approach D. Business Integration Audit

2. Which command level makes strategic decisions during a major incident?

A. Bronze B. Silver C. Gold D. Platinum

3. What is the maximum time to notify the ICO of a personal data breach under UK GDPR?

A. 24 hours B. 48 hours C. 72 hours D. 7 days

4. Which DR site type provides the fastest recovery?

A. Cold site B. Warm site C. Hot site D. Mobile site

5. The NIST incident response lifecycle includes which phases?

A. Plan, Do, Check, Act B. Preparation, Detection, Containment, Post-Incident C. Identify, Protect, Detect, Respond D. Assess, Mitigate, Monitor, Report

6. What is RPO?

A. Recovery Process Objective B. Recovery Point Objective C. Risk Protection Order D. Response Planning Output

7. Which organisation provides the UK's national CERT function?

A. ICO B. NCSC C. NCA D. BCI

8. What is the purpose of a tabletop exercise?

A. Physical security testing B. Discussion-based scenario walkthrough C. Penetration testing D. Backup verification

9. Which company's entire IT infrastructure was destroyed by the NotPetya attack?

A. Equifax B. TalkTalk C. Maersk D. SolarWinds

10. ISO 22301 covers which discipline?

A. Information security management B. Business continuity management C. Quality management D. Digital forensics

11. What does SIEM stand for?

A. Security Incident and Event Monitoring B. Security Information and Event Management C. System Integration and Enterprise Management D. Strategic Incident Escalation Model

12. Which backup strategy protects against ransomware encrypting backups?

A. Full backup B. Incremental backup C. Immutable backup D. Logical backup

13. What was a key communications failure in the TalkTalk breach?

A. No breach occurred B. CEO made public statements before facts were verified C. ICO was never notified D. No customers were affected

14. MTPD stands for:

A. Maximum Time for Process Delivery B. Maximum Tolerable Period of Disruption C. Minimum Technical Protection Duration D. Managed Threat Prevention Dashboard

15. Which is the first principle of crisis communication?

A. Minimise information B. Delay until all facts are known C. Speed of response D. Only communicate good news

16. DRaaS stands for:

A. Data Recovery as a Standard B. Disaster Recovery as a Service C. Distributed Response and Security D. Digital Risk Assessment System

17. The SolarWinds attack was primarily a:

A. Ransomware attack B. DDoS attack C. Supply chain attack D. Insider threat

18. Under the Gold-Silver-Bronze model, who coordinates tactical response?

A. Gold B. Silver C. Bronze D. All levels equally

19. Which tool type provides real-time endpoint monitoring and response?

A. SIEM B. EDR C. Firewall D. IDS

20. Cyber resilience includes which capability that goes beyond prevention?

A. Only detection B. Only encryption C. Ability to recover and adapt D. Only access control

Answers to True/False Questions

1. True. CERT and CSIRT are essentially the same concept – teams dedicated to incident response.

2. False. Gold handles strategic decisions; Bronze handles operational tasks.

3. True. A BIA identifies critical processes, assesses disruption impact, and establishes recovery priorities (RTO, RPO).

4. False. RPO measures maximum acceptable data loss (in time). RTO measures maximum acceptable downtime.

5. True. ISO 22301:2019 is the international standard for Business Continuity Management Systems.

6. False. A cold site has the slowest recovery time. A hot site provides the fastest recovery.

7. True. UK GDPR requires notification to the ICO within 72 hours of becoming aware of a qualifying breach.

8. True. Immutable backups cannot be modified or deleted, protecting them from ransomware.

9. False. The CMT operates at the Gold (strategic) level, not Bronze.

10. True. Isomorphic learning applies lessons from other organisations to one's own context.

11. True. The NCSC is part of GCHQ and provides the UK's national CERT function.

12. True. A warm site has hardware installed but is not fully configured or synchronised with live data.

13. False. EDR stands for Endpoint Detection and Response, not Enterprise Data Recovery.

14. True. The 3-2-1 rule recommends 3 copies, on 2 different media types, with 1 copy offsite.

15. False. Both speed and accuracy are essential; communications should be rapid but only include confirmed information.

16. True. The TalkTalk CEO made public statements before the full extent of the breach was understood.

17. True. DRaaS uses cloud infrastructure to provide disaster recovery capabilities.

18. True. SIEM provides centralised log collection, correlation, and alerting.

19. True. Maersk estimated the total cost of the NotPetya attack at approximately $300 million.

20. False. Cyber resilience encompasses prevention, detection, response, recovery, and adaptation.

Answers to Multiple Choice Questions

1. (B) Business Impact Analysis

2. (C) Gold

3. (C) 72 hours

4. (C) Hot site

5. (B) Preparation, Detection, Containment, Post-Incident

6. (B) Recovery Point Objective
7. (B) NCSC
8. (B) Discussion-based scenario walkthrough
9. (C) Maersk
10. (B) Business continuity management
11. (B) Security Information and Event Management
12. (C) Immutable backup
13. (B) CEO made public statements before facts were verified
14. (B) Maximum Tolerable Period of Disruption
15. (C) Speed of response
16. (B) Disaster Recovery as a Service
17. (C) Supply chain attack
18. (B) Silver
19. (B) EDR
20. (C) Ability to recover and adapt