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 4 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 4 Units

The Level 4 Diploma in Cyber Security consists of the following units:

Unit Title	Credits	Status
Cyber Security Threat and Risk	20	Mandatory
Network Security and Data Communications	20	Mandatory
Database Security and Computer Programming	20	Mandatory
Incident Response, Investigations and Forensics	20	Mandatory
Security Strategy: Laws, Policies and Implementation	20	Mandatory
Cyber Security Threats and Risk: Banking and Finance	20	Optional
Cyber Wars	20	Optional

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 leading organisations.
🧭	**'Did you know?'** highlights interesting facts or surprising information to deepen your understanding.
💼	**'Case studies:'** realistic business scenarios to reinforce and test your understanding.
❗	**'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 4 Incident Response, Investigations and Forensics

About this unit

In this unit you will examine Incident Response, Computer Emergency Response Teams (CERTs), and events requiring investigative techniques. You will identify and examine aligned business tasks and task forces including Disaster Recovery, Business Continuity Management and Crisis Management.

Incident Response is the organised approach to addressing and managing the aftermath of a security breach or cyber attack. The goal of incident response is to handle the situation in a way that limits damage, reduces recovery time and costs, and prevents future occurrences. Every organisation that depends on IT systems – which in the modern world means virtually every organisation – needs a robust incident response capability.

The unit then focuses on exploring cyber-related incident investigations, including evidential analysis gathering, logging and reporting. You will examine the principles of forensic science as they apply to digital evidence, and learn about the legal and ethical frameworks that govern how investigations are conducted. You will have the opportunity to study case studies and assess how the approaches used could be applied in your own workplace.

By the end of this unit, you will be able to explain the people, structures, processes and tools involved in incident response; discuss CERT roles; analyse BC, DR and CM standards; explain investigation processes; analyse evidence handling; and examine the legal framework governing computer investigations.

Unit code: **T/617/1132**

RQF level: **4**

Credits: **20**

Assessment: **Written Assignment – Incident Response Plan and Investigation Report**

Chapter One – Incident Response and Computer Emergency Response Teams

Introduction

This chapter provides a comprehensive examination of incident response as a business function and the role of Computer Emergency Response Teams (CERTs) within organisations. Incident response is not simply a technical activity – it is a business-critical function that involves coordination between technical teams, management, legal counsel, communications, and external stakeholders. The speed and effectiveness of an organisation's response to a cyber security incident can mean the difference between a minor disruption and a catastrophic business failure.

You will explore the full lifecycle of incident response, from preparation and detection through to recovery and lessons learned. You will also examine the different roles within a CERT, how these teams are structured, and why their composition and operation are critical to organisational resilience. This chapter emphasises both the human and technical dimensions of incident response, recognising that even the best technology is only as effective as the people who operate it.

Learning Outcomes

On completing the chapter, you will be able to:

1. **Understand the role and composite parts of Incident Response as a business function and how CERTs operate.**

Assessment Criteria

1.1 Explain the people, structures, processes and tools involved in Computer Incident Responses.

1.2 Discuss the different roles within a Computer Emergency Response Team and their importance.

1.1 People, structures, processes and tools in incident response

Over to you – Video Watch: What is Incident Response?

Watch these two YouTube videos:

Video 1 Title: Incident Response Process – CompTIA Security+ – Professor Messer

Link: https://youtu.be/X2UiMLxRdhE?si=59VMWOf7a3trzy-5

Video 2 Title: What Is Incident Response? – IBM Technology

Link: https://youtu.be/XyOvdhjrEX4?si=RW73QlHkHg9HDohN

After watching both videos, compare the two explanations. What are the key phases of incident response? Why is preparation considered the most important phase? Write a 300-word comparison.

What is a Computer Security Incident?

Before examining incident response processes, it is important to understand what constitutes a 'computer security incident'. NIST Special Publication 800-61 defines a computer security incident as 'a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.' This broad definition encompasses a wide range of events, from unauthorised access attempts and malware infections to data breaches, denial of service attacks, and insider misuse.

Not every security event is an incident. An event is any observable occurrence in a system or network – a user logging in, a firewall blocking a connection, or a server generating an error message. An incident is an event (or series of events) that actually or potentially compromises the confidentiality, integrity, or availability of an information system. The process of distinguishing between events and incidents – known as triage – is one of the most critical skills in incident response.

Incidents can be categorised by severity to ensure appropriate resource allocation and escalation. A common classification scheme uses four levels: Critical (active breach with significant data loss or system compromise requiring immediate executive involvement), High (confirmed security incident requiring urgent response), Medium (suspected incident requiring investigation within a defined timeframe), and Low (anomalous activity requiring monitoring and assessment).

The Incident Response Lifecycle

The NIST Incident Response Lifecycle, described in SP 800-61, provides the most widely adopted framework for incident response. It consists of four phases that form a continuous cycle:

! Need to know – The Four Phases of Incident Response (NIST SP 800-61)

Phase 1: Preparation – Establishing the incident response capability before incidents occur. This includes creating policies and procedures, forming the incident response team, acquiring tools, conducting training and exercises, and establishing communication channels. Preparation is widely considered the most important phase.

Phase 2: Detection and Analysis – Identifying potential incidents through monitoring, alerts, and reports, then analysing them to determine their scope, impact, and root cause. This phase requires strong analytical skills and access to comprehensive logging and monitoring data.

Phase 3: Containment, Eradication, and Recovery – Containing the incident to prevent further damage, removing the threat from the environment, and restoring affected systems to normal operation. Short-term containment provides immediate protection; long-term containment enables forensic analysis.

Phase 4: Post-Incident Activity – Conducting a thorough review (lessons learned) to identify what happened, assess the effectiveness of the response, and implement improvements. This phase feeds back into Phase 1, creating a continuous improvement cycle.

Phase 1: Preparation – Building the Foundation

Preparation is the foundation upon which all other incident response activities depend. An organisation that has invested in thorough preparation will respond more quickly, more effectively, and with less damage than one that has not. Key preparation activities include:

- **Incident Response Plan (IRP)** – a documented, approved plan that defines the organisation's approach to handling incidents. The IRP should include: the plan's purpose and scope; definitions and severity classifications; roles and responsibilities; escalation procedures; communication templates (internal and external); contact lists for key personnel, vendors, and authorities; procedures for each phase of the lifecycle; and review and update schedules.
- **Incident Response Team** – assembling a team with the right mix of technical, managerial, and communication skills. The team structure, roles, and responsibilities are covered in detail in section 1.2.
- **Tools and technology** – deploying the monitoring, detection, analysis, and response tools that the team will need. This includes SIEM systems, EDR (Endpoint Detection and Response) tools, network forensics tools, malware analysis sandboxes, ticketing systems for tracking incidents, and secure communication channels for the team.
- **Training and awareness** – ensuring that all members of the incident response team are trained in their roles and that the wider organisation understands how to report suspected incidents. Regular training ensures skills remain current and team members are familiar with the latest threats and techniques.
- **Exercises and simulations** – conducting tabletop exercises (discussion-based walkthroughs of hypothetical scenarios), functional exercises (testing specific components of the IRP), and full-scale simulations (realistic drills that test the entire response capability). Exercises reveal gaps and weaknesses in the plan before a real incident exposes them.
- **Legal and regulatory preparation** – establishing relationships with legal counsel, law enforcement, and regulatory bodies before incidents occur. Understanding reporting obligations (e.g. 72-hour GDPR breach notification) and preserving the option to pursue legal action requires advance preparation.

Industry Insight – The Cost of Poor Preparation

Research by the Ponemon Institute consistently shows that organisations with a tested incident response plan and a dedicated incident response team experience significantly lower breach costs. The 2023 IBM Cost of a Data Breach Report found that organisations with high levels of incident response planning and testing saved an average of $1.49 million per breach compared to those with low levels. Additionally, the average time to identify and contain a breach was 54 days shorter for organisations with mature incident response capabilities.

Read more: https://www.ibm.com/security/data-breach

Over to you – Tabletop Exercise Design

Design a 30-minute tabletop exercise scenario for a medium-sized accounting firm. The scenario should involve a ransomware attack that encrypts the firm's client financial data two weeks before the tax deadline. Include: (a) the scenario narrative (what happened, when, and how it was discovered), (b) five discussion questions for the exercise participants, (c) expected actions at each phase of the NIST lifecycle, and (d) inject cards – new information revealed during the exercise to test adaptability (e.g. 'The attackers have now posted a sample of client data online'). Present your exercise in a professional format suitable for distribution to participants.

Phase 2: Detection and Analysis – Finding and Understanding the Threat

Detection is the process of identifying that a security incident may be occurring. Analysis is the process of determining the scope, impact, and root cause of the incident. Together, these activities are among the most technically demanding aspects of incident response.

Incidents can be detected through multiple channels:

- **Automated detection** – SIEM alerts, IDS/IPS alerts, EDR detections, antivirus alerts, anomaly detection systems, and automated threat intelligence feeds. The challenge with automated detection is managing the volume of alerts and minimising false positives.
- **Manual detection** – security analyst observations during threat hunting, log review, or network monitoring. Skilled analysts can identify subtle indicators of compromise (IOCs) that automated systems may miss.
- **User reports** – employees, customers, or partners reporting suspicious activity such as phishing emails, unusual system behaviour, or unauthorised access. User reporting is a critical detection channel and depends on effective security awareness training.
- **External notification** – law enforcement agencies, threat intelligence providers, security researchers, or affected third parties informing the organisation of a breach. In many cases, external notification is the first indication of a compromise – this highlights the importance of reducing dwell time through proactive monitoring.
- **Threat intelligence** – proactive use of threat intelligence feeds and dark web monitoring to identify threats before they materialise. Threat intelligence can provide early warning of targeted attacks, leaked credentials, or emerging vulnerabilities.

Once a potential incident is detected, analysis involves several key activities: initial triage (determining whether the event is a genuine incident and its severity), scope assessment (identifying which systems, networks, and data are affected), impact assessment (evaluating the potential business impact), root cause analysis (determining how the incident occurred and what vulnerabilities were exploited), and attribution (where possible, identifying the threat actor responsible).

Did you know?

The MITRE ATT&CK framework is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations. It provides a common language for describing attack behaviours and is widely used by incident response teams to identify what stage of an attack they are observing, predict the attacker's next moves, and develop appropriate response strategies. The framework covers 14 tactics (from Reconnaissance to Impact) and hundreds of specific techniques. Security analysts use ATT&CK to map observed activity to known adversary behaviours.

Read more: https://attack.mitre.org/

Example – Indicators of Compromise (IOCs)

IOCs are pieces of forensic data that identify potentially malicious activity. Common types include:

Network-based IOCs: Unusual outbound traffic to unknown IP addresses, DNS queries to known malicious domains, unexpected data transfers during off-hours, connections to known command-and-control (C2) servers.

Host-based IOCs: Unexpected processes running on systems, modified system files or registry entries, unusual scheduled tasks or cron jobs, new or modified user accounts, anti-forensic tools present on the system.

Application-based IOCs: Failed login attempts exceeding normal thresholds, database queries returning unusually large result sets, web application errors consistent with injection attempts, unusual API calls or access patterns.

Phase 3: Containment, Eradication, and Recovery

Once an incident has been confirmed and analysed, the response moves to containment, eradication, and recovery. These three activities often overlap and are closely coordinated.

Containment strategies must balance the need to stop the incident from spreading with the need to preserve evidence for investigation. Two types of containment are typically employed:

- **Short-term containment** – immediate actions to stop the incident from causing further damage. This might include isolating affected systems from the network, blocking malicious IP addresses or domains at the firewall, disabling compromised user accounts, or shutting down affected services. Short-term containment should be implemented as quickly as possible.
- **Long-term containment** – more sustainable measures that allow the organisation to continue operating while the incident is fully investigated and remediated. This might include rebuilding affected systems on clean media, implementing additional monitoring, applying emergency patches, or deploying temporary security controls.

Eradication involves completely removing the threat from the environment. This includes removing malware from all affected systems, closing the vulnerability that was exploited, resetting compromised credentials, and verifying that no backdoors or persistence mechanisms remain. Eradication must be thorough – if any element of the threat remains, the incident will recur.

Recovery involves restoring affected systems to normal operation, confirming that they are functioning correctly, and monitoring them closely for any signs of recurring compromise. Recovery activities include restoring systems from clean backups, rebuilding compromised servers, re-enabling disabled services, and gradually returning to normal operations while maintaining heightened monitoring.

Case Study – The Norsk Hydro Ransomware Attack (2019)

In March 2019, Norwegian aluminium producer Norsk Hydro was hit by the LockerGoga ransomware, affecting operations across 40 countries. The company's response was widely praised: they immediately isolated affected systems, switched to manual operations where possible, communicated transparently with employees, customers, and the public through regular press conferences, and refused to pay the ransom. The company estimated the total cost at $71 million.

Norsk Hydro's Chief Financial Officer described the incident response as 'a testament to the resilience and dedication of our employees.' The company's transparency during the

incident – including live-streaming press conferences and providing detailed technical updates – was cited as a model for crisis communication.

Task: (1) Using the NIST lifecycle, map Norsk Hydro's response to each phase. (2) Evaluate the decision not to pay the ransom – what are the arguments for and against? (3) Analyse the role of crisis communication in Norsk Hydro's response. (4) What lessons can other organisations learn from this incident? (5) Calculate the per-day cost of the incident over the recovery period. Write a comprehensive 700-word analysis.

Phase 4: Post-Incident Activity – Learning and Improving

The post-incident phase is often neglected but is essential for improving the organisation's security posture and incident response capability. Key activities include:

- **Lessons learned meeting** – a structured review session held shortly after the incident is resolved, involving all key participants. The meeting should address: what happened and when, how the incident was detected, how effective the response was, what worked well and what did not, what could be improved, and what specific actions will be taken to prevent recurrence.
- **Incident report** – a formal document that records all details of the incident, the response, and the outcomes. The report should be factual, thorough, and suitable for sharing with management, legal counsel, and regulatory authorities as required.
- **Evidence retention** – determining how long incident evidence should be retained, considering potential legal proceedings, regulatory requirements, and organisational policies. Evidence should be stored securely and in accordance with any applicable chain of custody requirements.
- **Security improvements** – implementing specific changes based on the lessons learned. This might include updating the incident response plan, deploying new security controls, revising security policies, providing additional training, or modifying network architecture.
- **Metrics and reporting** – tracking key metrics such as time to detect, time to contain, time to recover, number of incidents by category, and trend analysis over time. These metrics provide management with visibility into the organisation's incident response performance and help justify security investments.

Over to you – Incident Metrics Dashboard Design

Design a monthly incident response metrics dashboard for a CISO (Chief Information Security Officer). Include at least eight key metrics that would provide meaningful insight into the organisation's incident response capability. For each metric, specify: the metric name, how it is calculated, what 'good' looks like, and why it matters. Sketch the dashboard layout showing how the metrics would be visually presented. Consider using categories such as: detection effectiveness, response efficiency, impact metrics, and trend indicators.

Reporting and Recording Incident Response Activity

Accurate, timely reporting and recording of incident response activity is essential for several reasons: it supports the investigation and prosecution of cyber crimes; it demonstrates compliance with regulatory obligations (such as GDPR's 72-hour breach notification

requirement); it provides the basis for lessons learned analysis; it enables trend analysis and risk assessment; and it protects the organisation's legal position.

Key reporting and recording practices include:

- **Incident logging** – recording all actions taken during an incident in a chronological timeline. Each entry should include: date and time (using UTC for consistency), the person taking the action, the action taken, the reason for the action, and the outcome. Logs should be contemporaneous (recorded at the time, not retrospectively) and tamper-proof.
- **Internal reporting** – escalating incidents to appropriate management levels based on severity. Critical incidents should be reported to the CISO, CEO, and board as appropriate. Regular status updates should be provided throughout the incident.
- **External reporting** – notifying relevant external parties as required. This includes: the Information Commissioner's Office (ICO) for personal data breaches under GDPR (within 72 hours); law enforcement (National Crime Agency, Action Fraud) for criminal activity; sector regulators (FCA, PRA for financial services; NHS Digital for healthcare); affected individuals (if the breach poses a high risk to their rights and freedoms); and insurers (as required by the cyber insurance policy).
- **Stakeholder communication** – keeping customers, partners, employees, media, and other stakeholders informed as appropriate. Communication should be honest, timely, and coordinated through a single spokesperson to avoid conflicting messages.

1.2 Roles within a Computer Emergency Response Team and their importance

A Computer Emergency Response Team (CERT) – also known as a Computer Security Incident Response Team (CSIRT) or Security Operations Centre (SOC) – is a group of professionals responsible for detecting, analysing, and responding to computer security incidents. The effectiveness of a CERT depends on having the right people in the right roles with the right skills, tools, and authority.

CERT Organisational Models

CERTs can be structured in several ways, depending on the organisation's size, resources, and risk profile:

- **Dedicated CERT** – a full-time, permanent team whose sole function is incident response. Common in large organisations, financial institutions, and government agencies. Provides the fastest response times and deepest expertise.
- **Distributed CERT** – team members have incident response as part of their broader IT or security responsibilities. They come together when an incident occurs. Common in medium-sized organisations. Less expensive but potentially slower to respond.
- **Hybrid CERT** – a small dedicated core team supplemented by subject matter experts drawn from across the organisation as needed. Provides a balance between cost and capability.
- **Outsourced CERT** – incident response is provided by an external managed security service provider (MSSP) or incident response retainer firm. Useful for small organisations that lack the resources for an internal team, but requires clear service level agreements and pre-established access arrangements.

- **National/sector CERTs** – government-operated CERTs that provide incident response support and threat intelligence for a country or sector. In the UK, the National Cyber Security Centre (NCSC) operates the national CERT function and provides guidance and support to organisations across all sectors.

Key Roles Within a CERT

Role	Responsibilities and Skills
Incident Manager / Coordinator	Overall responsibility for managing the incident response process. Coordinates between technical teams, management, legal, and communications. Makes escalation decisions. Requires strong leadership, communication, and decision-making skills under pressure.
Tier 1 Analyst (Triage)	First responder who monitors alerts, performs initial triage, and classifies incidents. Determines whether an alert is a true positive or false positive. Escalates confirmed incidents to Tier 2. Requires attention to detail and knowledge of monitoring tools (SIEM, IDS).
Tier 2 Analyst (Investigation)	Conducts deeper investigation of confirmed incidents. Performs log analysis, correlates data from multiple sources, and determines the scope and impact of the incident. Requires advanced analytical skills and knowledge of attacker techniques.
Tier 3 Analyst (Threat Hunter)	Proactively searches for hidden threats that have evaded automated detection. Conducts advanced analysis, reverse engineering, and malware analysis. Develops custom detection rules and contributes to threat intelligence. Requires expert-level skills.
Forensic Analyst	Collects, preserves, and analyses digital evidence in accordance with legal and procedural requirements. Creates forensic images, examines file systems, recovers deleted data, and produces reports suitable for legal proceedings. Requires specialist forensic training.
Malware Analyst	Analyses malicious software to determine its capabilities, communication methods, persistence mechanisms, and indicators of compromise. Uses static analysis (examining code without execution) and dynamic analysis (executing malware in a sandbox). Requires reverse engineering skills.
Communications Lead	Manages all internal and external communications during an incident. Drafts press statements, customer notifications, and internal updates. Coordinates with the legal team and senior management. Requires excellent written and verbal communication skills and media training.
Legal Advisor	Advises on legal obligations (data breach notification, evidence preservation), regulatory requirements, and potential liability. Guides the team on what can and cannot be shared with external parties. Ensures the investigation is conducted in a legally defensible manner.

Subject Matter Experts (SMEs)	Specialists from across the organisation (network engineering, database administration, application development, business operations) who provide domain-specific knowledge during an incident. SMEs help the team understand the affected systems and their business context.

Industry Insight – The NCSC and UK CERT

The UK's National Cyber Security Centre (NCSC), part of GCHQ, provides the UK's national CERT function. The NCSC responds to nationally significant incidents, provides threat intelligence and guidance to organisations of all sizes, and runs the Cyber Essentials certification scheme. The NCSC also operates the Active Cyber Defence programme, which provides free tools and services to protect UK organisations from common cyber attacks. For critical incidents, the NCSC can deploy specialist teams to assist affected organisations on-site.

Read more: https://www.ncsc.gov.uk/

Over to you – CERT Staffing Plan Activity

You have been asked to design a CERT for a retail bank with 5,000 employees across 50 branches. The bank processes online banking transactions 24/7 and holds sensitive customer financial data. Design a CERT staffing plan that includes: (a) the organisational model you would recommend (dedicated, distributed, hybrid, or outsourced) with justification, (b) the specific roles you would include, (c) the number of staff for each role, (d) the shift pattern for 24/7 coverage, (e) the key skills and qualifications required for each role, and (f) the estimated annual budget. Present your plan in a professional format suitable for the bank's board of directors.

Over to you – Video Watch: Inside a SOC

Title: Day in the Life of a SOC Analyst

Link: https://youtu.be/r6uGbvUdyVw?si=m67QjuEsi--JBcnq

After watching, reflect on: What surprised you about the daily work of a SOC analyst? What skills would you need to develop to work in this role? How does the SOC analyst's work relate to the NIST incident response lifecycle?

Reading List

- Cichonski, P., Millar, T., Grance, T. and Scarfone, K. (2022) *NIST SP 800-61 Rev. 3: Computer Security Incident Handling Guide.* Gaithersburg, MD: NIST. Available at: https://csrc.nist.gov/publications/detail/sp/800-61/rev-3/final (Accessed: 15 March 2026).
- Anson, S. (2023) *Applied Incident Response.* 2nd edn. Indianapolis, IN: Wiley.
- Johansen, G. (2022) *Digital Forensics and Incident Response.* 3rd edn. Birmingham: Packt Publishing.
- Murdoch, D. (2022) *Blue Team Handbook: SOC, SIEM, and Threat Hunting.* 3rd edn. Independently published.

- NCSC (2024) *Incident Management.* London: National Cyber Security Centre. Available at: https://www.ncsc.gov.uk/collection/incident-management (Accessed: 15 March 2026).
- Sanders, C. and Smith, J. (2023) *Applied Network Security Monitoring.* 2nd edn. Waltham, MA: Syngress.

Summary

In this chapter, you have examined the full lifecycle of incident response, from preparation through detection and analysis, containment, eradication, and recovery, to post-incident activity. You have explored the different organisational models for CERTs, the key roles within a response team, and the importance of accurate reporting and recording. You have also examined how industry frameworks such as NIST SP 800-61 and MITRE ATT&CK support effective incident response, and have applied these concepts through case studies and practical exercises.

Chapter Two – Business Continuity, Disaster Recovery and Crisis Management

Introduction

This chapter examines the three closely related disciplines that support organisational resilience: Business Continuity Management (BCM), Disaster Recovery (DR), and Crisis Management (CM). While incident response focuses on detecting and handling specific security events, these disciplines address the broader challenge of ensuring that the organisation can continue to function during and after disruptive events of any kind – not just cyber incidents, but also natural disasters, infrastructure failures, pandemics, and other crises.

Understanding the relationships and distinctions between BC, DR, and CM is essential for cyber security professionals because cyber incidents frequently escalate into business continuity events that require coordinated response across multiple organisational functions. A ransomware attack, for example, may begin as a technical security incident but quickly become a business continuity crisis requiring disaster recovery procedures and executive-level crisis management.

Learning Outcomes

On completing the chapter, you will be able to:

1. **Understand aligned task/task forces for Business Continuity, Disaster Recovery and Crisis Management.**

Assessment Criteria

2.1 Explain the terms BC, DR and CM.

2.2 Analyse the standards, protocols and concepts underpinning BC, DR and CM and their application within organisations.

2.1 Defining Business Continuity, Disaster Recovery and Crisis Management

! Need to know – BC, DR and CM Defined

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

Disaster Recovery (DR) is the subset of business continuity that specifically focuses on restoring IT systems, applications, and data after a disruptive event. DR plans define the technical procedures for recovering technology infrastructure and are typically more technically detailed than BC plans.

Crisis Management (CM) is the process of managing an organisation's response to a major, unpredictable event that threatens to harm the organisation, its stakeholders, or the general public. Crisis management focuses on strategic decision-making, leadership, and communication at the executive level during high-impact events.

The relationship between these three disciplines can be understood as concentric circles. Crisis Management provides the overarching strategic leadership during a major event. Business Continuity Management ensures that critical business functions continue to operate. Disaster Recovery provides the technical mechanisms for restoring IT systems and data. All three work together to ensure organisational survival and recovery.

Business Continuity Management in Detail

BCM is a continuous process, not a one-off activity. The BCM lifecycle typically includes the following stages:

- **Programme management** – establishing governance, policies, and resources for BCM. This includes appointing a BC manager or team, defining the scope of the programme, securing senior management commitment, and allocating budget.
- **Business Impact Analysis (BIA)** – identifying the organisation's critical business functions and determining the impact of their disruption over time. The BIA establishes key metrics including Recovery Time Objective (RTO) – the maximum acceptable time to restore a function; Recovery Point Objective (RPO) – the maximum acceptable data loss measured in time; Maximum Tolerable Period of Disruption (MTPD) – the absolute maximum time a function can be unavailable before the organisation faces unacceptable consequences; and Minimum Business Continuity Objective (MBCO) – the minimum level of service that must be maintained during a disruption.
- **Risk assessment** – identifying and evaluating the threats and vulnerabilities that could cause disruption to critical business functions. This assessment considers both the likelihood and impact of potential disruptions, including cyber attacks, natural disasters, infrastructure failures, and supply chain disruptions.
- **Strategy development** – selecting and implementing strategies to maintain critical business functions during and after a disruption. Strategies may include alternative work locations, manual workarounds, reciprocal arrangements with partner organisations, outsourcing critical functions, and maintaining spare capacity.
- **Plan development** – documenting the specific procedures, roles, and resources required to implement the continuity strategies. BC plans should be practical, accessible, and usable under stressful conditions.
- **Testing and exercising** – regularly testing BC plans through tabletop exercises, simulation drills, and full-scale tests. Testing validates that plans work in practice and identifies areas for improvement. Industry best practice recommends testing BC plans at least annually.
- **Maintenance and review** – continuously reviewing and updating BC plans to reflect changes in the organisation, its risk profile, and its operating environment. Plans should be reviewed after every significant change and after every exercise or real invocation.

Over to you – Video Watch: Business Continuity Planning

Title: Business Continuity Planning

Link: **https://youtu.be/G9JANBmTdqA?si=byxFWYLljZuTx_hK**

After watching, explain in your own words: What is the difference between a BIA and a risk assessment? Why are both necessary? How does the BIA inform the recovery strategy?

Disaster Recovery in Detail

Disaster Recovery focuses specifically on the technical aspects of restoring IT systems after a disruptive event. A comprehensive DR plan addresses:

- **Data backup and restoration** – implementing robust backup strategies (such as the 3-2-1 rule and the GFS rotation scheme covered in the Database Security unit). Backups must be regularly tested to confirm successful restoration. The backup strategy must align with RPO requirements – if the RPO is 1 hour, backups must be taken at least hourly.
- **DR site strategies** – maintaining alternative IT infrastructure that can be activated during a disaster. Options range from cold sites (empty facilities with power and networking but no pre-installed equipment), through warm sites (facilities with pre-installed hardware but not fully configured), to hot sites (fully operational duplicate facilities that can take over immediately). Cloud-based DR (Disaster Recovery as a Service / DRaaS) has become increasingly popular as it eliminates the need for physical secondary sites.
- **Failover and failback procedures** – documented procedures for switching operations from the primary site to the DR site (failover) and returning to the primary site once it is restored (failback). These procedures must be tested regularly to ensure they work correctly under pressure.
- **Communication during DR events** – ensuring that all stakeholders are informed of the disruption, the expected recovery timeline, and any actions they need to take. Communication channels must be independent of the affected IT systems (e.g. mobile phones, personal email, physical notice boards).

Example – RTO and RPO in Practice

An online banking system has an RTO of 15 minutes and an RPO of 0 (zero data loss). This means the system must be restored within 15 minutes of a disruption, and no transaction data can be lost. To achieve this, the bank implements: synchronous database replication to a hot standby site, automated failover mechanisms, and continuous transaction logging. The DR infrastructure costs millions of pounds annually, but the cost of extended downtime or data loss for an online banking system would be far greater.

A marketing department's content management system has an RTO of 48 hours and an RPO of 24 hours. Daily backups and a warm site arrangement are sufficient. The lower RTO/RPO reflects the lower business impact of this system's disruption.

Crisis Management in Detail

Crisis Management operates at the strategic and executive level during major events. While BC and DR focus on maintaining operations and restoring systems, crisis management focuses on protecting the organisation's reputation, making high-stakes decisions under pressure, and coordinating the overall organisational response. Key elements of crisis management include:

- **Crisis Management Team (CMT)** – a senior leadership team, typically including the CEO, CFO, General Counsel, Head of Communications, CIO/CISO, and HR Director.

The CMT makes strategic decisions about the organisation's response, authorises expenditure, and sets the tone for external communications.

- **Crisis communication** – managing information flow to internal and external stakeholders during a crisis. Effective crisis communication is honest, timely, empathetic, and consistent. The organisation should designate a single spokesperson to avoid conflicting messages. Social media monitoring and response should be included in the communication plan.
- **Decision-making frameworks** – pre-established protocols for making rapid decisions under uncertainty. In a crisis, there is rarely perfect information, and decisions must be made quickly. Decision-making frameworks help leaders structure their thinking and avoid cognitive biases.
- **Psychological support** – providing support to employees who may be affected by the crisis, including those directly involved in the response (who may experience stress and burnout) and the wider workforce (who may feel anxious about job security or organisational stability).

2.2 Standards, protocols and concepts underpinning BC, DR and CM

International Standards

Several international standards provide frameworks for BC, DR, and CM:

- **ISO 22301:2019 (Business Continuity Management Systems)** – the primary international standard for BCM. It specifies requirements for planning, establishing, implementing, operating, monitoring, reviewing, maintaining, and continually improving a documented management system to protect against, reduce the likelihood of, prepare for, respond to, and recover from disruptive incidents. ISO 22301 is certifiable, meaning organisations can be independently audited against its requirements.
- **ISO 22313:2020** – provides guidance on implementing ISO 22301, including detailed recommendations for each clause of the standard.
- **ISO 27031:2011 (ICT Readiness for Business Continuity)** – provides guidance on concepts and principles of ICT readiness for business continuity, specifically addressing the DR aspects within the broader BCM framework.
- **BS 11200:2014 (Crisis Management)** – the British Standard for crisis management, providing guidance on establishing effective crisis management arrangements, including strategic response, decision-making, and communication.
- **NIST SP 800-34 (Contingency Planning Guide)** – provides guidance for IT contingency planning, including IT disaster recovery, for US federal information systems. While US-focused, it is widely referenced internationally.

Case Study – COVID-19 Pandemic and Business Continuity

The COVID-19 pandemic of 2020-2021 was the most significant business continuity event in modern history. Organisations worldwide were forced to rapidly transition to remote working, reconfigure supply chains, and adapt their operations to unprecedented restrictions. The pandemic exposed significant weaknesses in many organisations' BC plans, which had not adequately considered a scenario involving prolonged global disruption affecting all business functions simultaneously.

Key lessons from the pandemic for BC planners include: the importance of planning for prolonged disruptions (not just short-term events); the need for flexible work arrangements and remote access capabilities; the critical role of digital transformation in organisational resilience; the importance of supply chain diversification; and the need for psychological support for employees during extended crises.

Task: (1) How did the pandemic challenge traditional assumptions in BC planning (e.g. that physical relocation to an alternative site is always the solution)? (2) Identify three specific changes your organisation (or a hypothetical organisation) should make to its BC plan based on pandemic lessons. (3) How does the cyber security threat landscape change during a pandemic (consider: remote access, VPN capacity, shadow IT, phishing targeting remote workers)? (4) Design a BC strategy for a university that must continue teaching, research, and student support during a future pandemic scenario. Write a comprehensive 700-word analysis.

Over to you – BIA Exercise

Conduct a simplified Business Impact Analysis for a small medical clinic. Identify five critical business functions (e.g. patient appointments, prescriptions, medical records, payment processing, emergency response). For each function, determine: (a) the RTO, (b) the RPO, (c) the MTPD, (d) the impact of disruption at 1 hour, 4 hours, 24 hours, and 1 week, and (e) any dependencies on other functions or external services. Present your BIA in a formatted table with a 300-word executive summary.

Over to you – Video Watch: Disaster Recovery Strategies

Title: Hot Site vs Cold Site vs Warm Site – Explained – PowerCert Animated Videos

Link: https://youtu.be/xWTbPY0OfB0?si=Eb2aXRQtr-lZv-W7

After watching, create a comparison table of hot, warm, and cold DR sites covering: cost, setup time, data currency, suitable scenarios, and advantages/disadvantages. Which would you recommend for an online stock trading platform, and why?

Reading List

- Hiles, A. (2022) *Business Continuity Management: Global Best Practices.* 5th edn. Brookfield, CT: Rothstein Publishing.
- Drewitt, T. (2023) *A Manager's Guide to ISO 22301: A Practical Guide to Developing and Implementing a Business Continuity Management System.* 2nd edn. Ely: IT Governance Publishing.
- BSI (2022) *BS 11200:2014 Crisis Management – Guidance and Good Practice.* London: British Standards Institution.
- Watters, J. (2023) *Disaster Recovery, Crisis Response, and Business Continuity: A Management Desk Reference.* 2nd edn. New York: Apress.
- Graham, J. and Kaye, D. (2021) *A Risk Management Approach to Business Continuity.* 2nd edn. Brookfield, CT: Rothstein Publishing.
- ISO (2019) *ISO 22301:2019 Security and Resilience – Business Continuity Management Systems – Requirements.* Geneva: International Organisation for Standardisation.

Summary

In this chapter, you have explored the definitions, principles, and practices of Business Continuity Management, Disaster Recovery, and Crisis Management. You have examined the BCM lifecycle including BIA, risk assessment, strategy development, and testing. You have learned about DR site strategies, RTO/RPO metrics, and failover procedures. You have also examined crisis management at the executive level, including crisis communication and decision-making. Finally, you have analysed the international standards that underpin these disciplines, including ISO 22301, ISO 27031, and BS 11200.

Chapter Three – Major Computer Incident Investigations

Introduction

This chapter examines how major computer incidents are formally investigated. Digital forensics is the application of scientific methods to the collection, preservation, analysis, and presentation of digital evidence. It is a discipline that bridges computer science, criminal justice, and legal practice, requiring both technical expertise and meticulous attention to procedural correctness.

You will explore the investigation process from initial response through to final reporting, learn about the principles of forensic science as they apply to digital evidence, and understand the tools and techniques used by investigators. You will also analyse how evidence is contained, analysed, processed, and deployed in major cyber-related investigations, including the critical concept of chain of custody.

Learning Outcomes

On completing the chapter, you will be able to:

1. **Understand how major computer incidents are formally investigated.**

Assessment Criteria

3.1 Explain the processes, people and tools used in a planned and structured major incident investigation.

3.2 Analyse how evidence is contained, analysed, processed and deployed in a major cyber-related investigation.

3.1 Processes, people and tools in major incident investigations

Over to you – Video Watch: Digital Forensics Introduction

Watch these videos:

Title 1: Introduction to Digital Forensics – 13Cubed

Link: https://youtu.be/VYROU-ZwZX8?si=BQYu5sYAPGb8rjoP

Title 2: How Digital Forensics Works – Computerphile

Link: https://youtu.be/06OHfIWNCOE?si=udvu1cKtJYhAMcp2

After watching, explain: Why is the scientific method important in digital forensics? How does digital evidence differ from physical evidence? What is the significance of hash values in forensic investigations?

Principles of Forensic Science Applied to Digital Evidence

Digital forensics applies the same fundamental principles as traditional forensic science, adapted for the digital environment. The key principles include:

- **Locard's Exchange Principle** – every contact leaves a trace. In the digital world, this means that attackers inevitably leave digital traces of their activities – log entries, file modifications, registry changes, network connections, and metadata. Similarly, the act of investigating a system also leaves traces, which is why forensically sound acquisition methods are essential.
- **The scientific method** – forensic investigations must follow a systematic, repeatable process. Hypotheses are formed based on evidence, tested against the data, and revised as new evidence emerges. Conclusions must be supported by evidence, not assumptions.
- **Reproducibility** – forensic analysis must be reproducible – another qualified examiner should be able to follow the same process and reach the same conclusions. This requires thorough documentation of every step taken during the investigation.
- **Proportionality** – the investigation should be proportionate to the incident. Not every security event requires a full forensic investigation. The scope and depth of the investigation should be appropriate to the severity and impact of the incident.
- **Integrity** – the integrity of digital evidence must be preserved at all times. Evidence must not be altered, tampered with, or contaminated during collection, storage, analysis, or presentation. Cryptographic hashing (MD5, SHA-256) is used to verify that evidence has not been modified.

The Digital Forensics Investigation Process

A structured digital forensics investigation follows a well-defined process. The ACPO (Association of Chief Police Officers) Guidelines for Computer-Based Electronic Evidence – now maintained by the National Police Chiefs' Council (NPCC) – establish four key principles that govern the handling of digital evidence in the UK:

> **! Need to know – The Four ACPO Principles**
>
> **Principle 1:** No action taken by law enforcement agencies, persons employed within those agencies, or their agents should change data which may subsequently be relied upon in court.
>
> **Principle 2:** In circumstances where a person finds it necessary to access original data, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.
>
> **Principle 3:** An audit trail or other record of all processes applied to digital evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.
>
> **Principle 4:** The person in charge of the investigation has overall responsibility for ensuring that the law and these principles are adhered to.

The investigation process typically follows these phases:

- **Identification** – determining that a potential incident has occurred and deciding whether a forensic investigation is warranted. This involves initial assessment of the scope, severity, and potential legal implications of the incident.
- **Preservation** – securing and protecting evidence from alteration, damage, or destruction. This includes isolating affected systems, creating forensic images (bit-for-bit copies) of storage media, capturing volatile data (RAM contents, running processes, network connections), and establishing a chain of custody.

- **Collection** – systematically gathering all relevant evidence. Collection must follow established procedures to ensure evidence is admissible in legal proceedings. The order of volatility principle (collect the most volatile evidence first) guides the collection sequence: CPU registers and cache, memory (RAM), network state, running processes, disk storage, removable media, and printed documents.
- **Examination** – processing the collected evidence to extract relevant data. This includes recovering deleted files, examining file metadata, analysing log files, reconstructing timelines, and extracting artefacts from browsers, email, and applications.
- **Analysis** – interpreting the extracted data to understand what happened, when, how, and by whom. Analysis involves correlating evidence from multiple sources, constructing a coherent narrative of events, and forming conclusions supported by the evidence.
- **Reporting** – presenting the findings in a clear, comprehensive report suitable for the intended audience. Forensic reports may be used for internal decision-making, regulatory compliance, or legal proceedings. The report should include an executive summary, a detailed description of the methodology, a chronological narrative of events, the evidence supporting each finding, and conclusions.

Digital Forensics Tools

A wide range of tools is used in digital forensic investigations. Key tools include:

Category	Tool Examples	Purpose
Forensic Imaging	FTK Imager, dd, Guymager, EnCase	Creating bit-for-bit forensic copies of storage media with hash verification.
Forensic Suites	EnCase Forensic, FTK (Forensic Toolkit), Autopsy/Sleuth Kit	Comprehensive platforms for evidence examination, including file system analysis, keyword searching, and reporting.
Memory Forensics	Volatility, Rekall	Analysing RAM captures to identify running processes, network connections, encryption keys, and malware.
Network Forensics	Wireshark, NetworkMiner, tcpdump, Zeek (Bro)	Capturing and analysing network traffic to identify communications, data transfers, and attack patterns.
Mobile Forensics	Cellebrite UFED, Oxygen Forensic Detective, MSAB XRY	Extracting and analysing data from mobile devices including smartphones and tablets.
Log Analysis	Splunk, ELK Stack (Elasticsearch, Logstash, Kibana), Graylog	Aggregating, searching, and analysing log data from multiple sources to reconstruct event timelines.
Malware Analysis	Cuckoo Sandbox, Any.Run, IDA Pro, Ghidra	Analysing malicious software through static analysis (code examination) and dynamic analysis (controlled execution).

Timeline Analysis	Plaso/log2timeline, AXIOM	Creating unified timelines from multiple evidence sources to reconstruct the sequence of events.

3.2 Evidence handling: containment, analysis, processing and deployment

Chain of Custody

The chain of custody is the documented, unbroken trail that accounts for the handling of evidence from the moment it is collected to the moment it is presented in court or disposed of. Maintaining a proper chain of custody is essential to ensure that evidence is admissible in legal proceedings and has not been altered or contaminated.

A chain of custody record typically includes: a unique evidence identifier, a description of the evidence item, the date and time of collection, the name and signature of the person who collected it, the location where it was collected, a log of every person who subsequently handled the evidence (including date, time, purpose, and any actions taken), the storage location and security measures applied, and the hash values recorded at each transfer point to verify integrity.

Did you know?

In 2019, a UK court ruled that digital evidence from a major fraud case was inadmissible because the investigating agency could not demonstrate an unbroken chain of custody. The evidence – which included email records and financial documents stored on seized hard drives – had been stored in an unsecured location, and the agency could not account for a 48-hour period during which the drives were unmonitored. The case was dismissed. This example illustrates why meticulous evidence handling is not merely a procedural formality but a practical necessity.

Forensic Acquisition: Write Blockers and Imaging

Forensic acquisition is the process of creating an exact copy of digital evidence for examination. The fundamental rule is that the original evidence must never be examined directly – all analysis is performed on forensic copies. Key concepts include:

- **Write blockers** – hardware or software devices that prevent any data from being written to the original evidence media during the acquisition process. Hardware write blockers are physical devices placed between the evidence media and the forensic workstation. Software write blockers achieve the same effect through operating system configuration. Write blockers are essential for complying with ACPO Principle 1.
- **Forensic imaging** – creating a bit-for-bit copy (image) of the entire storage device, including unused space, deleted files, and file system structures. Unlike a standard file copy, a forensic image captures everything on the device. Tools such as FTK Imager, dd, and EnCase are used for this purpose.
- **Hash verification** – calculating cryptographic hash values (typically MD5 and SHA-256) of both the original evidence and the forensic image to verify that they are identical. If the hash values match, the image is a perfect copy. Hash values should

be recorded in the chain of custody documentation and recalculated at each significant point in the investigation.

- **Volatile data capture** – some evidence exists only in RAM and will be lost when the system is powered off. Volatile data includes running processes, network connections, logged-in users, clipboard contents, and encryption keys. Capturing volatile data requires accessing the live system, which must be done by a competent person in accordance with ACPO Principle 2.

Types of Digital Evidence

Digital evidence can be found in many locations and takes many forms:

- **File system evidence** – documents, images, databases, executables, and other files stored on hard drives, SSDs, and removable media. This includes both existing files and deleted files that may be recoverable from unallocated space.
- **Log files** – system logs, application logs, security logs, web server logs, firewall logs, and authentication logs. Logs provide a chronological record of system activity and are often the primary source of evidence in network intrusions.
- **Email evidence** – email messages, headers, attachments, and metadata. Email evidence can establish communication patterns, confirm identity, and reveal the content of discussions relevant to the investigation.
- **Browser artefacts** – browsing history, cache, cookies, bookmarks, download history, and form data. Browser artefacts can reveal what websites were accessed, when, and what content was viewed or downloaded.
- **Registry data (Windows)** – the Windows registry contains a wealth of forensic data, including information about installed software, recently accessed files, USB devices that have been connected, user activity, and system configuration changes.
- **Network traffic** – captured network packets can reveal communication patterns, data transfers, command-and-control activity, and the content of unencrypted communications.
- **Cloud evidence** – data stored in cloud services (email, file storage, collaboration tools) may be relevant to an investigation but raises jurisdictional and access challenges. Cloud evidence may require cooperation from the cloud service provider and may be subject to different legal frameworks depending on where the data is physically stored.
- **Mobile device evidence** – smartphones and tablets contain a rich source of evidence including call logs, messages (SMS, WhatsApp, Telegram), location data (GPS, cell tower records), photographs, application data, and browsing history.

Case Study – Operation Ore and Digital Evidence Challenges

Operation Ore (2002-2012) was a major UK law enforcement operation that investigated individuals who had used stolen credit card details to access illegal online content. The operation highlighted significant challenges in digital forensics, including the risk of false positives (some suspects had their credit card details stolen and used without their knowledge), the importance of thorough technical analysis (rather than relying solely on credit card transaction records), and the devastating consequences of wrongful accusations based on incomplete digital evidence. Several convictions were subsequently overturned.

Task: (1) What does this case teach us about the importance of thorough forensic analysis? (2) How could the investigation have been improved from a forensic methodology perspective? (3) What is the risk of relying on a single source of digital evidence? (4) How should investigators balance the need to pursue serious crime with the rights of individuals who may be falsely implicated? Write a 500-word analysis.

Over to you – Evidence Handling Procedure

You are the lead forensic investigator called to a company where an employee is suspected of stealing intellectual property. When you arrive, the suspect's computer is still running, and several USB drives are on the desk. Write a step-by-step evidence collection procedure covering: (a) how you secure the scene, (b) the order in which you collect evidence (explain the order of volatility), (c) how you use write blockers and imaging tools, (d) how you maintain chain of custody, and (e) how you document your actions. Your procedure should reference the ACPO principles.

Over to you – Hands-On Forensics Activity

Download and install Autopsy (https://www.autopsy.com/), the free open-source digital forensics platform. Download one of the available practice forensic images from the Digital Corpora project (https://digitalcorpora.org/). Open the image in Autopsy and: (a) examine the file system structure, (b) search for deleted files, (c) review browser artefacts, (d) examine file metadata, and (e) create a timeline of activity. Write a 400-word summary of your findings as if you were preparing a preliminary forensic report.

Reading List

- Casey, E. (2023) *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet.* 4th edn. London: Academic Press.
- Carrier, B. (2024) *File System Forensic Analysis.* 2nd edn. Boston, MA: Addison-Wesley.
- Johansen, G. (2022) *Digital Forensics and Incident Response.* 3rd edn. Birmingham: Packt Publishing.
- NPCC (2020) *Authorised Professional Practice: Digital Evidence.* London: College of Policing. Available at: https://www.college.police.uk/guidance/digital-evidence (Accessed: 15 March 2026).
- Nikkel, B. (2022) *Practical Forensic Imaging: Securing Digital Evidence with Linux Tools.* 2nd edn. San Francisco, CA: No Starch Press.
- Sammons, J. (2023) *The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics.* 3rd edn. Waltham, MA: Syngress.

Summary

In this chapter, you have examined how major computer incidents are formally investigated using digital forensic methodologies. You have explored the principles of forensic science as they apply to digital evidence, the ACPO/NPCC principles, the investigation lifecycle from identification through to reporting, and the tools used by forensic investigators. You have also analysed the critical importance of evidence handling, including chain of custody,

forensic imaging, hash verification, and volatile data capture. These skills are essential for ensuring that investigations are thorough, legally defensible, and capable of supporting both internal decisions and legal proceedings.

Chapter Four – Laws and Professional Practice in Incident Investigations

Introduction

This chapter examines the legal and ethical frameworks that govern the conduct of planned and structured major incident investigations. Digital forensics investigations operate within a complex legal landscape that includes criminal law, civil law, data protection regulations, employment law, and professional standards. Understanding these frameworks is essential because improperly conducted investigations can result in evidence being ruled inadmissible, legal liability for the investigator or their organisation, and violations of individual rights.

You will explore the key UK legislation relevant to computer incident investigations, examine professional codes of conduct and ethical standards, and analyse how legal requirements are applied in practice. This chapter emphasises that forensic investigators must be not only technically competent but also legally informed and ethically grounded.

Learning Outcomes

On completing the chapter, you will be able to:

1. **Understand laws and guidance in relation to the conduct of planned and structured major incident investigations.**

Assessment Criteria

4.1 Examine how relevant laws and professional practice are applied to computer incident investigations.

4.1 Relevant laws and professional practice in computer investigations

Key UK Legislation

Several pieces of UK legislation are directly relevant to the conduct of computer incident investigations:

Legislation	Relevance to Incident Investigations
Computer Misuse Act 1990	The primary UK legislation criminalising unauthorised access to computer systems. Three main offences: (1) unauthorised access to computer material, (2) unauthorised access with intent to commit further offences, and (3) unauthorised acts with intent to impair the operation of a computer. Investigators must ensure their activities do not constitute unauthorised access. Amended in 2015 to include life sentences for attacks on critical national infrastructure.
Data Protection Act 2018 / UK GDPR	Governs the processing of personal data. Investigators who handle personal data during an investigation must comply with data protection principles including lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, and security. The 72-hour

	breach notification obligation to the ICO is triggered when a personal data breach is likely to result in a risk to individuals.
Regulation of Investigatory Powers Act 2000 (RIPA)	Regulates the use of surveillance and investigation powers by public bodies. RIPA governs the interception of communications, the acquisition of communications data, covert surveillance, and the use of covert human intelligence sources. Private organisations are generally not covered by RIPA but must still comply with data protection and privacy law when conducting investigations.
Police and Criminal Evidence Act 1984 (PACE)	Provides the framework for the collection and handling of evidence by law enforcement. While PACE applies directly to police investigations, its principles (particularly regarding evidence integrity and admissibility) are relevant to any investigation that may result in legal proceedings.
Human Rights Act 1998	Incorporates the European Convention on Human Rights into UK law. Article 8 (right to respect for private and family life) is particularly relevant – investigations must be proportionate and respect individuals' privacy rights. Monitoring employee communications, for example, must be conducted in accordance with legitimate purpose and proportionality.
Investigatory Powers Act 2016	Known as the 'Snoopers' Charter', this act provides the legal framework for the interception of communications by intelligence agencies and law enforcement. It also requires internet service providers to retain internet connection records for 12 months. Relevant context for understanding the powers available to law enforcement during major cyber investigations.
Fraud Act 2006	Criminalises fraud by false representation, fraud by failing to disclose information, and fraud by abuse of position. Relevant to investigations involving financial fraud conducted through computer systems.
Proceeds of Crime Act 2002	Provides powers for the confiscation and recovery of criminal assets. Relevant to investigations involving ransomware payments, cryptocurrency-related crime, and financially motivated cyber attacks.

Industry Insight – GDPR Breach Notification in Practice

Under UK GDPR, organisations must notify the ICO of a personal data breach within 72 hours of becoming aware of it, unless the breach is unlikely to result in a risk to the rights and freedoms of individuals. If the breach poses a high risk to affected individuals, the organisation must also notify those individuals without undue delay. The ICO has published detailed guidance on what constitutes a notifiable breach, what information must be included in the notification, and how organisations should assess the risk to individuals.

In practice, the 72-hour clock starts when the organisation becomes 'aware' of the breach – which the ICO interprets as when there is a 'reasonable degree of certainty' that a breach has occurred. This means that the incident response team must be able to triage and assess potential breaches quickly to determine whether they are notifiable.

Read more: https://ico.org.uk/for-organisations/report-a-breach/

Ethical Principles in Digital Forensics

Beyond legal compliance, forensic investigators must adhere to ethical principles that ensure the integrity and credibility of their work:

- **Objectivity and impartiality** – investigators must approach every case without preconceptions or bias. The role of the investigator is to discover the truth, not to prove a particular theory. Evidence that exonerates a suspect is just as important as evidence that incriminates.
- **Competence** – investigators must only undertake work for which they are qualified and competent. Using unfamiliar tools or techniques without adequate training risks damaging evidence and producing unreliable results.
- **Confidentiality** – investigators have access to highly sensitive information and must protect it from unauthorised disclosure. Information obtained during an investigation should only be shared with authorised parties on a need-to-know basis.
- **Professional development** – the digital forensics field evolves rapidly, and investigators must maintain their knowledge and skills through continuous professional development, including attending training courses, conferences, and obtaining relevant certifications.
- **Accountability** – investigators must be prepared to explain and justify their actions, methods, and conclusions. In legal proceedings, this means being able to withstand cross-examination from opposing counsel and demonstrate that their work was conducted to professional standards.

Professional Standards and Certifications

Several professional certifications demonstrate competence in digital forensics:

- **Certified Computer Examiner (CCE)** – issued by the International Society of Forensic Computer Examiners (ISFCE). A vendor-neutral certification covering forensic examination procedures and evidence handling.
- **GIAC Certified Forensic Examiner (GCFE)** – issued by the SANS Institute. Focuses on Windows forensics and analysis techniques.
- **GIAC Certified Forensic Analyst (GCFA)** – an advanced SANS certification covering threat hunting, incident response, and digital forensics analysis.
- **EnCase Certified Examiner (EnCE)** – vendor-specific certification for the EnCase forensic platform, widely used in law enforcement and corporate investigations.
- **Certified Cyber Forensics Professional (CCFP)** – issued by (ISC)², covering digital forensics, electronic discovery, and incident response at a managerial level.
- **ISO 17025 accreditation** – laboratories that process digital evidence for law enforcement may seek accreditation to ISO 17025, the international standard for testing and calibration laboratories. This demonstrates that the laboratory's processes meet rigorous quality standards.

Over to you – Legal Scenario Exercise

A company discovers that an employee has been emailing confidential customer data to a personal email address. The company wants to investigate but is concerned about legal issues. Write a 600-word advisory memo covering: (a) which laws are relevant (consider the Computer Misuse Act, DPA 2018/UK GDPR, Human Rights Act, and employment law), (b) what the company can legally do to investigate (e.g. monitoring, accessing the employee's work email, forensic imaging of their work computer), (c) what the company cannot legally do (e.g. accessing personal devices without consent), (d) how evidence should be handled to preserve its admissibility, and (e) whether and when the company should involve law enforcement.

Over to you – Video Watch: Cyber Law

Title: Computer Misuse Act Explained

Link: https://youtu.be/ws4CrncWEwE?si=MPn-Apfr-Q_s8NLv

After watching, answer: What are the three main offences under the Computer Misuse Act? How does the Act apply to ethical hackers and penetration testers? What amendments were made in 2015 and why?

Case Study – R v Caffrey (2003) and Expert Evidence

In 2003, Aaron Caffrey was charged under the Computer Misuse Act for launching a DDoS attack against the Port of Houston, Texas. Despite digital evidence on his computer linking him to the attack, Caffrey was acquitted after his defence argued that a trojan on his computer could have been responsible for the attack without his knowledge – the so-called 'trojan defence'. The case highlighted the challenges of attributing cyber attacks to specific individuals and the importance of thorough forensic analysis that considers alternative explanations for digital evidence.

Task: (1) What is the 'trojan defence' and why was it effective in this case? (2) How could the prosecution's forensic evidence have been strengthened? (3) What forensic techniques could be used today to distinguish between user activity and trojan-controlled activity? (4) What are the implications of this case for digital forensic practitioners? Write a 500-word analysis.

Over to you – Research: International Jurisdictional Challenges

Research the challenges of investigating cyber crimes that cross international boundaries. Consider: (a) the Budapest Convention on Cybercrime (2001) and its role in international cooperation, (b) Mutual Legal Assistance Treaties (MLATs) and their limitations, (c) the US CLOUD Act and its implications for accessing data stored abroad, (d) the challenge of attributing cyber attacks to specific nation-states, and (e) examples of successful international cooperation in cyber crime investigations. Write a 500-word briefing note.

Reading List

- Gillespie, A.A. (2023) *Cybercrime: Key Issues and Debates.* 3rd edn. Abingdon: Routledge.

- Wall, D.S. (2021) *Cybercrime: The Transformation of Crime in the Information Age.* 2nd edn. Cambridge: Polity Press.
- ICO (2024) *Guide to the UK General Data Protection Regulation (UK GDPR).* London: Information Commissioner's Office. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/ (Accessed: 15 March 2026).
- Lloyd, I.J. (2023) *Information Technology Law.* 9th edn. Oxford: Oxford University Press.
- Mason, S. and Seng, D. (2022) *Electronic Evidence.* 5th edn. London: University of London Press.
- College of Policing (2020) *Authorised Professional Practice: Digital Evidence.* London: College of Policing.

Summary

In this chapter, you have examined the legal and ethical frameworks governing computer incident investigations. You have analysed key UK legislation including the Computer Misuse Act, Data Protection Act/UK GDPR, RIPA, PACE, and the Human Rights Act. You have explored the ethical principles that guide forensic investigators – objectivity, competence, confidentiality, professional development, and accountability. You have also examined professional certifications and standards that demonstrate investigator competence. Understanding this legal and ethical landscape is essential for conducting investigations that are both effective and legally defensible.

Glossary

Word / Term	Explanation
ACPO Principles	Four principles governing the handling of digital evidence in the UK, now maintained by the NPCC.
BIA	Business Impact Analysis – identifies critical functions and quantifies the impact of their disruption.
Business Continuity (BC)	Holistic management process for building organisational resilience and maintaining critical functions during disruptions.
CERT/CSIRT	Computer Emergency Response Team / Computer Security Incident Response Team.
Chain of Custody	Documented record of every person who handled evidence, from collection to presentation.
Cold Site	An empty DR facility with power and networking but no pre-installed equipment.
Crisis Management (CM)	Strategic leadership during major events, focusing on decisions, reputation, and communication.
Disaster Recovery (DR)	Technical procedures for restoring IT systems and data after a disruption.
Dwell Time	The period between initial compromise and detection of the breach.
Forensic Imaging	Creating a bit-for-bit copy of storage media for examination without altering the original.
Hash Value	A fixed-length digital fingerprint calculated from data, used to verify evidence integrity (e.g. SHA-256).
Hot Site	A fully operational DR facility that can take over immediately during a disaster.
IOC	Indicator of Compromise – forensic data identifying potentially malicious activity.
ISO 22301	International standard for Business Continuity Management Systems.
Locard's Exchange Principle	Every contact leaves a trace – a foundational principle of forensic science.
MITRE ATT&CK	A knowledge base of adversary tactics and techniques based on real-world observations.
MTPD	Maximum Tolerable Period of Disruption – the longest acceptable downtime for a business function.
NIST SP 800-61	The NIST Computer Security Incident Handling Guide.
Order of Volatility	The principle of collecting the most volatile evidence first (RAM before disk).

RPO	Recovery Point Objective – maximum acceptable data loss, measured in time.
RTO	Recovery Time Objective – maximum acceptable time to restore a function after disruption.
SIEM	Security Information and Event Management – aggregates and analyses security log data.
Triage	The process of prioritising incidents based on severity and potential impact.
Volatile Data	Data that exists only temporarily (e.g. in RAM) and is lost when a system is powered off.
Warm Site	A DR facility with pre-installed hardware but not fully configured for immediate use.
Write Blocker	Device preventing data from being written to evidence media during forensic acquisition.

MCQs and True & False Questions (self-assessment)

True or False Questions

1. The NIST Incident Response lifecycle has four phases.
2. Preparation is considered the least important phase of incident response.
3. A CERT and a CSIRT are different names for essentially the same type of team.
4. The ACPO principles govern the handling of digital evidence in the UK.
5. A forensic image is a standard file copy of selected documents.
6. Business Continuity focuses specifically on restoring IT systems.
7. RTO measures the maximum acceptable time to restore a function.
8. A hot DR site can take over operations almost immediately.
9. Chain of custody documentation is optional in forensic investigations.
10. The Computer Misuse Act 1990 criminalises unauthorised access to computer systems.
11. GDPR requires breach notification to the ICO within 72 hours.
12. Volatile data such as RAM contents is preserved when a computer is shut down.
13. Locard's Exchange Principle states that every contact leaves a trace.
14. Crisis Management operates at the operational, not strategic, level.
15. MITRE ATT&CK provides a knowledge base of adversary tactics and techniques.
16. The order of volatility principle means disk evidence should be collected before RAM.
17. A write blocker prevents data from being written to evidence media.
18. ISO 22301 is the international standard for Business Continuity Management.
19. The trojan defence was successfully used in R v Caffrey (2003).
20. Tier 1 SOC analysts are primarily responsible for threat hunting.
21. RPO measures the maximum tolerable data loss in time.
22. Hash values are used to verify the integrity of forensic evidence.
23. Private organisations are generally covered by RIPA.
24. A cold site has pre-installed, fully operational equipment ready for immediate use.
25. Post-incident lessons learned sessions help improve future incident response.

Multiple Choice Questions

1. How many phases does the NIST Incident Response lifecycle have?

A. Two
B. Three
C. Four
D. Five

2. Which is the MOST important phase of incident response?

A. Detection
B. Containment
C. Preparation
D. Recovery

3. What does RTO stand for?

A. Recovery Test Objective
B. Recovery Time Objective
C. Risk Tolerance Objective
D. Resilience Testing Output

4. ACPO Principle 1 states that:

A. Evidence should be destroyed after analysis
B. No action should change data relied upon in court
C. Only police can collect digital evidence
D. All evidence must be encrypted

5. Which tool is used for forensic imaging?

A. Microsoft Word
B. FTK Imager
C. Adobe Photoshop
D. Slack

6. The three tiers of SOC analysts are:

A. Bronze, Silver, Gold
B. Junior, Senior, Manager
C. Triage, Investigation, Threat Hunting
D. Network, Database, Application

7. Business Continuity Management is governed by which standard?

A. ISO 27001
B. ISO 22301
C. ISO 9001
D. ISO 14001

8. What is a 'warm site'?

A. A site with no equipment
B. A fully operational duplicate site
C. A site with equipment but not fully configured
D. An outdoor backup location

9. The Computer Misuse Act was first enacted in:

A. 1985
B. 1990
C. 2000
D. 2010

10. Which hash algorithm is commonly used in forensics?

A. AES-256
B. SHA-256
C. RSA-2048
D. DES

11. GDPR breach notification must be made to the ICO within:

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

12. What does the order of volatility determine?

A. Which systems to patch first
B. The sequence for collecting evidence
C. The severity of an incident
D. The priority of backup restoration

13. Crisis Management primarily focuses on:

A. Technical system restoration
B. Strategic leadership and communication
C. Database backup procedures
D. Network configuration

14. MITRE ATT&CK covers how many tactics?

A. 5
B. 10
C. 14
D. 20

15. Which certification is specific to the EnCase forensic platform?

A. GCFE
B. EnCE
C. CCFP
D. CEH

16. What is Locard's Exchange Principle?

A. All evidence must be exchanged between parties
B. Every contact leaves a trace
C. Evidence must be copied before analysis
D. Digital evidence expires over time

17. A DRaaS solution provides:

A. Physical security guards
B. Cloud-based disaster recovery
C. Compliance certificates
D. Employee training

18. Which act regulates surveillance by UK public bodies?

A. Fraud Act 2006
B. Data Protection Act 2018
C. RIPA 2000
D. Computer Misuse Act 1990

19. The Norsk Hydro ransomware attack occurred in:

A. 2017

B. 2018
C. 2019
D. 2020

20. What is MBCO?

A. Maximum Business Continuity Objective
B. Minimum Business Continuity Objective
C. Managed Backup and Cloud Operations
D. Multi-Business Coordination Office

Answers to True/False Questions

1. *True.* NIST SP 800-61 defines four phases: Preparation; Detection and Analysis; Containment, Eradication, and Recovery; Post-Incident Activity.

2. *False.* Preparation is widely considered the most important phase.

3. *True.* CERT and CSIRT are essentially interchangeable terms for the same type of team.

4. *True.* The ACPO principles (now NPCC) govern digital evidence handling in the UK.

5. *False.* A forensic image is a bit-for-bit copy of the entire storage device, not a selective file copy.

6. *False.* Business Continuity encompasses all critical business functions. Disaster Recovery focuses specifically on IT systems.

7. *True.* RTO is the maximum acceptable time to restore a business function after disruption.

8. *True.* A hot site is a fully operational duplicate facility capable of immediate takeover.

9. *False.* Chain of custody documentation is essential and must be maintained for evidence to be admissible.

10. *True.* The CMA 1990 is the primary UK legislation criminalising unauthorised computer access.

11. *True.* UK GDPR requires notification within 72 hours of becoming aware of a notifiable breach.

12. *False.* Volatile data in RAM is lost when the system is powered off.

13. *True.* Locard's principle states that every contact between two items results in an exchange of material.

14. *False.* Crisis Management operates at the strategic and executive level, not operational.

15. *True.* ATT&CK maps real-world adversary tactics, techniques, and procedures (TTPs).

16. *False.* The order of volatility states that the most volatile evidence (RAM) should be collected first, before disk.

17. *True.* Write blockers prevent any modification of the original evidence media.

18. *True.* ISO 22301:2019 specifies requirements for a Business Continuity Management System.

19. *True.* Caffrey was acquitted after successfully arguing that a trojan could have been responsible.

20. *False.* Tier 1 analysts handle triage. Tier 3 analysts are responsible for threat hunting.

21. *True.* RPO defines the maximum tolerable data loss, measured as a time period before the disruption.

22. *True.* Hash values (MD5, SHA-256) provide a digital fingerprint to verify evidence has not been altered.

23. *False.* RIPA generally applies to public bodies and law enforcement, not private organisations.

24. *False.* A cold site has no pre-installed equipment. A hot site has fully operational equipment.

25. *True.* Lessons learned sessions are essential for continuous improvement of incident response.

Answers to Multiple Choice Questions

1. (C) Four
2. (C) Preparation
3. (B) Recovery Time Objective
4. (B) No action should change data relied upon in court
5. (B) FTK Imager
6. (C) Triage, Investigation, Threat Hunting
7. (B) ISO 22301
8. (C) A site with equipment but not fully configured
9. (B) 1990
10. (B) SHA-256
11. (C) 72 hours
12. (B) The sequence for collecting evidence
13. (B) Strategic leadership and communication
14. (C) 14
15. (B) EnCE
16. (B) Every contact leaves a trace
17. (B) Cloud-based disaster recovery
18. (C) RIPA 2000
19. (C) 2019
20. (B) Minimum Business Continuity Objective