Domain 2: Incident Response, Business Continuity and Disaster Recovery Concepts

▼ Recovery Strategies

Concepts Covered:

- The Goal of Business Continuity
- The Goal of Disaster Recovery
- Disaster Recovery in the Real World
- Components of a Disaster Recovery Plan

1. Business Continuity (BC)

Definition

- **Business Continuity** is the ability of an organization to keep its most critical functions operating during and after a disruption, even if at a reduced capacity.

Types of Disruptions

- Disruptions can be caused by:
  - Attacks (e.g., cyberattacks)
  - Infrastructure failures (e.g., power outages)
  - Natural disasters (e.g., earthquakes, floods)
  - Other disturbances (e.g., human error)

Incident Handling

- **Minor Incidents:** Most disruptions are minor (e.g., a system reboot) and have minimal impact.
- **Major Incidents:** Occasionally, a major event interrupts business for a longer, unacceptable period. In such cases, the organization must activate its business continuity plan.

Scope of Business Continuity

- **What it covers:** Planning, preparation, response, and recovery operations for critical services and products.
- **What it doesn't cover:** Full restoration of all business activities and services. Focus is only on what's essential to keep the organization running at a basic level.

Example

- If a bank's main office is flooded, business continuity ensures that essential banking services (like ATM withdrawals and online banking) continue, even if some branches are closed.

Planning Requirements

- **Organizational Commitment:** Requires significant resources (personnel, financial).
- **Executive Support:** Must be supported by top management or an executive sponsor. Without this, the plan is unlikely to succeed.

2. Disaster Recovery (DR)

Definition

- **Disaster Recovery** is the process of restoring IT and communication systems to full, reliable operation after a disruption.

Relationship to Business Continuity

- **Where it fits:** DR begins where business continuity ends. While BC maintains critical functions, DR aims to fully restore all systems.

Scope of Disaster Recovery

- Focuses on:
  - IT systems (servers, databases, networks)
  - Communication systems (phone, email, messaging)
- **Independent Recovery:** Sometimes, business functions can be restored before IT systems, but IT is often crucial for overall recovery.

Example

- After a ransomware attack, disaster recovery involves restoring clean backups of servers and databases so the business can return to normal operations.

3. Disaster Recovery in Practice

Critical Systems and Backups

- **Identification:** Organizations must identify which systems are critical.
- **Backups:** Regular, tested backups are essential.
- **Detection Delays:** Sometimes, incidents (like malware infections) go undetected for months.

Example: Hospital Case

- A hospital discovered a system compromise after 260 days.
- **Problem:** The most recent backup was infected with malware.
- **Solution:** They had to restore from a backup nearly a year old and carefully recover newer data to avoid reinfection.
- **Lesson:** Multiple backup levels and long retention periods are needed.

Complex Systems and Dependencies

- **Multiple Systems:** Large organizations often have interconnected systems and databases.

- **Data Flow:** Data may be entered in one system and copied to others (e.g., hospital registration, lab, and radiology systems).
- **Importance:** Understanding these dependencies is vital for effective disaster recovery planning.

Example

- In a hospital, the registration system feeds data to both laboratory and radiology systems, each with separate databases. A disaster recovery plan must account for restoring all these systems and their data flows.

4. Components of a Disaster Recovery Plan (DRP)

Types of Documents

- **Executive Summary:** High-level overview for leadership.
- **Department-Specific Plans:** Tailored to the needs of each department.
- **Technical Guides:** Detailed instructions for IT staff on backup and restoration procedures.
- **Full Plan Copies:** Provided to critical disaster recovery team members.

Checklists

- **Purpose:** Help guide actions during the chaos of a disaster.
- **For Whom:**
  - **Critical Team Members:** Step-by-step tasks to follow.
  - **IT Personnel:** Instructions for setting up alternate sites and restoring systems.
  - **Managers/Public Relations:** High-level documents to help communicate with stakeholders and the public, freeing up technical staff to focus on recovery.

Summary Table

Concept	Focus Area	Example/Explanation
Business Continuity	Keep critical functions running (reduced)	Bank keeps ATMs working during flood, even if branches are closed
Disaster Recovery	Restore IT and communications to full ops	Restore clean server backups after ransomware attack
Real World Example	Importance of backups and system mapping	Hospital needed year-old backup after malware; must understand system dependencies
DRP Components	Documentation and checklists for all roles	Executive summaries, IT guides, checklists for all involved in disaster recovery

Key Takeaways

- **Business Continuity** ensures essential services continue during a disruption, focusing on critical areas, not full operations.
- **Disaster Recovery** restores IT and communications to pre-disaster state, enabling full business restoration.
- **Effective DR planning** requires understanding system interdependencies, regular and diverse backups, and clear, role-specific documentation.
- **Executive support and organizational commitment** are crucial for successful continuity and recovery planning.

▼ Continuity Strategies

Concepts Covered:

- Incident Terminology
- Business Continuity in the Workplace
- The Importance of Business Continuity
- Components of a Business Continuity Plan

- Business Continuity in Action

Incident Terminology

1. Breach

- **Definition:** Loss of control, compromise, unauthorized disclosure, or acquisition of personally identifiable information (PII) by someone not authorized, or by an authorized user for an unauthorized purpose.
- **Example:** If an employee accesses customer data for personal gain, or a hacker steals a database of PII, it is a breach.

2. Event

- **Definition:** Any observable occurrence in a network or system. This can be normal or abnormal activity.
- **Example:** A user logging in, a server crash, or a firewall blocking a connection attempt are all events.
- **Note:** Not all events are harmful; only those that negatively impact security may escalate to incidents.

3. Exploit

- **Definition:** A specific attack that takes advantage of a system vulnerability.
- **Example:** Using a software bug to gain unauthorized access to a system.

4. Incident

- **Definition:** An event that actually or potentially jeopardizes the confidentiality, integrity, or availability (CIA) of an information system or its data.
- **Examples:** Malware infection, data breach, denial-of-service attack.
- **Difference from Event:** All incidents are events, but not all events are incidents. An incident is more severe, causing or threatening harm.

5. Intrusion

- **Definition:** A deliberate security incident where an unauthorized person gains or attempts to gain access to a system or resource.

- **Example:** A hacker breaking into a company's network.

6. Threat

- **Definition:** Any circumstance or event with the potential to negatively impact an organization's operations, assets, individuals, or reputation through unauthorized access, destruction, disclosure, modification, or denial of service.
- **Example:** Malware, phishing, insider threats.

7. Vulnerability

- **Definition:** A weakness in a system, procedure, or control that can be exploited by a threat.
- **Example:** Unpatched software, weak passwords.

8. Zero Day

- **Definition:** A previously unknown vulnerability that can be exploited before it is detected or patched.
- **Example:** Attackers use a new flaw in a web browser that has no fix yet, often going undetected because it doesn't match known attack patterns.

Business Continuity in the Workplace

- **Business Continuity Plan (BCP):** A documented strategy to sustain and restore business operations after a significant disruption.
- **Digital vs. Hard Copy:** Most plans are digital, but this can be risky if systems are down. Some organizations maintain a *hard copy* (often called a "red book") stored offsite for emergencies (e.g., natural disasters, power outages).
- **Red Book:** Contains all critical procedures and is updated alongside the electronic version to ensure consistency.

Importance of Business Continuity

- **Purpose:** To keep business operations running during and after a disruption.

- **Key Elements:**
  - **Communication:** Multiple contact methods and backup numbers in case of power or communication failures.
  - **Phone Tree:** A structured list of who to contact if someone is unavailable.
  - **Checklists:** Detailed procedures to ensure nothing is missed, similar to pilots' pre-flight checks.
  - **Activation:** The plan is activated by contacting key individuals, including management, to prioritize actions and execute operations.
  - **Critical Contacts:** Includes supply chain, law enforcement, and external partners.
  - **Special Networks:** In critical sectors (e.g., hospitals), special communication networks may be used during cyberattacks to maintain essential services.

Components of a Business Continuity Plan

Component	Description
BCP Team List	Names, contact methods, and backup members
Management Guidance	Specifies authority and responsibilities for managers
Immediate Response Procedures	Security, safety, fire suppression, emergency notification procedures
Plan Activation	Guidelines on when and how to enact the plan
Notification Systems & Call Trees	Methods for alerting personnel when the BCP is activated
Critical Contacts	Vendors, customers, emergency providers, third-party partners

- **Cross-Departmental Involvement:** Members from across the organization contribute to ensure all processes are covered.
- **Alignment:** Technology and business needs must be aligned to protect confidentiality, integrity, and availability.

Business Continuity in Action (Example Scenario)

- **Scenario:** A fire destroys the billing department overnight.
- **Preparation:** A Business Impact Analysis (BIA) previously identified billing as important but not immediately critical.
- **Response:**
  - An alternative workspace is ready for the billing team within a week.
  - Customer service handles billing inquiries during the transition.
- **Result:** No significant interruption in business or customer service, demonstrating effective BCP execution.

Summary of Key Concepts with Examples:

Term	Definition/Explanation	Example
Breach	Unauthorized access/disclosure of PII	Hacker steals customer records
Event	Any observable occurrence in a system	User login, server crash
Exploit	Attack using a vulnerability	Malware uses software bug to infect system
Incident	Event compromising CIA of data/systems	Ransomware attack
Intrusion	Unauthorized access attempt or success	Hacker breaks into network
Threat	Potential cause of harm	Phishing email, malware
Vulnerability	Weakness that can be exploited	Outdated antivirus software
Zero Day	Unknown vulnerability actively exploited	New browser bug used before patch is available

Business Continuity:

- Plans must be accessible, up-to-date, and include both digital and hard copies.
- Communication, clear roles, and pre-identified alternative procedures are essential for resilience during disruptions.

▼ Incident Management

Concepts Covered:

- The Goal of Incident Response
- Components of the Incident Response Plan
- Consulting with Management
- Incident Response Team

1. The Goal of Incident Response

Definition and Importance

- **Incident Response**: The organized approach to addressing and managing the aftermath of a security breach or cyberattack.
- **Inevitability of Incidents**: Despite strong security measures, organizations will eventually face adverse events (incidents) that could disrupt business operations.

Primary Objectives

- **Protect Life, Health, and Safety**: The top priority in any incident is ensuring the safety of people. For example, in a fire or a data breach exposing sensitive health data, protecting individuals is more important than protecting assets.
- **Preparation**: Being ready with policies and plans before an incident occurs. This is sometimes called **crisis management**.
- **Preserve Business Viability**: The goal is to minimize impact and resume normal operations quickly.

Events vs. Incidents

- **Event**: Any observable occurrence (e.g., a user logging in, a file being accessed). Most are harmless.

- **Incident**: An event that threatens or disrupts the business mission (e.g., ransomware attack, data theft).

Relation to Business Continuity

- **Incident Response Planning**: Part of **Business Continuity Management (BCM)**, which ensures the organization can continue functioning after disruptions.

2. Components of the Incident Response Plan

Incident Response Policy and Plan

- **Policy**: High-level statement outlining the organization's approach to incident response.
- **Plan**: Detailed steps and procedures for staff to follow during an incident. It is a "living document" that evolves with the organization.

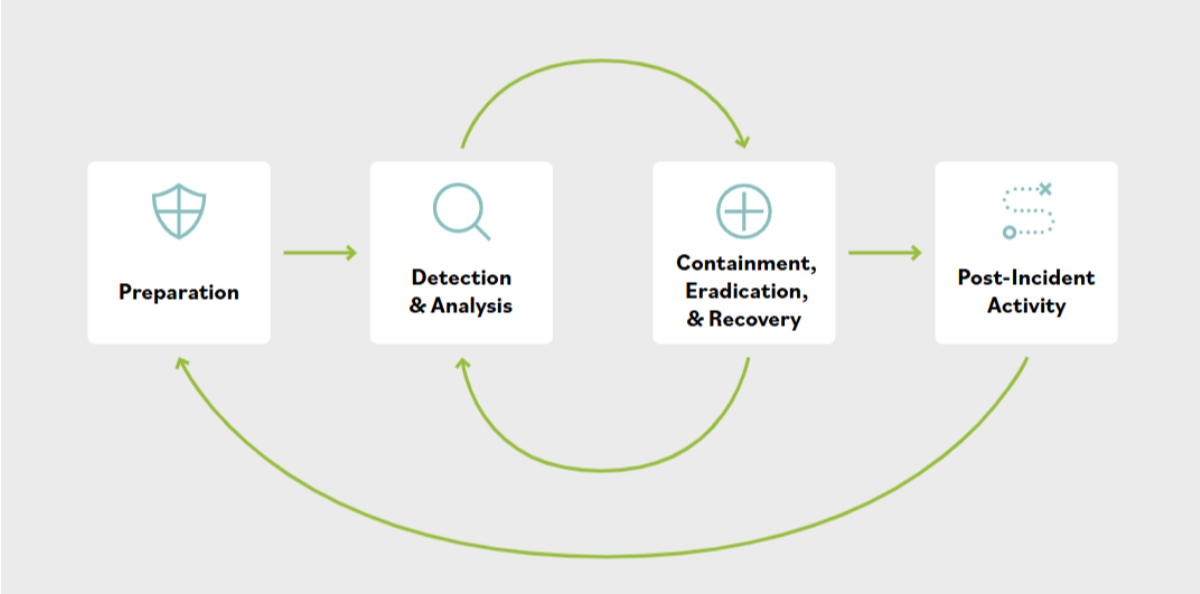
Alignment with Organizational Vision

- The plan should reflect the organization's mission, strategy, and values.

Procedures and Tools

- Include technical processes, techniques, checklists, and tools for responding to incidents.

Phases of Incident Response



A. Preparation

- **Policy Approval**: Management must approve the incident response policy.
- **Identify Critical Assets**: Determine which data and systems are most important (e.g., customer databases, financial records).
- **Single Points of Failure**: Avoid having only one protection layer (e.g., only one firewall). Use **defense in depth**—multiple security layers.
- **Staff Training**: Regular training and simulations to ensure everyone knows their role.
- **Incident Response Team**: Designate and train a team responsible for handling incidents.
- **First Response Practice**: Ensure staff can recognize and report incidents quickly.
- **Roles and Responsibilities**: Clearly define who does what during an incident.
- **Communication Plans**: Plan how to communicate with stakeholders (internal and external), considering that usual channels (like email) may be unavailable.

B. Detection and Analysis

- **Monitor Attack Vectors**: Watch for threats from all possible sources (e.g., phishing emails, network intrusions).
- **Analysis Using Threat Intelligence**: Use data and external intelligence to understand incidents.
- **Prioritization**: Decide which incidents need immediate attention.
- **Standardized Documentation**: Use consistent methods to record incidents and actions taken.

C. Containment

- **Gather Evidence**: Collect logs, files, and other data for investigation and legal purposes.
- **Containment Strategy**: Decide how to limit the spread of the incident (e.g., disconnecting affected systems).
- **Identify Attacker**: Try to determine who is behind the incident.
- **Isolate Attack**: Prevent further damage by isolating compromised systems.

D. Post-Incident Activity

- **Retain Evidence**: Keep necessary evidence for audits or legal investigations.
- **Lessons Learned**: Document what happened, what worked, and what didn't.
- **Retrospective Review**: Analyze all phases (preparation, detection, containment, recovery, and post-incident) to improve future responses.
- **Regulatory Compliance**: Ensure all required documentation is completed, especially if sensitive or legally protected data was involved.

3. Consulting with Management

Critical Information and Defense in Depth

- **Identify Critical Information**: Know what needs the most protection (e.g., customer data, intellectual property).

- **Defense in Depth**: Use multiple layers of security (like multiple locked doors in a fortress) to protect critical assets.

Staff Training and Communication

- **Training**: Use scenarios and simulations to prepare staff for real incidents.
- **Stakeholder Communication**: Plan how to communicate with different groups (staff, management, customers, media), ensuring sensitive information is only shared with those who need to know.

Detection, Documentation, and Prioritization

- **Monitor and Analyze**: Continuously watch for and analyze potential threats.
- **Standardized Documentation**: Use templates and consistent processes for recording incidents.
- **Task Assignment**: Ensure everyone knows their responsibilities during an incident.

Containment and Investigation

- **Containment**: Stop the spread of the incident.
- **Identify Attacker and Method**: Understand how the attack happened.
- **Evidence Collection**: Gather data for internal or external investigations.

Post-Incident Activities

- **Retain Evidence**: For legal or regulatory reasons.
- **Internal/External Audits**: Review what happened and how it was handled.
- **Lessons Learned**: Update plans and training based on what was learned.

4. Incident Response Team (IRT)

Team Structure

- **Dedicated, Leveraged, or Hybrid Teams**: Some organizations have full-time teams, others use staff as needed, or a mix.
- **First Responders**: IT professionals trained to identify and escalate security incidents, much like medical first responders assess and triage injuries.

Team Composition

- **Cross-Functional**: Includes members from:
  - Senior Management
  - Information Security
  - Legal
  - Public Affairs/Communications
  - Engineering (Systems and Network)

Team Member Roles

- **Training**: All team members must be trained in incident response.
- **Responsibilities**:
  - Investigate incidents
  - Assess damage
  - Collect evidence
  - Report incidents
  - Initiate recovery
  - Participate in remediation and lessons learned
  - Conduct root cause analysis

Specialized Teams

- **CIRT/CSIRT**: Computer (Security) Incident Response Teams focused on cyber incidents.

Primary Responsibilities

1. **Assess Damage**: Determine the scope and impact.
2. **Check for Data Compromise**: Was confidential information accessed or stolen?
3. **Recovery Procedures**: Restore systems and security.
4. **Implement Additional Security**: Prevent future incidents.

Summary Table

Phase/Component	Key Actions/Concepts	Example
Preparation	Policy, training, team, identify assets, communication	Fire drill, backup policies
Detection & Analysis	Monitor, analyze, prioritize, document	IDS alerts, threat intelligence
Containment	Gather evidence, isolate, identify attacker	Quarantine infected machines
Post-Incident Activity	Retain evidence, lessons learned, audits, compliance	Incident report, policy update
Incident Response Team	Cross-functional, trained, responsible for investigation & recovery	CSIRT handling a ransomware attack