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:**

  Ensures critical aspects of an organization continue functioning (even at reduced capacity) during disruptions (e.g., attacks, infrastructure failure, natural disasters).

- **Incident Handling:**
  - Most incidents are minor (e.g., system reboots) and quickly resolved.
  - Major incidents may require shifting from incident response to business continuity.
- **Scope of BC:**
  - Involves planning, preparation, response, and recovery operations.
  - Does **not** include full restoration of all business activities.
  - Focuses on maintaining critical products/services at a minimal operational level until normalcy returns.

- **Planning Requirements:**
  - Requires significant commitment of personnel and financial resources.
  - Needs executive management or executive sponsor support for success.

2. Disaster Recovery (DR)

- **Definition:**
  - Begins where business continuity ends.
  - Focuses on restoring IT and communication systems to full, reliable operation after a disruption.
- **Scope of DR:**
  - Guides emergency response personnel through restoration processes.
  - IT and communication recovery is often essential for overall business recovery.
  - Business function recovery may occur independently, but IT is usually critical.
- **BC vs. DR:**
  - BC: Maintains critical functions during disruption.
  - DR: Restores IT/communications to full operations post-disruption.

3. Disaster Recovery in Practice

- **Critical Systems & Backups:**
  - Identify critical systems.
  - Maintain and regularly test backups.
  - Incidents may go undetected for extended periods (e.g., 260 days in a hospital breach).
- **Example: Hospital Incident:**
  - Malware undetected for months; backups also infected.

    - Required restoring from backups nearly a year old and careful data recovery to avoid reinfection.
    - Emphasizes need for multiple backup layers and long retention periods.
- **Complex Systems:**
    - Data often distributed across multiple servers and databases.
    - Dependencies between systems (e.g., radiology and laboratory in hospitals) must be understood and documented.
    - DR plans must account for data flow and system interdependencies.

4. Components of a Disaster Recovery Plan (DRP)

- **Plan Documentation:**
    - Organizations may have multiple DRP documents for different audiences.
- **Types of Documents:**
    - **Executive Summary:** High-level overview.
    - **Department-Specific Plans:** Tailored to individual departments.
    - **Technical Guides:** For IT staff managing backup and recovery.
    - **Full Plan Copies:** For critical DR team members.
    - **Checklists:**
        - For DR team: Action steps during disaster.
        - For IT: Steps to activate alternate sites.
        - For Managers/PR: Simple guides for communication, minimizing the need for technical input during crises.

Summary Table

Aspect	Business Continuity (BC)	Disaster Recovery (DR)
Focus	Maintain critical operations	Restore IT/communications

Aspect	Business Continuity (BC)	Disaster Recovery (DR)
Scope	Planning, response, recovery	Restoration to full operations
Involvement	Organization-wide	Primarily IT/communications
Documentation	BC plan	Multiple DRP documents
Key Requirement	Executive support	Regular testing, multiple backups

Key Takeaway:

Effective business continuity and disaster recovery require thorough planning, executive support, understanding of system dependencies, and well-documented, regularly tested procedures tailored to the organization's needs.

▼ 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

- **Security Professionals' Role:**
  - Aim to protect systems from attacks and errors.
  - Act as first responders when incidents occur.
  - Understanding incident response starts with knowing key terms.
- **Key Terms:**
  - **Breach:**

        - Loss of control, unauthorized access/disclosure/acquisition of personally identifiable information (PII).
        - Can occur if unauthorized users access PII or authorized users misuse access.
        - (NIST SP 800-53 Rev. 5)
    - **Event:**
        - Any observable occurrence in a network/system.
        - (NIST SP 800-61 Rev 2)
    - **Exploit:**
        - A specific attack exploiting a system vulnerability.
    - **Incident:**
        - An event that jeopardizes confidentiality, integrity, or availability of information or systems.
    - **Intrusion:**
        - Deliberate incident where an intruder gains or attempts unauthorized access.
        - (IETF RFC 4949 Ver 2)
    - **Threat:**
        - Any circumstance/event that could negatively impact operations, assets, individuals, or the nation.
        - Includes unauthorized access, destruction, disclosure, modification, or denial of service.
        - (NIST SP 800-30 Rev 1)
    - **Vulnerability:**
        - Weakness in systems, procedures, or controls that could be exploited.
        - (NIST SP 800-30 Rev 1)
    - **Zero Day:**

        - Newly discovered vulnerability, unknown to defenders, exploitable before detection or prevention.

Business Continuity in the Workplace

- **Plan Accessibility:**
    - BCP should be accessible, usually digital, but digital-only storage is risky.
    - Some organizations maintain a hard copy ("red book") offsite for emergencies (e.g., power outage, disaster).
    - The hard copy must be updated whenever the electronic version changes to ensure consistency.

The Importance of Business Continuity

- **Purpose:**
    - To sustain operations during and after significant disruptions.
    - Ensures business can continue despite environmental disturbances.
- **Key Elements:**
    - **Communication:**
        - Multiple contact methods and backup numbers are essential.
        - Phone trees are used to ensure everyone can be reached.
    - **Procedures and Checklists:**
        - Clearly defined roles and responsibilities.
        - Checklists ensure no steps are missed, similar to pilots' pre-flight checks.
    - **Activation:**
        - Notify and involve management and authorized personnel to prioritize and execute operations.

        - Critical contact numbers for supply chain, law enforcement, and external sites should be readily available.
    - **Special Provisions:**
        - In critical sectors (e.g., hospitals), special communication networks may be available during cyberattacks.

Components of a Business Continuity Plan (BCP)

- **Definition:**
    - Proactive development of procedures to restore operations after disaster/disruption.
- **Development:**
    - Involvement from all organizational areas to ensure completeness.
    - Technology must support business needs for confidentiality, integrity, and availability.
- **Common Components:**
    - List of BCP team members with multiple contact methods and backups.
    - Management guidance and authority designations.
    - Immediate response procedures and checklists (security, safety, emergency notifications).
    - Criteria for enacting the plan.
    - Notification systems and call trees.
    - Contact numbers for critical supply chain members and external partners.

Business Continuity in Action (Example Scenario)

- **Scenario:**
    - Billing department loses facility in a fire (no personnel harmed).
    - BIA identified billing as important but not immediately critical.

- Pre-arranged alternative workspace available within a week.
- Customer service temporarily handles billing inquiries.
- Billing staff move to alternate area until permanent space is ready.
- Company’s cash reserves allow for a week’s interruption without major impact.
- Pre-planning and execution of BCP prevent service interruption, demonstrating successful business continuity.

Summary:

Understanding incident terminology is foundational for effective incident response. Business continuity planning ensures organizations can maintain and restore operations during disruptions, relying on accessible plans, robust communication, clear procedures, and pre-planned alternatives. Regular updates and involvement across the organization are crucial for a successful BCP. Real-world application, as shown in the billing department example, highlights the importance of preparation and flexibility in maintaining business operations.

▼ Incident Management

Concepts Covered:

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

1. Goal of Incident Response

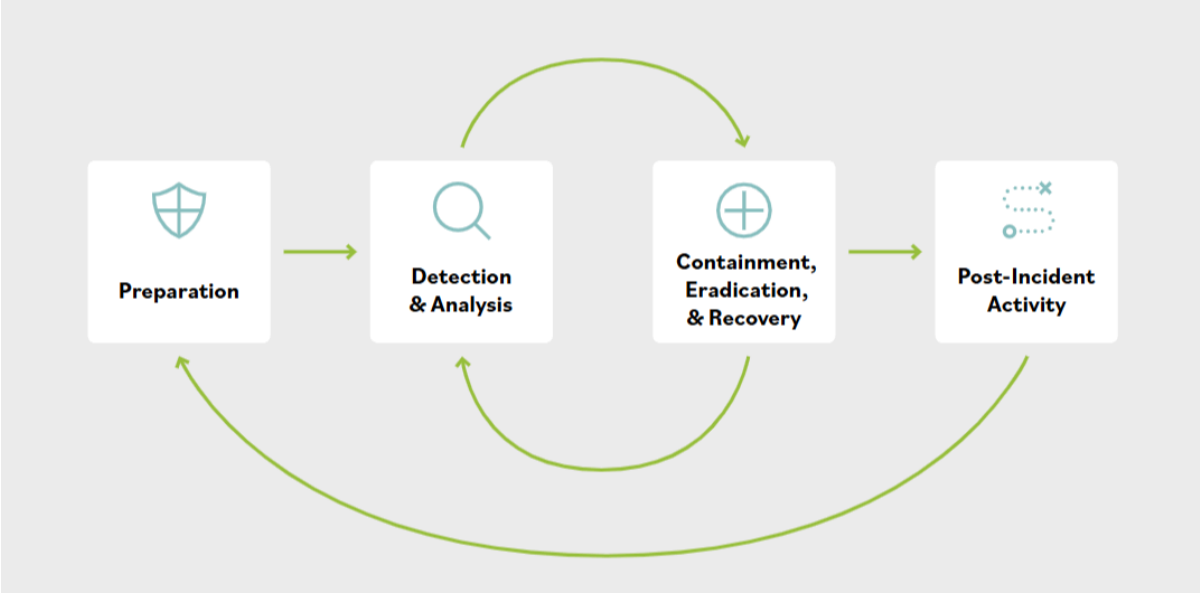
- **Inevitability of Incidents**: Despite best efforts, adverse events are unavoidable and can impact business objectives.

- **Top Priority**: Protecting life, health, and safety always comes first in decision-making.
- **Primary Goal**: Be prepared with policies and plans to guide the organization through crises (sometimes called crisis management).
- **Definition of Incident**: An event becomes an incident if it can disrupt the business mission.
- **Purpose of Incident Response**: Minimize impact and resume normal operations quickly.
- **Relation to BCM**: Incident response is a subset of business continuity management (BCM).

2. Components of the Incident Response Plan

Incident Response Policy and Plan

- **Policy**: References a plan for all employees, aligned with the organization's vision, strategy, and mission.
- **Plan**: Includes procedures, standards, technical processes, checklists, and tools for incident response.
- **Living Document**: The plan must evolve as the organization changes.



Preparation

- Develop and get management approval for policy.
- Identify critical data, systems, and single points of failure.
- Train staff (including simulations and scenarios).
- Establish an incident response team.
- Practice incident identification (first response).
- Define roles and responsibilities.
- Plan stakeholder communication, considering possible communication failures.

Detection and Analysis

- Monitor all potential attack vectors.
- Analyze incidents using available data and threat intelligence.
- Prioritize response actions.
- Standardize documentation for consistency.

Containment

- Gather and preserve evidence.
- Select an appropriate containment strategy.
- Identify and isolate the attacker and the attack.

Post-Incident Activity

- Retain necessary evidence.
- Document lessons learned.
- Conduct a retrospective review of all stages (preparation, detection, containment, recovery, post-incident).
- Meet regulatory documentation requirements, especially for legally protected data.

3. Consulting with Management

- **Critical Information & Defense in Depth**: Identify and protect critical assets with multiple layers of defense.
- **Staff Training & Communication**: Ensure everyone knows their role and how to communicate, considering confidentiality and audience.
- **Standardized Documentation**: Ensures clarity and accountability.
- **Containment and Investigation**: Identify attack vectors, isolate threats, and retain evidence for possible audits or legal investigations.
- **Continuous Improvement**: Document lessons learned and improve the plan after each incident.

4. Incident Response Team (IRT)

- **Structure**: Can be dedicated, leveraged, or hybrid, based on organizational needs.
- **First Responders**: IT professionals trained to distinguish between regular IT issues and security incidents.
- **Cross-Functional Team**: Includes senior management, security professionals, legal, communications, and engineering representatives.
- **Training**: All team members must be trained on the incident response plan.
- **Responsibilities**:
  - Investigate incidents and assess damage.
  - Determine if confidential information was compromised.
  - Initiate recovery and remediation.
  - Supervise implementation of improved security measures.
- **Specialized Teams**: Computer Incident Response Teams (CIRT/CSIRT) handle computer security incidents.

5. Key Takeaways

- **Preparedness** is essential: Have a policy, plan, trained team, and clear procedures.
- **Safety First**: Always prioritize life, health, and safety.
- **Communication**: Must be planned, secure, and role-appropriate.
- **Continuous Learning**: Post-incident reviews and lessons learned are crucial for improvement.
- **Compliance**: Documentation and evidence retention may be legally required, especially for sensitive information.