L2 Incident Response, Business Continuity and Disaster Recovery Concepts

Introduction

When we're talking about IR, BC and DR, we're focus on availability, which is accomplished through those concepts.

- **Incident Response** (IR) plan responds to unexpected changes in operating conditions to keep the business operating;
- **Business Continuity** (BC) plan enables the business to continue operating throughout the crisis;
- **Disaster Recovery** (DR) plan is activated to help the business to return to normal operations as quickly as possible, if Incident Response and Business Continuity plans fail.

Module 1: Understand Incident Response

Domain D2.3.1, D2.3.2, D2.3.3

Incident Terminology

- **Breach** (NIST SP 800-53 Rev. 5): The **loss of** control, compromise, unauthorized disclosure, unauthorized acquisition, or **any similar occurrence** where: **a person other than an authorized user accesses or potentially accesses personally identifiable information**; or an authorized user accesses personally identifiable information for other than an authorized purpose.

- **Event** (NIST SP 800-61 Rev 2): **Any observable occurrence** in a network or system.

- **Exploit**: **A particular attack**. It is named this way because **these attacks exploit system vulnerabilities**.

- **Incident**: **An event that actually or potentially jeopardizes** the confidentiality, integrity or availability of an information system or the information the system processes, stores or transmits.

- **Intrusion** (IETF RFC 4949 Ver 2): A security event, or combination of events, that constitutes a deliberate security incident in which an intruder gains, or attempts to gain, access to a system or system resource without authorization.

- **Threat** (NIST SP 800-30 Rev 1): **Any circumstance or event with the potential to adversely impact organizational operations** (including mission, functions, image or reputation), organizational assets, individuals, other organizations or the nation through an information system via unauthorized access, destruction, disclosure, modification of information and/or denial of service.

- **Vulnerability** (NIST SP 800-30 Rev 1): **Weakness** in an information system, system security procedures, internal controls or implementation that could be exploited by a threat source.
- **Zero Day**: **A previously unknown system vulnerability with the potential of exploitation without risk of detection or prevention because it does not**, in general, fit recognized patterns, signatures or methods.

The Goal of Incident Response

The priority of any incident response is to protect life, health and safety. When any decision related to priorities is to be made, **always choose safety first**. **The primary goal of incident management is to be prepared**. Preparation requires having a policy and a response plan that will **lead the organization through the crisis**. Some organizations use the term "crisis management" to describe this process, so you might hear this term as well. An event is any measurable occurrence, and most events are harmless. However, if the event has the potential to disrupt the business's mission, then it is called an incident. **Every organization must have an incident response plan that will help preserve business viability and survival.** The incident response process is aimed at reducing the impact of an incident so the organization can resume the interrupted operations as soon as possible. Note that incident response planning is a subset of the greater discipline of business continuity management (BCM).

Components of the Incident Response Plan

The incident response policy should reference **an incident response plan** that all employees will follow, depending on their role in the process. **The plan may contain several procedures and standards related to incident response**. It is a living representation of an organization's incident response policy. The organization's vision, strategy and mission should shape the incident response process. Procedures to implement the plan should define the technical processes, techniques, checklists and other tools that teams will use when responding to an incident.

- Preparation: Develop a policy approved by management; **Identify critical data and systems**, **single points of failure**; **Train staff on incident response**; Implement an incident response team. (covered in subsequent topic); Practice Incident Identification. (First Response); Identify Roles and Responsibilities; Plan the coordination of communication between stakeholders; **Consider the possibility that a primary method of communication may not be available.**
- Detection and Analysis: Monitor all possible attack vectors; Analyze incident using known data and threat intelligence; Prioritize incident response; Standardize incident documentation;
- Containment, eradication and recovery: Gather evidence; Choose an appropriate containment strategy; Identify the attacker; Isolate the attack.
- Post-incident activity: Identify evidence that may need to be retained. Document lessons learned. Retrospective, Preparation, Detection and Analysis, Containment, Eradication and Recovery Post-incident Activity.

Incident Response Team

Along with the organizational need to establish a **Security Operations Center (SOC)** is the need to create a suitable **incident response team**. A typical incident response team is a cross-functional group of individuals who represent the management, technical and functional areas of responsibility most directly impacted by a security incident. Potential team members include the following:

- Representative(s) of senior management
- Information security professionals
- Legal representatives
- Public affairs/communications representatives
- Engineering representatives (system and network)

Team members should have training on incident response and the organization's incident response plan. Typically, team members assist with **investigating the incident**, **assessing the damage**, **collecting evidence**, **reporting the incident and initiating recovery procedures**. They would also participate in the remediation and lessons learned stages and help with root cause analysis.

Many organizations now have a dedicated team responsible for investigating any computer security incidents that take place. These teams are commonly known as computer incident response teams (CIRTs) or computer security incident response teams (CSIRTs). When an incident occurs, the response team has four primary responsibilities:

- Determine the amount and scope of damage caused by the incident.
- Determine whether any confidential information was compromised during the incident.
- Implement any necessary recovery procedures to restore security and recover from incident-related damage.
- Supervise the implementation of any additional security measures necessary to improve security and prevent recurrence of the incident.

Module 2 Understand Business Continuity (BC)

Domain D2.1.1, D2.1.2, D2.1.3

The Importance of Business Continuity

The intent of a **business continuity plan** is **to sustain business operations while recovering from a significant disruption**. A key part of the plan is **communication**, including multiple contact methodologies and backup numbers in case of a disruption of power or communications. Many organizations will establish a phone tree, so that if one person is not available, they know who else to call.

Management must be included, because sometimes priorities may change depending on the situation. Individuals with proper authority must be there to execute operations, for instance, **if there**

are critical areas that need to be shut down. **We need to have at hand the critical contact numbers for the supply chain**, as well as law enforcement and other sites outside of the facility. For example, a hospital may suffer a severe cyberattack that affects communications from the pharmacy, the internet or phone lines. In the United States, in case of this type of cyberattack that knocks out communications, specific numbers in specific networks can bypass the normal cell phone services and use military-grade networks. Those will be assigned to authorized individuals for hospitals or other critical infrastructures in case of a major disruption or cyberattack, so they can still maintain essential activity.

Components of a Business Continuity Plan

Business continuity planning (BCP) is the **proactive development of procedures to restore business operations after a disaster or other significant disruption to the organization**. Members from across the organization should participate in creating the BCP to ensure all systems, processes and operations are accounted for in the plan. **In order to safeguard the confidentiality, integrity and availability of information, the technology must align with the business needs**.

- List of the BCP team members, including multiple contact methods and backup members
- Immediate response procedures and checklists (security and safety procedures, fire suppression procedures, notification of appropriate emergency-response agencies, etc.)
- Notification systems and call trees for alerting personnel that the BCP is being enacted
- Guidance for management, including designation of authority for specific managers
- How/when to enact the plan. It's important to include when and how the plan will be used.
- Contact numbers for critical members of the supply chain (vendors, customers, possible external emergency providers, third-party partners)

How often should an organization test its business continuity plan (BCP)?

Routinely. Each individual organization must determine how often to test its BCP, but it should be tested at predefined intervals as well as when significant changes happen within the business environment.

Module 3: Understand Disaster Recovery (DR)

Domain D2.2, D2.2.1, D2.2.2, D2.2.3

The Goal of Disaster Recovery

Disaster recovery planning **steps in where BC leaves off**. When a disaster strikes or an interruption of business activities occurs, the Disaster recovery plan (DRP) guides the actions of emergency response personnel **until the end goal is reached—which is to see the business restored to full last-known reliable operations.** Disaster recovery refers specifically to **restoring the information technology and communications services and systems needed by an organization**, **both during the period of**

disruption caused by any event and during restoration of normal services. The recovery of a business function may be done independently of the recovery of IT and communications services; however, the recovery of IT is often crucial to the recovery and sustainment of business operations. Whereas business continuity planning is about maintaining critical business functions, disaster recovery planning is about restoring IT and communications back to full operations after a disruption.

Components of a Disaster Recovery Plan

- Executive summary providing a high-level overview of the plan
- Department-specific plans
- Technical guides for IT personnel responsible for implementing and maintaining critical backup systems
- Full copies of the plan for critical disaster recovery team members
- Checklists for certain individuals:
    - Critical disaster recovery team members will have checklists to help guide their actions amid the chaotic atmosphere of a disaster.
    - IT personnel will have technical guides helping them get the alternate sites up and running.
    - Managers and public relations personnel will have simple-to-follow, high-level documents to help them communicate the issue accurately without requiring input from team members who are busy working on the recovery.
- Executive management should approve the plan and should be provided with a high-level summary of the plan.
- Public Relations should be a member of the disaster recovery plan to handle communications to all stakeholders.
- IT Personnel are primarily responsible for the disaster recovery team.