L2 Incident Response, Business Continuity and Disaster Recovery Concepts 事件應變、業務持續營運和災難恢復概念

Introduction

- When we're talking about IR, BC and DR, we're focus on availability, which is accomplished through those concepts.
    - 當我們正在談論有關事件應變、業務連續性和災難恢復，我們專注於可用性，這是通過這些概念實現的。
- **Incident Response** (IR) plan responds to unexpected changes in operating conditions to keep the business operating;
    - 事件應變計劃是為了應對營運環境的意外變化，以確保業務的正常運作；
- **Business Continuity** (BC) plan enables the business to continue operating throughout the crisis;
    - 業務持續營運（BC）計劃能夠使企業在危機期間繼續運作；
- **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.
    - 災害恢復（DR）計劃在事件應變和業務持續運營計劃失效時啟動，以幫助企業盡快恢復正常運營

Module 1: Understand Incident Response 了解事件應變

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

Incident Terminology 事件術語

- **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.

    - 違反（NIST SP 800-53 Rev. 5）：控制失去、危害、未經授權揭露、未經授權取得或任何類似事件，其中：非授權使用者存取或潛在存取個人身份資訊；或授權使用者以非授權目的存取個人身份資訊。

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

    - 事件（NIST SP 800-61 Rev 2）：在網路或系統中的任何可觀察的發生。

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

    - Exploit：特定的攻擊。之所以被稱為這個名字，是因為這些攻擊利用系統漏洞。

- **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.

    - 事件：實際上或潛在地危及資訊系統的機密性、完整性或可用性，或危及系統所處理、儲存或傳輸的資訊。

- **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.

    - 入侵（IETF RFC 4949 Ver 2）：安全事件或多個事件的組合，構成一種故意的安全事件，其中入侵者未經授權地獲得或試圖獲得對系統或系統資源的存取。

- **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.

    - 威脅（NIST SP 800-30 Rev 1）：任何可能對組織運營（包括使命、功能、形象或聲譽）、組織資產、個人、其他組織或國家造成不利影響的情況或事件，透過未經授權存取、破壞、揭露、修改資訊和/或拒絕服務等方式，透過資訊系統來實現。

- **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.

    - 弱點（NIST SP 800-30 Rev 1）：資訊系統、系統安全程序、內部控制或實施中的缺陷，可能被威脅來源利用的漏洞。

- **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.

    - 零日：一個先前未知的系統漏洞，由於通常不符合公認的模式、特徵或方法，因此有潛在的被利用的可能性，而且不易被檢測或預防。

The Goal of Incident Response 事件應變的目標

- 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).
    - 任何事件回應的首要目標是保護生命、健康和安全。在做出任何與優先順序相關的決策時，始終要優先選擇安全。事件管理的主要目標是做好準備。準備工作包括制定政策和應變計劃，將組織引領度過危機。有些組織使用「危機管理」一詞來描述這個過程，所以你可能也會聽到這個術語。事件是指任何可量測的發生，大多數事件都是無害的。然而，如果該事件有潛力干擾企業的使命，那麼就被稱為事件。**每個組織都必須擁有一個事件回應計劃，以幫助保護業務的可行性

和生存能力。**事件回應過程旨在減少事件的影響，使組織能夠盡快恢復中斷的運營。請注意，事件回應計劃是業務持續管理（BCM）的一個子集。

Components of the Incident Response Plan 事件應變計劃的組成部分

- 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.
    - 事件回應政策應引用事件回應計劃，所有員工根據其在過程中的角色遵循該計劃。該計劃可能包含多個與事件回應相關的程序和標準。它是組織事件回應政策的具體體現。組織的願景、策略和使命應該塑造事件回應過程。實施計劃的程序應該定義技術過程、技巧、檢查清單和其他工具，團隊在回應事件時將使用這些工具。
- 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.**
    - 準備工作：制定經管理層批准的政策；識別關鍵資料和系統，單一故障點；培訓員工進行事件回應；建立事件回應團隊（在後續主題中介紹）；實踐事件識別（第一反應）；確定角色和責任；計劃利害關係者之間的溝通協調；考慮主要溝通方法可能無法使用的可能性。
- Detection and Analysis: Monitor all possible attack vectors; Analyze incident using known data and threat intelligence; Prioritize incident response; Standardize incident documentation;
    - 偵測與分析：監控所有可能的攻擊向量；使用已知資料和威脅情報分析事件；優先處理事件回應；標準化事件文件記錄
- Containment, eradication and recovery: Gather evidence; Choose an appropriate containment strategy; Identify the attacker; Isolate the attack.
    - 遏制、清除和恢復：收集證據；選擇適當的遏制策略；識別攻擊者；隔離攻擊。
- 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.
    - 事後活動：識別可能需要保留的證據。記錄吸取的教訓。事後活動包括回顧、準備、偵測與分析、遏制、清除和恢復。

Incident Response Team 事件應變小組

- 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:

  - 在建立一個安全操作中心（SOC）的組織需求之外，還需要建立一個適合的事件回應團隊。典型的事件回應團隊是一個跨功能的小組，由各個代表管理、技術和功能領域負責的成員組成，這些領域直接受到安全事件的影響。潛在的團隊成員包括以下人員：

- Representative(s) of senior management
  - 資深管理層代表
- Information security professionals
  - 資訊安全專業人員
- Legal representatives
  - 法定代表人
- Public affairs/communications representatives
  - 公共事務/傳播代表
- Engineering representatives (system and network)
  - 工程代表（系統和網絡）
- 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.
  - 團隊成員應該接受有關事件回應和組織事件回應計劃的培訓。通常，團隊成員協助調查事件，評估損害，收集證據，報告事件並啟動恢復程序。他們還將參與糾正措施和吸取教訓階段，並協助進行根本原因分析。
- 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:
  - 現在許多組織都有專門負責調查發生的電腦安全事件的團隊。這些團隊通常被稱為電腦事件回應團隊（CIRT）或電腦安全事件回應團隊（CSIRT）。當發生事件時，回應團隊有四個主要責任：
- Determine the amount and scope of damage caused by the incident.
  - 確定事件造成的損害程度和範圍。
- Determine whether any confidential information was compromised during the incident.
  - 確定事件期間是否有任何機密資訊被洩露。
- Implement any necessary recovery procedures to restore security and recover from incident-related damage.
  - 實施任何必要的恢復程序，以恢復安全並從與事件相關的損害中恢復。

- Supervise the implementation of any additional security measures necessary to improve security and prevent recurrence of the incident.
    - 監督實施任何額外的安全措施，以提高安全性並防止事件再次發生。

Module 2 Understand Business Continuity (BC) 了解業務持續營運

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

The Importance of Business Continuity 業務連續性的重要性

- 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.
    - 業務持續運營計劃的目的是在從重大中斷中恢復的同時維持業務運營。計劃的重要組成部分是溝通，包括在電力或通訊中斷的情況下的多種聯繫方式和備用號碼。許多組織將建立一個電話樹，這樣如果某人不可用，他們就知道應該聯繫誰。
- **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.
    - 管理層必須參與其中，因為有時候優先事項可能根據情況而變化。必須有具有適當權限的人員在場執行操作，例如，如果有需要關閉的關鍵區域。我們需要掌握供應鏈的關鍵聯繫號碼，以及法執和設施外的其他機構的聯繫號碼。例如，醫院可能遭受重大的網絡攻擊，影響了藥房、互聯網或電話線的通訊。在美國，如果發生這種導致通訊中斷的網絡攻擊，特定網絡中的特定號碼可以繞過正常的手機服務，使用軍事級網絡。這些號碼將分配給醫院或其他重要基礎設施的授權人員，在發生重大中斷或網絡攻擊時，他們仍然可以維持基本活動。

Components of a Business Continuity Plan 業務連續性計劃的組成部分

- **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**.
    - 業務持續性規劃（BCP）是在災難或組織遭受重大中斷後，主動開發恢復業務運營的程序。來自組織各部門的成員應該參與制定BCP，以確保計劃中涵蓋了所有系統、流程和運營。為了保護信息的保密性、完整性和可用性，技術必須與業務需求相符。

- List of the BCP team members, including multiple contact methods and backup members
    - BCP團隊成員名單，包括多種聯繫方式和備用成員
- Immediate response procedures and checklists (security and safety procedures, fire suppression procedures, notification of appropriate emergency-response agencies, etc.)
    - 即時應變程序和檢查清單（安全程序和安全程序、滅火程序、通知相關應急機構等）
- Notification systems and call trees for alerting personnel that the BCP is being enacted
    - 通知系統和呼叫樹，用於通知人員啟動BCP。
- Guidance for management, including designation of authority for specific managers
    - 針對管理層的指導，包括指定特定經理的職權。
- How/when to enact the plan. It's important to include when and how the plan will be used.
    - 計劃如何/何時啟動。重要的是包括計劃的使用時間和方式。
- Contact numbers for critical members of the supply chain (vendors, customers, possible external emergency providers, third-party partners)
    - 供應鏈中關鍵成員（供應商、客戶、可能的外部應急提供者、第三方合作伙伴）的聯繫號碼。

How often should an organization test its business continuity plan (BCP)? 一個組織應該多久測試其業務持續性計劃（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.
    - 定期進行測試。每個組織都需要自行確定測試業務持續性計劃（BCP）的頻率，但應在預定間隔進行測試，同時在業務環境發生重大變化時進行測試。

Module 3: Understand Disaster Recovery (DR) 了解災難恢復

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

The Goal of Disaster Recovery 災難恢復的目標

- 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.
    - 當業務持續性計劃（BCP）無法滿足需求時，災難恢復計劃（DRP）介入。當災難發生或業務活動中斷時，災難恢復計劃指導緊急應急人員的行動，直到實現最終目標，即將業務恢復到完全恢復到最後已知可靠操作狀態。災難恢復專指恢復組織所需的信息技術和通信服務與系統，無論是在任何事件引起的中斷期間還是在恢復正常服務期間。恢復業務功能可以獨立於IT和通信服務的恢復進行，但IT的恢復通常對業務運營的恢復和維持至關重要。而業務持續性計劃是關於維護關鍵業務功能，災難恢復計劃則是在中斷後將IT和通信恢復到正常運營。

Components of a Disaster Recovery Plan 災難恢復計劃的元件

- Executive summary providing a high-level overview of the plan
    - 高層次概述提供計劃的概要。
- Department-specific plans
    - 各部門專用計劃
- Technical guides for IT personnel responsible for implementing and maintaining critical backup systems
    - 針對負責實施和維護關鍵備份系統的IT人員的技術指南。
- Full copies of the plan for critical disaster recovery team members
    - 提供給關鍵災難恢復團隊成員的完整計劃副本。
- Checklists for certain individuals: 針對特定個人的檢查清單
    - Critical disaster recovery team members will have checklists to help guide their actions amid the chaotic atmosphere of a disaster.
        - 關鍵災難恢復團隊成員將擁有檢查清單，以協助他們在災難的混亂環境中指引行動。
    - IT personnel will have technical guides helping them get the alternate sites up and running.
        - IT人員將擁有技術指南，以幫助他們啟動並運行替代性的場所。
    - 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.
        - 經理和公共關係人員將擁有簡單易懂的高層文件，以幫助他們在不需要忙於恢復工作的團隊成員的參與下，準確地傳達問題。
- Executive management should approve the plan and should be provided with a high-level summary of the plan.
    - 執行管理層應核准該計劃並應提供一份高層摘要。
- Public Relations should be a member of the disaster recovery plan to handle communications to all stakeholders.
    - 公共關係應該是災難恢復計劃的成員，負責與所有利益相關方進行溝通。
- IT Personnel are primarily responsible for the disaster recovery team.
    - IT人員主要負責災難恢復團隊的工作。