L5 Security Operations 安全運營

Module 1: Understand Data Security 了解數據安全

Domain D5.0, D5.1.1, D5.1.2, D5.1.3

- **Hardening** is the process of applying secure configurations (to reduce the attack surface) and locking down various hardware, communications systems and software, including the operating system, web server, application server and applications, etc. This module introduces configuration management practices that will ensure systems are installed and maintained according to industry and organizational security standards.
    - 「硬化（Hardening）」是一個過程，其中應用安全配置（以減少攻擊面）並鎖定各種硬件、通信系統和軟件，包括操作系統、Web伺服器、應用伺服器和應用程式等。本模組介紹了配置管理的實踐，確保系統根據行業和組織的安全標準進行安裝和維護。

Data Handling 數據處理

- Data itself goes through **its own life cycle as users create**, **use**, **share and modify it**. The data security life cycle model is useful because **it can align easily with the different roles that people and organizations perform during the evolution of data from creation to destruction (or disposal)**. It also helps put the different **data states of in use, at rest and in motion, into context**.
    - 資料本身會在使用者創建、使用、分享和修改的過程中經歷自己的生命周期。資料安全生命周期模型非常有用，因為它可以與不同的角色在資料從創建到銷毀（或處置）的演化過程中所執行的不同角色相融合。它還有助於將資料在使用中、靜態和移動中的不同狀態放入上下文中。
- All ideas, data, information or knowledge can be thought of as going through six major sets of activities throughout its lifetime. Conceptually, these involve: 所有觀念、資料、訊息或知識在其生命週期中可以被視為經歷六個主要的活動集合。從概念上講，這些活動包括：
    1. Creating the knowledge, which is usually tacit knowledge at this point.
        - 創造知識，這通常是隱性知識的階段。
    2. Storing or recording it in some fashion (which makes it explicit).
        - 以某種方式存儲或記錄它（使其變得明確）。
    3. Using the knowledge, which may cause the information to be modified, supplemented or partially deleted.
        - 使用這個知識，可能會導致信息被修改、補充或部分刪除。
    4. Sharing the data with other users, whether as a copy or by moving the data from one location to another.
        - 將數據與其他用戶分享，無論是作為副本還是通過將數據從一個位置移動到另一個位置。
    5. Archiving the data when it is temporarily not needed.
        - 將數據存檔，當暫時不需要時使用。
    6. Destroying the data when it is no longer needed.
        - 數據不再需要時，銷毀該數據。

Data Handling Practices 數據處理實踐

- **Classification**: classifications dictate **rules and restrictions about how that information can be used**, **stored** or **shared with others**. All of this is done to keep the temporary value and importance of that information from leaking away. Classification of data, which asks the question “Is it secret?” determines the labeling, handling and use of all data. **Classification is the process of recognizing the organizational impacts if the information suffers any security compromises related to its characteristics of confidentiality**, **integrity** and **availability**. **Information is then labeled and handled accordingly**. Classifications are derived from laws, regulations, contract-specified standards or other business expectations. One classification might indicate “minor, may disrupt some processes” while a more extreme one might be “grave, could lead to loss of life or threaten ongoing existence of the organization.” These descriptions should reflect the ways in which the organization has chosen (or been mandated) to characterize and manage risks. The immediate benefit of classification is that it can lead to more efficient design and implementation of security processes, if we can treat the protection needs for all similarly classified information with the same controls strategy.
    - 分類：分類規定了關於信息使用、存儲或與他人共享的規則和限制。所有這些都是為了防止信息的暫時價值和重要性外泄。數據的分類，即“它是秘密的嗎？”確定了所有數據的標記、處理和使用方式。分類是識別信息的機密性、完整性和可用性特徵受到任何安全威脅影響對組織的影響的過程。然後，根據這些特徵對信息進行標記和處理。分類來源於法律、法規、合同指定的標準或其他業務期望。一個分類可能表示“輕微，可能干擾一些流程”，而一個更極端的分類可能是“嚴重，可能導致生命損失或威脅組織的持續存在”。這些描述應該反映出組織選擇（或被授權）的風險特徵和管理方式。分類的直接好處是，如果我們可以將同樣分類的信息的保護需求與相同的控制策略相結合，它可以促使安全流程的更高效設計和實施。
- **Labeling**: **security labels are part of implementing controls to protect classified information**. It is reasonable to want a simple way of assigning a level of sensitivity to a data asset, such that the higher the level, the greater the presumed harm to the organization, and thus the greater security protection the data asset requires. This spectrum of needs is useful, but it should not be taken to mean that clear and precise boundaries exist between the use of “low sensitivity” and “moderate sensitivity” labeling, for example. 標記：安全標籤是實施保護分類信息控制的一部分。我們希望能夠簡單地對數據資源進行敏感性級別的劃分，高級別表示對組織的潛在傷害更大，因此對數據資源的安全保護要求也更高。這種需求的譜系很有用，但不應該認為“低敏感性”和“中等敏感性”標記之間存在明確而精確的界線。
    - **Data Sensitivity Levels and Labels**: unless otherwise mandated, organizations are free to create classification systems that best meet their own needs. In professional practice, it is typically best if the organization has enough classifications to distinguish between sets of assets with differing sensitivity/value, but not so many classifications that the distinction between them is confusing to individuals. Typically, two or three classifications are manageable, and more than four tend to be difficult.
        - 數據敏感性級別和標籤：除非另有要求，組織可以自由制定最符合其需求的分類系統。在專業實踐中，通常最好的做法是組織擁有足夠的分類，以區分具有不同敏感性/價值的資產集，但不要有太多分類，以免對個人造成混淆。通常，管理兩到三個分類比較容易，而超過四個則往往很困難。
    - **Highly restricted**: Compromise of data with this sensitivity label could possibly put the organization’s future existence at risk. Compromise could lead to substantial loss of life, injury

or property damage, and the litigation and claims that would follow.

        - 極度限制: 具有此敏感性標籤的資料遭到破壞可能會對組織的未來存在造成風險。遭到破壞可能導致重大的生命、傷害或財產損害，以及隨之而來的訴訟和索賠。

    - **Moderately restricted**: Compromise of data with this sensitivity label could lead to loss of temporary competitive advantage, loss of revenue or disruption of planned investments or activities.

        - 中度限制: 具有此敏感性標籤的資料遭到破壞可能導致暫時競爭優勢的損失、收入損失或計劃中的投資或活動受到干擾。

    - **Low sensitivity (sometimes called "internal use only")**: Compromise of data with this sensitivity label could cause minor disruptions, delays or impacts.

        - 低敏感性（有時稱為「僅供內部使用」）：具有此敏感性標籤的資料遭到破壞可能會導致輕微的干擾、延誤或影響。

    - Unrestricted public data: As this data is already published, no harm can come from further dissemination or disclosure.

        - 不受限制的公開資料: 由於這些資料已經公開，進一步傳播或披露不會造成任何損害。

- **Retention**: **Information and data should be kept only for as long as it is beneficial, no more and no less**. Certain industry standards, laws and regulations define retention periods, when such external requirements are not set, it is an organization's responsibility to define and implement its own data retention policy. **Data retention policies are applicable both for hard copies and for electronic data**, and no data should be kept beyond its required or useful life. **Security professionals should ensure that data destruction is being performed when an asset has reached its retention limit**. For the security professional to succeed in this assignment, an accurate inventory must be maintained, including the asset location, retention period requirement, and destruction requirements. Organizations should conduct a periodic review of retained records in order to reduce the volume of information stored and to ensure that only necessary information is preserved.

    - 保留期: 資訊和資料應該只保留在有益的時間範圍內，既不多也不少。某些行業標準、法律和法規會定義保留期限，當沒有外部要求時，組織有責任自行定義和實施自己的資料保留政策。資料保留政策適用於紙本和電子資料，且不應超過其所需或有用的生命週期。安全專業人員應確保當資產達到保留限制時進行資料銷毀。為了使安全專業人員在這項任務中成功，必須維護準確的資產清單，包括資產位置、保留期要求和銷毀要求。組織應定期審查保留的記錄，以減少儲存的資訊量，確保只保留必要的資訊。

- Records retention policies indicate how long an organization is required to maintain information and assets. Policies should guarantee that: 記錄保留政策指示組織需要保留資訊和資產的時間長短。政策應該確保：

    - Personnel understand the various retention requirements for data of different types throughout the organization.
        - 人員了解組織內各種類型資料的保留要求。

    - The organization appropriately documents the retention requirements for each type of information.
        - 組織適當地記錄每種類型資訊的保留要求。
    - The systems, processes and individuals of the organization retain information in accordance with the required schedule but no longer.
        - 組織的系統、流程和個人按照所需的時間表保留資訊，但不超過這個期限。
    - A common mistake in records retention is applying the longest retention period to all types of information in an organization. This not only wastes storage but also increases risk of data exposure and adds unnecessary “noise” when searching or processing information in search of relevant records. It may also be in violation of externally mandated requirements such as legislation, regulations or contracts (which may result in fines or other judgments). Records and information no longer mandated to be retained should be destroyed in accordance with the policies of the enterprise and any appropriate legal requirements that may need to be considered.
        - 在記錄保留中的一個常見錯誤是將最長的保留期適用於組織中的所有資訊類型。這不僅浪費存儲空間，還增加了資料曝露的風險，並在搜索或處理資訊以尋找相關記錄時增加了不必要的「噪音」。這可能違反外部強制性要求，例如法律、法規或合同（可能導致罰款或其他判決）。不再需要保留的記錄和資訊應根據企業的政策和任何適用的法律要求進行銷毀，這些要求可能需要考慮。

- Destruction: Data that might be left on media after deleting is known as remanence and may be a significant security concern. Steps must be taken to reduce the risk that data remanence could compromise sensitive information to an acceptable level. This can be done by one of several means:
銷毀：在刪除後可能在媒體上留下的資料稱為殘留數據，可能是一個重要的安全問題。必須採取措施將資料殘留的風險降低到可接受的水平，以防止其危害敏感資訊。可以通過以下幾種方式之一來實現：

    - Clearing the device or system, which usually involves **writing multiple patterns of random values throughout all storage media**. This is sometimes **called “overwriting” or “zeroizing” the system**, although writing zeros has the risk that a missed block or storage extent may still contain recoverable, sensitive information after the process is completed.
        - 清除設備或系統，通常包括在所有儲存媒體上寫入多種隨機值模式。這有時被稱為「覆寫」或「清零系統」，儘管寫入零值的風險是，即使在完成過程後，可能仍有遺漏的區塊或儲存範圍中包含可恢復的敏感資訊。
    - Purging the device or system, which eliminates (or greatly reduces) the chance that residual physical effects from the writing of the original data values may still be recovered, even after the system is cleared. Some magnetic disk storage technologies, for example, can still have residual “ghosts” of data on their surfaces even after being overwritten multiple times. Magnetic media, for example, can often be altered sufficiently to meet security requirements; in more stringent cases, degaussing may not be sufficient.
        - 清除設備或系統，可以消除（或大幅減少）原始資料值寫入後，仍有可能被恢復的殘留物理效應。例如，某些磁碟儲存技術即使經過多次覆寫後，表面仍可能保留著資料的殘留痕跡。例如，磁性媒體通常可以進行足夠的改變以符合安全需求；在更嚴格的情況下，消磁可能不足夠。
    - Physical destruction of the device or system is the ultimate remedy to data remanence. Magnetic or optical disks and some flash drive technologies may require being mechanically

shredded, chopped or broken up, etched in acid or burned; their remains may be buried in protected landfills, in some cases.
        - 對設備或系統進行物理破壞是解決資料殘留問題的終極方法。磁性或光學磁碟和某些快閃記憶體技術可能需要進行機械粉碎、切割、破壞、用酸蝕刻或燒毀；它們的殘骸可能被埋藏在受保護的垃圾掩埋場中，某些情況下可能需要這樣處理。
    - In many routine operational environments, security considerations may accept that clearing a system is sufficient. But when systems elements are to be removed and replaced, either as part of maintenance upgrades or for disposal, purging or destruction may be required to protect sensitive information from being compromised by an attacker.
        - 在許多例行的運營環境中，安全考慮通常會接受清除系統的做法。但是，當系統元素需要被移除和更換時，無論是作為維護升級的一部分還是處理棄置，為了保護敏感信息不被攻擊者破壞，可能需要進行清除、清除或銷毀等措施。

Logging and Monitoring Security Events 記錄和監控安全事件

- Logging is the primary form of instrumentation that attempts to capture signals generated by events. Events are any actions that take place within the systems environment and cause measurable or observable change in one or more elements or resources within the system. **Logging imposes a computational cost but is invaluable when determining accountability**. Proper design of logging environments and regular log reviews remain best practices regardless of the type of computer system.
    - 記錄是一種主要的儀器，試圖捕捉事件生成的信號。事件是在系統環境中發生的任何行動，並導致系統內的一個或多個元素或資源發生可測量或可觀察的變化。記錄會帶來計算成本，但在確定責任方面非常寶貴。不論計算機系統的類型如何，適當設計記錄環境並定期審查日誌仍然是最佳做法。
- Major controls frameworks emphasize the importance of organizational logging practices. Information that may be relevant to being recorded and reviewed include (but is not limited to): user IDs, system activities, dates/times of key events (e.g., logon and logoff), device and location identity, successful and rejected system and resource access attempts, system configuration changes and system protection activation and deactivation events.
    - 主要的控制框架強調組織的記錄實踐的重要性。可能需要記錄和審查的相關信息包括（但不限於）：用戶ID、系統活動、關鍵事件的日期/時間（例如，登錄和登出）、設備和位置識別、成功和被拒絕的系統和資源訪問嘗試、系統配置更改以及系統保護啟用和停用事件。
- **Logging and monitoring the health of the information environment is essential to identifying inefficient or improperly performing systems**, detecting compromises and providing a record of how systems are used. **Robust logging practices provide tools to effectively correlate information from diverse systems to fully understand the relationship between one activity and another**.
    - 記錄和監控信息環境的健康狀態對於識別效率低下或運行不正確的系統、檢測侵害以及記錄系統使用方式至關重要。強大的記錄實踐提供了有效地將來自不同系統的信息相關聯的工具，以充分理解一個活動與另一個活動之間的關係。
- Log reviews are an essential function not only for security assessment and testing but also **for identifying security incidents, policy violations, fraudulent activities and operational problems**

near the time of occurrence. Log reviews support audits – forensic analysis related to internal and external investigations – and provide support for organizational security baselines. Review of historic audit logs can determine if a vulnerability identified in a system has been previously exploited.

    - 日誌審查是一項重要的功能，不僅用於安全評估和測試，還用於在事件發生時識別安全事件、政策違規、詐騙活動和操作問題。日誌審查支持審計-與內部和外部調查相關的法庭分析-並為組織的安全基準提供支持。審查歷史審計日誌可以確定系統中發現的漏洞是否曾經被利用過。

- It is helpful for an organization to create components of a log management infrastructure and determine how these components interact. This aids in preserving the integrity of log data from accidental or intentional modification or deletion and in maintaining the confidentiality of log data.

    - 對於組織來說，建立日誌管理基礎設施的組件並確定這些組件之間的互動方式是很有幫助的。這有助於保護日誌數據的完整性，避免意外或故意的修改或刪除，並保持日誌數據的保密性。

- Controls are implemented to protect against unauthorized changes to log information. Operational problems with the logging facility are often related to alterations to the messages that are recorded, log files being edited or deleted, and storage capacity of log file media being exceeded. Organizations must maintain adherence to retention policy for logs as prescribed by law, regulations and corporate governance. Since attackers want to hide the evidence of their attack, the organization's policies and procedures should also address the preservation of original logs. Additionally, the logs contain valuable and sensitive information about the organization. Appropriate measures must be taken to protect the log data from malicious use.

    - 實施控制措施以防止對日誌信息進行未授權的更改。與日誌記錄相關的操作問題通常涉及記錄的消息被修改、日誌文件被編輯或刪除，以及日誌文件媒體的存儲容量超過限制。組織必須根據法律、法規和公司治理的規定，保持對日誌的保留政策的遵守。由於攻擊者希望隱藏他們的攻擊證據，組織的政策和程序還應該涉及原始日誌的保留。此外，日誌中包含組織的有價值和敏感信息。必須採取適當的措施保護日誌數據免受惡意使用。

Event Logging Best Practices 事件記錄最佳實踐

- Different tools are used depending on whether the risk from the attack is from traffic coming into or leaving the infrastructure.

    - 根據攻擊對基礎設施的風險是來自進入還是離開的流量，使用不同的工具。

- **Ingress monitoring refers to surveillance and assessment of all inbound communications traffic and access attempts.** Devices and tools that offer logging and alerting opportunities for ingress monitoring include: Firewalls, Gateways, Remote authentication servers, IDS/IPS tools, SIEM solutions, Anti-malware solutions.

    - 入口監控是指對所有入站通信流量和訪問嘗試進行監視和評估。提供入口監控的設備和工具包括：防火牆、閘道器、遠程驗證伺服器、入侵檢測/防禦系統工具、安全資訊和事件管理解決方案，以及防惡意軟體解決方案。

- **Egress monitoring is used to regulate data leaving the organization's IT environment.** The term currently used in conjunction with this effort is **data loss prevention (DLP)** or **data leak protection**. The DLP solution should be deployed so that it can inspect all forms of data leaving the organization,

including: Email (content and attachments), Copy to portable media, File Transfer Protocol (FTP), Posting to web pages/websites, Applications/application programming interfaces (APIs).

    - 出口監控用於監管離開組織的資訊科技環境的數據流動。 目前與此相關的術語包括資料遺失防護 (DLP) 或 資料外洩保護。應部署 DLP 解決方案，以檢查所有離開組織的數據形式，包括：電子郵件（內容和附件）、複製到可攜式媒體、檔案傳輸協定 (FTP)、發佈到網頁/網站、應用程式/應用程式介面 (API)

Encryption Overview 加密概述

- Almost every action we take in our modern digital world involves cryptography. Encryption protects our personal and business transactions; digitally signed software updates verify their creator's or supplier's claim to authenticity. Digitally signed contracts, binding on all parties, are routinely exchanged via email without fear of being repudiated later by the sender.
    - 在現代數位世界中，我們幾乎每一個動作都涉及到密碼學。加密保護了我們的個人和商業交易；數位簽名的軟體更新可以驗證其創作者或供應商聲稱的真實性。數位簽署的契約可對所有當事人具有約束力，通常透過電子郵件交換，而不用擔心發送者之後會否否認。
- Cryptography is used to protect information by keeping its meaning or content secret and making it unintelligible to someone who does not have a way to decrypt (unlock) that protected information. The objective of every encryption system is to transform an original set of data, called the plaintext, into an otherwise unintelligible encrypted form, called the ciphertext.
    - 密碼學用於保護資訊，通過保持其含義或內容的秘密性，使其對於沒有解密（解鎖）受保護資訊的方法的人變得難以理解。每個加密系統的目標是將一組原始資料，稱為明文（plaintext），轉換成另一種難以理解的加密形式，稱為密文（ciphertext）。
- **Properly used**, singly or in combination, **cryptographic solutions provide a range of services that can help achieve required systems security postures in many ways**: 適當使用的話，單獨或結合使用，密碼學解決方案可以提供各種服務，以多種方式幫助實現所需的系統安全架構，包括：
    - **confidentiality**: Cryptography provides confidentiality by hiding or obscuring a message so that it cannot be understood by anyone except the intended recipient. Confidentiality keeps information secret from those who are not authorized to have it.
        - 機密性：密碼學通過隱藏或混淆訊息，使其除了預期的接收者之外，無法被任何人理解。機密性可以將資訊對未經授權的人保密。
    - **integrity**: hash functions and digital signatures can provide integrity services that allow a recipient to verify that a message has not been altered by malice or error. These include simple message integrity controls. Any changes, deliberate or accidental, will result in the two results (by sender and by recipient) being different.
        - 完整性：哈希函數和數位簽章可以提供完整性服務，讓接收者驗證訊息未被惡意或錯誤地修改過。這包括簡單的訊息完整性控制。任何變更，無論是故意還是意外，都將導致發送者和接收者的兩個結果不同。

Module 2: Understand System Hardening 了解系統強化

Domain D5.2.1

Configuration Management Overview 配置管理概述

- **Configuration management** is a process and discipline used **to ensure that the only changes made to a system are those that have been authorized and validated**. It is both a decision-making process and a set of control processes. If we look closer at this definition, the basic configuration management process includes components such as **identification**, **baselines**, **updates** and **patches**.
    - 組態管理是一個過程和紀律，用於確保系統上的變更只有經過授權和驗證的變更。它既是一個決策過程，也是一組控制過程。如果我們仔細看這個定義，基本的組態管理過程包括識別、基準線、更新和補丁等組件。
- Configuration Management 配置管理
    1. **Identification**: baseline identification of a system and all its components, interfaces and documentation.
        - 識別：對系統及其所有組件、接口和文件進行基準線識別。
    2. **Baseline**: a security baseline is a minimum level of protection that can be used as a reference point. Baselines provide a way to ensure that updates to technology and architectures are subjected to the minimum understood and acceptable level of security requirements.
        - 基準線：安全基準線是一個最低的保護水平，可用作參考點。基準線提供了一種確保對技術和架構的更新符合最低的已理解和可接受的安全要求的方式。
    3. **Change Control**: An update process for requesting changes to a baseline, by means of making changes to one or more components in that baseline. A review and approval process for all changes. This includes updates and patches.
        - 變更控制：通過對基準線中的一個或多個組件進行更改的方式，請求對基準線進行變更的更新過程。對所有變更進行審查和批准的過程。這包括更新和修補程式。
    4. **Verification & Audit**: A regression and validation process, which may involve testing and analysis, to verify that nothing in the system was broken by a newly applied set of changes. An audit process can validate that the currently in-use baseline matches the sum total of its initial baseline plus all approved changes applied in sequence.
        - 驗證與稽核：回歸和驗證過程，可能涉及測試和分析，以驗證系統中沒有因新應用的一組變更而破壞的內容。稽核過程可以驗證當前使用的基準線是否與初始基準線以及按順序應用的所有已批准變更的總和相符。
- **Effective use of configuration management gives** systems owners, operators, support teams and security professionals another important set of tools they can use to monitor and oversee the configuration of the devices, networks, applications and projects of the organization.An organization may mandate the configuration of equipment **through standards and baselines**. The use of **standards and baselines can ensure that network devices, software, hardware and endpoint devices are configured in a consistent way and that all such devices are compliant with the security baseline established for the organization**. If a device is found that is not compliant with the security baseline, it may be **disabled or isolated into a quarantine area** until it can be **checked and updated**.
    - 有效運用組態管理能夠為系統的擁有者、操作者、支援團隊和安全專業人員提供一套重要的工具，用於監控和監督組織的設備、網路、應用程式和專案的配置。組織可以通過標準和基準線來規定設備的配置。使用標準和基準線可以確保網路設備、軟體、硬體和端點設備以一致的方式進

行配置，並且所有這些設備都符合組織設定的安全基準線。如果發現一個設備不符合安全基準線，可能會將其停用或隔離到隔離區，直到進行檢查和更新為止。

- **Inventory**: Making an inventory, catalog or registry of all the information assets **is the first step in any asset management process**. **You can't protect what you don't know you have**.
    - 庫存管理：建立資訊資產的庫存、目錄或註冊是資產管理過程的第一步。如果不知道自己擁有什麼，就無法保護它們。
- **Baselines**: The baseline **is a total inventory of all the system's components, hardware, software, data, administrative controls, documentation and user instructions**. **All further comparisons and development are measured against the baselines. When protecting assets, baselines can be particularly helpful in achieving a minimal protection level of those assets based on value.** If classifications such as high, medium and low are being used, baselines could be developed for each of our classifications and provide that minimum level of security required for each.
    - 基準線：基準線是系統所有組件、硬體、軟體、資料、行政控制、文件和使用者指引的總庫存。所有進一步的比較和發展都是相對於基準線進行的。在保護資產時，基準線對於基於價值的最低保護水準特別有幫助。如果使用高、中、低等分級，可以為每個分級制定基準線，為每個分級提供所需的最低安全水準。
- Updates: Such modifications **must be acceptance tested to verify that newly installed (or repaired) functionality works as required**. They must also be **regression tested to verify that the modifications did not introduce other erroneous or unexpected behaviors** in the system. **Ongoing security assessment and evaluation testing evaluates whether the same system that passed acceptance testing is still secure**.
    - 更新：這些修改必須經過驗收測試，以驗證新安裝（或修復）的功能是否按要求正常運作。它們還必須進行回歸測試，以驗證修改是否在系統中引入了其他錯誤或意外行為。持續的安全評估和評估測試評估經過驗收測試的系統是否仍然安全。
- Patches: **The challenge for the security professional is maintaining all patches**. **Some patches are critical and should be deployed quickly, while others may not be as critical but should still be deployed because subsequent patches may be dependent on them**. Standards such as the **PCI DSS require organizations to deploy security patches within a certain time frame**. **An organization should test the patch before rolling it out across the organization**. If the patch does not work or has unacceptable effects, it might be necessary to **roll back to a previous (pre-patch) state**. Typically, **the criteria for rollback are previously documented and would automatically be performed when the rollback criteria were met**. The risk of using unattended patching should be weighed against the risk of having unpatched systems in the organization's network. Unattended (or automated) patching might result in unscheduled outages as production systems are taken offline or rebooted as part of the patch process.
    - 修補程式：對於安全專業人員來說，維護所有的修補程式是一項挑戰。有些修補程式非常重要，應該迅速部署，而其他一些修補程式可能沒有那麼重要，但仍應該部署，因為後續的修補程式可能依賴它們。像PCI DSS這樣的標準要求組織在一定的時間範圍內部署安全修補程式。組織在將修補程式推出組織範圍之前，應該進行測試。如果修補程式無效或產生了無法接受的影響，可能需要回滾到之前（未套用修補程式）的狀態。通常，回滾的標準是事先記錄下來的，並且在滿足回滾標準時將自動執行回滾操作。使用無人值守的修補程式應該權衡尚未套用修補程式的系統在

組織網絡中帶來的風險。無人值守（或自動化）的修補程式可能會導致非計劃停機，因為生產系統需要下線或重新啟動以進行修補程式處理。

Module 3: Understand Best Practice Security Policies 了解最佳實踐安全策略

Domain D5.3, D5.3.1, D5.3.2, D5.3.3, D5.3.4, D5.3.5, D5.3.6

- An organization's security policies define what "security" means to that organization, which in almost all cases reflects the tradeoff between security, operability, affordability and potential risk impacts. Security policies express or impose behavioral or other constraints on the system and its use. Well-designed systems operating within these constraints should reduce the potential of security breaches to an acceptable level.
    - 一個組織的安全政策定義了對該組織而言「安全」的意義，幾乎所有情況下都反映了安全、可操作性、負擔能力和潛在風險影響之間的權衡。安全政策對系統及其使用者施加行為或其他限制。在這些限制下運作良好的系統應該將安全漏洞的潛在風險降低到可接受的水平。
- Security governance that does not align properly with organizational goals can lead to implementation of security policies and decisions that unnecessarily inhibit productivity, impose undue costs and hinder strategic intent.
    - 如果安全治理與組織目標不適當地對齊，就可能導致實施安全政策和決策，這些政策和決策無謂地抑制生產力，增加不必要的成本並阻礙戰略意圖。

Common Security Policies 通用安全策略

- All policies must support any regulatory and contractual obligations of the organization. Sometimes it can be challenging to ensure the policy encompasses all requirements while remaining simple enough for users to understand.
    - 所有政策必須支持組織的監管和契約義務。有時候，確保政策包含所有要求，同時對使用者來說足夠簡單易懂，可能是一個具有挑戰性的任務。
- Here are six common security-related policies that exist in most organizations.
    - 以下是大多數組織中存在的六個常見的與安全相關的政策
- Data Handling Policy: Appropriate use of data: This aspect of the policy defines whether data is for use within the company, is restricted for use by only certain roles or can be made public to anyone outside the organization. In addition, some data has associated legal usage definitions. The organization's policy should spell out any such restrictions or refer to the legal definitions as required. Proper data classification also helps the organization comply with pertinent laws and regulations. For example, classifying credit card data as confidential can help ensure compliance with the PCI DSS. One of the requirements of this standard is to encrypt credit card information. Data owners who correctly defined the encryption aspect of their organization's data classification policy will require that the data be encrypted according to the specifications defined in this standard.
    - 資料處理政策：資料的適當使用：該政策的這一方面定義了資料是供公司內部使用，還是僅限特定角色使用，或者可以公開提供給組織外的任何人。此外，某些資料有相關的法律使用定義。組

織的政策應該明確規定這些限制，或根據需要引用法律定義。適當的資料分類還有助於組織遵守相關法律和法規。例如，將信用卡資料分類為機密可以確保符合PCI DSS的要求。該標準的要求之一是對信用卡資訊進行加密。正確定義其組織資料分類政策中的加密方面的資料所有者將要求按照該標準中定義的規格對資料進行加密。

- Password Policy: Every organization should have a password policy in place that defines expectations of systems and users. The password policy should describe senior leadership's commitment to ensuring secure access to data, outline any standards that the organization has selected for password formulation, and identify who is designated to enforce and validate the policy.
    - 密碼政策：每個組織都應該制定一項密碼政策，明確系統和使用者的期望。密碼政策應該描述高級管理層確保安全訪問資料的承諾，概述組織選擇的密碼設定標準，並確定誰負責執行和驗證該政策。
- Acceptable Use Policy (AUP): The acceptable use policy (AUP) defines acceptable use of the organization’s network and computer systems and can help protect the organization from legal action. It should detail the appropriate and approved usage of the organization’s assets, including the IT environment, devices and data. Each employee (or anyone having access to the organization’s assets) should be required to sign a copy of the AUP, preferably in the presence of another employee of the organization, and both parties should keep a copy of the signed AUP.
    - 適用使用政策（AUP）：適用使用政策（AUP）定義了組織網絡和電腦系統的合理使用，有助於保護組織免受法律訴訟。它應詳細說明組織資產的適當和批准使用，包括IT環境、設備和數據。每位員工（或任何能夠訪問組織資產的人）都應該被要求簽署一份AUP的副本，最好在組織的另一名員工的陪同下進行簽署，雙方都應保存簽署的AUP副本。
- Policy aspects commonly included in AUPs: Data access, System access, Data disclosure, Passwords, Data retention, Internet usage, Company device usage
    - 常見包含在AUP中的政策方面：數據訪問、系統訪問、數據披露、密碼、數據保留、互聯網使用、公司設備使用。
- Bring Your Own Device (BYOD): An organization may allow workers to acquire equipment of their choosing and use personally owned equipment for business (and personal) use. This is sometimes called bring your own device (BYOD). Another option is to present the teleworker or employee with a list of approved equipment and require the employee to select one of the products on the trusted list.
    - 自帶設備（BYOD）：組織可能允許員工自行選購設備並將個人擁有的設備用於商業（和個人）用途。這有時被稱為自帶設備（BYOD）。另一個選擇是向遠程工作者或員工提供一份批准的設備清單，並要求員工從受信任的清單中選擇一款產品。
- Letting employees choose the device that is most comfortable for them may be good for employee morale, but it presents additional challenges for the security professional because it means the organization loses some control over standardization and privacy. If employees are allowed to use their phones and laptops for both personal and business use, this can pose a challenge if, for example, the device has to be examined for a forensic audit. It can be hard to ensure that the device is configured securely and does not have any backdoors or other vulnerabilities that could be used to access organizational data or systems.

    - 讓員工選擇對他們最舒適的設備可能有助於提高員工士氣，但對於安全專業人員來說，這也帶來了額外的挑戰，因為這意味著組織失去了一些對標準化和隱私的控制。如果員工被允許將他們的手機和筆記本電腦用於個人和商業用途，這可能帶來一些挑戰，例如，如果需要對設備進行法庭審計，這可能會造成困擾。很難確保設備配置安全，並且沒有任何後門或其他漏洞，可用於訪問組織的數據或系統。

- All employees must read and agree to adhere to this policy before any access to the systems, network and/or data is allowed. If and when the workforce grows, so too will the problems with BYOD. Certainly, the appropriate tools are going to be necessary to manage the use of and security around BYOD devices and usage. The organization needs to establish clear user expectations and set the appropriate business rules.

    - 在允許訪問系統、網絡和/或數據之前，所有員工必須閱讀並同意遵守該政策。如果員工人數增加，使用BYOD的問題也將隨之增加。當然，將需要適當的工具來管理BYOD設備和使用的安全性。組織需要建立清晰的用戶期望並設定適當的業務規則。

- Privacy Policy: Often, personnel have access to personally identifiable information (PII) (also referred to as electronic protected health information [ePHI] in the health industry). It is imperative that the organization documents that the personnel understand and acknowledge the organization's policies and procedures for handling of that type of information and are made aware of the legal repercussions of handling such sensitive data. This type of documentation is similar to the AUP but is specific to privacy-related data.

    - 隱私政策：通常，人員可以訪問包含個人身份信息（PII）的數據（在醫療行業中也稱為電子受保護的健康信息[ePHI]）。組織必須記錄人員對處理該類信息的組織政策和程序的理解和認可，並讓他們了解處理此類敏感數據的法律後果。這種文檔與AUP類似，但專門涉及與隱私相關的數據。

- The organization's privacy policy should stipulate which information is considered PII/ePHI, the appropriate handling procedures and mechanisms used by the organization, how the user is expected to perform in accordance with the stated policy and procedures, any enforcement mechanisms and punitive measures for failure to comply as well as references to applicable regulations and legislation to which the organization is subject. This can include national and international laws, such as the GDPR in the EU and Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada; laws for specific industries in certain countries such as HIPAA and Gramm–Leach–Bliley Act (GLBA); or local laws in which the organization operates.

    - 組織的隱私政策應規定哪些信息被視為PII/ePHI，組織使用的適當處理程序和機制，用戶應按照所述政策和程序執行的期望，任何執行機制和對未能遵守的懲罰措施，以及組織受到的適用法規和法律的參考。這可能包括國家和國際法律，如歐盟的GDPR和加拿大的個人信息保護和電子文件法（PIPEDA）；某些國家特定行業的法律，如HIPAA和格拉姆-利奇-布萊利法（GLBA）；或組織所在地的地方法律。

- The organization should also create a public document that explains how private information is used, both internally and externally. For example, it may be required that a medical provider present patients with a description of how the provider will protect their information (or a reference to where they can find this description, such as the provider's website).

    - 該組織還應該創建一份公開文件，解釋私人信息在內部和外部的使用方式。例如，可能需要醫療服務提供者向患者提供有關該提供者如何保護其信息的描述（或提供該描述的參考資料，例如提供者的網站）。

- Change Management Policy: Change management is the discipline of transitioning from the current state to a future state. It consists of three major activities: deciding to change, making the change, and confirming that the change has been correctly accomplished. Change management focuses on making the decision to change and results in the approvals to systems support teams, developers and end users to start making the directed alterations.
    - 變更管理政策：變更管理是從當前狀態過渡到未來狀態的紀律。它包含三個主要活動：決定變更、進行變更，以及確認變更已正確完成。變更管理專注於做出變更的決策，並獲得系統支援團隊、開發人員和終端用戶的批准，開始進行指定的改變。

- Throughout the system life cycle, changes made to the system, its individual components and its operating environment all have the capability to introduce new vulnerabilities and thus undermine the security of the enterprise. Change management requires a process to implement the necessary changes so they do not adversely affect business operations.
    - 在整個系統生命周期中，對系統、其各個組件和運行環境所做的變更都有可能引入新的漏洞，從而削弱企業的安全性。變更管理需要一個過程來實施必要的變更，以確保其不會對業務運營造成不利影響。

Common Security Policies Deeper Dive 通用安全策略深入探討

- Policies will be set according to the needs of the organization and its vision and mission. Each of these policies should have a penalty or a consequence attached in case of noncompliance. The first time may be a warning; the next might be a forced leave of absence or suspension without pay, and a critical violation could even result in an employee's termination. All of this should be outlined clearly during onboarding, particularly for information security personnel. It should be made clear who is responsible for enforcing these policies, and the employee must sign off on them and have documentation saying they have done so. This process could even include a few questions in a survey or quiz to confirm that the employees truly understand the policy. These policies are part of the baseline security posture of any organization. Any security or data handling procedures should be backed up by the appropriate policies.
    - 這些政策將根據組織的需求、願景和使命來設定。每個政策在不遵守的情況下都應該有相應的處罰或後果。第一次可能是警告；下一次可能是強制休假或停薪留職；而嚴重違規可能導致員工被解雇。在入職時，特別是對於信息安全人員，所有這些內容都應該明確地條列出來。應明確指出誰負責執行這些政策，並要求員工簽署並保留相應的文件以證明他們已經這樣做。這個過程甚至可以包括在調查或測驗中提出一些問題，以確認員工真正理解政策。這些政策是任何組織基本的安全立場的一部分。所有安全和數據處理程序都應該有相應的政策作為支持。

Change Management Components 變更管理組件

- The change management process includes the following components.
    - 變更管理流程包括以下組件。
- Documentation: All of the major change management practices address a common set of core activities that start with a request for change (RFC) and move through various development and test stages until the change is released to the end users. From first to last, each step is subject to some

form of formalized management and decision-making; each step produces accounting or log entries to document its results.
    - 文檔記錄：所有主要的變更管理實踐都涉及一組共同的核心活動，從變更請求（RFC）開始，通過各種開發和測試階段，直到變更釋放給最終用戶。從頭到尾，每一個步驟都需要某種形式的正式管理和決策；每一個步驟都會生成會計或日誌條目，以記錄其結果。
- Approval: These processes typically include: Evaluating the RFCs for completeness, Assignment to the proper change authorization process based on risk and organizational practices, Stakeholder reviews, resource identification and allocation, Appropriate approvals or rejections, and Documentation of approval or rejection.
    - 批准：這些流程通常包括：評估RFC的完整性，根據風險和組織實踐將其指派給適當的變更授權流程，利益相關者審查，資源識別和分配，適當的批准或拒絕，以及批准或拒絕的文檔記錄。
- Rollback: Depending upon the nature of the change, a variety of activities may need to be completed. These generally include: Scheduling the change, Testing the change, Verifying the rollback procedures, Implementing the change, Evaluating the change for proper and effective operation, and Documenting the change in the production environment. Rollback authority would generally be defined in the rollback plan, which might be immediate or scheduled as a subsequent change if monitoring of the change suggests inadequate performance.
    - 回滾：根據變更的性質，可能需要完成各種活動。一般而言，這些活動包括：安排變更，測試變更，驗證回滾程序，實施變更，評估變更的適當和有效操作，以及在生產環境中記錄變更。回滾權限通常在回滾計劃中進行定義，如果監控變更表明性能不足，則可能立即執行回滾，或將其安排為後續的變更。

Module 4: Understand Security Awareness Training 了解安全意識培訓

Domain D5.4, D5.4.1, D5.4.2, D5.3.2

- **To reduce the effectiveness of certain types of attacks** (such as social engineering), it is crucial that the organization informs its **employees and staff how to recognize security problems and how to operate in a secure manner**. While the specifics of secure operation differ in each organization, there are some general concepts that are applicable to all such programs.
    - 為了降低某些攻擊類型（例如社交工程）的效力，組織必須向員工和人員告知如何識別安全問題以及如何以安全的方式操作的重要性。雖然安全操作的細節在每個組織中可能不同，但有一些通用的概念適用於所有此類方案。

Purpose 目的

- The purpose of awareness training is to make sure everyone knows what is expected of them, based on responsibilities and accountabilities, and to find out if there is any carelessness or complacency that may pose a risk to the organization. We will be able to align the information security goals with the organization's missions and vision and have a better sense of what the environment is.
    - 宣導訓練的目的是確保每個人根據其責任和義務知道對他們有什麼期望，並查明是否存在任何疏忽或自滿，可能對組織構成風險。我們將能夠將信息安全目標與組織的使命和願景相協調，並對環境有更好的認識。

What is Security Awareness Training? 什麼是安全意識培訓？

- Let's start with a clear understanding of the **three different types of learning activities that organizations use**, whether for information security or for any other purpose:

    - 讓我們首先清楚了解組織使用的三種不同類型的學習活動，無論是用於信息安全還是其他任何目的：

- **Education**: The overall goal of education is to help learners **improve their understanding of these ideas and their ability to relate them to their own experiences and apply that learning in useful ways**.
    - 教育：教育的整體目標是幫助學習者提高對這些概念的理解能力，並能將其與自身經驗相關聯，並以有用的方式應用所學。
- **Training**: Focuses on **building proficiency in a specific set of skills or actions**, including sharpening the perception and judgment needed to make decisions as to which skill to use, when to use it and how to apply it. **Training can focus on low-level skills, an entire task or complex workflows consisting of many tasks**.
    - 訓練：著重於建立對特定技能或行動的熟練程度，包括提升辨識力和判斷力，以便做出關於何時使用哪種技能、如何使用以及如何應用的決策。訓練可以針對低層次技能、整個任務或由多個任務組成的複雜工作流程進行。
- **Awareness**: These are activities that attract and engage the learner's attention by acquainting them with aspects of an issue, concern, problem or need.
    - 認知：這些活動通過使學習者熟悉問題、關注點、問題或需求的方面，吸引並引起他們的注意。
- You'll notice that none of these have an expressed or implied degree of formality, location or target audience. (Think of a newly hired senior executive with little or no exposure to the specific compliance needs your organization faces; first, someone has to get their attention and make them aware of the need to understand. The rest can follow.)
    - 你會注意到，這些都沒有明示或暗示的正式程度、地點或目標受眾。（想像一下一位新雇用的高級主管，對貴組織面臨的具體合規需求幾乎沒有了解；首先，需要有人引起他們的注意，讓他們認識到需要理解這個需求。其餘的事情可以隨之而來。）

Security Awareness Training Examples 安全意識培訓示例

- Let's look at an example of security awareness training by using an organization's strategy to improve fire safety in the workplace:
    - 讓我們通過使用一個組織改善工作場所防火安全策略的例子來了解安全意識訓練：
- Education may help workers in a secure server room understand the interaction of the various fire and smoke detectors, suppression systems, alarms and their interactions with electrical power, lighting and ventilation systems. Training would provide those workers with task-specific, detailed learning about the proper actions each should take in the event of an alarm, a suppression system going off without an alarm, a ventilation system failure or other contingency. This training would build on the learning acquired via the educational activities. Awareness activities would include not only posting the appropriate signage, floor or doorway markings, but also other indicators to help workers detect an anomaly, respond to an alarm and take appropriate action. In this case, awareness is a constantly available reminder of what to do when the alarms go off.

    - 教育可以幫助在安全伺服器室工作的人了解各種火災和煙霧探測器、壓制系統、警報器之間的互動，以及它們與電力、照明和通風系統的互動。訓練將向這些工作人員提供具體任務的詳細學習，使他們了解在發生警報、壓制系統未經警報啟動、通風系統故障或其他突發情況時應該採取的正確行動。此訓練將建立在通過教育活動所獲得的學習基礎上。認知活動不僅包括張貼適當的標示、地板或門口標記，還包括其他指標，以幫助工作人員檢測異常、對警報作出反應並采取適當行動。在這種情況下，認知是一個不斷可用的提醒，提醒人們警報器響起時應該怎麼做。

- Translating that into an anti-phishing campaign might be done by:
    - 將其轉化為一個反釣魚運動可能可以通過以下方式進行：
- Education may be used to help select groups of users better understand the ways in which social engineering attacks are conducted and engage those users in creating and testing their own strategies for improving their defensive techniques.
    - 教育可以用來幫助選擇一些使用者群體更好地理解社交工程攻擊的方式，並讓這些使用者參與創建和測試改進自己防禦技巧的策略。
- Training will help users increase their proficiency in recognizing a potential phishing or similar attempt, while also helping them practice the correct responses to such events. Training may include simulated phishing emails sent to users on a network to test their ability to identify a phishing email.
    - 訓練將幫助使用者提高他們識別潛在釣魚或類似企圖的能力，同時也幫助他們練習對這類事件的正確應對。訓練可能包括向網絡上的使用者發送模擬釣魚郵件，以測試他們辨識釣魚郵件的能力。
- Raising users' overall awareness of the threat posed by phishing, vishing, SMS phishing (also called "smishing) and other social engineering tactics. Awareness techniques can also alert selected users to new or novel approaches that such attacks might be taking.
    - 提高使用者對釣魚、語音釣魚、短信釣魚（也被稱為「smishing」）和其他社交工程策略威脅的整體認識。認知技巧還可以向選定的使用者提醒這類攻擊可能采取的新方法或新策略。
- Let's look at some common risks and why it's important to include them in your security awareness training programs.
    - 讓我們來看看一些常見的風險以及為什麼將它們納入您的安全意識訓練計劃中是很重要的。

Phishing 網絡釣魚

- The use of phishing attacks to target individuals, entire departments and even companies is a significant threat that the security professional needs to be aware of and be prepared to defend against. Countless variations on the basic phishing attack have been developed in recent years, leading to a variety of attacks that are deployed relentlessly against individuals and networks in a never-ending stream of emails, phone calls, spam, instant messages, videos, file attachments and many other delivery mechanisms.
    - 使用釣魚攻擊來針對個人、整個部門甚至公司，是安全專業人員需要意識到並準備好防禦的重大威脅。近年來，針對基本釣魚攻擊的無數變體已經被開發出來，導致各種攻擊無情地部署在不斷湧現的電子郵件、電話、垃圾郵件、即時消息、視頻、附件文件和許多其他傳遞機制中，對個人和網絡進行攻擊。

- Phishing attacks that attempt to trick highly placed officials or private individuals with sizable assets into authorizing large fund wire transfers to previously unknown entities are known as whaling attacks .
    - 試圖欺騙高層官員或擁有大量資產的私人個人，使其授權將大筆資金轉移到先前未知實體的釣魚攻擊被稱為鯨魚攻擊。

Social Engineering 社交工程

- Social engineering is an important part of any security awareness training program for one very simple reason: bad actors know that it works. For the cyberattackers, social engineering is an inexpensive investment with a potentially very high payoff. Social engineering, applied over time, can extract significant insider knowledge about almost any organization or individual.
    - 社交工程是任何安全意識訓練計畫中的重要一環，原因非常簡單：惡意行為者知道它有效。對於駭客來說，社交工程是一個投入少但可能回報極高的廉價投資。長期應用社交工程可以提取關於幾乎任何組織或個人的重要內部知識。
- One of the most important messages to deliver in a security awareness program is an understanding of the threat of social engineering. People need to be reminded of the threat and types of social engineering so that they can recognize and resist a social engineering attack.
    - 在安全意識計畫中傳達的最重要信息之一是對社交工程威脅的理解。人們需要被提醒社交工程的威脅和類型，以便他們能夠辨識和抵抗社交工程攻擊。
- Most social engineering techniques are not new. Many have even been taught as basic fieldcraft for espionage agencies and are part of the repertoire of investigative techniques used by real and fictional police detectives. A short list of the tactics that we see across cyberspace currently includes:
    - 大多數社交工程技巧並不新鮮。許多甚至作為間諜機構的基本野外技能被教授，並成為真實和虛構警探所使用的調查技巧的一部分。目前在網絡空間中，我們看到的一系列策略包括：
- Phone phishing or vishing: Using a rogue interactive voice response (IVR) system to re-create a legitimate-sounding copy of a bank or other institution’s IVR system. The victim is prompted through a phishing email to call in to the “bank” via a provided phone number to verify information such as account numbers, account access codes or a PIN and to confirm answers to security questions, contact information and addresses. A typical vishing system will reject logins continually, ensuring the victim enters PINs or passwords multiple times, often disclosing several different passwords. More advanced systems may be used to transfer the victim to a human posing as a customer service agent for further questioning.
    - 電話釣魚或語音釣魚（vishing）：使用一個惡意互動式語音回應（IVR）系統來重新創建銀行或其他機構的合法聽起來的IVR系統副本。受害人會在釣魚郵件中被提示通過提供的電話號碼致電「銀行」，以驗證帳戶號碼、帳戶存取代碼或個人識別碼（PIN），並確認安全問題的答案、聯絡信息和地址。一個典型的語音釣魚系統會持續拒絕登錄，確保受害人多次輸入PIN或密碼，通常洩露出多個不同的密碼。更先進的系統可能會將受害人轉接到冒充客戶服務代理人的人類，進一步詢問資訊。

- Pretexting: The human equivalent of phishing, where someone impersonates an authority figure or a trusted individual in an attempt to gain access to your login information. The pretexter may claim to be an IT support worker who is supposed to do maintenance or an investigator performing a company audit. Or they might impersonate a coworker, the police, a tax authority or some other seemingly legitimate person. The goal is to gain access to your computer and information.
    - 冒名頂替：這是與釣魚相當的人類詐騙手法，其中有人假冒權威人士或受信任的個人，試圖獲取您的登錄信息。冒名者可能聲稱自己是IT支援人員，需要進行維護工作，或者是進行公司審計的調查員。或者他們可能冒充同事、警方、稅務機構或其他看似合法的人。其目標是獲得您的計算機和信息存取權限。
- Quid pro quo: A request for your password or login credentials in exchange for some compensation, such as a “free gift,” a monetary payment or access to an online game or service. If it sounds too good to be true, it probably is. Tailgating: The practice of following an authorized user into a restricted area or system. The low-tech version of tailgating would occur when a stranger asks you to hold the door open behind you because they forgot their company RFID card. In a more sophisticated version, someone may ask to borrow your phone or laptop to perform a simple action when he or she is actually installing malicious software onto your device. Social engineering works because it plays on human tendencies. Education, training and awareness work best to counter or defend against social engineering because they help people realize that every person in the organization plays a role in information security.
    - 交換：要求您提供密碼或登錄憑據，以換取某種補償，例如「免費禮品」、金錢支付或訪問網絡遊戲或服務。如果聽起來太好以至於難以置信，那可能就是如此。 尾隨：跟隨授權用戶進入限制區域或系統的行為。低技術版本的尾隨可能發生在當一個陌生人請求您將門留開，因為他們忘記了公司的 RFID 卡。在更複雜的版本中，有人可能會要求借用您的手機或筆記型電腦進行一個簡單的操作，而實際上他們正在您的設備上安裝惡意軟件。 社交工程之所以有效，是因為它利用了人類的傾向。教育、培訓和意識對抗或防禦社交工程效果最佳，因為它們幫助人們意識到組織中的每個人在信息安全中扮演著一個角色。

Password Protection 密碼保護

- We use many different passwords and systems. Many password managers will store a user’s passwords for them so the user does not have to remember all their passwords for multiple systems. The greatest disadvantage of these solutions is the risk of compromise of the password manager.
    - 我們使用許多不同的密碼和系統。許多密碼管理器可以為用戶存儲他們的密碼，這樣用戶就不必為多個系統記住所有密碼。這些解決方案最大的缺點是密碼管理器被破壞的風險。
- These password managers may be protected by a weak password or passphrase chosen by the user and easily compromised. There have been many cases where a person’s private data was stored by a cloud provider but easily accessed by unauthorized persons through password compromise.
    - 這些密碼管理器可能受到用戶選擇的弱密碼或密語保護，容易受到破壞。曾經發生過許多情況，一個人的私人數據被雲服務提供商存儲，但通過密碼被未經授權的人輕易地訪問的情況。
- Organizations should encourage the use of different passwords for different systems and should provide a recommended password management solution for its users.

    - 組織應該鼓勵用戶在不同系統中使用不同的密碼，並為其用戶提供一個推薦的密碼管理解決方案。

- Examples of poor password protection that should be avoided are:
    - 應該避免的糟糕密碼保護的例子包括：
- Reusing passwords for multiple systems, especially using the same password for business and personal use.
    - 在多個系統中重複使用密碼，尤其是在商業和個人用途中使用相同的密碼。
- Writing down passwords and leaving them in unsecured areas.
    - 將密碼寫下來並將其留在不安全的區域。
- Sharing a password with tech support or a co-worker.
    - 與技術支援或同事共享密碼。