

17389_企業資訊安全認知（二） 課程摘要

本摘要由 Gemini AI 協助生成，僅供參考

1. 適合對象與能力門檻

- **適合族群：**初學者 / 中小企業主 / 資訊與資安主管 / 企業內部稽核人員。特別適合需要建立基礎資安認知、了解常態資安威脅（如社交工程與勒索軟體），並規劃企業基本防護架構的跨領域主管與同仁。
- **能力門檻：**入門。課程從資安基本三要素（CIA）切入，結合真實企業新聞案例進行講解，無須具備資工程式開發或高級網路攻防背景。

2. 課程核心大綱與架構圖

- **章節架構：**
 - **章節一：資訊安全定義與核心三要素（CIA）** — 解析機密性（Confidentiality）、完整性（Integrity）與可用性（Availability），並對照國內科技大廠（如宏碁、華碩）資安新聞案例。
 - **章節二：資安長（CISO）與資安主管職務範疇** — 解構資安建構、資安操作/維運、計畫管理、網路風險/情報、資料漏失預防、身分與存取管理、數位鑑識/調查法證及管理體系運作。
 - **章節三：三大主流資安威脅剖析** — 深入探討歷史悠久的「社交工程（釣魚郵件/心理人性探討）」、衝擊最大的「勒索軟體（Ransomware/暗網產業鏈）」及近年盛行的「第三方/供應鏈威脅（軟體套件/硬體/維運廠商）」。
 - **章節四：技術層面基本資安防護措施** — 涵蓋資安組織設計（治理與維運小組）、管理體系 PDCA 循環、弱點掃描/滲透測試、密碼複雜度（12 碼以上/密碼用語）、社交工程演練、權限清查、異地備份/備援與日誌（Log）留存。
 - **章節五：聯防機制與台灣資安資源** — 介紹跨企業資安聯防概念，以及 TWCERT/CC、F-ISAC、H-ISAC 等國家級情資分享與通報平台。

3. 必備前置知識清單

- **基礎電腦與網路使用認知**：瞭解日常辦公電腦操作、電子郵件收發、帳號密碼登入及基礎網路連線概念。
- **無須程式或攻防技術**：本課程著重於資安意識建立、管理架構與防護觀念，無須撰寫程式碼。

4. 專有名詞與概念辭典

- **CIA 資安三要素**：
 - **機密性 (Confidentiality)**：保護資料不外洩，確保只有獲授權者能存取。
 - **完整性 (Integrity)**：保護資料在傳輸與處理過程中不被未授權竄改。
 - **可用性 (Availability)**：確保企業在需要時能隨時存取資訊與系統（如避免電力中斷或勒索軟體癱瘓）。
- **社交工程 (Social Engineering)**：利用人的心理弱點（如恐懼、好奇或貪小便宜）製造情境，誘使目標點擊非法連結或提供機密資訊的無技術攻擊手段。
- **勒索軟體 (Ransomware)**：入侵企業系統後加密機密檔案與資產，藉由癱瘓營運或威脅公開資料向企業勒索贖金的惡意軟體。
- **第三方/供應鏈威脅**：駭客不直接攻擊目標企業，而是透過其軟體廠商、開源套件（如第三方元件弱點）或硬體/維運服務商等供應鏈漏洞間接入侵。
- **PDCA 循環**：資安管理體系（如 ISO 27001）的生命週期：Plan（定義範圍與資產）→ Do（風險評鑑與保護）→ Check（評估防護有效性）→ Act（持續改善與宣導）。

5. 課程學習職能對照

- **對應職能名稱**：資訊安全管理師、企業風險管理師
- **主要工作任務/能力指標**：

- **資安風險辨識與威脅評估能力：**能辨識社交工程、勒索軟體與供應鏈漏洞風險，並依 CIA 三要素評估對營運之衝擊。
- **資安防護部署與管理體系維運能力：**能協助規劃跨部門資安組織、推動 PDCA 管理循環、落實密碼原則與社交工程演練，並運用國家級通報資源（TWCERT/CC）建立防禦機制。