出國報告(出國類別：其他)

參加「SEACEN-BIS Course on IT Risk Management and Cybersecurity」課程報告

服務機關：中央銀行
姓名職稱：袁鴻文 三等專員
派赴國家/地區：印度/清奈
出國期間：113 年 8 月 26 日至 9 月 1 日
報告日期：113 年 11 月 21 日

摘要

本次課程係由「東南亞國家中央銀行聯合會」（South East Asian Central Banks, SEACEN）於印度清奈舉辦，為期 4 天（8 月 27 日至 30 日）；參加學員均為各國央行人員，共計 23 位；講者為各界對相關資安主題有深入研究或具體成果之學者、專家。

課程內容主要包含：當前資安威脅發展、資安風險管理框架、新興科技（如：AI、雲端、數位貨幣等）帶來的資安挑戰與因應措施等。相關課程內容不但以理論及實際案例講述說明，也安排上線實作課程以展示與操作網路偵測及防護作業，讓參訓學員實際體驗遭受資安攻擊時的緊迫感，進而了解資安防護的重要。

課程心得：(一)資安威脅日趨多元化和複雜化；(二)資安風險管理框架應與時俱進；(三)供應鏈管理與零信任架構是關鍵策略。建議事項：(一)鼓勵同仁多參加資安相關之訓練課程；(二)重視量子運算對資安的衝擊。

本報告第壹章為課程之目的與過程，第貳章說明最新資安威脅趨勢；第參章簡介資安風險管理框架；第肆章概述量子運算及其對資安的衝擊；第伍章簡述供應鏈管理與零信任架構；第陸章為其它資安議題；最後為心得與建議。

目　次

壹、課程之目的與過程

一、目的

本次「SEACEN-BIS Course on IT Risk Management and Cybersecurity」課程係由「東南亞國家中央銀行聯合會」（South East Asian Central Banks, SEACEN）於印度清奈舉辦，為期 4 天（8 月 27 日至 30 日）；參加學員均為各國央行人員，共計 23 位；講者為各界對相關資安主題有深入研究或具體成果之學者、專家。

課程內容主要包含：當前資安威脅發展、資安風險管理框架、新興科技（如：AI、雲端、數位貨幣等）帶來的資安挑戰與因應措施等。相關課程內容不但以理論及實際案例講述說明，也安排上線實作課程以展示與操作網路偵測及防護作業，讓參訓學員實際體驗遭受資安攻擊時的緊迫感，進而了解資安防護的重要。

課程目的是為能提升參與者在資訊安全方面的知識、技能與意識，以便能對資安威脅與防護獲得更全面的觀點，促進組織建立更安全的數位環境，相關的因應措施亦可做為本行資訊安全防護之參考。

二、過程

本次課程學員分別來自韓國、印度、柬埔寨及菲律賓等 11 個國家央行，共 23 人。課程方式，除講師對資安防護相關主題進行說明外，亦安排學員就特定個案議題進行分組意見交流與討論，過程中學員除能分享自身監理及政策推行經驗外，亦能瞭解其他國家的因應作法與面臨的挑戰。派員參加之機構如下：

No.	Name of Insitution	No. of Participants
1	The Bank of Korea	1
2	Reserve Bank of India	4
3	National Bank of Cambodia	4
4	Nepal Rastra Bank	2
5	Bangko Sentral ng Pilipinas	2
6	Central Bank of Sri Lanka	1
7	Central Bank, Chinese Taipei	1

8	Bank of Thailand	2
9	State Bank of Vietnam	2
10	Bank of Papua New Guinea	3
11	Bank of the Lao PDR	1
	TOTAL	23

本次課程之講師除有幾位為 SEACEN 及 BIS 之專任研究者之外，亦有來自微軟、世界銀行、南非 Pretoria 大學等對資安相關主題有深入研究或具體成果之學者、專家。課程除安排講師說明及學員分組討論外，另有上線實作課程，加深學員對資安防護重要性的體認。課程主題及講師如下表：

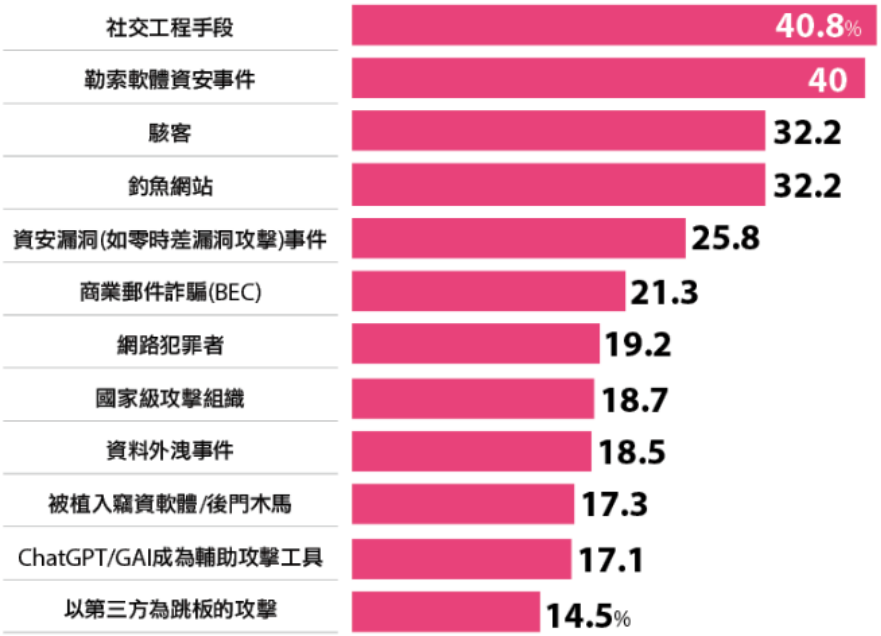
日期	課程	講師	職稱
113.8.27	Cyber Threat Landscape Update	David Whyte	Head of Corporate Security and Cyber Resilience Coordination Centre, BIS
	IT Risk Frameworks	Kalaranjani Mahavir	Deputy General Manager, Department of Supervision, Cyber Security & IT Risk Group, Reserve Bank of India
	Emergent Technologies - AI Risks	Roger Halbheer	Chief Security Advisor, Microsoft
	Cyber Resilience & Benchmarking in the CB Community	Sukhvir Notra	Senior Security Specialist, BIS
	Case Study: Ransomware Negotiations	Dougie Grant	Managing Director - EMEA, Nihon Cyber Defence
113.8.28	IT Assurance & Controls	Chu Ei Chong	Senior Supervisor, Risk & Technology Supervision Department, Bank Negara Malaysia
	Emergent Technologies - CBDC - Project Polaris	William Zhang	Advisor, BIS Nordic Innovation Hub
	IT Security & Resilience Testing (Purple/Red Teaming)	Sukhvir Notra	Senior Security Specialist, BIS
	Roundtable Discussion - Topics of Cyber Risks & Risk Managemenet	All Participents	

	Emergent Technologies - Quantum Cryptography	Mikala Mosca	Co-fonder & CEO of EvolutionQ Inc.
113.8.29	Cyber Attack - In the Theory & Lab Set up	Sukhvir Notra	Senior Security Specialist, BIS
	Practical Lab		
	BIS-GPT	Hiren Jani	Head of Data & Analytics, BIS
	Zero Trust Architecture & Implementations	Clay Lin	CISO & Director of IT Risk, World Bank Group
113.8.30	Cloud Computing: Emerging Opportunities, Challenges & Risks	Yogesh Simmhan	Associate Professor, Department of Computatinal & Data Sciences, IISc., Bangalore
	Closing the CBDC Cyber Threat Modelling Gaps	Ying/Jonathan	
	Incident Reporting & Sharing within CBs	Jacques Theron	
	Roundtable Discussion - CBs to Discuss their Approach on Incident Reporting / Information Sharing	All Participents	

貳、 最新資安威脅趨勢

綜合 BIS、Gartner 等組織研究及 CrowdStrike、Check Point 等網路安全公司公布的報告，近年主要的資訊安全威脅包括**身分竊取及社交工程攻擊**、**勒索病毒的持續氾濫**、**進階持續性滲透攻擊**（Advanced Persistent Threat，APT）、**利用 AI 技術發展的攻擊手法**以及**供應鏈跳板攻擊**等資安威脅。據一份針對 BIS 會員國相關組織的調查指出，各國組織認為的資安攻擊威脅度排名如下圖（百分比代表憂心遭受攻擊的組織比率）。

圖 1.資安攻擊威脅度排名



資料來源：David W., BIS (2024), 作者翻譯

一、身分竊取及社交工程攻擊

跨越地區限制的全球性攻擊者，持續利用**網路釣魚**（Phishing）技術欺騙系統或資料之合法用戶，竊取有效的身分資訊、其他身分驗證或識別資料以進行攻擊，進一步取得系統或資料之存取權。除了**竊取帳戶憑證**外，其他容易遭受攻擊的目標還包括 API **金鑰**等重要資訊、**網頁存取** session cookie、**一次性密碼**（One-time Password，OTP）以及**第三方身分驗證之** Kerberos token 等。

二、勒索病毒持續氾濫

根據研究報告，銀行、科技與政府機關是 2024 年上半年遭勒索病毒攻擊最多的前三大產業，即便歐洲刑警組織（Europol）於 2024 年 2 月成功瓦解 LockBit 的攻擊行動，LockBit 仍是上半年檔案偵測數量最多的勒索病毒，偵測數量超過其他勒索病毒家族的一半以上。雖然 LockBit 集團遭受打擊，但勒索病毒集團仍不斷地演變，試圖採用各種不同的攻擊手法、技巧與程序來進行突破防線、長期潛伏受害者系統、存取登入憑證等動作以竊取資料、操作加密勒索行動。

三、進階持續性滲透攻擊（APT）

APT 集團一直在探索新的方法，潛入連網路由器、甚至利用全球事件議題來變換其發展攻擊的工具和手法，擴大攻擊範圍。知名駭客集團 Earth Lusca 使用 OpenAI 的服務來執行如蒐集資訊、生成用於網路釣魚的內容與翻譯，及用來微調攻擊腳本等工作，使得 OpenAI 被迫停用與這些 APT 集團有關的帳號。此外，該集團也利用地緣政治議題作為社交工程手法，散播含有惡意程式的電子郵件以竊取機密文件。

四、利用 AI 技術發展的攻擊手法

值得留意的一項快速浮現的風險是「**深偽技術（Deepfake）冒用事件**」。早在 2022 年，美國聯邦調查局就發布警告，提醒組織和企業小心深偽技術的風險，但是直到 2024 年 2 月，香港爆發一起結合商業郵件詐騙和深偽技術的詐騙攻擊，損失高達 2 億港幣，才引起全球注意，金融界及銀行業更是高度警戒。

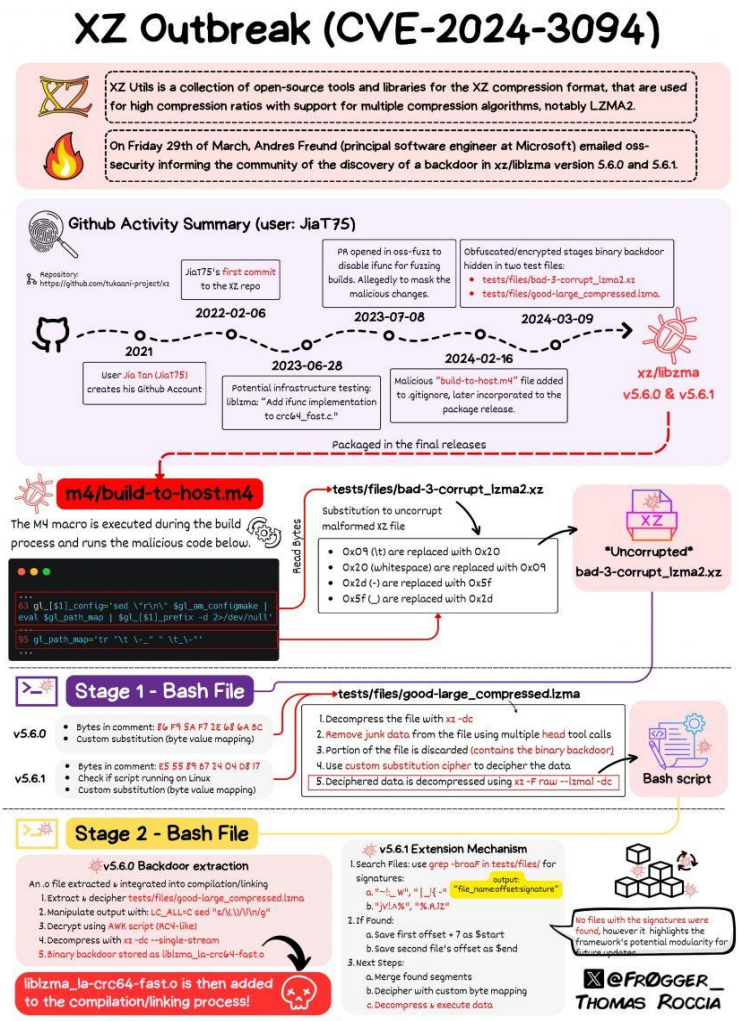
隨著 AI 技術的蓬勃發展，另一種名為「**越獄服務**」（Jailbreak-as-a-service）的攻擊手法開始興起，它利用各種方法來繞過 AI 大語言模型（Large Language Model，LLM）內建的倫理規範，例如使用假設性問題、角色扮演情境或是外國語言來向 LLM 提問，以達到利用 AI（如 ChatGPT）來產生具攻擊傾向的資料內容。此外，也有資安機構發現某些駭客集團嘗試利用正常的 AI 軟體來挾帶惡意檔案，例如散播含有惡意安裝程式的 AI 換臉程式（Face Swapper）以及其

他深偽生成工具以擴大受害族群。因此，組織在探索 AI 技術應用時，應時時謹慎並考量資訊安全，以免為駭客製造新的犯罪機會。

五、供應鏈跳板攻擊

供應鏈跳板攻擊（以第三方為跳板攻擊）在調查的排名中雖不顯眼（詳圖 1），但卻是有可能對組織或企業造成重大打擊的攻擊手法。2024 年 3 月 29 日發生一起震驚 IT 界的 **XZ 程式庫遭植入後門事件**，攻擊者精心潛伏，扮演熱心的開源貢獻者，花了 2 年時間參與開放原始碼軟體專案 XZ 的維護，為的就是暗中植入惡意程式碼；所幸有開發者察覺 SSH 登入失敗或登入過程變慢 500 毫秒等的異狀，才揪出暗藏的後門程式碼，揭露了此項精心設計的供應鏈攻擊。

圖 2. XZ 跳板攻擊



資料來源：Thomas Roccia, X (2024)

隨著 XZ 資安後門事件的爆發，軟體供應鏈資安勢必再次成為資安界的熱門課題，各界也應正視這項風險，以對應的措施進行防護。

六、其他須注意之資安威脅

除上述各項威脅以外，駭客也經常鎖定暴露在外的資源、系統漏洞及遭外洩的登入憑證來入侵組織內部。根據 CrowdStrike 2024 年度資安風險報告顯示，前三大的風險事件即為「**可被外界存取的高風險雲端應用程式**」、「**閒置的帳號**」及「**零時差攻擊手法**」。面對現今的資安態勢，各界針對受管理的裝置應強化偵測回應威脅的能力、做好攻擊面管理，同時加強端點防護，才能真正有效地管控風險。

參、 資安風險管理框架

一、何謂資安風險管理框架

資安風險管理框架是一套結構化的方法，用於識別、評估、應對和監控組織面臨的資訊安全風險。它幫助組織制定策略，以保護其數位資產（例如資料、系統和網路），同時確保運營效率和法規合規性。

這種框架通常提供明確的步驟和指導，協助組織在動態的資安威脅環境中保持適應性和持續性。以下是資安風險管理框架的核心元素：

(一) 風險識別

- 確定所有潛在的資安威脅，例如網路攻擊、內部資料洩露、第三方供應商風險等。
- 相關資源識別(例如關鍵資料、應用程式和系統)以及這些資源的潛在風險。

(二) 風險評估

- 分析風險的可能性和影響，將風險按照嚴重性進行分類（如高、中、低風險）。
- 評估組織現有的控制措施是否足夠應對這些威脅。

(三) 風險處置

制定策略來管理或減輕風險，通常包含以下幾種作法：

- 風險避免：改變業務流程以完全消除風險。
- 風險降低：採取技術或管理措施（如防火牆、加密技術）來減少風險。
- 風險接受：承擔可控範圍內的風險。
- 風險轉移：例如購買商業保險。

(四) 實施安全控制

- 根據風險優先等級，部署適當的安全措施，例如身分驗證、存取控制、威脅檢測工具、資料加密等。

- 對應緊急事件建立緊急應變計畫。

(五) 持續監控與改善

- 持續監控風險環境和資安控制的有效性，確保隨著威脅的演變進行必要的調整。
- 定期進行風險評估和查核，並更新框架。

二、常見的資安風險管理框架

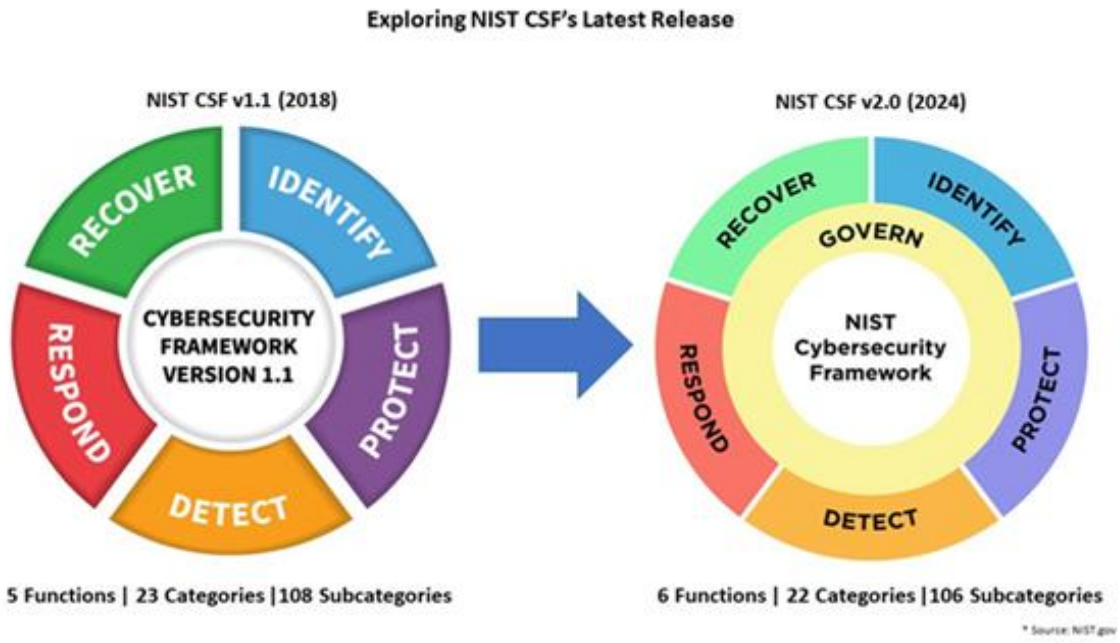
(一) ISO/IEC 27001

ISO/IEC 27001 全名 Information technology - Security techniques - Information security management systems - Requirements。它是一套完整的資訊安全管理國際標準，由國際標準化組織（ISO）與國際電工委員會（IEC）在 2005 年聯合發布，其列出有關資訊安全管理制度（Information Security Management System，ISMS）的架構、實施、維護、及持續改善的要求，目的是要幫助組織更加安全地管理資訊資產。此標準是目前國際上最廣泛使用，且最為完整的 ISMS 資安管理制度規範。

(二) NIST 網路安全框架

是由美國國家標準與技術研究所（National Institute of Standards and Technology，NIST）發布的網路安全框架（Cybersecurity Framework），或簡稱 NIST CSF)。如今這套框架是全球最廣泛認可和使用的框架之一，2018 年公布 1.1 版，2024 年更新為 2.0 版，當中特別將治理的位階提升並且獨立，是相當重大的演進。

圖 3. NIST CSF 1.1 及 2.0 版

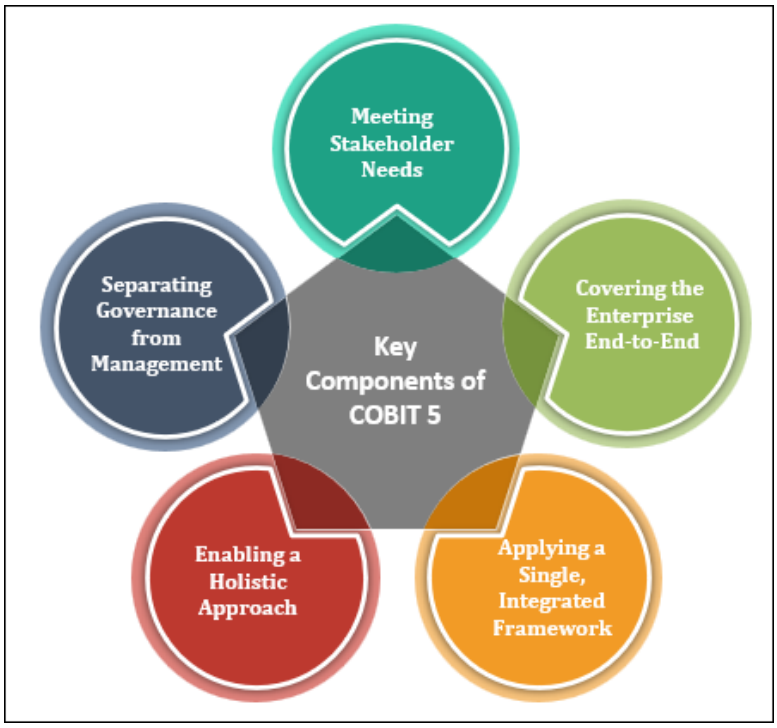


圖片來源: Kalaran J. M., RBI (2024)

(三) COBIT

COBIT（Control Objectives for Information and Related Technology），中文譯為：資訊及相關技術的管理、控制與稽核。它是一系列關於資訊治理最佳實踐（框架）的集合，由國際電腦稽核協會（Information Systems Audit and Control Association，ISACA）和 IT 治理委員會於 1992 年提出。COBIT 提供全球可接受的原則、實務、分析工具及模式，可作為管理人員、稽核人員及資訊用戶的通用資訊治理架構及最佳實務，幫助組織提高相關個人或團體對於組織資訊及科技資產的信任度，並從中獲得最大效益。

圖 4. COBIT 管理架構



圖片來源: Kalaran J. M., RBI (2024)

三、資安風險管理框架的價值

通過資安風險管理框架，組織能夠：

(一) 提高風險意識，了解可能的威脅來源和影響。

(二) 制定預防措施，減少風險對業務的潛在損害。

(三) 提高合規性，滿足相關法規和標準的要求。

(四) 增強韌性，在威脅發生後快速恢復運營。

這是一個不斷演進的過程，在組織導入管理框架的過程中必須根據組織的變化和外部威脅的發展進行調整，以便能順暢地完成組織調整與內部人員的適應，發揮該框架在管理上的最大效益。

肆、 量子運算及其對資安的衝擊

一、何謂量子運算

量子運算（Quantum Computing）是一種基於量子力學原理的新型計算方式，其處理信息的方式與傳統計算機截然不同。它利用量子位元（Qubits）進行計算，能夠同時處理大量資料並執行高度複雜的運算，因此在某些特定應用中擁有極大的潛力。其核心概念如下：

(一) 量子位元（Qubit）

傳統計算機使用位元(bit)，以 0 和 1 表示信息。量子運算則使用量子位元，它可以同時處於 0、1 和 0 與 1 的疊加態（superposition），這使得量子計算能在同一時間進行多個運算。

(二) 疊加（Superposition）

在量子力學中，粒子可以同時處於多種可能狀態的組合中。量子計算利用這一特性，讓量子位元可以同時表示多種狀態，從而大幅提升計算效率。

(三) 量子糾纏（Entanglement）

兩個或多個量子位元之間可以建立一種特殊的關聯性，即使在空間上分隔，它們的狀態變化仍能相互影響。這種現象被用來提高量子運算的精確性和速度。

(四) 量子干涉（Quantum Interference）

通過干涉效應，量子運算可以增強正確的計算路徑，同時削弱錯誤的路徑，從而提高計算結果的準確性。

二、量子運算的潛在運用

由於量子運算目前尚未能大規模發展，相關的應用領域也同樣還在研究階段，但已有相當驚人的展現。潛在的應用領域如下：

(一) 密碼學

傳統加密技術（如 RSA 演算法）大多基於數學難題的計算複雜度，但

運用量子運算中的特定算法可以高效破解這些加密，同時也對現有網路安全體系構成嚴重的衝擊。

(二) 優化問題

量子運算能快速解決複雜的優化問題，如物流路徑規劃、供應鏈管理等。

(三) 人工智慧與機器學習

量子運算可以加速資料處理和模式識別，提升人工智慧模型的訓練速度和效果。

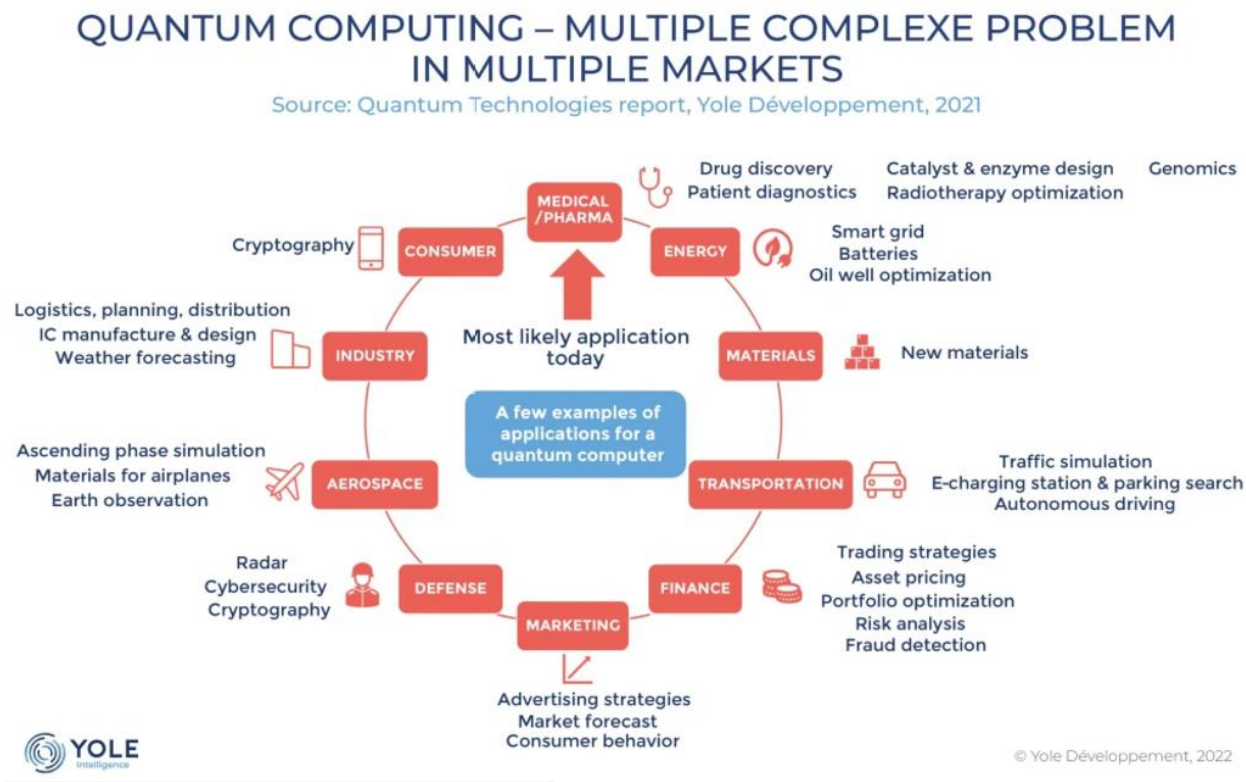
(四) 藥物開發與材料科學

量子模擬能更準確地模擬分子結構和化學反應，有助於發現新藥物和材料。

(五) 金融市場分析

量子運算可應用於高頻交易、風險管理和市場模擬等領域。

圖 5. 量子運算運用領域



資料來源：Yole Delevpement, 2022

三、量子運算的挑戰與限制

(一) 技術挑戰

- 量子位元需要在極低溫和無干擾的環境中運行，技術條件苛刻。
- 現在的量子電腦仍處於實驗和初期商業化階段，距離大規模應用還有一段路。

(二) 穩定性與糾正錯誤

- 量子系統極易受到環境噪聲干擾，導致計算錯誤。
- 需要開發強大的量子糾錯機制。

(三) 應用普及性

- 雖然量子運算對某些問題具備顯著優勢，但對大多數日常應用，傳統計算仍是更為實用的解決方案。

四、對資訊安全的衝擊

傳統加密方法是基於數學問題的難解性進行加密。生活中，從遊戲、電子郵件、各類個人帳號乃至金融交易，甚至是區塊鏈都脫離不了密碼學的應用。然而，量子電腦強大的運算能力能夠迅速解決這些數學問題，進而破解傳統的加密方法。這可能導致數位通訊、個人敏感資料以及金融交易的安全性受到嚴重影響。

RSA 加密演算法是最常使用的非對稱加密法，其金鑰的產生建立在質因數分解的基礎上，目前被普遍應用在國防和商業相關的通訊和情報傳遞上。這種建立在質因數分解的加密方式，是利用現今傳統電腦對極大整數進行質因數分解需花費極長時間的特性，使加密金鑰無法於短時間內被破解，進而達到通訊安全的效果。量子電腦藉由秀爾演算法（Shor's Algorithm）能快速找出整數的質因數，使看似不可能破解的 2048 位元 RSA 加密可以被破解，因此量子電腦的發展將會嚴重威脅現有加密演算法的安全性。

根據報導，中國大陸目前是在此加密演算法破解研究上發展的最快速的地區，早於 2023 年 1 月，中國大陸清華大學物理系教授龍桂魯所帶領的研究團

隊宣稱他們成功開發出只需在中階量子電腦上運行的全新密碼破解演算法，可以破解 RSA-2048 加密資料。雖然當時公布的論文引起學界不同看法而引起爭議，但在 2024 年 9 月，上海大學王潮研究團隊再度發表研究報告，聲稱成功利用量子電腦對廣泛使用的加密方法進行有效攻擊。這項研究使用了加拿大 D-Wave Systems 公司的量子電腦，針對現代密碼學中常用的置換排列網路（Substitution-Permutation Network，SPN）結構進行破解，引發全球資安專家的高度關注。

五、如何因應

為了因應後量子時代所面臨的資安問題，各國政府、學界及資安從業人員目前皆致力於研究新的技術與方法，以應對這項挑戰。目前大致有兩個研究方向：

(一) 量子安全密碼學（Post-quantum cryptography，PQC）

量子安全密碼學是為了探討密鑰抵抗攻擊的理論與實作方式，使任何資料皆可免受使用傳統電腦或量子電腦的駭客攻擊。量子安全密碼學也被稱為後量子密碼學。現有的加密標準，如進階加密標準（Advanced Encryption Standard，AES）、橢圓曲線加密（Elliptic Curve Cryptography，ECC）、RSA 等，都是僅使用數學方式生成密文；但有了量子密碼學，就可以用物理和數學方程式生成密文。

美國國家標準暨技術研究院（NIST）正致力於徵求、評估和標準化可抵抗量子運算之公鑰加密算法，並於 2024 年 8 月公布 FIPS-203、FIPS-204、FIPS-205 3 項 PQC 相關標準。一旦它們被公眾及業界確認可行，由量子密碼學產生出密鑰及相關的應用將指日可待。

(二) 量子密鑰分發（Quantum Key Distribution，QKD）

量子密鑰分發 QKD 主要目標是：若有第三方試圖竊聽密碼，則通訊的雙方便會察覺；這種性質基於量子力學的基本原理：任何對量子系統的測量都會對系統產生干擾。第三方試圖竊聽密碼，必須用某種方式測量它，而這些測量就會帶來可察覺的異常。通過量子疊加態或量

子糾纏態來傳輸資訊，通訊系統便可以檢測是否存在竊聽，並藉此保障金鑰及通訊的安全性。

QKD 也涉及通過光纖傳送資料，使傳送中的資料免於遭受各種形式的攻擊。理論上，QKD 提供了更高形式的安全性，它可以快速地檢測到任何類型的入侵，及時提醒傳輸者丟棄當前用於資料傳輸的密鑰，重新進行資料的加密、傳輸，避免被入侵者竊取資料。

量子運算有望在未來幾十年內改變許多行業。隨著技術的進步和應用的拓展，它將補充甚至在某些領域取代傳統運算技術，從而推動科學、商業和社會的進步。然而，與此同時，也需要正視它對資安、隱私和經濟的潛在影響，提前制定應對策略。

伍、 供應鏈管理與零信任架構

一、供應鏈管理

在當前數位化時代，供應鏈的管理不僅僅關乎物流、採購與供應的效率，更與資訊安全緊密相關。隨著供應鏈逐漸依賴數位技術和全球化合作，資安風險也隨之增加。供應鏈管理中的資訊安全，對於組織的穩定運作和競爭力至關重要，原因如下：

(一) 供應鏈的連結性增加了攻擊面

現代供應鏈涉及眾多參與者，包括供應商、製造商、物流公司和經銷商。這些環節的資料共享與系統整合使得整個供應鏈成為一個複雜的網絡，也因此成為網路攻擊的目標。例如，駭客可能攻擊供應鏈中的較弱環節，進而滲透到整個系統。

(二) 第三方風險不可忽視

組織依賴第三方供應商提供關鍵服務或技術，但這些供應商可能成為安全漏洞的來源。如果供應商的安全措施不足，將可能導致敏感資料洩漏或惡意軟體的傳播。因此，需要組織針對第三方供應商進行嚴格的資安審核與監控。

(三) 合規與信任的保障

許多產業受到嚴格的法規管控，如醫療、金融與公共服務等，違反資安法規可能帶來高額罰款和聲譽損害。通過強化供應鏈資安管理，不僅能確保合規，還能增強客戶與合作夥伴的信任。

(四) 避免業務中斷與財物損失

供應鏈攻擊，例如勒索軟體或針對供應商的資料竊取，可能導致業務中斷，甚至影響整個行業的運作。良好的資安管理可降低這類風險，確保供應鏈的穩定性與連續性。

隨著供應鏈管理在資訊安全的角色愈加重要，組織也必須採取主動措施以提升供應鏈的整體安全性，其中最核心的策略即為零信任架構。

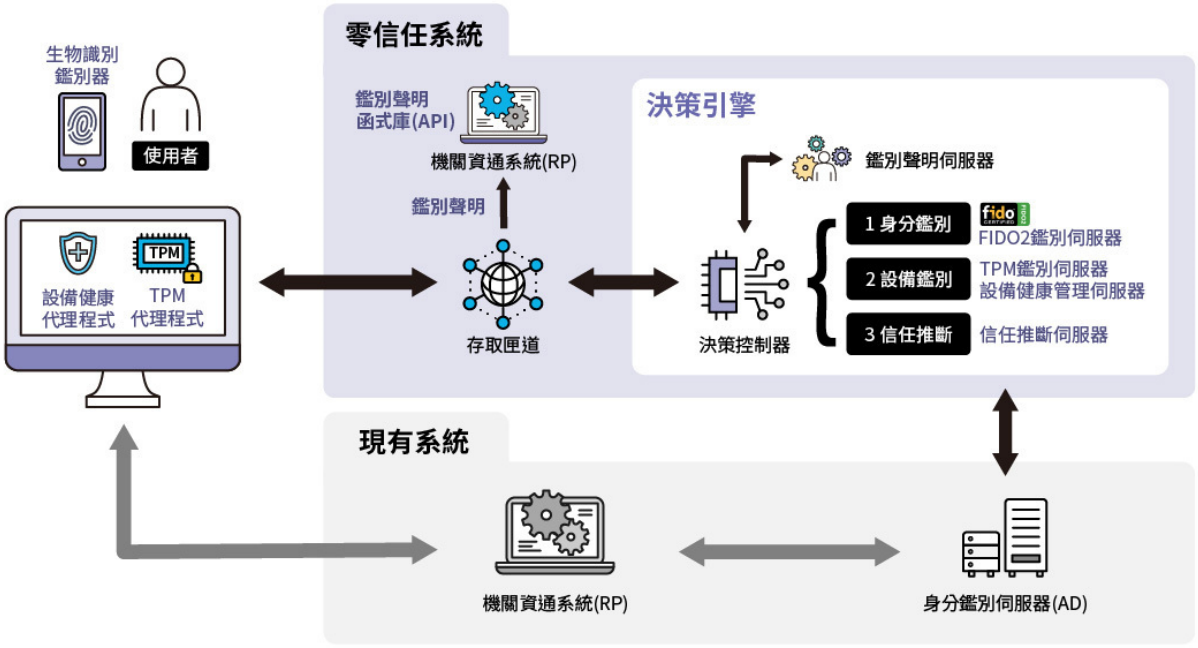
二、零信任架構

隨著網路威脅日益複雜，傳統的周邊防禦策略已難以應對現代化攻擊手段；零信任架構（Zero Trust Architecture，ZTA）應運而生，成為資安領域的重要策略。它以「永不信任，始終驗證」為核心理念，徹底改變組織應對資安風險的方式。

(一) 何謂零信任架構

零信任架構的關鍵在於去除對內部網路的默認信任。傳統模式假設內部系統是安全的，但零信任認為，威脅可能來自任何地方，包括內部員工、設備或第三方。它要求在每一次存取，無論用戶或設備是否位於內部網路，都必須進行嚴格的身分驗證和授權。

圖 6. 零信任系統架構



資料來源：數位發展部

(二) 零信任的三大核心原則

1. **最小權限原則**：只授予用戶或系統完成特定任務所需的最低權限，避免過多的存取權限成為攻擊的入口。
2. **持續驗證**：每次存取請求都需經過重新驗證，包括身分驗證、設

備狀態檢查和上下文分析。

3. **微分段網路**:將系統分成多個隔離的區域,限制威脅的橫向移動,即使攻擊者突破某一環節，也無法輕易擴展。

(三) 零信任架構的優勢

1. **加強資料保護**：即使資料存儲於雲端或跨越多地點，零信任策略也能確保存取安全。
2. **減少內部威脅**：針對內部使用者實施同樣嚴格的安全驗證，降低內部威脅帶來的風險。
3. **適應分散式工作環境**：隨著遠端工作和混合雲架構的普及，零信任能提供彈性且可靠的安全保護。

三、將零信任架構運用於供應鏈管理

將零信任架構應用於供應鏈管理，組織可以實現對每個供應商和合作夥伴的嚴密監控和驗證，確保每一次資料交換和存取請求都符合安全標準。這不僅提高了整體供應鏈的安全性，還能及時發現並阻止潛在的攻擊行為。

總結來說，結合零信任架構的供應鏈管理策略，是應對現代資安挑戰的有效方法。它不僅能保護組織的核心資料和系統，還能增強對供應鏈環節中潛在威脅的抵禦能力，確保業務運營的穩定和安全。

陸、 其他資安議題

一、AI 造成的資安衝擊：機會與挑戰並存

人工智慧（AI）的快速發展為各行各業帶來巨大變革，然而，也為資訊安全領域帶來前所未有的衝擊。AI 既可成為資安防禦的利器，也可能被不法分子利用，成為攻擊者的強大工具。這種雙刃劍的特性，使 AI 在資安領域既充滿機遇，也面臨挑戰。

(一) AI 帶來的資安威脅

1. **自動化攻擊的增長：**AI 能協助攻擊者快速分析大量資料，發現漏洞並自動化執行攻擊。例如，AI 驅動的釣魚攻擊能生成高度個性化的詐騙郵件，增加成功率。
2. **深偽技術的濫用：**深偽技術可以生成虛假的聲音、影像或文字，欺騙用戶或系統。例如，攻擊者可能利用偽造的高層指令竊取資金或敏感資料。
3. **逃避偵測的惡意軟體：**AI 技術使惡意軟體更加智能，能學習如何躲避傳統的安全防禦系統，增加威脅的隱匿性。
4. **資安防禦技術的反利用**：一些攻擊者可能利用資安 AI 模型中的漏洞（例如對抗樣本攻擊），削弱防禦系統的有效性。

(二) AI 在資安防禦中的運用

1. **威脅偵測與預測：**AI 能快速分析網路流量和行為資料，發現異常活動並預測潛在威脅。
2. **自動化回應：**AI 可以加快安全事件的響應速度，協助安全團隊迅速封鎖攻擊並減少損失。
3. **增強身分驗證：**AI 技術能通過行為分析、聲紋識別等手段，提高用戶身分驗證的準確性和安全性。
4. **學習與適應新型威脅：**AI 能持續學習新型攻擊手段，更新安全策略，使防禦體系更具韌性。

(三) 如何應對 AI 造成的資安衝擊

- **強化 AI 治理與透明性：**制定 AI 開發與應用的倫理規範，確保技術不被濫用。
- **發展對抗 AI 技術：**設計能防禦 AI 驅動攻擊的解決方案，例如防範深偽內容的工具。
- **提升資安教育與意識：**加強對員工和公眾的培訓，幫助識別 AI 相關威脅。

AI 的發展給資安帶來新的挑戰，但也提供強大的工具。為了充分發揮 AI 潛力，組織必須建立更堅實的資安策略，積極應對 AI 產生的威脅，同時利用 AI 提升防禦能力。在這場技術博弈中，資安防禦方唯有持續創新，才能在不斷變化的風險環境中立於不敗之地。

二、網路攻擊

網路攻擊是指惡意行為者（駭客）通過技術手段，對電腦系統、網路或資料進行未經授權的存取、破壞或控制。了解網路攻擊的種類、手段及典型流程，有助於加強防禦並迅速應對威脅。

(一) 攻擊者的種類

1. **愛好者（Hobbyist）：**較不具備專業技能，僅憑著好奇心嘗試駭客攻擊的業餘者，通常獨自行動，沒甚麼特定目的。
2. **駭客行動主義者（Hacktivist）：**具備一定程度的技能，通常為了某些特定目的（如政治、彰顯特定議題等）而行動，可以單獨也可以是一群人組織行動。
3. **網路犯罪組織（Cyber Criminal Group）：**具備較專業的駭客技能，通常為了取得錢財而進行有組織化的犯罪活動。
4. **進階持續性滲透攻擊發起者（Advanced Persistent Threat）：**通常指以政治或國家利益為目的發起攻擊，由特定政府組織支持，具備高等專業技能的駭客組織（或網軍）。

(二) 攻擊的手段

- 惡意軟體/後門程式
- 勒索攻擊
- 分散式阻斷服務攻擊
- 網路釣魚/社交工程
- 中間人攻擊
- 網路資料竊取
- 零時差攻擊
- 供應鏈攻擊

(三) 網路攻擊流程分解

1. **偵察（Reconnaissance）**

   在攻擊的第一步，攻擊者會蒐集目標的相關信息，包括網路結構、系統配置、員工資料等。此階段可能使用工具如網域查詢(DNS 查詢)、掃描工具（如 Nmap）或社交工程技巧（如釣魚郵件）來蒐集漏洞信息。

2. **製造武裝（Weaponization）**

   攻擊者利用偵察階段蒐集的信息，選擇適合的攻擊手段進行入侵。例如：

   - 利用漏洞：使用已知的軟體或系統漏洞執行攻擊。
   - 暴力破解：嘗試通過密碼破解獲取未授權的存取。
   - 釣魚攻擊：透過欺騙性電郵或網站獲取憑證。

3. **傳送（Delivery）**

   將攻擊工具送到目標環境中，例如將釣魚信件寄至目標信箱。

4. **觸發（Exploitation）**

   入侵者的攻擊或惡意程式遭觸發，例如點擊釣魚信中的惡意連結。

5. **安裝（Installation）**

   若未阻斷觸發，攻擊者會等待該攻擊武器被觸發，並接續植入惡

意軟體或代碼，例如：

- 木馬程式：暗中控制目標系統。
- 勒索軟體：加密資料以勒索贖金。
- 後門(Backdoor)：建立長期未經授權的存取途徑。

6. **控制（Control）**

攻擊者逐漸控制目標環境與系統，並嘗試在內部網路中橫向移動，尋找更多的高價值目標，例如伺服器或敏感資料儲存設備。他們可能利用已竊取的憑證進一步提升權限。

7. **目標實現（Action On Objectives）**

這是攻擊的最終階段，攻擊者達成其目的，可能包括：

- 資料竊取：擷取敏感信息如商業機密或個人資料。
- 系統破壞：刪除或損壞資料以造成業務中斷。
- 勒索或敲詐：威脅公開資料以獲取贖金。

圖 7. Cyber Kill Chain-網路攻擊流程

資料來源: Sukhvir Notra, BIS (2024)

網路攻擊通常具有高度的計畫性和組織性，攻擊者會根據目標的弱點設計針對性的攻擊流程。防禦者需要在每個階段設置防線，例如進行漏洞掃描、強化身分驗證、實施異常行為監控等，以降低攻擊成功的可能性並減少損失。同時，提升員工的資安意識也是防止網路攻擊的重要手段之一。

三、雲端運算對資安的衝擊

雲端運算（Cloud Computing）以其高效率、彈性和成本效益，成為現代組織數位轉型的核心；然而，雲端運算的普及同時帶來了全新的資安挑戰。由於資料儲存和處理已從傳統內部伺服器轉移至第三方雲端服務提供商，資安風險隨之增加。

(一) 可能的資安衝擊

1. **資料洩漏風險增加**

   組織將敏感資料存放在雲端，會使其成為網路攻擊者的首要目標。一旦雲端存儲系統遭入侵，可能導致大量資料洩漏，對組織形象和合規性造成重大影響。

2. **共享責任模型的模糊性**

   雲端服務提供商和用戶之間存在共享責任模型，但責任範圍常被誤解，例如，雲端提供商負責基礎設施的安全，但資料保護和存取控制則由用戶負責。這種模糊性可能導致安全漏洞的產生。

3. **多租戶環境的挑戰**

   雲端架構通常採用多租戶模式，即多個用戶共享同一實體基礎設施。若隔離機制不完善，攻擊者可能利用漏洞實現用戶間的資料竊取或干擾。

4. **遠端存取與身分驗證風險**

   雲端服務強調任何時間、任何地點的存取，這雖然提升了便利性，但也增加了未授權存取的風險。弱密碼或缺乏多因子身分驗證（Multi-Factor Authentication，MFA）可能成為攻擊者入侵的入口。

5. **依賴性與供應鏈風險**

雲端運算讓組織高度依賴第三方服務提供商，一旦雲端提供商的系統遭到攻擊或發生服務中斷，可能對組織造成大規模影響。此外，攻擊者也可能通過供應鏈滲透到目標系統。

(二) 如何應對雲端運算的資安挑戰

1. **加強存取控制**

實施嚴格的身分驗證機制，包括多因子驗證和以角色為基礎的存取控制（Role-Based Access Control，RBAC）。

2. **資料加密**

確保在傳輸和存儲過程中加密敏感資料，即使資料被攔截也難以破解。

3. **定期審核與監控**

對雲端配置進行安全審核，並使用日誌監控工具檢測異常活動。

4. **清楚了解責任分工**

熟悉雲端服務提供商的共享責任模型，確保所有資安責任均有明確對策。

5. **備份與應變計畫**

定期備份資料並測試回復方案，以減少因攻擊或中斷造成的損失。

雲端運算為組織帶來巨大便利，但也讓資安環境更加複雜。組織需要在享受雲端優勢的同時，建立全面的資安策略，主動識別和減少潛在風險。只有平衡效率與安全，才能確保雲端運算真正成為推動業務的助力，而非潛在的威脅來源。

四、勒索攻擊與談判：風險與對策

勒索攻擊（Ransomware Attack）是近年來威脅組織和個人資安的主要手段之一。攻擊者透過加密受害者的重要資料或系統，要求支付贖金以換取解密密鑰。當面臨勒索攻擊時，是否進行談判成為受害者的關鍵抉擇，但這背後蘊含

著複雜的風險與道德挑戰。

(一) 勒索攻擊的過程

1. **初步感染：**攻擊者通常利用釣魚電郵、系統漏洞或惡意軟體入侵受害者的網路系統。
2. **資料加密：**成功入侵後，攻擊者會迅速加密目標資料，使受害者無法正常存取或使用。
3. **勒索要求：**攻擊者發送訊息，要求受害者支付贖金，通常以加密貨幣（如比特幣）形式進行交易，因其難以追蹤。
4. **談判或回應：**受害者需在短時間內決定是否支付贖金、展開談判或採取其他應對措施。

(二) 談判的挑戰

1. **贖金支付的道德問題：**支付贖金可能鼓勵攻擊者繼續實施更多攻擊，甚至擴大其行動。
2. **不確定的結果:**即使支付贖金,攻擊者未必提供有效的解密密鑰,或者可能再次勒索。
3. **法律風險**：某些國家禁止與特定的犯罪組織進行交易，支付贖金可能導致法律後果。

(三) 談判策略

1. **專業支持：**受害者可尋求資安專家或專門應對勒索攻擊的顧問協助，以評估攻擊規模、談判風險及回應策略。
2. **拖延與情報收集：**透過談判爭取時間，讓資安團隊有機會分析攻擊模式，並尋求可能的解密方法。
3. **尋求執法協助**：某些情況下，與執法機構合作可能有助於追蹤攻擊者或減少損失。

(四) 防範勒索攻擊的建議做法

1. **資料備份：**定期備份關鍵資料並儲存於隔離的設備，降低因勒索導致的業務中斷風險。

2. **強化網路防禦：**更新系統漏洞、實施多因子身分驗證、加強員工的釣魚攻擊識別能力。
3. **制定應變計畫：**提前準備勒索攻擊應對策略，包括與保險公司、執法機構及資安專家的合作機制。

勒索攻擊與談判是一個充滿風險與挑戰的過程。無論是否支付贖金，最重要的是提升防禦能力，減少成為攻擊目標的可能性。同時，組織應加強資安文化，定期演練應變方案，確保在遭遇勒索攻擊時能迅速回應，將損害降至最低。

柒、心得與建議

一、心得

(一)資安威脅日趨多元化和複雜化

隨著資訊技術的快速發展，駭客和惡意攻擊者的手段也日益精進，從傳統的病毒和木馬程式，發展到現今常見的勒索軟體、釣魚攻擊、社交工程和零時差攻擊等。此外，隨著物聯網（IoT）的普及、雲端運算和大數據的廣泛應用，也增加資料洩露的風險。攻擊者可以利用複雜的技術手段，突破傳統的防火牆和安全系統，竊取敏感資訊。

面對多元化的資安威脅，單一安全措施已不足應對。必須規劃多層次的防禦策略，結合人員培訓、先進技術工具以及全面的監控系統，才能有效抵禦各種形式的攻擊。同時，保持對最新威脅的警覺和持續更新防護措施，也是確保資安的關鍵。

(二)資安風險管理框架應與時俱進

隨著資安威脅的日益頻繁且複雜，資安風險管理框架也成為組織保護其數位資產的重要工具。這些框架除針對技術層面的防護，更強調全面性的風險管理，涵蓋從風險識別到應對措施的各個階段。

目前大部分的組織應已套用適合於自身的資安風險管理框架，但要確保完整發揮監管功能，除了需要組織全員參與，更須時時檢視，保持風險管理框架及時更新，才能在變幻莫測的數位環境中保持機動性，有效防護資安威脅。

(三)供應鏈管理與零信任架構是關鍵策略

在現今高度互聯的數位環境，供應鏈管理和零信任架構已成為各組織資安防護的兩大關鍵策略。供應鏈管理涉及組織與眾多相關供應商的合作，而這些第三方關係也帶來潛在的資安風險。隨著供應鏈複雜化，攻擊者利用鏈上弱點作為突破口之事件也時有所聞，加強供應鏈的安全性亦日趨重要。

零信任架構打破傳統的信任邊界，其基本假設為每一個網路節點和用戶都有可能遭受攻擊，因此需要持續驗證。它強調「永不信任，始終驗證」的原則，即使是在內部網路環境，每一次存取請求也都需要經過嚴格的身分驗證和權限檢查。

將零信任架構應用於供應鏈管理，組織可以實現對每個供應商的嚴密監控和驗證，確保每一次資料交換和存取都符合安全標準，不僅提高整體供應鏈的安全性，還能及時發現並阻止潛在的攻擊行為，有效應對資安挑戰。

二、 建議

(一)鼓勵同仁多參加資安相關之訓練課程

在現今數位化的工作環境中，資訊威脅日趨複雜，安全防護亦格外重要。建議鼓勵同仁多參加各種資安相關訓練課程，以瞭解最新的資安威脅形勢、識別潛在威脅及保護敏感資料，並強化日常工作中的安全意識。

維護資通安全應是全體同仁的共同使命，透過提升所有同仁資安知識與技能，才能更有效地防止網路攻擊和資料外洩，達到更佳的資安防護。

(二)重視量子運算對資安的衝擊

量子運算是一種革命性的運算科技，然其快速運算複雜數學問題的獨特能力，可能會使目前廣泛使用的加密技術變得脆弱不堪。由於現今資料的保護大多依賴基於數學難題的加密演算法，例如 RSA、AES 和 ECC 等，原需要相當長的時間才能破解；然而，它們卻可能在短時間內被量子運算破解，從而威脅到資料的機密性和完整性，這對依賴加密技術的金融領域來說將是一場重大挑戰。

面對此一潛在威脅，資安界已開始研究量子安全的加密技術，量子密鑰分配（QKD）就是其中一種被廣泛關注的技術。儘管量子運算離大規模應用還有一段時間，但其對現有資安架構的潛在威脅已經無法忽視。為了應對這場即將到來的變革，建議持續瞭解量子計算及相關安全技術的發展，提前做好準備。

參考資料

1. 本次訓練課程講義資料 (2024)。
2. 中央銀行 (2022)，「零信任架構介紹」，中央銀行資訊通報第 295 期。
3. Gartner (2024), “Top Cybersecurity Trends for 2024,” Feb.
4. CrowdStrike (2024), “Global Threat Report,” Feb.
5. Check Point (2024), “Cybersecurity Inside & Cloud Computing Security Report,” Final Ed., March.
6. The Quantum Insider (2024), “Chinese Scientists Report Using Quantum Computer to Hack Military-grade Encryption,” Oct.
7. The Express Tribune (2023), “China hacks military-grade encryption using quantum computer, poses threat to West,” Jan.
8. NIST (2024), “Announcing Approval of Three Federal Information Processing Standards (FIPS) for Post-Quantum Cryptography,” Aug.
9. LogPoint (2024), “XZ Utils Backdoor: Supply Chain Vulnerability (CVE-2024-3094),” April.
10. Lockheed Martin (2015), “Gaining the Advantage – Applying Cyber Kill Chain Methodology to Network Defense,” Nov.