出國報告（出國類別：開會）

出席2023年Gartner安全與風險管理峰會（Gartner Security & Risk Management Summit）

服務機關：數位發展部資通安全署
姓名職稱：陸芃緁視察
派赴國家：英國
出國期間：112年9月24日至9月30日
報告日期：112年12月28日

摘要

顧能公司（Gartner）為國際資訊科技分析和研究顧問諮詢公司，其研究範圍涵蓋資通訊科技產業、市場趨勢、人力資源及相關管理實務運用等主題，每年皆辦理多場資訊科技相關研討會或峰會，其中以安全與管理風險為主題的峰會於 2023 年共辦理 6 場次。

本次參與 112 年 9 月 26 至 28 日於英國倫敦舉辦的峰會，其發表的主題包含應用程式安全、組織韌性、雲安全、網路架構安全、隱私及零信任等主題，提供網路安全管理領導者、資安長或是相關決策者瞭解如何精進網路安全風險管理的策略，並針對目前因應新興科技趨勢所致的不確定性提出未來預測，使組織面對衝擊時能有更良好的適應力，本報告將說明本次參與議程的重點，並提出心得及建議，做為日後推動相關工作之參考。

內容

壹、目的

本次會議將提供安全與風險管理領導者、資安長及相關決策者提供研究和建議，使組織能在風險持續升級的世界中做好準備，並提供客觀且可執行的的見解，使領導層能重新構建組織的安全策略並與業務目標對齊，促進組織可在最優先關鍵的事項做出更明智的決策。

安全與風險管理領導者或相關決策者必須推動組織安全數位轉型的變革，不僅需要關注防禦，而要能夠預見並管理安全風險，以追求卓越，本次會議也可幫助組織不斷提升安全風險管理技術的靈活性和韌性，為了解未來目前最新威脅的資訊及新興科技產業發展趨勢，爰派員了解網路安全風險管理、雲安全、組織韌性、零信任架構及網路安全網狀架構等議題內容，以學習更好的安全與風險管理發展策略及模式。

貳、 會議過程

本次會議為期 3 日，自 112 年 9 月 26 日至 9 月 28 日止，於英國倫敦 ExCel 國際會展中心辦理，參加場次如下表：

日期	參加場次
9 月 26 日	Gartner Opening Keynote： Dispelling 4 Myths That Prevent Cybersecurity From Unlocking Its True Value
	Outlook for Cloud Security
	Outlook for Network security,2023
	Accelerate Cybersecurity Effectiveness： 8 Tactics to Deliver Value Faster
	Outlook for Organizational Resilience, 2023
9 月 27 日	Guest Keynote： Never Give UP
	Crossfire： Zero Trust Debate
	The Future of Security Defense in Depth： Cybersecurity Mesh
	Keynote： Gartner Futures Lab： Its Most Provocative （Far） Future Predictions
9 月 28 日	Guest Keynote： Using the Science of Behavior Change to Reduce Risk
	2023 Zero Trust Predictions
	The Top Predictions for Cybersecurity, 2023-2024
	Outlook for Cyber Risk Management, 2023

參、 會議重點摘要

一、 Gartner Opening Keynote： Dispelling 4 Myths That Prevent Cybersecurity From Unlocking Its True Value（打破阻礙網路安全發揮正確價值的四個迷思，講者：Christopher Mixter, Jie Zhang）

「網路安全可以為企業產生巨大的價值，但前提是從業人員要有勇氣挑戰錯誤觀念，並且能不受過時原則的限制。」，在開幕主題演講中，兩位講者討論了網路安全領導者必須採取的決策和步驟，以實現他們應得的成功，這段討論強調了在網路安全領域採用最小有效心態的重要性，並一一打破了一些常見的迷思。

講者首先提到了最小有效觀念（Minimum Effective Mindset）的重要性，為了得到最大的效益，網路安全需要在業務參與、技術和人才方面採取最小有效的觀念，最小有效是一種有計畫並以投資報酬率為導向的途徑，最小有效心態強調以最小的投入來實現最大的成果，並強調在達到目標時，最大程度地減少資源、成本或其他投入，以下針對四個阻礙網路安全發展的迷思摘要說明：

(一) 更多數據等於更好的保護

在網路安全領域中，不是追求更多數據，而是尋找所需信息最小量的理念。這樣的方法有助於提高網路安全投資的可見性，確保各項投資可解決實際存在的漏洞，而不僅是增加數據量。講者也提到「與其繼續追求更多數據和更多分析，有能力的資安長們應該採用最小有效洞察（Minimum Effective Insight）的方法」，確定所需的最少信息，以便在組織的網路安全資金和該資金解決的漏洞數量之間找出問題所在，建議使用以結果為導向（Outcome-Driven Metrics，ODM）的方法來實現最小有效洞察，ODM 的作用是將網路安全和風險操作的度量指標與企業所追求的業務結果相關聯，可解釋目前實施的保護水準以及可用資金所能提供的替代保護水準，有助於更好地理解安全措施對業務的實際影響以及確保網路安全策略與企業目標的一致性，亦可幫助管理者做出明智的決策。

(二) 更多技術等於更好的保護

這個迷思可能奠基於另一個普遍的錯誤觀念，即「在不久的未來，某種技術將來拯救我們」，對技術的追求可能會讓我們在確定其實際價值之前就購買或投資，進而導致資源浪費。講者提醒，引入新技術前需要謹慎思考，確保它確實能夠提供實質的附加價值，而不僅僅是基於未來的期望，講者另補充，全球資訊安全和風險管理產品與服務的支出，預測將在 2023 年增長 12.7%，達到 1,898 億美元。然而，即使組織在網路安全工具和技術上的支出不斷增加，網路安全領導者仍然感到他們沒有得到適當的保護。「網路安全治理往往陷入一種著迷於購買設備的心態，認為總會遇到更好的東西」，講者認為資安長們必須接納最小有效工具組（Minimum Effective Toolset）的心態，即監測、防禦和應對曝險所需的最少技術，可使網路安全有自己的架構，降低管理和整合這些工具的難度，同時還要確保它們能夠協同工作，有助於提高網路安全架構的效率和可持續性。

講者另外提到，組織亦可透過人力成本的角度去達成最小有效工具的方式，確保管理網路安全工具的專業人員所需的成本和工作量相對較低，並且這種成本要低於使用這些工具在減輕風險方面所獲得的實際效益，同時採取一種架構性的視野，評估各項工具是否對保護企業的能力有增減值的效果，網路安全網狀架構（Cybersecurity Mesh Architecture, CSMA）即可評估網路安全工具對企業保護能力的影響。

(三) 更多網路安全專業人員等於更好的保護

講者提到，若僅透過招聘更多的網路安全專業人員，是無法使資安服務與企業發展的速度保持一致的，當企業快速發展時，單純增加人力資源的方法是不可行的，因為網路安全領域需要更多的綜合性和創新性的解決方案，「資安長們難以應對網路安全人才的供需不平衡，安全性是數位轉型的一個巨大阻礙，多半是因為人們普遍認為網路安全專業人員才能進行緊急的網路工作，將網路安全專業知識大眾化會是比試圖彌補人才缺口更好的解決方案。」，根據顧能公司的預測，到 2027 年，75%的員工將在 IT 部門的業務範圍外獲取、修改或創建技術，而這

一比例在 2022 年是 41%，表示有越來越多的業務部門將在不需要 IT 部門直接參與的情況下，自主採用、調整或創建技術，資安長們可以通過幫助這些業務人員構建最小有效專業知識（Minimum Effective Expertise），從而減輕團隊的負擔。

另講者補充顧能公司的一項調查發現，有高度網路安全判斷能力的商業技術人員，在開發分析時比起未具相關判斷能力者，有 2.5 倍的人更可能考慮網路安全風險，這顯示在商業技術領域中擁有網路安全意識和判斷力的重要性，且更能將網路安全整合到商業和技術的開發過程中。

(四) 更多控制措施等於更好的保護

最近一項顧能公司的調查發現，69%的員工在過去一年中曾經規避組織內的網路安全指引，而 74%的員工表示，若能有助於實現業務目標，他們會傾向規避組織內的網路安全指引，「網路安全部門十分了解這些員工們普遍存在的不安全行為，但是增加更多控制措施反而產生了反效果，被規避的控制比根本沒有控制還要糟糕」，最小有效摩擦（Minimum Effective Friction）優先考慮用戶體驗而非技術性能，可再檢視網路安全對安全控制性能的評估，顧能公司預測到 2027 年，50%的大型企業資安長將採用以人為本的安全設計，達到網路安全措施摩擦最小化及控制措施採行最大化。

圖 1：四種最小有效的觀念（資料來源：講者簡報）

二、 Outlook for Cloud Security（雲安全展望，講者：Richard Bartley）

本主題以現今雲安全的挑戰與風險、如何建立有效的雲安全及雲安全的新趨勢等三個部分進行說明，分別摘要如下：

(一) 現今雲安全的挑戰與風險

雲安全面臨的挑戰是多方面的，並且這些挑戰相互關聯，共同影響著組織的雲計算環境安全，講者提出 10 個雲安全的挑戰，如下：

1. 缺乏治理（Lack of Governance）：有效的治理策略能確保雲資源的正確使用和管理，缺乏治理可能導致安全漏洞、資料洩露或不遵守法規要求。
2. 錯誤政策（Policy Errors）：不恰當或過時的安全政策可能無法應對新興的安全威脅，導致組織易受攻擊。
3. 技術缺口（Skill Gaps）：隨著雲技術的快速發展，許多組織發現其團隊缺乏相關技能和專業知識來有效管理雲安全。
4. 共同責任的誤解（Shared Responsibility Misunderstandings）： 許多組織誤解了在雲計算模型中安全責任的分配，可能錯誤地認為雲服務提供商會處理所有安全問題。
5. 缺少指引（Lack of Guardrails）：未能設置適當的規範和限制來指導員工如何安全地使用雲服務。
6. 合規性落差（Compliance Gaps）：遵守各種法規和標準對於雲環境至關重要，合規性的不足可能導致法律風險和罰款。
7. 設定缺陷（Misconfiguration）：不正確的雲服務配置是導致資料洩露和其他安全事件的主要原因。
8. 存取權利的複雜性（Access and Entitlement Complexities）：管理具使用雲資源權限者及其許可權範圍的複雜性增加了安全風險。
9. 改變的速度（Speed of Change）：雲技術的快速更迭可能使得相關部門難以跟上最新的安全措施和策略。

10. 缺少可視性（Lack of Visibility）：在雲環境中，缺乏對資產和操作的完全可視性，可能導致未被察覺的安全漏洞。

以上這些挑戰需要透過綜合性的策略、持續的技能培訓、與雲服務提供商的緊密合作，並運用先進的技術和工具來克服。此外講者分析了以下對雲安全面臨的風險協助更好地理解和應對這些挑戰：

1. 雲複雜性（Cloud Complexity）：隨著雲服務的快速發展，其架構和管理變得越來越複雜，這增加了管理難度，可能導致安全漏洞和管理錯誤。
2. 不可控的攻擊面（Uncontrolled Attack Surface）：雲環境的擴展增加了攻擊面。開放的 API、多租戶環境和複雜的服務集等，都可能成為潛在的攻擊點。
3. 規範、合規性及主權性（Regulations, Compliance, Sovereignty）：不同地區有不同的法規和合規性要求，且持續滾動調修。保持合規並保護數據主權成為雲安全的重要部分。
4. 不安全的雲供應鏈或流程（Insecure Cloud Supply Chain/Pipeline）：雲供應鏈的安全性是關鍵，因為任何供應鏈中的弱點都可能影響整體雲安全。
5. 安全團隊缺乏解決問題的途徑或方法（Security Teams Do Not Have a Path to Remediate）：雲安全問題的解決需要特定技能和工具。如果安全團隊缺乏這些量能，將難以有效應對安全威脅。
6. 資源盜竊 （Resource Theft）：雲環境容易受到駭客攻擊，駭客可能利用盜取的雲資源進行不法活動，如加密貨幣挖礦或發動網路攻擊，或是盜取敏感數據。
7. 影響規模 （Scale of Impact）：雲環境通常支持大規模基礎架構和服務，一件資安事件可能對大量用戶和服務產生廣泛影響。
8. 數據遺失和外洩 （Data Loss/Exfiltration）： 雲存儲的數據可能因錯誤配置、攻擊或其他安全漏洞而遺失或被未經授權的使用。

以上這些風險促使組織採取綜合性策略，包括持續的風險評估、員工培訓、與雲服務提供商的合作，並投資先進技術或工具來加強雲環境的安全性，必須要留

意的是，雲所面臨的風險可能與數據中心所面臨的相似，然而兩者所部署的控制措施可能完全不同，才足以應對這些風險。

(二)如何建立有效的雲安全

雲就緒方法（Cloud-Ready Approach）指的是一種策略，用於準備和優化組織的資源和流程，以有效地遷移和使用雲服務，這個方法涉及多個面向，包括技術、人員、流程和政策的調整，以確保組織能夠充分利用雲技術帶來的好處，以下為實施雲就緒方法之注意事項：

1. 雲模式的安全需求：強調在雲環境中確保數據和系統的保護和完整性所需的安全措施、實踐或策略，包括了制定有效的安全政策和控制措施來應對雲環境中的特定安全挑戰。
2. 雲相關技能提升：涉及組織獲得與雲運算相關的新技能或加強現有技能的過程，並重視發展與使用雲技術和服務相關的能力和知識，可透過以下面向提升組織內的雲相關技能:
   (1) 建立雲卓越中心：建立一個專門的組織或團隊，致力於在組織中推動雲運算相關的最佳實踐、策略和專業知識。
   (2) 提升安全團隊的技能：在組織內提供培訓和更新關於最新安全威脅和技術的知識，以及通過不斷學習和適應來提高安全專業技能。
   (3) 在組織中推廣雲安全的重要性：鼓勵組織內成員遵循雲安全最佳實踐和採用相應的安全措施，包括提供培訓、分享成功案例和強調安全意識。

   為有效實踐上述面向，另提出以下建議:
   (1) 策略與架構：建立雲安全框架，提供一個結構化的方法來識別、評估和管理雲環境中的安全風險，設計雲基礎設施和服務時採用的安全架構和模式，有助於確保安全性貫穿於系統的整個生命周期。
   (2) 雲原生：檢視雲供應商安全能力、確立安全服務邊緣、使用雲原生應用保護平台（Cloud-Native Application Protection Platforms, CNAPP）及雲開發安全運營方法（Cloud DevSecOps），將安全整合到雲開發和維運

的持續集成/持續部署（CI/CD）流程中。

(3) 技術支援：保護容器化應用和 Kubernetes[1]（K8S）應用程式的技術及雲環境中的 API 和應用程序，防止不安全的接口和應用程式漏洞。另外使用代碼來管理、自動化基礎設施的配置及安全政策，有助於提高安全性和運營效率。

3. 安全工具的使用：通常指用於監控、管理和增強主機系統、網絡、應用程序和數據安全性的工具，這些工具有助於識別、防止或應對安全威脅和漏洞。

4. 保護混合雲：為確保混合雲環境的安全性而採取的行動和措施，包含實施安全協定、實踐和技術等。

以上這些概念構成了一個全面的雲安全策略，旨在保護雲環境免受各種安全威脅，並確保合規性，以實現安全的雲運營。隨著雲計算的快速發展和普及，這些安全措施和管理實踐，對於任何使用雲服務的組織都至關重要，組織在選擇和使用安全工具時應考慮的關鍵點，應先了解供應商工具的不足之處，建議在原有控制措施不足、系統複雜度提高或面對較高風險時，考慮使用第三方工具，隨著越來越多的企業系統遷移到雲端，建議可採取以下步驟來加強整體組織安全：

1. 評估雲安全的成功案例，了解哪些策略和控制措施有效。

2. 評估哪些成功的雲安全措施可以應用到本地或數據中心系統。

3. 考慮從雲控制安全，利用雲平台的先進技術和能力。

4. 盡可能有多種控制措施，以保持安全策略的一致性和效率。

(三)雲安全的新趨勢

近來，雲安全的新興趨勢已擴及到持續整合與持續部署（CI/CD）、開發安全運營 DevSecOps、安全數據分析與人工智能/機器學習的應用、風險排序和緩解效率、資安態勢管理的擴展、零信任架構、安全工具的持續融合、保密計算、雲檢測和回應及數據和雲主權等領域，突顯了雲安全領域的快速發展和創新，並指出組織在保護其資產和數據時需要關注的關鍵領域。

[1] Kubernetes 是一個開源平台，可用於自動化部屬、擴展及管理容器應用程式和服務。

另外講者介紹如何利用雲工具來強制執行零信任原則的方法，包括利用雲安全工具來提高企業基礎設施和應用程序的可見性、加強身份和訪問管理、增強網路安全，以及提高數據安全性等，這些措施有助於實現零信任架構，即不信任任何內部或外部的系統，而是通過持續驗證和最小權限原則來保護資源和數據。此外，由於平台工程、開發運營、人工智能/機器學習的挑戰以及雲環境變化的快速性，需要持續強調風險優先排序、安全治理、資產和活動的可見性，在面對這些新興技術和快速變化時，維持高標準的安全意識和適應性是至關重要的。

現已有多種第三方雲原生安全工具的使用，講者建議相關部門領導者應根據組織的情況匹配對應的控制措施，並考慮到 SaaS、PaaS 和 IaaS 的差異，業務部門成員與開發人員需要相互合作，嚴格控制身份和特殊權限存取並進行監控，當組織轉移到雲端的這些過程，亦可加速實施零信任架構的進度。

三、 Accelerate Cybersecurity Effectiveness： 8 Tactics to Deliver Value Faster（加速網路安全效能：提供 8 個策略以更快速度展現價值，講者：Jie Zhang）

根據顧能公司於 2023 年對董事會成員們的調查，有 64%的董事們預計將提高他們的風險承受能力，另外有 60%的董事會認為數位科技計畫是最優先的事項。而另一份顧能公司於 2022 年對企業資安長的調查，有 59%的受訪者認為他們的企業領導對數位科技投資完成的速度不滿意。有 47%的人認為降低網路安全風險的過程阻礙了數位科技執行。除了前述商業價值的因素之外，其他促使資安長加速他們計畫的因素還包含了：

(一) 提高董事會對風險的承受度：這將影響著企業的網路安全策略和資源配置。

(二) 人為因素對安全結果的影響：員工行為和文化對於網路安全的成效有顯著影響。

(三) 去中心化的數位科技決策：決策過程在組織內部逐漸分散，網路安全的策略應要跟得上這速度。

(四) 保護數位科技業務：隨著業務越來越數位化，網路安全成為核心要素。

(五) 增加董事會監管：董事會對網路安全的關注和監管越來越密集。

(六) 提升董事會的網路安全素養：提高董事會成員對網路安全問題的認識和理解，以支持更有效的治理和決策。

講者提到以上這些調查結果及因素，突顯了網路安全在現代企業治理中的重要性，以及領導層在網路安全問題上扮演者至關重要的角色，網路安全加速器是組織領導者及資安長們可以建立並持續維護的策略，其關鍵在於建立和維持一個更敏捷、反應更快的網路安全能力，並區分為以下四個類別說明:

(一) 首先必須要有以不同方式取勝的心態（Win Differently），資安長們必須要有的基本心態是有意識地執行策略並審視結果，然而更重要的是如何重新定義成功，以及如何使用不同的策略並挑戰現狀，達到以不同方式取勝的目的。

(二) 其次是使用力量倍增器（Force Multipliers），以最小的努力來抵擋傷害，或者是試圖將你的敵人變成擁護者，藉此來擴散網路安全團隊的影響力。

(三) 第三則是識別並消除阻礙網路安全進展的因素（Banish Drags），例如過時的流程或不兼容的技術。

(四) 最後則是重新分配資源（Redirect Resources），將資源從低效或不再重要的領域轉移到更關鍵的網路安全活動上。

講者從上述四個類別區分出以下 8 個策略，並提到在進行策略規劃時，應注意到影響力、需要努力的程度、時間、預算以及風險，以下針對各個策略摘要說明：

(一) 重新審視組織的商業策略（Business Strategy Review）：這是一個快速且容易成功的方法，透過團隊集體反思，確認組織內的安全計畫跟商業策略要如何保持一致，這樣的作法可提升安全部門與業務部門的協調及一致性，並且可增加成員們對組織目標的參與度。

(二) 挑戰現狀（Challenge the Status Quo）：建立一個破除常規的會議，提供一個安全的環境，授權成員們可以自由思考，可培養解決問題的能力，並且更貼近業務需求，從而讓成員感到自己被重視而更有積極性。

(三) 爭取反對者的支持（Win Over Your Critics）：部分組織內的成員認為網路安全政策是必要之惡，因為組織的監管政策，導致必須遵守這些規則，而這些人對

於網路安全計畫可能並無直接影響，然而在組織中識別並理解最大的反對者，並在實際可行的狀況下先關注他們的擔憂，或許有助於未來的討論更加順暢，甚而，若能將反對者轉變為支持者，還能建立其對改革項目的支持，增強團隊內外部的聲譽。

(四) 安全冠軍計畫（Security Champions Program）：培養組織內部成員的支持，透過安全冠軍計畫，可以更有效地提高安全訊息的滲透力，參與計畫的成員將更加意識到安全的重要性，並將這意識傳播給更多同事，這個計畫也可能發掘出潛在的安全人才。

(五) 移除不必要的控制措施（Remove Unnecessary Controls）：根據顧能公司的調查，有許多的員工會忽略組織的安全政策，在這樣的情況下，控制措施就無法達到其價值，更影響用戶體驗，對控制措施進行評估並移除，可提高操作效率。

(六) 以原則為基準的政策（Principles-Based Policies）：降低政策的規範性，著重於標的（what），而非具體做法（how），並且透過各方共同參與政策的制定，強化政策的有效性及接受度，並採用基於原則的政策框架，讓政策更貼近業務需要，而非僅作為規範和限制。

(七) 停止多餘的安全項目（Stop Redundant Security Initiatives）：重新盤點組織擁有的資源，識別、評估並停止不再需要的安全項目，因為業務優先項目隨時會變化，應該要更頻繁地審查安全計畫，減少技術支出和錯誤投資，可以將資源重新分配到更關鍵的領域。

(八) 嘗試機器人流程自動化（Trial RPA）：自動化重複性和一般性的安全任務，若組織內有 60%的控制措施都是技術控制，則可將其部署在數據庫或應用程式上，確保所有安全任務都按照同一標準和流程進行，並將它們整合到自動化儀表板中，減少手動工作，提高整體安全團隊的效率，另講者提醒，執行時仍應謹慎勿過度依賴工具。

圖 2：八種加速網路安全效益的策略（資料來源：講者簡報）

講者最後總結，應評估組織情境以了解業務驅動因素，並透過以下方式加速安全計畫：

(一) 以不同的方式獲勝：實施解決挑戰的新方法。

(二) 發揮力量乘數的效益：採取創造動力的行動。

(三) 消除阻礙：減少抑制加速的限制。

(四) 資源重定位：將有限資源集中在推動最佳成果上。

四、 Outlook for Organizational Resilience,2023（2023 年組織韌性展望，講者：Arthur Sivanathan）

韌性，是每個組織的目標，也是當今錯綜複雜世界的必要戰略措施，然而，很少組織能在實務上完全實現，有韌性的組織可從其準備工作中獲得 4 個好處，首先是可以更快的識別威脅，其次是可以抵抗或承受初期衝擊的能力，再來是擁有良好的復原速度，以及擁有從衝擊中更快因應的能力。

講者提到如何為組織開發一個韌性框架，面對日新月異的科技發展，網路攻擊不斷增加，並且變得越來越複雜，若再加上新一代的生成式 AI，組織在營運上變得更加複雜。有鑑於此，講者提出當組織試圖建立韌性規劃時將面臨的一些挑戰，首先是關於韌性這個詞的定義或範圍，每個人對其看法不同，導致關注點不同。另組織內部的僵化，也將導致組織內部變革時對於產生抗拒，然而，最關鍵的仍是業務營運或是影

響評估，這將實際影響組織內部進行演練的規劃。因此，必須將韌性刻意設計到組織的結構中，擴及到整個組織，包含資訊、業務、採購及人資等部門，且必須有領導階層來關注整個韌性策略的實施，可能是風控長（Chief Risk Officer; CRO）、營運長（Chief Operating Officer,COO）或財務長（Chief Financial Officer; CFO），或者是一個更新更全面的角色-韌性長（Chief resilience officer, CRO）。

因為韌性樣貌不斷的演變，所以必須建立共通的詞彙，例如網路安全與網路韌性、營運韌性與業務連續性及供應鏈風險與供應鏈韌性是否都指涉同一件事?目前這些工作在組織中很多都是分開進行的。講者補充，可透過法規來達成一致性，並提出金融服務部門對於韌性的分類，英國金融服務監管機構可能是組織韌性的先驅之一，他們非常關注客戶對於服務中斷的容忍度，而澳洲稅務局的角度可能是最全面的，其包含了對資訊與通信科技產業（Information and Communication Technology, ICT）供應商及雲服務供應商的關注，雖然他們將名稱定義為營運風險管理，但大致上都圍繞著業務持續性管理、網路安全及 IT 風險管理等項目的融合，實際上正在成為營運韌性的全景。

隨著對於韌性的討論範圍越來越廣，不僅是金融服務業，組織必須要確認他們需要做什麼才能達到韌性目標，組織應該專注於協調管理而非單獨管理，必須有更完善的規劃，來面對多重和持續的威脅。由於現在眾多任務都採外包處理，且趨於數位化，導致連業務部門都有大量隱藏的資訊業務，間接使得風險轉介到業務部門，雖然可能不會發生實體損害，但會導致應用程式或數據的橫向整合議題，講者提出以下架構說明如何實現營運韌性的工作：

(一) 領導與文化韌性：領導層需要採取不同的方法，並將韌性融入組織文化中，韌性不能僅由領導層在危機時刻關注，而是必須將韌性建立和運作於公司文化之中，必須貫穿整個組織以及不同的業務單位，有效的領導對於發展、促進和維持重視韌性的文化至關重要，包括預見、回應和從挑戰及中斷中復原的能力，一個有韌性的組織文化，主要以適應性、持續學習和積極的風險管理方法為特徵，領導者負責將這些價值觀植入組織的基礎，確保韌性成為組織身份和運營策略不可或缺

的一部分。

(二) 人力/員工韌性：建立一個強大的工作基礎，以確保組織在面對挑戰時能夠有效回應和復原，這包括確保關鍵職位是否有合適的主要與備用人員，以及這些人員是否具備必要的技能和訓練，此外，也應提倡變革管理，訓練並傳授新技能予員工以適應韌性。

(三) 系統/流程韌性：建立與維護組織內部所有流程和系統韌性，將韌性整合到業務運營的每一個環節中，確保無論遇到什麼挑戰或中斷，整個業務流程都能持續運作，並以端對端的角度定義重要關鍵業務的流程及營運。

(四) 設施韌性：專注於提高組織內部設施的抵抗力和復原力，確保實體設施如辦公室、工廠、倉庫等，在面對自然災害、技術故障或其他潛在威脅時能夠維持運作，訂定有效的災難準備和應急計畫，以及對設施進行定期評估與升級，以應對不斷變化的環境和技術要求，必須要注意的是，組織內外的設施，也可能引發連鎖反應，從韌性的角度來看，須確定是否需要至另一個地點重啟營運，或是轉移到替代地點，並且根據韌性需求評估遠距工作者的風險。

(五) IT 韌性：將以下幾個關鍵因素用於設計和營運，使其具 IT 韌性

1. 可靠性：系統在面對潛在 IT 風險時能夠保持性能、安全性，並滿足服務水平目標（Service Level Objectives，SLOs）的程度。
2. 可容忍性：IT 風險所造成的明顯不良後果，能在可容忍的範圍內進行管理的程度。
3. 可復原性：組織在其明確 IT 風險容納範圍內，能夠有信心地恢復系統和數據的程度，以面對已知和未知的 IT 風險。

(六) 隨著雲業務的發展，講者提出以下 9 項原則來改善雲韌性

1. 業務對齊：利用業務影響分析（Business Impact Analysis, BIA）確認韌性需求，才能有助於關注業務需求。
2. 基於風險的原則：使用風險管理的方法以對應高頻率的瞬態故障。
3. 依賴關係映射：有效掌握所有元素並組織成一個整體處理系統。

4. 連續可用性：得以在失敗發生時限制可預見的影響。

5. 韌性設計：設計具有韌性的架構，並使用該模式在應用程式內構建韌性。

6. 災難復原自動化：可以提供快速的最低復原時間目標。

7. 韌性標準：該標準必須要可以融合要求、得以實踐以及營運。

8. 傾向以原生雲解決的方案：避免需要投資於自有方案的相關成本和複雜性。

9. 聚焦於業務功能：藉由尋求轉移應用程式的替代方案，而非僅透過故障轉移的應用程式來實現必要功能。

(七) 講者另說明從勒索軟體攻擊中復原與傳統災難復原的不同之處，並提出以下最佳實踐：

1. 確定企業對關鍵業務功能和資源的共識。

2. 向業務部門宣導錯過復原時間目標（Recovery Time Objective, RTOs）和復原點目標（Recovery Point Objective, RPOs）的影響。

3. 將數據備份到不可變的的資料庫中。

4. 建立一個隔離的復原環境並進行測試。

5. 為應用程序和基礎設施的每一層設計復原計畫。

6. 制定勒索軟體復原計畫。

7. 與所有利害關係人進行跨職能的桌上模擬演練。

(八) 當組織的供應商發生業務中斷，要如何讓業務層面持續運作?講者以下列六大構面供組織來思考供應鏈韌性的相關議題：

1. 配銷網絡：有無運輸替代方案？是否使用當地倉庫，以及有沒有備用路線？

2. 產品組合：有無標準平台或通用組件?檢視存貨單位合理化，透過降低庫存，提高資源配置效率等，進而協助組織降低成本。

3. 協作生態系統：審視該供應鏈的生態系統和合作夥伴關係，以共同監控並緩解風險，並可以在業務連續性及災難復原演練利用之。

4. 庫存及產能：有無安全及緩衝的庫存?該供應商是否有靈活的生產和物流能力?

5. 採購網絡：是否為單一來源供應商或是本地供應商？以便在不同的供應中斷時

仍能獲得所需的供應。

6. 製造網絡：重新審視關鍵供應商的製造和購買決策已具備多樣化網路，不論是本土化（Reshoring）或近岸化（Nearshoring），抑或自製或採購等決策。

(九) 第三方韌性：講者認為第三方韌性是一個重要的議題，並且有越來越多的監管機構開始關注這一點，然而部分的組織仍無法識別誰為關鍵供應商，所以首先要能識別提供最重要關鍵業務的供應商，並與該供應商建立正式協議，規範在中斷事件中如何維持營運韌性，此外，要建立一個當第三方服務失敗或中斷的業務連續性計劃，監測供應商在中斷期間繼續提供服務的能力，驗證供應商是否有健全的風險管理實踐和控制措施，尋找在現有供應商無法提供關鍵服務時，可能提供協助的替代供應商，並且也要識別可能影響第三方管理中斷能力的風險。

圖 3：組織韌性定義（資料來源：講者簡報）

講者提到可以下列 5 個步驟來設計和實施韌性計畫：

(一) 定義韌性對組織的意義。

(二) 建立一個韌性策略並且規畫執行。

(三) 設計一個治理和營運模型，具有明確的責任、明確定義的角色和職責，包括關鍵利害關係人。

(四) 建立共同目標並整合計畫和活動，以支持韌性計畫。

(五) 使用關鍵績效指標向領導階層報告。

最後講者建議，可建立一個整合式的營運韌性計畫框架，並包含 3 個部分，首先必須要有執行發起人及監督的角色，能夠了解公司政策、範圍和目標，並且負起向董事會和其他關鍵利益關係人匯報的責任；再者，計畫治理包含了組織角色和職責的定義、與計畫活動的協作、韌性度量和關鍵績效指標、對韌性報告的協調及韌性計畫的倡導者等元素；然而最關鍵的元素在於建立一個韌性計畫管理辦公室（Operational Resilience Program Management Office），將前述所有個別的功能整合到一個的單位。講者再次強調，組織韌性是一個戰略必需品，採用這些韌性原則的組織表現總是優於其他組織，最關鍵的一點則是能夠將韌性整合到業務運營和決策過程的核心。

五、 Crossfire: Zero Trust Debate(交火:零信任辯論,講者: Jeremy D'Hoinne,Thomas Lintemuth,John Watts)

本場主題為零信任辯論，主持人為 Thomas Lintemuth，贊同零信任方的分析師為 John Watts，反對零信任方的分析師則為 Jeremy D'Hoinne，以下針對各爭點摘要說明：

(一) 為什麼要嘗試零信任？

1. 正方：組織想要採用零信任的原因，第一是消除或減少攻擊面，若採取虛擬私人網路（Virtual Private Network, VPN）可能還需要進行修補管理。第二則是減少橫向移動，如果確實遭到了入侵，該如何限制影響範圍?這些都是組織實施零信任時的考量。
2. 反方:微切分技術（Micro-Segmentation）也可以達到減少橫向移動的目標，而且 VPN 自實行以來也都提供了相當安全的權限控制措施,現在只是有了一個改變定義的名稱，而這個名稱卻比各種技術的價格都還要貴。

(二) 零信任的命名

1. 正方：零信任涉及到使用者或設備的因果關係，但對 VPN 來說，只是一個二元的問題，只要有一個已驗證的帳戶，並且組態評估是良好的，就可以連線，而一旦連線了，這個帳戶就可以進去該網路的任何地方，但零信任會考量到因果

關係，讓其變得更具適應性，如果在帳號登入之連線期間觸動了端點偵測回應（Endpoint Detection and Response, EDR）事件，就會限制其連線權限，並可限制該帳戶可連線的區域。

2. 反方:組織都想實施最安全的措施，但並不代表擁有無限的預算，零信任的概念是一個典範，它是一系列的網路安全原則，我們都同意最小權限訪問、加密、數據安全、機密性及完整性等術語，而零信任就是將所有概念集合在一起的術語，這其實有助於人們站在同一個立場上。

(三) 零信任長期部署的可行性

1. 反方：無論使用什麼技術都不可能在短期內對 5,000 個資產進行微切分，零信任就有點像個花俏的新名稱，像是生成式 AI，或許短期內有幫助，但是不會長期存在。

2. 正方：是否可以獲得長期營運的成功，端視其定義範圍，如果把零信任當作一個戰略或架構，架構設計的一部分就是設定範圍，對於那些不能納入零信任範圍的事物，是否有一個明確的計畫?將定義範圍的概念視為最關鍵的工作之一，零信任不用包括一切，它可以是合理範圍內的應用程序和用戶，如果不事先定義要完成的範圍，實際上無法實施零信任。

3. 反方：所以組織礙於經費考量，必須要信任舊系統，就不用將舊系統納入實行零信任的範圍，這似乎是在最脆弱的資產周圍建造一個圍欄，只因為無法施行新技術。

4. 正方:這確實是零信任的一個挑戰，更精準的說法應該是減少信任到幾乎為零，麻省理工學院林肯實驗室曾經做了一項訪問，受訪公司普遍都認為要完整實現零信任需要多年努力，並非一蹴可幾；另以 Google 的 Beyond Corp Enterprise 為例，十年前他們的白皮書說明有些應用程式和服務無法適用於他們的零信任架構，雖然這份白皮書近期做了更新，但他們至今仍在解決這些例外情形，所以對於要執行多久必須要設定合理的期望值。

(四) 零信任施行的困難

1. 正方：舉一個我曾遇過錯誤的執行方式，該服務採用非常高度微切分的環境來構建用戶端到應用程序的分割，並在零信任上建立了一個端對端的分割概念，每個端點都為每個訪問的應用程序定義了一個策略，雖然有良好的安全性，但這過於細緻到無法構建成一個策略，因為這必須得有成千上萬個規則，當然這項服務最後是終止了。實際上大部分的組織會對用戶身分進行屬性控制，建立一個屬性列表，這些屬性驅動了決策；在應用程式方面，則對其敏感性進行評級，因此，當他們制定策略時，實際上是這些屬性具有對這些應用程序的訪問權限及端對端配對，這樣就變得更加自動化，所以當你跳脫了分割每個用戶到每個應用程式的思維模式，零信任就變得更容易實施和操作了，要注意的是，有個預測是有 50%的零信任施行將會失敗。
2. 反方：其實在 2020 年有很多成功的零信任項目，在當時的時空背景下必須採取遠距辦公模式，導致很多組織利用這個機會採取零信任網路存取，以更安全的方式來遠距辦公，如果沒有某種激勵措施，不太可能獲得資源和時間來重建組織的策略。所以我認為零信任的施行或許需要一些激勵措施。
3. 正方補充：很多人會認為組織內部已經有一個完全受保護、完全分割的 VPN，為什麼還需要零信任?其實零信任是一種風險緩解，最終的目標是優化組織的風險態勢，並不是要排除風險，所以組織可以使用零信任減少用戶在處理最不關鍵資產時的衝突，達成最小有效摩擦的模式。

六、 The Future of Security Defense in Depth： Cybersecurity Mesh（深度防禦的未來：網路安全網狀架構，講者：Jon Amato）

本主題主要討論的議題為如何改變我們對網路安全監控的方法，特別是對於資通安全威脅偵測管理（Security Operation Center, SOC）服務，能夠在被攻擊鏈攻擊前預測並阻止，當駭客已經可以建立自己的人工智慧模型來攻擊，組織或許可以思考使用人工智慧來防禦。

網路安全網狀架構（Cybersecurity Mesh Architecture, CSMA）的核心概念是識別和檢測變化的能力，人腦是我們所知最大的識別引擎，人類通常可以隨著時間的推移來理解識別正常及異常行為，故以這樣的概念進行規劃。講者並強調，過去組織在使用 SOC 的方式中，通常使用各自獨立且無法互相操作的產品，而為了讓 CSMA 得以發揮網狀的功能，必須要有協同工作的概念。

要成功實現 CSMA 前，得先理解 SOC 目前出現的障礙，例如 SOC 儀表板上的偵測反應，是否如實反應了組織所受的威脅?是否有反應延遲或誤報等情形?各工具是否相容?以及信息量過多等問題。若組織可藉由開發人工智慧來發展自動化決策，當自動化到某種程度的自主性，就可以委派給人工智慧，授權機器做出一些決定，或許可以比人工做出更合理且更快速地決定。此外，駭客常使用的戰爭迷霧（Fog of War）所製造的混亂與不確定性，使得 SOC 營運效果下降。

正因 SOC 面臨上述的障礙，CSMA 可達到分析與整合各工具之間的協作，大幅增加組織對攻擊的應對能力，有效達成更高水準的防禦效果。講者提到 2.0 版本的 CSMA 在身份網絡動態環境（Identity Fabric Dynamic Context）的監測上增加補強，例如監測這些用戶打字和使用滑鼠的方式，這種微小的行為在個體用戶間實際上是非常一致的，同一個人會以相同的節奏打字或使用滑鼠，若模式改變了，或許有些異常行為正在發生。另外，用戶所在位置的敏感性也變得更加重要，當發現用戶位置異常的情形，像是使用飛機上的無線網路，就可避免讓他們存取或使用機敏資料。

講者最後提到，因應新興科技的蓬勃發展，CSMA 的內容仍持續更迭，例如數據管理、人工智慧及自動化計算等，所以組織應開始發展圍繞這些技術的流程和政策，而 CSMA 是目前在組織環境中進行運營、監控和預測性防禦的新方法，它是一個策略、一種技術及一個營運過程，CSMA 正在改變我們看待深度防禦策略和架構的方式，建立 CSMA 並使用生成式人工智慧進行防禦，為組織打造一個可以快速部署並方便維護的網路安全技術環境。

七、 Keynote: Gartner Futures Lab: Its Most Provocative (Far) Future Predictions

(顧能未來實驗室：最具挑戰性的（遠期）未來預測，講者：Frank Buytendijk)

講者首先說明顧能未來實驗室所做的是挑戰常規，並且試圖探索事物不同的面相，未來是一個動態且複雜的系統，思考未來，預為因應可能發展的情景，有助於我們對組織戰略進行測試，使組織更適應未來；然而，有時提出某些預測，是因為不希望它發生，講者提醒，本主題所提的 10 個預測，或許聽眾會有些質疑，但可以提供一種全新的視角，進而引發組織策略的改變，以下摘要各預測的內容：

(一) **嚴正抵制機器學習**：即使在未來，人們仍傾向自己做出每天 80%的決策，而不是將它們交給人工智慧，只有 1%的高階主管認為可以使用完全自動化進行決策。這預測說明我們會抵制人工智慧決策的興起，然後向人工智慧學習，成為更好的人類決策者，提出這項預測的分析師認為人類本質上是決策性的生物，如果都外包給了人工智慧，會剝奪我們部分的人性，人工智慧當然可以取代所有常規、標準化及乏味的決策，但要注意的是，在成為某個領域的專家前，通常都是從這些基本且簡單的事情開始，如果連這些事情都被奪走，是否就不再有精通技能的機會了?另講者以自動駕駛為例，雖然道路死亡事故的數量下降了 99%，但是社會可以接受另外 1%的致命事故是由機器引起的嗎?這些道德問題到了法律層面變得難以解決，雖然我們一直以來的立場都是用戶使用這項技術，所以責任應歸屬於用戶，但是做為安全專業從業人員，這些都是機器學習興起時得參與討論的問題。

(二) **尤達[2]錯了!未來是可預見的**：到 2050 年，預測模型及模擬將變得更強大，以至於我們不再將未來視為不可預測和不確定的，就像預測一群人的行為比預測個體更容易一樣，一旦系統的複雜性超過一定程度，便可以透過更少的信息做出更好的預測，這項預測說明，複雜的系統會有湧現和自我組織的特性，這些特性可以從數學模型中推導出來，而不需要理解系統的具體細節。

[2] 譯註：尤達（Yoda）為電影星際大戰（Star Wars）系列中的虛擬角色，因該角色一句經典台詞「陰暗面籠罩了一切，未來是不可預見的」(The dark side clouds everything. Impossible to see the light, the future is.)，故本預測原文說其錯了。

(三)**「雲」在天空中**：到 2040 年，太空中的數據處理將超過地球上的數據處理，在過去 15 年間，每公斤的太空飛行成本下降了 70%。過去 10 年間太陽能每兆瓦小時的成本下降了 80%，由於太空飛行成本的下降，將能夠實現大規模的太空太陽能發電，將需求轉移到能源來源更為合適。然而，是否能將太空太陽能源送回地球的議題則仍待觀察。

(四)**活體機器人恐懼**：到 2032 年，惡意編程或有編程缺陷的活體機器人（Xenobots）將對實體環境造成破壞，活體機器人是小於 1 毫米可自我複製的合成生命形式，可以被編程以執行特定功能的人造微生物，應用於生物醫學和其他學科；然而，一個自我複製的活體機器人可能會損害它執行功能的環境，例如被設計用於清潔海洋的活體機器人，若編程錯誤，可能會造成浮游生物滅絕，對海洋環境造成不可逆的損害。

(五)**大眾化的太空戰爭**：到 2030 年，至少會有一顆低地球軌道（Low-Earth Orbit, LEO）衛星被非政府壓力團體攻擊並遭到破壞，太空發射將變得更加普及且得以負擔，非政府壓力團體將能夠建造並發射衛星，以攻擊其他 LEO 衛星，使用的戰術包括動能碰撞、定向能量或干擾，動機則可能包含政治與意識形態、激進抗議、勒索和恐怖主義。

(六)**單一全球通用身分**：到 2030 年，元宇宙應用的普及度，將使所有用戶的線上訪問徹底簡化為單一的通用身份，目前多樣的線上帳戶已對多數用戶造成難以管理的狀況，且目前的方法缺乏用戶所期望的安全、隱私和信任度，而對於元宇宙應用來說，單一的全球通用身份將滿足利害關係人對於安全、隱私和信任度的期望。

(七)**不願到校學習**：到 2028 年，62%的高中畢業生將不會上大學，看似與目前的情況完全相反，隨著高中畢業生中有 60%的人不會完成大學教育，一些替代教育的形式，如生成式人工智慧師徒制和微學習等替代方案將變得越來越受歡迎，尤其在兒童教育中相當受歡迎，而生成式人工智慧將使知識獲取更加大眾化並符合個人需求，使得在高等教育外可以更有效率的獲取相關技能。

(八) **哪裡有大量的電能?**：到 2030 年，由於全球電力供應的限制，將使得數據中心和其他基礎設施的成長率至少縮減為近十年標準的達三分之二，全球資訊和通信技術（Information and Communications Technology, ICT）產業在 2020 年消耗世界總能源不到 1%，而這比例將在 2030 年增加到超過 6%，ICT 產業總能源的消耗增長速度是全球能源產量的 8 倍，新的可再生能源並未能快速地投入使用，導致資安長們將不得不對應用程式進行運作時間限制，而大型能源的消費者可能會被要求關閉（例如美國德州的比特幣礦工）。

(九) **有限的執法力道**：到 2030 年，人工智慧的監管將會失敗，每位公民和組織都將自行保護他們的隱私和智慧財產，然而歐盟提出監管此技術的法案尚未包括可執行多任務的新型人工智慧系統，導致無法為未來做好準備，未來人們將需要對具攻擊性的數據採取行動，或許自行監管是好事，可以使人們對自己的生活或業務負起責任。

(十) **抵抗是無效的，你將會被同化**[3]：到 2034 年，90%擁有 IT 技能的員工將被科技或服務供應商雇用，這一比例從 2023 年的 30%大幅上升；另外，到 2030 年，整體 IT 預算中用於 IT 技能的支出將少於 5%，較 2023 年的 85%大幅下降，由於未來許多業務都將在雲端運行並由人工智慧完成，科技供應商可提供更好的技術及薪酬，使得擁有 IT 技能的員工若離職或退休將成為風險，最終導致所有 IT 技能集中在供應商端，但由於標準化和改進的安全措施，仍有許多人認為使用供應商所提供的解決方案，較能提升整體安全性，但組織可思考將技術專長分散或多樣化到不同的實體或層級可能會更有效。

講者最後提到，我們應該從這些預測來思考其假設的立場為何?不論是否支持上述預測，都應得到一些啟發性的想法，並進而從小決策影響未來。

[3] 譯註：此句原文（Resistance Is Futile, You Will Be Assimilated）為電影星際爭霸戰（或譯為星際迷航）中博格人的台詞。

圖 4：十大未來預測（資料來源：講者簡報）

八、 2023 Zero Trust Predictions（2023 年零信任預測，講者：John Watts）

講者首先提到，零信任的預測可幫助決策者避免失敗，在說明各個預測前，講者提到零信任預測有 3 個必須要考慮的面向，首先，零信任是安全計畫的一部分，它不一定是整體安全策略，可以僅占一部分；其次，零信任必須是奠基於風險策略的決定，所以會從組織內最關鍵影響的部分開始；最後，進行零信任的每一步都將增加其價值，當開始實行這些步驟時，實際上就已經在改善組織的整體安全計畫，以下針對講者所提 3 個預測摘要說明：

(一) 到 2026 年，超過 10%的大型企業會有更成熟及可量測的零信任計畫，至少會比今日多 1%，講者提到，目前很少看到組織有一個良好的衡量指標計畫來評估他們的零信任策略；若以商業性組織來說，董事會所關心的是投資有無相對的回報，所以網路風險量化（Cyber risk Quantification, CRQ）是很重要的，必須能夠說明隨著時間的推移，風險可以降低多少，零信任策略就跟其他的安全計畫一樣，必須經過計畫和衡量，以確保其有效性並達到適當的成熟度。此外，在規劃安全生命週期時，應於規劃與設計階段納入零信任，避免後續架構複雜化，並且在實施階段為為營運成本做好準備，以採取必要的措施或策略來應在業務運作中可能出現的額外成本或開支。

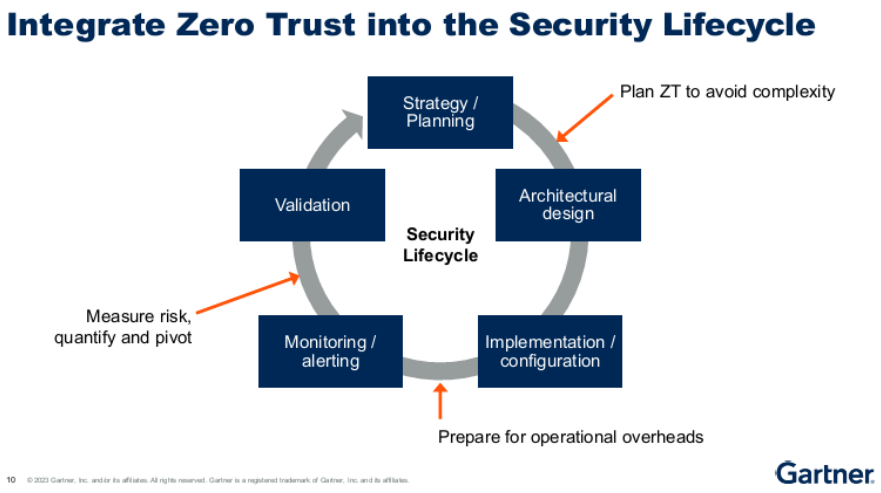


圖 5：將零信任概念整合至安全生命週期示意圖（資料來源：講者簡報）

(二) 到 2026 年，超過一半的網路攻擊將以零信任未涵蓋且無法緩解的領域為目標，講者再次重申，零信任就是風險減少及威脅緩解，但若零信任的技術非常堅固及成熟，或是領導者採取平衡策略，則可避免發生這類的預測。然而零信任有個殘餘風險是當組織所信任的供應商有缺陷時產生的問題，所以領導者必須關注實施零信任架構和技術的供應商。此外，零信任是有限的，它可以緩解橫向移動、訪問權限和權限帳戶所造成的威脅，至於若是擁有合法存取權限的惡意內部人士，零信任是無能為力的，所以領導者必須理解組織威脅的全貌，平衡組織對於網路安全威脅防禦的努力，並透過零信任來加強。

(三) 到 2027 年，有 20%的組織將在零信任網路和微切分架構的服務項目，將同一供應商列入候選名單，而這一比例在 2022 年時還不到 5%，零信任服務目前處於分裂的市場，眾多分散的解決方案以及供應商能力成熟度的問題仍待改善，如要達到成熟的市場狀態，應有統一的政策或度量指標、降低營運過程所需的時間及提供良好的安全控制效能等，零信任政策的整合將能有效提升其營運流程的能見度及管理措施。

最後，講者提到實施零信任策略需要更謹慎的規劃，需基於對組織風險和威脅的理解，還必須思考如何在組織文化和流程中融入零信任的原則，零信任需要持續的調整和改進，以確保其有效性和持續性，若沒有必要，不應嘗試將零信任應用於組織內

的一切程序，只有當風險緩解的效益超過挹注成本時，才應將零信任應用於特定使用案例。

九、 The Top Predictions for Cybersecurity, 2023-2024（2023-2024 年網路安全最佳預測，講者：Wam Voster）

講者認為安全和風險管理的決策者和領導者們能從過去經驗中汲取教訓，以便在現在獲得利益，並迎接更美好的未來，而這些網路安全的預測不僅是基於技術，還含括了其他的因素，以下就其預測摘要說明：

(一) 到 2024 年，消費者數據將可得到隱私法規的保護，但不到 10%的組織將成功地利用隱私作為競爭優勢，組織開始意識到隱私計畫得以讓他們更廣泛地使用數據，並與客戶、合作夥伴、投資者和監管機構建立信任關係，講者建議領導者應執行與一般資料保護規範（General Data Protection Regulation, GDPR）相符的隱私標準，因為隱私保護已經成為顧客執行購買決策的考量。

(二) 到 2025 年，將近一半的網路安全領導者將因工作相關的壓力更換工作，其中 25%會轉向完全不同的職位，經歷了 Covid-19 疫情後，混合工作模式改變了組織的營運模型，除了遭受攻擊面大幅增加以外，更意味著我們的工作與生活無邊界感，組織應優先考慮改變觀念，增加自主風險意識的決策，另可考量將人為錯誤視為組織網路安全疲勞的關鍵指標。

(三) 到 2025 年，50%的網路安全領導者將徒勞地嘗試網路風險量化（Cyber Risk Quantification, CRQ）來推動企業決策，顧能公司的研究指出，62%採用 CRQ 的人士提及其可信度和網路風險方面的好處，但只有 36%達成預期成果，CRQ 很少產生可執行的決策且仍存在許多限制，而網路安全領導者應實施決策者所需的量化分析。

(四) 到 2026 年，10%的大型企業將擁有一個全面、成熟且可衡量的零信任計畫，而目前這比例不到 1%，一個成熟及廣泛部署的零信任施行需要整合多個不同的組件，這可能變得較技術性和複雜化。然而，部署零信任並不代表可以擺脫目前的

威脅，應優先考慮對最關鍵資產的風險緩解，將零信任措施與其他安全策略結合，並設定合理期望值，因為這並不是一次性的投資。

(五) 到 2026 年，超過 60％的威脅偵測、調查和回應（Threat Detection, Investigation and Response, TDIR），將利用曝險管理資料來驗證和優先處理偵測到的威脅，而這比例目前不到 5%，隨著軟體即服務（SaaS）和雲應用的普及，組織需要範圍更廣、可視化更好及可以不斷監控威脅的中心位置，TDIR 即提供了這樣的平台，提供組織監測風險和潛在影響的完整樣貌，講者建議組織可實施持續威脅暴露管理（Continuous Threat Exposure Management, CTEM）計畫，幫助組織主動管理內外部威脅的影響。

(六) 到 2026 年，70%的董事會將包含至少一名具有網路安全專長的成員，網路安全領導者需要認識董事會和企業的風險胃納，不僅要展示網路安全計畫如何防範未然，還要展示它如何提高企業承擔風險的能力，講者建議資安長預先適應這一變化，以促進董事會對網路安全的支持。

(七) 到 2027 年，將有 75%的員工在 IT 部門的業務範圍之外獲取、修改或創建技術，這一比例較 2022 年的 41%有所上升。人人都可成為技術人員，資安長的角色和責任範圍正從負責控制措施轉變為風險決策促進者，重新構建網路安全營運模式是應對此轉變的關鍵。

(八) 到 2027 年，50%的資安長將採取以人為本的的精神，並納入他們的網路安全計畫中，根據顧能公司的調查，超過 90%的員工承認，在知道會增加組織風險的情形下，仍於執行業務時規避網路安全政策，引入以人為本的理念重點來提升用戶體驗，藉此減少安全營運時的摩擦。

十、 Outlook for Cyber Risk Management, 2023（2023 年網路風險管理的展望，講者：Jie Zhang）

目前影響網路風險管理的環境因素有網路領導技能短缺、生成式人工智慧、網路戰爭、供應鏈相互依存性及快速變化的監管環境等等，講者另提出顧能公司所建立的

網路風險管理技術成熟度曲線，目前達到過高期望峰值期（Peak of Inflated Expectations）的項目為網路風險量化，顯見組織目前多半較關切這項技術，領導者們應考量每一個控制措施的成果是否與付出的成本有相對的價值。

講者以 5D 模型來談網路風險管理的展望，以下分別摘要說明：

(一) 動態（Dynamic）：在數位環境快速變化條件下，採取一個持續與適應性過程，使用風險分類來達到遵循最佳實踐、進行風險量化與定性風險評估的目標，而網路風險管理軟體將有助於將上述的分類納入工作流程中，並提供相關數據以做出明智決策，此外，動態風險治理（Dynamic Risk Governance，DRG）將成為網路風險管理的核心。

(二) 分散式（Distributed）：能夠個別快速應用，並為個別領域的成功業務營運貢獻具有指標性結果，從分散的角度來看待事物，考量多數員工會規避組織內的網路安全政策來達到他們的業務目標，提升員工網路判斷（Cyber Judgment）能力似乎可成為一個新方法，可降低風險暴露並讓更多員工展現高度的網路判斷力，此外，轉變營運模型，可使得 67%的領導階層希望更多的技術工作可直接在業務部門完成，而非資訊技術部門，以前述兩種面向可達成分散式決策的目標。

(三) 可辯護的（Defensible）：網路風險管理必須要有易於理解且合理的成果，能夠證明執行網路風險管理對業務結果的貢獻，講者建議使用影響分析及網路安全計畫績效管理，因為決策者需要易於理解的投資數據和攤銷計算，以便能夠做出可辯護的決策。

(四) 數據驅動（Data-Driven）：基於組織相關的事實必須是可計算且相稱的，風險管理軟體的核心能力在於得以透過持續控制監控（Continuous Control Monitoring, CCM）或其他操作工具（如 VM, CAASM, CSPM, CCM, SIEM 及 SOAR 等）來實現自動化且即時的目標。此外，隨著對新興風險及內外部要求的反應增加，以及監管環境的變化，目前網路風險管理軟體會加強融合第一道防線和第二道防線的措施。

(五) 決策支持（Decision Enabling）：到 2025 年，75%的網路風險管理軟體供應商將與專業風險數據經紀人（data broker）合作，以豐富其網路風險量化的功能，並能夠提供可辯護的結果，有助於風險擁有者做出與價值和風險成比例的明智決策。

網路風險管理是現代業務管理的重要組成部分，它必須整合到更廣泛的數位環境及業務流程中，領導者需要考慮將網路風險決策過程嵌入整個組織中，使組織成員得自主做出決策並利用技術，此外，通過統計數據與建模，將網路風險與業務結果相聯，最後，則應有一套簡易且可辯護的方式向非網路安全人員解釋如何嵌入戰略決策和業務流程中，促使決策層（或董事會）投資並支持業務優先事項。

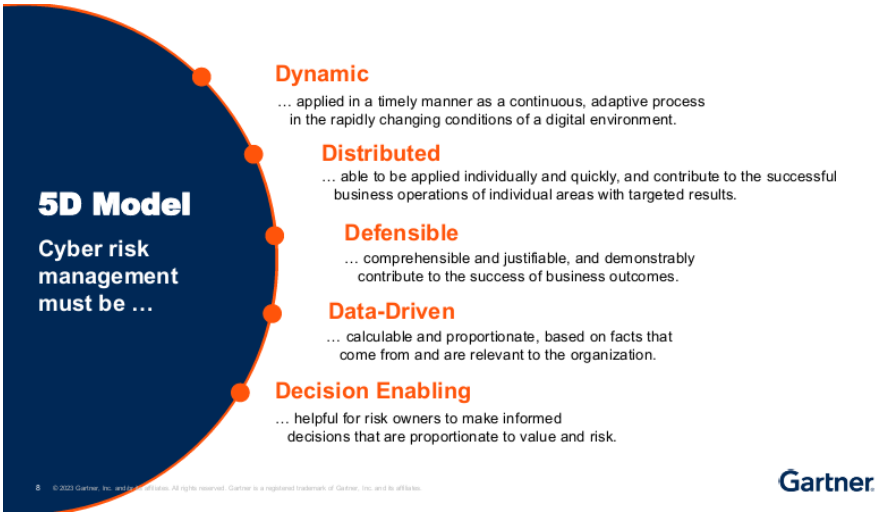


圖 6：網路風險管理 5D 模型（資料來源：講者簡報）

肆、 心得與建議事項

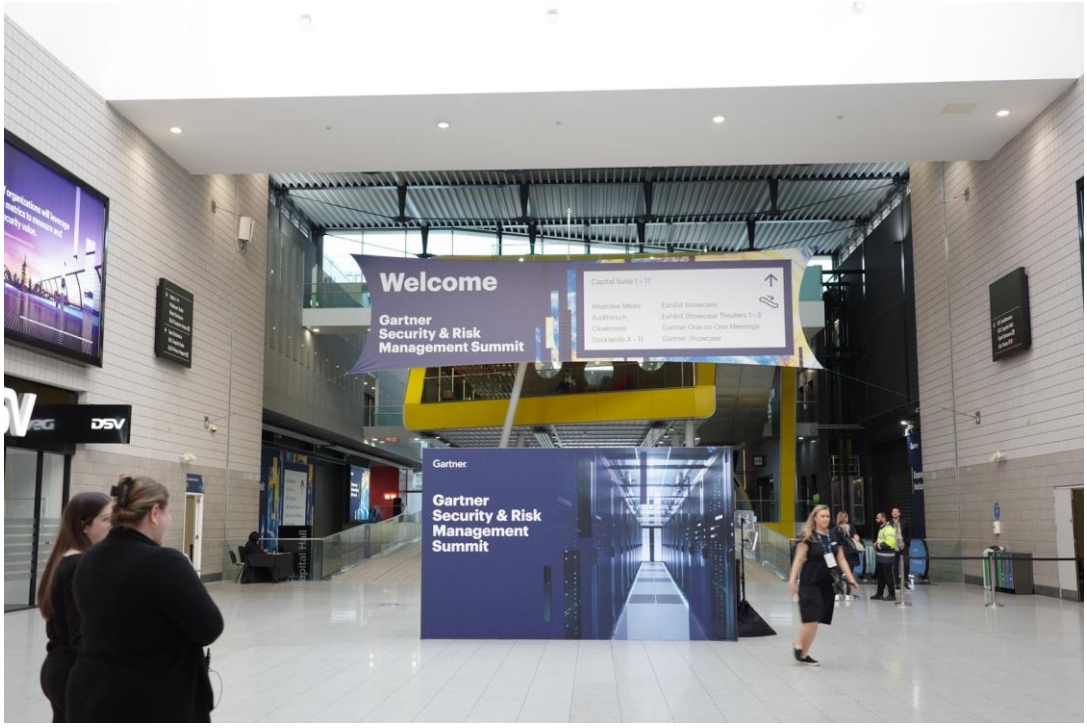
本次會議分享了多種關於安全與風險管理相關的分析結果及預測趨勢等報告，對於公私部門的組織提供諸多策略面建議，以下從本次參與主題提出幾點值得關注的議題與建議：

一、 就會議中所分享網路安全發展的常見迷思，例如更多數據、技術、網路安全專業人員及控制措施並不等於更好的保護；另面對日益複雜的雲環境及現行公部門上雲政策，以及零信任計畫越趨成熟及更多員工將具備專業技術等趨勢，可作為後續資安作業研議參考。

二、 有關組織韌性的措施，首先應將韌性於組織文化中建立和運作，並貫穿整個機關以及不同的業務單位，確認關鍵業務功能和資源、將數據備份到不可變的資料庫、設計應用程式和基礎設施的復原計畫及關注供應商與第三方韌性等議題，相關概念亦可融入我國現行推動機關資安作業要求，協助機關面對多重及持續性的威脅。

三、 類此會議可獲得最新國際資安趨勢發展及新興科技未來走向等，有助於了解全球科技及資安議題趨勢，進而回饋至我國推動資安相關策略及作法，建議可持續參與以掌握全球技術及資安面臨之問題與因應策略。

伍、 附錄-會議照片



照片 1:會場指示

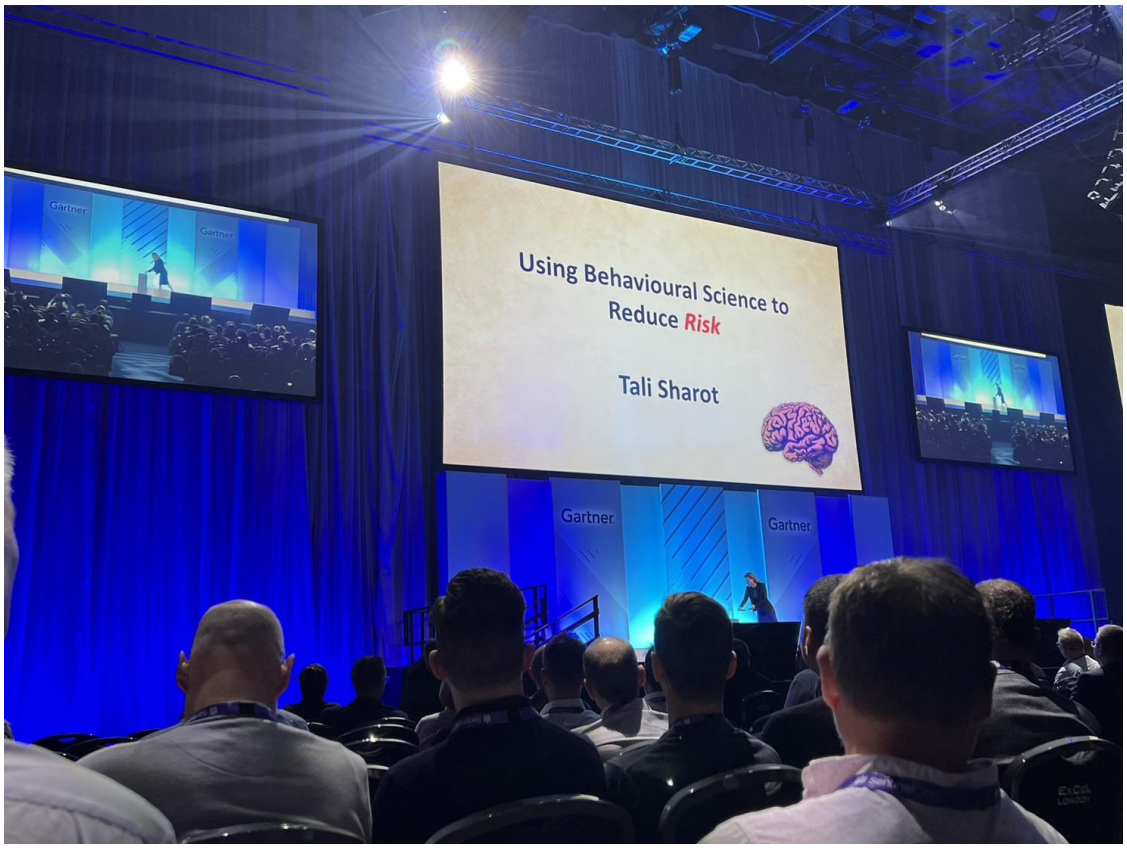
照片 2:參展廠商展示處

照片 3:開幕主題演講

照片 4:雲安全展望主題分享

照片 5：第二日主題演講

照片 6：交火：零信任辯論的三位講者



照片 7：第三日主題演講

照片 8：2023 年零信任預測主題分享