出國報告（出國類別：開會）

參加安全與風險管理研討會(Gartner Security & Risk Management Summit)

服務機關：台灣中油股份有限公司
姓名職稱：翁仲正電腦軟體工程師
派赴國家/地區：日本
出國期間：113 年 7 月 23 日至 113 年 7 月 27 日
報告日期：113 年 8 月 22 日

摘要

Gartner 於日本舉辦之安全與風險管理研討會議程，內容針對不斷變化的數位風險情勢和韌性策略進行探討，邀請各領域專家、學者及業者分享經驗，演講議程多達數十場，包含生成式人工智慧風險、雲服務安全、資料保護、漏洞管理等網路安全策略及風險管理，本次研討會主題為在複雜世界中建立網路安全韌性，其中複雜世界表達出網際網路危機四伏、錯綜複雜 ，更顯現出韌性的重要。雖然網際網路風險重重，但為了提高作業效率和滿足客戶需求， 網路服務已成為企業營運不可或缺的一部分，在數位轉型的過程中， 不僅要投資先進的資訊技術，相對的安全防護策略及機制，更應納入整體性的風險評估和制定應變計畫，以確保企業在面對潛在威脅時，能夠迅速有效地應對，維持營運的穩定性與持續性。

目次

目的.....4

過程.....6

具體成效.....15

心得及建議.....19

本文

壹、目的

由於資訊與通訊技術的快速發展，網際網路與日常生活已密不可分，許多事務皆可透過網路即時辦理，大幅縮短業務處理的時程，及增加人際溝通的便利性。面對數位化的時代，網路服務已經成為企業運營和發展的重點項目，利用網路來提升業務效率和競爭力 ，縮短決策和執行的時間，降低成本及優化資源配置，並進行新市場的拓展。但在網際網路與企業營運關係緊密相連的情況下 ，眾多的資安風險也隨之而來，且企業面臨的網路威脅也越來越多樣化和複雜化 ，這些威脅不僅可能造成企業的財務損失，還可能損害企業的聲譽和客戶民眾的信任。 對於日益嚴峻的網路威脅 ，企業更需採取有效的防護措施，來保障自身的資訊作業環境，並應建立緊急應變機制，使業務運營持續不致中斷。

資訊處為健全資訊安全管理制度，已於 95 年間導入國際資訊安全管理系統（Information Security Management System，簡稱 ISMS）標準，並持續落實資訊安全管理系統之有效性，目前已逐步依資訊應用之進展，訂定相關作業要點，但就所對應的控制措施之實行，仍須多方面瞭解外界的發展趨勢，藉以審視目前公司資安防護部署，是否有可調整精進之對策 。

本次 Gartner 於日本舉辦的安全與風險管理研討會(Security & Risk Management Summit)，主旨為「在複雜世界中建立網路安全韌性 (Building Cybersecurity Resilience in a Complex World)」，是相當適合做為應對快速且多變威脅手法之方針。由於近年來地緣政治因素逐漸升溫，攻擊的來源已上升至國家層級，因此加強網路安全韌性對於組織的持續營運尤為重要。另外，近年來公司積極推展人工智慧的應用，但人工智慧所帶來的風險也讓資安情勢更加複雜多變。本次研討會匯集各方的專家、學者及相關廠商，研討資安風險的演變，以及資訊環境韌性的應對策略，三天的研討會議程中，提

供多個領域範疇的專業演講，內容包含生成式 AI 到風險與合規管理、安全指標、雲端安全、資安治理與政策、資料安全、漏洞管理等主題，涵蓋近期重要的資安議題，也是目前公司所需面對的課題，藉由本次國際研討會，汲取各界在資訊安全策略的建議 ，對於提升個人網路安全的視野相當有助益。

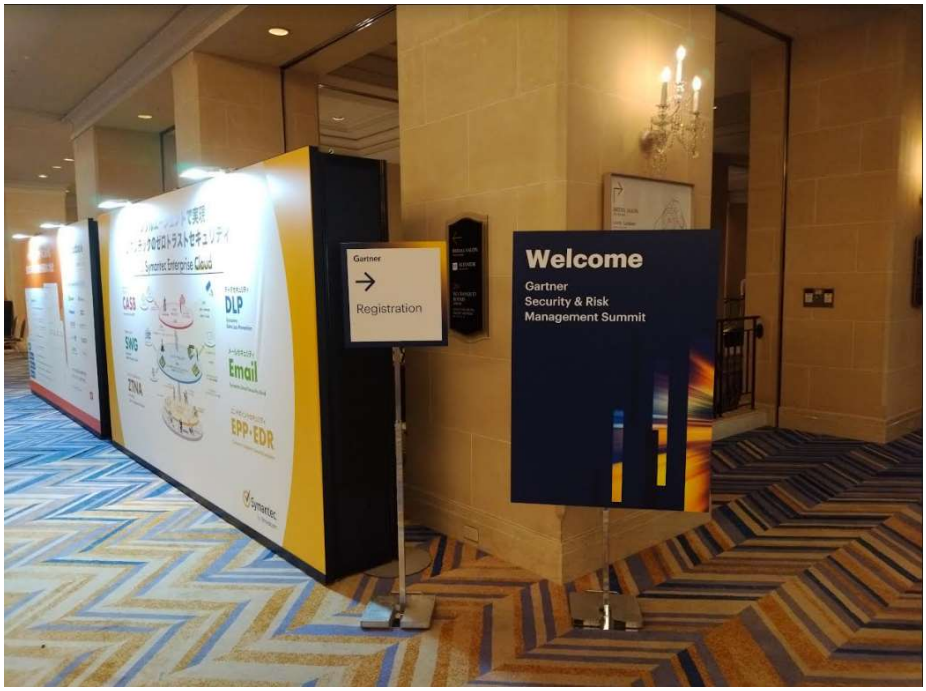
貳、過程

本次出國期間為 113 年 7 月 23 日至 27 日，其中研討會舉辦的期間為 24 日至 26 日，共計有 3 天，開幕主題演講題目是「 Augmented Cybersecurity: How to Thrive Amid Complexity」，有關本次出國行程、議程內容、會場地點、研討會會場入口及展場照片，分別如表一、表二、圖一、圖二及圖三。

起迄日期	天數	到達地點	詳細工作內容
113 年 07 月 23 日	1	台北->日本	出發前往日本
113 年 07 月 24 日至 26 日	3	日本	參加 Gartner Security & Risk Management Summit
113 年 07 月 27 日	1	日本->桃園	返回台灣
合計 5 天			

表一、出國行程表

圖一、舉辦地點東京台場



圖二、研討會會場入口

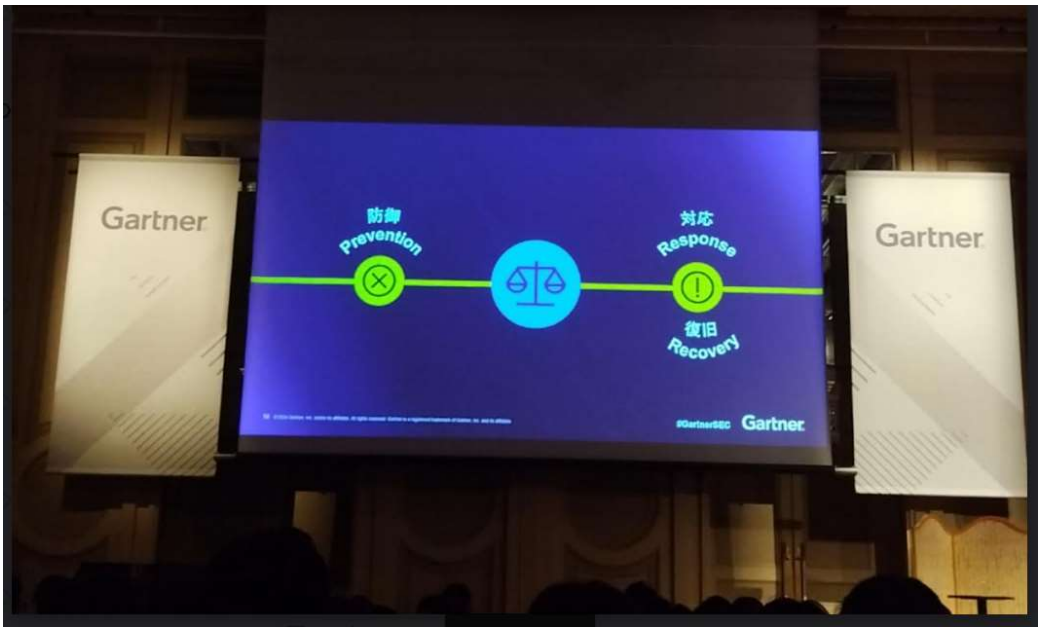
圖三、研討會會場

• Cybersecurity Vision and Strategy	• Application Security
• Cybersecurity management governance & policy	• Cloud Security
• Cybersecurity operating model	• Endpoint Security
• AI in cybersecurity	• Network Security
• Business Resilience and Continuity	• Privacy
• Zero Trust	• Risk and Compliance Management
• Identity and Access Management	• Security Awareness, Behavior and Culture
• SASE and Mesh Architectures (Evolved)	• Security Talent and Skills Management
• Data security and governance	• Ransomware
• Cyber-Physical Systems Security	• Security Monitoring, Detection and Response
• ESG and Diversity, Equity and Inclusion (DEI)	• Executive communication and metrics

表二、會議議程主題

由於本次研討會於同一時間舉辦多場演講，因此，僅能從中挑選較符合目前公司資安需求之議題聆聽，第一天開幕演說(如圖四)內容將研討會各議題進行統整，主要是以增強網路安全的韌性為出發點，提出多項策略如下:

1. 除了建置防禦機制外，更應將「回應/恢復」的優先順序提高至與「防禦」相同級別。
2. 網路風險範圍應涵蓋第三方供應商。
3. 由於生成式人工智慧的發展快速，為確保人工智慧運用的安全，未來所需的防護資源將會大幅增加。
4. 利用控制框架盤點現有資安防護設備，以確認是否有冗餘及不足之處。
5. 建構資安工作人員韌性的策略。



圖四、開幕演講

第二天的主題演講題目是「日本的安全與風險管理」，內容指出其管理以 Cybersecurity Framework (NIST)2.0 為基礎建立分析矩陣，將常見的安全威脅、外部環境變化(如法律法規、地緣政治)、技術演進(如雲端、行動人工智慧)等議題，分別與治理、識別、防禦、偵測、回應、復原等研討因應作為，並對安全治理、工作方式、資料與營運變化的安全性提出新的策略，簡單說明如下:

1.安全治理

每年至少一次向管理階層進行威脅情勢及國際法規報告，以利於管理階層評估網路安全情勢，掌握資安風險。

2.資料保護

由於企業所擁有的資料眾多且分散，須由管理者、使用者及資安部門共同擔保護資料責任。

3.因應營運演變的安全作為

為配合企業營運型態轉變如遠距工作、雲端服務或生成式人工智慧，資安作為可

由過去的攻擊行為分析及強化防護轉變為預防及自動化復原。

而在本次主題演講中提及一個觀念「專注掌握風險的變化，而非僅關注風險本身」，值得進行風險的評估作業時，多加思考的部份。

此外，本次於研討會議程的選擇分別以資安治理、防護機制及新興技術發展等層面，擇定之演講議題包含零信任網路、密碼學趨勢、生成式人工智慧安全、雲服務安全、第三方風險管理及網路安全韌性等，並參訪現場資安相關廠商攤位，以下係對三天會議所參與演講之內容進行整理簡述(現場情形如圖五)：

(1)零信任網路

捨棄傳統隱性信任(implicit trust)方式，採取持續性的動態信任等級方式存取資源，等級評定可基於身份及上下文(context)，如地理資訊、連線時間等，將端點整合至零信任架構，採取統一的端點管理工具，並可使用雙因子驗證或 ITDR (Identity Threat Detection and Response）工具 ，強化身份驗證機制。然而實踐零信任策略涉及許多工具整合，應先盤點組織現有相關設備，建構合適的安全架構。

(2)生成式人工智慧

目前企業對於人工智慧安全的投資經費仍有不足，相較於傳統的攻擊方式，對於生成式人工智慧的攻擊手法，主要是惡意詢問輸入，如提示注入、惡意輸入，有幾種與人工智慧安全相關的方向須注意，分別是檢測異常內容、資料保護及應用程式防護，因此，可透過模型的可解釋性及透明性與模型管理、監控、更新等方式著手 ，並提升模型對抗攻擊的能力，雖然使用生成式人工智慧將會耗費更多安全成本，但相對地也會替企業帶來更多營收成長。

(3) 密碼學趨勢

為保護資料的完整性、機密性及真實性，通常會利用密碼保護 ，並可確保

資源授權的合法性，在資訊系統會採取金鑰方式實踐密碼學的理論，以目前的運算能力須耗費許多時間才能解開金鑰，但未來隨著量子電腦的普及，部份過去常用金鑰的密碼演算法將很容易被破解，對於現行的金鑰系統會造成衝擊，各國也開始進行研究加深計算複雜度之密碼演算法。

(4)網路安全韌性

網路安全的韌性主要是避免營運中斷，致使企業信譽受到影響，因此，韌性應考量客戶或民眾的容忍度，建構韌性的益處有縮短發現威脅的時間、減少事件發生時的衝擊及加快復原速度，企業也應該於支援主要(核心)營運的系統或設備，設計備援機制及其安全架構。預先規劃恢復關鍵資訊系統設備和營運的策略。復原的策略應先由管理階層排定業務的優先順序，做為計畫制定的考量，並將營運韌性納入管理文化。

身份衛生(Identity Hygiene)與資安情勢(Posture)管理可以增強韌性，身份威脅的因應策略分為預防、偵測及回應，身份衛生具有預防的作用，可減少非法入侵者的攻擊面；偵測範圍涵蓋資安情勢改變之因應及攻擊行為的發生；回應策略則是快速識別威脅，以上每個階段皆須分別藉由不同的管理工具。

(5)因應勒索軟體的策略

首先建立勒索軟體事件復原計畫，包含復原的優先性、事件處理流程、在事故的每個階段中，使用 RACI 模型。而建立團隊人員的韌性也是策略之一；當事件解決後，審視復原計畫流程是否有須修訂之處。

當面對被加密資料無法復原時，若支付贖金可能易成為其他攻擊者的目標，而被加密的資料也有被出售的可能性，因此，對於重要的資訊資產應使用備份系統，確保重要資料皆已備份，並建構安全的架構保護備份資料，對於備份資料定期進行資料復原演練，以確認資料的有效性。

(6) 第三方風險管理

有關第三方的風險管理可分為第三方控制措施、偵測第三方網路安全事件及第三方事件的衝擊，第三方風險管理責任分別是由業務管理者決定是否於合約簽訂載明或是接受風險，而資安部門應對第三方風險的嚴重性提供專業建議，並提出因應的對策。另外須對企業委託的所有第三方進行重要性評估，篩選出重要的第三方，訂定第三方應急計畫及辦理第三方事件演練，由風險迴避改變成風險處理，以防範來自第三方的未知網路風險。

對於網路安全作為可以與重要的第三方合作，如分享資安情資、事件應對策略等，共同建構網路的韌性，其他風險管理方式尚有維護第三方人員聯繫名單、定期與重要第三方開會、評估第三方的網路安全狀態等。

(7)網路安全與網路韌性

網路安全是為了保護網路資產，對人員、技術、流程等進行整合；網絡韌性是指系統從不利情況中恢復以及系統因應壓力、攻擊或不利條件的能力。此外，網路安全控制措施的評估可參考 NIST CSF v.2.0 建立控制矩陣，這對於網路韌性建立是十分重要的，而網路安全與網絡韌性量化的評估原則會所差異，例如網路安全是以防護的覆蓋率或權限控管等為主，網路韌性的考量項目會是復原時間、計畫及演練等。

(8)雲服務安全

雲服務的安全應依不同的雲服務架構(SaaS、PaaS、IaaS)選擇相對應的安全管理機制 ，如 SaaS 可用 SMP、SSPM，PaaS 與 IaaS 可用 CNAPP、CWPP，但對於身分管理、安全架構及風險評估則是相同的，雲服務的身份權限可採用 CIEM(雲端基礎架構權利管理)，使用者與雲服務的存取管理可利用 CASB(雲端存取安全性代理程式)，結合多個不同的安全性原則 ，雲服務的 SaaS 架構可用 SMP 集中管理各項資源及應用程式狀態。

(9)曝險管理

曝險管理的目的主要是要瞭解攻擊者如何繞過層層管制，由於攻擊的範圍持續擴大，由使用者終端至第三方都有可能是曝險之標的，曝險管理是讓企業持續地評估其資訊資產的可視性、可存取性和脆弱性。而安全漏洞有時會出現在意想不到的地方，傳統的漏洞管理已無法因應攻擊面擴大的情勢，可使用 CTEM(持續威脅暴露管理)持續性評估潛在威脅和安全曝露，分為五個部份：界定、發現 、優先排序 、驗證及動員 。當漏洞因某些原因無法修復時，可藉由補償性控制措施，但有時只能部分解決這個問題，無法完全移除風險。


Gartner
クラウド・セキュリティ中級編:
混在するクラウド・セキュリティに
どう対処すべきか
デール・ケッペン
Gartner


認証情報の脅威に対するレジリエンスを高めるテクノロジとツール
Gartner

圖五、演講議程現場


Gartner

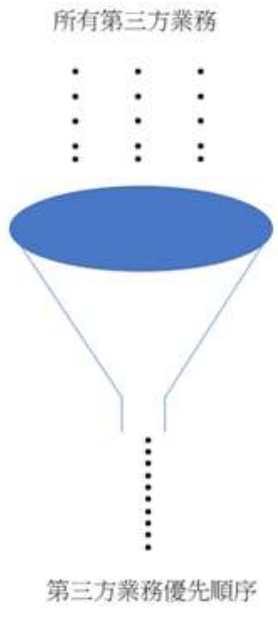
參、具體成效

資安的風險管理是相當複雜，隨著網路服務應用的層面逐漸擴展，非法入侵者的攻擊面變得更加廣泛，再者運用雲服務及生成式人工智慧所衍生的資安問題，使得網路情勢更加複雜多變，傳統的網路防護策略須再調整，本次透過參與研討會講者所提供之策略，反思目前公司所訂定的資安方針或機制，是否有可借鏡之處，做為具體成效之說明，從聆聽的議題選擇網路安全韌性、零信任架構及生成式人工智慧三個安全管理項目， 由講者對於三項議題的說明，將所獲得的想法敘述如下。

本次會議的主題闡述在複雜的世界建立網路安全的韌性，揭櫫面對危機四伏的網路世界，強化網路安全的韌性，是目前適合採取的因應策略，針對重要資訊技術之發展，探討其安全與風險之管理。 本次研討會有提到 75%的網路專業人士認為當前的網路情勢較過去 5 年更具挑戰性，但資安人力卻是持續短缺，因此，會議有特別提到資安人員的韌性，也是網路安全韌性十分重要的一環，須顧及人員的福利及訓練。有關資安政策的制定、預算需求或是風險管理，講者認為應由高層進行決策，目前公司資安相關政策的推動，每年至少會由資安長召開一次會議，審查資通安全事項之規劃與推動，與講者傳達的理念相符。過去企業對於網路安全的理念是決不容許失敗（Zero Tolerance for Failure)，對於防護攻擊面廣泛的資安同仁，長期以來容易產生無力感，進而影響網路安全韌性的強度，及降低事件發生時的應變復原處理效率，據調查有 62%的資安領導人在一年間至少經歷到 1 次的倦怠感。因此，講者認為了可持續地保護企業，將「應變和恢復」提升到與「防禦」同等的重要地位，容許資安事件的發生，過去網路服務應用侷限時，相對地攻擊手法變化較少，著重於資安防護的策略是有效的，但隨著企業營運對於網路服務應用層面的擴張，及資訊技術日益複雜與種類繁多，傳統的資安防護難以全面涵蓋，若將資源一味投入於防護機制，成效恐會不如預期。面對今日多元且變化不斷的攻擊手法，再加上可攻擊面的增加，對於異常事件仍應保

持警戒，但對於資安事件的發生不須太過於驚慌，只要遵照既定的事件應變及復原策略進行，則可降低企業的損失；而網路韌性的培養和強化則應由平時做起。

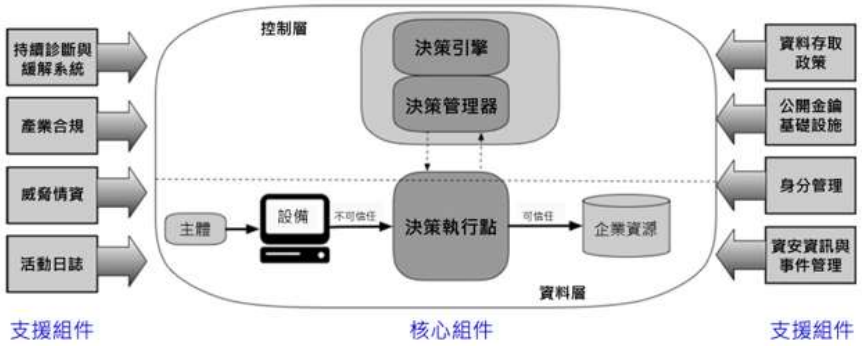
為維持網路安全的韌性而提升投入「應變和恢復」的資源時，考量資安事件發生可能影響企業各部門的運作，對於應變策略的訂定應由企業各部門共同合作，甚至須納入第三方的應變策略如第三方發生服務中斷時之應變。對於第三方風險管理，根據調查儘管對於第三方已發現有網路風險，基於某些原因，約 40%的企業管理者仍繼續使用該第三方，這是屬於企業的風險接受，但相對的第三方應變策略就應包含當接受的風險發生時，所須遵循的因應流程。講者提出企業營運持續應導入第三方網路風險管理（TPCRM），以目前企業逐步將部分營運導入的雲服務為例，須訂定當雲服務發生中斷或資安事件時之應變機制。而 TPCRM 的管理步驟可分為識別第三方、風險評估、風險緩解、監控及合約議定，首先經由識別第三方將對企業營運具關鍵性或有接觸企業重要資料的第三方篩選出來(如圖六)，以做為後續風險評定及應變優先順序之參考。在企業業務委外比例逐步增加的趨勢下，第三方風險管理已成為強化網路安全韌性的重要議題。



圖六、篩選重要第三方業務統

由於傳統網路邊界的模糊化，單靠資安防護設備仍有不足，使得身份權限的管理相對重要，本次研討會於不同的會議演講也皆有提及 IAM(身份管理)的策略，足見身份管理是網路安全的關鍵點，傳統的驗證方式通常採用密碼或憑證，其中憑證濫用已成為威脅的因素，動態認證機制將是未來身份管理的趨勢，雙因子驗證是其中一種方式，傳統身份管理與零信任架構(Zero Trust　Architecture、圖

七)的差別在於傳統方式為信任但需驗證，零信任架構則為任何時間點皆採不信任的狀態。而零信任架構並非單一產品，而是多種網路安全產品的整合。



圖七、零信任架構　　圖片來源: 國家資通安全研究院

NIST 早於 2020 年 8 月已公布「SP 800-207 零信任架構」，將零信任架構分成核心組件與支援組件，決策引擎為核心，包含身分鑑別、設備鑑別及信任推斷 3 大關鍵技術，零信任架構的建置通常是逐步完成，首先盤點企業所有的資安防護軟硬體，因為許多零信任架構的設備已存在企業環境，但如何相互整合則是建構零信任架構的重點。而端點的防護整合是最關鍵的，因其具多樣性及作業地點的多變性，端點常是攻擊的源頭，經統計預測未來三到四年內，超過 60%的數據洩露是由於端點或安全工具配置不當造成的。最後，通常建置零信任網路會先由技術層面著手，卻忽略了制定策略及架構設計的重要性，須注意零信任並非是萬能的技術，可以阻絕所有外部的攻擊，而只是透過零信任架構，減少攻擊面，例如有良好的端點安全管理，可減少攻擊的起始途徑。

對於減少攻擊面，講者有提出幾項建議如下；

1. 列出端點的應用程式、使用者及其權限的清單，以評估當前狀態。
2. 僅允許核准的應用程序，並限制正常行為的執行。
3. 構建設備之控制措施，可利用內建於主機的防火牆，或是透過作業系統的強

化規則 (hardening features)。

4. 須識別技術上過時但仍在使用的軟硬體系統，以及調整資安工具的錯誤配置。
5. 持續性監控端點行為。

在疫情期間為避免新冠肺炎傳染，許多企業採取居家上班的模式，以減少人與人的接觸，而疫情後動態工作環境已成為常態，但卻衍生出端點管控的問題，講者提出幾項管理策略主要是將原本仰賴公司內部網路進行管理的端點、身份安全工具，轉移至雲平台，利用條件存取政策進行管理，另須限制未受管理端點的存取權限。最後，在講者所總結零信任的幾項建議中，其中一項可以納入評估的是整合端點的身份及網路安全工具至 SIEM，以取得單一數據的來源，進行主動威脅追蹤。

生成式人工智慧（Generative AI）在企業中的應用越來越廣泛，它不僅能提高作業效率，且能提高營收，卻也產生有別於傳統的攻擊方式，常見的攻擊手法透過查詢攻擊（Query attacks) 獲取有關模型內部運作的信息，或是利用惡意的詢問，破壞數據的完整性(Data poisoning)，因此，模型管理、資料的保護及異常輸入(出)的偵測，是生成式人工智慧安全的重要工作，預估到 2026 年，生成式人工智慧所需的網絡安全資源仍快速增加，進而使應用程式和數據安全上的支出增加超過 15%。對於生成式人工智慧安全的實踐，仍是由企業治理開始，訂定可接受的使用政策，重新檢視資料分類與落實存取管理，對於用戶申請、證明和控制，建立系統進行記錄和審查，實施 AI 信任、風險和安全管理 TRiSM(AI Trust, Risk, and Security Management)框架，其中 TRiSM 控制措施可用於模型運維（Model-Ops）、資料保護、對抗惡意攻擊、模型管理控制以及異常內容檢測，而最終仍須持續治理、監控、驗證、測試和合規，以降低使用生成式人工智慧所產生的資安風險。

肆、心得及建議

過去常在國內參加各界舉辦的研討會，很榮幸有這個機會，能被選派出國參加 Gartner 在日本舉辦的 Security & Risk Management Summit ，藉由許多專家精闢的演說，汲取最新的資訊安全與風險管理，會場並有知名的資安廠商參展，可以瞭解資安防護及管理工具發展趨勢。本次研討會參與的場次大多是由 Gartner 分析師主講，因此，內容多以資訊安全策略方針為主，對於產品介紹著墨較少，如此安排的方式可於會議瞭解風險的管理，再至會議展場與廠商訪談適用之管理工具，我認為資訊安全的管理須先有政策建立框架後，制定出各項控制措施，再依控制措施的目的尋找適合的產品，可避免資安設備的選定不盡正確。

由於會議內容涵蓋資訊技術多個領域，在建議上會聚焦在重點議題的策略方向及安全強化；開幕演講提出防禦與應變復原應具相同等級的概念，這是在攻擊面持續擴展的情形下，建議可以採納的策略，畢竟網路應用服務之提供已由內部網路到雲服務及第三方，若採取過去全面防護的做法，已難以顧及，再者對於資安人員的韌性更是一大挑戰，因此，容許資安事件的發生應該要被接受，但重點是各資通系統的應變計畫是否完善，尤其是影響公司營運的關鍵系統之應變及復原程序，更是須多方考量規劃，而計畫是否周全，就須依靠假想多種情境進行演練確認及步驟調整。最後就是快速復原，當資通系統運作遭受影響或無法復原時，如何縮短恢復正常服務水準的時間，備份/備援機制是常用的方法之一，更重要的是備份資料保護，以及增加重要資料還原測試的頻率，以確認資料的有效性。此外，將應變復原作業程序應融入日常作業，可以避免事件發生時過於慌張或過於生疏。

對於防護的策略，如同演講所提可由身份管理著手，由於攻擊者通常須取得權限後，才能進行系統破壞或竊取資料的動作，過去一次性的驗證或單一簽入(single sign on)，在身份驗證上相對便利，但已難防範現今的攻擊手法，而零信任架構具備完善身分管理的功能，但其整體架構須由各種設備相互整合，若要實踐零信任架構並非單由購買設備可以達成，因此在逐步建構的過程中，為達成動態驗證，利用多因子驗證當是常見的初期身分管理方法，目前公司已對於入侵風險較高的服務採用多因子驗證，建議可逐步擴大適用範圍，以摒除傳統帳號密碼驗證的缺點，降低因身份驗證所產生的風險。

強化資訊作業環境設備的「可視性」對於預防是相當重要的一環，因為入侵的途徑常藉由缺乏管理的設備進入，而能夠掌握內部網路中的所有資通設備，可避免遺漏的設備因缺乏管控或系統軟體過時，產生可供駭客攻擊的漏洞，為降低人工盤點疏漏的風險，公司已有引進相關工具，建議可持續擴大網路環境可視性的範圍，相信資安風險之預防是有所助益。

隨著委外業務的增加，無論在防禦、應變及復原皆須考量第三方的風險，而要進行第三方風險管理建議由識別開始，對委外業務的重要程度進行排序，評估委外可能的風險來源，如遠端作業的管控、第三方人員使用的設備、委外業務的備援、資料的保護/保密等，依風險來源編訂相對之因應計畫，特別是當委外業務發生中斷時，是否有其他替代措施，此外，為避免關鍵業務長期委外而失去控制，宜考量逐步回歸由公司自行辦理。以上的建議主要包含四個方向分別是提升應變復原的重要性、評估零信任架構、擴大網路可視性範圍及第三方風險管理。