CYCRAFT WHITE PAPER

資安曝險調查白皮書

EASM White Paper

本報告由奧義智慧規劃執行，國家資通安全研究院（簡稱資安院）
之前瞻研究籌獲中心協助共同完成。

國家資通安全研究院
National Institute of Cyber Security

2024.09

2024 台灣資安曝險調查盤點

95% 有偽冒風險

63.5% 有外洩資料

50.8% 有憑證瑕疵

盤點了 87 家公司與 58 個政府單位，涵蓋 6 大產業、歸類出 8 大風險類型，特別針對曾被勒索軟體攻擊過的機構，掃描外網與暗網曝險情資。

本白皮書蒐集前述實際數據，量化政府單位、電子上中下游、金融機構與醫療產業等各產業的資安衛生 PR 值後，發現：電子中游、政府單位與金融業在外部攻擊面上有較高風險；當結合暗網情資分析時，則是以政府單位、電子下游、金融業為前三大攻擊目標。企業可根據此白皮書的技術解決方案與管理策略建議，量身訂製改善計畫，系統化且有效降低曝險風險。

前言

近年來，網路世界急速演變，新興技術如物聯網、區塊鏈和人工智慧的使用逐漸顛覆了我們對傳統網路邊界的認知。這些技術不僅打破了既定的網路界線，更在企業架構中導入各種非實體的資產，進而導致資產被使用但未被識別的隱藏問題。當我們無法確切管理隱匿的數位資產，也將提高相對的安全風險。

2022 年，Gartner 提出了 CTEM（持續威脅曝露管理）的概念，希望解決企業環境中、不明確資產邊界導致的資安風險。因此，奧義智慧研究團隊遵循此理念，匯集被動情資及大數據資料，針對此次普查對象進行資安曝險調查，以達到下列目的：

1. **預視企業潛在風險類別**
   將風險特性聚焦成八大風險類別，預視企業潛在的外部攻擊面，讓企業識別自身組織風險範疇，進一步制訂風險修補策略，並持續管理與監控曝險因子。
2. **比較台灣產業資安風險**
   本次普查研究涵蓋六大產業 (包含金融業、政府機關、傳統產業、電子上游、電子中游與電子下游)，透過非侵入檢測方式描繪各產業的外部風險，同時比較各大產業的資安概況。
3. **提供資安防禦策略規劃**
   透過比對駭客組織利用的曝險向量與威脅，提供企業管理層各產業最佳資安防禦建議與規劃，作為強化產業資安策略之參考指標。

產業分類依據及評估方式

此次普查對象包括台灣上市公司與政府單位，共計 87 家公司以及 58 個政府單位。在普查所有公司中，我們依照指數彙編分類來區分產業別，其中以傳產及金融單位為大宗。其中電子上游包含設計、製造、封測，如台積電、聯發科、日月光，中游包含面板、EMS，如台達、友達，下游包含資訊通路、電信服務等，如聯強、仁寶。

此外我們也針對近期（資料搜集時間為 2024 年 3 月 26 日至 4 月 15 日）ransomwatch 上公開遭勒索軟體攻擊、以國外為主的 129 家公司進行分析，並比對這些公司與台灣上市公司與政府單位的曝險結果。

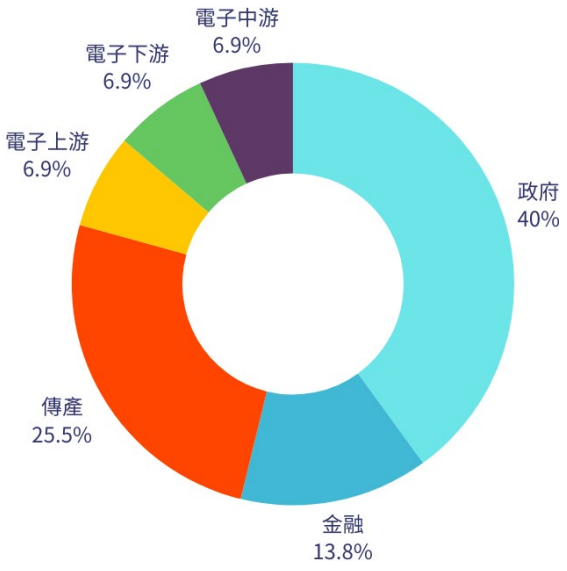


圖 1 普查結果產業分布圖

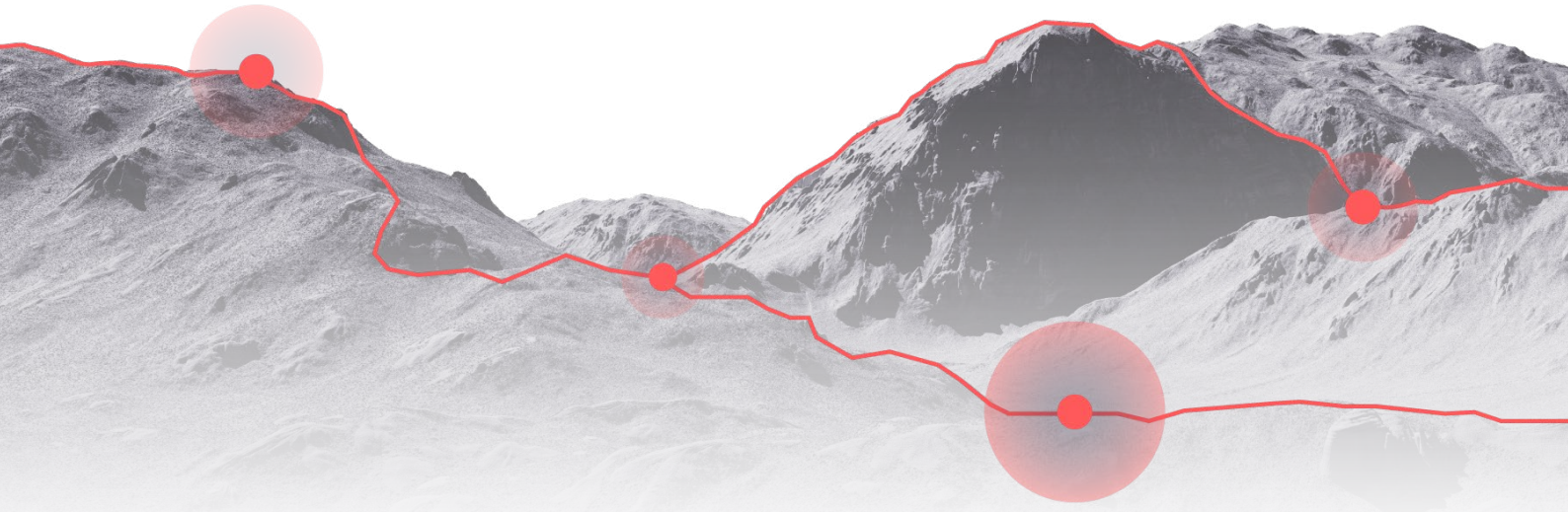
外部攻擊面管理（External Attack Surface Management, EASM）是一種安全技術，用以識別和管理組織在網際網路上的可見資產，以及潛在的安全漏洞。這包括未被識別或被遺忘的資產，例如未受保護的伺服器、域名、雲服務和開放端口等。EASM 旨在勾勒內部資產的全貌，預判攻擊者可能濫用的外部攻擊面，幫助組織減少未知的安全風險，並更好地保護其資訊系統與資產。

外部攻擊面管理與其他幾種常見的安全技術（如弱點掃描（Vulnerability Scanning）和入侵與攻擊模擬(Breach and Attack Simulation, BAS)）的主要差異如下：

1. **弱點掃描（Vulnerability Scanning）：**
   - **目的**：識別特定已知資產的已知弱點，例如作業系統、應用程式和網路設備中的漏洞。
   - **範圍**：通常針對組織已知並管理中的內部和外部資產。
   - **運作**：進行定期掃描，對已知資產進行評估，並產生相關潛在漏洞的報告。
   - **差異**：弱點掃描主要評估已知資產的安全狀態，EASM 可以更廣泛地識別和管理企業的全部數位足跡（包括未知資產）。

2. **入侵與攻擊模擬（Breach and Attack Simulation, BAS）：**
   - **目的**：模擬真實的攻擊情境，測試組織的防禦能力。
   - **範圍**：通常聚焦於模擬攻擊者的行為，測試特定存取控制和應對程序。
   - **運作**：透過自動化工具模擬各種攻擊類型（如惡意軟體、網路釣魚等），檢查防禦措施的有效性。
   - **差異**：BAS 專門測試和改進現有的存取控制和應對策略，EASM 能在更廣的範圍內識別可能被攻擊的資產。

外部攻擊面管理的獨特之處在於它不僅能識別和評估已知資產的安全風險，還能揭示組織未知、未控制或忽略的資產，並將發現到的威脅，根據其對應資產在企業中的定位進行排序，提供更貼近企業營運的安全風險評估，讓相關人員在處理風險時更有所適從。此外，EASM 常常依賴自動化工具來持續監控和更新資產的狀態，從而實現持續的安全監管，「全面的外部視角」是 EASM 與其他安全技術最大的不同點。



奧義智慧科技研究團隊在本篇白皮書中針對八大風險類別（如表一） - EmailSecurity、CertificateHealth、SslTlsStrength、IPDomainReputation、DnsSecurity、DnsHealth、NetworkSecurity、DarkWebLeak，共計 233 項資安風險進行掃描，透過普查台灣各產業，建立全面的資安風險評估。掃描範圍為企業對外攻擊面（External Attack Surface），包含但不限於 Domain、IP、URL 等，且檢測過程中遵循一般訪問方式取得相關配置設定，不包含任何滲透、攻擊過程等侵入式行為。同時，由於我們長期監控和分析暗網市場中正在販售的端點及帳密資訊，可進一步回溯各筆資料所屬的組織，作為企業外洩曝險分析的另一面向。

表（一）：普查掃描類別介紹

風險類別	簡述	測試項目案例
EmailSecurity	EmailSecurity 檢測 28 項常見的郵件伺服器設定，包括檢查 SPF、DMARC 記錄完整性、MTA-STS 設置、FCrDNS 檢測、SMTP 安全性等，確保郵件系統運行安全。 忽略這些檢測項目可能導致郵件服務易受釣魚攻擊、垃圾郵件影響，危害組織資安聲譽。	1. 缺失相關 SPF（寄件者政策框架）記錄：SPF 是一種 DNS TXT 記錄，用於識別哪些郵件伺服器被允許代表特定域名寄送郵件。缺漏 SPF 記錄表示該域名沒有明確規定哪些郵件伺服器被授權得以寄送郵件，這可能導致偽造郵件和釣魚攻擊，攻擊者可以在未經授權下寄送看似來自該域名的郵件。 2. 缺失 DMARC 紀錄：DMARC 可決定當電子郵件未通過 SPF 或 DKIM 驗證時，該通過、隔離或拒絕此郵件。缺漏 DMARC 紀錄將使相關原則的制定變得複雜與缺少判斷標準。
CertificateHealth	CertificateHealth 檢查憑證各方面的安全問題，確認基於憑證的通訊及身份認證是否有資安風險，包含了 22 項不同的項目，如：演算法、金鑰、序號、SAN 支持、自簽名、憑證不匹配、信任、過期、未來開始時間、到期警示等。 忽略此檢測項目可能導致憑證安全漏洞，使通訊易受竊取和偽裝攻擊，影響身份認證及網路通訊的可靠性和保密性。	1. Certificate with weak signature algorithm：此功能會檢測憑證是否使用了較弱的簽名檔演算法，這可能導致安全性風險。 2. Certificate with very short key size：檢測憑證中使用的密鑰大小是否過小，這可能會降低加密強度。
SslTlsStrength	SslTlsStrength 檢測企業利用 SSL/TLS 的對外服務，分析 SSL/TLS 協議錯誤設定帶來的資安風險，檢測項目包括檢查通訊協定弱點、漏洞，強制使用安全加密套件，防範協定攻擊，確保通訊安全。 忽略此項目可能導致密碼被解密、通訊被竊取，危及系統機密性和完整性。	1. NULL ciphers：支援 eNULL/NULL 加密套件，即不提供任何加密。 2. Anonymous NULL ciphers：Anonymous NULL ciphers 是一種加密配置，不提供身份驗證，意味著客戶端和伺服器之間的通訊沒有經過驗證，容易受到攔截和竊聽。這些加密套件容易遭受「中間人攻擊」，因此不建議使用。

IPDomainReputation	IPDomainReputation 檢測 IP 或域名在黑名單上的聲譽，評估對通訊和資訊安全的潛在風險。 此檢測項目反映了組織過往在處理資安事件（如：垃圾信件、殭屍網路等等）上的信用程度。	1. Blacklist：IP 或域名已被網路聲譽服務列入黑名單，表示他們被政府官方或執法單位視為具有潛在威脅。這可能使其服務受到限制，需面對隨之而來的監控與可能的法律後果。 2. Mail Server Blacklist：郵件伺服器已被列入黑名單，表示它被識別為垃圾郵件或惡意活動的來源，將使該伺服器寄出的郵件被郵件提供者封鎖或標記為垃圾郵件。
DnsSecurity	DnsSecurity 檢測 DNS 安全性，透過檢查 SPF、DMARC、DNS 記錄是否受 DNSSEC 保護，確保 DNS 記錄受到適當的保護，預防 DNS 相關攻擊和漏洞。 忽略此項目可能導致 DNS 相關攻擊、DNS 記錄竄改等，危及網站的可用性和資訊安全。	1. Badly configured localhost records：本地主機記錄使具有活躍使用者的網頁伺服器容易遭受跨網站指令碼攻擊。 2. SPF record is not protected by DNSSEC：SPF（寄件者政策框架）是一個透過驗證寄件者 IP 地址，來檢測電子郵件真偽的郵件驗證系統。當 SPF 記錄未受 DNSSEC 保護，攻擊者即可利用偽造電子郵件進行攻擊，並危及電子郵件溝通的完整性。
DnsHealth	DnsHealth 檢測 DNS 健康狀態，透過檢查 DNS CNAME 記錄指向 IP 地址、存在於區域頂點、與其他 RR 共存等，確保 DNS 記錄符合最佳實踐，避免可能的資安風險和運作問題。 忽略此項目可能導致 DNS 解析錯誤、造成服務中斷、影響域名解析正確性和效率。	1. DNS CNAME record points to IP address：在域名系統（DNS）中，CNAME（規範名稱）記錄用於將一個域名別名指向另一個域名。當 CNAME 記錄直接指向 IP 地址時，它會繞過解析過程，造成負載平衡、故障切換和其他與 DNS 相關的功能出現問題。此外，這可能暴露基礎 IP 地址，以及相對應的安全風險。 2. Multiple SOA records found at the zone apex：在區域頂點發現了多個 SOA 記錄，違反了區域頂點僅有單一 SOA 記錄的要求。
NetworkSecurity	NetworkSecurity 檢測網路安全性，透過檢查是否缺少必要的 HTTP 安全性標頭，以及 HTTP 通訊的錯誤設定等問題，確保網路通訊和資料傳輸安全，並檢測可能的攻擊和漏洞。 忽略此項目可能導致網路應用程式遭受攻擊、資料外洩，危害使用者隱私和系統安全。	1. Missing HTTP security headers：應用程式缺少建議的 HTTP 安全性標頭，這些標頭對於提高應用程式的安全性至關重要。這些標頭包括 'Cache-Control'、'Clear-Site-Data'、'Content-Type'、'Cross-Origin-Embedder-Policy'、'Cross-Origin-Opener-Policy'、'Cross-Origin-Resource-Policy'、'Content-Security-Policy'、'NEL'、'Permissions-Policy'、'Referrer-Policy'、'Strict-Transport-Security'、'X-Content-Type-Options' 和 'X-Permitted-Cross-Domain-Policies'。 2. Set-Cookie' doesn't contain secure attributes：當使用 HTTPS 協議時，應在 Set-Cookie 中設置 HttpOnly 和 Secure 屬性。
DarkWebLeak	在暗網中發現被販賣的個資、帳號。	1. 識別在暗網上提到的組織資訊、外洩憑證，以及與網路攻擊或非法活動有關的訊息。 2. 偵測從駭客論壇和暗網市場中被竊取的使用者名稱、密碼和其他敏感資料，這些資料可用於未經授權的存取。

資安曝險普查與風險趨勢

在此次普查的 145 個組織或企業中，我們共檢測出 18,704 項資安風險，也就是平均每間公司都會有超過 100 個資安風險。根據這些資訊，我們定義了「資安衛生 PR 值」，區分各組織或企業的資安衛生排名百分比。資安衛生 PR 值越高，代表企業的資安曝險程度低、整體資安態勢較好。

我們比較了各產業後（如下表二），發現電子中游產業的資安風險，不論是單就數量、或是以嚴重性加權後，都是相對危險、具有較高的風險。但與已遭受勒索軟體攻擊的組織相比，台灣各產業的資安風險都相對較低。

表（二）各產業資安衛生 PR 值

	公司數量	發現風險數量	平均每間公司風險數量	資安衛生 PR 值
傳產	37	2110	57.02702703	46
金融	20	1902	95.1	52
電子上游	10	944	94.4	31 (需改善)
電子中游	10	1661	166.1	20 (需改善)
電子下游	10	994	99.4	57
政府	58	7544	130.0689655	51
產業平均	145	15155	104.5172414	-
勒索軟體受駭公司	234	46353	198.089	-

不同產業的風險類別差異分析

在本章節中，我們進一步聚焦八種風險類別，探究產業特性之差異是否也將體現在其風險類別上。

一、電子中游的整體資安風險高於其他產業 50%

根據上表（二）電子中游廠商平均具有 166 個資安風險，相對於全體平均的 104 個風險高出 50%，顯示了電子中游產業整體而言具有較高的資安風險。即使我們以不同風險類別進行分析，電子中游在 CertificateHealth、DarkWebLeak、DnsHealth、DnsSecurity、NetworkSecurity 五個領域，都相對表現不彰。

電子業普遍具有相當高的資安風險，除了電子上游產業（如：台積電、聯發科、日月光）近年開始重視資安，逐漸導入各項資安防禦技術，較為成熟之外，電子中下游產業在各項資安指標皆位居落後。例如在 DnsSecurity 類別中，資安衛生指數為 21，低於其他產業，電子中游在 NetworkSecurity 也以加權資安衛生指數 23 落後於其他產業。

相較於電子上游已推廣並施行的資安標準規範（如：SEMI E187 等），電子中游仍沒有制定相關的資安標準。電子中游廠商多半專注於生產及加工關鍵零組件，雖然自有 IT 技術能力、選擇自行建置開發許多服務以節省成本，但在資安議題上卻不一定有足夠的專業技能。除此之外，因為電子中游廠商較無終端品牌的市場壓力或能見度，在與品牌形象相關的資訊安全資源（DNS、Certificate、SSL）投入上也相對較少，種種因素皆導致此產業需承擔較高的資安風險。

SslTlsStrength

	發現風險數量	平均每間公司風險數量	資安衛生 PR 值
電子中游	80	8.00	43
電子下游	76	7.60	37
傳產	213	5.76	38
政府	307	5.29	44
金融	84	4.20	46
電子上游	33	3.30	39

NetworkSecurity

	發現風險數量	平均每間公司風險數量	資安衛生 PR 值
電子中游	835	83.50	23
政府	2300	39.66	42
金融	670	33.50	41
電子上游	266	26.60	41
傳產	523	14.14	65
電子下游	133	13.30	66

DnsSecurity

	發現風險數量	平均每間公司風險數量	資安衛生 PR 值
電子中游	325	32.50	21
電子上游	219	21.90	33
政府	899	15.50	45
金融	269	13.45	45
電子下游	108	10.80	46
傳產	390	10.54	33

二、政府單位的電子郵件服務資安衛生指數僅有 25，易受社交工程攻擊

此次分析結果顯示政府單位在 EmailSecurity 類別的風險數量最高，推測可能是因為政府單位需要直接面對民眾、大量仰賴對外的郵件服務。政府各級單位雖然都有獨立的郵件伺服器域名，但卻沒有足夠的資安能量來確保郵件服務設定無誤，不僅導致整體風險數量偏高，也易受社交工程攻擊。

經過資安衛生 PR 值排序後，我們發現數值呈現兩極化的分布，由於加權分數分布相當集中，導致資安衛生 PR 值震盪較大。加權分數集中主要是因為有些與 email 相關的安全議題如：DMARC、SPF 設置錯誤等都是大家共同容易出錯的地方，導致公司之間的表現沒有明顯差距。只要做得稍微好一點的公司、資安衛生 PR 值就相對表現很好，因此還需輔以風險數量觀察。資安衛生 PR 值較低的產業中，政府機關因外曝資產過多，所以累計的風險總量也較多，其資產數量是電子上游的 6.5 倍，從問題總量上來看更為嚴重。

EmailSecurity

	發現風險數量	平均每間公司風險數量	資安衛生 PR 值
政府	3740	64.48	25
電子下游	624	62.40	93
金融	790	39.50	27
電子上游	382	38.20	23
電子中游	357	35.70	94
傳產	869	23.49	24

CertificateHealth

	發現風險數量	平均每間公司風險數量	資安衛生 PR 值
電子中游	21	2.10	36
政府	120	2.07	37
電子下游	18	1.80	19
金融	30	1.50	37
傳產	42	1.14	38
電子上游	2	0.20	39

三、金融單位在 IPDomainReputation 風險類別上資安衛生分數較低

此項目主要關注是否有 IP 或域名被納入黑名單，若曾有濫發廣告信、被當作 botnet 等行為皆會造成該單位的 IP 聲譽下降。我們發現金融單位在此類別的風險較高，可能是因為金融單位常是攻擊者社交工程的標的，間接造成資安聲譽低落。

IPDomainReputation

	發現風險數量	平均每間公司風險數量	資安衛生 PR 值
金融	46	2.30	43
政府	123	2.12	46
電子下游	19	1.90	45
電子上游	13	1.30	43
電子中游	12	1.20	45
傳產	36	0.97	44

Dark Web 暗網曝險分析：政府機構、電子下游、金融業深受地下產業青睞

除了前述的非侵入式檢測，奧義智慧科技研究團隊也進行暗網曝險分析，在不取得機敏資料為前提的狀況下進行本次研究，研究標的為 Infostealer 在暗網上販售的資料。

Infostealer 攻擊自 2021 年逐漸興起，攻擊者將 Infostealer 惡意程式（如：Redline、Raccoon、Vidar）植入受害者端點，並竊取端點資訊，包含：網站的帳號密碼、網站的 Cookie 及其他機敏資訊等。接著，攻擊者可利用取得的資料登入企業內部網站，或進一步散佈後續的惡意程式（如：勒索軟體等），這類攻擊手法被稱為 IAB（Initial Access Broker）。我們透過 IAB 的外洩資料（IAB Logs），可以分析被 Infostealer 感染的端點，外洩了哪些網站的資訊。

在這 145 家組織中，我們發現共有 92 家曾發生外洩事件且資料已在暗網上被販賣，外洩比例達 63.45%。普查範圍內共有 3,549 筆資料外洩，以政府機構（平均 87 筆）、電子業下游（平均 26.98 筆）、金融業（平均 21.95 筆）為前三高。

政府機構、電子業下游與金融業容易淪為暗網兜售資料的主要目標，因為政府機構涉及國家安全、公民個人資料、政策制定的內部溝通，具有高度機敏性；電子業下游富含高科技產品的知識產權和生產機密；金融機構儲存大量的個人和企業財務資料，包括銀行帳戶和交易資訊等，控制了銀行帳戶則可以直接提領帳戶內的現金，是犯罪集團的首要目標之一。

DarkWebLeak

	發現風險數量	平均每間公司風險數量	資安衛生 PR 值
傳產	561	15.16	64
電子上游	53	5.30	62
電子下游	870	87.00	62
電子中游	61	6.10	62
政府	1565	26.98	61
金融	439	21.95	60

資安曝險普查，四大趨勢與問題

一、雲端資產比例漸增，成為企業新的資安威脅

透過此次普查，奧義智慧科技研究團隊發現了四大趨勢與問題。首先，雲端資產比例大幅提高，成為企業新的資安挑戰。在外部掃描可以接觸到的數位資產中，各產業都有使用雲端資產：電子產業已經使用大量的雲端資產，比例約 40%~50%；政府單位佔 25.86%、傳產 21.62%、金融業較少但也有 5% 的公司正在使用雲端服務。過往金融機構嚴格禁止使用雲端服務、以地端服務為主，但近年來為加強資安韌性、資料異地備份及對外服務不中斷等監管需求，逐漸鬆綁上雲規範，使金融單位的雲端資安需求因而上升。

企業普遍使用的雲端資產目前仍以 AWS、Azure 及 Microsoft 365 為主，各產業依其使用情境有所不同。較多企業優先使用 Azure 及 Microsoft 365 是出於 IT 管理方便，選擇 AWS、GCP 則多是為了使用雲端廠商提供的服務，以及提供雲端服務給使用者。電子產業大多與內部 IT 環境串接，所以大部分傾向使用 Azure 與 Microsoft 365；金融單位雖然逐漸上雲，但仍以雲端廠商提供的服務為主，不會將雲端與內部 IT 環境相互介接，因此以 AWS 為主。

表（三）各產業雲端服務使用現狀普查

產業類別	產業中採用的公司比例	產業中平均每家的雲端用量
電子中游	50.00%	3.10
電子上游	40.00%	7.00
電子下游	40.00%	5.00
政府	25.86%	2.24
傳產	21.62%	1.68
金融	5.00%	0.25

表（四）各產業每家公司平均使用的雲端服務量

產業類別 \ 雲端	AWS	Akamai Connected Cloud	Azure	Cloudflare	GCP	Microsoft 365
政府	1.09	0.07	0.21	0.60	0.28	0.00
傳產	0.73	0.14	0.43	0.08	0.22	0.08
金融	0.25	0.00	0.00	0.00	0.00	0.00
電子上游	2.60	0.20	1.10	0.00	0.30	2.80
電子下游	1.00	0.20	1.70	0.00	1.00	1.10
電子中游	1.10	0.00	1.80	0.00	0.20	0.00

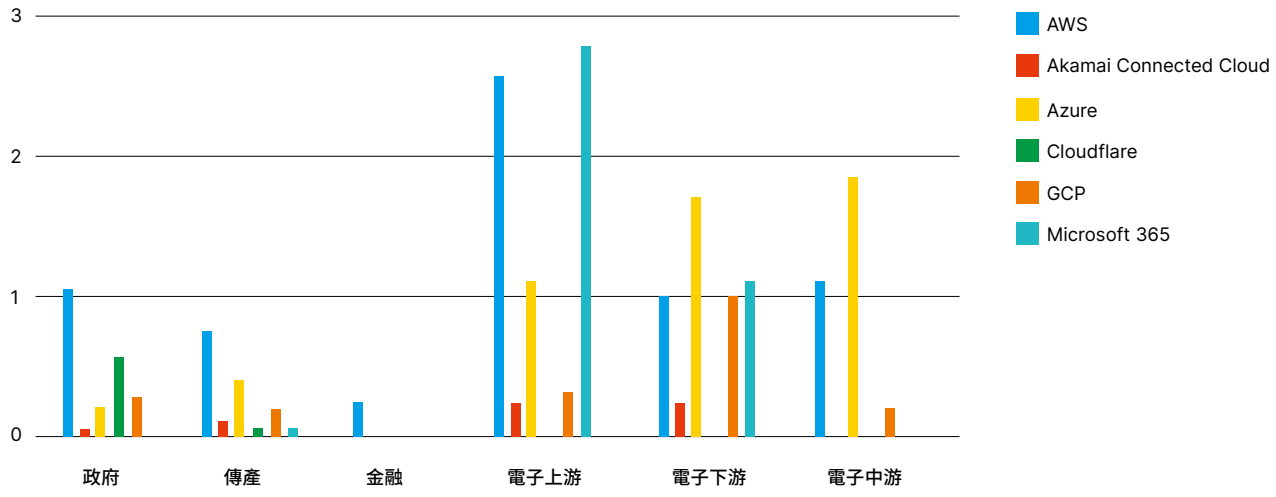


圖 2 各產業每家公司平均使用的雲端服務比例圖

表（五）各產業雲端與地端服務比例

產業類型	雲端服務數量	地端服務數量	雲地比	雲端占比
電子上游	76	185	41.08%	29.12%
電子下游	47	335	14.03%	12.30%
傳產	86	613	14.03%	12.30%
政府	185	1526	12.12%	10.81%
電子中游	37	320	11.56%	10.36%
金融	8	392	2.04%	2.00%

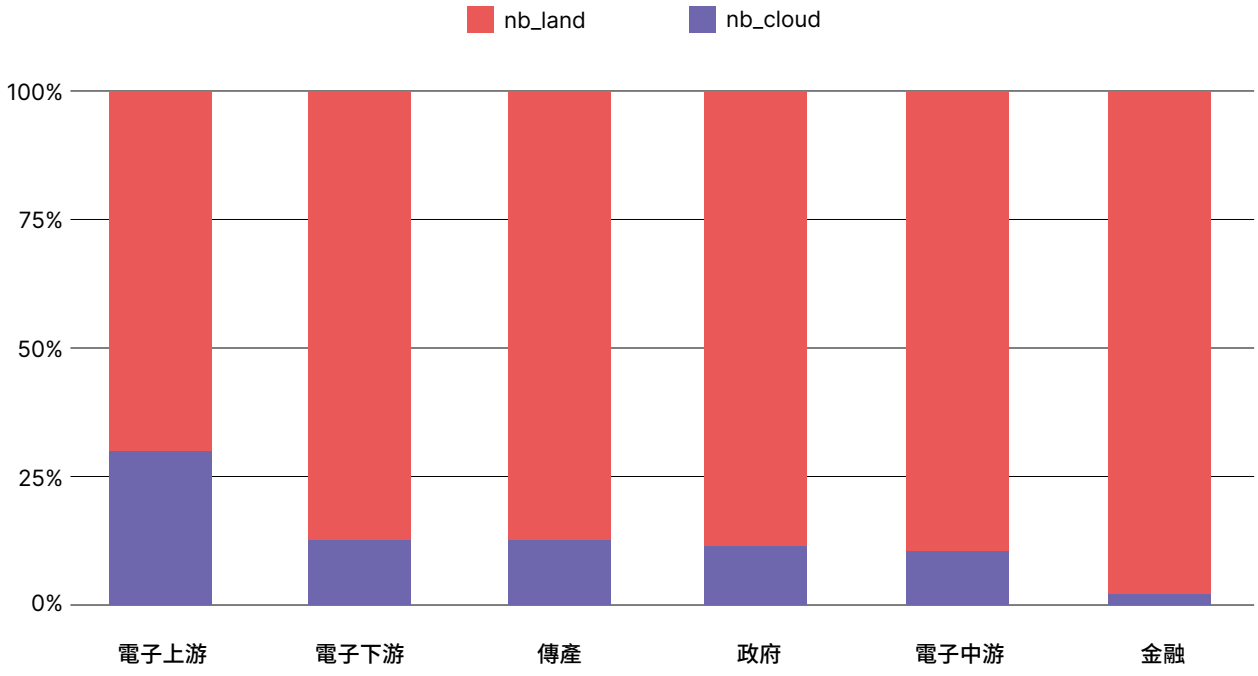


圖 3 各產業雲端及地端服務的占比

二、95% 的企業未正確設置 SPF、DKIM、DMARC，易受社交工程影響

一直以來，釣魚信件攻擊都是企業面臨的重大安全挑戰之一。儘管企業常透過釣魚信件教育訓練來提高員工安全意識，但這僅是治標而非治本的解決方法，因為攻擊者仍然能夠利用各種技巧輕易地發動社交工程攻擊，並取得機密資訊。

對此，企業可以透過實施 SPF (Sender Policy Framework)、DKIM (DomainKeys Identified Mail)、DMARC (Domain-based Message Authentication, Reporting, and Conformance) 等機制來提升釣魚信件攻擊的防護能力。這些機制可以有效防止攻擊者偽冒企業網域，減少釣魚信件的產生。企業不僅要加強自身安全防護措施，還需要確保供應商、合作廠商等相關單位也正確設置了這些安全機制。在整體產業生態圈裡建造良好的資安衛生習慣，才能有效降低社交工程的風險。

然而，普查結果顯示許多企業仍未意識到前述設定的重要性。在 145 個單位中，有 138 個組織未設置 SPF、137 個組織未設置 DMARC，以及各種其他錯誤的設定。我們認為這代表在台灣，幾乎沒有人設定此類安全機制，間接使釣魚信件攻擊愈演愈烈。因此，我們呼籲企業應該重視 SPF、DKIM、DMARC 等安全機制的設置，並加強監督與培訓產業生態鏈裡的各級單位，共構更加安全的電子郵件生態系統。

SPF 技術介紹

SPF（Sender Policy Framework）是一種用於防止垃圾郵件和偽造郵件的電子郵件驗證機制，主要目的是確保發送郵件的伺服器是被允許送出郵件的伺服器。SPF 的技術實作方式是在 DNS 中設置 SPF 記錄，記錄中列出了被允許發送郵件的伺服器 IP 地址或主機名。

當郵件伺服器收到一封郵件時，如果接收郵件伺服器支援 SPF，它將查詢寄件者的 SPF 設定，並檢查寄件者的 IP 地址是否被授權發送郵件。 如果 SPF 設定正確，郵件伺服器將會接受這封郵件。如果 SPF 設定不正確，郵件伺服器便會將這封郵件視為垃圾郵件或可能的詐騙郵件，阻擋或標記為垃圾郵件。因此，透過 SPF 技術，可以有效地減少垃圾郵件的數量，提高郵件的安全性和可信度。

未使用 SPF 可能帶來以下風險。首先，未使用 SPF 容易讓偽造郵件繞過防護機制，增加組織受到釣魚郵件攻擊的風險。這樣的情況不僅會干擾組織的正常運作，還可能導致機敏資訊外洩。其次，缺乏 SPF 設置可能導致接收方無法確認郵件的真實性，從而影響郵件的可靠性和信任度。最後，一些郵件服務提供商可能將未設置 SPF 的郵件視為潛在的垃圾郵件，進而導致部分郵件無法正常送達。這不僅會影響郵件的準時交付，還可能導致重要資訊的遺漏，對組織的業務運作帶來不利影響。因此，企業應當重視 SPF 的設置，並定期審查和更新其 SPF 設定，以保障郵件系統的安全性和可靠性。

DMARC 技術介紹

DMARC（Domain-based Message Authentication, Reporting, and Conformance） 是一種用來驗證電子郵件的標準，主要用於防止釣魚郵件和域名偽造。DMARC 結合了 SPF（Sender Policy Framework）和 DKIM（DomainKeys Identified Mail）的技術，讓寄件者可以更容易地驗證自己的郵件，同時讓收件者更容易識別郵件的真實性。 DMARC 的實作方式是在寄件者的 DNS 設定中添加 DMARC 記錄，規定如何處理未通過驗證的郵件。當收件者收到郵件時，郵件伺服器會對郵件進行驗證，如果驗證未通過，便會根據 DMARC 記錄中的指示進行相應的處理，例如標記郵件為垃圾郵件或直接拒收。未使用 DMARC 可能會導致企業或組織的電子郵件遭受釣魚攻擊，進而損失或洩露敏感資訊。此外，未使用 DMARC 也可能讓企業或組織的品牌形象受損，因為釣魚郵件可能會冒充該企業或組織的身份，惡意誤導收件者。 因此，使用 DMARC 可以提高郵件的安全性，防止釣魚攻擊和域名偽造，幫助企業或組織保護品牌形象和資訊安全。

三、SSL/TLS 版本過舊仍是常見問題

如今，網站連線的安全性已成為企業資安保護不可或缺的一部分， SSL/TLS 協議則成為保障網路通訊安全的重要工具。然而 TLS 1.2 之前的協議版本皆有已知安全問題，而其使用的加密演算法也難以滿足現今日益提升的資訊安全需求。為了應對這些安全威脅，大型瀏覽器業者於 2020 年陸續終止支援 TLS 1.0/1.1 ，IETF 也在 2021 年正式棄用了這些舊版協議。同時，美國國家安全局（NSA）亦在 2021 年呼籲所有使用者升級至更安全的 TLS 1.2 或 TLS 1.3 版本。

雖然 TLS 1.2 自 2008 年推出以來已有長達 16 年的歷史，並受到多種攻擊手法的挑戰，但相對於 TLS 1.1，它依然具有較高的安全性。2018 年，TLS 1.3 正式發佈、逐漸取代 TLS 1.2 成為網站連線的首選協議。TLS 1.3 不僅提供更強大的加密算法和安全特性，還通過簡化交握階段和減少輪次來提高傳輸效率。總的來說，當前使用 TLS 1.2 或 TLS 1.3 是維護網路通訊安全較為可靠的選擇。在本次普查中，仍檢測到 40 次使用 TLS 1.1 甚至更舊的版本，我們建議企業應該積極升級協議版本，以確保資料的機密性和完整性，並保護用戶的隱私安全。

SSL/TLS 技術介紹

SSL/TLS（Secure Sockets Layer/Transport Layer Security）是一種用於保護網路通訊安全的協議，主要目的是確保資料在網路上的安全傳輸，防止敏感資訊被未經授權的人員讀取、竊取或篡改。SSL/TLS 通過加密通訊內容、驗證通訊方身份和確保資料的完整性等手段來實現通訊的安全性。

SSL/TLS 協議涉及到多種技術，包括：

- **加解密演算法**：用於對資料進行加密，如對稱加密算法（如 AES）和非對稱加密算法（如 RSA）。
- **數位簽名演算法**：用於驗證資料的完整性和真實性，以及證明通訊方的身份。
- **交握協議**：用於建立安全連接，協商加密算法和密鑰，以及進行身份驗證。
- **數位憑證**：用於證明網站身份和公開密鑰的有效性。

使用舊版 TLS 1.2 或更舊的版本存在風險，主要包括：

- **安全漏洞**：舊版 TLS 存在已被發現的安全漏洞和弱點，如 BEAST、POODLE、Heartbleed 等，容易受到攻擊者的利用。
- **加密演算法較弱**：舊版 TLS 使用的加密算法可能較弱，容易被現代計算資源攻擊破解。
- **性能和功能限制**：舊版 TLS 可能缺乏一些性能最佳化設定和安全功能，如前向保密性、更安全的加密算法等，導致性能和安全性不佳。

因此，為了確保通訊的安全性，建議使用最新的 TLS 1.3 協議，並定期更新和升級相關的安全措施和加密算法。

四、12 個機構具高風險的 DNS IXFR 設置錯誤

IXFR 是 DNS 中一種用於傳輸 DNS 區域更改的機制，它允許 DNS 伺服器之間僅傳輸區域中已更改的部分，而不是整個區域資料。當 DNS 中的資料發生更改（例如新增、修改或刪除 DNS 記錄時），DNS 伺服器需要向其他伺服器同步這些變動，以保持資料的一致性。因為 IXFR 請求僅傳輸部分被修改的資料，可以更快速地同步資料。

若 DNS 伺服器回應全球 IXFR 請求，將導致區域資訊外洩。攻擊者可向目標 DNS 伺服器發送 IXFR 請求，請求傳輸目標區域的增量更新資料，取得該區域的敏感資訊，包括主機名、IP 地址和其他 DNS 記錄等。為了減輕 DNS 區域轉移攻擊的風險，必須在 DNS 伺服器上實施適當的存取控制和安全設定，例如：將區域轉移請求限制為授權的 IP 地址、實施防火牆規則來阻止未授權的請求、定期監控 DNS 伺服器日誌以檢測可疑活動等。在我們分析中，這是一項可能直接造成資安問題的高風險檢測項目，共有 12 個組織在 DNS 的設置上有問題，需要儘速修正。

近期受駭公司與本次普查對象比較結果

奧義智慧科技研究團隊不僅普查了國內企業、機構，也對近期遭勒索軟體的公司做曝險分析，兩次分析比較結果如下表（六）。

補充說明
本章節所提出受駭公司與正常公司的差異，並不直接代表受駭公司遭駭之根因。研究目標是區別受駭公司與一般公司的差異，但不代表其中的因果關係。

一、受駭公司在 CertificateHealth 風險類別普遍具有較高資安風險

我們發現在各風險類別中，受駭公司的資安衛生的確較正常公司來得差，特別在數位憑證相關的類別上有顯著的差異。

表（六）正常公司與受害公司之風險類別比例對照

風險類別	正常公司比例存在該風險比例	受駭公司存在該風險比例
CertificateHealth	0.3774834437	0.510460251
EmailSecurity	0.9602649007	0.9581589958
DnsSecurity	0.9205298013	0.9581589958
SslTlsStrength	0.4900662252	0.5523012552
NetworkSecurity	0.8476821192	0.8577405858
IPDomainReputation	0.4503311258	0.2552301255
DnsHealth	0.3973509934	0.5941422594

為了明確揭露哪些風險檢測項目可能導致受駭公司的曝險程度比普查對象來得高，我們更進一步建立了一個機器學習模型，並用該模型分析各風險項目的重要性，以分析哪些風險檢測項目是重要且具有辨別性的。我們發現在以下三個檢測項目中，呈現出明顯的差異：

- No DoT 與 No DoH
- DNSSEC 相關風險
- HTTP 相關風險

二、No DoT 與 No DoH

DNS over HTTPS (DoH) 和 DNS over TLS (DoT) 是兩種旨在增強 DNS 查詢的安全技術，它們將 DNS 查詢封裝在 HTTPS 或 TLS 加密通道中，保護查詢免受中間人攻擊和監聽。當這些安全措施未被實施時，網路流量和使用者行為可以被輕易地監控和攔截。

不使用 DoH 或 DoT 意味著 DNS 流量是明文傳輸的，讓攻擊者可以輕易地進行 DNS 劫持或中間人攻擊以修改 DNS 請求的回應，或導向惡意的網站。這不僅提高使用者面臨釣魚攻擊和惡意軟體的風險，還可能使得敏感資料（例如登入憑證、個人資訊等）遭到竊取。

雖然這不是攻擊者可以直接利用的漏洞，卻間接地反映出公司的資訊安全衛生狀況。根據統計，遭受勒索軟體攻擊的公司中，高達 81% 公司存在 DoT 和 DoH 的設定問題。相比之下，正常營運的公司中只有 27% 出現這類問題。

三、DNSSEC 相關風險

另一個具顯著差異的風險，是與 DNSSEC（網域名稱系統安全擴充程式）相關的項目。DNSSEC 旨在確保 DNS 查詢過程中，該記錄從權威名稱伺服器傳輸至使用者時不被竄改。若缺乏此類保護或相關設定錯誤，則會產生以下風險：

- 郵件流量攔截或篡改：若 MX 記錄遭到篡改，攻擊者可能將郵件流量重新導至未經授權的郵件伺服器。這不僅會威脅資料的隱私性，還可能導致敏感資訊的外洩。
- 繞過郵件認證系統：透過修改 TXT 紀錄，攻擊者能夠繞過郵件認證機制，發起釣魚攻擊或傳播惡意軟體，直接威脅組織的網路安全。
- 引導使用者訪問惡意網站：通過篡改 NS 記錄，攻擊者能引導使用者至被控制的 DNS 伺服器，進而導至惡意網站，增加遭受網路釣魚或下載惡意程式的風險。
- DNS 服務的不穩定或中斷：SOA 記錄的篡改可能造成 DNS 解析的延遲或中斷，嚴重時可能影響整個組織的 DNS 服務穩定性，對業務執行造成不利影響。

我們發現 DNSSEC 的涵蓋率時至目前還是偏低，我們推測這與採用 DNSSEC 會有效能疑慮及難以良好設定等原因相關，暗示了企業在資安風險與系統可用性上的風險評估與取捨。有能力及資源設置 DNSSEC 的公司，其對資安的重視程度可見一斑、整體資安的衛生習慣較好，與受駭單位有所差距的原因便在於此。

四、HTTP 相關風險

網頁伺服器的 HTTP 配置失誤一直是駭客入侵企業系統的常見途徑，因此關於其安全配置問題是評估企業網路安全的重要指標。在我們分析中，發現兩個具差異性的風險分別是， HTTP response header vulnerable to fingerprinting 和 Missing HTTP security headers。這兩者各自揭示了不同的資安風險：

- HTTP response header vulnerable to fingerprinting

  HTTP response header 的伺服器特徵（fingerprinting）揭露了伺服器的軟體類型、版本號等詳細資訊，使得伺服器易於被外部所識別。這種過多的資訊揭露增加了攻擊者針對特定伺服器進行攻擊的可能性，例如利用已知的漏洞發起攻擊。

- Missing HTTP security headers

  HTTP security header 如 Strict-Transport-Security、X-Frame-Options、X-Content-Type-Options、Content-Security-Policy 等，都是設計來增強網站安全的重要工具。這些安全性標頭能防止點擊劫持（Clickjacking）與跨網站指令碼攻擊（XSS）等常見的網路攻擊手段。

這兩個風險在 MITRE ATT&CK 模型中對應於「偵查」階段的 Gather Victim Host Information 和「初始入侵」階段的 Exploit Public-Facing Application 技術。這兩種攻擊手段是企業常常面臨的威脅，意味著 HTTP 標頭設定的問題不僅相互關聯，且對安全風險評估至關重要。單一設定的不當就可能觸及到多個攻擊面，由此可見嚴格管理 HTTP 標頭設定的重要性。

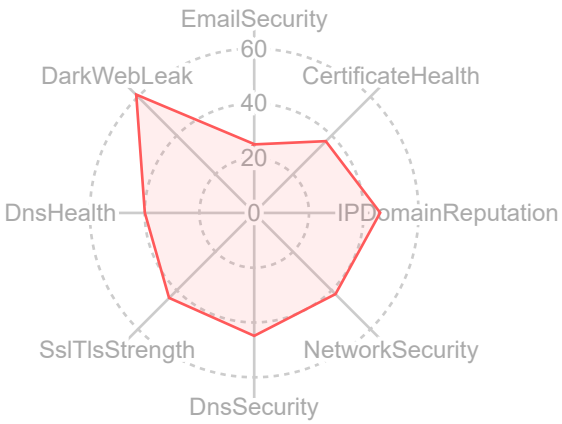
產業資安體質分析與建議

在普查與剖析各產業資安衛生指數、風險類別與外網曝險現況後，奧義智慧科技研究團隊針對不同產業提出相對應的資安管理策略：

政府組織

政府組織在本次普查中，各資安風險類別都落在稍低於平均左右的指數。在 EmailSecurity、DnsSecurity、 CertificateHealth 三個項目需要大幅加強；在其他項目上，也有不少可進步的空間。

風險類別	風險總數	資安衛生 PR 值
EmailSecurity	3740	25
CertificateHealth	120	37
IPDomainReputation	123	46
NetworkSecurity	2300	42
DnsSecurity	899	45
SslTlsStrength	307	44
DnsHealth	55	40
DarkWebLeak	1565	61



常見風險

- EmailSecurity: 缺少 SPF 和 DMARC 保護可能導致郵件欺詐和網路釣魚攻擊。
- DnsSecurity: 未受保護的 DNSSEC 可能遭到竄改，影響其真實性與完整性。
- CertificateHealth: 憑證資訊有誤，像是過期、網域名稱不相符以及信任等問題，可能導致中間人攻擊或服務中斷，影響信任和合法性。

技術解決方案

- EmailSecurity: 配置完整的郵件安全政策，包含 SPF、DKIM、DMARC 等，避免郵件詐騙。
- DnsSecurity: 正確設置 DNSSEC 可保護 DNS 紀錄的完整性。
- CertificateHealth: 週期性更新以及檢查憑證，使用自動化工具來管理憑證的有效性和配置。

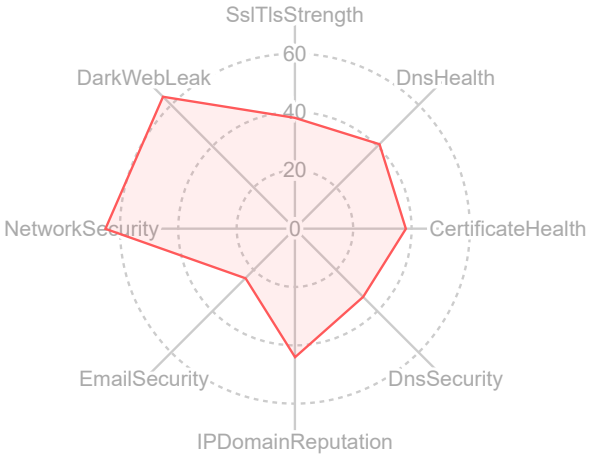
管理策略

- 制定或更新適用於 DNS、電子郵件安全、憑證的內部政策，明確訂立技術標準和作業程序。
- 定期進行網路安全培訓和演練，特別是針對識別釣魚攻擊和操作安全檢查。

傳產企業

傳產在 DnsSecurity 及 EmailSecurity 風險類別中，落在整體公司的 35% 以下，綜觀來看資安風險較高，需要改善計畫。

風險類別	風險總數	資安衛生 PR 值
SslTlsStrength	213	38
DnsHealth	37	41
CertificateHealth	42	38
DnsSecurity	390	33
IPDomainReputation	36	44
EmailSecurity	869	24
NetworkSecurity	523	65
DarkWebLeak	561	64



常見風險

- EmailSecurity: 缺少 SPF 和 DMARC 保護可能導致郵件詐騙和網路釣魚攻擊。
- DnsSecurity: 未受保護的 DNSSEC 可能遭到竄改，影響其真實性與完整性；未使用 DoT 或 DoH 影響 DNS 資料傳遞中的安全和隱私問題，導致竊聽的狀況發生。

技術解決方案

- EmailSecurity: 配置完整的郵件安全政策，包含 SPF、DKIM、DMARC 等，避免郵件詐騙。
- DnsSecurity: 正確設置 DNSSEC 可保護 DNS 紀錄的完整性。啟用 DoT 或 DoH 加密 DNS 查詢，增強隱私與安全。

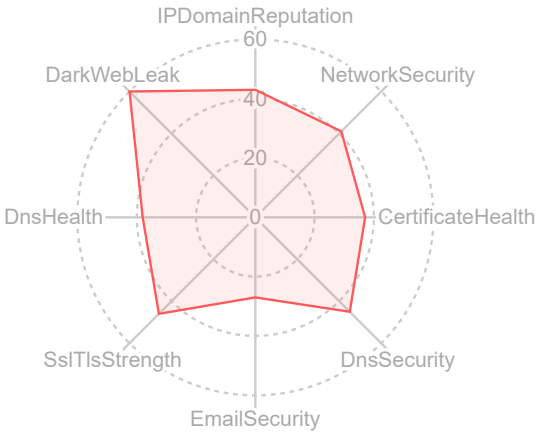
管理策略

- 建立定期審核機制，檢查安全設置的有效性，即時發現並解決安全漏洞。
- 制定或更新相關的網路及資訊安全政策，包括處理和回應安全事件的程序。

金融企業

金融企業在 EmailSecurity 風險類別落在整體公司的 35% 以下，風險較高，需要改善。

風險類別	風險總數	資安衛生 PR 值
IPDomainReputation	46	43
NetworkSecurity	670	41
CertificateHealth	30	37
DnsSecurity	269	45
EmailSecurity	790	27
SslTlsStrength	84	46
DnsHealth	13	38
DarkWebLeak	439	60



常見風險

- EmailSecurity: 缺少 SPF 和 DMARC 保護可能導致郵件詐騙和網路釣魚攻擊。

技術解決方案

- EmailSecurity: 配置完整的郵件安全政策，包含 SPF、DKIM、DMARC 等，避免郵件詐騙。

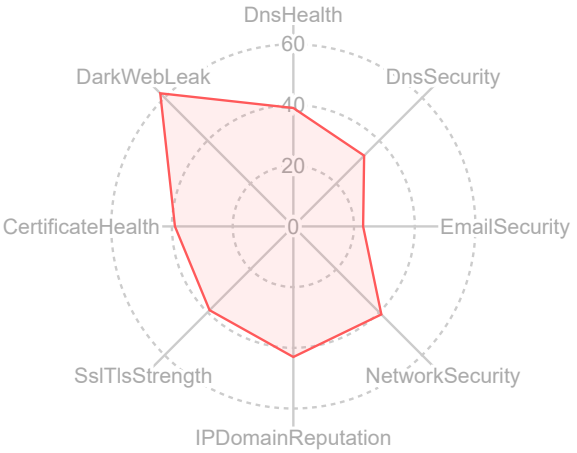
管理策略

- 制定一個全面的電子郵件安全政策，明確界定員工在使用郵件時需要遵守的安全措施。
- 定期對員工進行安全培訓和演練，強化其對於釣魚郵件和其他社交工程攻擊的識別能力。

電子上游企業

電子上游企業則在 DnsSecurity 及 EmailSecurity 兩項資安風險較高，需要改善。

風險類別	風險總數	資安衛生 PR 值
DnsHealth	29	39
DnsSecurity	219	33
EmailSecurity	382	23
NetworkSecurity	266	41
IPDomainReputation	13	43
SslTlsStrength	33	39
CertificateHealth	2	39
DarkWebLeak	53	62



常見風險

- EmailSecurity: 缺少 SPF 和 DMARC 保護可能導致郵件詐騙和網路釣魚攻擊。
- DnsSecurity: 未受保護的 DNSSEC 可能遭到竄改，影響其真實性與完整性；未使用 DoT 或 DoH 影響 DNS 資料傳遞中的安全和隱私問題，導致竊聽。

技術解決方案

- EmailSecurity: 配置完整的郵件安全政策，包含 SPF、DKIM、DMARC 等，避免郵件詐騙。
- DnsSecurity: 正確設置 DNSSEC 可保護 DNS 紀錄的完整性；啟用 DoT 或 DoH 加密 DNS 查詢，增強隱私與安全。

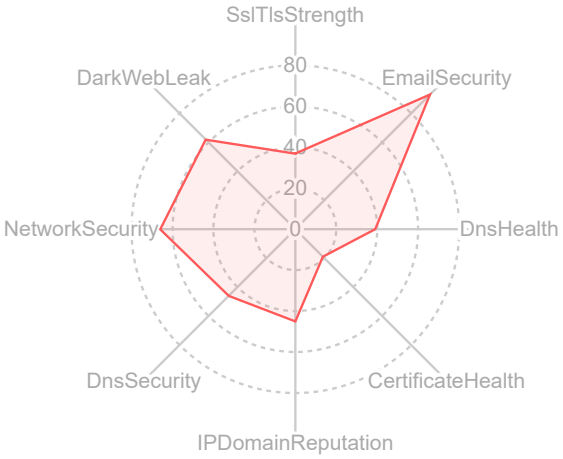
管理策略

- 定期對員工進行資安培訓和意識提升，特別是在識別釣魚攻擊和其他社交工程攻擊方面。
- 建立和更新資訊安全政策，確保所有的安全措施得到恰當的執行與監管。

電子下游企業

電子下游企業則在 CertificateHealth 項目資安風險較高，需要改善。

風險類別	風險總數	資安衛生 PR 值
SslTlsStrength	76	37
EmailSecurity	624	93
DnsHealth	16	39
CertificateHealth	18	19
IPDomainReputation	19	45
DnsSecurity	108	46
NetworkSecurity	133	66
DarkWebLeak	870	62



常見風險

- CertificateHealth: 憑證資訊有誤，像是過期、網域名稱不相符以及信任等問題，可能導致中間人攻擊或服務中斷，影響信任和合法性。

技術解決方案

- CertificateHealth: 週期性更新以及檢查憑證，部署工具以自動化憑證的續訂、安裝和配置，減少人為錯誤。設定警報通知，對即將過期或配置錯誤的憑證發出示警，確保及時處理。

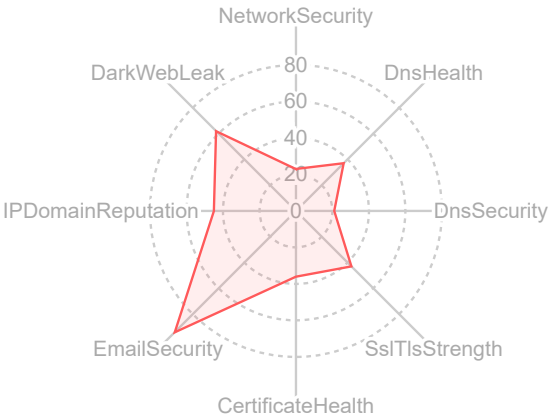
管理策略

- 培訓員工了解憑證健康的重要性，並教授基本的憑證檢查方法。
- 建立或修訂企業內憑證生命週期管理政策，包括取得、安裝、監控、續訂和撤銷的完整流程。

電子中游企業

電子中游企業則在 NetworkSecurity、DnsSecurity 兩項，資安風險較高，需要改善。

風險類別	風險總數	資安衛生 PR 值
NetworkSecurity	835	23
DnsHealth	31	37
DnsSecurity	325	21
SslTlsStrength	80	43
CertificateHealth	21	36
EmailSecurity	357	94
IPDomainReputation	12	45
DarkWebLeak	61	62



常見風險

- NetworkSecurity: 缺少或不當配置的 HTTP 安全性標頭將導致資料洩露、跨網站指令碼攻擊（XSS）及其他安全漏洞，攻擊者可利用這些漏洞存取未經授權的資料或進行服務拒絕攻擊（DoS）。
- DnsSecurity: 未受保護的 DNSSEC 可能遭到竄改，影響其真實性與完整性；未使用 DoT 或 DoH 影響 DNS 資料傳遞中的安全和隱私問題，導致竊聽。

技術解決方案

- NetworkSecurity: 配置正確且必須的 HTTP 安全性標頭，如「Strict-Transport-Security」、「Content-Security-Policy」等，以增強安全性。
- DnsSecurity: 正確設置 DNSSEC 可保護 DNS 紀錄的完整性；啟用 DoT 或 DoH 加密 DNS 查詢，增強隱私與安全。

管理策略

- 制定或更新公司的資訊安全政策，明確規定如何處理及更新 HTTP 安全性標頭設置和 DNS 配置。
- 建立定期安全審核機制，包括自動化的安全掃描和專家審查，以確保持續遵循行業最佳實踐和法規要求。

改善執行時間表

短期 (1-3 個月)

- 完成現有配置和政策的全面審核。
- 進行初步的技術評估和風險評估報告，並計畫各階段的執行詳情。
- 初步實施各項改善建議，測試可行性以及擴展性。

中期 (3-6 個月)

- 實施技術更新，完成改善建議。
- 更新公司安全策略，並進行員工安全培訓。
- IT 部門和第三方安全顧問合作，確保配置和部署的正確性。

長期 (6 個月以上)

- 持續監控、評估與調整安全措施，持續實施員工持育。
- 建立持續的安全文化和快速回應的安全事件處理機制。

結論

為什麼駭客能夠看穿攻擊目標、規劃攻擊，但企業卻難以掌握自身環境，提前設想應對措施？多數網路犯罪組織在攻擊前會進行網路偵察，鎖定疏於外部攻擊面管理的企業。
奧義智慧科技研究團隊在此白皮書中針對八大風險類別、共 233 項資安風險，盤點了 145 個單位（包含國內重要上市公司、重要政府單位及醫療機構）的外網與暗網曝險情資，發現最嚴重的三大問題為：

1. 95% 的企業未正確配置電子郵件安全設定，易受社交工程威脅： 釣魚信件攻擊一直以來都是企業的重大安全挑戰，儘管可以透過教育訓練提高員工安全意識，這仍是治標的解決方法。企業可以採取更為治本的措施，如啟用 SPF (Sender Policy Framework)、DKIM (DomainKeys Identified Mail)、DMARC (Domain-based Message Authentication, Reporting, and Conformance) 等機制有效防止攻擊者偽冒其網域，以減少釣魚信件。但本次普查結果顯示：145 個企業組織中，有 138 個組織未正確設置 SPF、137 個組織未正確設置 DMARC，意即在此普查範圍中大部分的企業都沒有正確設定電子郵件安全機制。

2. 63.5% 的企業曾被外洩，並於暗網上被販賣：
普查範圍內共有 3,549 筆資料外洩，以政府機構（平均 87 筆）、電子業下游（平均 26.98 筆）、金融業（平均 21.95 筆）為前三高。政府機構涉及國家安全、公民個人資料、政策制定與其他敏感資訊、電子業富含高科技產品的知識產權，金融業掌握大量個人和企業財務資料，容易淪為勒索軟體犯罪集團的首要目標。

3. 50.8% 遭勒索的企業對外網站憑證有瑕疵
我們將近期遭勒索的國外企業與台灣企業交叉比對後，一如預估，受駭公司的資安管理敏捷度的確與正常公司有別，以數位憑證相關的類別為例，超過半數遭勒索的企業對外網站憑證有明顯瑕疵，差異極為顯著。

若能掌握外部曝險、即可預視資安風險，奧義智慧科技 XCockpit 協助企業依照 CTEM (Continuous Threat Exposure Management) 框架判斷自身資安態勢，持續檢視與監控企業內部潛在威脅；亦可參考此白皮書針對六大產業（政府機關、傳產企業、電子上中下游等）的常見風險、技術解決方案與管理策略等建議，根據曝險概況採取對應的解決方法、訂定改善時間表，具體且全面地逐一攻破。

關於奧義智慧科技

奧義智慧科技 (CyCraft Technology) 是一間專注於 AI 技術的資安科技公司，研發出自動化威脅曝險管理平台「XCockpit」，由獨家 Cyber x AI 技術針對端點安全、特權帳號、外部攻擊面等三大核心面向，提供視覺化的態勢管理介面與時時的攻擊面監測。

創立於 2017 年，企業總部位於臺灣，於日本、新加坡皆設有子公司，為亞太地區的政府機關、警政國防、銀行和高科技製造產業提供專業資安服務，並受 Gartner、IDC 等世界級權威機構認可，選為 AI 資安報告之代表性案例企業，並曾多次斬獲海內外大獎肯定。

官方網站：www.cycraft.com


CYCRAFT
國家資通安全研究院
National Institute of Cyber Security