CLOUDFLARE

應對全新安全局勢：台灣地區網路安全準備情況調查

在過去 12 個月裡，台灣地區的威脅態勢仍然不穩定，26% 的受訪者表示他們遭受過資料外洩[1]。

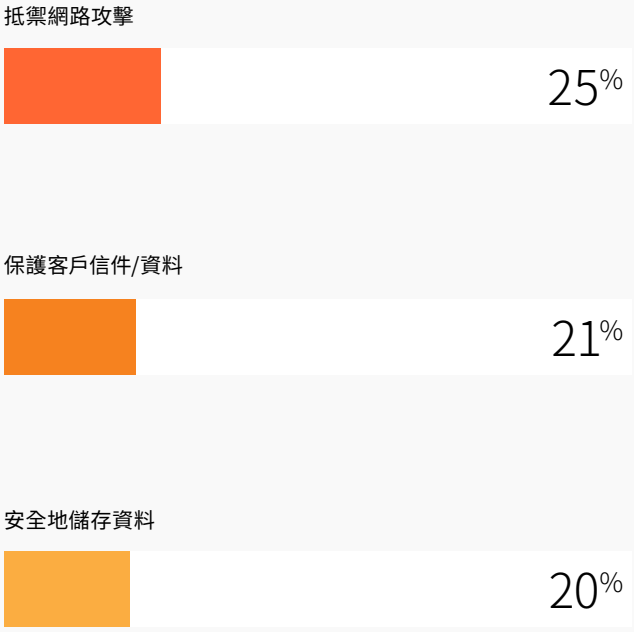
在遭受過資料外洩的受訪者中，70% 的人表示資料外洩發生頻率有所增加，37% 的受訪者聲稱遭受過 11 次或以上的資料外洩。小型組織遭受的資料外洩最多 (29%)，而零售 (46%)、建築和房地產 (43%) 以及商業和專業服務 (42%) 是最常見的目標產業。

網路安全仍然是一個關鍵的 IT 投資領域，82% 的受訪者表示，其組織超過 10% 的 IT 預算用於網路安全，而網路安全的主要優先任務包括抵禦網路攻擊 (25%)、保護客戶信件/資料 (21%)，以及在允許企業適當取用的同時安全儲存資料 (20%)。

與區域內其他國家/地區相比，台灣地區在哪些方面比較突出

	台灣地區	亞太地區
不太可能為防止資料外洩做好準備	75%	86%
不太可能將客戶壓力作為支付贖金的主要因素	17%	44%
更有可能擔心 AI 會使資料外洩的情況更加複雜和嚴重	90%	87%

網路安全的首要任務



多廠商帶來的挑戰不斷增長，整合似乎是一種常用的策略。這些挑戰包括：需要操縱過多的解決方案來補救網路攻擊 (50%)、在重複性工作/非關鍵網路安全功能上花費的時間太多 (46%)，以及在與其他解決方案/軟體整合方面遇到挑戰 (45%)。

Web 攻擊 (57%)、網路釣魚 (51%) 和惡意程式碼 (34%) 是導致資料外洩的前三大攻擊手段，而客戶資料 (75%)、使用者存取認證 (70%) 和個人識別資訊 (55%) 是最常受到攻擊的資產。調查結果還顯示，90% 的受訪者擔心 AI 會使資料外洩的情況更加複雜和嚴重。

儘管威脅具有挑戰性，但有跡象表明，復原能力正在增強。75% 的受訪者認為他們已做好防止資料外洩的準備，89% 的受訪者認為他們組織的網路安全狀態至少「比較成熟」。遊戲、金融服務、媒體和電信領域的組織在防止資料外洩方面最有可能「有所準備」。

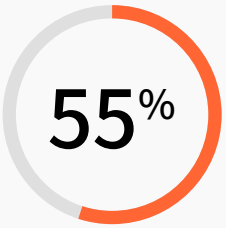
1.資料外洩是指攻擊者未經授權存取組織的應用程式、資料和網路的事件，而事件是指可能損害系統完整性的行為。

Zero Trust 的採用進展順利，40% 的受訪者表示其組織目前正在投資 Zero Trust 解決方案。另有 39% 的受訪者計劃在未來 12 個月內投資 Zero Trust。主要投資驅動因素包括降低易受攻擊的 IoT 裝置帶來的風險 (55%)、透過要求採用多個因素來減輕使用者認證盜竊和網路釣魚的影響 (54%)，以及在確實發生攻擊時將損害隔離在較小區域內 (54%)。

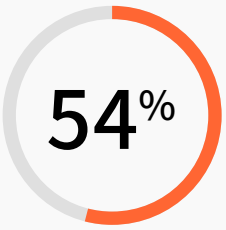
受訪者面臨的其他挑戰包括缺乏網路安全人才 (36%) 以及 AI 帶來的新威脅 (38%)。受訪者主要根據偵測網路攻擊 (49%) 並對此做出回應 (49%) 所需的時間來評估他們的網路安全解決方案。

勒索軟體仍然是一個日益嚴重的問題。24% 的受訪者擔心勒索軟體，其中，攻擊者所採用的最常見入侵方式是利用 Web 應用程式或伺服器中未修補的漏洞 (46%)。

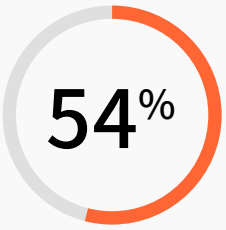
採用 Zero Trust 的主要投資驅動因素



降低易受攻擊的 IoT 裝置帶來的風險



透過要求使用多個驗證因素，減少使用者認證盜竊和網路釣魚的影響



在攻擊發生時將損害隔離在較小區域內

用於監管及合規性的資源

36% 的受訪者組織將超過 5% 的 IT 預算用於滿足監管及合規性要求

41% 的台灣地區受訪者表示，他們每週要花費超過 10% 的工作時間來滿足產業監管和認證要求

在過去兩年內遭受勒索軟體攻擊的組織中，46% 的受訪者表示他們的組織支付了贖金，儘管其中 54% 的組織已公開承諾不支付贖金。客戶壓力 (17%) 是支付贖金的主要因素。然而，受訪者認為，在透過部署員工訓練 (54%)、雙重驗證 (46%) 和反惡意程式碼軟體 (46%) 來緩解勒索軟體威脅方面，他們的組織至少「比較成熟」。

監管與合規性也成為今年研究的重要主題。36% 的受訪者組織將超過 5% 的 IT 預算用於滿足監管及合規性要求。41% 的受訪者表示，他們每週要花費超過 10% 的工作時間來滿足行業監管和認證要求。然而，這種在監管和合規性方面的投資對組織產生了積極影響，例如提高了組織的聲譽和品牌形象 (51%)、提高了組織的基準隱私權和/或安全性層級 (48%)，以及提高了組織的技術和資料完整性 (46%)。

建議

鑒於以上研究結果，就 CISO 在未來一年工作中提出了以下六項建議：

簡化解決方案以降低複雜性

在去年的報告中，我們建議透過 SASE 簡化安全架構。今年，這項建議不僅仍然有效，而且證據確鑿：更多的解決方案和 IT 廠商根本無法降低風險。組織應考慮採取更謹慎的方法，以最大限度減少已部署的解決方案數量，並整合從其獲取解決方案的 IT 廠商的數量。

加強供應鏈中最薄弱的環節

在當今全球互連的環境中，每個組織都依賴於軟體供應鏈。基於開放原始程式碼構建的應用程式、API 以及第三方整合都會促使攻擊面不斷擴大。正是因為這種攻擊面的擴大，所以引入新的合作夥伴意味著選擇信任其整個開發生態系統，而不僅僅是工具本身。Zero Trust 模型不僅不信任任何人，還會假設攻擊者已在網路內，並根據身分和環境評估使用者、裝置和工作負載，因此從基於邊界的安全模型過渡到該模型可以降低與供應鏈入侵相關的風險。尋找致力於安全納入設計原則的合作夥伴。

限制勒索軟體攻擊者的影響力並制定需求方案

勒索軟體攻擊不斷增多，因此，CISO 及其董事會必須制定一個應對計畫。從這項研究的證據來看，該計畫不應包括支付贖金，因為幾乎在所有情況下，這樣做的組織都會對自己的行為感到後悔。我們建議，在發生入侵時應採取策略，以最大限度地減少橫向移動，並利用 Zero Trust 功能。此外，強大的復原計畫將減少攻擊者的勒索要求所帶來的影響力。保障從定期資料備份開始，這一操作經過測試，可確保最關鍵的系統和資料的效率和完整性。定期災害復原測試是識別漏洞並增強實力以恢復營運和降低影響的關鍵。

準備好應對 AI 使攻擊倍增和加劇的情況

AI 已成為攻擊者的利器，因此 CISO 需要部署 AI 防禦策略。網路安全領導者應警惕簡單地將問題外包，檢查人才模型、治理框架、合規性要求和監控使用情況是絕對有必要的。現在，所有組織都可以採取的一個重要舉措是，審查與第三方廠商的合作條款，確保瞭解他們在其 AI 模型中使用您的資料的情況，且這種使用符合您的要求。目前的安全工具如何對抗 AI 攻擊的增加？很多 Cloudflare 產品利用我們龐大的全球威脅情報網路來主動對抗新威脅。

將投資從資本支出轉移至營運支出

大多數組織都面臨著預算壓力，因此，網路安全領導者需要成為優秀的財政管家。考慮提升現有團隊成員的技能以符合未來狀態，降低複雜性和簡化流程。探索重組角色的機會以最大限度提高效率，同時縮短延遲時間。可以考慮將一些功能外包給 MSP，從而將投資從資本支出轉移至營運支出。

坦然應對更多的審查

網路安全領導者面臨愈發嚴格的內部和外部審查，這使得他們本就巨大的壓力倍增。這種審查將繼續進行，因此 CISO 必須勤於尋找機會，以遵守不斷變化的法規（本地或國際），並能夠滿足董事會成員的需求。確保透過協商達成稽核承諾以明確範圍和時間表，從而減少既不會增加客戶價值也不會降低風險的工作。

遷移到全球連通雲

Cloudflare 提供一種名為全球連通雲的新服務類別，以連接和保護公司的人員、應用程式和網路，因此在提供全方位安全方面發揮著至關重要的作用。透過 Cloudflare 廣泛的安全產品組合（例如應用程式、API 和網路安全、Zero Trust 和全球威脅情報），組織可以加強其數位基礎架構以抵禦網路攻擊。組織可以確保其線上資料和智慧財產權的安全，並保護其品牌的完整性。

這些安全服務構建於 Cloudflare 統一且可程式設計的全球雲端網路服務平台上，該平台用於連接並保護全球大部分網際網路流量，平均每天阻止 1820 億次威脅。這種全球雲端網路會針對網路中斷和基礎架構故障提供備援和復原能力，最大限度地降低停機風險，確保高可用性。

若要深入了解 Cloudflare 的解決方案套件，並向銷售代表申請示範或 POC，請造訪：**cloudflare.com**。我們將幫助評估您現有的安全狀態，並合作制定行動方案，以增強人員、應用程式、裝置、網路和資料的網路安全。

掃描這裡以閱讀完整報告

* **《應對全新安全局勢：亞太地區網路安全準備情況調查》**介紹了亞太地區、日本和中國安全市場的調查結果。該項研究涉及 14 個市場的 3,844 名網路安全決策者與領導者。