CLOUDFLARE

應對全新安全局勢：香港地區網絡安全就緒情況調查

在過去 12 個月裡，香港地區的威脅態勢仍然不穩定，31% 的受訪者表示他們遭受過數據外洩[1]。

在遭受過數據外洩的受訪者中，74% 的人表示數據外洩發生頻率有所增加，62% 的受訪者聲稱遭受過 11 次或以上的數據外洩。小型組織遭受的數據外洩最多 (75%)，而政府 (86%)、建築和房地產 (74%) 以及旅行、旅遊與旅遊服務 (67%) 是最常見的目標行業。

網絡安全仍然是 IT 支出的一個關鍵領域，90% 的受訪者表示，其組織將超過 10% 的 IT 預算用於網絡安全，而網絡安全的首要任務是保護組織的網絡和數據 (23%)、實現企業所用的應用程式現代化 (19%)，以及實現企業營運的網絡現代化 (18%)。

與區域內其他國家／地區相比，香港地區在哪些方面比較突出

	香港特別行政區	亞太地區
在過去的 12 個月裡，更有可能遭受過 11 次或以上的數據外洩	62%	47%
更有可能在遭受勒索軟件攻擊時支付贖金	67%	59%
不太可能花費 5% 或更多的 IT 預算來滿足監管及合規性要求	25%	43%

網絡安全的首要任務

保護組織的網絡和數據 23%

實現應用程式現代化 19%

實現網絡現代化 18%

由於眾多供應商帶來的挑戰，整合似乎是一種常用的策略；包括功能重疊導致某些解決方案備援 (43%)、網絡攻擊需要更長的時間才能修補 (42%) 以及人力資源壓力 (36%)。

惡意程式碼 (46%)、內部人員威脅/被盜認證 (39%)、網絡釣魚 (37%) 和 Web 攻擊 (37%) 是導致數據外洩的主要攻擊手段，而客戶數據 (77%)、用户存取認證 (75%) 和財務數據 (69%) 是最常見的目標資產。調查結果還顯示，76% 的受訪者擔心 AI 會使數據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。89% 的受訪者認為他們已做好防止數據外洩的準備，86% 的受訪者認為他們組織的網絡安全狀態至少「有些成熟了」。在防止數據外洩方面，運輸、旅行、旅遊與旅遊服務以及醫療保健領域的組織最有可能做好「充分準備」。

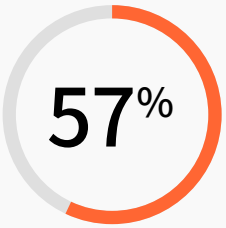
1.數據外洩是指攻擊者未經授權存取組織的應用程式、數據和網絡的事件，而事件是指可能損害系統完整性的行為。

採用 Zero Trust 進展順利，54% 的受訪者表示他們的組織目前正在投資 Zero Trust 解決方案。另外 28% 的受訪者計劃在未來 12 個月內投資 Zero Trust。主要的投資驅動因素包括：透過多重要素驗證減少用户認證盜竊和網絡釣魚的影響 (57%)、降低易受攻擊的 IoT 裝置帶來的風險 (57%)，以及持續監控和驗證所連接的用户和裝置 (54%)。

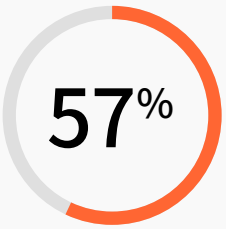
受訪者面臨的其他挑戰包括缺乏網絡安全人才 (33%) 以及 AI 帶來的新威脅 (33%)。受訪者主要根據偵測網絡攻擊 (43%) 並對此做出回應 (41%) 所需的時間來評估他們的網絡安全解決方案。

勒索軟件越來越受到關注，這一點並未改變。19% 的受訪者擔心勒索軟件，其中最常見的入侵方式是入侵遠端桌面通訊協定 (RDP) 或虛擬專用網絡 (VPN) 伺服器 (50%)，以及攻擊者利用 Web 應用程式或伺服器中未修補的漏洞 (50%)。

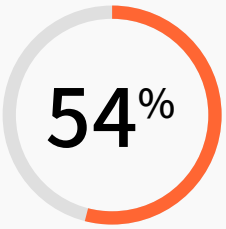
採用 Zero Trust 的主要投資驅動因素



透過多重要素驗證減少用户認證盜竊和網絡釣魚的影響



降低易受攻擊的 IoT 裝置帶來的風險



持續監控和驗證所連接的用户和裝置

用於監管及合規性的資源

25% 的受訪者的組織將超過 5% 的 IT 預算用於滿足監管及合規性要求

48% 的香港地區受訪者表示，他們每週要花費超過 10% 的工作時間來滿足行業監管和認證要求

在過去兩年內遭受勒索軟件攻擊的組織中，67% 的受訪者表示他們的組織支付了贖金，儘管其中 66% 的組織已公開承諾不支付贖金。客戶壓力 (60%) 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 (84%)、雙重驗證 (84%) 和反惡意程式碼軟件 (84%) 來緩解勒索軟件威脅方面，他們的組織至少「有些成熟了」。

監管及合規性也成為了今年研究的重要主題。25% 的受訪者的組織將超過 5% 的 IT 預算用於滿足監管及合規性要求。48% 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，在監管和合規性方面的投資對組織產生了積極影響，比如提高組織的基準隱私權和/或安全水平 (53%)、提高組織的聲譽和品牌 (49%)，以及增加私營部門的銷售機會 (49%)。

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件供應鏈。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絡內，並根據身分和環境評估用户、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。

限制勒索軟件攻擊者的影響力並制定需求方案

勒索軟件攻擊不斷增多，因此，CISO 及其董事會必須制定一個應對計劃。從這項研究的證據來看，該計劃不應包括支付贖金，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，一項強大的復原計劃將減少攻擊者需求的影響力。保證從定期數據備份開始，經過測試可確保最關鍵的系統和數據的效率和完整性。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 將被攻擊者利用，因此 CISO 需要部署 AI 防禦策略。網絡安全領導者應提防簡單地將問題外包，但絕對有必要檢查人才模型、治理框架、合規性要求和監控使用情況。現在，所有組織均可採取的重要措施就是查看與第三方廠商合作的條款，以確保他們在其 AI 模型中使用您的數據得到了理解，並符合您的要求。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絡來主動對抗新威脅。

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，網絡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

網絡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、應用程式和網絡，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 和網絡安全、Zero Trust 和全球威脅情報），組織可以加強其數位基礎結構以抵禦網絡攻擊。組織可以確保其線上數據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 可編程全球雲端網絡服務的統一平台上，該平台用於連接並保護全球大部分網絡流量，平均每天阻止 1820 億次威脅。這種全球雲端網絡會針對網絡中斷和基礎結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、網絡和數據的網絡安全。

掃描這裡以閱讀完整報告

*《應對全新安全局勢：亞太地區網絡安全就緒情況調查》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 名網絡安全決策者與領導者。