thalescpl.com

THALES

2019 年亞太地區資安報告

（上半年回顧）

內容

簡介

亞太地區的企業組織紛紛力求快速創新，透過不斷發展其商業模式來保持競爭力。這股演進風潮的核心，便是敏感資料的爆炸性增長、收集及分享。在此同時，網路犯罪分子虎視眈眈覬覦這個資料金礦，企圖大賺不法之財！亞太地區的企業組織該如何安全地因應這些變化？

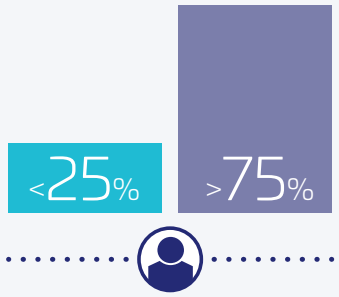
為了找出答案，Thales 與 Ecosystm 聯合 針對亞太地區的資安局勢進行市場調查。

[1] https://www.ecosystm360.com/#/tech-vendor/research-detail/bcedcea0-56d0-4acd-8aae-654e123dd73b

研究報告：2019 年亞太地區資安報告（上半年回顧）

重要調查結果

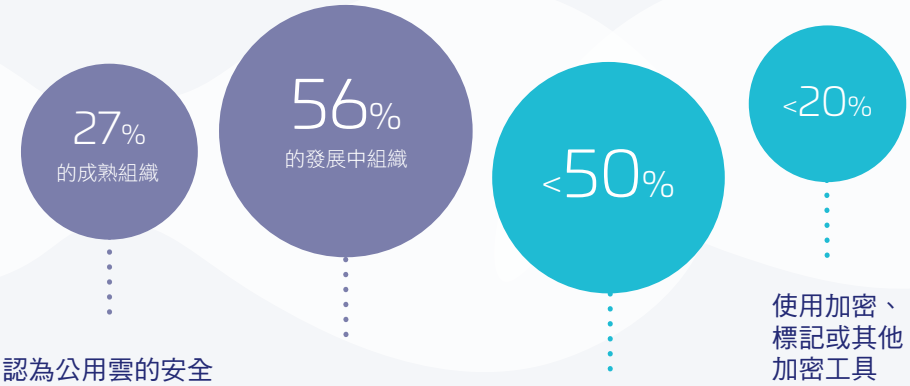
亞太地區企業仍在摸索如何保護其業務



>75%

不知道從何開始或應在哪個領域投入資源，以保護其企業免受網路攻擊

公用雲安全性



認為公用雲的安全措施已足夠

認為公用雲的安全措施已足夠

的組織使用多因素驗證

使用加密、標記或其他加密工具

處理資料外洩的就緒程度

95%

表示不曾發生資料外洩或不確定是否發生過

73%

聲稱不曾發生資料外洩的人，表示外洩是不可避免的

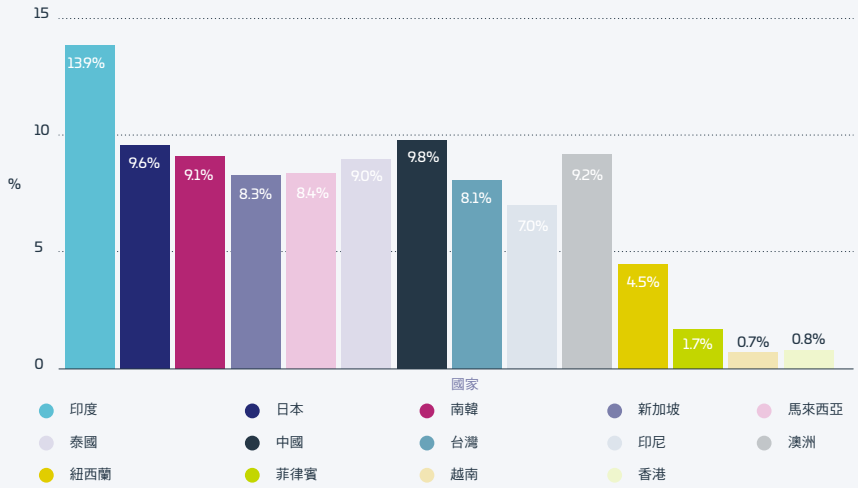
70-80%

的組織了解在發生外洩事件時，他們必須通知監管機構，但很少會考慮通知他們的客戶

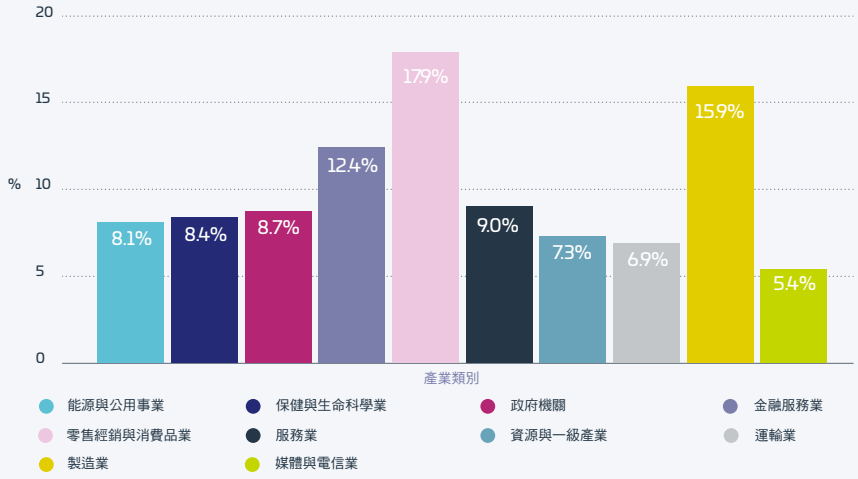
人口統計

在本研究中，我們收集了來自亞太地區 14 個國家（包括澳洲和紐西蘭）各行各業，超過 1,700 名資深經理的意見。

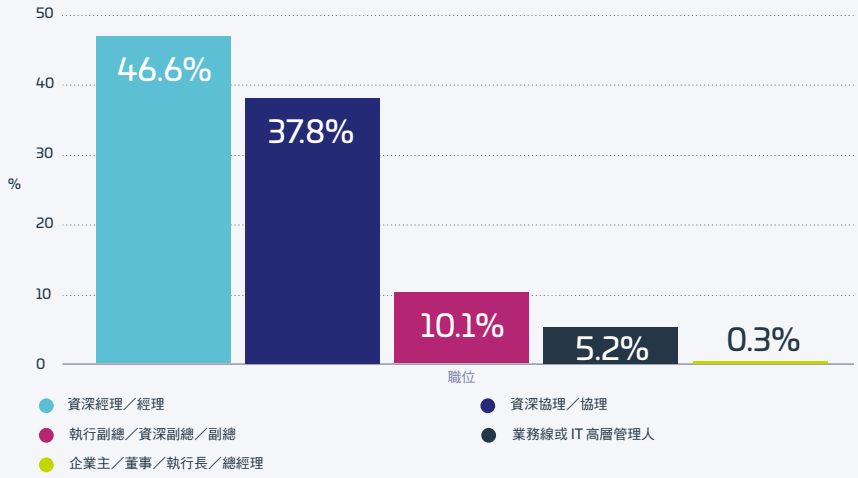
調查涵蓋國家 - 網路安全



調查涵蓋產業 - 網路安全



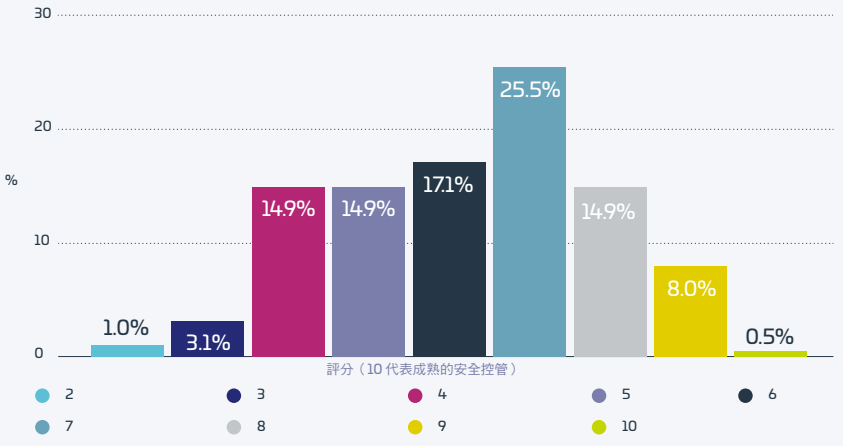
調查涵蓋職位 - 網路安全



網路安全防護趨勢

參與調查的受訪者當中，僅有不到 30% 認為他們的組織具備成熟的網路安全計劃。最令人憂心的是，其餘的組織（超過 70%）只有少量或正在開發中的網路安全計劃，或是完全沒有任何網路安全計劃。

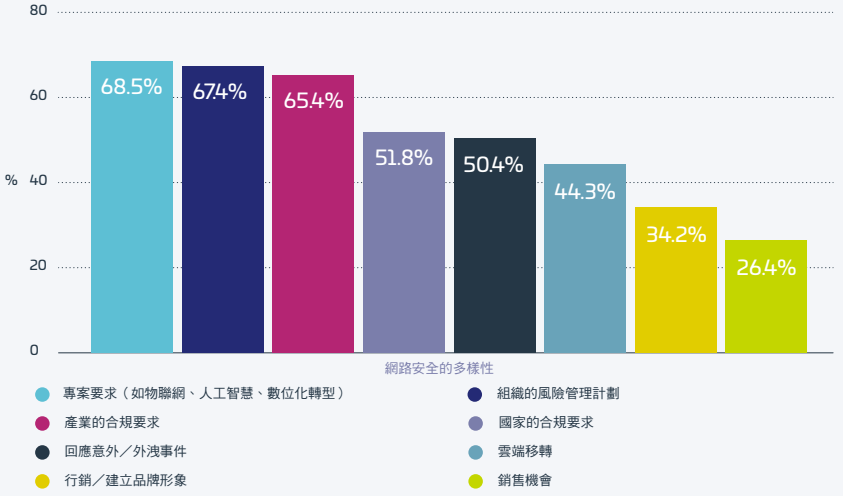
組織的網路安全部署成熟度



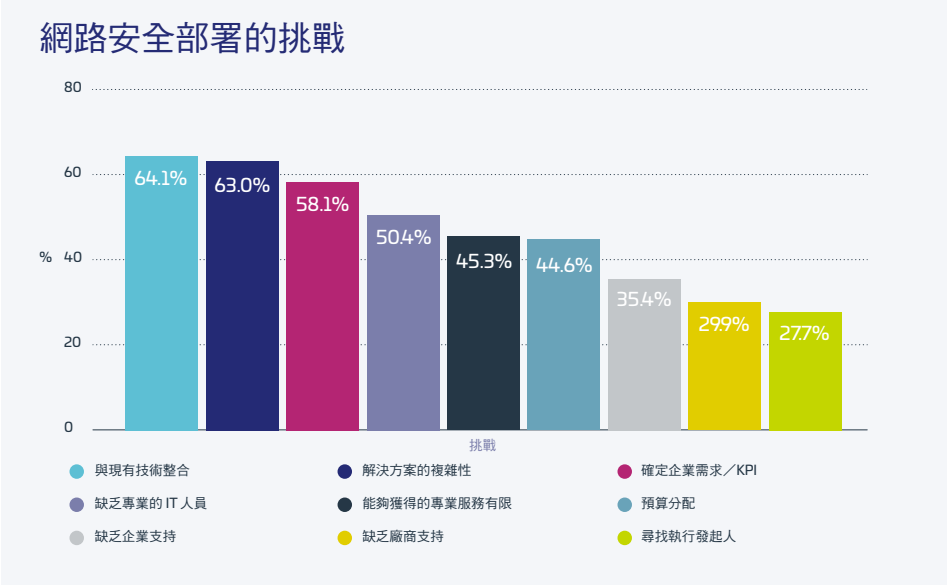
8 分（含）以上的安全解決方案，代表組織的網路安全性已成熟 - 他們的政策以及實行方案通常與發展中組織有所不同。

投資網路安全的兩大驅動因素分別為**數位轉型**以及**新興技術**。制定一個優於基本規定的強大風險管理計劃，對每個組織來說至關重要。然而，有半數的受訪者表示，他們的組織只有在發生意外或出現漏洞後才會關注網路安全！

持續關注網路安全的驅動因素



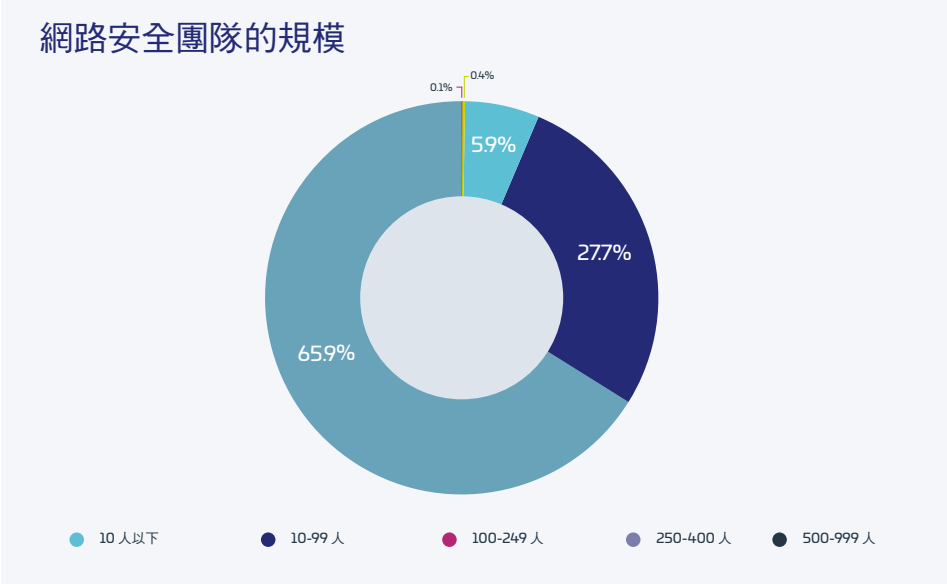
各大組織在部署網路安全解決方案時共同面臨的最大挑戰在於：在缺乏專業 IT 人員的情況下，將複雜的安全解決方案與現有的技術進行整合。



本調查顯示，組織無法承受因**資料外洩**而帶來的財務及商譽損失的**高風險**，**IT 已不再主導網路安全的策略及預算**，轉而負責**實務操作的角色**。

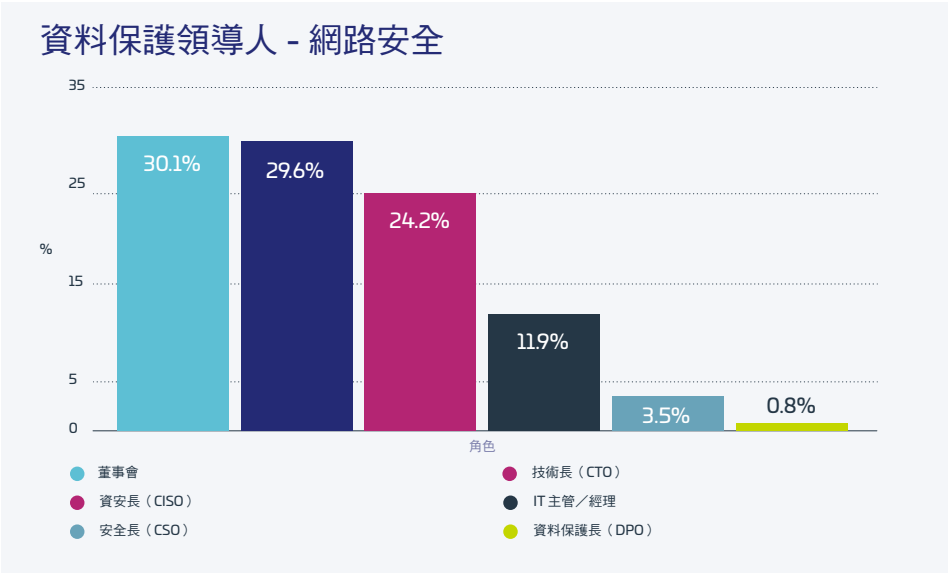
網路安全團隊和政策

對亞太地區的組織來說，網路安全團隊的規模主要取決於組織本身的規模、業務資料多寡，以及組織對於託管服務供應商（MSP）的依賴程度。



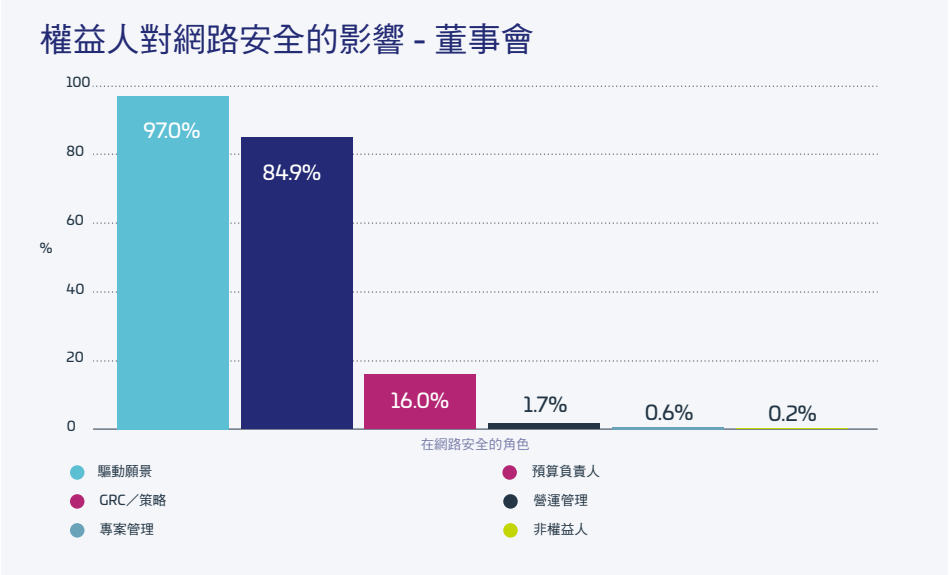
一個組織若要成功轉型並保持競爭力，必須有一個領導人專門負責組織的網路安全和資料保護需求。亞太地區多數的成熟組織傾於聘請專職的資安長，負責協調策略與技術並落實組織願景。

但是網路安全攸關整個組織，因此亞太地區的執行高層現在也直接參與網路安全方面的治理、風險管理與合規（GRC）、策略和預算。



當今行銷部門以前所未有的方式**運用技術並產生越來越多資料**。他們在組織的**網路安全策略**中所扮演的角色將不斷演進。

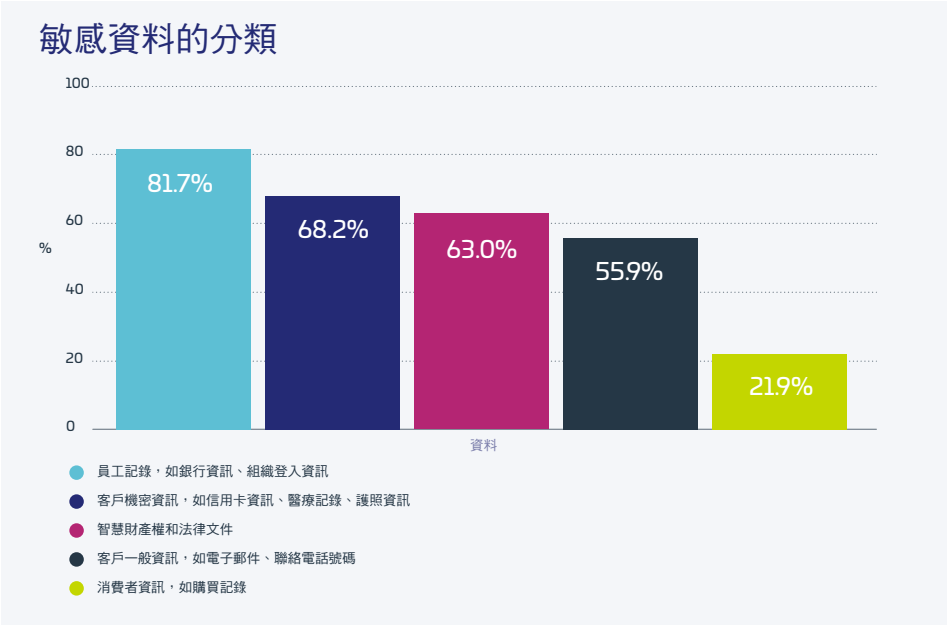
亞太地區的組織開始出現專門的網路安全團隊，負責確保策略和 GRC 與安全解決方案的實際落實情形並行一致。



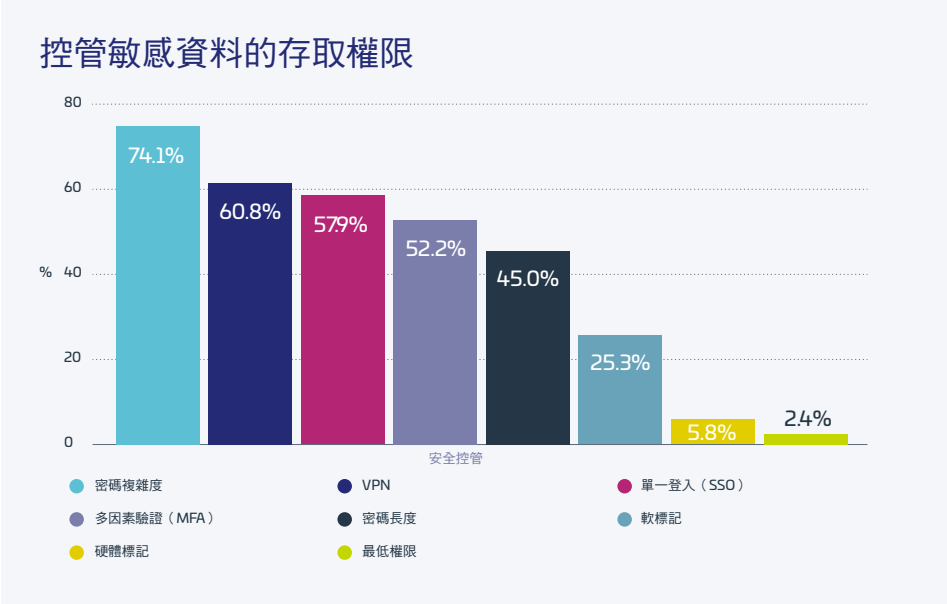
可想而知，財務部門成了管理預算的負責單位。隨著組織對科技的依賴性越來越高，組織營運必須與專門的安全團隊密切合作。同時，研發團隊應在專門的資安團隊和資安長的指導下工作。

保護敏感資料的程序

在落實網路安全藍圖和解決方案之前，保護敏感資料之路始於資料分類。然而，許多亞太地區組織無法識別智慧財產權與法律以外的敏感資料。

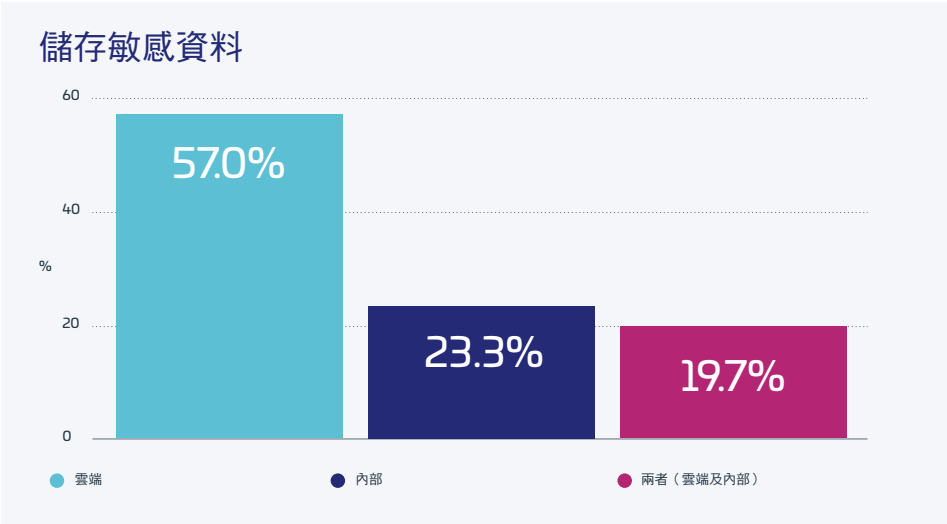


現今的組織採用多種方式來控管敏感資料的存取權限，其中以設定密碼的方式居多，受訪的亞太地區組織中僅有一半採用「多因素驗證」（MFA）。



雲端的安全性

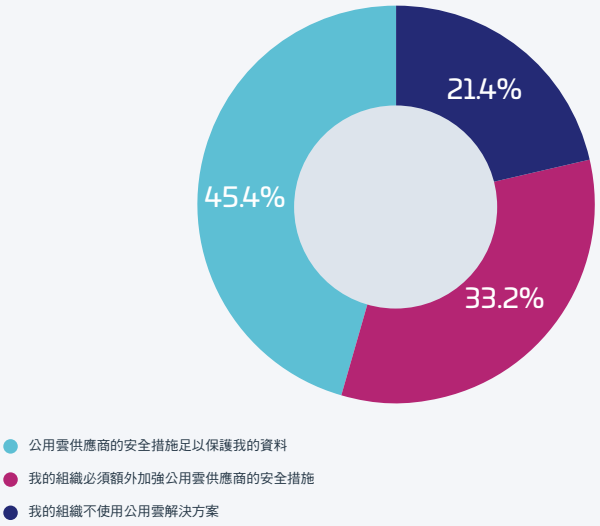
在亞太地區，將近 60% 的受訪組織將其敏感資料儲存於公用雲。不意外地，其中大部分是初創組織善用公用雲的低成本優勢來增加彈性效益。而成熟組織對於公用雲的使用，則是採取較謹慎保守的方式以規避風險。



有將近半數（45.5%）的受訪組織認為公用雲的安全措施足以保護他們的資料。尤其是那些 IT 資源有限的初創組織，不得不仰賴公用雲供應商的安全措施。三分之一（33.2%）的受訪組織表示，他們必須額外加強公用雲供應商的安全措施。

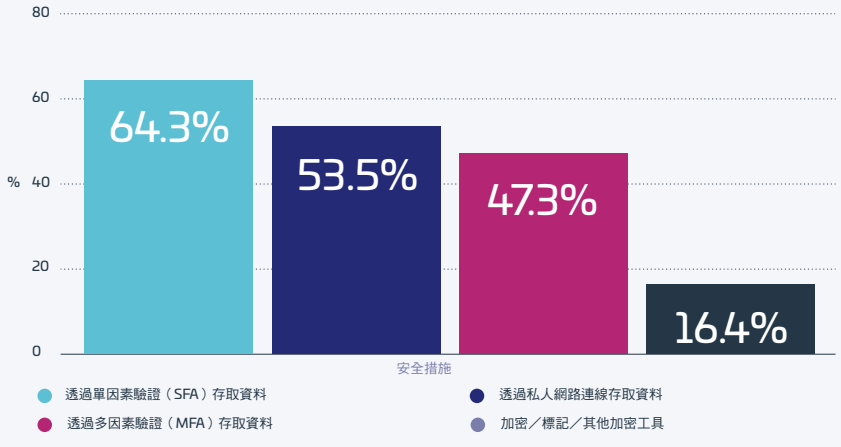
僅**一半**的受訪組織使用**安全性較高的「多因素驗證」**，而只有**極少數**的受訪組織會加密或標記儲存在**雲端**的敏感資料。

公用雲安全的認知



令人訝異的是，儘管全球身分遭竊的案例頻傳，亞太地區仍普遍使用「單因素驗證」（如密碼）的方式來存取雲端。

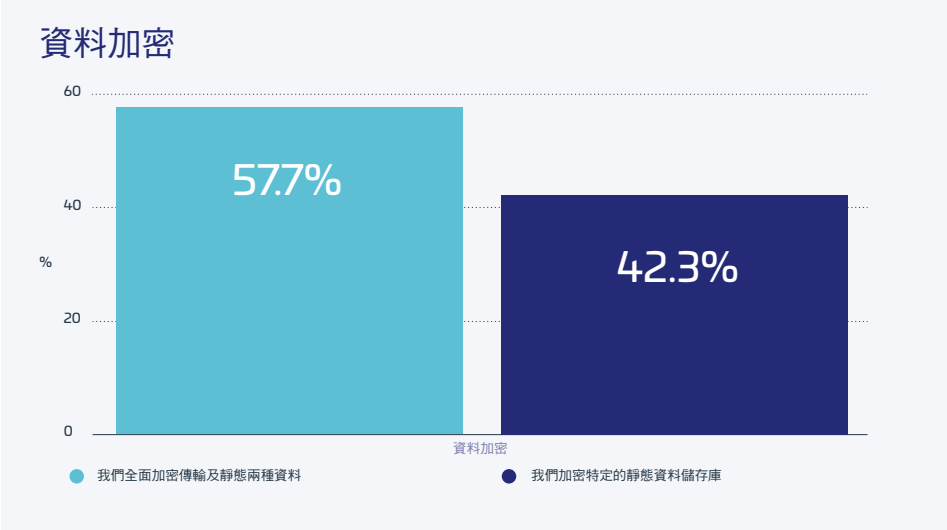
保護雲端敏感資料的方法



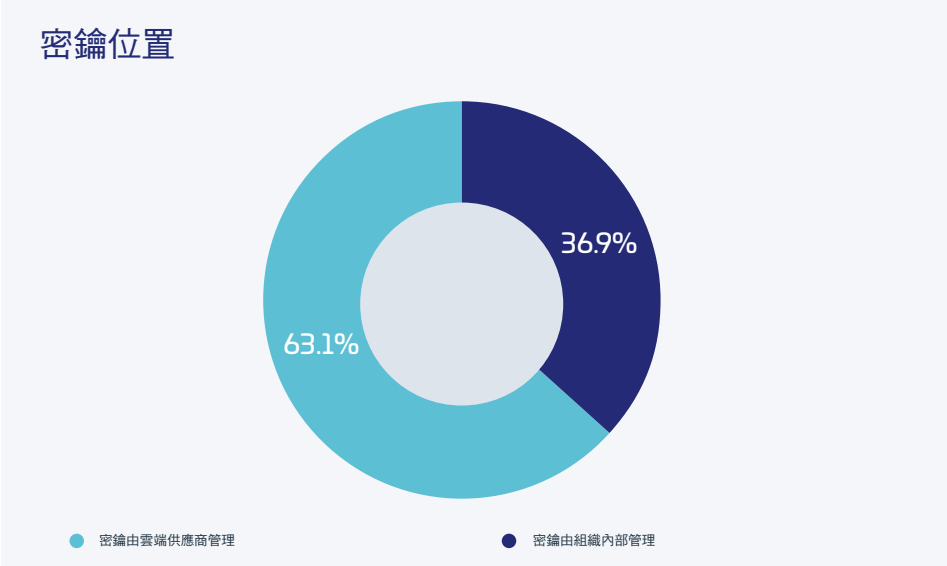
資料加密

資料在靜態或傳輸過程中（如將資料從辦公室伺服器移轉至雲端）都可能面臨風險，因此在這兩種情況下皆須受到保護。對敏感資料進行加密的受訪者中，近 60% 的人會加密傳輸和靜態資料，而約 40% 的人只會對儲存的資料進行加密。

掌握**密鑰，即掌握資料。**

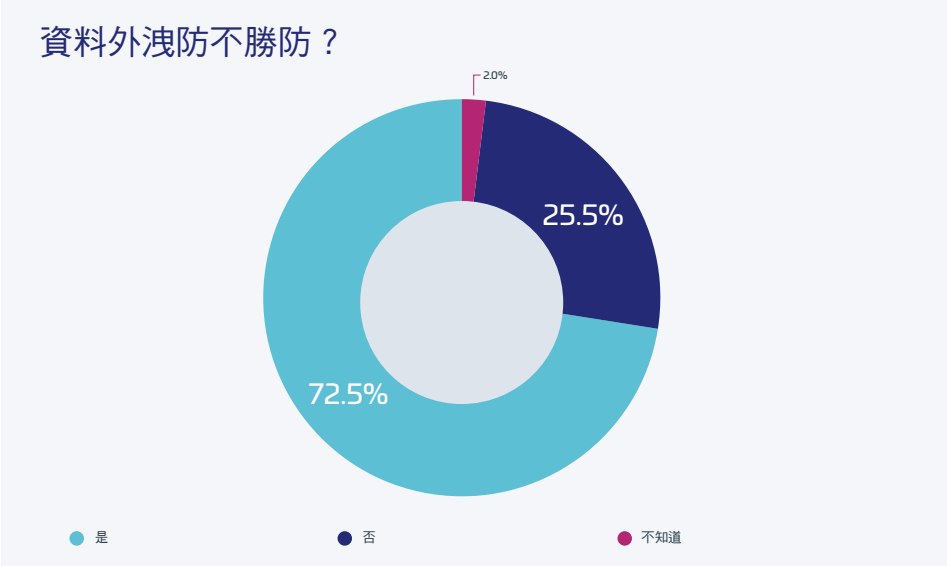


對資料進行加密受訪者之中，有將近三分之二的人會自行管理密鑰，而非交由雲端供應商。其餘的人則是將密鑰交由他們的雲端供應商管理，但這種做法風險甚高。

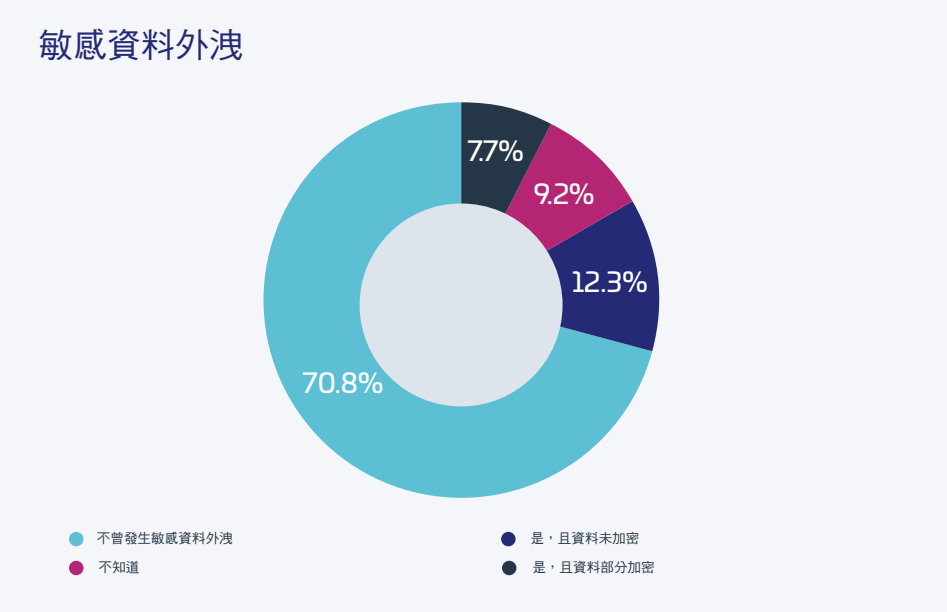


資料外洩政策

大眾普遍認為資料外洩是一大隱憂，其癥結點不在於資料外洩「是否發生」，而是「何時發生」。受訪的亞太地區組織中，有 70% 以上認為資料外洩是無法避免的。這足以讓各組織更積極主動地採取網路安全措施。

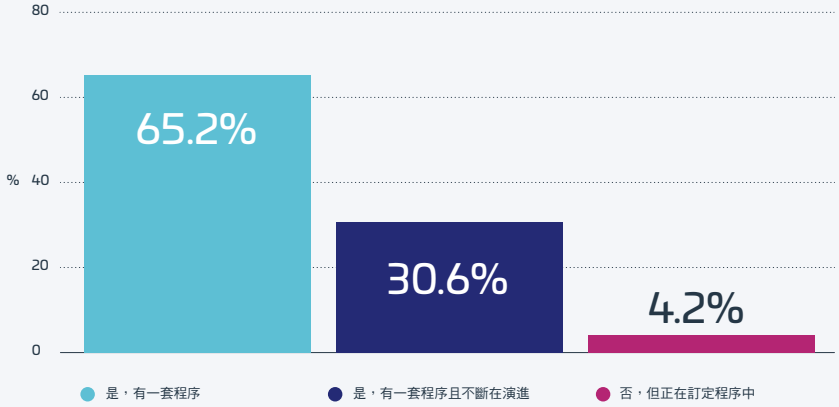


資料外洩的代價遠遠超出勒索軟體贖金和相關罰金，受害的組織見識到資料外洩對股價（雅虎）、商譽（Equifax、萬豪集團）的負面衝擊，以及長遠的財務影響。

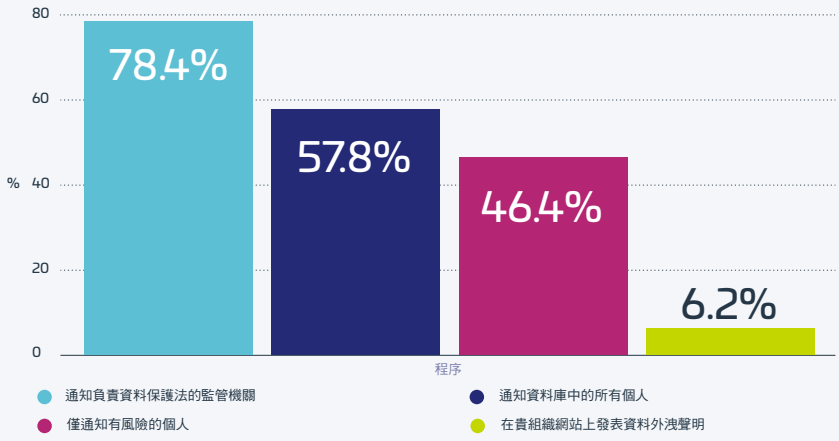


大多數受訪組織認為資料外洩是不可避免的，因此在資料外洩事件發生前，應當確立通報程序。

資料外洩的通報程序



資料外洩的處理程序



雖然亞太地區大部分的受訪組織皆有**資料外洩通報程序**，但是他們必須不斷改進其程序，以跟上**全球（例如 GDPR）或當地法規**和**資料保護法**的變化。

改善資料保護的建議

1. 確認敏感資料所在的位置

關鍵第一步是建立一個完整且準確的敏感個人資料所在位置藍圖。

- 針對各個系統或服務，哪些人具有存取權限？如何追蹤並將存取權限和其他活動指派給特定個人？
- 資料儲存於多少個不同位置和環境？這包括詳細的地理位置以及資料中心或延伸資料中心內的位置（包括虛擬和雲端環境），以及資料是否儲存於伺服器（檔案伺服器、資料庫或虛擬主機）、儲存區或共享區，還是硬碟、磁帶或其他媒體。
- 哪些類型的資料需要受到保護？敏感資料僅以結構化資料的格式儲存（如資料庫中的欄位），還是以非結構化檔案的格式儲存（如 PDF、影像或文字檔）？
- 資料傳輸的位置？這可能包括在資料中心之間的資料傳輸網路，無論是在點對點還是多點環境中。

2. 盡可能減少資料儲存庫的數量

一旦確認並瞭解資料位置，就必須盡可能減少儲存敏感資料的位置數量。如果組織可以減少儲存個人資料的環境或系統數量，便可大幅簡化對於資料保護法的法規遵循作業。

3. 利用加密和金鑰管理來保護資料

加密是建立資料的機密性和完整性的重要方式。事實上，資料保護法只會日益重視加密需求。

- 根據資料保護法的規定，未落實適當技術保護措施的組織必須制定資料外洩通報程序，但加密措施可讓組織免於使用通報程序的必要性。如果資料外洩，但資料已加密且密鑰受到保護，那麼入侵者將無法解密並存取實際資訊。
- 即使他國政府發出傳票或秘密存取私人資料庫，組織依然能夠握有資料最終解密的控制權。
- 藉由刪除與消費者加密記錄相關的密鑰，組織可以確保資料絕不會遭到非法存取。

4. 控管權限

弱式的靜態認證方式不斷成為入侵者下手的目標，讓他們得以在未經授權的情況下存取敏感資源，甚至引爆全面的資料外洩危機。因此，組織必須透過對任何具有價值的資源（無論是網路、入口網站或應用程式）建立強大的「多因素驗證」來消弭這類安全漏洞。

THALES

亞太地區

UNIT 904-906A, CORE D, CYBERPORT 3, 100 CYBERPORT ROAD, POKFULAM, HONG KONG

• 電話：+852 2815 8633 • 傳真：+852 2815 8141 • 電子郵件：InfoAPAC@gemalto.com

> www.thalescpl.com <