nCIPHER
AN ENTRUST DATACARD COMPANY

SYSTEX 精誠資訊

2020
台灣加密趨勢研究

Ponemon INSTITUTE

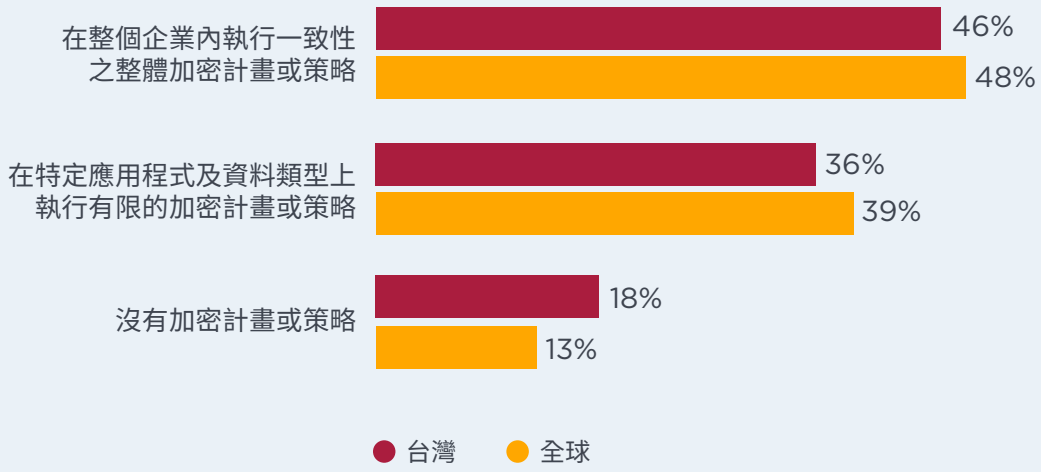
PONEMON INSTITUTE 很榮幸的發佈 2020 年台灣加密趨勢研究調查結果(本次研究由 NCIPHER 贊助)

我們在台灣對 302 位受訪者展開調查,旨在研究加密技術之使用情況,以及此技術對該地區企業安全狀況之影響。本次研究在全球範圍內對以下 17 個國家及地區多個行業領域的 6,457 人展開調查:澳洲、巴西、法國、德國、香港、印度、日本、墨西哥、中東(包括沙烏地阿拉伯及阿拉伯聯合大公國的受訪者)、荷蘭、俄羅斯聯邦、東南亞、韓國、瑞典、台灣、英國及美國。

46% 的受訪者表示,他們的企業在整個組織內執行一致性的整體加密策略。36% 的企業採用有限的加密計畫或策略。

以下頁面匯總了 2020 年的調查結果。

46% 的企業具備企業加密策略



加密策略及加密技術的採用

IT 營運對指導加密策略產生了最深刻的影響。儘管整個企業都有責任實行加密策略，但 IT 營運（30% 的受訪者）產生的影響最大。28% 的受訪者表示，並未組建單獨的職能部門來負責加密策略事務。

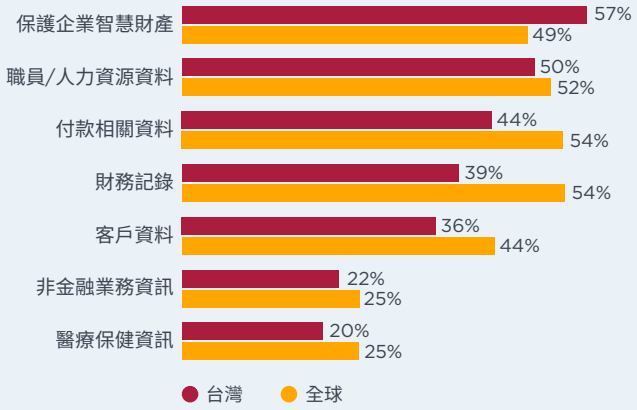
最常加密的資料類型有哪些？57% 的受訪者表示，他們的企業正在加密智慧財產，而 50% 的受訪者表示，職員/人力資源資料已經加密。

威脅、主要推動力及優先事項

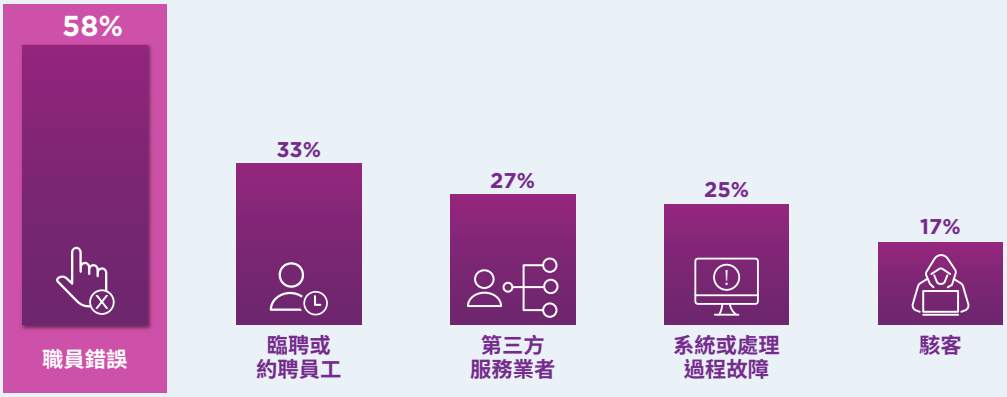
內部人員疏忽大意是機敏資料的最大威脅。58% 的受訪者表示，職員錯誤是洩露機敏資料或機密資料的最重大威脅。臨聘員工或約聘員工緊隨其後（33% 的受訪者）。

使用加密技術解決方案之主要推動力是保護個人資料及智慧財產。迄今為止，保護消費者個人資料是使用加密技術之主要推動力（62% 的受訪者），其次是保護智慧財產（57% 的受訪者）。

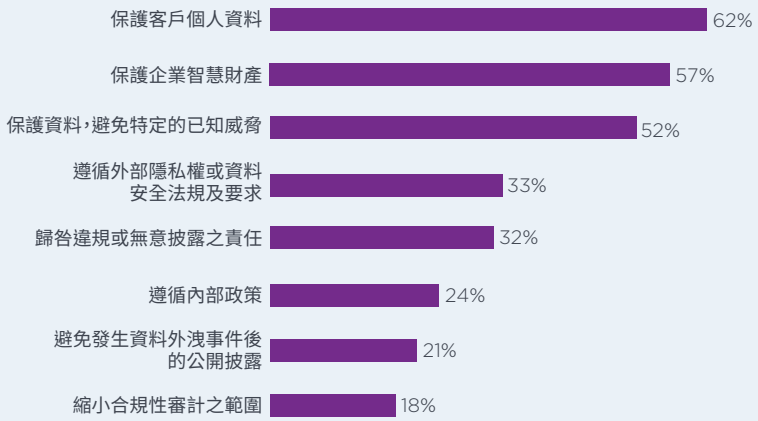
加密資料的主要類型



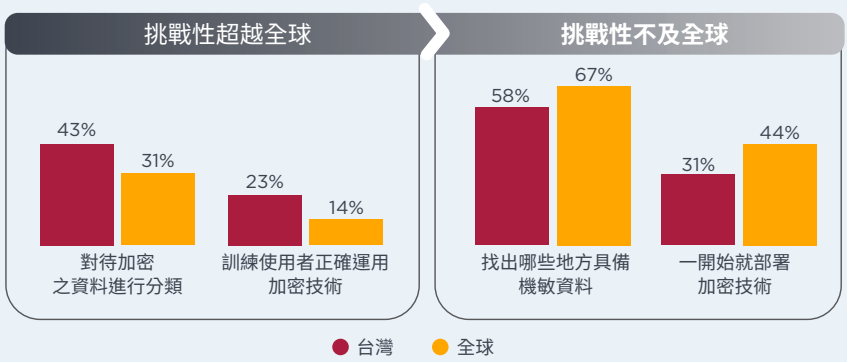
職員錯誤是洩露機敏資料的最重大威脅



運用加密技術之主要推動力



規劃及執行資料加密策略之最大挑戰是什麼？



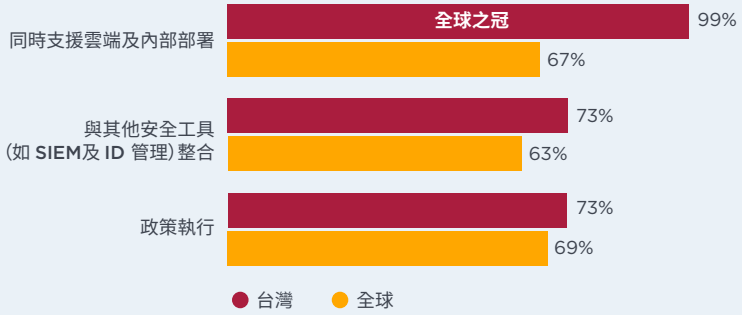
最大的難處在於尋找機敏資料在企業內的存放之地。58% 的受訪者表示，規劃及執行資料加密策略時，所面臨的最大難題是尋找機敏資料在企業內的存放之地。而 43% 的受訪者表示，第二大難題是對待加密資料進行分類。

某些加密功能比其他加密功能更加重要。本次研究要求受訪者將他們認為對所在企業之安全狀況最重要的加密技術功能予以評級。幾乎所有受訪者 (99% 的受訪者) 都將同時支援雲端及內部部署視為重要功能。其他重要功能為整合其他安全工具及執行政策 (佔所有受訪者的 73%)。

部署選擇

由於企業需求極其多樣化，並沒有哪一種加密技術佔主導地位。分別有 69%、56% 及 56% 的受訪者表示，最有可能廣泛部署的是資料庫、網際網路通訊及筆記型電腦和硬碟的加密。59% 的受訪者表示，物聯網 (IoT) 平台及/或資料儲存庫及物聯網裝置至少已部分部署加密技術。

台灣特別偏愛同時支援雲端及內部部署之加密解決方案



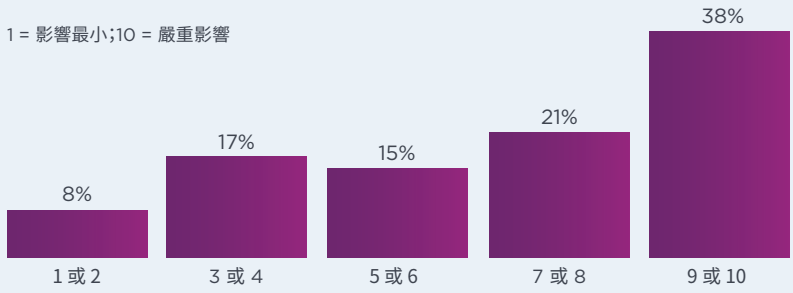
金鑰管理之相關態度

金鑰管理有多令人苦惱？59% 的受訪者將金鑰管理之苦惱程度評為極高。最主要的原因是：金鑰管理的工具不足、系統孤立而分散、缺乏專業人才。

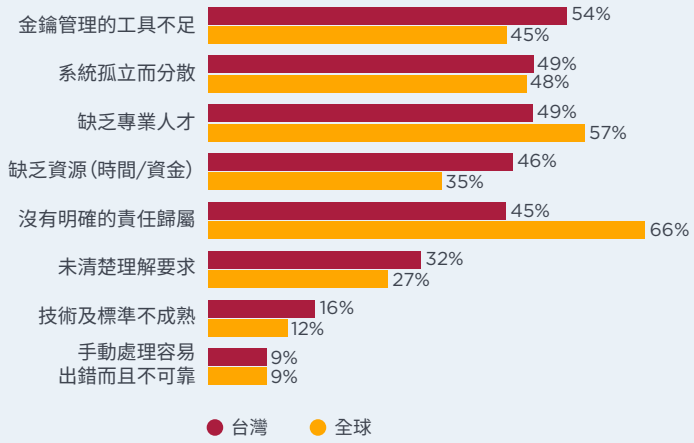
最難管理的金鑰有哪些？57% 的受訪者表示，管理難度最大的是最終使用者加密金鑰，其次是外部雲端或託管服務金鑰，包括自帶金鑰 (BYOK) 及簽章金鑰 (受訪者比例各佔 52%)。

企業大多採用正式的金鑰管理政策。47% 的受訪者表示，他們的企業使用正式的金鑰管理政策 (KMP)，手動處理的比例次之 (45% 的受訪者)。

近 60% 的受訪者認為金鑰管理令人苦惱不堪



金鑰管理令人苦惱不堪的原因有哪些？



新興技術

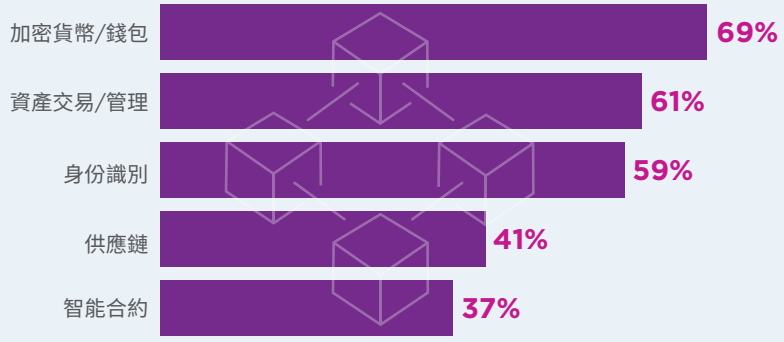
企業擬將區塊鏈用於加密貨幣/錢包及資產交易/管理。65% 的受訪者表示，他們的企業擬使用區塊鏈。分別有 69% 和 61% 的受訪者表示，兩大主要用例是加密貨幣/錢包及資產交易/管理。

主流企業採用多方運算要比量子演算法更早得多。本次研究要求受訪者評估採用量子演算法、同態加密及多方運算需要多長時間。據估算，採用量子演算法平均需要 8 年時間，而採用多方運算預計平均需要 6 年時間。

硬體安全模組 (HSM) 之重要性

未來 12 個月內，硬體安全模組對於加密策略或金鑰管理策略之重要性會持續上升。83% 的受訪者表示對硬體安全模組有所了解。我們詢問所在企業目前已部署硬體安全模組的受訪者（39% 的受訪者），硬體安全模組對其加密策略或金鑰管理策略的重要性如何。61% 的受訪者表示，硬體安全模組在現階段為很重要，而 66% 的受訪者認為，它們在未來 12 個月內會成為重要。

65% 的企業打算使用區塊鏈
前 5 個使用案例為：



硬體安全模組 (HSM) 用於加密或金鑰管理之重要性日趨增加

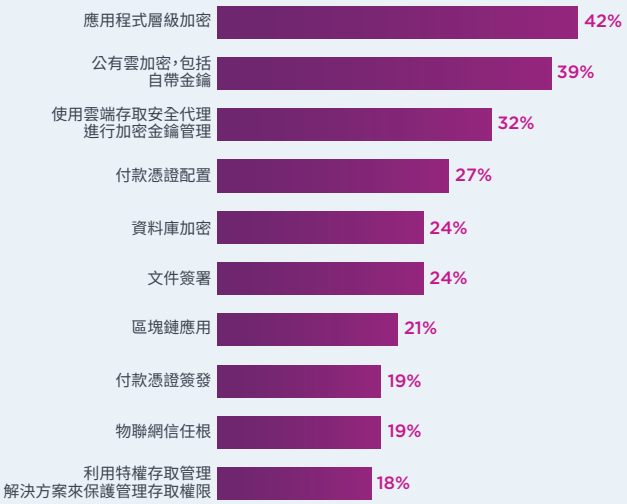
企業使用硬體安全模組之方式63% 的受訪者表示，他們擁有一個專門提供加密服務的團隊，37% 的受訪者表示，每個應用系統所有者/團隊均有責任處理各自的加密服務事務。如今，42% 的受訪者表示，他們的企業使用硬體安全模組來實行應用程式安全加密，而 39% 的受訪者表示，他們會將硬體安全模組用於公有雲加密，包括自帶金鑰。未來 12 個月，他們擬將硬體安全模組用於資料庫加密及應用程式層級加密，受訪者分別佔 40% 和 32% 的比例。

雲端加密

大多數企業會將機敏資料或機密資料傳輸至雲端。53% 的受訪者表示，他們的企業目前會將機敏資料或機密資料傳輸至雲端（無論是否已加密或藉由其他某些機制使之無法讀取），而 33% 的受訪者表示他們擬於未來 12 至 24 個月內實施此舉。

企業更願意管理用於加密雲端資料之金鑰。38% 的受訪者表示，企業會利用企業自己生成及管理之金鑰，先在內部實施加密，再將資料傳送至雲端，而 43% 的受訪者表示，所在企業僅會使用所管理之金鑰，對儲存於雲端之資料加密。

2020 年硬體安全模組 (HSM) 前 10 個使用案例



PONEMON INSTITUTE 簡介

Ponemon Institute© 致力於在商業及政府機構中推動實行負責任的資訊及隱私權管理實務。為實現此目標，該研究所開展獨立研究，對私營及公共部門領導者進行宣教指導，並對多個行業內企業的隱私權及資料保護實務予以證實。

NCIPHER SECURITY 簡介

Entrust Datacard旗下的nCipher Security為通用硬體安全模組（HSM）市場的領導品牌，為世界頂尖企業的重要業務資訊和應用系統提供可信度、完整性與管控力。當今快速發展的數位環境，提高了客戶的滿意度、競爭優勢和經營效率，卻也同時增加了安全上的風險。nCipher Security 的加密解決方案可以保護雲端應用、物聯網、區塊鏈、電子支付等新興技術，並滿足各種合規要求。為此，nCipher Security 一直提供值得全球企業信賴的技術來保護機敏資料、網路通訊及基礎設施免於威脅。任何時候，nCipher Security都能為企業的關鍵業務應用系統提供可信度，確保資料的完整性，並給予企業充分的管控力。
如欲瞭解更多，請瀏覽：**www.ncipher.com**

ENTRUST DATACARD 簡介

無論是登入公司網路、使用跨境服務、存取電子政務服務或購買商品，職員、民眾及消費者日趨期待能夠隨時隨地暢享體驗。他們還希望這個自由靈活的生態系統完全可靠、安全穩妥。Entrust Datacard 提供值得信賴的身份識別及安全交易技術，使這些生態系統得以實現。我們擁有逾 45 年的行業領先專業知識及經驗，擁有 2,000 多名職員，為全球 150 個國家/地區的客戶提供服務。
欲了解更多資訊，請造訪：**www.entrustdatacard.com**

SYSTEX CORPORATION 簡介

精誠資訊SYSTEX CORPORATION(台股代號6214) 成立於1997年，是台灣資訊服務產業龍頭企業。根據台灣權威財經媒體《天下雜誌》「台灣兩千大調查」，精誠蟬聯台灣軟體業第一名寶座超過10年。服務超過30,000家企業/機構客戶，代理經銷超過70項產品，提供大中華區的企業客戶跨域的專業資訊服務，幫助企業整合數據與變現，創造第二條成長曲線。
更多關於精誠資訊訊息，請上網：**www.systex.com**