CYBERARK 2019年全球進階威脅趨勢調查報告

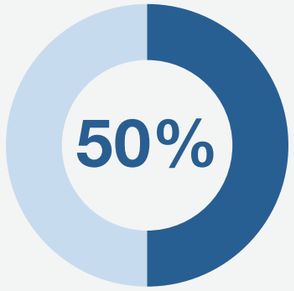
綜述

關於《CyberArk 2019 年全球進階威脅趨勢調查報告》

歡迎閱讀第 12 版年度《CyberArk 全球進階威脅趨勢調查報告》。今年的報告將分析在全球組織轉型成真正數位化企業過程中，企業主管展開的網路資安合作，並且繼續關注特權存取資安領域的做法。

2019 年初進行的調查總共有1,000 位 IT 資安決策者參與，受訪者分別來自美國、英國、法國、德國、新加坡、澳大利亞及以色列。大多數（88%）的受訪者為經理或以上級別。其中 21% 的受訪者為公司高層主管，而 35% 的受訪對象代表是有 3,000 名或更多員工的公司。

受訪者皆來自任何民營及公共部門（不包括消費者服務）中至少擁有 250 名員工的企業。所有受訪者都通過嚴格的多層篩選過程，並以線上方式接受調查，以確保只有適當的候選人才有機會參與調查。



的受訪者認同，無法防止攻擊者每次嘗試的滲透網路攻擊。

阻斷網際狙殺鍊的策略性資安投資

來自網路罪犯、競爭對手、民族國家、內部人士及其他人員的網路威脅皆無法避免，同時，業務運營成本日益增加。本次調查表明，在過去三年中，超過一半（53%）的受訪者的業務由於攻擊而受到影響，50% 的受訪者認同，攻擊者每次嘗試攻擊時，都無法防止攻擊者滲透網路。同時，數位化轉型的影響及需求也要求企業增加提升風險意識的資安投資。

經驗豐富的企業認識到，被破解的特權存取是攻擊者實現攻擊目標的捷徑。調查表明，資安開支的用途有所轉變，從邊界保護往內延伸，也包括追蹤攻擊者在網路內部的網際狙殺鍊關鍵點上的行動。在 24 個月的期間內，在計畫投入的資安預算中，有超過四分之一的預算將用於防止提權及隨後的橫向移動（結合起來平均占 28%），這是防禦攻擊能力增強的明顯指標。其他資料表明：

- 78% 的受訪者稱，駭客是他們的關鍵資產面臨的三大首要威脅之一
- 受訪者指出，網路釣魚等外部攻擊是他們面臨的最大資安風險（60%）
- 20% 的受訪者表示，他們的企業會定期進行紅隊演練（平均頻率為每三個月一次）

CyberArk 的觀點

隨著企業爭相開始數位化轉型，鑑於日益依賴自動化、雲端及 DevOps 流程方面的投資，資安團隊面臨的壓力不斷增加。通常，由於需要快速回應不斷變化的市場需求，即使攻擊面擴大或出現變化，資安風險增加，企業也往往會忽視或不會優先處理資安問題。

由於攻擊從未減弱，至關重要的是，應引導網路資安投資，加強資安控制並聘請技術熟練的員工，防止攻擊者在 IT 環境中橫向移動、破解允許攻擊者控制目標資產的特權憑證，並且發現其他想要竊取或破解的資源及資產。

在我們調查的所有領域中，在某個領域實施特權存取安全策略的受訪者均不超過一半

數位化轉型的資安障礙及特權優先順序

我們發現，在控制關鍵資產的存取權限方面，許多企業正面臨越來越大的挑戰，證據表明，從關鍵任務伺服器到物聯網（IoT），企業在基礎架構的某些方面落實特權存取資安策略。雖然在一定程度上，包括使用者電腦、機器人流程自動化（RPA）、IoT、基礎架構即服務（IaaS）及平台即服務（PaaS）環境等的整個IT環境都存在特權，但這也使我們有機會讓人們瞭解不斷擴大的特權攻擊面，尤其是這些攻擊面涵蓋基礎數位化轉型技術的情況下。

- 84% 的受訪者表示，如果特權帳號、憑證及資安憑證未受到有效保護，就無法全面保護IT基礎架構及關鍵資料
- 但是，**僅 35% 的受訪者為 DevOps** 或 CI/CD pipeline 實施特權存取資安策略，僅 32% 的受訪者為物聯網（IoT）實施資安策略
- 實際上，**在我們調查的所有領域中，在某個領域實施特權存取資安策略的受訪者皆不超過一半**

CyberArk 的觀點

從關鍵任務伺服器到雲端基礎架構及 RPA 工具，雲端基礎架構的每個環節都具有特權。企業應制定關鍵業務計畫，幫助增強意識並制定特權存取資安策略。在數位化轉型的過程中，由於需要更快推出新服務，管理層施加壓力，要求支援 SaaS 模型、更快推出新服務，或實現在全面整合資安控制之前敏捷開發，這些都是資安團隊需要瞭解並採取行動的重要新領域。

採取特權存取資安已達到一定成熟程度，各種產業中具有高度重要的資產及資料的企業（如金融、商業/專業服務及能源領域）引導潮流。企業及其相關生態系統要提高可靠性，必須在主動資安計畫中納入這個學科的重要領域，如即時監控特權連線活動，並能夠快速回應影響特權存取的高風險活動。資安專業人員必須洞察並以現代企業的速度執行的網路安全解決方案，且納入關鍵資料及資產的特權存取控制作為其計畫的基本要素。

抗拒遵從及被動式思維繼續存在

儘管做出轉變，開始擴大提升風險意識的資安投資並採取相應做法，但網路資安惰性及被動式思維仍繼續存在，使敏感性資料、基礎架構及資產面臨風險。令人擔心的是，41% 的受訪者表示，在網路攻擊得逞後，他們的企業寧願為資料丟失支付罰款，也不願更改安全性原則。

我們的調查深入研究企業為滿足日益嚴格的合規要求及避免創紀錄的經濟處罰所做的準備。

- **歐盟《一般資料保護條例》（GDPR）：**不到一半（46%）的企業充分準備好在規定的 72 小時內進行資料外洩調查及通知
- **《加州消費者隱私法案》（CCPA）：**儘管有 39% 的企業正在積極努力，但僅有 37% 的企業為遵守這項將於 2020 年生效的法規做好準備
- **《澳大利亞資料外洩通知法》：**62% 的澳大利亞受訪者稱，他們的企業已於該法律生效的一年多以前做好充分準備

CyberArk 的觀點

對整體網路資安局勢而言，僅僅擴大資安投資來滿足合規要求並不一定有效，儘管如此，GDPR 及 CCPA 等法規的頒佈，再加上新加坡有望於 2019 年修訂《個人資料保護法案》，這些都是企業需要投入鉅資來滿足的重要而全面的要求。

一般情況下，在發生資料外洩後需要在指定時間內通知主管機構，這意謂企業不僅需要快速偵測並回應外洩事件，而且需要能夠統計哪些記錄遭到外洩、有多少記錄可能會受到影響，並確定可採取的補救措施。為快速準確地報告外洩事件，或者更有效地，在外洩發生之前偵測到威脅，就有必要採取可靠的運營及資安控制措施。

CYBERARK 2019年全球進階威脅趨勢調查報告

威脅感知、資安投資及網際狙殺鏈

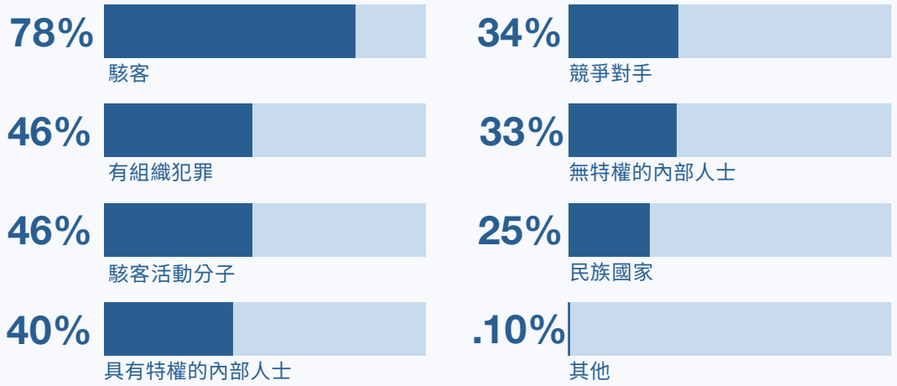
企業面臨著來自網路犯罪、攻擊者、民族國家、惡意內部人士及簡單人為錯誤的威脅，如今，這成為商業生活中的既定事實。如果攻擊得逞次數增多，展開業務運營的成本也隨之增加。

獨立調查表明，去年，資安事件的平均數量成長 11%，從 130 件增加到 145 件。同期，網路犯罪的善後平均成本增加 140 萬美元，達到 1300 萬美元。[i] 此外，全球攻擊者的駐留時間中值為 78 天，表明風險有所提升。[ii] 調查對象證實，他們對這些趨勢高度關注，82% 的受訪者稱他們的企業將防範網路風險作為一項重要的商業投資。

實際上，在過去三年中，超過一半（53%）的受訪者的業務由於網路攻擊而受到影響，**50% 的受訪者認同，攻擊者每次嘗試攻擊時，都無法防止攻擊者入侵**。攻擊者也認同這一觀點：Nuix [iii] 2018 年的一項調查表明，71% 的攻擊者認為他們能夠在 10 小時內突破鎖定目標的邊界。

在所有威脅之中，駭客會引起最明顯且切實的危險，**78% 的受訪者稱，駭客是關鍵資產面臨的三大首要威脅之一**。有組織犯罪（46%）及駭客活動分子（46%）也同樣名列前茅，而在今年，市場競爭對手嘗試實施的攻擊（34%）也突然成為一種威脅。

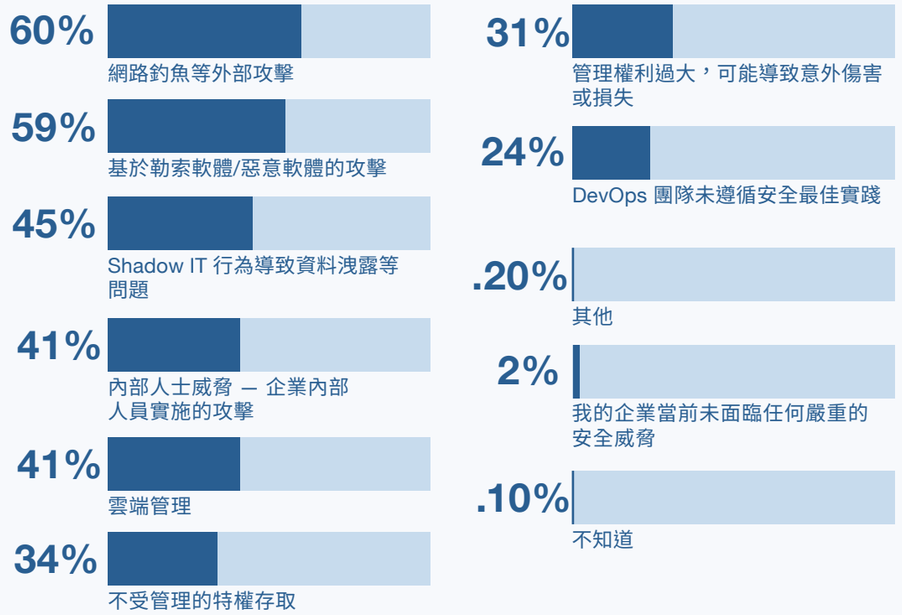
以下哪一種威脅實施者會造成貴企業關鍵資產的最大資安風險？



排名前三的回覆的組合

調查結果表明，受訪者意識到一系列資安風險。60% 的受訪者認為網路釣魚等外部攻擊是主要的資安風險，其次是基於勒索軟體/惡意軟體的攻擊（59%）、影子 IT 行為（45%）、內部人士威脅（41%）、雲端管理（41%）及不受管理的特權存取（34%）。當然，這些手段也可能在同一次攻擊中出現；例如，內部惡意人士通常會利用不受管理的特權存取。

您認為以下哪一項是企業當前面臨的最大資安風險？



對許多企業來說，最具破壞性的情景是攻擊者能夠存取重要的資料及資產。毫不奇怪的是，大多數（92%）的受訪者認為，為防止威脅滲入網路邊界，實施資安控制來保護關鍵資產至關重要 — 但關鍵是瞭解如何安排投資項目。網路資安支出是否用在相應的領域？網路資安是否能夠有效保護企業最具價值的資產？

要解答上述問題，必須首先瞭解網際狙殺鏈。

阻斷網際狙殺鏈的策略性資安投資

網路攻擊的動機各異：有組織犯罪通常會尋找可以變現的資料及資產；駭客活動分子會基於理念不同製造破壞；民族國家可能會竊取智慧財產權，或嘗試鼓動公民對資訊或可信流程提出質疑，從而引發社會混亂。

無論動機如何，攻擊者都會首先進行偵察，或研究針對類似企業實施的成功攻擊，以規劃執行攻擊或實現攻擊目標所需的分步驟路徑。雖然每次攻擊都各有不同，但是，有一點始終不變：攻擊者總是會尋找最便捷的攻擊路徑。

如果一開始就可以針對高特權個人的電腦發動攻擊來加速攻擊過程，攻擊者必然會這樣做。因此，企業必須仔細分析他們的環境，考慮各種攻擊方法，並採取以降低風險為首要目標的方法來保障此路徑中的潛在步驟的安全，以阻斷網際狙殺鏈。

運用分析全球資料外洩及網路攻擊的多年經驗，CyberArk Labs 團隊將定義任何攻擊中的關鍵步驟，以及可以阻斷狙殺鏈的時點，如下所述：

網際狙殺鏈中的步驟

1. **初步感染**是指攻擊者透過破解桌上型電腦、筆記型電腦、行動設備或伺服器等終端，在攻擊目標中建立據點的時刻。這是狙殺鏈中最關鍵的時點之一。

2. **偵察**始於狙殺鏈的早期階段，並貫穿整個攻擊過程。資安團隊面臨各種挑戰，不僅需要偵測網路探查，而且需要快速區分合法資訊收集與實際威脅。

3. **命令與控制**通訊通常很難被偵測。攻擊者會利用社群網路及合法服務來加密資料，以 SOC 團隊幾乎不可見的方式發送傳入命令並向外傳輸資料。

4. **提權及橫向移動**彼此密切相關，並且是關鍵時點，這時，攻擊者將有權存取進入特定系統所需的憑證，然後開始向目標移動。在這個階段，攻擊者將會曝光，攻擊目標（如資料庫、系統、雲端基礎架構）及途徑（如破解的憑證、易受攻擊的軟體）被揭示出來。但是，為偵測威脅，企業必須有效控制各種合法通訊及身份驗證方法，否則攻擊者將可以輕鬆入侵。

5. **中斷/破壞**是指攻擊得逞所造成的後果，也是狙殺鏈的末端。透過在網路或雲端環境中成功巡覽並存取目標系統及資料，攻擊者就能夠足夠有效地操縱整個網路，突破資安控制。勒索軟體及資料外洩是最近的攻擊事件所造成的一些最直接的後果。

攻擊者會設法以最便捷的方法破解特權憑證

網際狙殺鏈

24% 的總計畫資安開支 — 今後 24 個月

28% 的總計畫資安開支 — 今後 24 個月

透過分析網際狙殺鏈投資，調查表明，**企業計畫在今後 24 個月中將超過四分之一的總資安預算用於防止提權及隨後的橫向移動（組合起來平均占 28%）。**

最大的單項計畫投資用於防止初步感染（平均占 24%），這可能包括阻止惡意軟體獲得在系統中駐留所需的特權。隨後的投資用於防止中斷/破壞（平均占 18%）、防止偵察（平均占 15%），以及用於防止命令與控制（平均占 15%）。

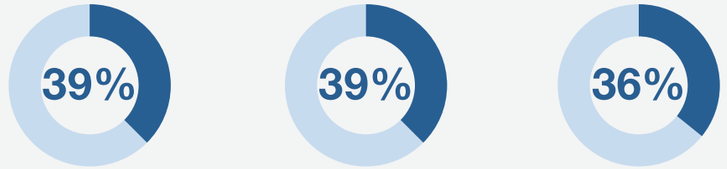
這種對資安的高度關注是我們聽到的好消息，這已延伸到邊界以外，還包括攻擊者存取及移動，以及阻斷網際狙殺鏈。有效的網路資安意謂瞭解攻擊者最終會入侵系統，並因此建立關鍵的 IT 安全層來保護整個企業的資料、部署在本地、雲端、終端上以及整個 DevOps 流水線中的基礎架構及資產準備好因應不可避免的攻擊。

採用特權存取資安措施的趨勢

雖然在過去兩年中，有 89% 的企業已實施或計畫實施新措施來管理特權存取，但是，很明顯（如圖所示），大多數企業離完全採取相關措施仍有一些差距。

60% 的企業使用特權存取安全解決方案來儲存及管理密碼，這是特權存取資安策略的首要重點。

排名前三的特權存取資安措施/引入的關注領域：



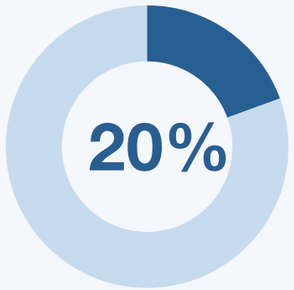
對負責管理關鍵基礎架構及應用程式的使用者實施更嚴格的存取策略

評估不受管理、不安全的特權帳號、憑證及資安憑證的數量，並採取管理措施且確保安全

引入更高效率監控手段，以更快速地回應高風險的特權相關活動

在實施特權存取資安計畫方面，垂直產業中擁有高價值資產及資料的公司（如金融、商業/專業服務及能源領域）引導潮流。

醫療、公用事業、能源及其他公司主要考慮關鍵基礎架構，並報告稱在特權存取資安的重要領域實施進階計畫。



的受訪者稱，
他們的企業會定期進行
Red Team 演練

此外，調查還表明，資安控制措施方面的投資正逐步成熟，有 63% 的企業正採取積極主動的方法，意謂他們會識別易受攻擊的資料或資產，並確保採取必要的控制措施來減少攻擊。根據假定的 ROI 排列這些投資的次序後發現，169% 的企業將資料加密納入前五項投資中，65% 的企業提名實施身份及存取控制，62% 的企業要求保護電子郵件及 Web 瀏覽器。在進行這些投資的同時，20% 的受訪者表示，他們的企業會定期進行紅隊演練（平均頻率為每三個月一次）。

在主動實施資安措施方面，法國、澳大利亞、美國及新加坡的企業（總占 68%）保持領先。在整個垂直產業，建築及能源領域是採取資安措施最積極主動的領域，這兩個領域的企業共占 72%。

[1] 這指每美元開支降低的關鍵資產風險，即最有效的開支

特權存取資安必須策略性成為確保資安的優先工作

備受矚目的資安事件一再證明，攻擊者會採取最便捷的攻擊路徑，幾乎總是針對可利用的特權憑證實施攻擊，以提升存取權限並進行橫向移動，直到接近攻擊目標。

許多企業將特權存取資安視為高效率網路資安計畫中的基本要素，計畫對網際狙殺鏈的這一關鍵領域的資安投資有所增加，即證明這種觀點。

與 2018 年全球進階威脅趨勢調查的結果類似，**大部分（84%）受訪者表示，如果未有效保護特權帳號、憑證及資安憑證，就無法全面保護 IT 基礎架構及關鍵資料。**

但也存在一些不一致的地方：雖然 84% 的受訪者認為整個企業已有效管理對特權存取，**但僅有 46% 的企業為保護關鍵任務伺服器（如網域控制站）等基本元件制定特權存取資安策略。**攻擊者破解網域控制站，就表示攻擊者完全控制整個網路。

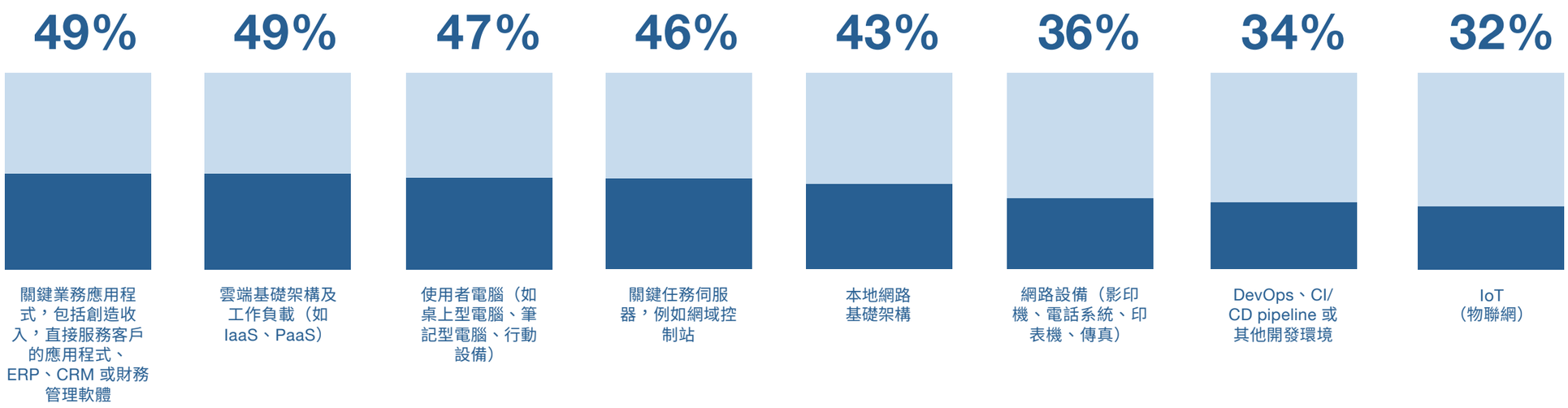
這強調應利用機會對企業進行進一步培訓，說明可以應用特權存取控制來加強整個網路的安全局勢。

特權無處不在：數位化轉型及風險

調查表明，雖然企業正競相開始數位化轉型，以最大幅度提高運營效率，創造最大的商業價值，但儘管意識到風險，許多企業尚未在這些關鍵計畫中整合特權存取資安控制。

分析數位化企業採用的基礎技術後發現，僅 35% 的企業為 DevOps 或 CI/CD 流水線實施特權存取資安策略，僅 32%的企業為物聯網（IoT）實施資安策略。實際上，在我們調查的所有領域中，在某個領域實施特權存取資安策略的受訪者皆不超過一半。

貴公司為以下哪些環境及設備制定特權存取管理策略？



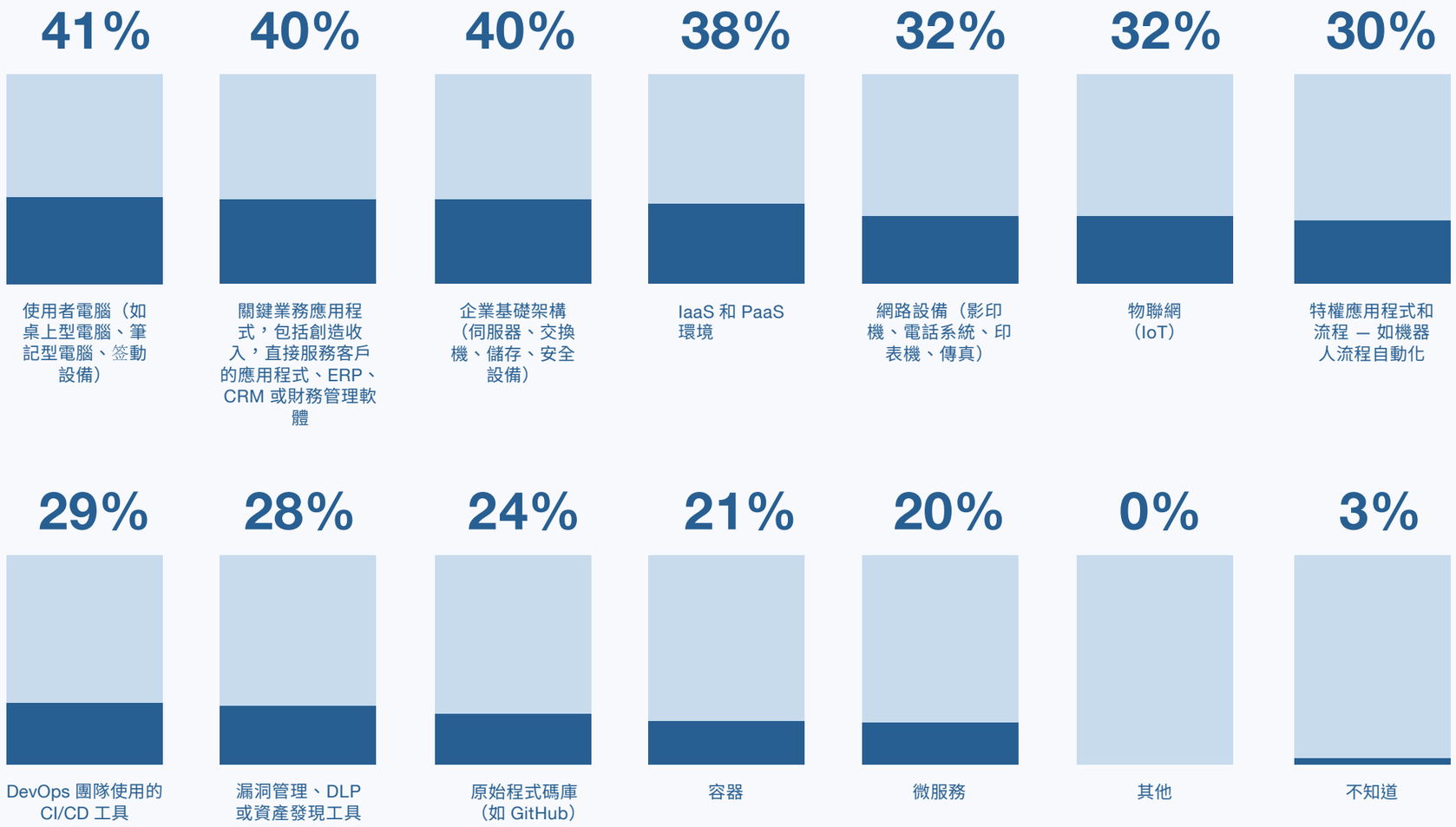
我們詢問，在他們企業IT環境的各個領域（包括與數位化轉型有關的領域）中，特權帳號、憑證及資安憑證存在於哪些地方。**雖然許多受訪者瞭解，我們提及的一系列技術都採用特權憑證，但他們的總體資安意識並不高。**

僅 20% 的受訪者瞭解微服務中存在特權帳號、憑證及資安憑證，21% 的受訪者瞭解它們存在於容器中，而只有 30% 的受訪者瞭解它們存在於機器人流程自動化（RPA）等特權應用程式及流程中。

因此，應該有機會介紹更多資訊，並協助瞭解特權攻擊面正在擴大 — 尤其是在數位化轉型基本技術中。

在我們調查的所有領域中，從關鍵業務應用程式（僅 49% 的受訪者制定策略）到 DevOps 環境（35%），在某個領域實施特權存取資安策略的受訪者皆不超過一半

您認為貴公司IT環境中哪些地方有特權帳號、憑證及資安憑證？



一旦攻擊者獲得特權憑證及資安憑證，他們就能夠全面存取 DevOps pipeline、敏感性資料庫甚至企業的整個雲端環境。只需瞭解最近的資安事件 （Uber、CityComp、SingHealth 等）就會發現，這些新型數位化技術使企業面臨更大網路風險。

大多數受訪企業都意識到這類威脅，並聲稱計畫增加提升風險意識的資安投資，以更有效地保護它們的數位化轉型專案：52% 的企業稱它們計畫增加雲端資安領域的投資，47% 的企業希望保護 IoT，42% 的企業計畫更有效地保護及管理SaaS應用程式。

法規實施及其對企業行為的影響

儘管取得這些進展，但是，在對待網路資安方面，35% 的企業仍採取更被動或反應式的方法，稱只有在不得已時才會花費資安開支，以滿足合規要求，在競爭對手進行投資時或在發生攻擊或資安事件後跟上步伐。如 2018 年報告中所述，由於網路資安惰性仍然存在，並且未能從過去的事故中汲取教訓，導致敏感性資料、基礎架構及資產繼續面臨風險。

令人驚奇的是，41% 的受訪者表示，在網路攻擊得逞後，他們的企業寧願為資料丟失支付罰款，也不願更改安全性原則。這可能是因為企業在經過分析後發現，資安投資的成本要高於違規成本。或者，可能是因為他們認為監管機構並不會徵收罰款。但是，更可能的情況是，他們無法核算成本，因為品牌受損、失去信任以及客戶忠誠度流失或降低這類成本非常難以進行量化。

本次調查深入研究全球的一些主要法規，包括：

- **歐盟《一般資料保護條例》（GDPR）**：自該條例於 2018 年 5 月生效以來，不到一半（46%）的企業充分準備好在規定的 72 小時內進行資料外洩調查及通知
- **《澳大利亞資料外洩通知法》**：62% 的澳大利亞受訪者稱，他們的企業已於該法律生效的一年多以前做好充分準備
- **《加州消費者隱私法案》（CCPA）**：儘管有 39% 的企業正在積極努力滿足要求，但僅 37% 的企業為遵守這項預計於 2020 年生效的主要法規做好準備

全球企業如何管理網路風險

雖然只有 5% 的受訪者根本未評估或報告網路風險，**但仍有 29% 的資安主管採用「紅綠燈」式的方法向董事會及高階主管上報風險。**

有許多不同的方法來評估網路資安風險計畫的強度。在被問及哪些因素促使他們在這些領域做出決策時，約三分之一（35%）的受訪者稱他們定義可接受的損失等級。這表示我們有機會在制定策略時提高成熟水準，考慮攻擊得逞後在財務上造成的「連鎖反應」，而不只是嘗試確定並彌補一次性漏洞。

另一方面，52% 的受訪者稱他們透過合規演練來評估網路風險計畫。但是，如我們所見， 從例行公事到強制實施控制（如 SWIFT 客戶資安計畫包含的控制措施），為合規所採取的資安措施很少充分有效率。

評估資安風險

調查表明，幾乎所有（94%）企業都採用某種形式的風險評估工具或框架來評估網路風險。例如，28% 的受訪者採用 FAIR （資訊風險因數分析）方法從企業角度評估、管理及報告資訊風險。我們問及的其他一些框架，如 TARA（威脅代理風險評估）及 NIST RMF（美國國家標準與技術研究院的風險管理框架），也有助於確定漏洞並就緩解策略提出建議，但卻無法評估漏洞對企業造成的財務影響。

結語

《CyberArk 2019 年全球進階威脅趨勢調查報告》表明，企業清楚瞭解網路風險以及網路風險可能造成的相應業務損失。企業漸漸認識到，最大的風險源於無法阻止攻擊者侵襲或存取關鍵資料及資產，而不是源於無法阻止攻擊者進行初步滲透，這幾乎無法阻止。

同時，企業及資安主管明白，不斷變化的業務流程以及為支援數位化轉型而增加的新技術投資也提高風險水準。他們意識到，企業需要採用數位化轉型所需的全新資安模型，但挑戰在於如何累積優勢，而不會擴大攻擊面。

企業需要做出合理的資安支出決策，以獲得最大報酬並降低網路風險。幸運的是，有跡象表明，資安專業人員意識到這一點。調查結果表明，受訪者清楚瞭解，從傳統本地系統到雲端及 DevOps 環境，特權存取資安在保護關鍵資產、基礎架構及資料等方面皆發揮的作用。

然而，調查也突顯一些明顯的矛盾。我們無法有效且自信地確定、管理並保護所有其中存在特權的領域，同時，也沒有為關鍵業務應用程式、開發環境及網域控制站等基本元件實施特權存取資安策略。

我們仍有機會對資安主管進行進一步培訓，指出特權相關的攻擊面正不斷擴大，幫助資安主管做出合理、以降低風險為首要目標的技術投資，為關鍵資料及資產提供更有效的保護，並最終為企業提供更全方位支援服務。

關於 CyberArk

CyberArk（NASDAQ：CYBR）是特權存取安全領域的全球領導者，特權存取安全是保護整個企業、雲端及 DevOps pipeline 內資料、基礎架構及資產的IT安全性的關鍵領域。CyberArk 提供業界最全方位解決方案，可降低特權憑證及安全憑證造成的安全風險。眾多全球知名機構（包括一半以上的財富 500 大企業）都依賴 CyberArk 公司來防範外部攻擊者和心懷不滿的內部人員。CyberArk 是一家總部位於以色列佩克提克瓦市的跨國公司，其美國總部位於麻塞諸塞州牛頓市。公司還在美洲、EMEA、亞太地區及日本設有辦事處。有關 CyberArk 的詳細資訊，請瀏覽 www.cyberark.com，閱讀CyberArk部落格 ，或關注 Twitter（@CyberArk） ， LinkedIn 或 Facebook。

[i] Accenture 網路犯罪成本調查，2019 年 3 月：https://www.accenture.com/us-en/insights/security/cost-cybercrime-study
[ii] 2019 年 Mandiant M-Trends 報告，2019 年 3 月：https://www.fireeye.com/current-threats/annual-threat-report/mtrends.html
[iii] Nuix Black Report，2018 年 4 月：https://www.nuix.com/black-report/black-report-2018

CYBERARK®

07.19.Doc.373314832