您的資安策略複雜性會不會是您最大的風險？

安永2023年全球資安長洞察調查

ey.com/cyberinsights

The better the question.
The better the answer.
The better the world works.

Building a better working world

目錄

第一章 - 採納新興科技：以簡化確保安全 5

第二章 - 安全創造企業可防護整體攻擊面 7

第三章 - 用業務口吻進行溝通 9

第四章 - 安全創造企業加速實現價值的五大方式 12

安永的「2023年全球資安長洞察調查」（EY 2023 Global Cybersecurity Leadership Insights Study）說明了領導企業如何在強化防禦措施同時，又能創造價值。

隨網路攻擊的威脅升高，對於資安的投資不斷增加，但只有五分之一的資安長(CISO)與其他高階主管認為他們的措施能有效因應當下及未來的挑戰。

安永「2023年全球資安長洞察調查」的受訪者也點出他們有所疑慮的原因。各企業平均每年面對44起重大資安事件，但它們偵測與反應的速度緩慢，有四分之三的企業平均需要六個月以上的時間來偵測並回應一個事件。同時，過去五年來已知網路攻擊次數增加約75%[1]，而勒索軟體導致的成本預計將從2021年的200億美元攀升至2031年的2,650億美元[2]。新型態、縝密的敵人正在利用最新的技術提高攻擊的速度與規模。對於財務、監管與商譽等層面的衝擊也日益加劇。

關於本研究

2023年2月及3月，安永在全球進行一項研究，以更加了解企業如何處理其組織的網路安全事宜，以為當下及未來的資安威脅做準備。我們調查美洲、亞太地區（APAC）、歐洲、中東、印度及非洲（EMEIA）共25個國家、涵蓋19個產業的500位高階主管與資安長，受訪企業年營收為10億美元以上的企業組織。

簡介

- 儘管各企業紛紛提高對資安的投資，但隨著敵人利用先進的科技並擴大攻擊面，威脅同樣加劇。
- 最傑出的資安長(CISO)們，會簡化他們的技術領域，強調自動化，並有效地在組織的各個層級之間進行溝通。
- 改善網路安全不僅可減少企業的網路弱點；更可以透過優化技術支出、促進合作及建立信任感來創造價值。

1 Cyber Events Database
2 Cybersecurity Ventures

我們透過統計模型，找出一些具備最有效資安管理的領導組織–我們稱這些組織為「安全創造企業」。相較於表現差強人意的「易受威脅企業」，這些安全創造企業較少發生資安事件，且對於事件的偵測和回應速度也更快。這些安全創造企業較為滿意其當下的資安措施 (51% vs. 36%)，也更加認為已做好因應未來威脅的準備 (53% vs. 41%)。

安全創造企業的資安措施不但可保護其組織，也能為組織創造價值。它們明顯地更能預見這些措施對其因應市場機會及轉型與創新步調的正面影響。安全創造企業在以下三個關鍵領域中的不同作為讓它們與眾不同：

- 它們能夠迅速地採納新興科技，並以自動化方式與資安技術搭配及簡化流程。
- 它們制定具體的策略以管理來自雲端、內部與第三方的複雜攻擊面。
- 它們將網路安全觀念深植到組織的三個層級之中，從高階主管到廣大的員工及資安團隊本身。

定義安全創造企業

為了找出資安管理成效較佳的企業，我們要求領導者就一系列客觀與主觀的資安指標來評估他們的企業：平均偵測時間 (MTTD)、平均回應時間 (MTTR)、資安事件次數、企業的資安整合程度，及資安對創新及價值創造的影響。

我們透過統計模型將受訪企業分為以下兩組：安全創造企業（高績效組織），占整體調查樣本的42%；及易受威脅企業（低績效組織），占調查樣本的58%。

1 採納新興科技：以簡化確保安全

企業正急於打造它們的網路技術堆疊，進而導致複雜度增加；故最有效的方式就是降低複雜度。

資安工具與應用程式近年來在精密度、速度與有效性方面頗有改進。根據 Pitchbook，這是因為大量投資推動的成果，2010年至2022年間，對資安的投資高達1.3兆美元，年複合成長率達16.6%。

本研究顯示有一波新的技術建置階段即將到來，84%的企業目前正處於在其既有資安解決方案中增加兩項以上新技術的早期階段。但諷刺的是，當下對於資安有效性的最大威脅就是各項安全措施的規模與其複雜度，因為它限制了可見度。

> 越是複雜的技術環境，越加難以迅速擷取信號並解決問題。
>
> **Richard Watson**
> 安永全球與亞太區資安顧問主管

將所有技術彙整至單一平臺並減少供應商產品數量，將簡化整合、使得遙測的數據更容易浮現出來，從而有助於資安團隊更有效率地發現事件。資安長必須轉變企業導入資安技術的方式，制定一套全面的技術策略，以合理化既有系統、解決如雲端與生態系統合作等新興業務的網路安全需求，並充分運用自動化。安全創造企業遵循此措施。

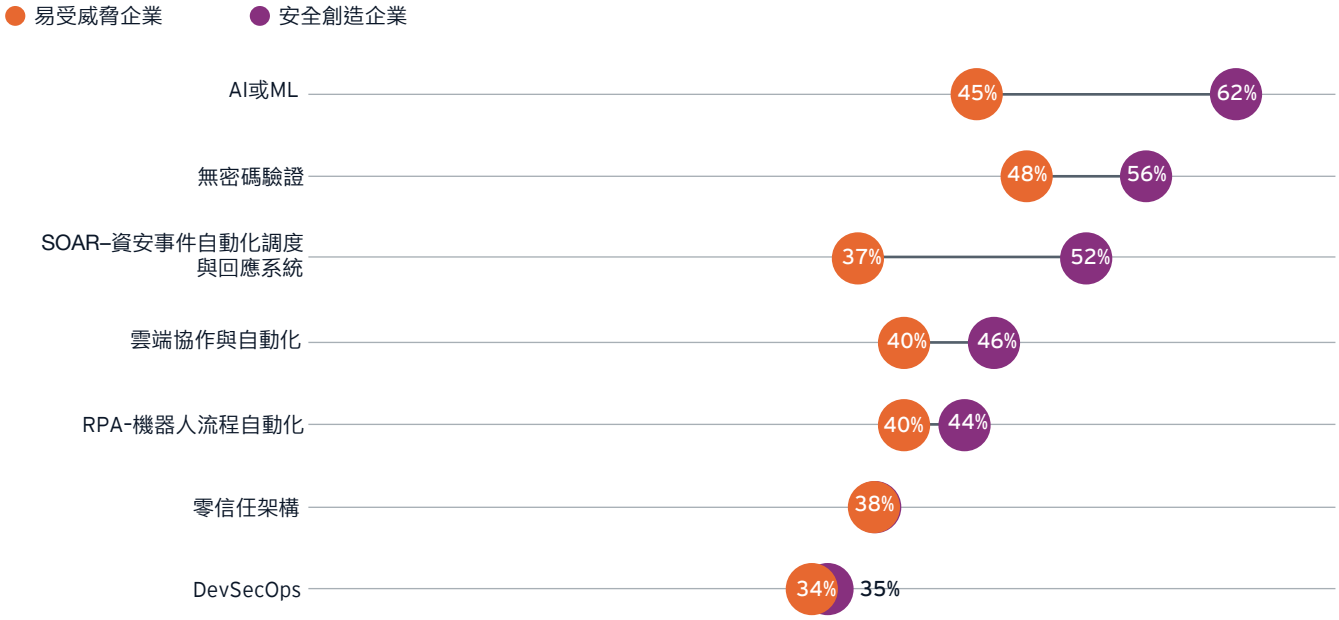
有70%受訪企業自定為新興科技的早期採用者，它們都著重於運用先進解決方案簡化其環境，特別是運用自動化。它們較傾向採用人工智慧（AI）或機器學習（ML）（62% vs. 45%）與資安事件自動化調度與回應系統（SOAR）（52% vs. 37%）等相關技術，或已處於後期採用階段。這為它們帶來了無縫式、全組織的防禦體系，並為資安事件提供清晰的見解。

安全創造企業中有較高比例受訪者表示它們的資安措施也會隨威脅變化而提高適應性（45%表示有正面影響）。相較之下，只有34%的易受威脅企業表示如此，反而有36%表示它們的措施對於適應性造成負面影響。儘管新興技術強化企業的能力，資安長必須確保它們制定一套簡化的方式提供具安全性的資安技術策略。資安長應：

- 簡化並合理化既有資安技術，以降低總持有成本，並建立可快速無縫運作的平臺。
- 檢視重複或整合不佳的固有系統，作為技術現代化的一部分。
- 採用簡化與自動化的資安流程，而非採用多個獨立的系統設置。
- 在不帶來新風險或使整體技術環境複雜化的前提下，採用新興技術。
- 考量以自動化為導向的措施，包含DevSecOps與SOAR。
- 追求合包（Co-sourcing）及一個可以簡化基礎設施、提高可見度，並產生成本效益的管理服務措施。

安全創造企業則更注重於促進自動化的技術

已經採用一項資安技術，或處於後期建置階段的受訪者。



以資料視覺化方式顯示安全創造企業與易受威脅企業個別已採用資安技術與措施，或處於後期採用階段者之比例。

SOAR-資安事件自動化調度與回應系統
RPA-機器人流程自動化

能源企業受制於分散的 IT 環境

在產業基礎上，我們的調查顯示能源企業在資安方面特別困難重重，只有35%表示它們的組織已做好因應未來威脅的準備，相較之下，其他產業此比例則達48%。此外，它們較其他產業更傾向「等待技術經試用與測試」，也更有可能將「未能優先考量新興技術整合」作為內部資安的最大挑戰。

僅有22%對其非IT員工採用最佳實務守則的情況感到滿意。

「近年來能源產業對於資安的投資漸增。其作為國家重要基礎設施的特性，有更嚴格的監管與法遵壓力，以確保其抵禦攻擊與故障的彈性。」安永全球資安主管Clinton Firth說道。再生能源轉型壓力迫使其將傳統營運技術轉為更分散的網路，包含透過物聯網（IoT）。大幅進步的資安技術有助於能源企業有效率地找出弱點，並發展關鍵控管技術，如特殊權限管理、威脅偵測與回應等。

然而，該產業有其結構性的重大挑戰。石油與天然氣企業是全球化的，但是資安標準與法規卻需要在地化。資安職能部門經常難以有效地與控管營運資產的電廠經理人進行合作，而原有的設備製造商與傳統的營運技術環境也是變革的障礙。

「過去幾年有許多能源企業已在資安投入與金融服務相近的金額，但它們的IT環境較為分散，」安永EMEIA 資安主管Alam Hussain表示，「能源企業像網路蜘蛛一樣，很難有一個解決方案可以因應各區域的網路風險。」

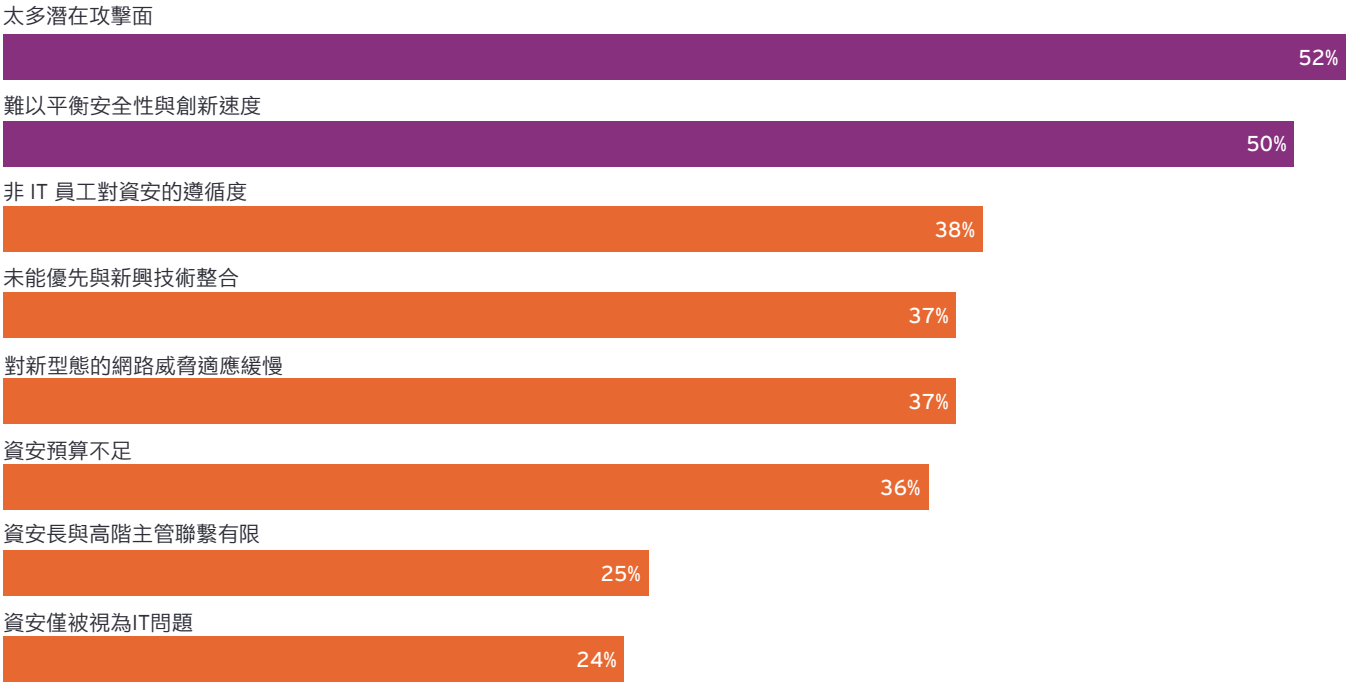
安全創造企業可防護整體攻擊面

「大規模的雲端」與更多層的供應鏈都會增加攻擊面。

而「太多潛在攻擊面」成為企業最常提起的資安內部挑戰。在企業內部，轉向大規模雲端運算及物聯網(IoT)增加了網路入侵的機會。再者，生態系統導向措施對當前的企業而言，雖然有助增進其價值，卻也為其帶來顯著的資安挑戰。整體而言，有53%的資安長認同，當前的數位生態系統中並不存在所謂的安全邊界。最危險的是供應鏈，2021年62%系統入侵事件都是由供應鏈造成的。[3]

企業面臨資安的最大內部挑戰

受訪者選出前三大挑戰項目。



以資料視覺化長條圖顯示企業面臨資安的最大內部挑戰。

3 Verizon Data Breach Investigations Report 2022

降低雲端與IoT建置的風險

四分之三的受訪者將雲端與IoT視為未來五年的最大技術風險。隨著雲端技術的採用，攻擊面大幅增加。變革的步調持續加快，而企業正在試圖迎頭趕上，若企業在未能充分設計規劃雲端介面與環境的情況下，就冒然採用雲端和IoT，這些快速的變革就可能使企業面臨資料遺失、外洩與中斷的風險。為克服此等複雜性，企業需要善用自動化方式。例如，有半數安全創造企業的資安長表示，他們的企業正使用雲端協作平臺及自動化措施來因應網路安全，或正處於晚期建置階段。

此外，企業不能預設所有網路攻擊都由雲端供應商負責處理。「雲端安全性是共同的責任，特別是在身分與存取權限方面，」安永資安顧問服務合夥人 Carolyn Schreiber 表示，「我們常見到錯誤的系統設置，建議在遷移到雲端時需要進行更多設置，而不僅僅是單純的『搬遷』。關鍵考量因素包括特殊權限管理，以避免權限越級、機密管理及避免橫向移動攻擊。從我們的客戶中，我們發現最安全的企業會詳細閱讀合約，並要求它們的雲端服務供應商 （CSP） 遵循與該企業相同的安全標準規範。讓內部團隊與CSP共同負責，是一個能在不增加雲端平臺與容器的安全風險控制情況下，完成移轉的方式。」

量化網路風險是一個新興領域，而透過自動化與資料分析可增加見解，並有助於風險優先度排序。各執行委員會與董事會對網路與數位風險的問題日益增加。資安主管階層應致力與利害關係人進行業務對話，用金額價值來解釋網路風險，遠比傳統上由資安長提供技術的方式將更新、更具說服力，也更有助於制定更好的決策。

APAC、EMEIA 及美洲地區的雲端規模及網路風險

APAC的受訪者較傾向將大規模雲端應用視為最容易引發威脅的技術之一 （占81%，相對於美洲的74%及EMEIA的 63%）。APAC 監理機關核准雲端服務的速度較慢，如此可能導致該地區延遲採用雲端，或使該地區對於過渡至雲端的信心落後於歐洲與美洲。

另一方面，EMEIA則較重視AI/ML帶來的風險（占49%，相對於美洲的38%與APAC的34%）。

供應鏈：早日參與並持續監控

當今所有企業都與它們的供應鏈有著密不可分的數位連結。網路攻擊者採用「從一到多」的策略，搜尋最薄弱的連結，來攻入成千上萬的企業。

> 過去五年來，我們確實見到攻擊者針對供應鏈的趨勢。若他們能入侵對30,000家企業至關重要的關鍵軟體供應鏈廠商，那他們就攻入了這30,000間企業內部。
>
> **Richard Bergman**
> 安永全球資安轉型主管

不過，儘管存在危險，易受威脅企業仍較注重於財務風險（占52%，相對於安全創造企業的 41%），而安全創造企業中，高度重視供應鏈風險的比例幾乎是易受威脅企業的兩倍(38%，相對易受威脅企業20%）及重視其相關風險（如智慧財產權保護風險）的比例（38%，相對於易受威脅企業24%）。認知風險是第一步，接下來資安長應致力順暢其組織的供應鏈，持續性而非一次性地掌握供應商對於網路攻擊的復原能力。與營運長(COO)及其他業務主管的深入合作，對於確保供應鏈中所有攻擊面的可視性至關重要。在較成熟的企業中，資安職能部門會參與供應商遴選，並建立更高標準的保障與持續管理。營運長與資安長的立場可能互相衝突，例如營運長可能因對資安的疑慮而錯失成長契機，而資安長作為企業組織的保護者，可能感覺到自己的價值被低估。但唯有雙方共同合作，資安防禦的復原力才可以真正實現的。[4]

4 How COOs and CISOs can build ransomware-resilient operations together

3 用業務口吻進行溝通

最有力的資安長會用高階主管與員工的語言，有效地進行企業內部溝通。

安全創造企業會在組織內部建立溝通橋樑。針對企業內部的三大層級-高階主管、資安團隊及其他多數員工，它們擅長與不同的利害關係人進行溝通，並明確意識到資安中的「人為因素」。

與高階主管溝通

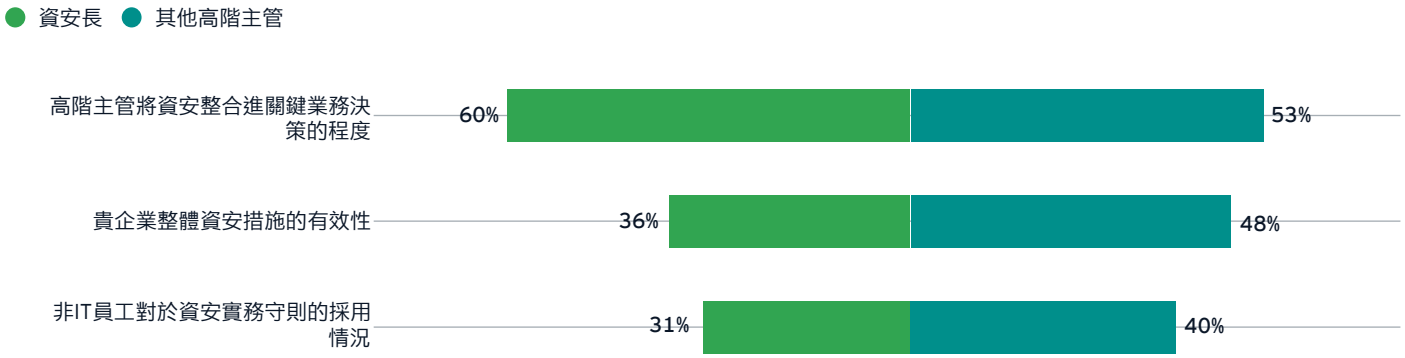
儘管過去資安長的角色主要在作業面與技術面，但在較成熟的企業中，資安可以作為一個部門與職能來運作，並在高階管理層中占有一席之地。我們的調查發現，受惠於資安長的角色日益重要，他們得以在當今的高風險環境下，成功取得必要的資源。預算在昔日曾經是最大的內部挑戰，但在本年度調查所列出的八大障礙中，僅排行第六。資安已逐漸被視為一項基本的業務復原能力、商譽及法遵問題，並願意為其提供充足的支援。

不過，儘管預算是一個關鍵因素，但資安需要充分植入在整體組織中。這需要高階管理層的認同、弭平知識差距，以及資安長與高階主管間的緊密溝通。然而，我們的調查顯示這些族群的意見並非是一致的。相較於高階主管，資安長們較少滿意於其組織整體資安措施的有效性（36%，相對於高階主管 48%），以及其組織因應未來威脅的能力（38%，相對於高階主管 54%）。

在安全創造企業中，其資安長與高階主管間的認知差距明顯較小，它們對高階主管將資安納入關鍵業務決策的程度較為滿意。這表示與高階管理層進行更有效的溝通，可以形成風險共識，並提高資安績效。對績效的一致共識，是較安全企業的標誌。能將資安營運融入核心業務優先事項與策略中的企業，發生資安事件的機率較低。最有力的資安長會將平鋪直敘的內容轉化為故事情節，從降低風險、業務影響與創造價值等方面引起共鳴。

資安長與高階主管對企業資安滿意度的大幅差距

選擇滿意或非常滿意的受訪者比例。



資料視覺化長條圖顯示，資訊長與其他高階主管的資安滿意度，以及此二族群間的差距。

為員工提供有效支援

更廣泛的整合重點是整體員工。人為錯誤一直是造成網路攻擊的主要因素。非IT部門單位沒有謹慎遵循資安實務守則，是我們的調查中排名第三大的內部挑戰。

僅半數的資安長表示其資安訓練是有效的，加上只有36%的人滿意非IT部門採行實務守則的程度，讓人不由質疑這些訓練的有效性。不過，安全創造企業對於採行資安最佳實務守則的滿意度高於易受威脅企業（47% vs. 27%）。重點在於對基礎知識的嫻熟度，各企業必須簡化其針對員工的最佳實務守則，並在各流程中設置防護步驟，以降低風險，不能單純仰賴法遵。較成熟的企業會進行漸進式的定期培訓，並善用最新的自動化與防護工具。將資安深植組織所有人員的心中，成為他們的第二天性，有助於確保更有效的訓練與依循。

人才：跳脫組織架構思考

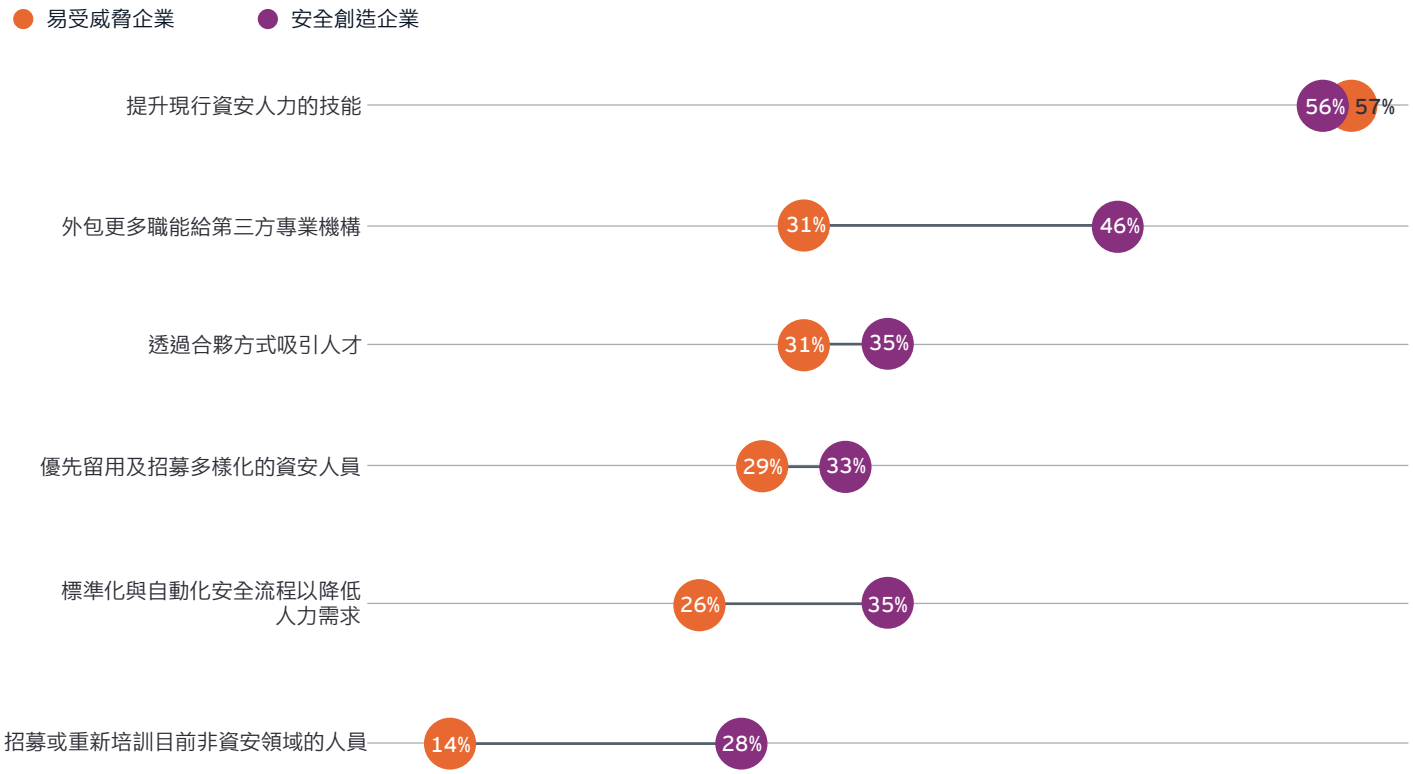
在網路勞動力中，人才是一個反覆出現的挑戰。過去一年中，資安人力缺口的成長速度是全球網路人力成長速度的兩倍以上[5]。資安正處於技能追趕階段，在我們的研究中，提高技能是大多數企業的關注重點。不過安全創造企業正以更有創意的方式因應此一挑戰。例如，他們優先招募或重新培訓目前非資安領域人員的意願較易受威脅企業高出一倍（28% vs. 14%）。非傳統招募員工可能來自各種背景，包括來自透過自動化顯著減少工作量的其他職能領域，如財務和一般IT部門，以及來自非傳統背景的學徒培訓。

主管會更靈活地思考如何塑造其網路職能的營運模式，如外包更多的安全營運工作（中位數25% vs. 15%），並更有可能在未來外包更多的職能予第三方專業機構（46% vs. 31%）。外包可以簡化企業內部資安職能，讓第三方專業機構專注於企業內部員工可能不具備的特定資安職能中。安全創造企業也會優先考量安全流程的標準化與自動化，以減少人力需求（35% vs. 26%），並進一步簡化其組織結構。

5 (ISC)² 2022 Cybersecurity Workforce Study

安全創造企業正靈活思考資安人力

將以下各項評為首要或重大優先事項的受訪者比例。



以資料視覺化方式呈現安全創造企業與易受威脅企業選用人才的優先標準。

儘管企業越來越傾向將資安工作的「人員與流程」外包，但對於技術本身卻更為謹慎。相對於外包公司受託管理眾多客戶的技術解決方案而言，企業通常更希望可以在自己的雲端擁有技術，並根據特定需求與風險偏好進行配置，同時又可受益於外包或合包所提供在技能與人員的支援。它們也受益於第三方外包機構的智慧財產權。

另一項創新能力策略，是透過制定個人職責來協調業務與資安團隊。「諮詢」能力透過理解需求並將資安考量因素融入業務之中，成為資安團隊與其他業務之間的溝通橋樑。有些企業正在嘗試一種「小組」方式，由一組資安顧問團隊在六個月或九個月的時間內管理一個進入該企業的「搬遷」過程，他們可能會執行一個安全開發週期、培訓相關人員，然後繼續進行下一週期。這可以為內部團隊注入新的技能，並使其透過實務操作進行學習。

安全創造企業加速實現價值的五大方式

領導者會利用自動化與協作方式來簡化技術環境，並在整體組織內有效地進行溝通。

資安不僅止於保護資產，若執行得當，也能夠支持並加速整個企業的創新與價值創造。在我們的客戶中，我們看見最好的企業會將資安植入企業的架構中。將資安融入企業與營運模式的各個部分，並將其功能從一個抑制因素轉變為價值驅動因素。

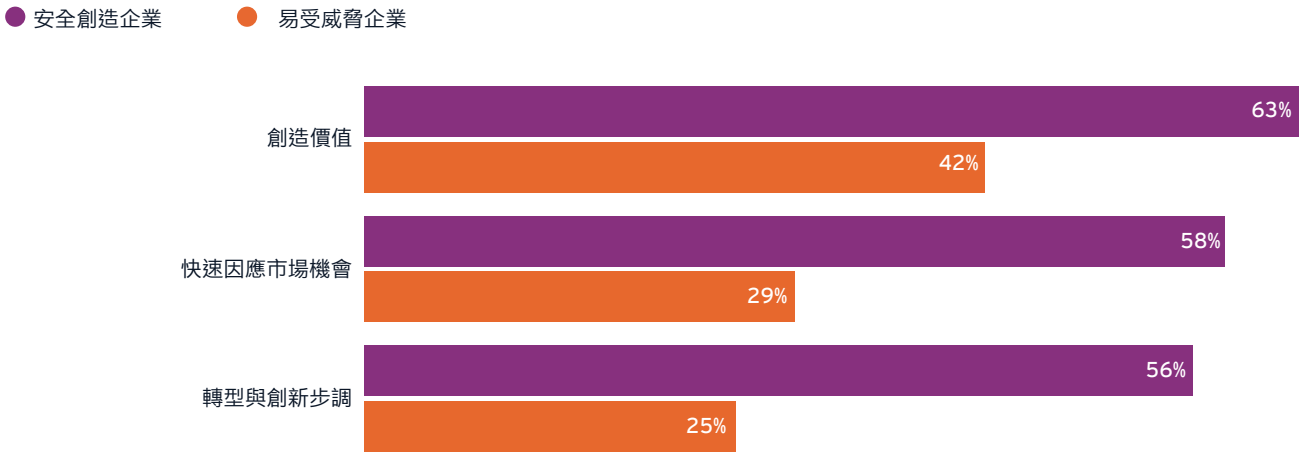
安全創造企業傾向表示它們的資安措施有助於組織的轉型與創新（56%，易受威脅企業25%）、快速因應市場機會的能力（58% vs. 29%），以及專注於創造價值而非僅保護價值的能力（63% vs. 42%）。價值創造可以用許多方式呈現。網路安全的企業可以贏得客戶與供應商更多信任，使其更放心與該企業進行交易。重新設計技術架構可以改善溝通、合作與員工生產力，並提升支出效率。

例如，安全風險促使一家零售巨頭進行網路改革措施，該措施除了降低脆弱性之外，也提高了價值，這點還是很重要。該措施包括更有效率的技術支出、去除過時及冗餘的工具、優化人力配置、細分角色與職責、更有效率的合作，以及強化該企業超過10億客戶群對其信任度。

我們的研究顯示，易受威脅企業較可能受困於在安全性與創新速度間取得平衡（55%，相對於安全創造企業的 42%），這進一步說明，有效的資安是達成價值與創新的平臺，而缺乏有效的資安則是一種障礙。無論是透過多品牌、全資或控股子公司、合作夥伴或合資企業，生態系統已經成為創造價值的基本業務策略。想充分發揮生態系統的優勢，就必須從一開始就將資安融入其中。資安長們必須透過標準化技術整合協議，確保在評估潛在合作夥伴時納入資安標準。他們也須與業務決策者進行有效溝通，以適當管理隨著業務擴張帶來的風險。比方說，雖然收購業務可能帶來資安風險，但如果該風險相對於機會而言微不足道，那麼它就如同其他任何業務風險決策，並不一定意味著須放棄追求收購。企業必須保持「合理的」風險程度。

安全創造企業的資安對於價值創造與創新有更正面的影響

受訪者表示他們的資安策略對以下方面有正面影響的比例。



以資料視覺化長條圖呈現就安全創造企業及易受威脅企業而言，資安為對價值創造、因應市場機會及轉型與創新步調的影響。

採取行動制定更有效及價值導向的資安策略

安永「2023年全球資安長洞察調查」的結果發人深省，高階主管正積極因應各種現行與預期的威脅。不過本研究也消除部分疑慮，亦即各企業之所以經歷非常不同的結果，其部分原因是由於它們的資安策略。透過向傑出者學習，企業可以在其組織內強調簡潔性、整體思維與整合資安考量因素，從而強化網路安全。這些都是易受威脅企業能力可及的範圍。本調查得出的主要行動要點包括：

1

簡化網路技術堆疊，以降低風險並提高能見度。自動化與協作可以減少技術環境的複雜性，以便能更快速地偵測信號並更有效地因應。

2

利用標準化與自動化來減少駭客對供應鏈的切入點，提高網路警覺性，並在不增加非必要機構的前提下持續監控性能。如此也可確保資安團隊在遴選供應商的初期階段就介入。

3

將平鋪直敘的內容轉化為故事情節，從降低風險、業務影響與創造價值等方面引起業務單位的共鳴。

4

結合漸進式且妥善設計的訓練與自動化和預防工具，透過設計讓員工具備資安意識。

5

將資安植入企業組織的結構當中，而非將其視為一種抑制因素。它能為企業提升價值，注入創新所必要的信心，並開啟新的收益與市場機會。

聯繫安永

張騰龍
總經理
安永諮詢服務股份有限公司
+886 2 2757 8888 ext. 88863
Tony.Chang@tw.ey.com

黃昶勳
總經理
安永企業管理諮詢服務股份有限公司
+886 2 2757 8888 ext. 88862
Jon.Huang@tw.ey.com

安永 | 建設更美好的商業世界

安永的宗旨是致力建設更美好的商業世界。我們以創造客戶、利害關係人及社會各界的永續性成長為目標，並協助全球各地資本市場和經濟體建立信任和信心。

以數據及科技為核心技術，安永全球的優質團隊涵蓋150多個國家的業務，透過審計服務建立客戶的信任，支持企業成長、轉型並達到營運目標。

透過專業領域的服務 - 審計、諮詢、法律、稅務和策略與交易諮詢，安永的專業團隊提出更具啟發性的問題，為當前最迫切的挑戰，提出質疑，並推出嶄新的解決方案。

加入安永LINE@好友

掃描二維碼，獲取最新資訊。

APAC No. 14007690
ED None

ey.com/zh_tw