cisco SECURE

資安

成果

研究

目錄

簡介

我們著手進行這項研究時，主要目標是為您（資安主管）提供實用的工具，指引您進行投資，成為推動力以協助您的資安計畫成功及更妥善管理風險。

我們的研究對象遍及全球（25 個國家/地區和超過 4,800 名受訪者），目的是以經驗衡量哪些因素可以帶來最優異的資安成果。這與我們過去在網路安全報告系列中傳達的內容截然不同，我們希望這種新作法和闡述風格能帶來令人耳目一新的感受且廣為接受。

眾所周知，資安技術不斷發展演變，以至於有時難以判斷成功與否。因此我們著手為本研究中的一些問題尋找解答：我們如何有效以高效率管理網路安全風險？為什麼即使是擁有高額資安預算的最大型公司仍難以取得一定程度的成果？可實現成功網路安全計畫的選項琳瑯滿目，從業人員應將重點放在哪些選項上？新技術？更多教育訓練？更妥善的事件回應程序？可能性沒有上限。資安團隊如何判斷哪一項最有效？又如何確定這種有效性不會改變？（搶先劇透：會改變的。）

這份研究將為您提供更多深入分析和信心，協助您集中注意力應對 2021 年及往後的景況。過去這一年充滿挑戰，嚴峻程度前所未見，但總是有措施可改善您的資安策略。請繼續閱讀，瞭解哪些措施最適合貴組織。

關於本調查		
採樣	**受訪者**	**分析**
思科與調查研究公司 YouGov 簽約，於 2020 年中進行一項完全匿名（來源和受訪者）的調查。	我們對來自 25 個國家/地區的 4,800 多名在職 IT、資安和隱私專業人員進行調查。包括產業、公司規模和所在地區在內的樣本人口統計資料列於附錄 A 中。	Cyentia Institute 代表思科對調查資料進行了獨立分析，得出本研究中提出的所有結果。

方法

- 我們詢問受訪者其組織是否遵循涵蓋控管、策略、支出、架構和營運領域的 25 種資安措施。
- 接著我們針對將近十二個高層級資安目標或成果（分為三個主要類別：為企業賦能、管理風險和高效營運），詢問每個計畫的成功程度。
- 接下來，我們進行了廣泛的多變量分析，目的是找出與成功計畫層級成果密切相關的資安措施。

為了使這份報告更加貼近真實情況，我們與世界各地的眾位專家緊密合作，包括我們的 CISO 顧問團隊。如果您需要一點繼續閱讀下去的動力，希望以下引言可以讓您獲得鼓舞：

「這不是一份您可以扔進禮品袋就視而不見的行銷報告，而是一份值得您捧在手心反覆閱讀的報告。事實上，這份報告將會改變我們對於執行資安計畫的看法。」

思科首席顧問資安長 Wendy Nather
思科旗下公司 Duo Security

主要發現

是否有證據可證實資安措施確實會影響計畫層級的成果？

在 275 種措施與成果的組合中，有 45% 呈現出顯著的相關性；這表示某個特定的措施會影響達成特定成果的可能性。

其中相關性最高的是哪一項？

主動同類最佳技術更新策略能讓您跟上業務成長的腳步。

相關性第二高的是什麼？

高度整合的技術堆疊可提高資安人才的招募和留任率。

想讓整體計畫取得成功嗎？

投入資源主動更新技術並整合您的技術。

想要建立人人接受的強大資安文化嗎？

聚焦於優良的設備、明確的方向、準確的警示和及時的資安問題修正。

希望避免將來發生資安事件和遭受損失？

對重大事件回應作業進行事後回顧。

哪些資安措施最難實行？

在全部 25 項措施中，屬於架構和營運類別的措施似乎最具挑戰性。

計畫最成功的地方在哪裡？最困難之處為何？

計畫在符合法規遵循規範方面最為成功。最困難之處是避免計畫外的工作和浪費精力。

NIST 網路安全架構的哪項功能對成功幫助最大？

識別功能是第一功臣。保護功能對計畫整體成功的貢獻度則排名倒數第二。

組織如何將 COVID-19 對營運造成影響降到最低？

組織維護現代化的 IT 和資安基礎架構、對角色型教育訓練進行投資，並讓高階主管掌握最新情況。

我們的目標是什麼？資安計畫成果

許多資安研究（和計畫）的起點都是聚焦於目前正在做的事情，而不是前進的目標。但是，成功的資安計畫的不只是一套方向指引，更是一段通往目的地的旅程。瞭解我們在旅途中的所處位置，有助於以正確的角度看待其他所有事物。

我們從一項公認的艱鉅任務開始：找出資安主管希望實現的一組多樣化計畫層級目標和相關成果。這些成果可以說是理想中的「資安目標」，雖然我們深知這個理想永遠不會實現。每個資安主管和計畫都不相同，因此我們確信您會根據自己的使用案例，對我們提議的清單加入各種內容和進行修改。同時，我們希望您認同這是一組合理且相關的策略成果，為展開這項研究奠定了扎實的基礎。

我們請受訪者思考並評估其組織在表 1 中每項成果的表現，以「艱難」到「成功」的程度進行評等。我們發現，主觀和抽象的概念（例如「滿足業務需求」）可能很難理解和加以評等，因此我們為受訪者提供了每項成果的例證，指引他們進行評等（請參閱附錄 B）。

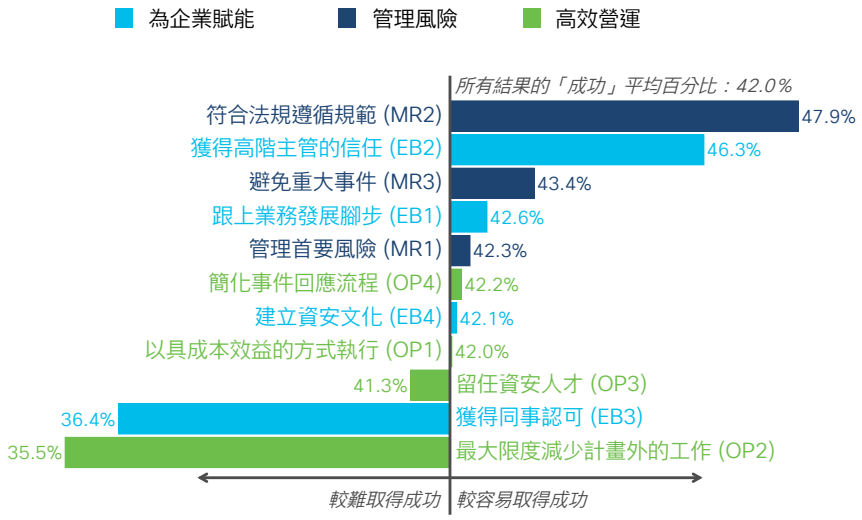
表 1：本研究中使用的資安計畫成果

目標：為企業賦能	目標：管理風險	目標：高效營運
• 跟上業務需求和成長的腳步 (EB1) • 取得領導階層的信心和信任 (EB2) • 獲得同事和其他組織單位的認可 (EB3) • 建立全體員工都接受的資安文化 (EB4)	• 管理組織面臨的頭號網路風險 (MR1) • 符合法規遵循要求 (MR2) • 避免重大資安事件和損失 (MR3)	• 執行具成本效益的資安計畫 (OP1) • 最大限度減少計畫外的工作和浪費精力 (OP2) • 招募和留任優秀的資安人員 (OP3) • 簡化事件偵測和回應流程 (OP4)

說明完背景資訊和須知事項後，讓我們回到眼前的問題：這項研究中代表的 4,800 個組織，在邁向成功資安計畫的旅程中居於什麼位置？圖 1 顯示認為自家資安計畫成功實現清單中各項成果的公司百分比。由此可見，大約 48% 的組織似乎符合法規遵循要求，46% 的組織取得高階主管的信任，以此類推，最後只有 36% 的組織表示其計畫正最大限度減少計畫外的工作。

計畫層級的整體成功率為 42%，我們不禁注意到，這恰好也是生命、宇宙及萬事萬物的終極答案。這是巧合嗎？我們不這麼認為，正因如此，我們以 42% 為軸心來呈現成功率高於和低於此百分比的成果。這個格式有助於受訪者之間達成共識，同意哪些成果較容易實現（靠近頂端者），哪些則較難達成（靠近底部者）。

圖 1：認為自家公司成功實現各項資安成果的受訪者百分比



資料來源：思科 2021 年資安成果研究

「維持法規遵循」和「最大限度減少計畫外工作」分別位於此圖表的兩極。對於許多將所謂的「勾選方框式法規遵循」視為低效率資安計畫象徵的資安專家來說，這並不會令人感到震驚。且這暗示著追求此處顯示的這類目標時，所存在的固有優劣權衡。之後我們找出計畫成功因素時，將會回頭討論優劣權衡的概念。

套上分類後為圖 1 增加了另一個有趣的維度。顯然受訪者傾向認為屬於「管理風險」目標的成果難度較低，而「有效營運」下的成果則較為困難。與「為企業賦能」相關的成果則涵蓋所有難度。

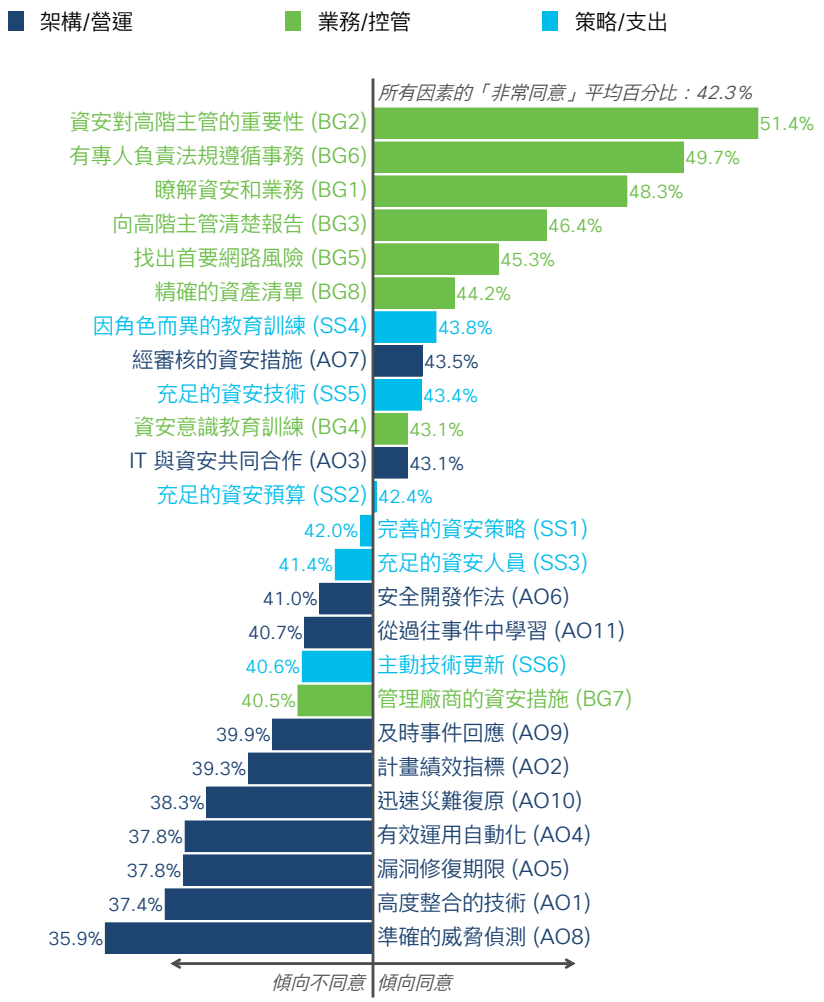
負責領導網路安全計畫的所有人都知道，要妥善管理網路風險並以最低的成本辦到絕非易事。如果可以選擇，大多數組織都會採取躲避風險的途徑，寧願增加支出，但求最大限度降低風險。

我們付出哪些努力？資安措施

現在我們來檢視組織為了實現上一節中討論的目標做出哪些努力。為此，我們向受訪者詢問了其組織的 25 種資安措施。這些措施是從 NIST 網路安全架構 (CSF) 等幾項標準中汲取而出，並區分為業務與控管、策略與支出、架構與營運幾個類別。與成果相同，這些措施的用意是代表而不是詳盡無遺。您可以在附錄 C 中找到分屬這些類別的完整措施清單。

圖 2 根據堅信自家組織遵循各個措施宗旨的受訪者所占百分比，對所有措施進行排名。我們認為圖表所描繪出的評等是出於樂觀看法，但是我們不會對此表示懷疑，因為控制措施的採用和網路安全計畫的成熟度並不是本研究的重點。我們對於（認知的）資安措施與上一節中（認知的）成果之間的關係更感興趣。但是我們還沒有準備好探究這層關係。

圖 2：堅信自家公司遵循各項措施的受訪者所占百分比



資料來源：思科 2021 年資安成果研究

我們首先要強調這些資安措施之間的相對差異。這個格式與圖 1 中用於成果的格式相同，並以在所有控制條件間觀察到的平均實作程度為中心 (42.3%)。據受訪者表示，頂端的措施對公司來說更容易實作，而底部的似乎較為困難。您可以挑出感興趣的特定措施，而我們的解說限於一些高層級的觀察。

我們再次發現，形成鮮明對比的兩極透露出的資安計畫多樣化性質令人想一探究竟。資安專業人員過去不得不為了取得高階主管的關注和認可而奮鬥，但是受訪者表示，我們在這方面已經走了很長一段路。另一方面，業界一直以來努力精益求精的一些基礎能力（例如威脅偵測和漏洞修復），對許多組織來說仍是一大挑戰。這提醒了我們，「回歸基礎」並不像聽起來那麼簡單。

從更廣泛的角度來看圖 2，我們在頂端看到了業務與控管因素的一般模式，在中間看到了策略，底部則可看到架構與營運。比起表面上可看出的「控管很容易，技術很困難」，其實這個模式所代表的含義更為深厚，它可能反映了這些類別之間的相依性，也就是說，沒有適當的控管與策略，就無法妥善完成工作。但是還有一個現實情況是，大多數資安事件的根源都是架構或營運問題。要持續把所有事情都做好相當困難。

想尋找一些速效方案嗎？

我們進行了其他分析，比較圖 2 中所描繪措施的相對難度，以及這些措施與圖 1 所列成果的相關性。我們的目標是找出不會太難實作，但可對資安計畫成功帶來巨大貢獻的措施。請參閱我們的 #SecurityOutcomes 部落格系列，深入瞭解這些速效方案。

我們如何達成目標？找出成功因素

我們已經釐清了我們的資安計畫目標，以及我們目前所做的努力。現在是時候找出實現這些成果的方法。我們的核心問題很簡單：什麼因素有助於資安計畫成功？

由於資安計畫是複雜且相互依賴的系統，因此我們分析了所有措施和成果以找出它們之間的關係。針對每種措施與成果組合，我們計算出與更高度遵循各項資安措施相關的成果實現機率變化。這種方法讓我們能針對以下這類問題，給出有統計資料為依據的答案：

- 是否有證據可證明更好的資安措施與更好的成果相關聯？
- 哪些措施對成功的資安成果貢獻最大？
- 實現每個特定成果的最有效措施是什麼？
- 如果進行 *y*，實現 *x* 的可能性會提高多少？

有些人可能認為這些簡單問題的答案很簡單。但是真的是這樣嗎？資安產業使用許多最佳作法當作其整體策略的一部分。但是我們不盡然會衡量這些措施的成效，並找出這些措施與期望成果的關聯。

不完全如此，您如何找出措施與成果的關聯？

統計資料！看到這句話很多人可能會睡著（或反復作惡夢），但答案就是嚴謹縝密的統計資料。尤其我們利用多變量線性模型來瞭解每種措施對每項成果的影響。也就是說，我們建立了一套邏輯迴歸，其中每個成果變項都是依變項，而所有因素都是自變項。這使我們能測試因素何時會在統計上產生顯著差異，以及何時可能偶然看到相關性。

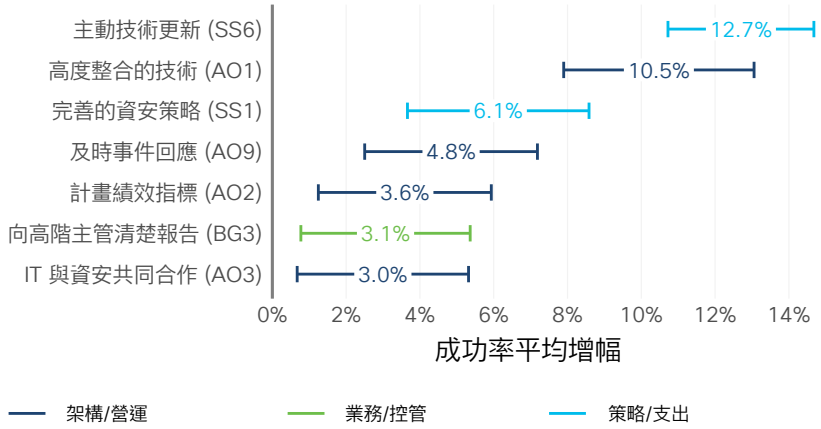
為了各位書呆子，我們也進行更深入的計算。您可能還記得，邏輯迴歸中因素的迴歸係數並不能直接轉換為機率變化。但是只要用一個便利的小技巧「平均邊際效應」，就可以算出組織能從每個因素獲得多少效益。眾所皆知的名言「相關不代表因果」仍然適用，但是這種方法可有效凸顯出可能有用的措施與成果關聯供我們思考。

整體計畫成功

首先我們將「整體計畫成功」成果獨立出來，因為它涵蓋了所有其他方面。圖 3 根據受訪者聲稱整體取得高度成功的資安計畫與各因素之間的相關性高低，從上至下列出因素。長條和值表示與每種措施相關的預期整體計畫成功機率增幅。由於統計變異，這裡以機率範圍表示增幅。中間值表示計畫成功可能性的平均（及最有可能的）增幅。

根據這些結果可知，理想情況下，想要最大限度提高資安計畫整體成功率的組織，應該從現代化高度整合的技術堆疊著手。有受訪者表示自家公司的技術更新策略著重使用同類最佳的 IT 和資安技術進行主動更新，其中大多數指稱的計畫成功可能性高出 11% 到 15%（平均 12.7%）。相反地，表示自家公司很少升級基礎架構，或只會在出現問題時才升級的受訪者，呈現的成功率則明顯較低。確保技術彼此合作無間以形成整合式防禦機制，可以使整體成功率平均提高約 11%。[1]

圖 3：與整體資安計畫成功最密切相關的措施



資料來源：思科 2021 年資安成果研究

圖 3 以範圍顯示整體計畫成功機率的變化。解讀方式如下：「主動技術更新策略使得回報資安計畫成功的機會提高大約 11% 至 15%，而平均為 12.7%。」每個這樣的圖表都可以用相同的方式解讀。

我們充分瞭解，這個發現看似對提供符合此描述之技術的公司有偏袒嫌疑，因此我們藉此機會重申，本調查是由專業調查公司 (YouGov) 進行，參與者不知道思科參與其中，且分析資料是交由獨立研究公司 (Cyentia Institute) 負責。我們很高興這些結果驗證了思科的策略和解決方案產品組合，但是我們並未做出任何行為來導向此結果。

[1]請務必注意，與措施和成果組合相關的機率不能相加。因此，不能說主動技術更新以及高度整合技術的成功率加起來會提高 23.2% (12.7% + 10.5%)。

我們瞭解對某些組織而言，主動技術更新策略有時絕非易事。有些組織沒有預算，有些則出於各種正當理由需要將其資源和精力集中在其他面向。好消息是，這些結果並不表示這些組織注定會失敗，只意味著他們需要找出適合其情況的其他成功因素。這正是我們希望這個分析能幫助他們做的事情。

畢竟，擁有足夠的資安預算只是我們測試的因素之一，它與整體計畫的成功並沒有顯著相關性，因此優良的資安並非只取決於金錢。繼續看圖 3 中前兩個因素後面的幾項，很高興看到可衡量的效益與具備完善資安策略密切關聯。這是所有類型和規模的組織都可以發展的因素，其他一切都源自於此。

人們常說，卓越的領導者之所以卓越，在於他們應對危機的方式。從圖 3 可以看出，這也是卓越資安計畫的重要組成要素。及時的事件回應需要完善的準備、智慧的工具和經實測的流程。如果您需要改善這些功能的正當理由，這個圖表應有所幫助。

接下來的兩個成功因素不分軒輊。使用績效指標來推動營運，然後將這些資訊清楚向領導階層報告，對計畫的成功有重大貢獻。這是 OODA 循環理論的核心，而且相當有效。

接下來帶到最後一個成功因素：IT、開發和資安團隊共同合作。這裡指的並不是以「想像」為背景進行某種公司工作外聚會信賴練習活動。這個因素點出了一個事實，那就是如果不能妥善進行 IT 和開發工作，資安就不能順利進行（反之亦然）。如果真是這樣，那麼進行溝通和協作來讓每個人的工作都更加成功，豈不是意義非凡？圖 3 顯示在整個組織單位之間建立穩固的同盟關係是有好處的。

最後要注意的一件事是，整體上最重要的成功因素涵蓋了所有類別：營運、控管和策略。這表示優秀的資安計畫不能單獨建立在優秀的控管、優秀的策略或優秀的營運之上。一個成功的計畫需要全部這些要素，且做的越多，成效就會越好。接下來幾節中，我們將分別針對 11 個計畫層級成果探討成功因素，屆時這個議題將會繼續浮現出來。

持續升級技術與計畫成功之間似乎有很強的相關性，這對於使用家具般技術（意思是會用到壞掉為止）的企業來說可能是個壞消息。這說明著「越新越好」不只是從矽谷誕生的一種生活方式選項。

請參閱思科資安底線報告，深入瞭解相關內容。

NIST CSF 功能

除了遵循特定的措施之外，我們還詢問了受訪者其資安計畫在投資、資源和人力方面最優先考慮哪些事項。為此，我們使用了 NIST 網路安全架構 (CSF) 中定義的高層級資安功能。

CSF 中的保護功能並不是在每個成果中都敬陪末座，它對促進資安計畫整體成功的貢獻排名倒數第二（識別功能排名第一）。這無疑是違背直覺的情況，但是我們並不認為這代表保護功能不重要。相反地，這表示最好的計畫會投資面面俱到的防禦措施，以識別、保護、偵測、回應網路威脅以及從中復原。長期以來這個領域一向以保護功能為重，這說明了單獨依賴保護功能並不是最有效的策略。

請參閱 #SecurityOutcomes 部落格系列，瞭解全部五個 NIST CSF 功能對計畫成果的貢獻情況。

達到資安目標

擁有一個整體上成功的資安計畫是值得努力的目標，但是追求特定的成果也是完全合理的作法（且通常是必要的）。也許您已看過表 1 的成果清單並思考：「我想知道哪些因素可以幫助我們實現 [x 成果]？」如果是這樣，本節內容相當適合您。

成果分為以下三類：為企業賦能、管理風險和有效營運。在這三大標題下，我們提供了幾種資安措施，這些措施與受訪者斷言他們的計畫成功實現各項目標的相關性最高。若您想看到任何特定成果的完整成功因素清單，請稍安勿躁，稍後我們會在本報告中為您提供一些特別的資訊。

主動技術更新 (SS6)、高度整合的技術 (AO1)、及時事件回應 (AO9) 和迅速災難復原 (AO10) 這四項措施幾乎對每個成果都有重大貢獻。因此，這幾項在本節中的所有圖表上出現的頻率相當高。為了使深入分析呈現多樣化，除了上述四項外，我們通常還會將觀察結果聚焦於每個成果排名前五的措施上。請不要以為我們是在淡化它們的重要性。在本研究中，將以強而有力的證據證明它們是最重要的成功因素。

「資安買家通常擁有多個廠商提供的數十種不同工具，且通常須耗費巨大心力將它們集合在一起才能讓它們共同合作。這產生了複雜性、成本和開銷。」

思科資安長 Steve Martino
閱讀更多內容

為企業賦能

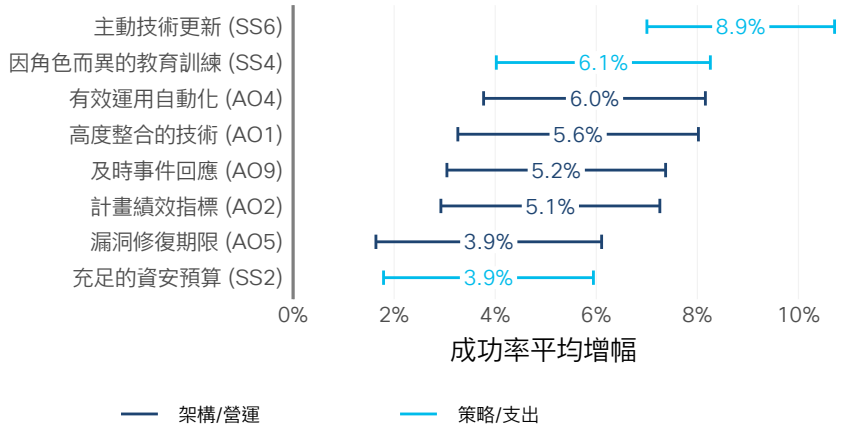
就像標題所暗示，本節說明的成果著眼於資安計畫支援和促進業務活動的任務。基於安全考量，這個類別認定資安不存在，完全只考量業務面。讓我們看看是否能找到如何達成此目標的提示。

跟上業務需求和成長的腳步

經常升級為最佳可用技術，並將它們整合在一起以順利共同合作，在圖 4 中再度名列前茅。由於我們已經討論過很多措施，這裡就簡單加上註解：這個發現對我們來說很合理。整個「跟上業務發展腳步」的概念意味著資安必須隨著產生營收的活動一起前進、變化和調整。企圖讓老狗學會新把戲的人都知道，這幾乎是不可能的任務。過時、分散的基礎架構會阻礙業務發展，毫無轉圜的餘地。

因角色而異的資安教育訓練與為企業賦能之間的緊密連結，對我們來說是一大福音。實際上，我們把它化為一句箴言：「嫻熟的能手造就靈活的計畫。」有人可能會爭辯說，這是現代資安計畫中最基本的議題之一。有效的教育訓練必須具備高品質、符合企業文化並針對特定對象量身設計。

圖 4：跟上業務發展腳步的首要資安成功因素 (EB1)



資料來源：思科 2021 年資安成果研究

圖 4 中包含自動化因素對我們來說也很有道理。自動化可消除瓶頸並提高人員、流程和技術的靈活性，進而協助資安計畫跟上業務發展的腳步。圖 4 強調了技術現代化、自動化和整合的重要性，開始明顯呈現出 DevSecOps 特色。

一開始看到將事件回應 (IR) 列為首要企業賦能要素可能會覺得奇怪。但是 IR 的作用不僅僅是滅火和清理混亂，最終目標是處理意外事件，並將對企業造成的影響降到最低。從這個角度來看，它在圖 4 中榜上有名其來有自。

表面上看來，指標導向的資安計畫是用來因應不斷變化的情況調整路線。我們懷疑這就是績效指標之所以在幫助資安跟上業務發展腳步方面榜上有名的原因。如果您不確定自己的現況或目標為何，那就沒有理由快速採取行動。

足夠的預算能幫助資安計畫跟上業務發展腳步，這不足為奇。這一點值得牢記，尤其是當您的商業模式會快速變動和急速發展時，在資安方面投入適當的投資很有希望助長這股推動力。

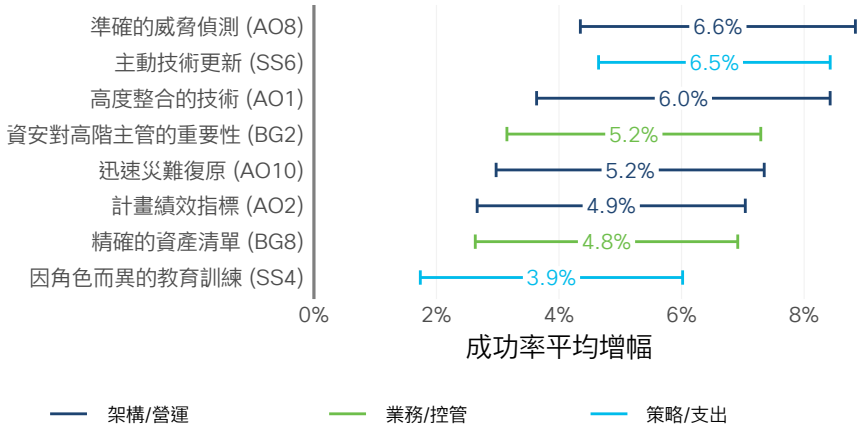
請前往這裡瞭解思科自家資安長如何藉由資安幫助推動業務發展。

取得領導階層的信心和信任

現代整合式技術可讓您再添一分。我們不禁想起當 SOC 高階主管來訪時的情況（我們突然得緊急清理辦公桌並擺出忙碌樣），但至少有一些證據可以證明「科技導覽之旅」式的冗長說明確實奏效！

許多高階主管將網路安全視為一種保險，防止公司因重大漏洞或業務中斷而登上新聞頭條。這些擔憂可能就是在與取得高階主管信任相關的因素中，準確偵測威脅和迅速災難復原之所以名列前茅的原因。若能展現出強勁的洞悉威脅和復原能力，便能將「放心交給我們就對了」的想法傳達給高階主管。

圖 5：取得高階主管信任 (EB2) 的首要資安成功因素



資料來源：思科 2021 年資安成果研究

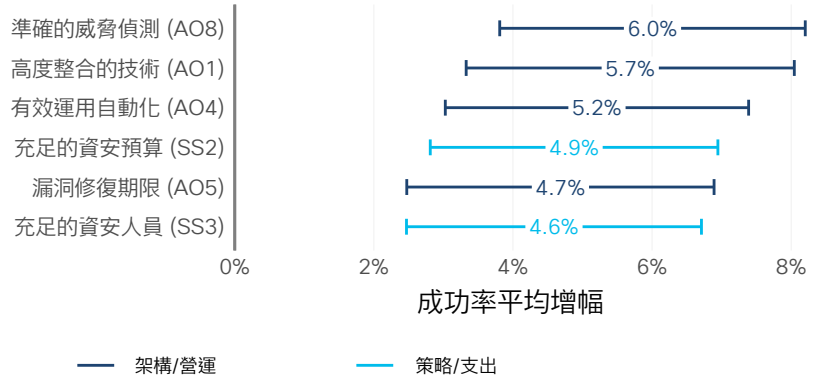
擁有精確的資產清單、計畫績效指標以及因角色而異的教育訓練似乎仍是緩解高階主管擔憂的議題。展現資安團隊知道最重要的方面為何、具備捍衛這些方面的技能，並追蹤可靠的指標來為「放心交給我們就對了」背書，對於贏得高層信任有很大的幫助。

「資安對高階主管來說很重要」以及「取得高階主管的信任」這兩句話似乎語意重複。這也許是「相關不代表因果」格言的一個很好的例子。如果資安對他們來說很重要，那麼他們很可能會充分支持計畫，並為計畫的成功進行投資。

獲得同事和其他組織單位的認可

我們之前已經看到並討論過圖 6 中的幾個首要成功因素。但是看到優良的資安作業（即偵測、整合和自動化）有助於贏得其他團隊/部門的尊重和參與，仍然很有幫助。甚至可以說這些資安作業與其他團隊息息相關。這些措施可減少摩擦、增加彈性，且通常可幫助資安計畫擺脫「只會說不行的部門」的烙印。

圖 6：獲得同事認可 (EB3) 的首要資安成功因素



資料來源：思科 2021 年資安成果研究

說到烙印，與資安相關的支出達到 IT 和開發組織預算的情況並不罕見（有時比他們希望的還困難）。這可能就是為資安計畫本身分配充足的預算，有助於獲得同事支持的原因。同樣的概念可能也是擁有足夠資安人員因素榜上有名的理由。「哦，我不需要為它付錢，也不必讓我的下屬離開他們的工作崗位嗎？那沒問題，我們會參加，謝謝！」

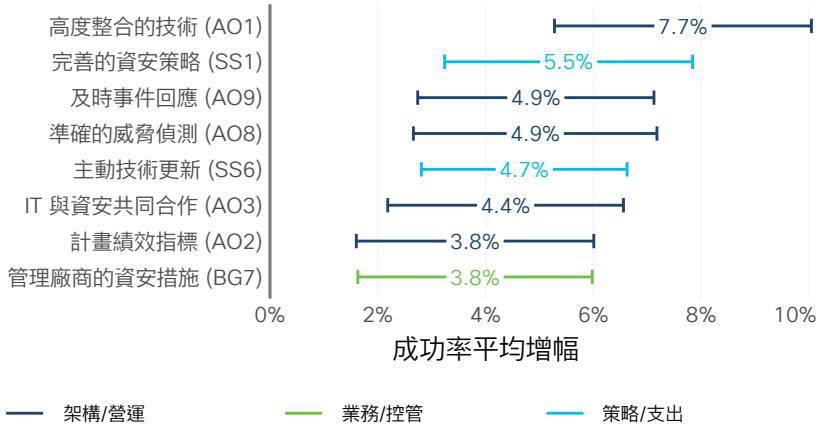
漏洞修復是上一段中所說明變動情況的具體範例。若沒有 IT 和資安團隊之間的協作，幾乎無法做到這件事。資安團隊通常負責發現錯誤，而 IT 團隊負責排除錯誤。這不難理解，協調不同部門的同事各自負責的工作，可以更有效進行合作。

建立全體員工都接受的資安文化

如何建立員工真正接受而不是想迴避的資安文化？圖 7 將以下項目列在清單的頂端：為員工提供可以滿足其需求的優良技術、明確的目標，以及出現問題時及時修正（或一開始就防止問題出現）。很難對這幾點提出質疑。

文化並非只代表教育訓練，尤其是人人討厭的那種年度線上宣導課程。當然，這不是指「每當你違反資安策略，我們都會讓你再接受一次相同教育訓練作為懲罰」。策略與文化的相關性值得特別提出來探討。這是「為企業賦能」類別中唯一的一項成果，針對這項成果，擁有完善的資安策略可顯著提高成功的可能性。這也許看似有點奇怪，但是考慮到有許多受挫的員工曾提出類似「為什麼我們必須經歷這一切？」的問題來回應新的資安策略，就不無道理。好的策略可以讓所有人達成共識，進而減輕挫敗感。

圖 7：建立強大資安文化 (EB4) 的首要成功因素



資料來源：思科 2021 年資安成果研究

上文中提到，IT、開發和資安團隊共同合作有助於整體計畫獲得成功，而這同時對文化有益也不足為奇。不能將資安強加於組織，資安必須內建在基礎架構和組織本身的結構中，才能真正發揮作用。技術團隊之間的良好協作對於實現這個目標來說至關重要。

圖 7 中包含「管理廠商的資安措施」因素讓我們停下來思考。不過這個問題的全文有助於洞悉其中道理：「我有信心我組織的價值/供應鏈中廠商的資安措施符合我們的標準，或是我們對此進行了相應的管理。」公司若將資安延伸到整個供應鏈中，也會提高讓資安滲透到其文化中的可能性，我們認為這個推斷並不會離題太遠。

cisco SECURE

資安案例

思科在資安案例 Podcast 中採訪了 Elevate Security 的共同創辦人 Masha Sedova。

聆聽這集具啟發性的內容，瞭解如何運用資料和分析來促使公司的網路安全作法產生文化和行為變化，進而實現以人為本的資安。

請造訪 cisco.com/go/securitystories。

管理風險

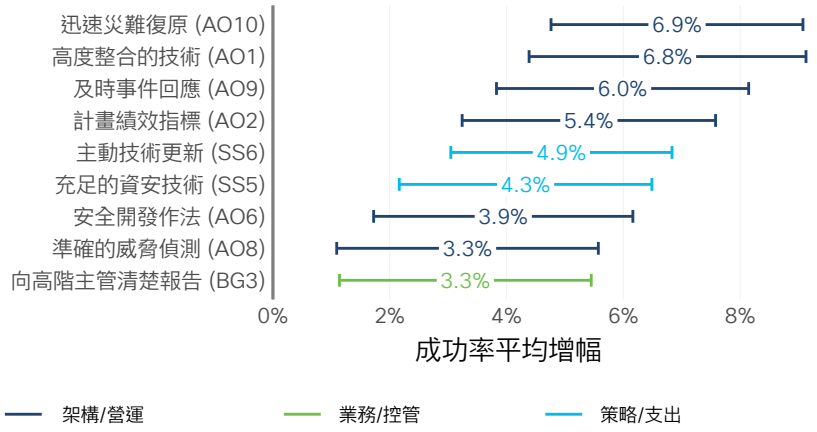
被問及資安計畫的主要職責時，大多數人都認為是風險管理。當然，風險具有許多面向，因此我們選擇檢視三個成果，每個成果都針對組織管理風險的方式提供不同視角。

管理組織所面臨的頭號網路風險

過分鑽研微小細節可能很危險，例如圖 8 中迅速災難復原因素的排名，高於在多團隊合作方面排名第一的更新和整合技術因素。但是有可能是資料在這裡發現什麼重要的事而想提醒我們，管理風險並不只是阻止壞事發生而已，在無法避免的情況下將影響降至最低也同樣重要，而這就是迅速災難復原的宗旨。

這是擁有充足資安技術和主動更新有所貢獻的兩個成果之一。我們認為這是因為資料所傳達的重點在於，處於最佳狀態的最佳工具可為管理重大風險帶來最佳機會。

圖 8：管理首要風險 (MR1) 的首要資安成功因素



資料來源：思科 2021 年資安成果研究

身為資安指標的長期提倡者，我們很高興看到制定出資料導向的計畫可以改善風險管理的效果。「如果你不能衡量它，就不能管理它」這句名言常被過度使用，但這不無道理。這句話在許多領域都適用，包括網路安全在內。

我們真正感到驚訝的是，這是唯一出現與應用程式安全開發方法密切相關的成果。但這相當合理，因為許多網路風險都存在著固有的軟體缺陷。

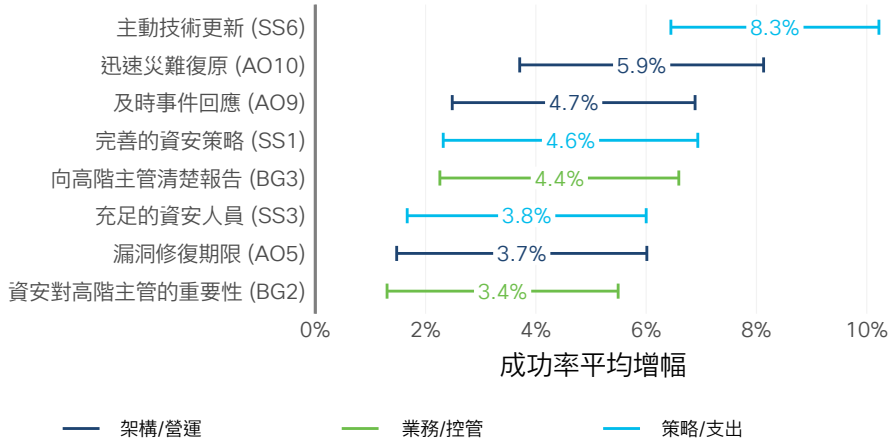
這也是向高階主管清楚報告的重要性第一次榜上有名，因此似乎值得一提。只向高階主管報告資安計畫的活動和有效性，就能有效減少面臨重大風險的機會，這一點著實令人質疑。雖然如此，這個作法確實意味著一定程度的監督和問責制，而這可能成為資安計畫言出必行的強制方法。當然，我們可能會看到相當於絕地控心術的說法：「這是您期望的保證；我們可以著手展開業務。」

符合法規遵循要求

主動技術更新已成為這些圖表中的永久固定項目，但它在符合法規遵循規範方面的領先地位有點令人費解。現代化同類最佳解決方案會在一堆方框中打勾，還是建立一流的稽核軌跡？我們不能完全確定，但這絕對是需注意的事情。

圖 9 中的幾項措施可視為證明資安計畫面面俱到的必要證據：制定完善的策略、及時修復漏洞、對事件快速做出回應以及迅速從重大事件中復原。確實做到這幾件事對於維持法規遵循有很大的幫助。

圖 9：符合法規遵循規範 (MR2) 的首要資安成功因素



資料來源：思科 2021 年資安成果研究

高階主管們可敏銳地意識到法律和法規風險，這就是在董事會層級資安報告中，這個議題之所以經常居於重要核心位置的原因。關於此表中包含的「向高階主管清楚報告」，資安主管若能清楚向高階主管傳達資安計畫的狀態和有效性，也許也可以對監管機關這麼做。或者，也許這些高階主管更能妥善與監管機關溝通，進而協助遵循法規。

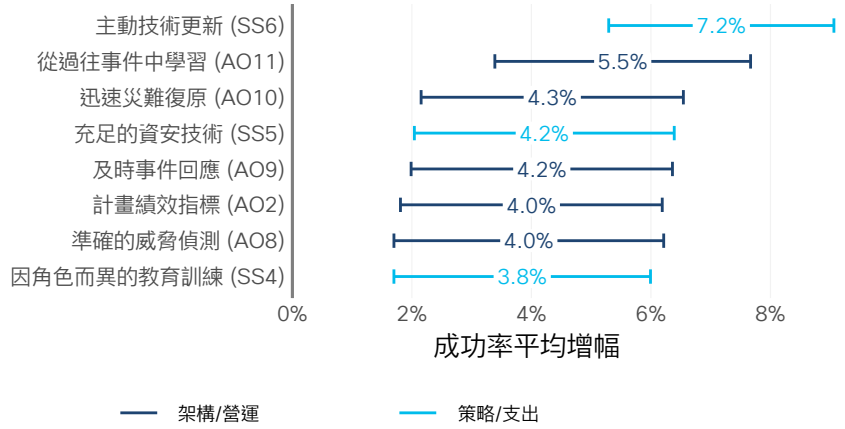
討論與成果無關的措施並不是我們的慣例，但這個措施卻不容我們忽視。我們分析的其中一個因素是聘請專職負責法規遵循事務的員工。但這並沒有提高任何成果的成功機率，包括這個成果在內。當然，單純聘請一個擁有法規遵循職稱的員工並不會讓監管機關感到滿意...但聊勝於無。如果這個作法有助於實現任何目標，那非這個目標莫屬。

避免重大資安事件和損失

對我們來說，圖 10 明確展現出「攻擊者不斷改革創新，我們也必須這麼做」的訊息。避免重大網路安全事件和損失的能力，似乎高度仰賴維護現代化高效 IT 和資安基礎架構，而這套基礎架構需有敏捷的回應和復原功能作為後盾。

主動更新策略的附帶好處之一是可以定期照料技術堆疊，且都會留下記錄並保持最新狀態。在過往的重大入侵事件中，因為組織忽略、沒有確實追蹤或沒有嚴密維護系統，而導致攻擊者得以在其環境中站穩立足點的案例層出不窮。停滯不前的基礎架構會使不肖人士能輕而易舉地趁虛而入並逗留徘徊。

圖 10：避免重大事件 (MR3) 的首要資安成功因素



資料來源：思科 2021 年資安成果研究

談到過往的入侵事件記錄，圖 10 指出我們不應只研究大型公共事件以尋求如何避免事件的線索，還應該研究我們自己遭遇的事件（以及未遂事件）。不斷學習的資安文化若能對重大事件進行事後回顧並記取這些教訓，便能更妥善應對未來的事件。

除了幫助管理首要網路風險外，績效指標還可提高資安計畫避開漏洞攻擊的機會。若結合準確的威脅偵測，這個組合便可提供全面性的情勢感知功能。知曉敵方的能力和活動以及您自己的防禦能力和活動，有助於平衡戰場的不對稱局勢。

最後重要的一點是，因角色而異的教育訓練可提升計畫避免重大事件和損失的能力。從正確的角度來看，資料顯示，在降低入侵風險方面，教育訓練和威脅偵測的成效幾乎不相上下。既然如此，其中哪一項在貴組織中獲得更多的資金？教育訓練是談到如何獲得成功時常被提出的必要事項之一，但是當預算緊縮時，教育訓練通常卻是首先被剔除的其中一件事。如果您需要證據來說服組織領導者，對員工進行投資符合他們的最大利益，請務必使用這個圖表。

聚焦重大事件和損失

發生重大資安事件或資料遺失並不代表資安計畫失敗（沒有發生這些事也不能證明獲得成功），但這無疑是組織領導階層首重的指標。某些受訪者表示他們的公司在避免事件發生方面遭遇困境，我們請他們針對遭遇哪些困難提供更多詳細資訊。最常接到報告的資安事件類型是資料洩露、勒索軟體和服務中斷。

我們也很有興趣瞭解這些事件造成的影響。營運影響最為常見，這其來有自，因為重大事件會迫使人員（和系統）為了回應事件而中止正常業務活動。接下來是管制行動，以及品牌形象損害、業務關係受損、收入損失和法律行動。請參閱 #SecurityOutcomes部落格系列，取得有關資安事件和損失的更多詳細資訊。

高效營運

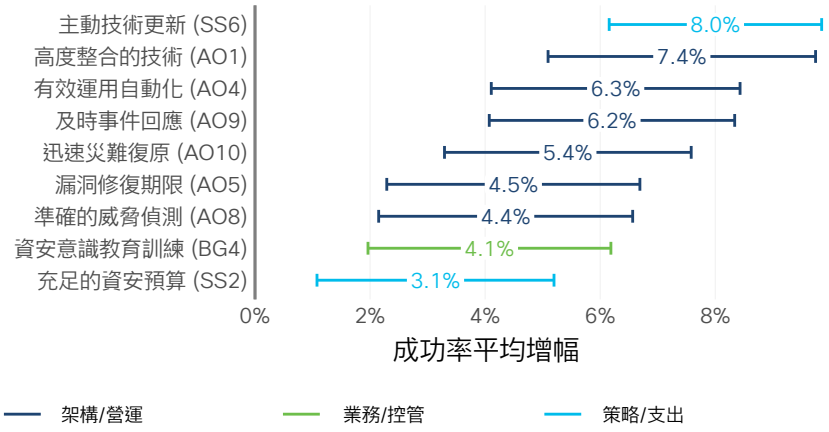
除了為企業賦能和管理風險外，高效營運的能力通常可讓優秀的資安計畫從不錯的資安計畫間脫穎而出。我們研究的最後一組成果是關於成本效益、執行策略、人才管理和事件回應流程。這些都很重要，對不對？現在來看看什麼因素可以為您的計畫帶來優勢。

執行具成本效益的資安計畫

採用主動技術更新策略有助於讓資安計畫保持具有成本效益，這個說法乍看之下似乎違背直覺。但是正如我們之前所說，這項措施不只是為資安撒下大把鈔票而已，這是一種策略，可確保您的團隊擁有最佳工具，幫助他們盡其所能。如果您的資安工具沒有保持最新狀態，則圖 11 中的下兩項措施（整合和自動化）將難以實現。最佳工具更加有效且更易於管理，因此從長遠角度來看，其成本較低。

圖 11 中接下來的兩項措施我們已經看過很多次。如果您曾經歷過重大資安事件，您就會知道在回應和復原過程中會耗費大量的時間和金錢。若能確保這些功能已蓄勢待發，隨時準備好在需要時啟動，便能同時控制住事件和相關成本。

圖 11：執行具成本效益的資安計畫 (OP1) 的首要成功因素



資料來源：思科 2021 年資安成果研究

資安方面的工作中，幾乎沒有工作的繁瑣程度比得過管理漏洞和分類無數誤判情形。在我們檢視過實作情況最不完善的措施中，這兩個功能在圖 2 中敬陪末座實在其來有自。這些工作相當艱難且需消耗大量資源。值得慶幸的是，圖 11 顯示修復期限和偵測準確性可提高效率，為疲憊不堪的人們帶來了希望。

關於這項成果，有一個適用於資安預算的「金髮女孩原則」區域。如果預算太少，無論再怎麼努力嘗試，仍無法完成所有工作。如果預算太多，浪費傾向便會悄然而生。但是當預算恰到好處時，計畫的能力可以剛好滿足任務的需求，並以最高的效率運作。

整體而言，若採用以高效營運為後盾且經過精心設計的架構，似乎最容易實現具成本效益的資安計畫。

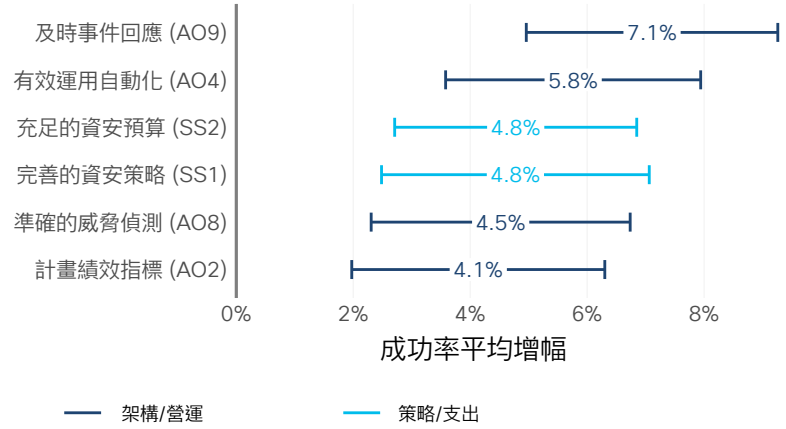
最大限度減少計畫外工作和浪費精力

這項成果類似於執行具成本效益的計畫，但更著重於執行策略而不出現重大挫折或偏差。這樣看來，最初制定優異的策略可以讓排名前五的措施與這個目標產生關聯，就有其道理。擁有足以實作該策略的預算也大有裨益。

圖表中的其他因素（及時回應、有效自動化和準確威脅偵測）為策略的日常執行提供了先行者優勢。不良的威脅偵測和回應能力尤其容易導致掉入未知風險的無底洞中。如前所述，不連貫的事件回應流程和追逐無止盡的誤判情形，會造成浪費時間、員工精疲力盡以及其他許多削弱價值的影響。資安自動化和協調流程的主要目的是消除營運作業的死角和瓶頸。若能驗證這個目的有確實達到將有所幫助。

績效指標也是實現此目標的重要因素，可以對資安計畫的方向提出需要深思的問題，並提供可判斷何時偏離方向的工具。

圖 12：最大限度減少浪費精力 (OP2) 的首要資安成功因素



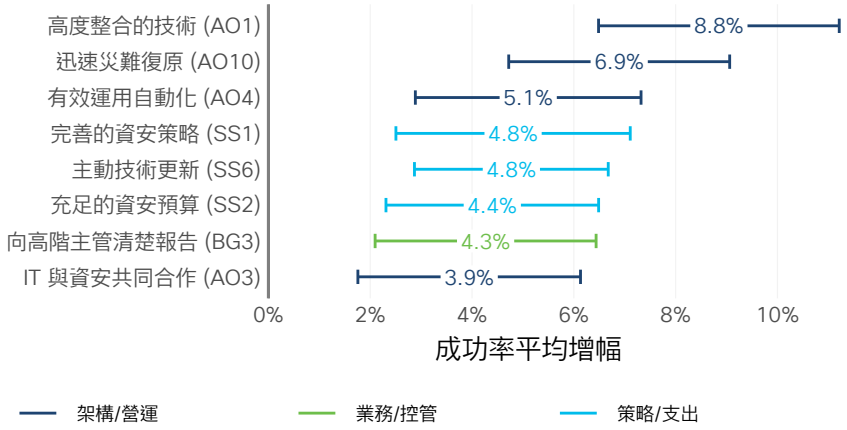
資料來源：思科 2021 年資安成果研究

招募和留任優秀的資安人員

業內對於招募和留任資安人員的難處有很多討論。以下是可能有所幫助的準則：準備聘請頂尖人才的預算、制定對他們合理的策略、讓他們與優秀的同事共事，並為他們提供成功所需的工具。您聘用的人才及其背景、技能與意見的多樣性，對於建立讓員工有歸屬感、感覺受到尊重及準備好發展其職涯的文化至關重要。

坦白說，圖 13 中列出的措施相當偏技術性，這導致我們重新審視了一番。我們希望看到稍微偏軟性的成功因素清單。但就如往常一樣，資料促使我們重新考慮了我們的預想前提。在此之後，我們承認架構和營運在吸引和留任頂尖資安人才方面發揮著重要的作用，這的確很有道理。絕對沒有人喜歡浪費時間和才能來克服不良的技術。

圖 13：留任資安人才 (OP3) 的首要成功因素



資料來源：思科 2021 年資安成果研究

關於浪費時間和人才，資安自動化值得在此提出來討論。有些人認為自動化的目的是取代人力，但是知道如何運用此技術的人，實際上理解其用意是減輕人力負擔，而不是取代人力。讓員工擺脫繁瑣的工作，可以使他們騰出時間精力來進行更具挑戰性、更有樂趣和更有價值的工作。而從這些結果可看出，資安專業人員對此表示讚賞。

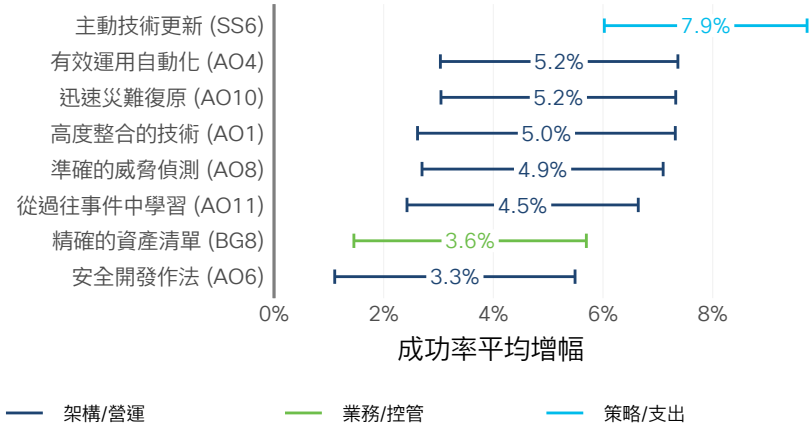
IT 和資安團隊共同合作是另一個值得一提的因素。建立協作文化並非易事，但出於許多原因，這樣做絕對值得。圖 13 將人才留任加到這堆原因中。

進入網路安全領域的途徑不只一種。網路安全多樣性：職業可能性的馬賽克這本電子書中，我們採訪了著名的網路安全專業人員，瞭解他們起步的過程，並請他們與年輕時的自己分享一些秘訣。

簡化事件偵測和回應流程

這個最終成果比其他許多成果更具策略性，且至少如標題所言，與「及時事件回應」措施重疊。然而，檢閱附錄 B 中針對此目標提供的說明和例證，可以發現簡化事件回應流程既可以當成一個目的，也可以作為一種手段。而威脅偵測以及歸入本節所介紹成果因素的其他核心 SecOps 措施，重要性與事件回應不相上下，令我們不由得想知道如何改善這些功能。

圖 14：簡化事件回應流程 (OP4) 的首要資安成功因素



資料來源：思科 2021 年資安成果研究

答案的一部分與本研究中很常強調的答案相同：有成熟的營運作業為後盾，且經過妥善調整的現代化資安架構。至此，我們已經準備好將它稱為賭注籌碼了。如圖 14 中最後三個因素所示，我們對什麼因素能為一手好牌提高賭注更感興趣。我們之前已經看過一次從過往事件中學習的價值（針對避免重大事件和損失），很高興看到它再次出現在這裡。儘管這顯而易見，您仍會驚訝地發現，有許多事件回應團隊並沒有花時間真正做到這一點。這也只是擁有精確資產清單扮演關鍵成功因素的第二個成果。聽過幾次「我們甚至不知道（遭入侵）的伺服器還運作著」和「我們不確定那個應用程式位於哪裡」的說法後，這種相關性就顯得相當合理。若您不知道資產位於何處、歸誰所有、它們的設定為何，就很難妥善做出回應。

希望合理採用安全開發生命週期時，通常不會想到簡化事件回應流程。但是這種措施意味著可以透過 DevSecOps，讓資安和開發團隊/流程之間更妥善整合。這會進而促使應用程式更加完善和靈活、對攻擊面取得更高的共識，以及對於漏洞以及問題時出現時的應對方式有更多瞭解。

減少 COVID-19 的影響

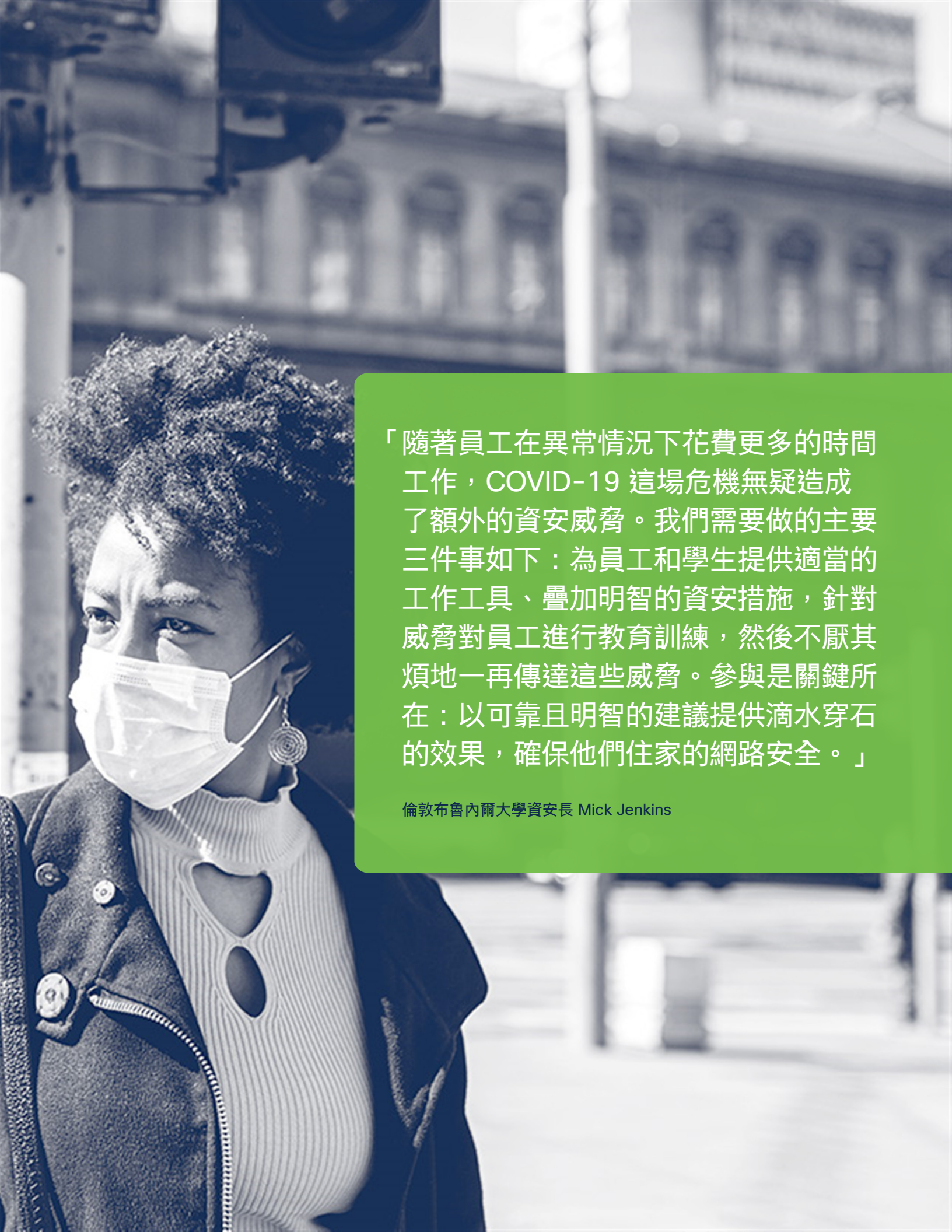
我們向受訪者詢問 COVID-19 疫情對其組織造成哪些影響，這可以視為「有效營運」分組中的另一個成果。在將 COVID-19 對營運和網路風險情勢的影響降到最低方面，最成功的公司具有以下特徵：

1. 他們制定了主動技術更新策略，強調經常升級為同類最佳的 IT 和資安技術。

2. 他們擁有充足的資安人力，並透過角色型教育訓練計畫對員工進行投資。

3. 他們清楚報告資安計畫的活動和有效性，讓高階主管掌握最新情況。

我們解析這些結果後，認為組織遭遇 COVID-19 疫情之類突發事件時保持韌性的能力，很大程度取決於由有能力的人員負責維護的現代化高效能技術堆疊，以及責任心強的組織領導階層。請參閱 #SecurityOutcomes 部落格系列，瞭解我們對於這個重要主題的其他發現。



「隨著員工在異常情況下花費更多的時間工作，COVID-19 這場危機無疑造成了額外的資安威脅。我們需要做的主要三件事如下：為員工和學生提供適當的工作工具、疊加明智的資安措施，針對威脅對員工進行教育訓練，然後不厭其煩地一再傳達這些威脅。參與是關鍵所在：以可靠且明智的建議提供滴水穿石的效果，確保他們住家的網路安全。」

倫敦布魯內爾大學資安長 Mick Jenkins

成功藍圖

在本研究的開頭，我們鼓勵希望搶先看到所有首要成功因素的人先忍住這個念頭，我們回頭會進行說明。我們要在這裡兌現承諾。圖 15 的底部顯示出本報告中討論到的所有資安措施，左側則顯示所有計畫層級的成果。如需措施和成果的完整問題全文，請參見附錄。

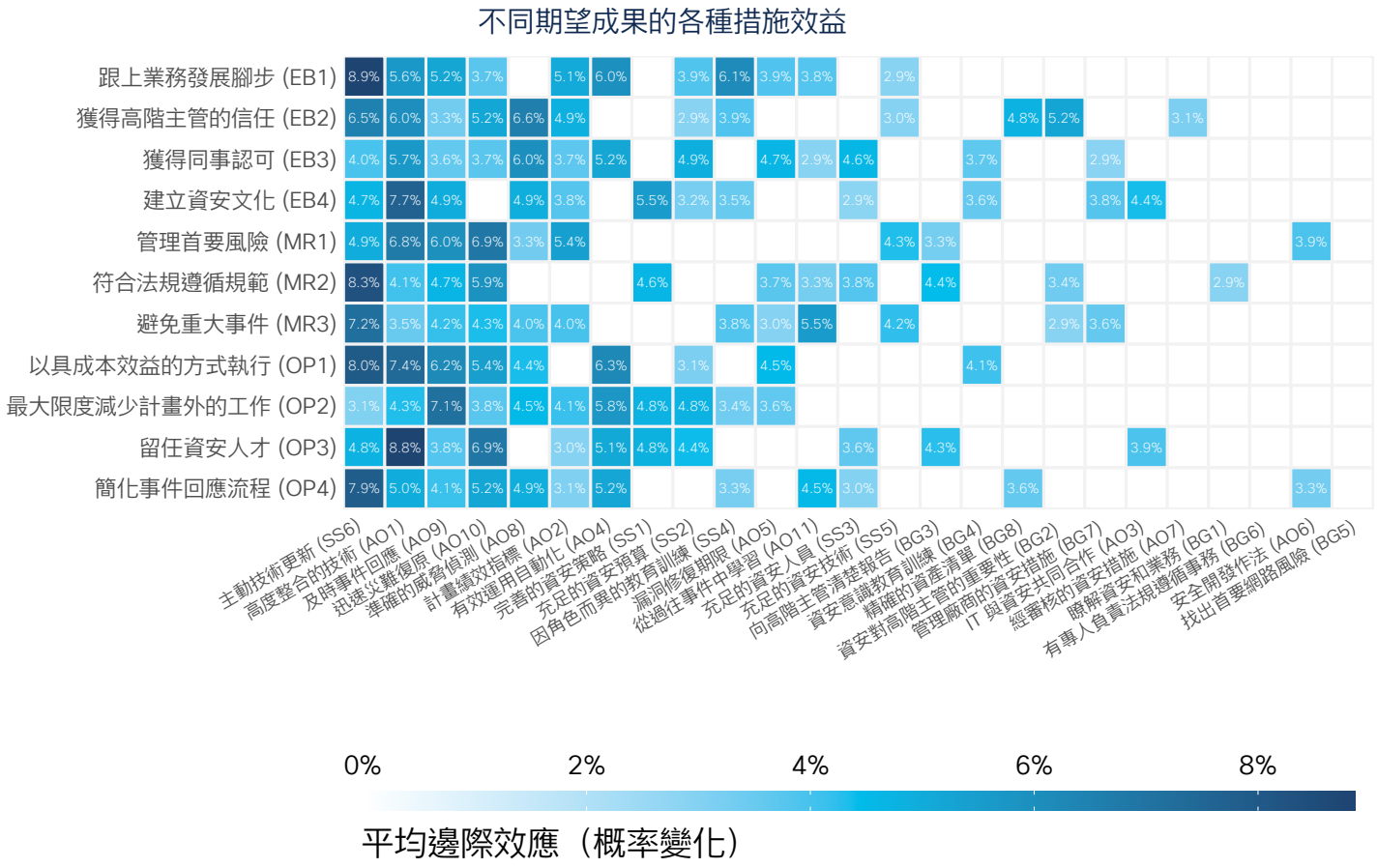
有底色的方塊表示相交的措施和成果之間在統計方面明顯呈現正相關（白色方塊表示沒有相關性）。底色深度表示每個措施與成果組合的成功機率平均增幅。底色下的值對應前文中的圖表所顯示的值。

我們決定不要加入一堆我們提出的建議，而是以展開研究之初的相同方式總結這份報告：讓資料本身說明一切。我們設計出這個圖表，幫助您以視覺化方式瞭解整體情況，並開始建立有證據為依據的藍圖，制定出更成功的資安計畫。這是選擇您專屬資安歷程的根本作法。

以下是規劃歷程的幾項技巧：

- 如果您想找出資料建議可幫助您的計畫實現特定成果的措施，請專注於個別列。
- 如果您想查看與特定措施相關的計畫（成果）潛在效益，請專注於個別列。
- 請注意，某些措施對多項成果有廣泛的影響，而另一些措施則提供了範圍較窄或較具針對性的效益。

圖 15：與各項資安計畫成果相關的所有資安措施



資料來源：思科 2021 年資安成果研究

圖 15 中的空白方塊不一定代表提及的措施對實現成果沒有幫助，而是只意味著，平均而言在所有受訪者間造成的效果從統計面來看並不明顯。依照產業、地區或組織規模對資料進行細分，會讓效果大幅改變。換句話說，您可獲得的效益可能會有所不同。如果您對其中的某些觀點感興趣，可以在 cisco.com/go/SecurityOutcomes 上的區域和垂直產業報告中找到其他深入分析。

感謝您投入寶貴的時間閱讀這份資安成果研究。不勝枚舉的資安產業報告爭相希望獲得您的青睞，我們期望這份報告提供一些以資料為依據且可付諸實行的深入分析，幫助您制定更成功的資安計畫。若您認為我們能透過其他任何方式支援您達成崇高的目標，請告訴我們，並在社交平台上使用 #SecurityOutcomes 加入我們的討論。

關於 Cisco Secure

思科經過長期的努力確立了自己的網路領導者地位，同時持續建立開放且整合的網路安全解決方案產品組合。我們認為，資安解決方案應設計成一支團隊。他們應該互相學習。他們應該以一個協同的單位傾聽並做出回應。如果能做到，資安將變得更具系統化且更有效率。多年來，客戶持續信任我們既是全球最大的 IT 基礎架構和網路服務提供者，也經營著全球規模最大 B2B 網路安全事業。

Cisco Secure 秉持的宗旨是資安貴在品質而非數量。我們提供一種以客戶為中心的簡化資安方法，確保易於部署、便於管理和容易使用，而且彼此可以合作無間。使用者和客戶是我們一切業務範疇的核心，這個理念驅使我們前進，我們理解客戶希望減少複雜性和干擾，並對其資安充滿信心，進而能專注於實現成果。這需要的是化繁為簡而不是過分單純化。在這方面，我們的雲端原生平台是一大躍進。

我們為資安社群帶來可靠性和信心，確保無論是現在還是未來，他們都能運用 SecureX 平台抵禦威脅。我們透過世界上最面面俱到的整合式網路安全平台，幫助《財富》100 大公司確保現在和未來均安全無虞。請造訪 cisco.com/go/secure，深入瞭解我們如何簡化體驗、加速成功及保護未來。

美洲總部
Cisco Systems, Inc.
加州聖荷西

亞太總部
Cisco Systems (USA), Pte. Ltd.
新加坡

歐洲總部
Cisco Systems International BV
荷蘭阿姆斯特丹

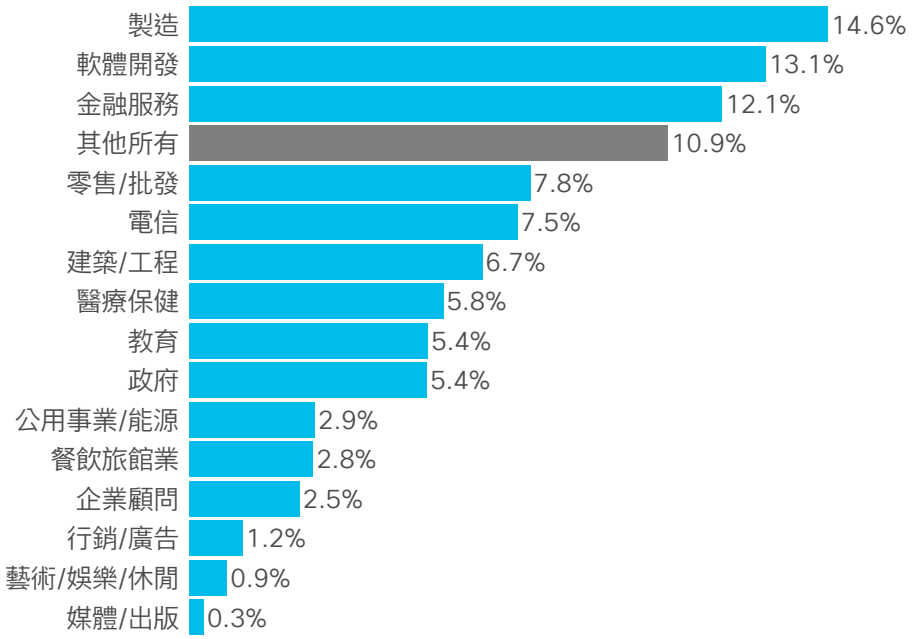
2020 年 12 月發佈 RPT_12_2020

cisco SECURE

附錄

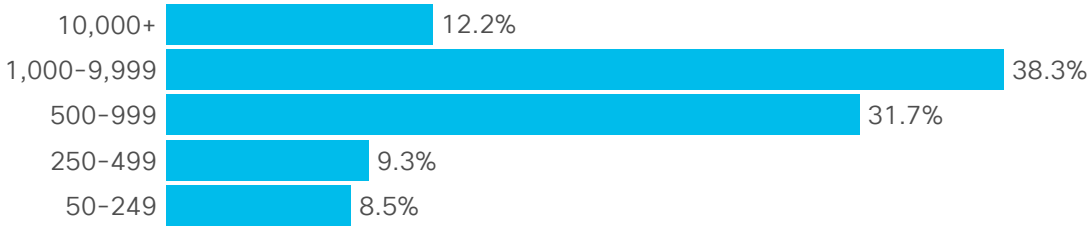
附錄 A：樣本人口統計資料

代表產業：



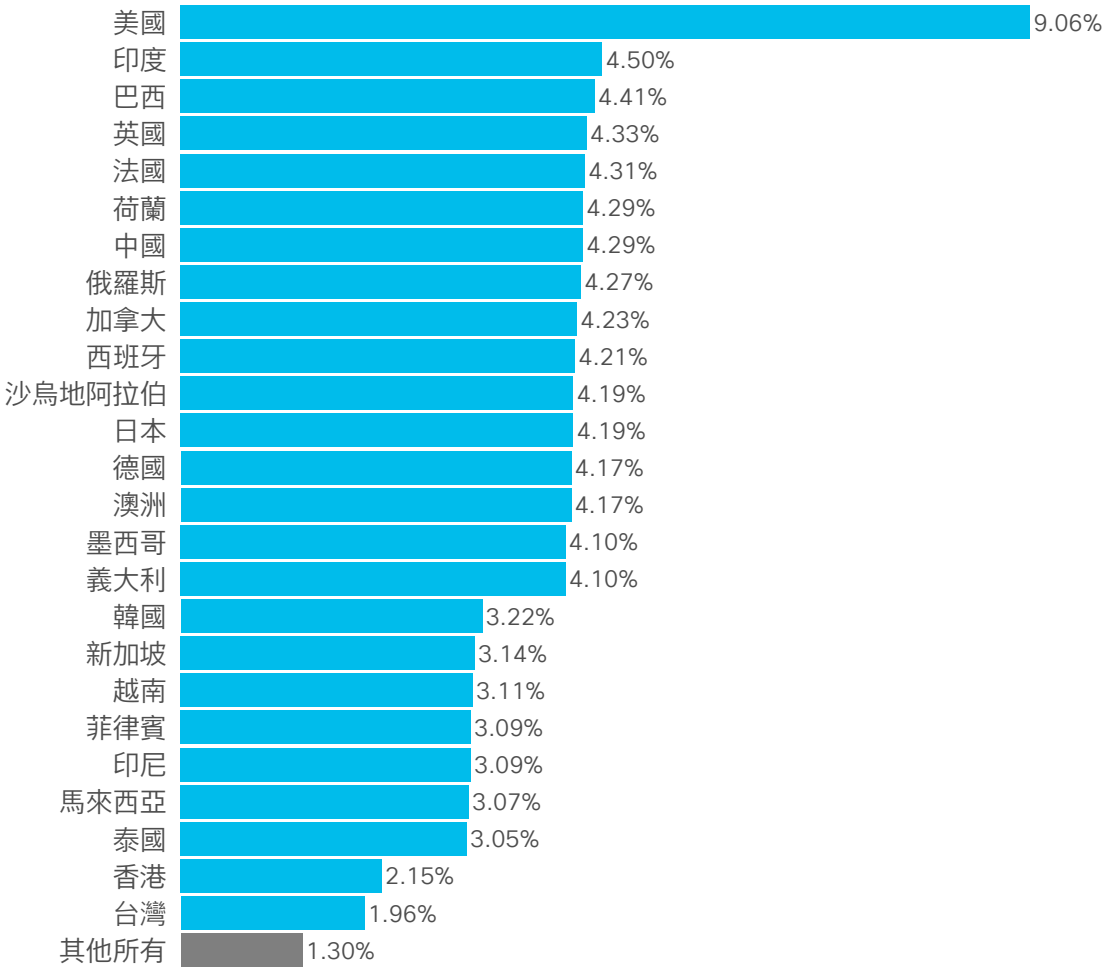
資料來源：思科 2021 年資安成果研究

代表的公司規模 (員工人數)：



資料來源：思科 2021 年資安成果研究

代表的國家/地區：



資料來源：思科 2021 年資安成果研究

附錄 B：資安成果完整清單

為企業賦能	
EB1	**跟上業務需求和成長的腳步**
	成功的範例與證據：資安計畫可以妥善因應不斷變化的業務需求，且不會阻礙新的收入來源。某些情況下，資安可以提供競爭優勢，甚至可以產生淨收入。如果企業高階主管純粹將資安視為成本中心或「只會說『不行！』的部門」，就是這個目標將難以實現的徵兆。
EB2	**取得領導階層的信心和信任**
	成功的範例與證據：資安主管定期與高階主管和董事會開會並取得正面反應。業務和資安主管之間的關係是相互尊重和協同合作的關係。如果高階主管常認為資安問題是燙手山芋，或是合理的資安支援請求經常遭拒絕，就是這個目標將難以實現的徵兆。
EB3	**獲得同事和其他組織單位的認可**
	成功的範例與證據：資安部門請求其他部門共同為組織建立合作防禦機制。溝通與協作的力量非常強大，帶著「互相遷就」的公平意識可實現更大的利益。非資安主管或部門可能有與資安相關的績效指標。部門間互相抱怨和爭執的文化是這個目標將難以實現的徵兆。
EB4	**建立全體員工都接受的資安文化**
	成功的範例和證據：將員工視為資安解決方案的一環而不是問題。在員工滿意度調查或離職對談中，資安並不是負面議題。非資安人員會定期報告網路釣魚攻擊企圖、潛在的惡意軟體和其他事件。頻繁違反資安政策和因應措施是這個目標將難以實現的徵兆。
管理風險	
MR1	**管理組織所面臨的頭號網路風險**
	成功的範例和證據：高階主管和資安主管已經商定了首要風險情境，且已為這些風險制定了緩解計畫（或已接受這些計畫）。潛在網路風險暴露情況目前在領導階層訂定的風險接受範圍之內。沒有證據顯示風險管理功能失效（例如頻繁的跡近錯失、偏差控制、回應/復原測試失敗等）。
MR2	**符合法規遵循要求**
	成功的範例和證據：沒有任何資安發現避開稽核人員和監管機關的審查。組織持續奮力追蹤和應對不斷變化的法規要求。有證據指出組織瞭解規範的內容、知悉任何發現和缺失，且正花費金錢/人力努力緩解這些問題。
MR3	**避免重大資安事件和損失**
	成功的範例與證據：我們料想成功實現此目標的組織在過去幾年間沒有發生過重大資安事件（內部和/或外部能見度很高）。此外，沒有理由懷疑重大資料遺失事件遲早會發生。輕微甚至中度的事件預期會發生，但是這裡探討的問題是組織是否已經且將繼續避免發生會登上頭條新聞的重大事件。

高效營運	
OP1	**執行具成本效益的資安計畫**
	成功的範例和證據：高階主管認為資安計畫的投資報酬率 (ROI) 不錯。沒有反覆出現關於資安成本過高的傳言。閒置軟體購買率很低。人員精簡但充足。高階主管和資安主管間擬定計畫，打算在不增加風險的情況下減少資安預算，將是實現這項成功的好徵兆。
OP2	**最大限度減少計畫外工作和浪費精力**
	成功的範例和證據：策略執行過程中沒有頻繁出現挫折和偏差。主動支出資安預算而非被動支出。員工將時間花在層級更高、更有價值的任務上，而不是埋頭處理單調的工作。不斷陷入救火模式或「故步自封」的計畫是這個目標將難以實現的徵兆。
OP3	**招募和留任優秀的資安人員**
	成功的範例與證據：組織在資安社群中以優良工作場所享負盛名。開出的資安職缺通常會迅速填補人力，且沒有過度的獎勵措施。有才能的員工會升職而不是離職，且維持低流動率。員工滿意度居高不下。
OP4	**簡化事件偵測和回應流程**
	成功的範例與證據：一般而言，資安作業能以高效執行。將資安事件分類並非猜謎遊戲，也不會花很長的時間。回應和修復事件的流程井然有序而不混亂。追蹤偵測時間和修復時間等指標，並隨著時間推移而逐漸縮短所需時間。

附錄 C：資安措施的完整清單

業務與控管	
BG1	我清楚瞭解我所參與的資安計畫如何支援組織的業務需求和目標
BG2	我有充分的理由相信我組織的高階主管認為資安對業務目標而言很重要
BG3	我組織的高階主管會收到有關資安計畫活動和有效性的清楚報告
BG4	我組織中的所有員工均會針對與其職責相關的威脅、政策和程序接受有效的資安意識教育
BG5	我知道我的組織認為我們所面臨的首要網路風險是什麼，而且相信我們已準確評估過這些風險
BG6	我組織中有專人負責管理資安和隱私法規遵循要求
BG7	我有信心我組織的價值/供應鏈中廠商的資安措施符合我們的標準，或是我們對此進行了相應的管理
BG8	我的組織維護著關鍵系統和資料的精確清單，並根據其資安要求和業務重要性加以分類
策略與支出	
SS1	為了成功實現使命，我們的資安計畫秉持並傳達著一套完善的整體策略
SS2	我們的資安計畫擁有成功實現其使命所需的財務預算
SS3	我們的資安計畫擁有成功實現其使命所需的人員
SS4	我們的資安人員接受了履行其職責所需的因角色而異的教育訓練
SS5	我們的資安計畫擁有成功實現其使命所需的技術和工具
SS6	我的組織已制定頻繁升級為最佳可用技術的主動技術更新策略 IT 和資安技術
架構與營運	
AO1	我們的資安技術經過妥善整合且能有效協作
AO2	我們的資安計畫使用績效指標來推動營運決策和行動
AO3	我組織的 IT、開發和資安作業人員可以有效共同合作
AO4	我們有效利用自動化來提高資安作業和人力的效率
AO5	我的組織符合修復系統和軟體中已知漏洞的既定 SLA 或期限
AO6	我的組織採用嚴格的方法進行開發和持續維持內部應用程式的安全性
AO7	我們主動監控並定期審查資安措施，以驗證並維持其有效性
AO8	我們的威脅偵測功能沒有重大盲點，可準確感知潛在的資安事件
AO9	我們的事件回應能力可及時且有效地調查和緩解資安事件
AO10	我們的復原能力可將影響降到最低，且能確實迅速復原受到資安事件影響的資產
AO11	我們付出特別的努力，找出從回應事件中學到的教訓，並運用在改善未來事件的資安措施上

CISCO

SECURE