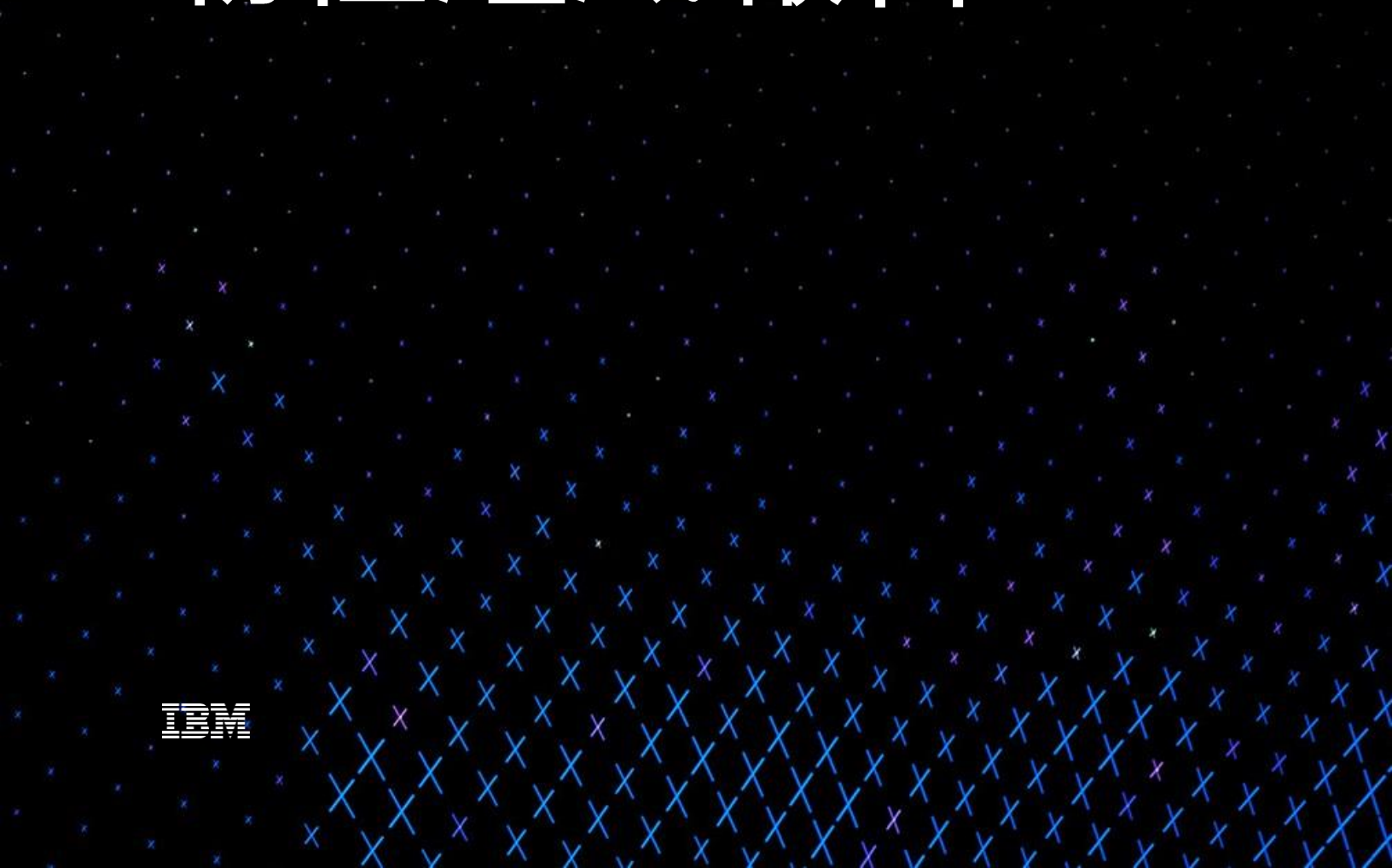
IBM Security

2020 年資安韌性組織報告



IBM

目錄

執行概要

由 Ponemon Institute 進行的一項全球調研而編寫，該項調研於 2020 年 4 月對全球 3,400 多名 IT 和安全專業人員進行了訪談，旨在確定受訪組織偵測、防範、遏制和回應網路安全事件的能力。

網路安全事件的數量有所增加，對 IT 和業務流程造成了嚴重破壞。與此同時，表示自身已實現了較高資安韌性的組織所占百分比從 2015 年的 35% 增加到了 2020 年的 53%，增幅為 51%。具有資安韌性的企業是指能夠更高效地防範、偵測、遏制並回應各種針對資料、應用程式和 IT 基礎架構的嚴重威脅的企業。

目前，超過四分之一的受訪者透過涵蓋整個企業範圍內且保持一致的網路安全事件回應計畫 (CSIRP) 來確保其資安韌性。大多數組織依靠自動化、機器學習、人工智慧、雲端和編排來加強其安全環境。

但是挑戰仍然存在 - 從資源和預算限制，到威脅的不斷複雜化和 IT 環境的複雜性，再到安全團隊遏制網路攻擊的能力下降。

該報告研究了受訪組織用以提高整體資安韌性的方法和最佳實務。它詳細說明了資安韌性作為強大安全防禦措施一部分的重要性，即，其在面對網路攻擊時能夠最大限度地減少業務中斷。最後，我們還提供了一些建議，旨在幫助您的組織提高資安韌性。

事實

51%

表示在過去兩年中曾由於網路安全事件而遭遇**嚴重業務中斷**的組織所占百分比

26%

使用**涵蓋整個企業範圍的 CSIRP** 的組織所占百分比

55%

表示**已透過自動化工具提高了資安韌性**的績效卓越組織所占百分比

52%

表示**雲端服務提高了其資安韌性**的受訪者所占百分比

45

受訪組織正在使用的**安全解決方案和技術**的平均數量

2020 年報告的新動態

為了體現不斷變化的安全格局，今年的報告首次研究了雲端服務的使用對提升組織的資安韌性有何影響以及使用雲端服務的主要優勢。此外，還增加了一些與組織使用特定回應計畫來應對常見安全攻擊（例如惡意軟體和網路釣魚攻擊）相關的問題。

我們擴展了去年引入的有關安全解決方案數量的問題，以進一步瞭解用於調查和回應安全事件的工具數量。

與去年類似，我們也從受訪者中分離出了最具資安韌性的組織（即「績效卓越組織」）並探究了他們的差異化優勢，以此方式建立了資安韌性衡量基準。該報告重點介紹了哪些策略有助於提升績效卓越組織的資安韌性，例如利用自動化工具、使用雲端服務並注重可互操作性等等。

重要調查結果

使用 CSIRP 的組織所遭遇的**業務中斷次數較少**。

網路安全事件回應計畫 (CSIRP) 可以最大程度地減少業務中斷。

自 2015 年以來，企業級 CSIRP 的採用率緩慢提升，增幅為 44%。儘管 CSIRP 的採用率有所提升，也給組織帶來了諸多優勢，但仍有 51% 的受訪者表示，他們並未在整個企業中統一使用 CSIRP，或者更糟糕的是，他們採用的 CSIRP 並非正式計畫或僅僅是臨時計畫。

在已採用正式 CSIRP 的受訪組織中，只有三分之一的組織擁有針對常見攻擊（如 DDoS 或惡意軟體）的攻擊特定教戰手冊。已針對勒索軟體等新興威脅進行了規劃的組織更是少之又少。

此外，只有 7% 的組織會每季度審查一次他們的 CSIRP，這一數字在過去五年中變化不大。實際上，40% 的組織在 CSIRP 計畫的審核和更新方面沒有設定期限，這一比例自 2015 年以來增加了 8%。如果沒有在整個企業範圍內運用最新的 CSIRP，則 23% 以上的組織會遭受 IT 和業務流程的重大破壞。

雖然無法阻止所有攻擊，但組織在回應攻擊方面的準備工作和流程可以大大減少損失。該研究顯示，缺少關於 CSIRP 的盡職調查可能會限制此類計畫在激進威脅環境中的有效性。

-8%

擁有 50 多種工具的組織，其網路攻擊偵測能力低 8%。

過多的工具會削弱資安韌性，不過自動化、可視性和可互操作性有助於改善事件回應能力。

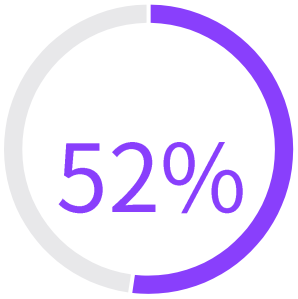
受訪組織使用大量工具來管理其安全環境並回應網路安全事件。在專門調查和回應網路安全事件時，將近 30% 的組織使用了 50 多種單獨的安全解決方案和技術，而 45% 的組織使用了 20 多種工具。

不過，使用過多互不關聯的工具會導致環境複雜化，進而降低效率。該調研表明，受訪組織所用安全解決方案和技術的數量會對其偵測、防範、遏制和回應網路安全事件的能力產生不利影響。

實際上，使用 50 種以上工具的組織，其網路攻擊偵測能力比使用的工具數量不足 50 種的組織低 8%，回應攻擊的能力低 7%。

在過去三年中，確保對應用程式和資料的可見性已成為組織提高其資安韌性的主要方式之一。在今年，自動化是另一個引人注目的原因，尤其是對於績效卓越組織而言更是如此。績效卓越組織表示，使用可互操作的工具有助於提高其資安韌性：在績效卓越組織中，如此表示的組織所占比例為 63%，而在其他組織中，這一比例為 46%。

強調交互操作性有助於提供多個供應商解決方案之間亟需的可視性，同時還能夠降低複雜性。



表示**雲端服務提升了其資安韌性**的受訪者所占比例

雲端服務帶來了更大的資安韌性。

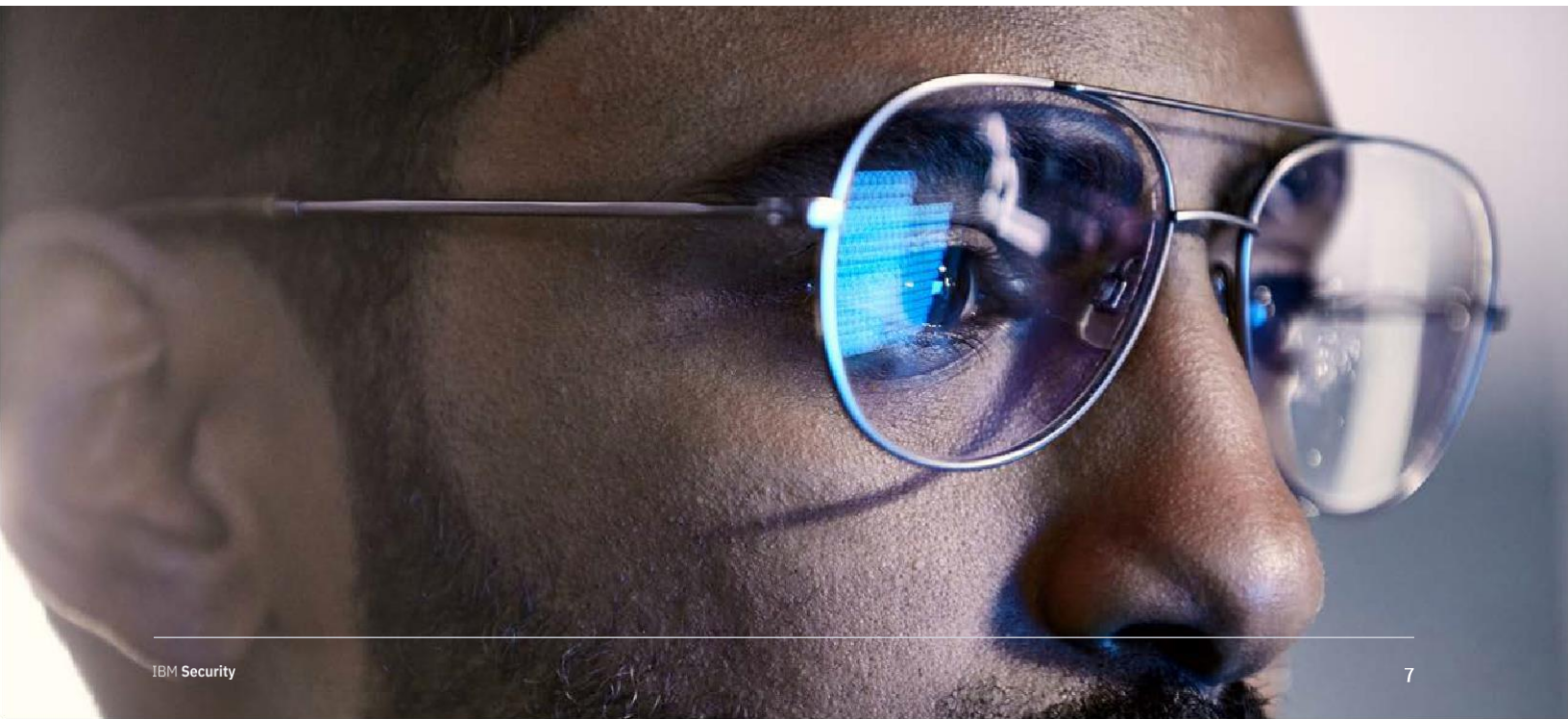
52% 的受訪者表示，雲端服務的使用提高了其資安韌性。在績效卓越組織中，有 63% 的組織表示雲端服務的使用提升了其資安韌性，而在其他組織中，如此表示的組織所占比例為 49%。

不出所料的是，60% 的金融服務組織（雲端技術的早期採用者）表示，使用雲端服務提高了其資安韌性。醫療保健組織和零售組織以及公共領域的組織也表示他們透過使用雲端服務實現了高於平均水準的資安韌性改善。

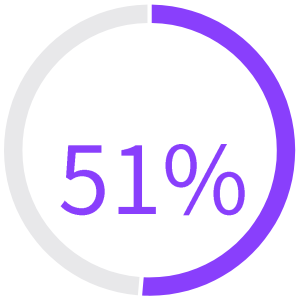
相比其他國家或地區，英國、德國、法國、美國和加拿大的組織更加看重雲端服務及其對實現資安韌性的重要性。具體而言，在這些國家/地區中，超過三分之二的組織重視雲端服務的使用。

據績效卓越組織表示，雲端服務之所以能夠改善資安韌性的主要原因在於利用分佈式環境所實現的優勢、規模經濟以及服務等級協定的可用性。另一方面，有 30% 的受訪組織表示，設定不當的雲端服務阻礙了其資安韌性的提升。

單單投資雲端服務是不夠的，優化對於確保環境的有效性來說也至關重要。



更多洞察

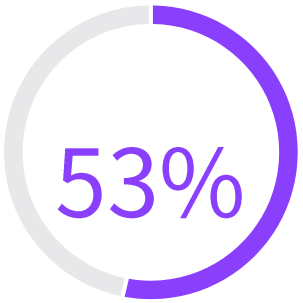


在過去兩年中**因網路攻擊而遭受嚴重業務中斷**的組織所占比例

網路攻擊的數量和嚴重性均已增加。

在過去兩年中，大多數受訪組織 (53%) 遭遇過涉及超過 1000 條包含有敏感資訊或機密客戶/企業資訊的記錄丟失或被盜的資料洩露事件。在過去兩年中，幾乎相同比例的受訪組織 (51%) 表示他們遭受過造成其 IT 和業務流程受到嚴重破壞的網路安全事件。

分別有 67% 和 64% 的受訪者表示，在過去 12 個月中，網路攻擊的數量和嚴重性大幅增加。嚴重性主要透過高價值資訊資產的洩露程度來衡量（佔比 57%），其次是員工生產力的降低（佔比 50%）。



資安韌性得到改善的組織所占比例

資安韌性總體上得到了提高，不過在過去五年中，提升幅度最大的是攻擊防禦能力。

在過去五年中，受訪組織的資安韌性得到了增強，提升幅度達 51%。這種提升與受訪組織網路攻擊防範能力的顯著提升（從 2015 年的 38% 增加到 2020 年的 53%）保持同步。

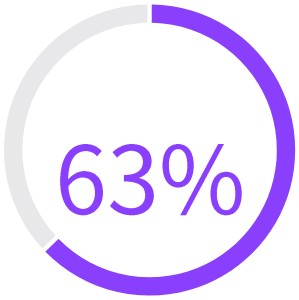
實際上，大多數受訪組織 (56%) 以成功防範的網路攻擊數量來衡量其資安韌性的提升情況。衡量資安韌性提升情況的其他關鍵指標包括遏制事件所需時間及員工生產效率的提升程度。

自 2015 年以來，組織的攻擊偵測能力略有提升 (11%)，這也是組織衡量其資安韌性時最常採用的第二種方法 (51%)。回應能力相比之前變化不大，但在遏制攻擊方面似乎愈發具有挑戰性，受訪者表示他們在該方面的能力下降了 13%。

儘管有 77% 的受訪組織制定了網路安全事件回應計畫 (CSIRP)，但只有 26% 的組織在整個企業範圍內運用了此類計畫，考慮到這些情況，出現這種下降就不足為怪了。另外，在前述 77% 的受訪組織中，有四分之一的組織表示他們的計畫為非正式計畫或僅是臨時計畫。

<50%

向高階主管/董事會報告資安韌性的組織所占比例



表示**自動化、機器學習、人工智慧和編排提升了其資安韌性**的組織所占比例

缺乏預算和技能仍然是提升資安韌性的障礙。

可以預見的是，技術人員流失 (41%) 和缺乏預算 (40%) 是受訪組織表示他們沒有改善資安韌性的主要原因。許多受訪者表示技術是增強安全態勢的關鍵，部分受訪者表示他們難以獲取最新工具或從其已擁有的工具中獲取最大收益。

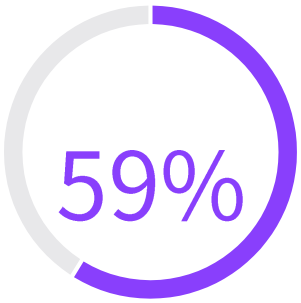
他們所面臨的挑戰包括：「筒倉」和「地盤」問題 (31%)、缺乏自動化等先進技術 (25%) 以及 IT 和安全基礎架構零散 (22%)。

令人驚訝的是，只有 45% 的受訪者表示其所在組織向其高階主管或董事會提交了有關資安韌性狀態的正式報告。不過，高階主管們的認可、對網路安全功能的支援以及向董事會報告是資安韌性未得到改善的最不重要的原因。

分析、自動化、人工智慧和機器學習有助於增強安全態勢。

受訪者表示，分析 (46%)、自動化 (42%) 以及人工智慧和機器學習 (41%) 等技術的實施提高了其所在組織的資安韌性。

總體而言，63% 的受訪組織表示，這些工具的採用幫助他們增強了資安韌性安全態勢，其次是強健的隱私態勢 (60%)。正如將在本報告後文中探討的那樣，技術是能否成為資安韌性方面績效卓越組織的關鍵。

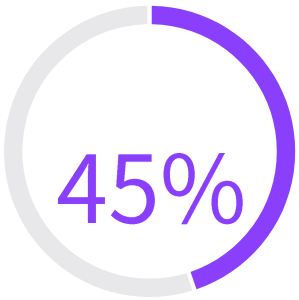


表示**共享威脅情報提升了其資安韌性**的組織所占比例

促進協作是共享威脅情報的主要優勢。

59% 的受訪者認為共享威脅情報有助於提升資安韌性。為了促進協作，57% 的受訪組織參與了與政府和/或同行共享網路威脅和漏洞相關資訊的共享倡議或計畫。

當被問及為何不共享網路威脅相關資訊時，受訪者最常提及的原因是：沒有意識到共享對組織所帶來的優勢 (70%)、缺乏資源 (58%) 和成本 (54%)。



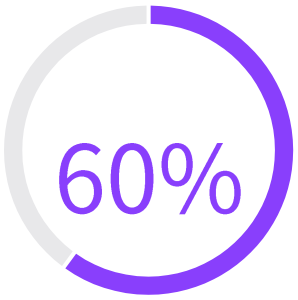
未針對勒索軟體攻擊制定相應計畫的組織所占比例

DDoS 是最常見的攻擊特定回應計畫類型。

此次調研首次詢問如何使用回應計畫來解決特定類型的攻擊。最常用的計畫是針對分散式阻斷服務 (DDoS)、惡意軟體（包括間諜軟體、病毒、木馬和蠕蟲）、內部人員事件和網路釣魚攻擊的計畫。

不出所料的是，攻擊計畫的使用因產業而異。針對惡意軟體攻擊的計畫是公共領域、零售、製造和消費品等產業使用最廣泛的回應計畫，而針對內部人員事件的回應計畫則在工業環境中的使用最廣泛。其他產業表示，針對 DDoS 攻擊的計畫是他們使用最廣泛的計畫。

即使在使用攻擊特定教戰手冊的組織中，也只有不到一半的組織 (45%) 制定了針對勒索軟體攻擊的計畫 - 根據 2020 年 *X-Force 威脅指數報告*所述，勒索軟體攻擊在近幾年增加了近 70%。絕大多數組織並不會經常更新其 CSIRP，因此該關鍵風險領域的規劃不足，凸顯了更頻繁地審查和更新計畫以反映最新攻擊方法的重要性。



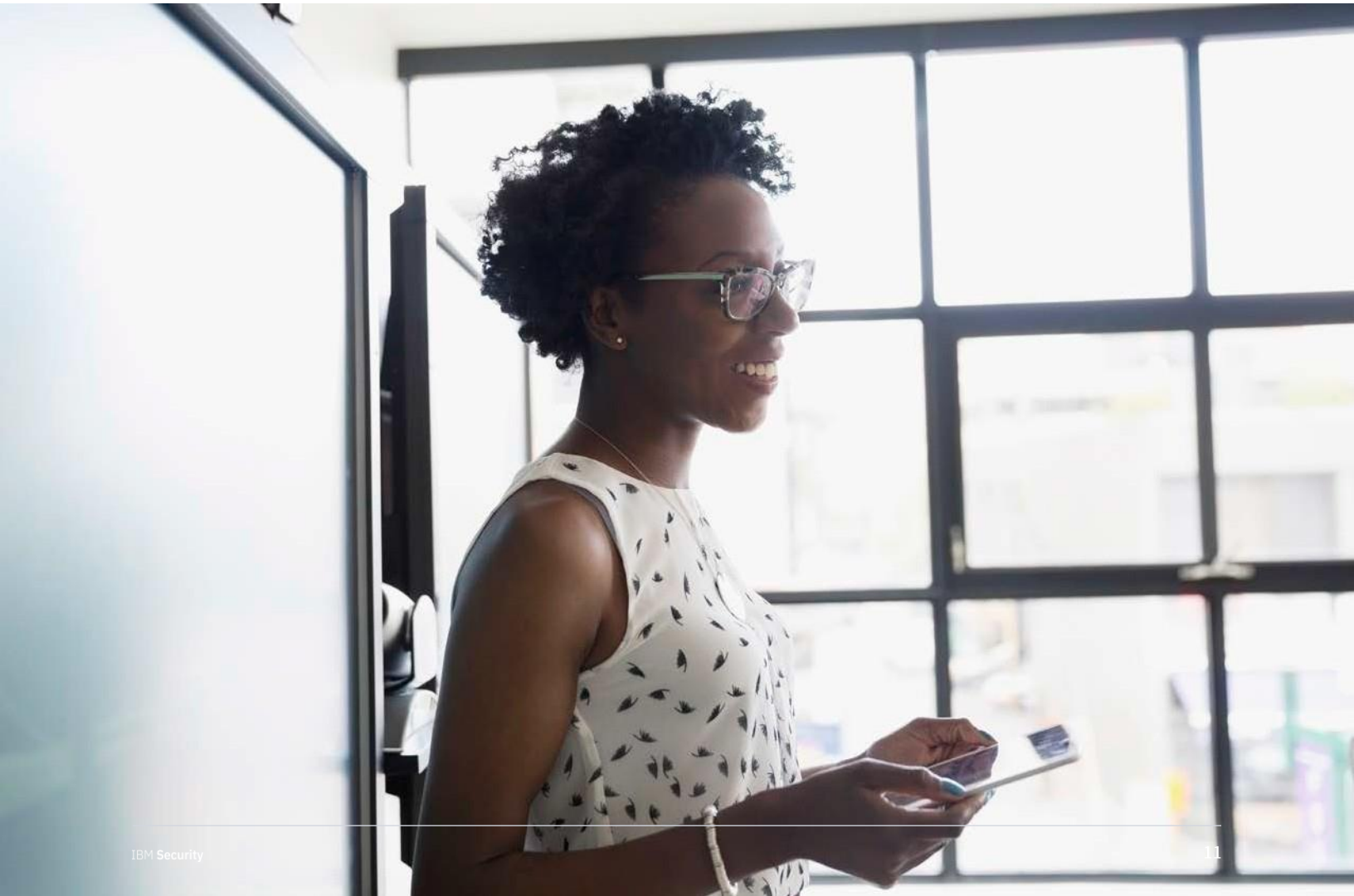
表示**強健的隱私態勢對實現資安韌性很重要**的組織所占百分比

隱私對於確保資安韌性至關重要。

在過去兩年中，53% 的組織因為涉及超過 1,000 條包含敏感資訊或機密資訊的記錄被洩露而遭受業務中斷，因此，95% 的受訪者已經意識到了隱私角色（組織中負責保護客戶資料和員工資料的角色）的重要性，這一點也就不足為怪了。

不過，超過三分之一的受訪組織認為該角色至關重要，但只有 1% 的組織設立了隱私長來負責指導組織在確保資安韌性方面的投入。在這兩類受訪組織中，分別有 22% 的組織表示隱私保護主要由業務部門負責人或 CIO 負責。

60% 的受訪者表示，「強健的隱私態勢」對於實現資安韌性而言至關重要，這一比例與 2019 年的情況相同。57% 的受訪者表示遵守資料保護法規，例如歐盟的《一般資料保護規則》 (GDPR) 和《加州消費者隱私法案》(CCPA) 對於實現資安韌性至關重要。

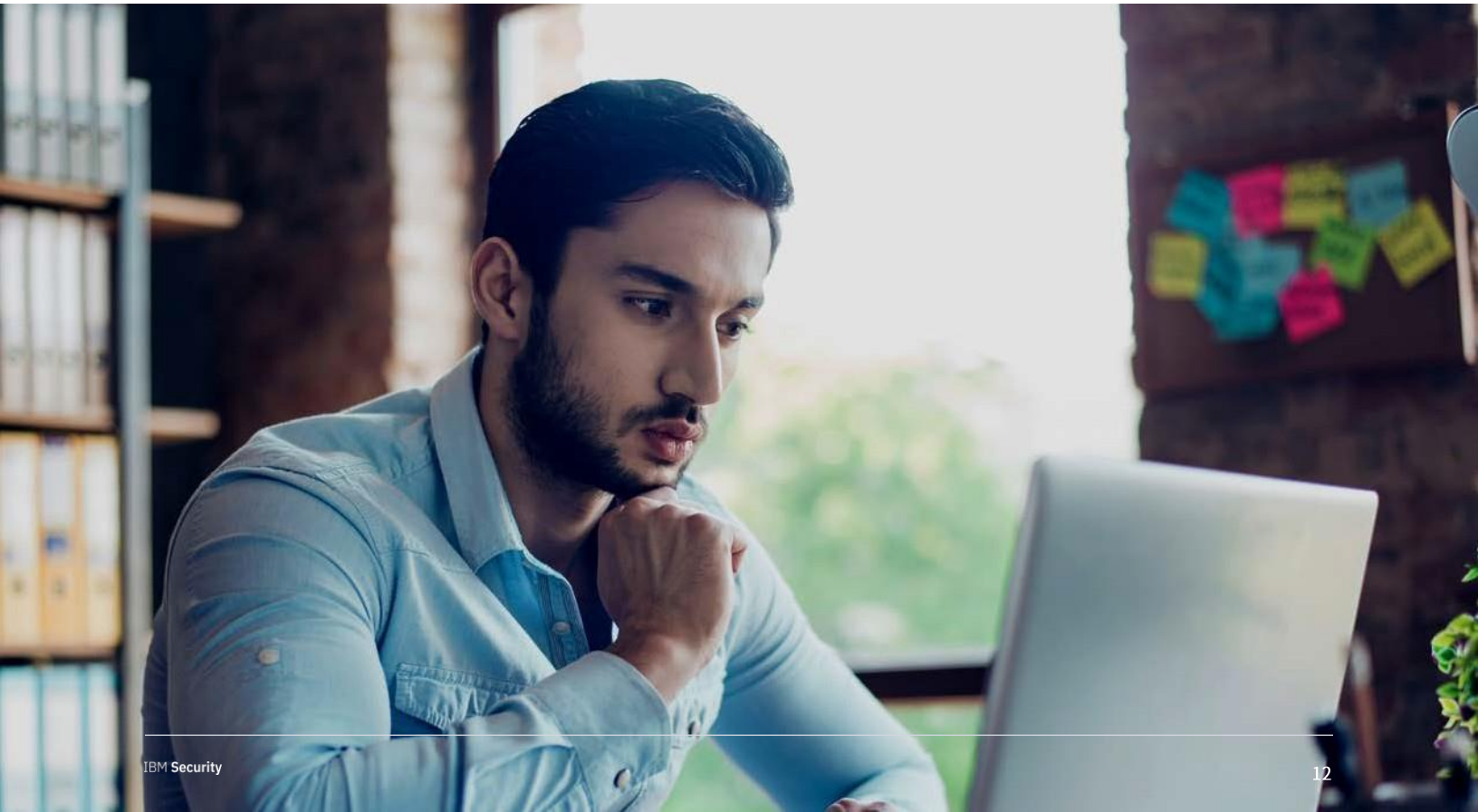


績效卓越組織有何不同之處

在被要求以 1 到 10 分對其所在組織的資安韌性進行評價時，近四分之一的受訪者給出的評分超過了 9 分。在此類受訪者中，59% 的受訪者表示他們所在組織的資安韌性在去年有了顯著改善。我們將這些組織稱為「績效卓越組織」。

與去年相似，在網路攻擊防範、偵測、遏制和回應方面，績效卓越組織的表現優於其他組織。不過，兩者在今年的差距更大一些。最大的區別在於攻擊遏制和回應能力。

去年，在攻擊遏制能力方面，績效卓越組織的表現比其他組織高 14%，但到了今年，這一差距增加到了 35%。同樣，去年，績效卓越組織與其他組織在攻擊回應能力方面的差異為 15%，而在 2020 年，這一差距拉大到了 31%。



顯然，績效卓越組織已開始採用最佳實務，而其他組織可以從中學習經驗。績效卓越組織的一些特徵及所採用的方法包括：

在整個企業範圍內實施 CSIRP：

43% 的績效卓越組織在其整個企業範圍內統一地運用了 CSIRP，而在其他組織中，這一比例只有 20%。每季度或每半年審查和測試一次 CSIPR 計畫的績效卓越組織所占百分比是其他組織中採用如此做法的組織的兩倍。

使用攻擊特定回應計畫：

50% 的績效卓越組織使用攻擊特定回應計畫，而在其他組織中，這一比例為 37%。

技術投資：

73% 的績效卓越組織將自動化、機器學習、人工智慧和編排視為實現強健資安韌性安全態勢的關鍵，而在其他組織中，這一比例為 60%。

大量使用自動化：

70% 的績效卓越組織表示他們的自動化使用程度為大量使用或中等。在此類組織中：

- 70% 的組織使用自動化來提高其營運效率。
- 64% 的組織使用自動化來支援其 IT 安全團隊。

共享威脅情報：

69% 的績效卓越組織共享了威脅情報，這幫助他們提高了他們的網路威脅偵測、遏制和回應的能力，而在其他組織中，採用如此做法的組織所占比例為 50%。

高階主管可視性：

超過一半的績效卓越組織向高階主管和/或其董事會提供了正式報告。

相比其他組織，績效卓越組織

39%

更有可能透過自動化工具實現了改善

25%

更有可能透過部署雲端服務實現了改善

20%

更有可能透過 AI 和機器學習實現了改善

31%

更有可能透過可互操作的網路安全工具實現了改善

資安韌性改善步驟*

在整個企業範圍內實施 CSIRP，最大程度地減少業務中斷。

單單擁有 CSIRP 是不夠的；應在整個組織中予以實施，並定期對其進行審查。隨著攻擊數量和嚴重性的逐年增加，缺少更新的 CSIRP 可能會增加 IT 和業務流程遭受嚴重破壞的風險。

量身定制針對您所在產業中的特定攻擊的回應計畫。

網路安全攻擊有多種形式。組織可以透過瞭解其所在產業中的主要威脅並制定詳細的回應計畫來增強其安全態勢，以幫助確保團隊成員瞭解調查和補救特定攻擊所需的步驟。

確保可互操作性，以提升可視性並降低複雜性。

當組織面臨複雜的安全環境時，最有效的團隊會利用可互操作性來提高工具和資料的可視性，以幫助防範和偵測攻擊。能簡化工作流程的方法有助於提高安全營運中心的生產力。

對技術進行投資，以加速事件回應。

自動化、分析、人工智慧和機器學習以及雲端服務等技術是組織提升其資安韌性的主要原因。尤其是自動化，它能夠讓相關人員騰出時間，專注於調查和回應所需的高價值任務，進而幫助公司提高營運效率並減少團隊流失。

*我們針對安全實務所提供的建議僅供教育用途，不保證任何結果。

協調您的安全團隊和隱私團隊。

具有更強資安韌性的組織已認識到安全和隱私是密不可分的。消除筒倉效應並鼓勵協作文化，以更有效地回應資料洩露。儘早並且經常讓這兩個團隊協同工作，會比他們在面臨大規模安全事件時才第一次協同工作更快地改善安全態勢。

制定正式的高階主管/董事會報告流程，以提高組織資安韌性的可視性。

業務領導者已經認識到，資安韌性會影響收入和聲譽，因此必須確保資安韌性性能始終處於領先和中心地位，以確保獲得所需的投資和資源水準。

完整調查結果

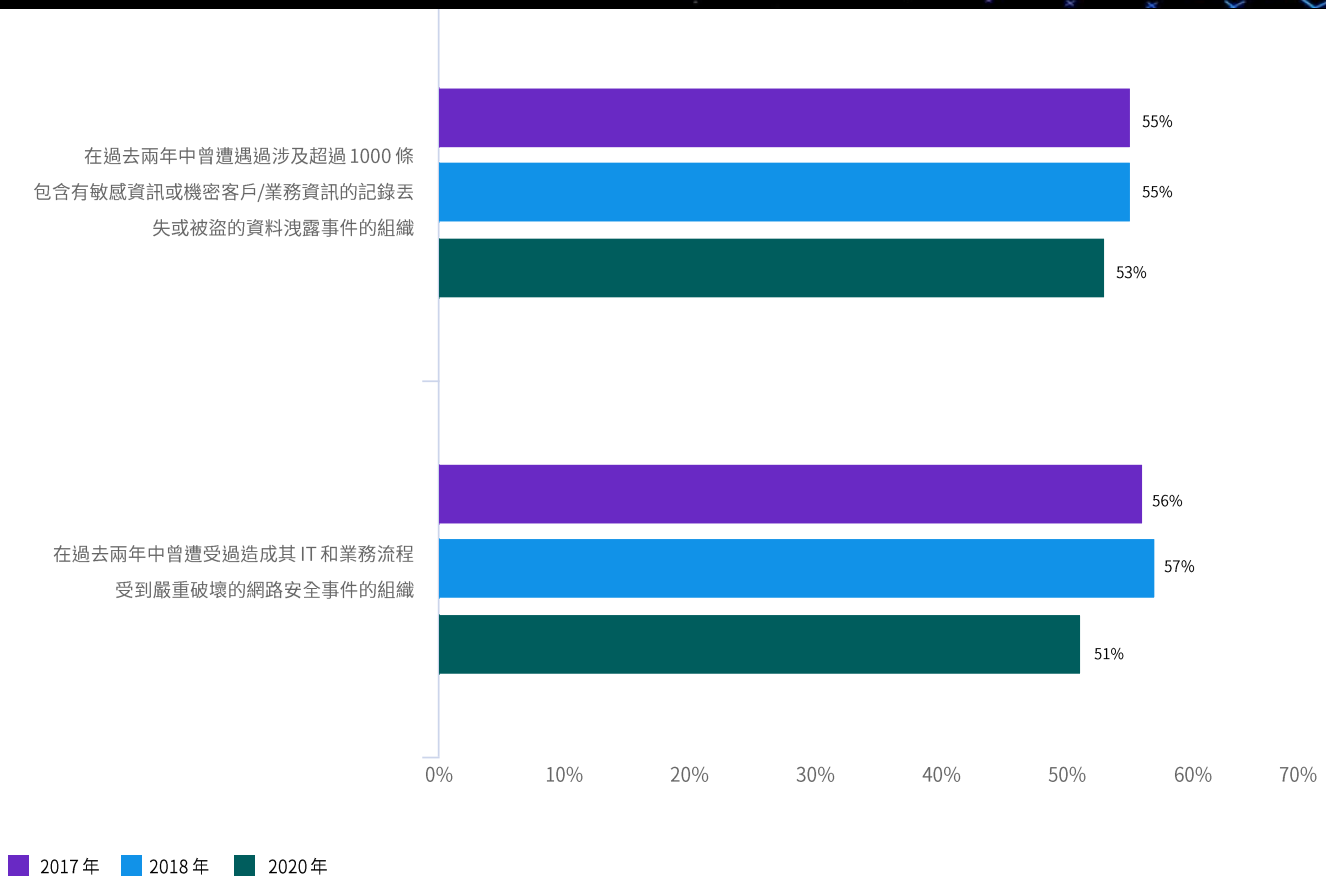


圖 1 顯示了過去兩年中有多少組織曾遭受過資料洩露或網路安全事件。

圖 2

如何衡量改善情況

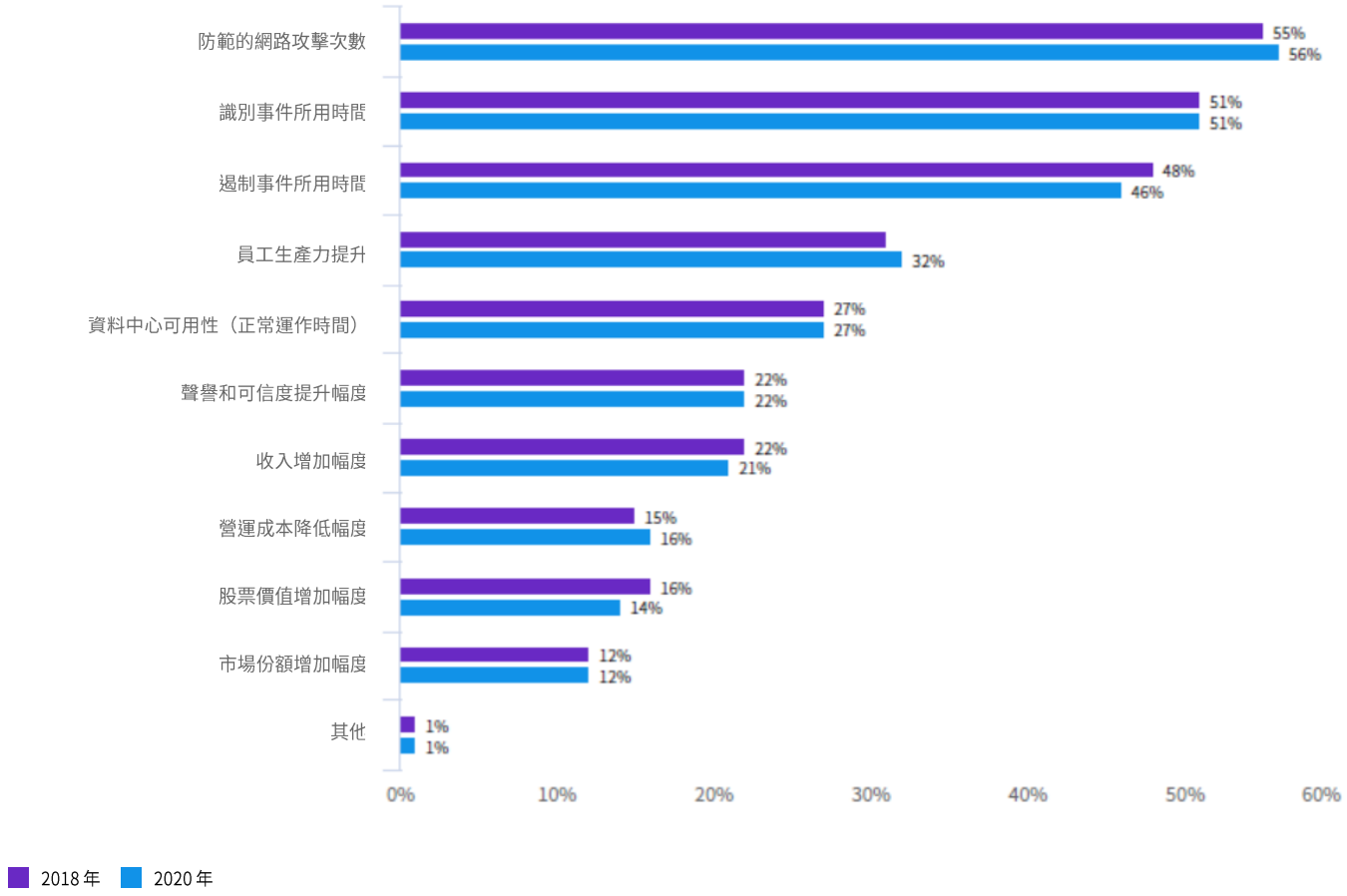


圖 2 提供了有關組織如何衡量資安韌性提升情況的洞察。在所列的 10 個因素中，排名前三的因素分別是：防範的網路攻擊次數、識別事件所需時間和遏制事件所需時間。

圖 3

資安韌性提高的原因

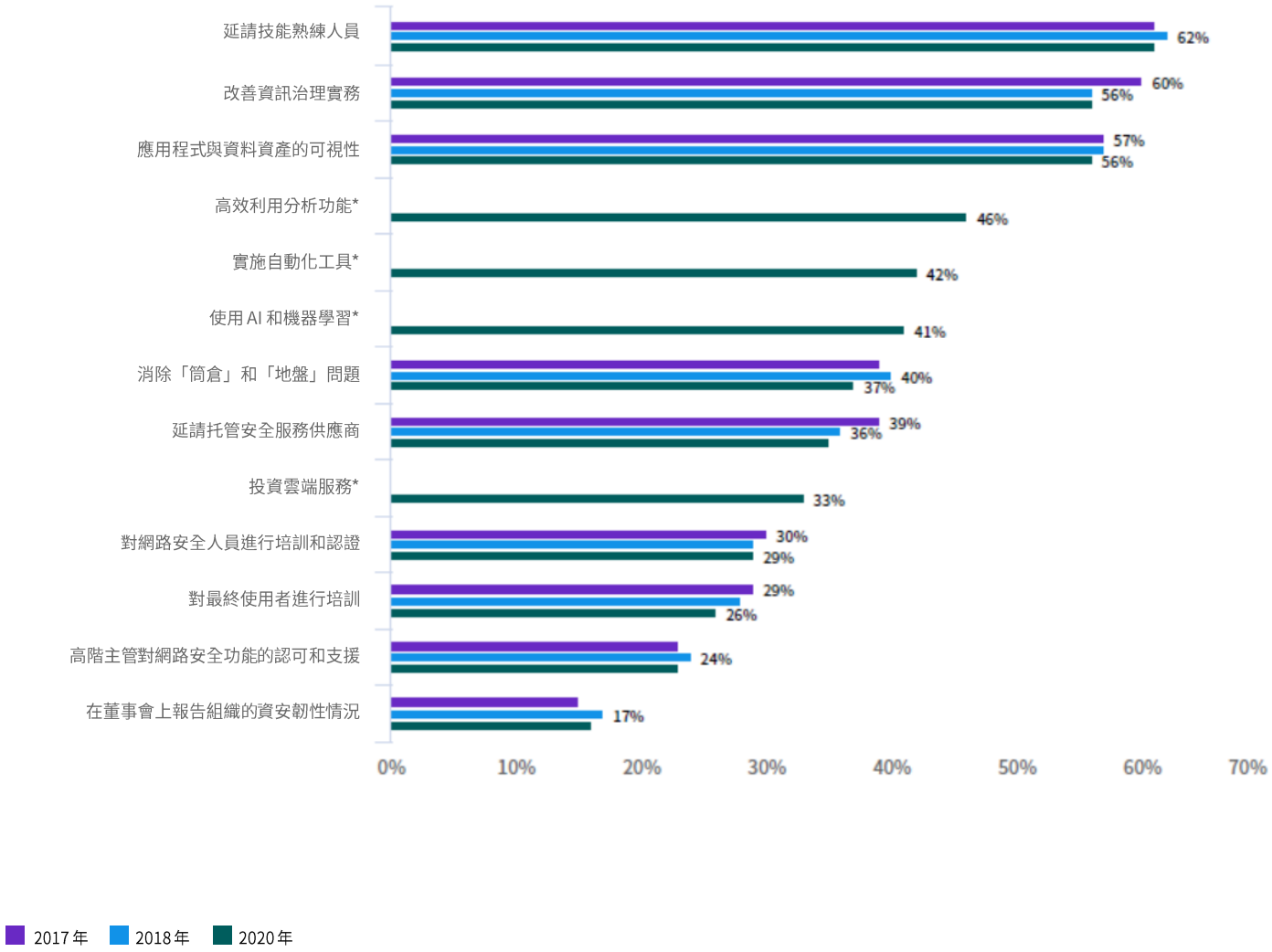


圖 3 顯示了組織提升其資安韌性的原因。儘管前三個因素的年成長率變化不大，但分析、自動化、人工智慧和機器學習卻在今年扮演了重要角色。

圖 4

資安韌性未提升的原因

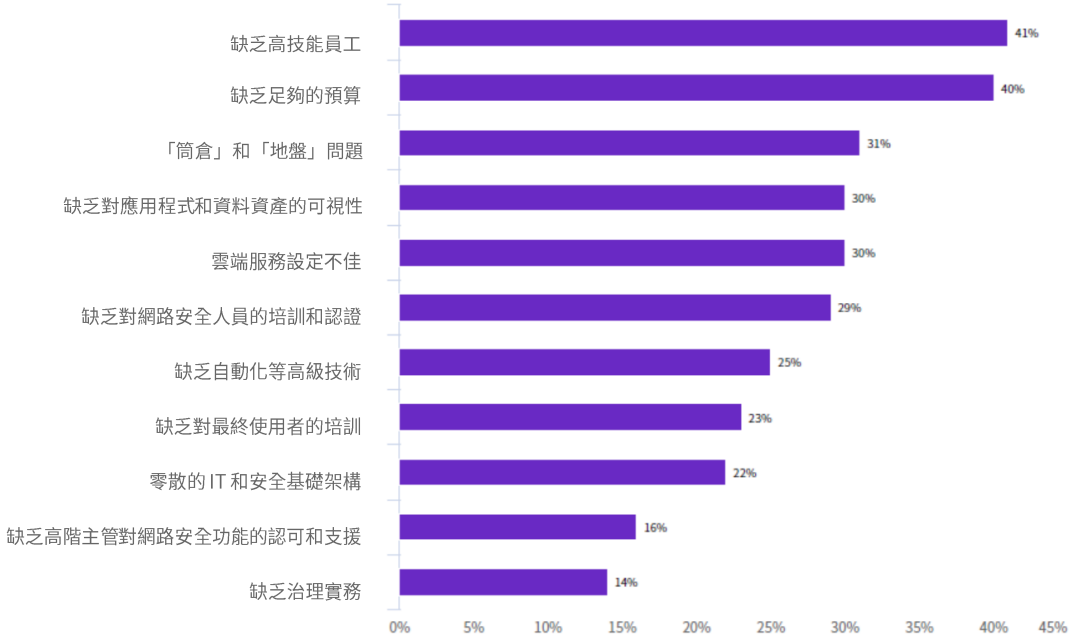


圖 4 解釋了組織未提升其資安韌性的原因。人員、流程和技術均帶來了相應的挑戰。

圖 5

雲端服務的使用對資安韌性提升有何影響

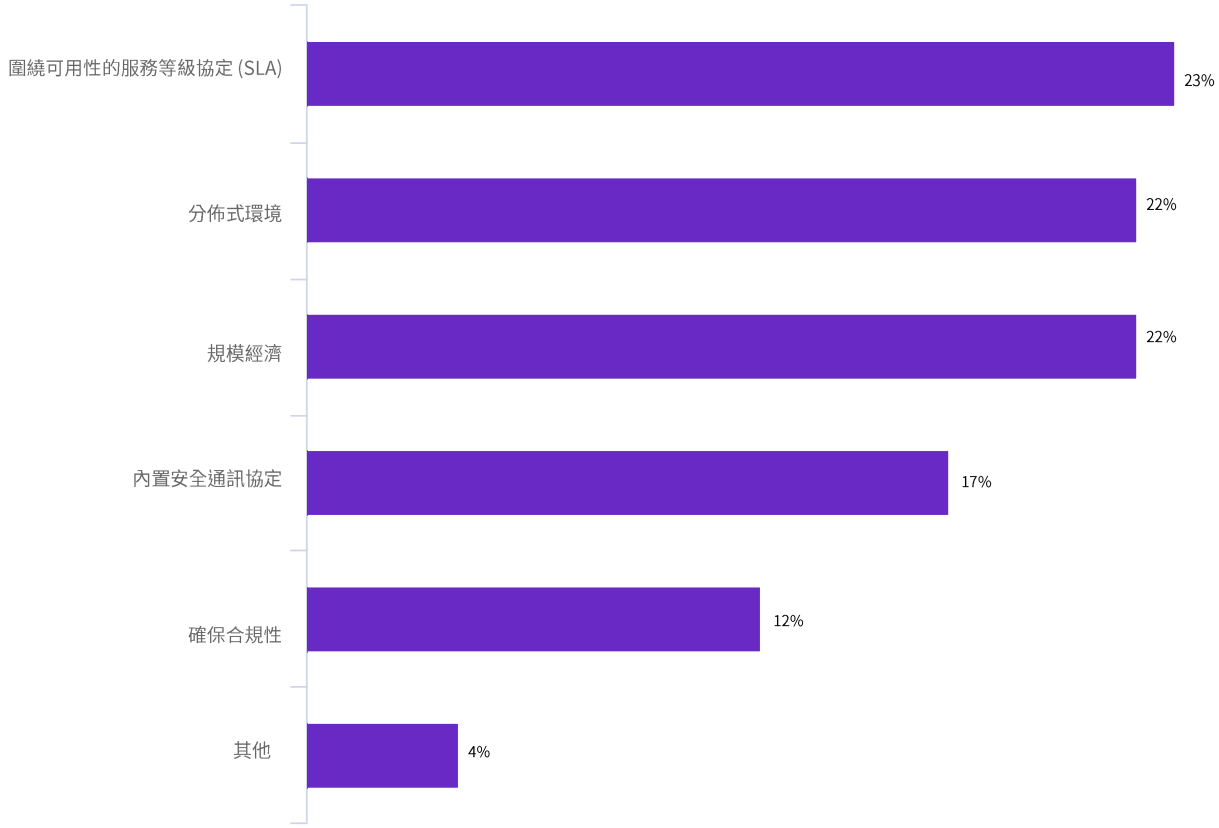


圖 5 細分了雲端服務的使用如何幫助組織提升資安韌性。排名前三的原因分別是圍繞可用性的服務等級協定、分佈式環境和規模經濟。

圖 6

使用的具體回應計畫

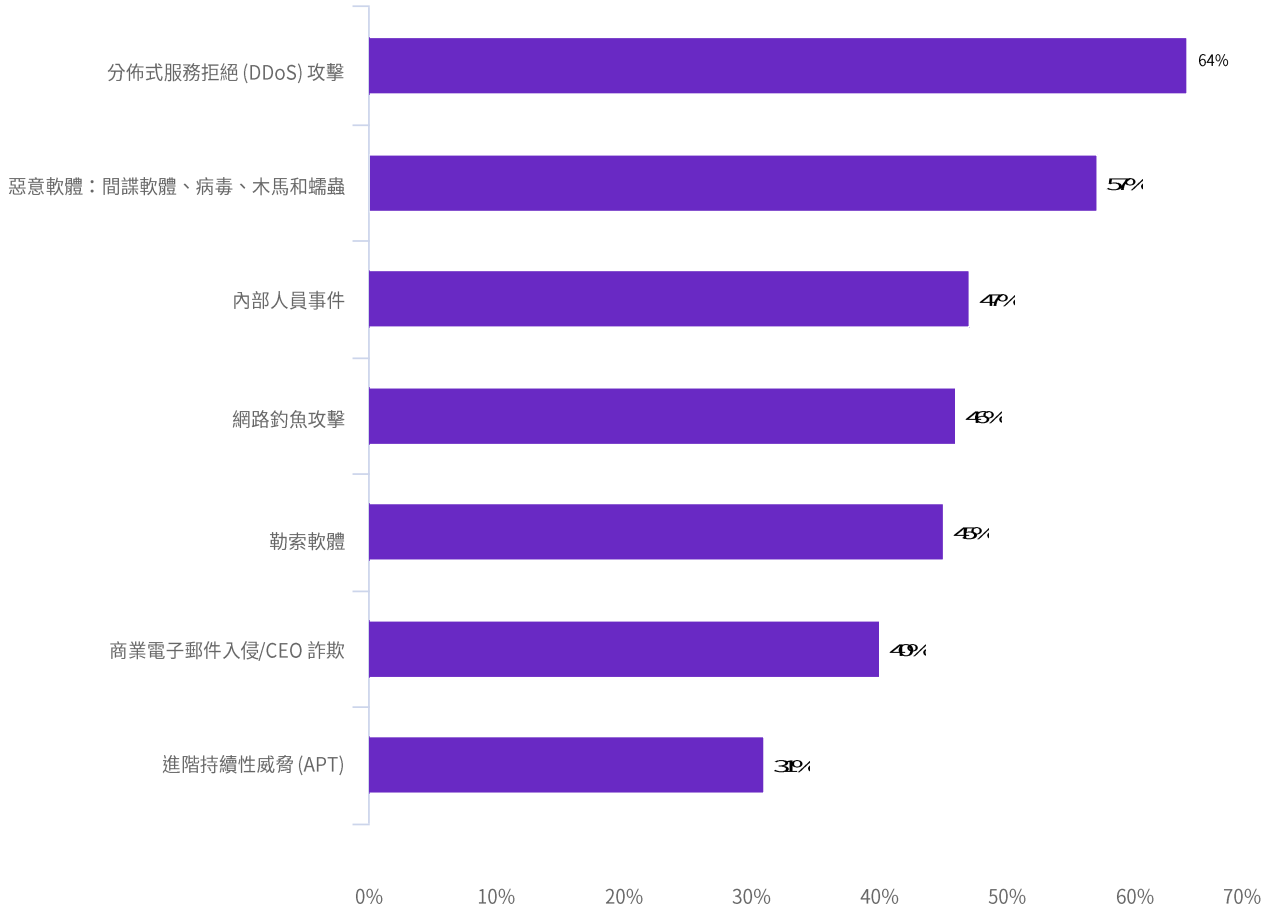


圖 6 顯示了組織量身定制了相應的回應計畫的特定威脅類型。排名前三的威脅類型分別是 DDoS 攻擊、惡意軟體和內部人員事件。

圖 7

如何衡量嚴重性

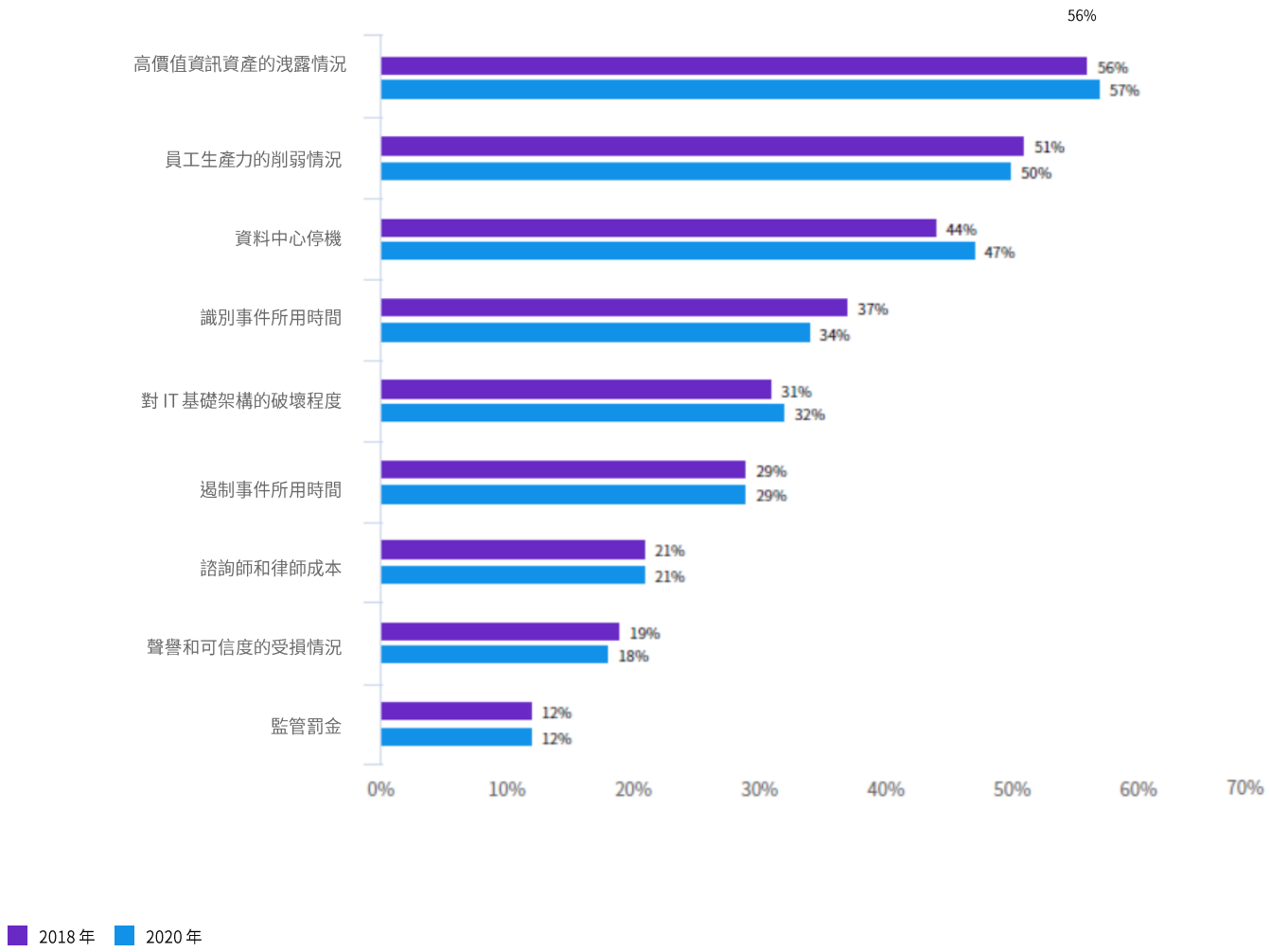


圖 7 顯示組織如何衡量過去兩年攻擊的嚴重性，高價值資訊資產遭洩漏排名第一。

圖 8

威脅情報如何改善資安韌性

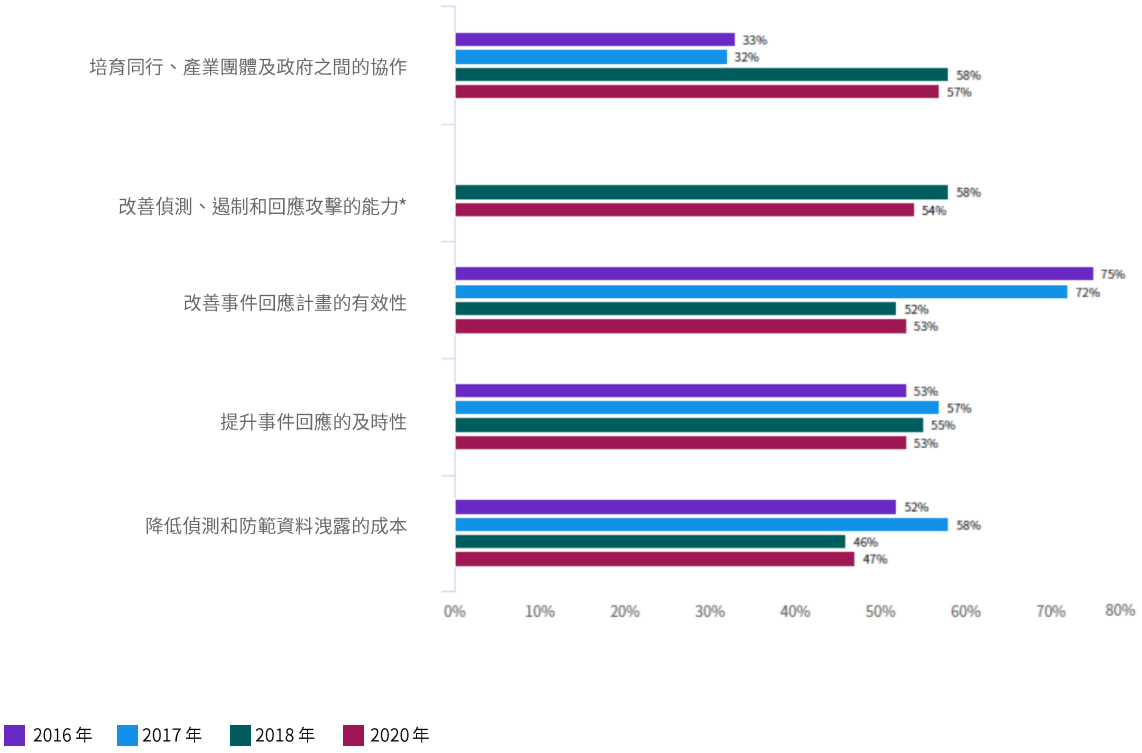


圖 8 評估了共享威脅情報的感知價值。在過去四年中，受訪者對威脅情報共享在提升事件回應計畫有效性方面的作用的信心下降了 29%。

圖 9

績效卓越組織改善資安韌性的原因

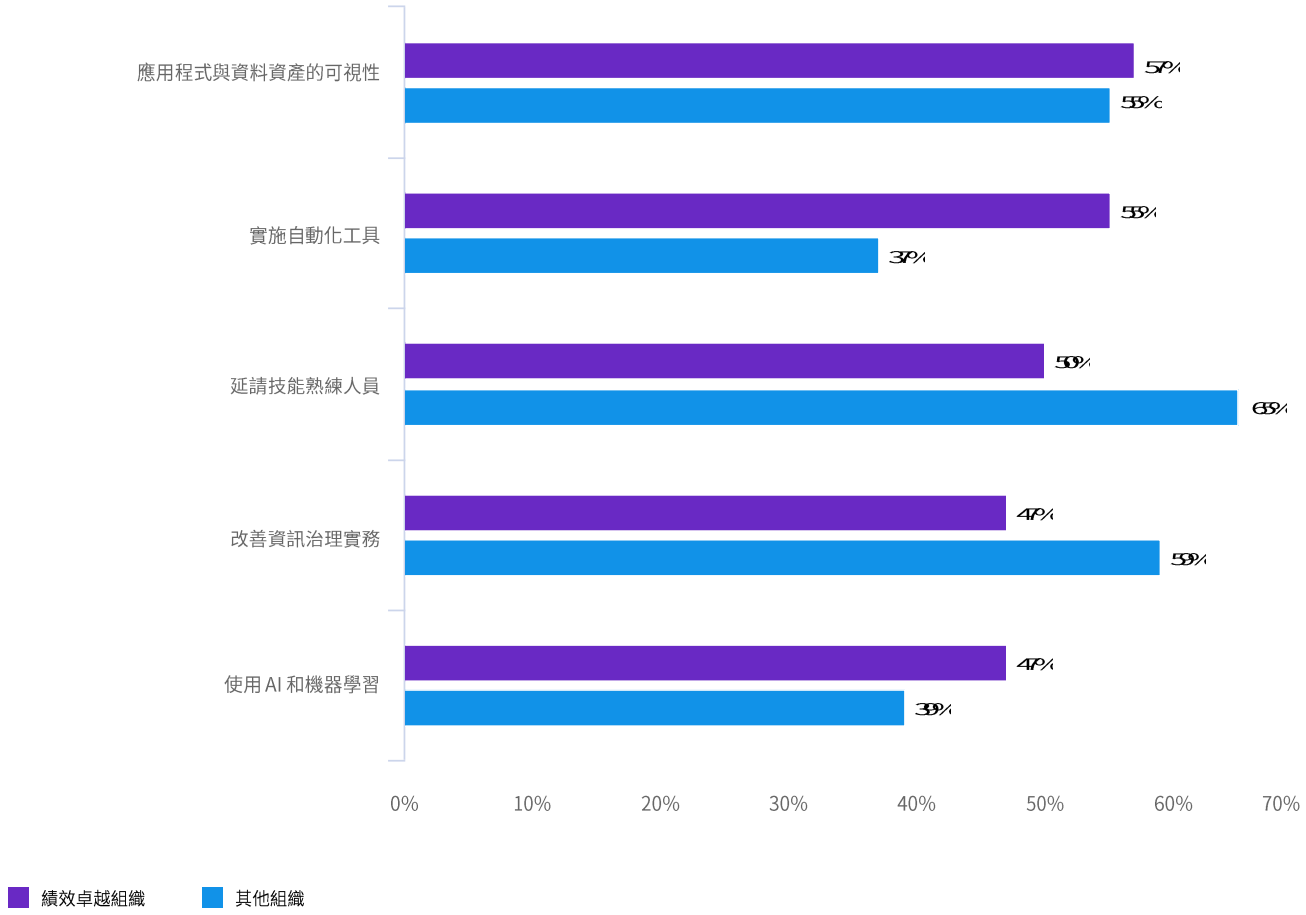


圖 9 顯示了與其他組織相比，績效卓越組織實現資安韌性提升的原因。

圖 10

績效卓越組織更具資安韌性的原因

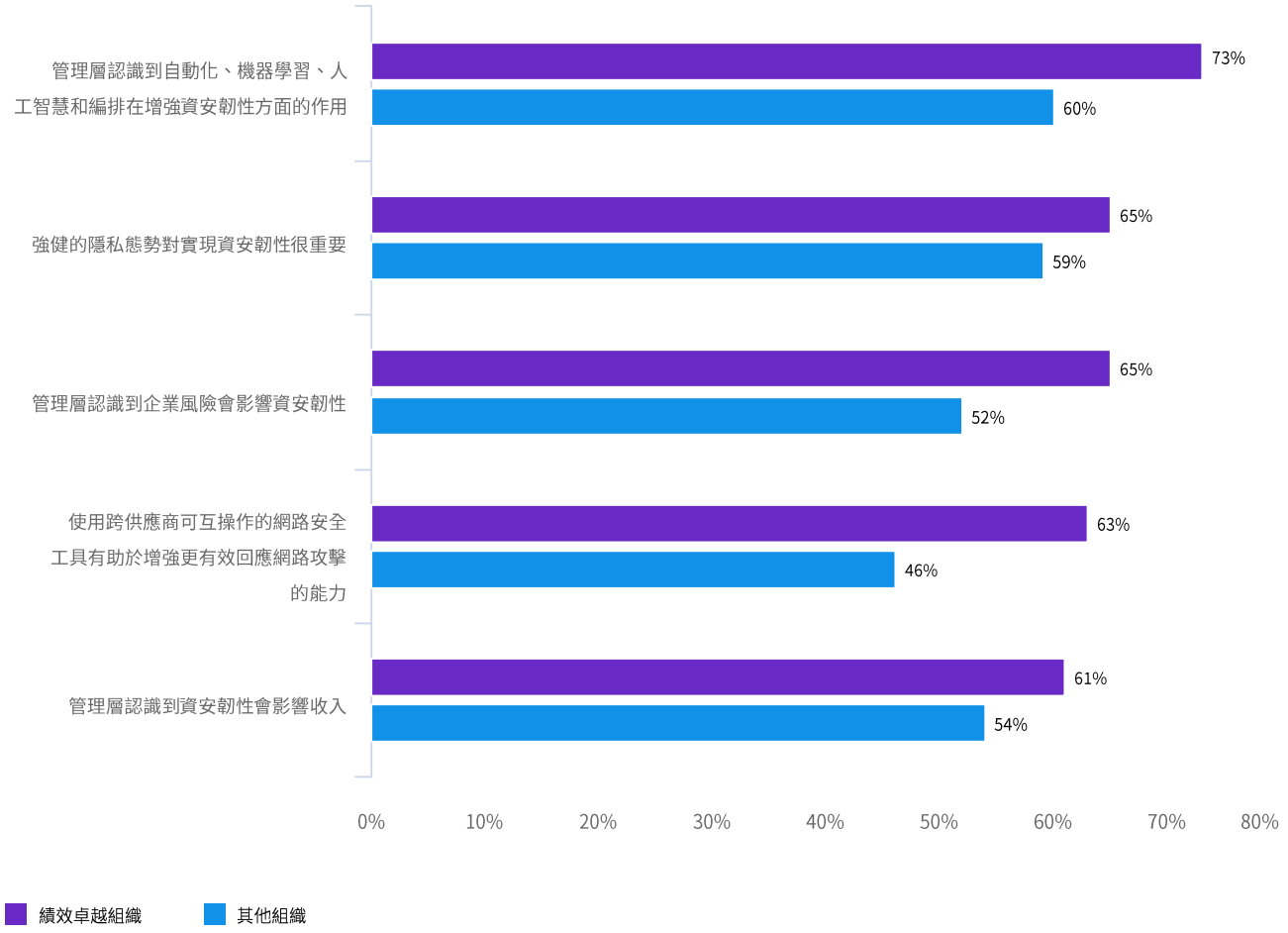


圖 10 顯示了績效卓越組織更具資安韌性的原因。

圖 11

績效卓越組織的資安韌性置信水準

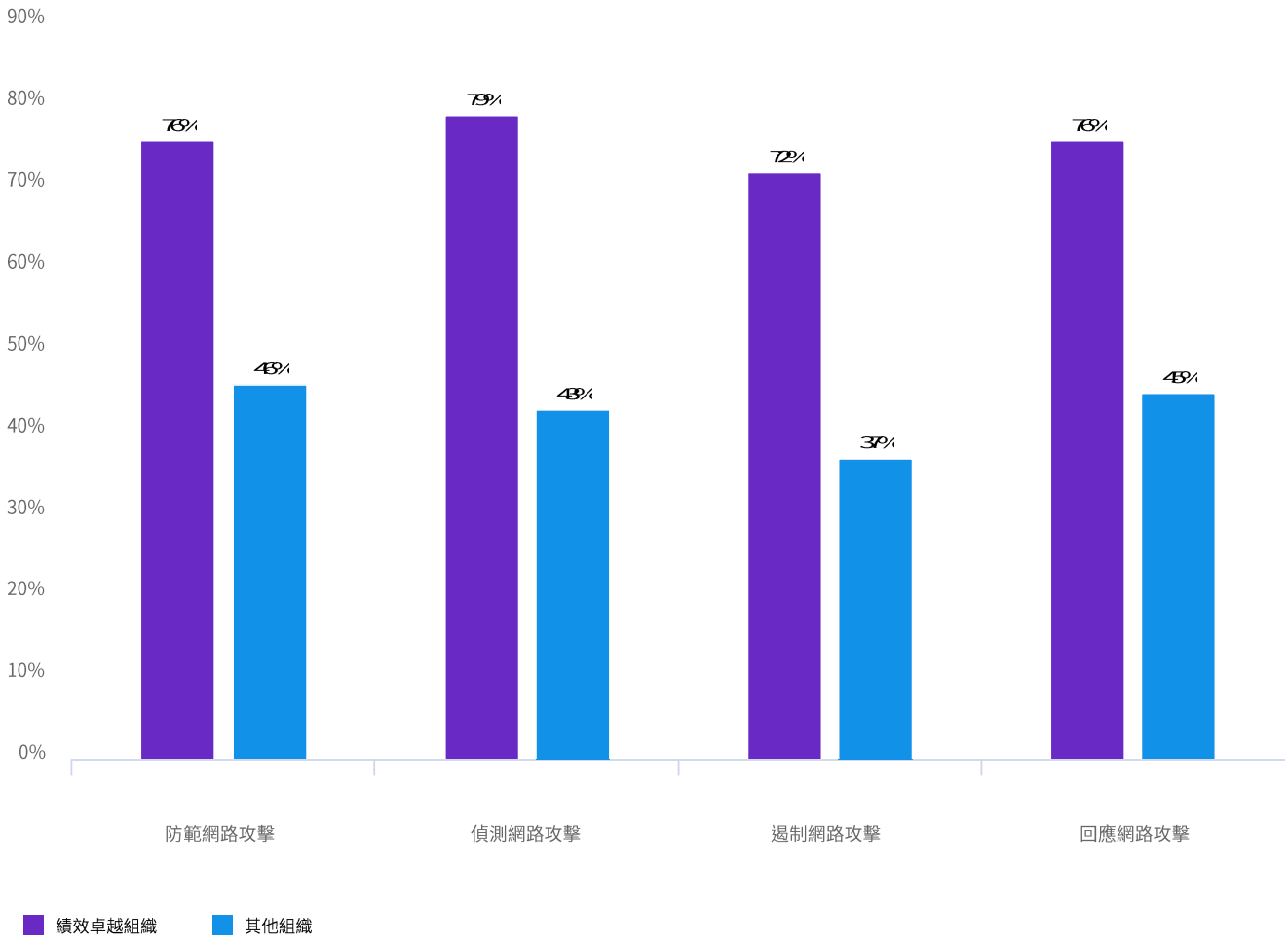


圖 11 顯示了績效卓越組織在網路攻擊方面的置信水準。績效卓越組織與其他組織之間的最大差距在於網路攻擊偵測能力。

圖 12

安全解決方案的數量對事件回應有何影響

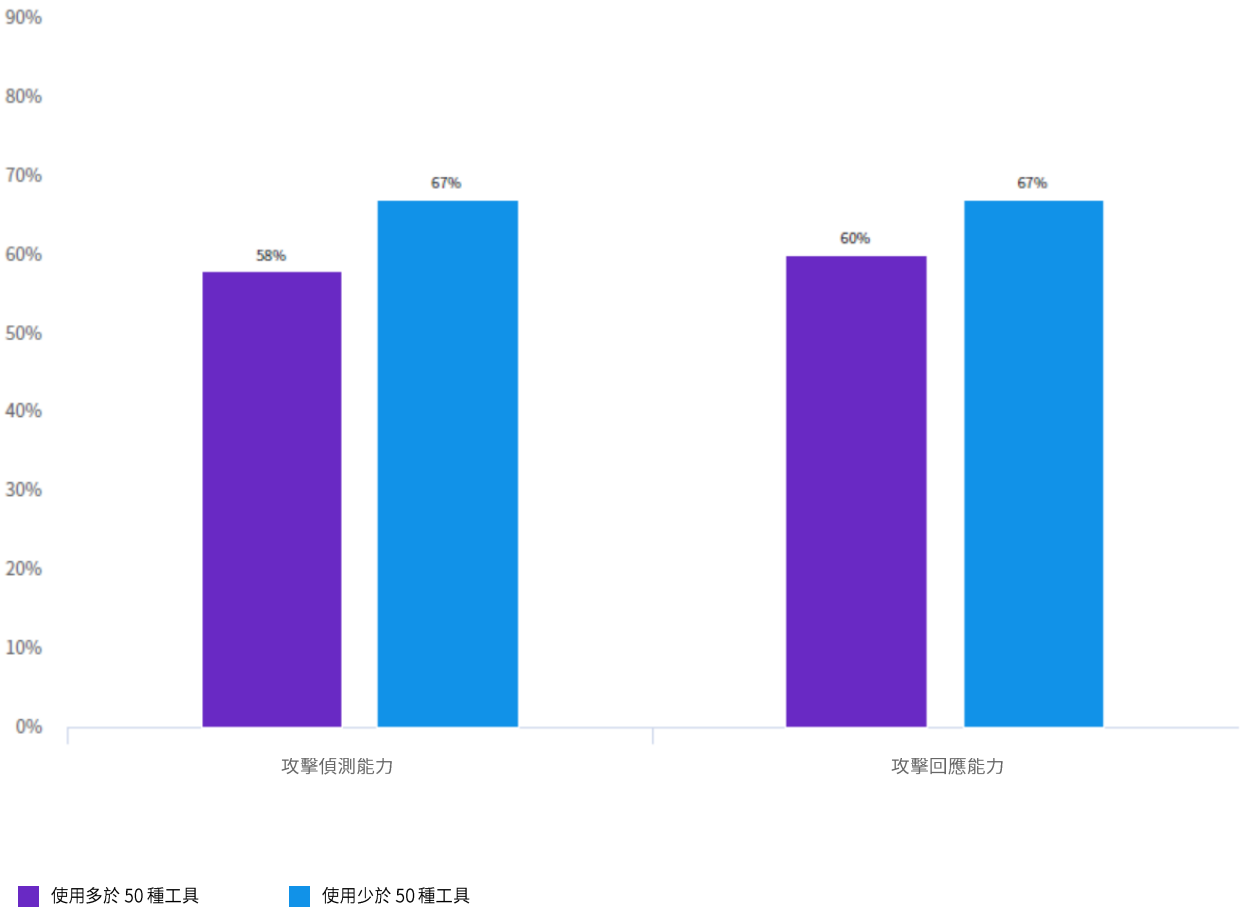


圖 12 顯示了擁有多於 50 種安全解決方案對事件回應能力的影響。使用少於 50 種工具的組織表示，他們處理網路攻擊的能力更強。

圖 13

各個地域的組織使用攻擊特定回應計畫的情況

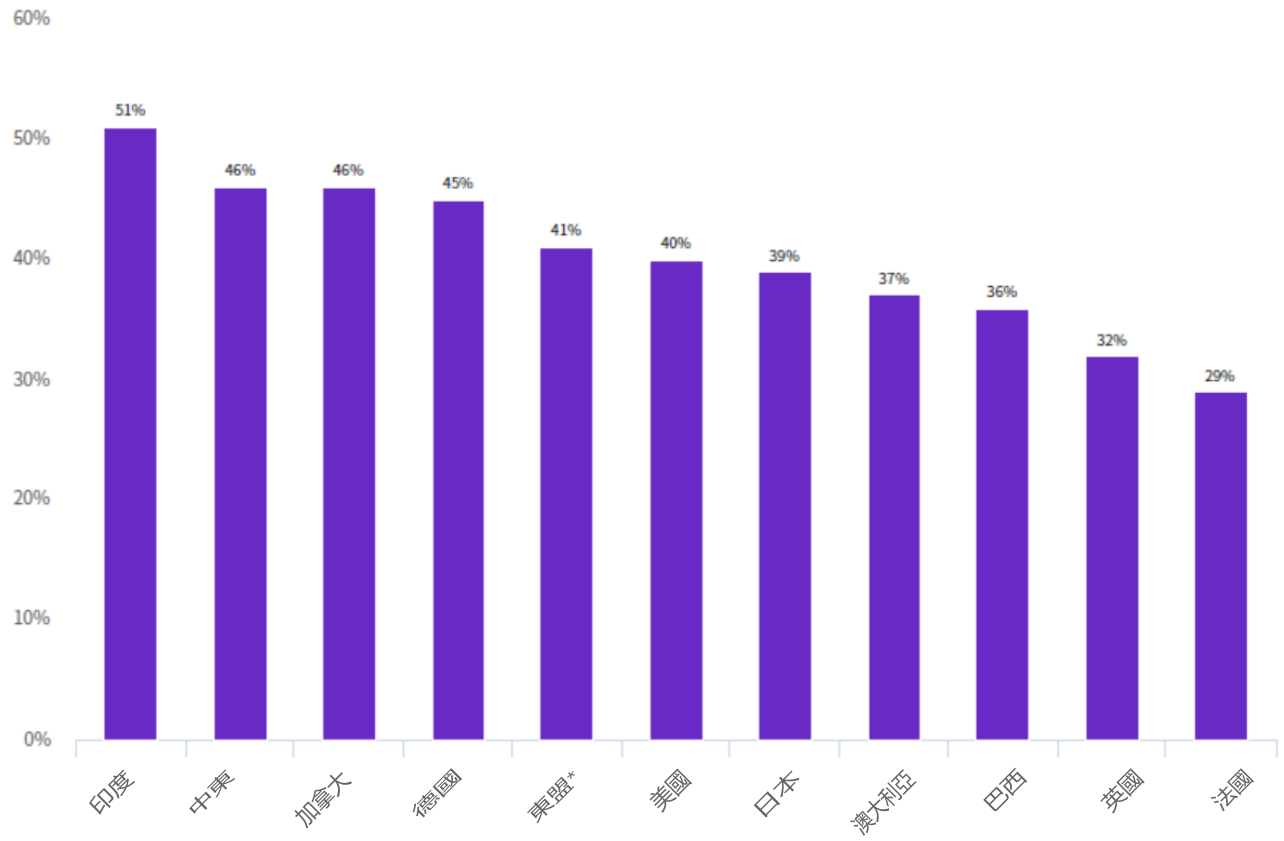


圖 13 顯示了調研中所代表的國家或地區之間的差異。印度組織更有可能針對不同類型的網路攻擊制定具體的回應計畫。英國和法國最不可能制定此類計畫。

·東盟代表了位於新加坡、菲律賓、越南、泰國、馬來西亞和印度尼西亞的受訪者樣本。

**中東代表了位於阿拉伯聯合大公國和沙烏地阿拉伯的受訪者樣本。

圖 14

雲端服務對各個地域的組織實現高水準資安韌性的價值

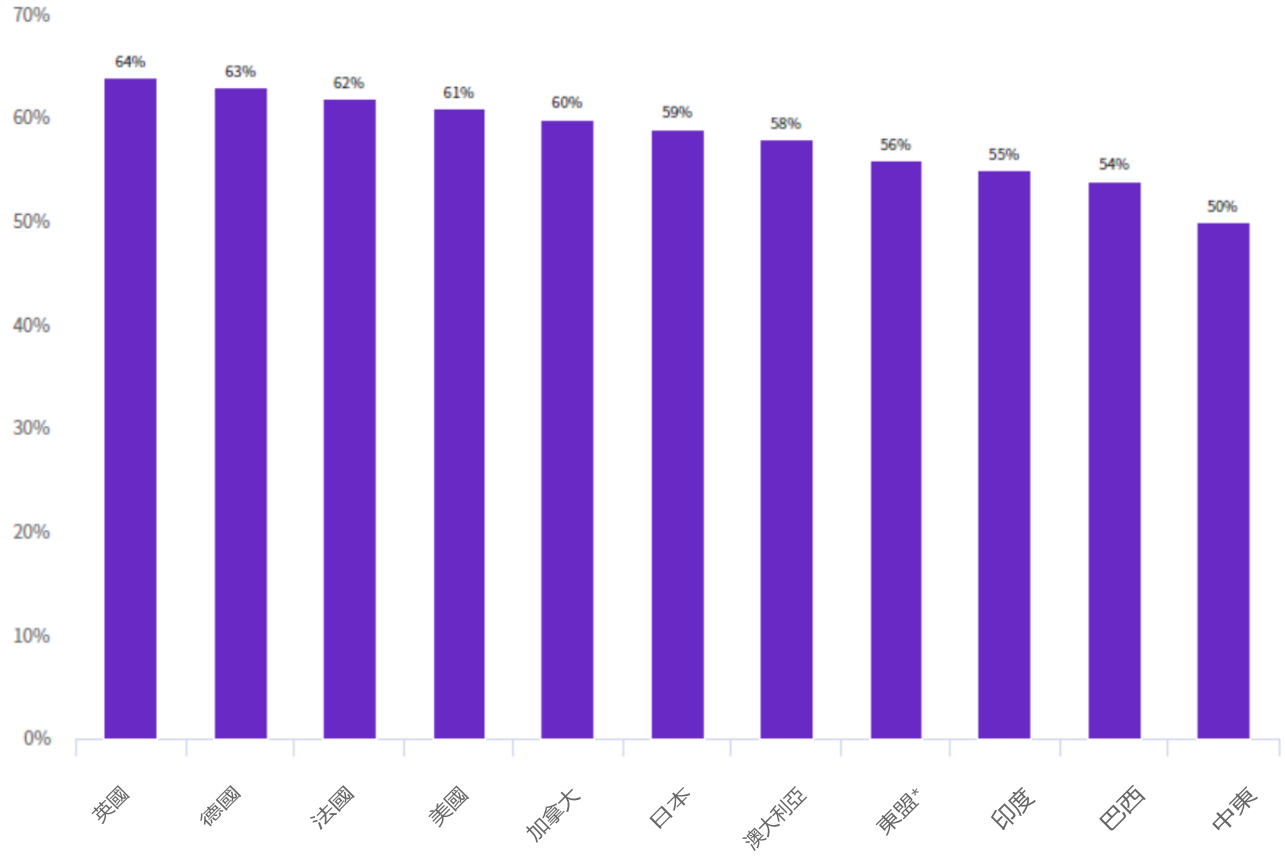


圖 14 顯示了雲端服務對資安韌性的感知影響的區域差異。英國、德國、法國和美國的組織在這方面差距很小。

·東盟代表了位於新加坡、菲律賓、越南、泰國、馬來西亞和印度尼西亞的受訪者樣本。

**中東代表了位於阿拉伯聯合大公國和沙烏地阿拉伯的受訪者樣本。

圖 15

各個產業如何透過使用雲端服務改善資安韌性*

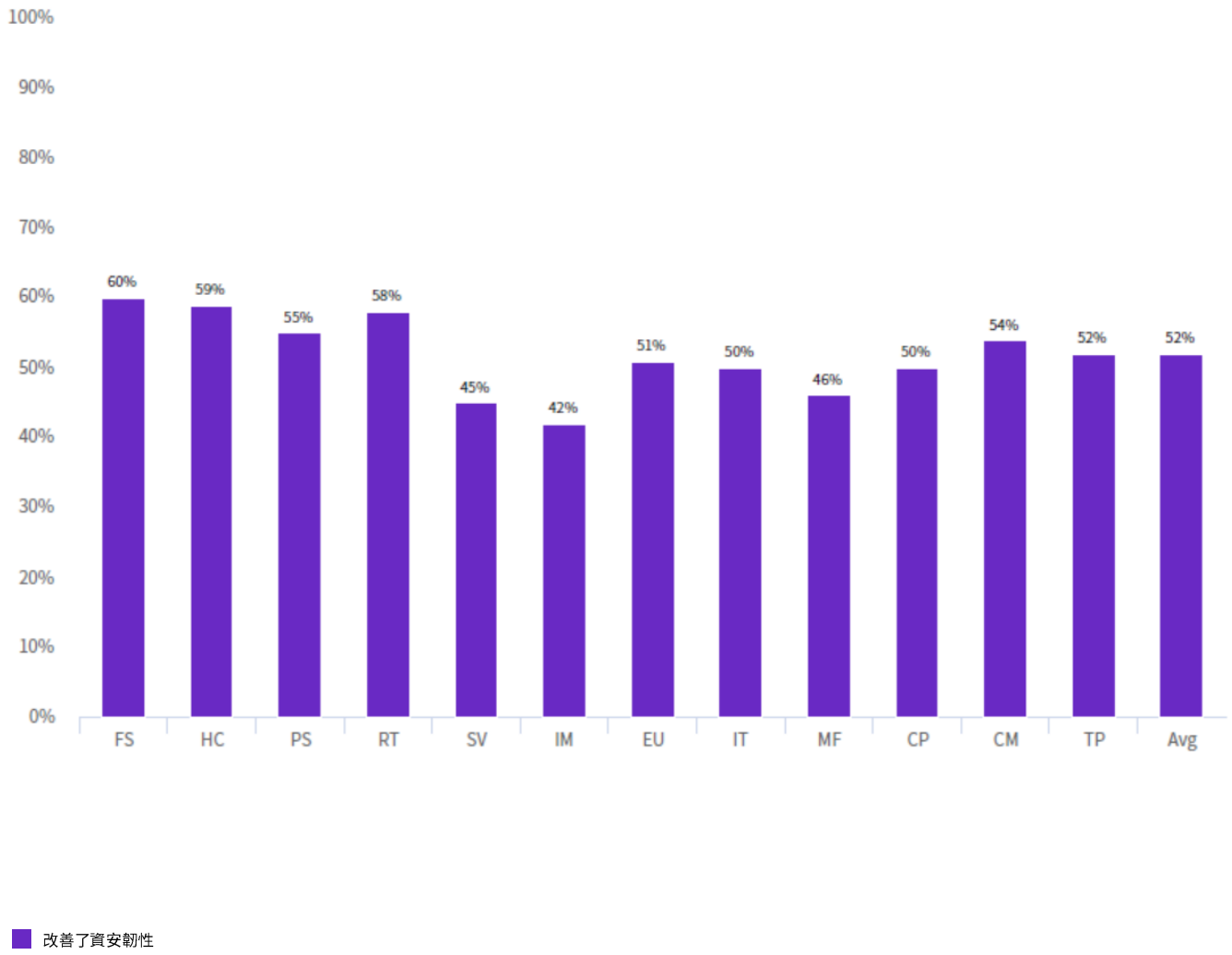


圖 15 顯示了各個產業在使用雲端服務提升資安韌性方面的差異

*產業縮寫：金融服務 (FS)、醫療保健與製藥 (HC)、公共領域 (PS)、零售 (RT)、服務 (SV)、工業 (IM)、能源與公共事業 (EU)、IT 與技術 (IT)、製造 (MF)、消費品 (CP)、通訊 (CM)、運輸 (TP)、娛樂與媒體 (EM)、教育與研究 (ED)、酒店 (HP)、國防與航天 (DF)、農業與食品服務 (AG)、物流與配送 (LD)。有關產業定義的完整清單，請參見第 34 頁。

圖 16

各個產業在 CSIRP 採用方面的差異*

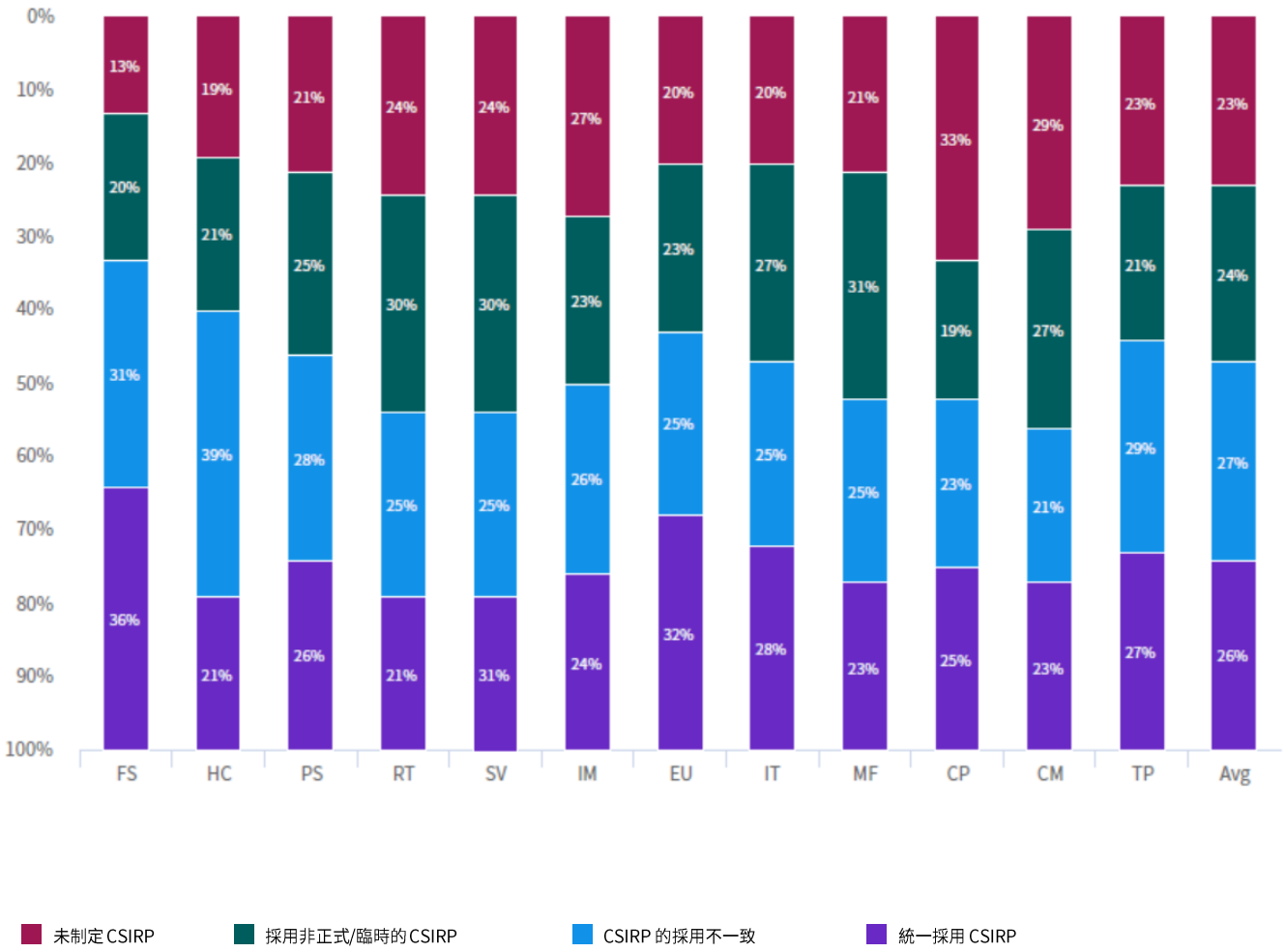


圖 16 顯示了各個產業在 CSIRP 採用方面的差異

*產業縮寫：金融服務 (FS)、醫療保健與製藥 (HC)、公共領域 (PS)、零售 (RT)、服務 (SV)、工業 (IM)、能源與公共事業 (EU)、IT 與技術 (IT)、製造 (MF)、消費品 (CP)、通訊 (CM)、運輸 (TP)、娛樂與媒體 (EM)、教育與研究 (ED)、酒店 (HP)、國防與航天 (DF)、農業與食品服務 (AG)、物流與配送 (LD)。有關產業定義的完整清單，請參見第 34 頁。

圖 17

為網路安全功能提供資金的合理性證明因素

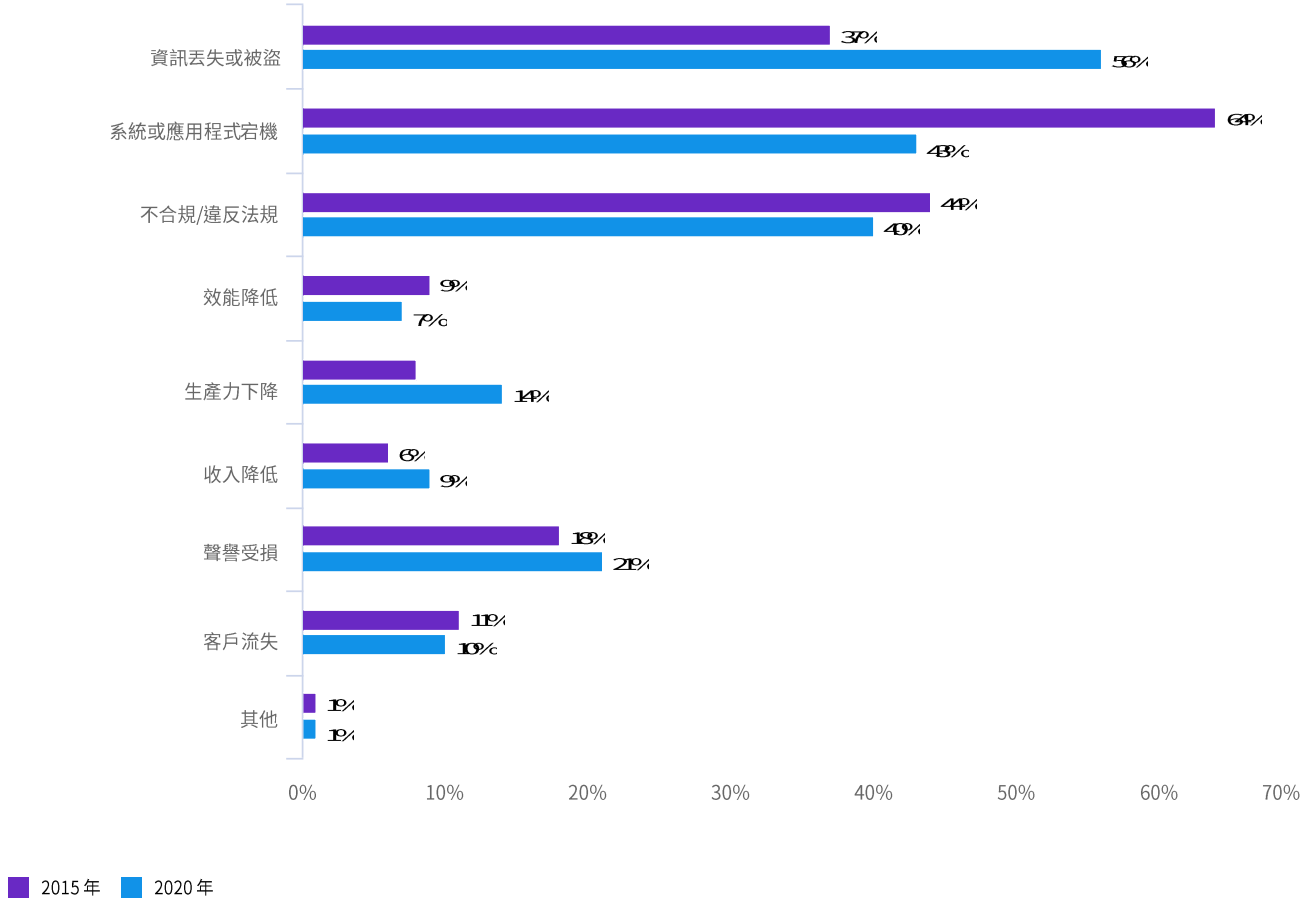


圖 17 顯示了為網路安全提供資金的合理性證明因素。自 2015 年以來，證明預算合理性的因素已從系統或應用程式宕機轉變為資訊丟失或被盜。

圖 18

為確保資安韌性而分配的網路安全預算

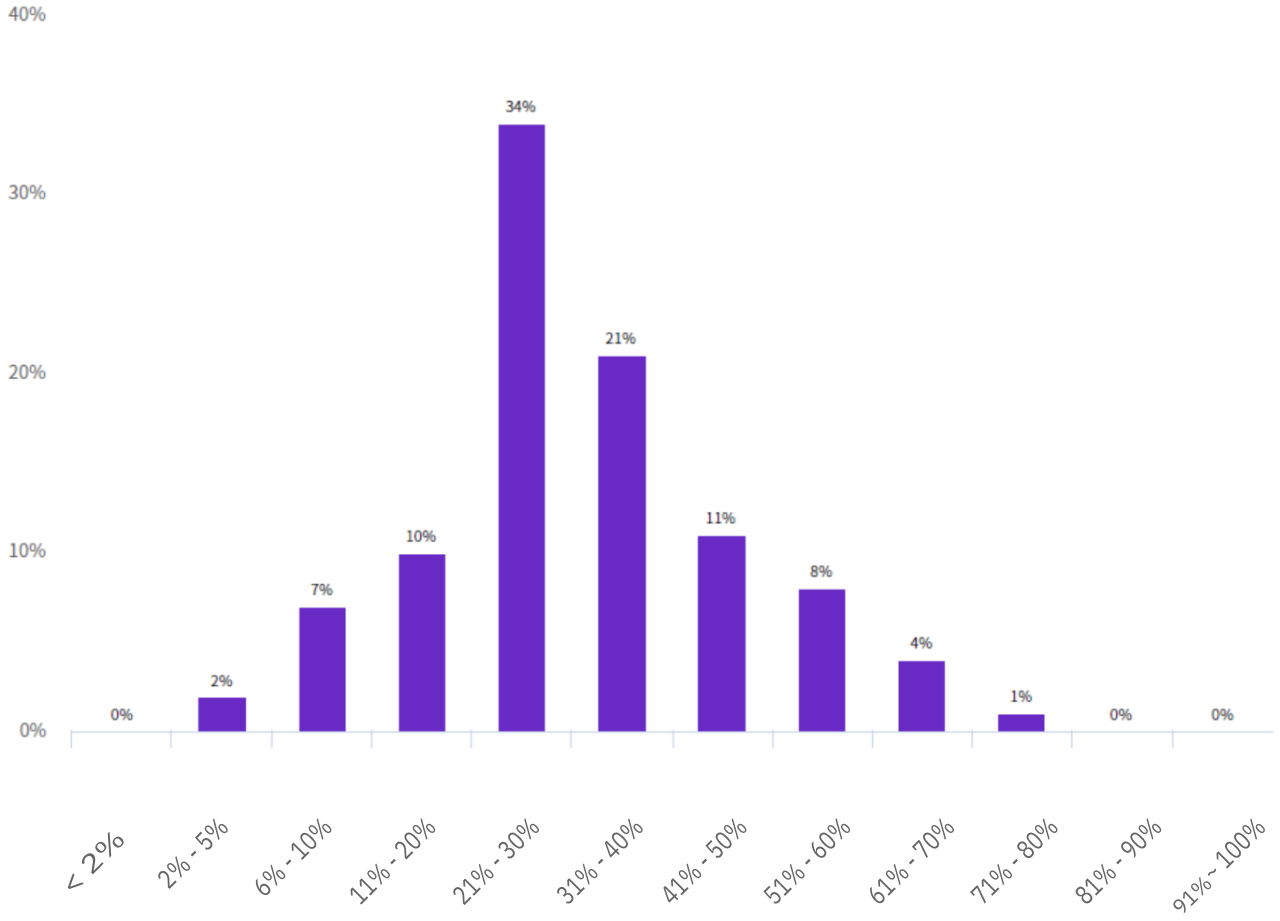


圖 18 顯示了為資安韌性相關活動而分配的預算所占百分比。

組織特性

本 2020 年資安韌性組織報告涵蓋了來自美國、印度、德國、英國、巴西、日本、澳大利亞、法國、加拿大、東盟* 和中東** 的 3,439 位 IT 和安全從業人員的回饋。

所代表的產業

樣本中包括 18 個產業細分。

金融服務
銀行、保險公司、投資公司

醫療保健與製藥醫院、診所和生物醫學生命科學

零售
實體店和網店

製造
大型商品或組件生產商

酒店
酒店、連鎖餐廳、郵輪公司

公共領域
聯邦政府、州政府和當地政府機構與非營利性組織

運輸
航空和鐵路

能源與公用事業
石油天然氣公司、公用事業公司、可替代能源生產商和供應商

消費品消費品製造商和分銷商

物流與配送
貨運和送貨公司、供應鏈管理

工業
化學加工、工程和製造公司

通訊報紙、圖書出版商、公關公司和廣告公司

IT 與技術軟體和硬體公司

服務
專業服務，比如律師事務所、會計師事務所和諮詢公司

娛樂與媒體電影製作、體育、遊戲和賭場公司

農業與食品服務農業，商業食品生產者（植物和牲畜）

國防與航天商業或國防相關飛機和系統的生產商和設計師

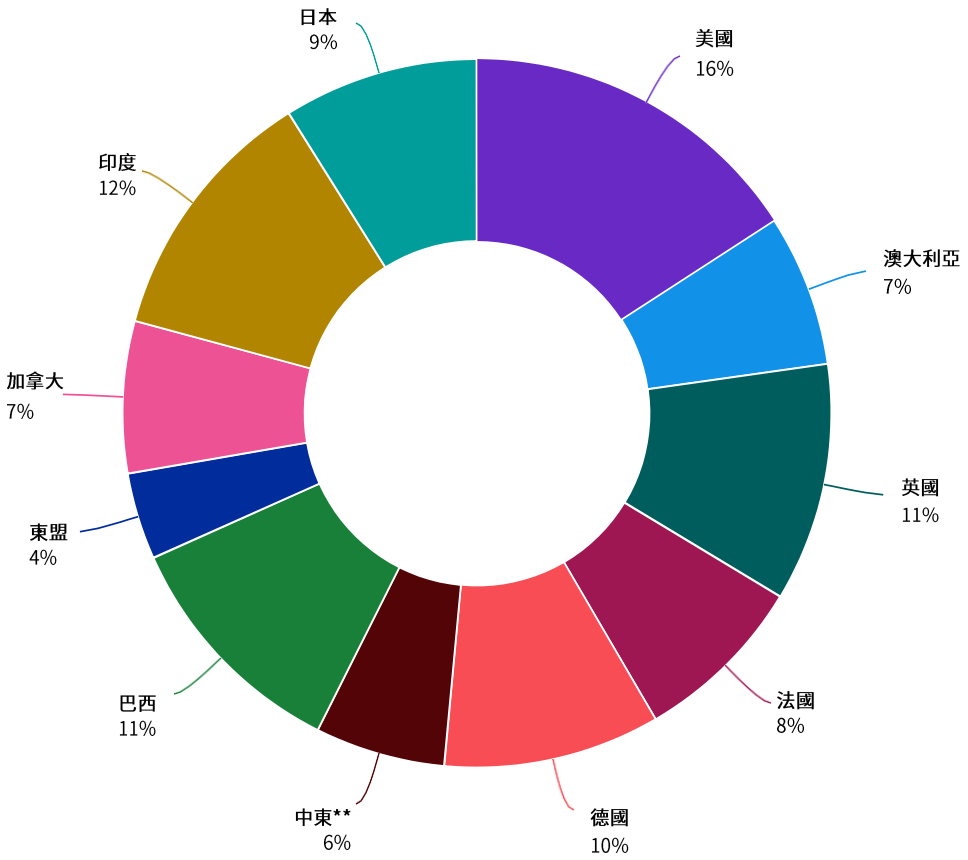
教育與研究
市場研究、智囊團、研發、公立/私立大學與學院、培訓與開發公司

·東盟代表了位於新加坡、菲律賓、越南、泰國、馬來西亞和印度尼西亞的受訪者樣本。

**中東代表了位於阿拉伯聯合大公國和沙烏地阿拉伯的受訪者樣本。

圖 19

樣本分佈（按國家/地區或區域）



·東盟代表了位於新加坡、菲律賓、越南、泰國、馬來西亞和印度尼西亞的受訪者樣本。

**中東代表了位於阿拉伯聯合大公國和沙烏地阿拉伯的受訪者樣本。

圖 20

基準樣本在產業細分中的分佈

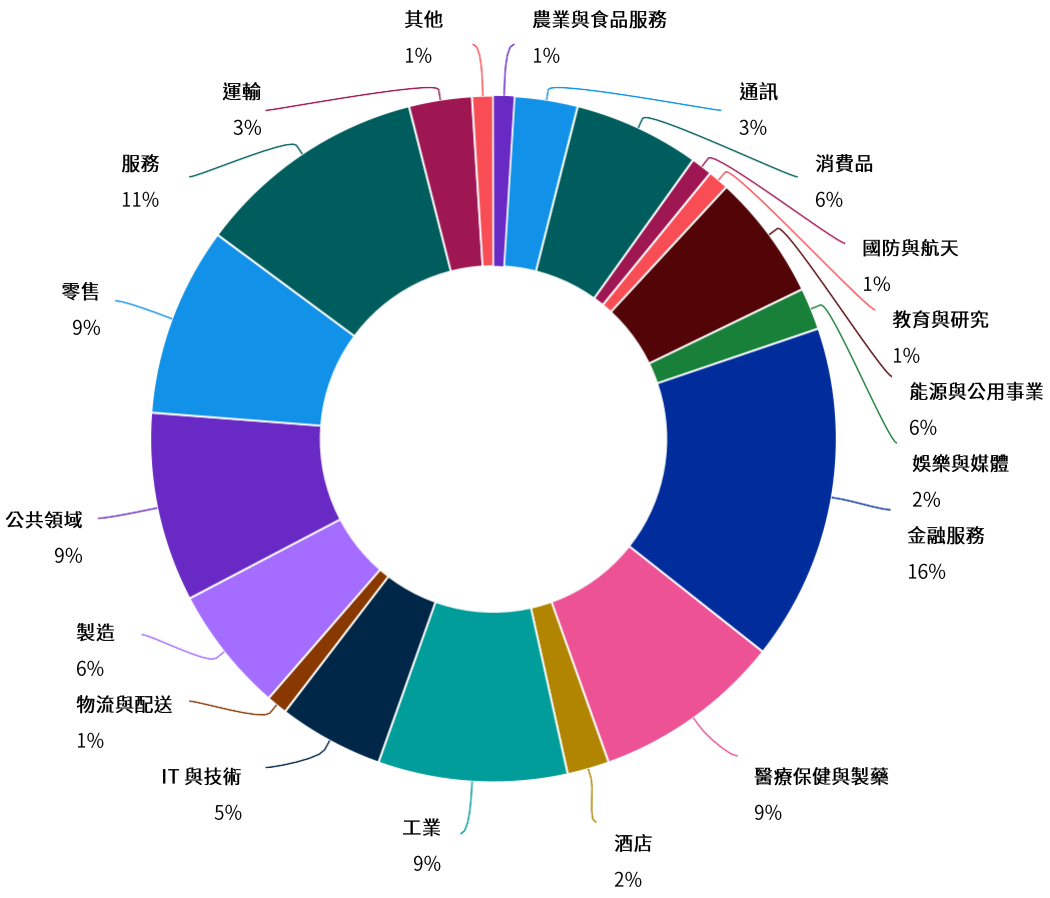


圖 21

按職務分佈情況

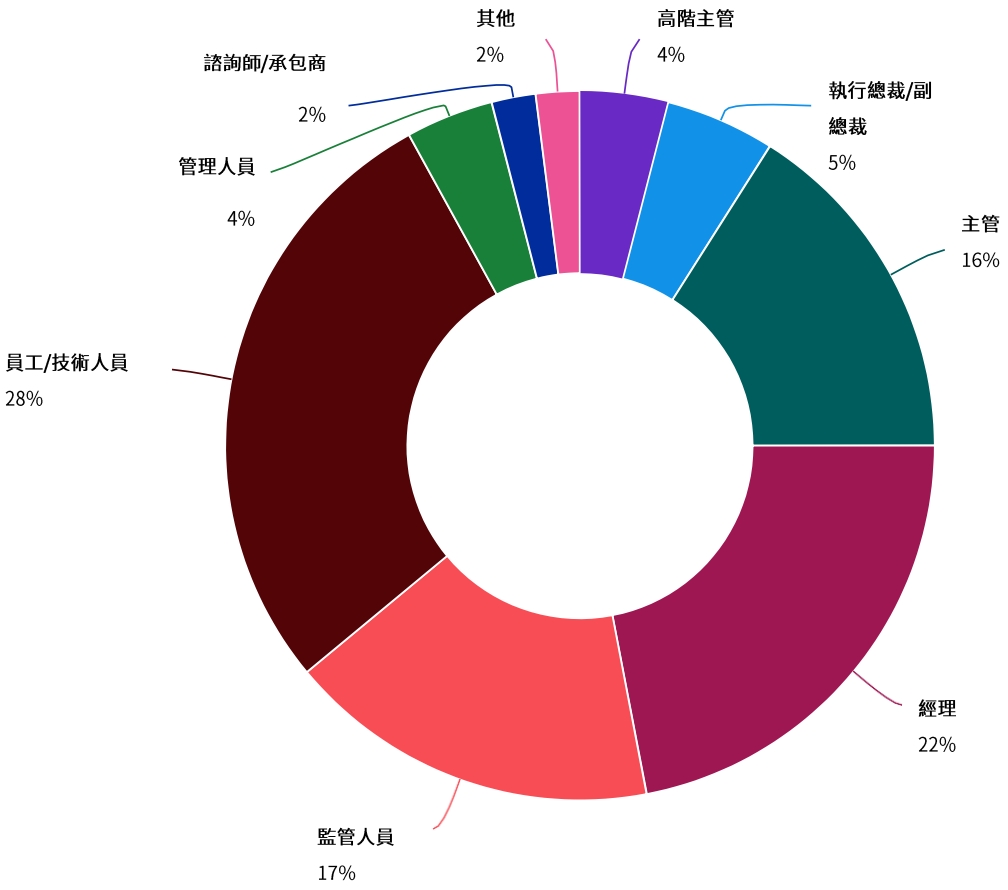
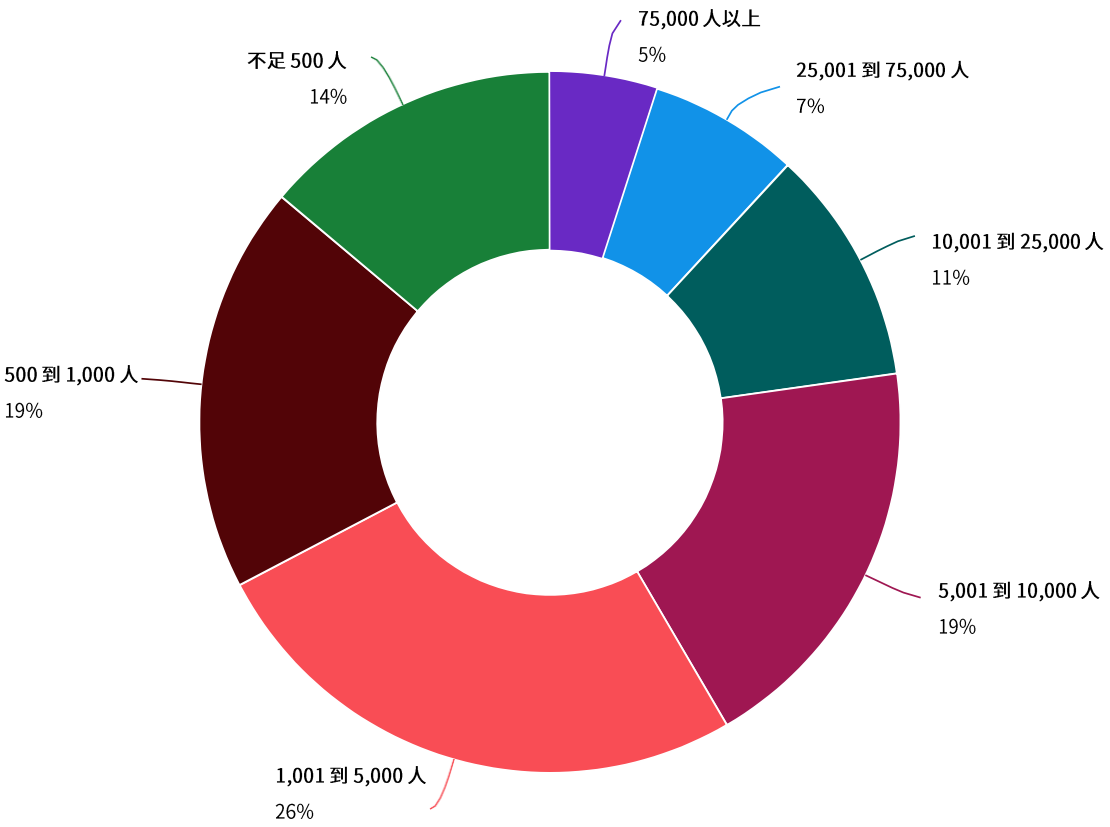

其他
2%
高階主管
4%
諮詢師/承包商
2%
執行總裁/副總裁
5%
管理人員
4%
主管
16%
員工/技術人員
28%
經理
22%
監管人員
17%

圖 22

按公司規模分佈


75,000 人以上
5%
25,001 到 75,000 人
7%
10,001 到 25,000 人
11%
5,001 到 10,000 人
19%
1,001 到 5,000 人
26%
500 到 1,000 人
19%
不足 500 人
14%

調研方法

我們要求來自美國、印度、德國、英國、巴西、日本、澳大利亞、法國、加拿大、東盟和中東的 IT 和安全從業人員完成了在線調查。

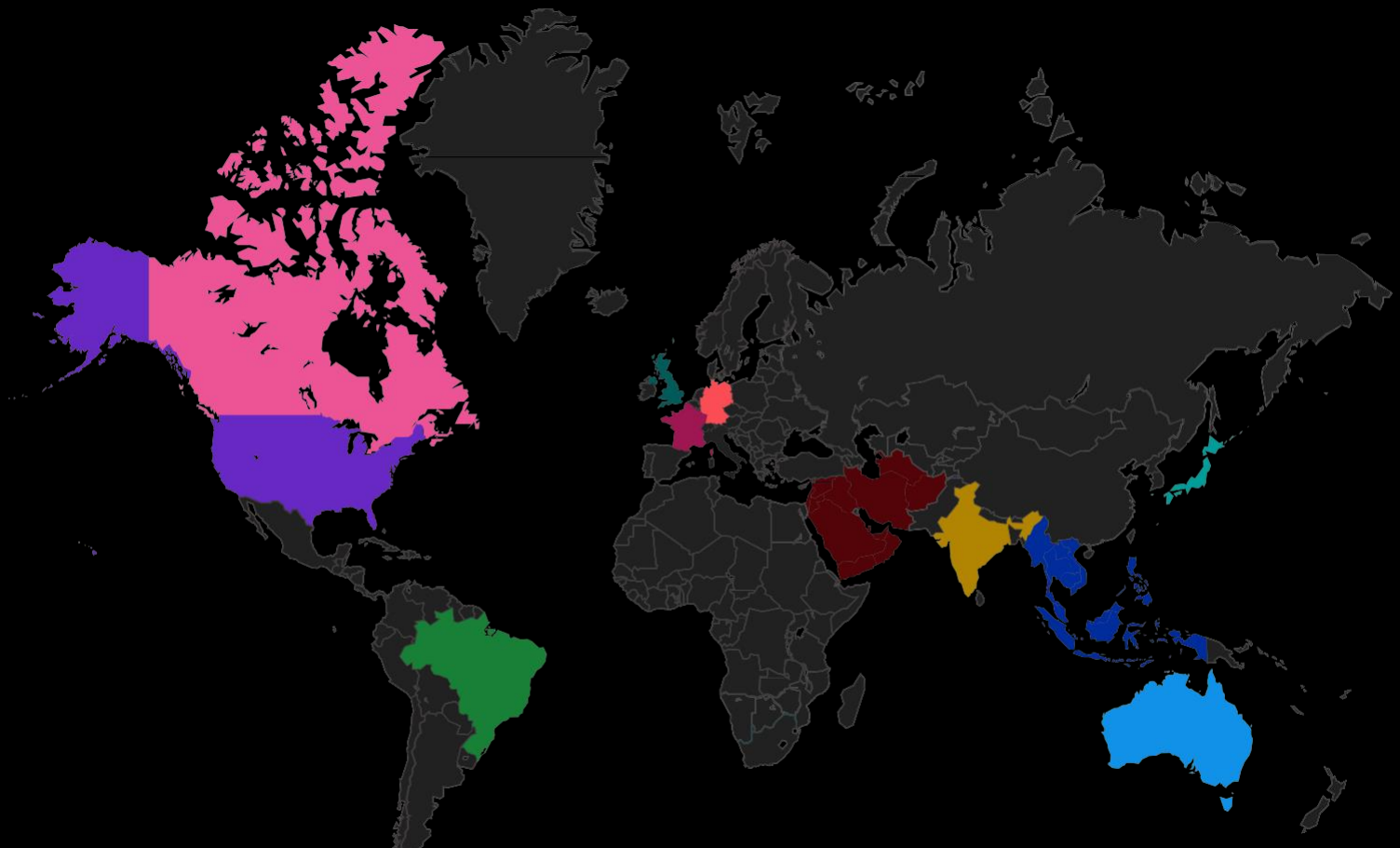
最終樣本由 3,439 位受訪者組成，總回應率為 3.3%。

11

個國家/地區和區域

3,439

名受訪者



東盟代表了位於新加坡、菲律賓、越南、泰國、馬來西亞和印度尼西亞的受訪者樣本。

**中東代表了位於阿拉伯聯合大公國和沙烏地阿拉伯的受訪者樣本。

定義

資安韌性

資安韌性的定義為：在應對網路攻擊的管理、延緩和恢復方面，所體現出的聯合防範、偵測和回應能力。這是指企業面對網路攻擊時保持其核心目標和完整性的能力。具有資安韌性的企業是指能夠防範、偵測、遏制針對資料、應用程式和 IT 基礎架構的各種嚴重威脅並從中恢復的企業。

績效卓越組織

在此次調研中，我們識別出自述其所在組織已實現了高水準資安韌性且能夠更好地緩解風險、漏洞和攻擊的受訪者。我們將這些組織稱為「績效卓越組織」。

研究局限性

此次調研中存在一些固有的限制事項，在根據調研結果作出結論之前，需要對這些事項加以審慎考慮。以下各項是與大多數基於 Web 的調研密切相關的特定限制事項。

無回覆偏差

當前的調研結果基於一些調查結果樣本。在調研中，我們將調查問卷發給具有代表性的個人樣本，最終收到了大量可用的回覆。儘管進行了無回應測試，但仍舊可能出現這樣的情況，即：沒有參與調研的個人的基本信念可能會與完成了調研的個人截然不同。

取樣範圍偏差

準確性基於聯絡資訊以及受訪者清單代表 IT 或 IT 安全從業人員的程度。我們也承認，結果可能會受到諸如媒體報道等外部事件的影響。最後，由於我們使用了基於 Web 的收集方法，因此透過郵件或電話進行的非 Web 回覆可能會導致不同的調研結果模式。

自報告結果

調研的品質高低取決於受訪者是否給出完整、可信的回覆。儘管我們可在調研過程中加入特定的制衡原則，但始終存在一種可能，即調研主體未給出準確的回答。

關於 Ponemon Institute 和 IBM Security

本「資安韌性組織報告」由 Ponemon Institute 和 IBM Security 共同編製。此次調研由 Ponemon Institute 在 IBM Security 的贊助下獨立進行，由 IBM Security 負責分析、報告和發佈。

Ponemon Institute 致力於進行獨立調研和培訓，旨在推動企業和政府中可靠的資訊和隱私管理實務。我們的使命是對可能影響人員和組織敏感資訊的管理和安全性的關鍵問題進行高品質的實證調研。

Ponemon Institute 遵守嚴格的資料保密、隱私和有道德調研標準，不會從個人收集任何個人識別資訊（或在業務調研中出現的公司識別資訊）。此外，我們還執行嚴格的品質標準，確保不會向當事人提出不相關或不適當的問題。

IBM Security 可以提供最先進、整合的企業安全產品和服務組合。此類組合由世界知名的 IBM X-ForceR 研究團隊提供支援，所提供的安全解決方案旨在幫助組織將安全性融入到他們的業務之中，進而在不確定的情勢下實現蓬勃發展。

IBM 營運著全球最廣泛、最深入的安全調研、開發和交付組織。IBM Security 每天在 130 多個國家/地區監控超過 2 萬億次事件，而且 IBM 擁有 3,000 多項安全專利。欲瞭解更多資訊，敬請造訪：ibm.com/security。

如果您對本調研報告有任何疑問或意見，包括如何獲得引用或複製本報告的許可，請透過信函、電話或電子郵件聯絡：

Ponemon Institute LLC

聯絡方式：Research

Department 2308 US 31

North

Traverse City, Michigan

49686 USA

1.800.887.3118

research@ponemon.org

下一步行動

跨多雲端環境整合工具

瞭解更多 →

偵測威脅

瞭解更多 →

編排您的回應流程

瞭解更多 →

補救並恢復

瞭解更多 →

免費咨詢熱線：0800-016-888 按 1

服務時間：9:00-17:00

IBM Corporation
New Orchard Road
Armonk, NY 10504

美國印刷
2020 年 7 月

IBM **Security**