CISCO
SECURE

中小型企業的網路資安：亞太地區企業為數位防禦做好準備

2021 年 9 月

內容

前言

網路資安是我們數位新常態的基礎

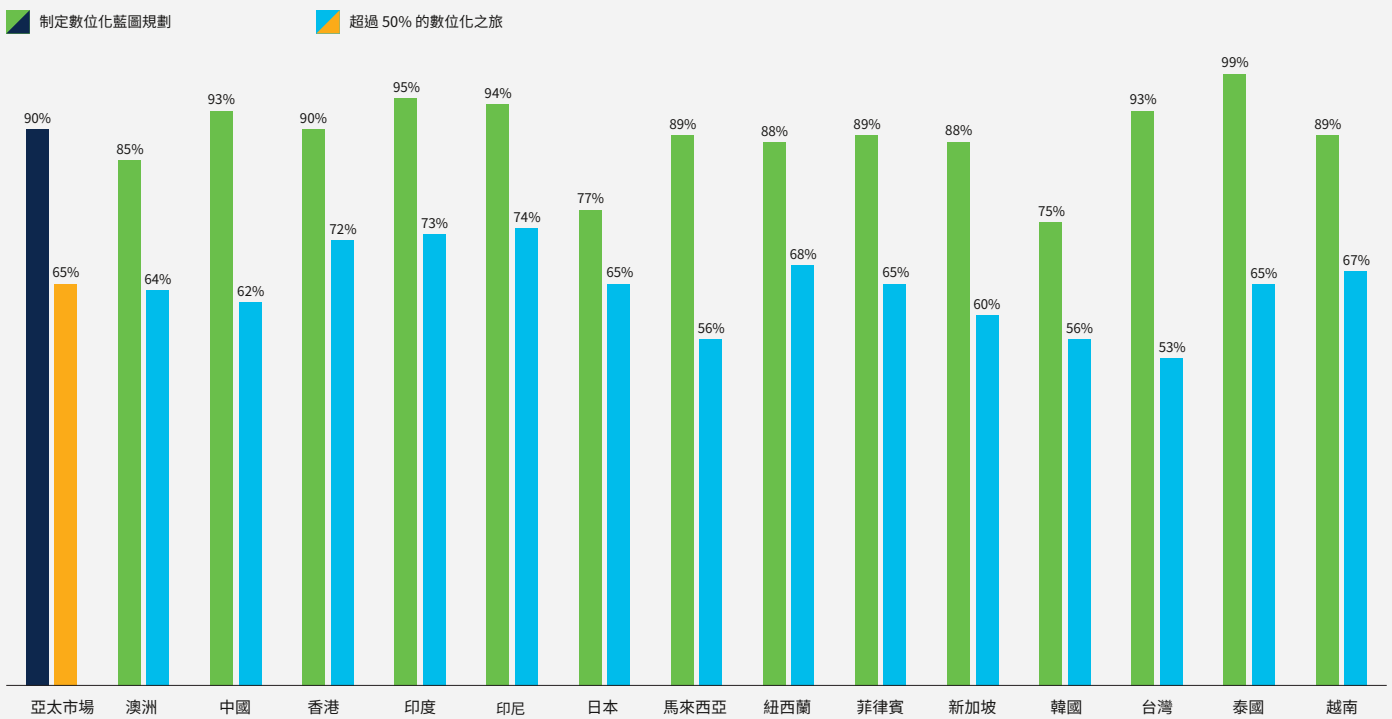
COVID-19 大流行促使各種規模的組織迫切需要投資於技術解決方案和能力。在大流行開始時，企業轉向技術以求生存。目標是即使在整個經濟體陷入封鎖並且大多數勞動力過渡到遠距辦公安排的情況下，仍能營運並繼續為客戶提供服務。親眼目睹了技術可以產生的積極影響，並且隨著各國現在希望逐步重新開放經濟，所有組織都熱衷於利用它在新常態中蓬勃發展。

對於亞太地區的中小型企業 (SMB) 而言尤其如此。我們委託進行了獨立研究，以更好地了解中小型企業的技術趨勢，尤其是與網路資安相關的趨勢。

研究發現，該地區 94% 的中小型企業採用了某種形式的技術。更令人鼓舞的是，絕大多數 (90%) 都有數位化藍圖規劃。泰國99% 有藍圖規劃，而在印度，95% 的中小型企業都有藍圖規劃，這一點尤為突出。不過，在日本和韓國等成熟經濟體中，這一數字略低，分別有 77% 和 75% 的中小型企業表示他們有數位化藍圖規劃或戰略。

在實施方面，65% 的中小型企業在他們的數位化之旅中進展順利，部署了超過 50% 的數位化計劃。印尼、印度和香港特別行政區的中小型企業至少已經走到了一半。相比之下，台灣、馬來西亞和韓國的差距最大。

按市場劃分的 APJC中小型企業數位化進程



隨著該地區中小型企業的數位化步伐加快，網路資安受到越來越多的關注，尤其是因為不法駭客和惡意行為者可用的攻擊面的增加反映了數位化的步伐。與 12 個月前相比，四分之三的中小型企業表示，他們今天更加關注網路資安，這並不奇怪。這很重要。但這也令人鼓舞，因為它表明中小型企業對網路風險的認識水平有所提高。

這些擔憂是有根據的。我們的研究表明，超過一半 (56%) 的亞太地區中小型企業在過去一年中經歷過網路事件，其中許多成為網路犯罪的受害者——85% 的企業遭受了惡意軟體攻擊。由於這些事件，惡意行為者正在獲取有價值的資料，從客戶訊息 (75%)、內部電子郵件 (62%)、員工資料 (61%) 到知識產權 (61%) 和財務詳細訊息 (61%） 。

這對中小型企業產生了切實的影響，62%　的受訪者表示網路事件擾亂了他們的營運，61%　的受訪者表示這導致了收入損失。

此外，57% 的人認為客戶失去了信任，而 66% 的人表示網路事件對公司的聲譽產生了負面影響。雖然無法量化，聲譽的下降和信任的削弱可能會給任何企業帶來災難性的後果。

從積極的方面來看，中小型企業意識到了這一挑戰。事實上，許多企業正在採取更有計劃的方法，通過戰略舉措來解決問題，以了解和改善他們的資安狀況。我們的研究表明，81% 的受訪者在過去 12 個月內對潛在的網路資安事件進行了情景規劃和/或模擬。大多數 (81%) 已製定響應計劃，而 82% 已準備好在需要時推出的恢復計劃。在即將到來的資安結果研究中，我們將深入探討這方面的哪些節奏對資安有更積極的影響。

我們希望這份報告能為亞太地區中小型企業面臨的網路資安挑戰提供有用的見解。隨著該地區的中小型企業為混合工作的未來做準備，員工在辦公室工作和遠距辦公之間徘徊，這為解決網路資安增加了另一層複雜性，我們希望所有閱讀它的人都能從提供的實用建議中受益提高網路準備和恢復能力。

在日益數位化的世界中，它強調了所有中小型企業利用時間和資源來管理和克服網路資安障礙以建立彈性、面向未來並最終取得成功的企業至關重要。

凱瑞・辛格爾頓

常務董事
亞太地區網路資安
日本和中國，思科

蒲田美智子

小型企業增長辦公室負責人
亞太地區，日本和大中華區，思科

比丹・羅伊

董事總經理
商業企業和中端市場部門
亞太地區，日本和大中華區，思科

介紹

本報告介紹並分析了對亞太地區 3,700 多家中小型企業中負責網路資安的業務和 IT 領導者的調查結果。實地工作於 4 月至 2021 年 7 月。

它旨在更深入地了解該地區中小型企業面臨的不斷變化的網路資安挑戰，中小型企業領導者如何進行網路準備，以及改進它的建議。

受訪者來自該地區的 14 個市場，包括澳洲、中國、香港、印度、印尼、日本、紐西蘭、馬來西亞、新加坡、韓國、台灣、泰國、菲律賓和越南。

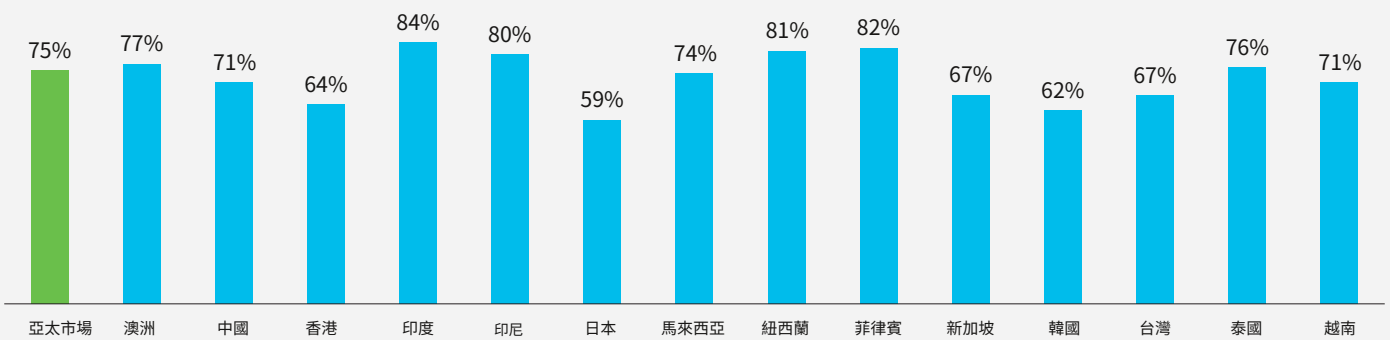
接受調查的中小型企業代表了廣泛的行業，包括商業服務；建造; 教育; 工程; 設計與建築；金融服務; 食品和飲料; 衛生保健; 製造業; 媒體與通訊；自然資源; 個人護理服務；專業的服務; 房地產; 零售; 技術服務；旅行; 運輸; 和批發。

(IN)secure 關於資安

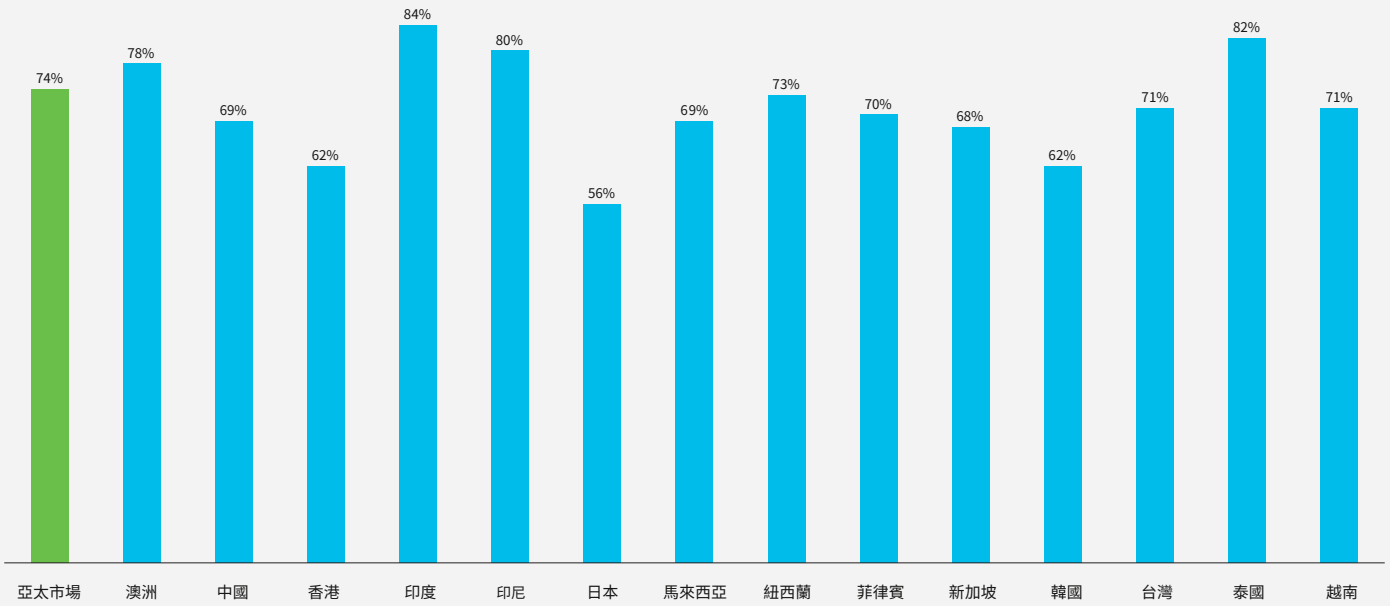
隨著商業環境的快速發展，網路威脅格局在過去一年也發生了顯著變化。這使得該地區的中小型企業更加擔心網路資安風險。該地區四分之三 (75%) 的中小型企業表示，他們現在比 12 個月前更擔心網路資安，其中最擔心的是印度(84%)、菲律賓 (82%) 和紐西蘭 (81%) 的中小型企業)、印尼 (80%) 和澳洲 (77%)。

部分原因是人們越來越意識到嚴重事件可能對其業務產生的影響。四分之三 (74%) 的接受調查的中小型企業領導人表示，一次重大網路事件可能意味著他們組織的終結。

相較 12 個月前，如今更擔心資安問題的中小型企業百分比



認為嚴重的網路事件可能導致其業務中斷的中小型企業之百分比



中小型企業也越來越意識到最大的威脅來自哪裡。該研究強調，網路釣魚被該地區的中小型企業視為最大的威脅，43% 的企業將其列為第一。網路釣魚是一種策略，不法駭客偽裝成可信賴的實體，試圖讓用戶打開發送給他們的特定數位訊息，例如電子郵件、或即時消息。儘管這是一種古老的策略，但由於其簡單性和有效性，它仍然很受歡迎。

與此同時，由大流行引發的快速發展的環境使中小型企業的營運方式發生了巨大變化。隨著向遠距辦公的大規模轉變，相當大比例的員工正在連接到公司的網路並從辦公室外連接訊息。許多人也在使用個人設備來這樣做。中小型企業強調，不安全的筆記本電腦（20%　排名第一）、惡意行為者的針對性攻擊（19%排名第一）和個人設備（12% 排名第一）是對其整體安全性的最大威脅。

您認為以下哪一個項目會為您的組織帶來最大的網路攻擊風險？

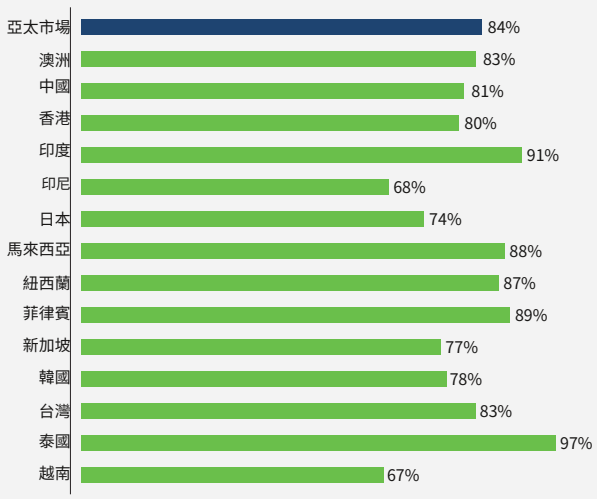
暴露和受到攻擊

中小型企業表達的擔憂是有根據的。亞太地區超過五分之四 (84%) 的中小型企業感到面臨網路威脅，三分之一的人感到非常暴露。這尤其是因為許多中小型企業都經歷過網路事件。我們的研究表明，56% 的亞太地區中小型企業在過去 12 個月內遭遇過網路事件。

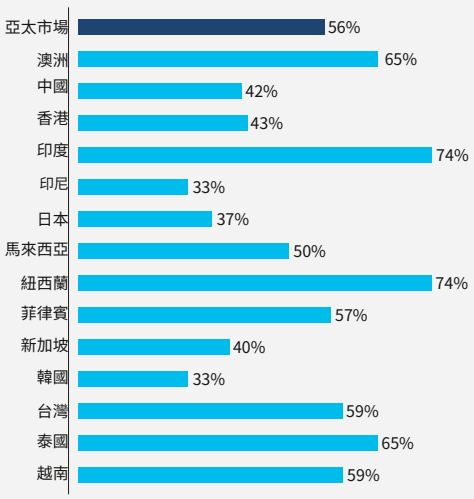
不過，該地區的數字各不相同，印度和紐西蘭 74% 的 SMB遇到了事故，而印尼和韓國祇有 33% 和日本的 37%表示他們遇到了事故。

此外，近一半的受訪者表示，他們在大流行期間經歷的網路事件有所增加，印度 (70%) 和紐西蘭 (61%) 的上升幅度最大，其次是菲律賓 (53%)、越南 (53%) 和澳洲(50%)。

感覺受到網絡威脅的中小企業百分比



在過去 12 個月內遭受網絡事件的中小型企業百分比

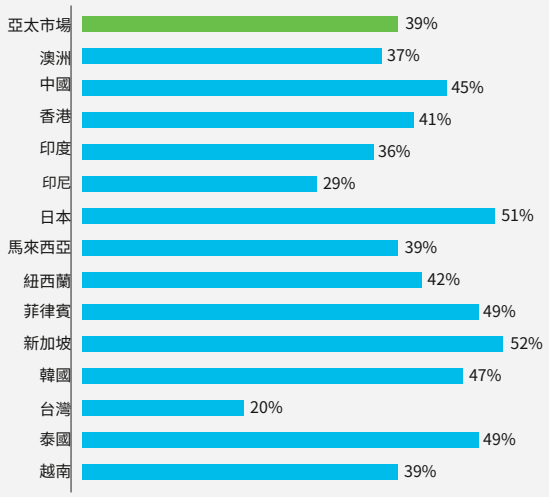


在遭受網路事件的人中有三分之一 (33%) 將沒有網路資安解決方案列為首要原因。不過，更有說服力的是，更多的中小型企業 (39%) 表示，首要因素是他們的網路資安解決方案不足以檢測和預防攻擊。這凸顯了一個事實，即擁有正確的技術對於建立強大的資安態勢至關重要。這也是 Cisco 的一個重要發現與資安結果研究它還深入研究了中小型企業領域。

在經歷過事件的那些中，SMB 看到了攻擊者試圖滲透其系統的無數不同方式。影響了 85% 的中小型企業的惡意軟體攻擊位居榜首。

隨著電腦、平板電腦和智慧手機等設備的普及和使用，攻擊者越來越多地嘗試在這些系統上部署惡意軟體。

認為網路資安解決方案不足以檢測和預防攻擊是遭受網路事件影響的首要因素之百分比



中小型企業尤其成為攻擊者的目標，他們希望部署惡意軟體，目的是破壞或未經授權連接目標設備。

攻擊者對中小型企業的興趣可歸因於幾個關鍵方面。首先，不法駭客社群普遍認為；與大型組織相比，中小型企業在網路資安方面的實力相對較弱，這使它們成為有吸引力的目標。其次，中小型企業越來越多地以某種形式與大公司合作。不法駭客的希望是，如果他們能夠滲透到特定中小型企業的網路，他們就可以將其用作跳板，然後藉此連接該中小型企業可能正在工作或進行數位交易或數位化的大公司的網路與通訊。

據受訪者稱，惡意軟體攻擊之後是網路釣魚，70%　的受訪者表示他們經歷過此類攻擊。受訪者報告的其他主要攻擊形式包括　DNS　隧道　(68%)、拒絕服務　(64%)、SQL注入(62%)、中間人(61%)和零日漏洞(60%).

定義

拒絕服務攻擊：試圖關閉機器或網路，使其目標用戶無法連接，通常是銀行、媒體公司或政府組織的網路伺服器

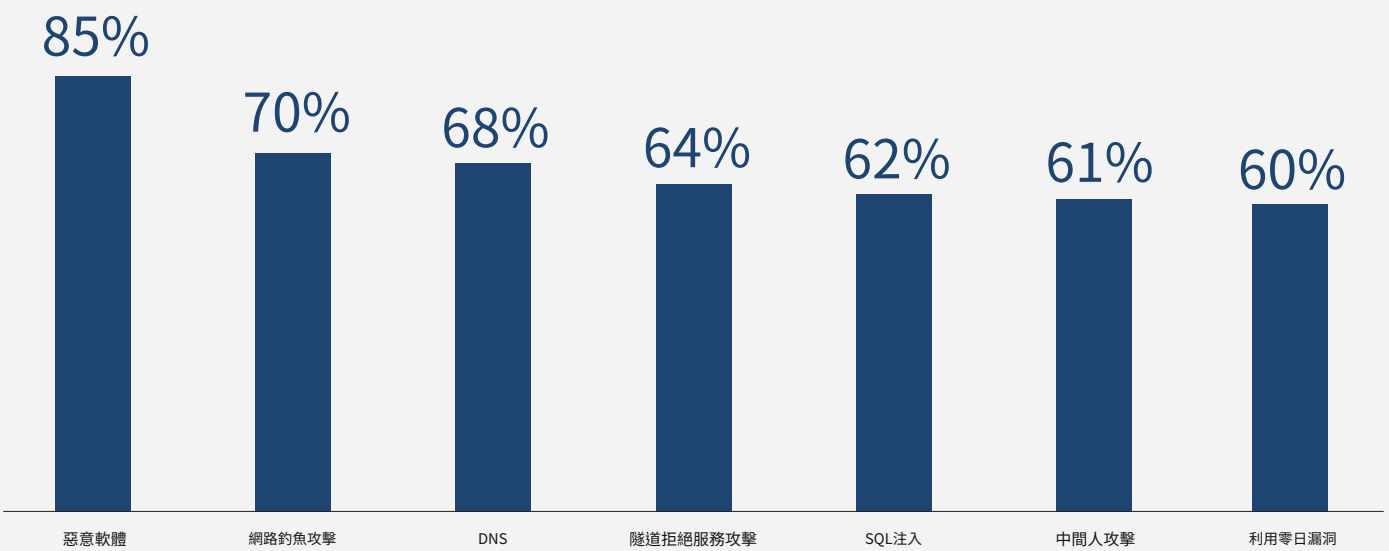
DNS隧道：在 DNS 查詢和響應中對其他程式或協議的資料進行編碼

SQL注入：用於攻擊資料驅動的應用程式，其中將惡意 SQL 語句插入到條目字段中以供執行（例如將資料庫內容轉儲給攻擊者）

中間人攻擊：當犯罪者將自己置於用戶和應用程式之間的對話中，使其看起來好像正在進行正常的訊息交換，目的是竊取個人訊息

零日漏洞利用：攻擊最近發現的軟體漏洞以竊取資料或造成損害

APJC 中小型企業在過去 12 個月中經歷的網絡事件類型



計算成本損失

大多數遭受事故的中小型企業都遭受了某種損失。
高達 75% 的中小型企業經歷過事故，表示這導致客戶資料丟失。每 10 家遭遇事故的中小型企業中就有 6家表示這對他們的收入產生了負面影響。

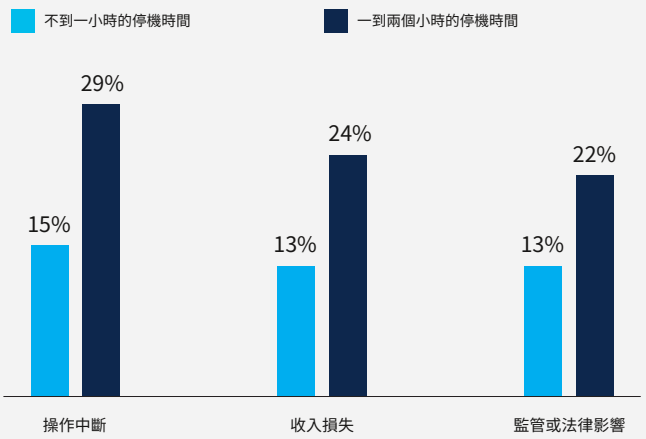
當涉及到對業務的影響時，每一秒都很重要

網路資安是一種賠率遊戲。然而，現實情況是，可能性有利於惡意行為者。他們不斷地攻擊他們的目標。那些受到攻擊的人每次都需要獲勝。另一方面，攻擊者只需一次突破防禦即可獲勝。

更重要的是，公司確實需要一些時間來檢測、調查和補救網路事件。這通常為惡意行為者提供了一種能夠造成損害的先機。

中小型企業現在面臨的挑戰是，我們生活在一個高度連接、數位優先的世界中，客戶想要即時滿足。這意味著他們幾乎沒有餘地，如果有的話，網路資安事件會破壞他們的營運。他們需要能夠盡快檢測、調查、阻止或補救任何網路事件。

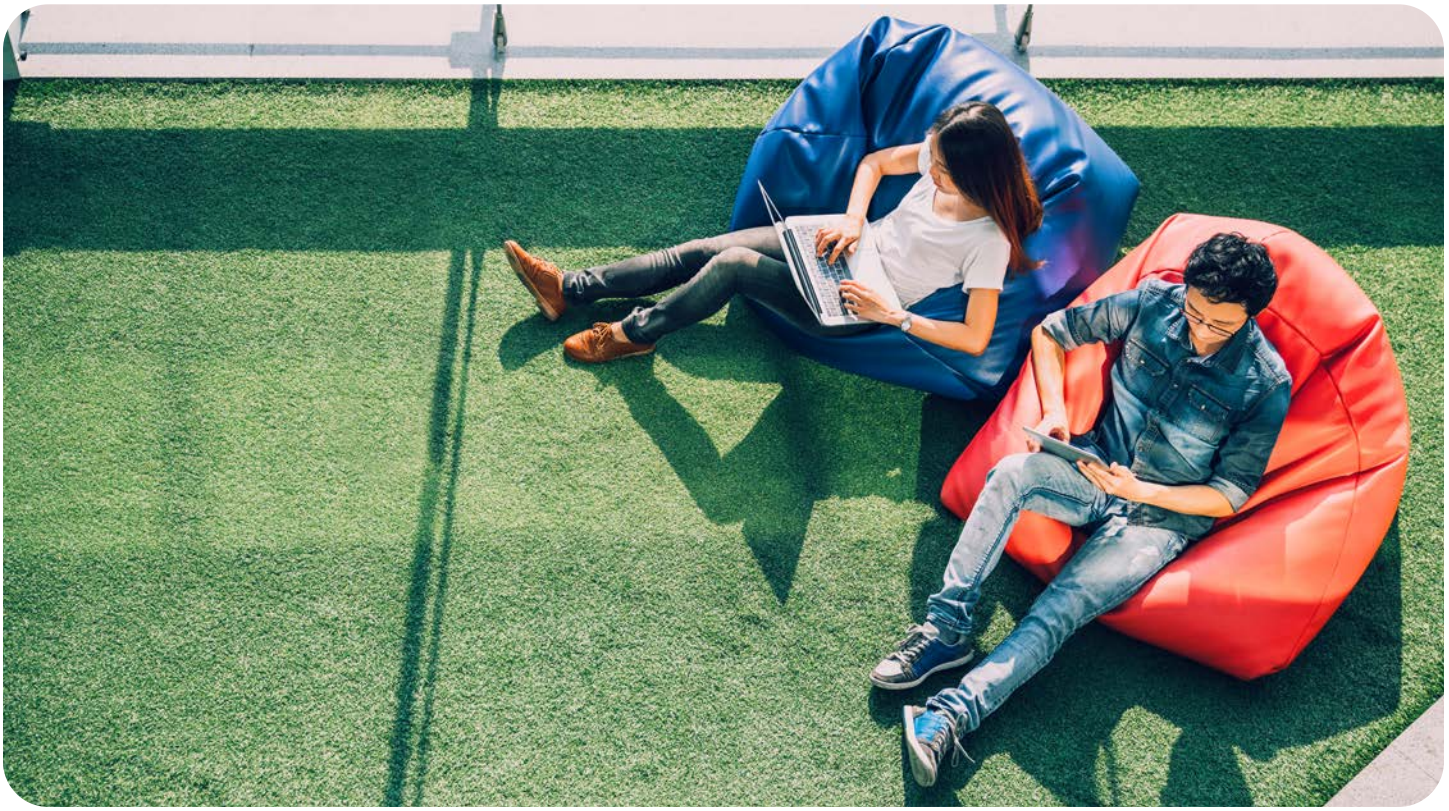
由於停機時間過長造成的影響升級*



* 有關這些指標的全市場細分，請參閱附錄 A 中的圖表

研究強調，亞太地區 15% 的中小型企業表示，即使不到一小時的停機時間也會導致營運中斷，而 29% 的中小型企業表示，1到 2 小時的停機時間也會導致同樣的情況。影響可以量化，因為 13% 的受訪者表示停機時間少於一個小時會嚴重影響收入，而 24% 的人表示 1 到 2 小時的停機時間也會造成同樣的影響。

最能說明問題的是，十分之一的中小型企業表示，一天的停機時間將導致其組織關閉。



同時，隨著各國開始引入和實施網路資安指導方針和法規，網路事件造成的停機時間也會產生法律影響。這種趨勢已經開始出現，13% 的中小型企業表示不到一小時的停機時間會對他們產生法律影響，而 22% 的中小型企業表示 1 到 2 小時的停機時間會導致同樣的問題。

只有 15% 的受訪者表示他們可以在一個小時內檢測到網路事件，這一事實突顯了這對中小型企業來說是多麼大的挑戰。可以在一小時內修復它的數量甚至更低，只有 10%。

% 中小型企業以及檢測和修復事件所用的時間長度

	亞太市場	澳洲	中國	香港	印度	印尼	日本	馬來西亞	紐西蘭	菲律賓	新加坡	韓國	台灣	泰國	越南
檢測事件所需的平均時間															
不到一小時	15%	8%	13%	11%	17%	17%	16%	17%	24%	9%	8%	11%	25%	13%	8%
一到兩個小時	30%	28%	36%	28%	34%	31%	18%	32%	28%	28%	16%	34%	16%	33%	33%
修復事件所需的平均時間															
不到一小時	10%	6%	8%	3%	12%	12%	9%	12%	11%	9%	5%	4%	16%	7%	3%
一到兩個小時	23%	20%	31%	26%	23%	27%	13%	21%	17%	22%	21%	18%	21%	26%	24%

考慮到反應遲緩可能對企業產生的影響，對事件的反應速度變得至關重要。

中小型企業不得不應對的不僅僅是收入損失。網路事件也對整體貨幣產生影響。該地區超過一半 (51%) 在過去 12 個月遭受網路事件的中小型企業表示，這些事件使企業損失了 50 萬美元或更多，13% 表示成本超過 100 萬美元。

事實上，大多數遭受事故的人都看到了金錢上的影響。總體而言，83% 的受訪者表示事故的成本超過 100,000 美元。

還有無形成本。在過去一年遭受過事故的人中，57% 的人表示這導致客戶失去信任，而 66% 的人表示這對他們的聲譽產生了負面影響。雖然無法量化，但聲譽的下降和信任的削弱可能會給任何企業帶來災難性的後果。

過去 12 個月網絡事件的財務影響（美元）

	亞太市場	澳洲	中國	香港	印度	印尼	日本	馬來西亞	紐西蘭	菲律賓	新加坡	韓國	台灣	泰國	越南
500,000 美元或更多	51%	64%	41%	39%	62%	43%	49%	32%	62%	28%	51%	58%	27%	47%	30%
100 萬美元或更多	13%	33%	3%	10%	13%	12%	6%	6%	18%	10%	11%	10%	2%	28%	4%

做好準備戰勝恐懼

儘管他們擔心網路事件的實際影響，但該地區的中小型企業並沒有簡單地放棄並準備與之抗爭。他們從規劃和培訓開始，81% 的受訪者表示他們已經完成了情境規劃與模擬。

逼真的情境規劃和模擬是網路準備的一個關鍵特徵，尤其是因為它可以幫助中小型企業在攻擊者利用它們之前發現其資安態勢中的弱點。在該地區開展模擬演練的中小型企業中，85% 表示他們發現了網路防禦方面的弱點或問題。

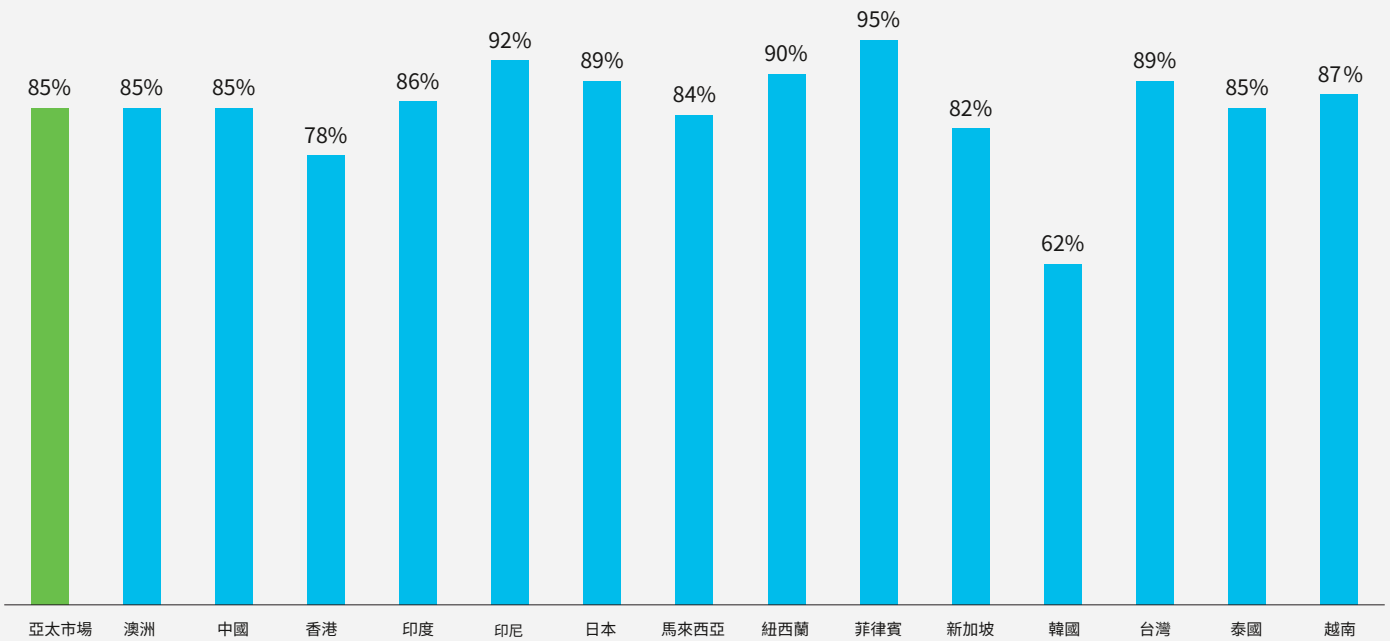
在發現弱點的那些人中，95% 的人表示演習揭示了沒有合適的技術解決方案來檢測網路攻擊或威脅的問題。相同數量的人發現他們擁有太多技術並且難以將它們整合在一起，而96% 的人發現他們沒有正確的技術解決方案來阻止攻擊。

很大一部分人還認識到他們應對網路攻擊的流程不明確 (94%)。與此同時，95% 的受訪者表示，雖然他們擁有合適的技術，但他們沒有足夠的具備合適技能的員工來利用這些技術。

令人鼓舞的是，大約一半的中小型企業能夠在兩週內解決其情境規劃中發現的差距或問題。唯一的例外是中小型企業發現問題是沒有合適的技術來檢測攻擊或威脅，而大多數情況下需要更長的時間來解決。

雖然該地區的中小型企業正在採取正確的步驟進行情景規劃，以在網路資安方面變得更具彈性，但在其他領域仍有工作要做。其中最重要的是教育所有利益相關者。近五分之一 (17%) 表示他們的領導者對當地網路資安法律和監管要求的了解有限。這種知識差距在紐西蘭 (30%)、香港 (29%)、日本 (28%) 和韓國 (27%) 中更為突出。

您的網路資安情境規劃與模擬是否發現了網路防禦中的弱點（回答「是」的百分比）



調整投資並使其發揮作用

中小型企業還確保他們通過投資支持他們的準備計劃。事實上，研究表明，該地區的網路資安投資水平很高。

該地區三分之二 (63%) 的中小型企業平均將年收入的 4% 用於網路資安，其中 30% 的支出至少為 6%，9% 的支出超過 10%。

事實上，自疫情大流行開始以來，大約四分之三的亞太中小型企業已經全面增加了對網路資安的投資，其中大約五分之二的投資增加了 5% 以上。

一個令人鼓舞的一點是，增加的支出已平均分配到關鍵領域，這表明對建立強大網路態勢的多方面綜合方法的必要性有了深刻的理解。

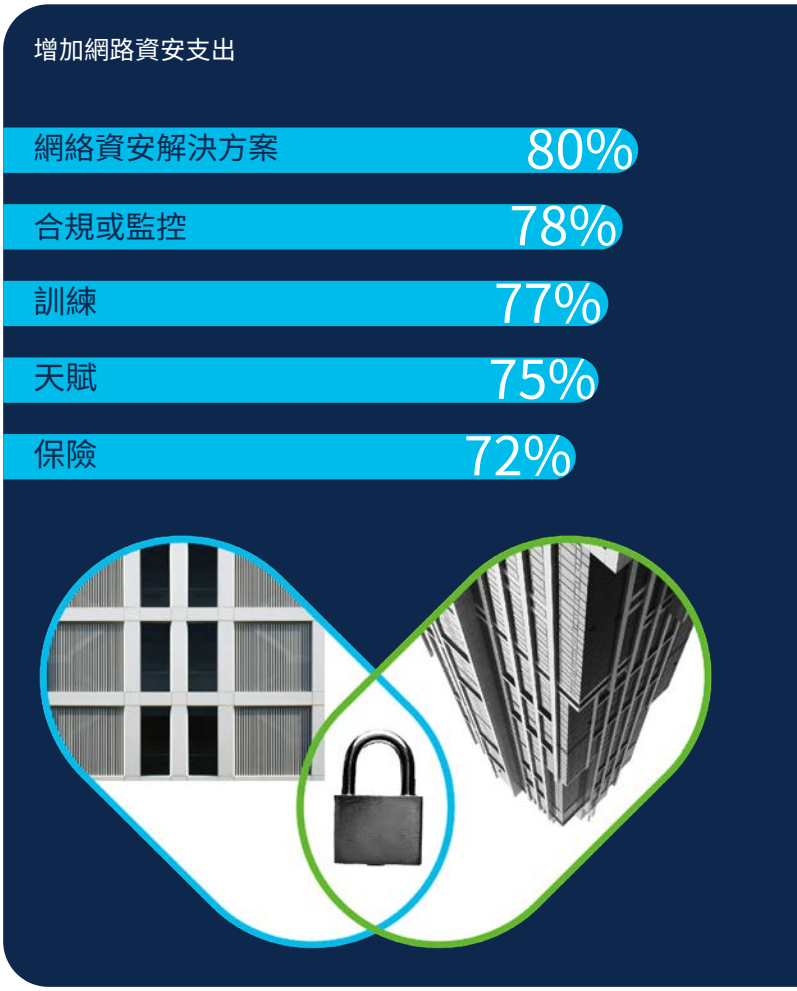
用於網路資安的年收入平均百分比

	亞太市場	澳洲	中國	香港	印度	印尼	日本	馬來西亞	紐西蘭	菲律賓	新加坡	韓國	台灣	泰國	越南
無	1%	1%	0%	2%	1%	1%	8%	0%	0%	1%	2%	3%	0%	1%	0%
小於 1%	8%	11%	4%	7%	6%	5%	18%	13%	17%	7%	9%	15%	13%	6%	2%
1-3%	27%	27%	30%	38%	20%	14%	33%	28%	26%	32%	29%	37%	42%	19%	18%
4-5%	33%	34%	45%	40%	30%	37%	29%	23%	24%	32%	36%	28%	24%	32%	53%
6-10%	21%	15%	15%	9%	30%	34%	9%	24%	21%	14%	17%	15%	17%	27%	16%
超過 10%	9%	11%	6%	3%	13%	9%	3%	12%	11%	15%	7%	2%	4%	15%	11%

在挑戰方面，中小型企業表示要跟上不斷發展的技術和資安要求(77%)；跟上不斷變化的網路威脅（76%）；使員工圍繞職責參與的挑戰（75%）；行業過於複雜（75%）；和能力招聘（73%）是他們在提高網路資安彈性方面面臨的主要障礙。

如右圖所示，增加對解決方案、合規性、人才和培訓等領域的投資是該地區中小型企業建立適當網路資安態勢的正確方向的一步。

中小型企業對網路資安的理解日益成熟，這可能最好地體現在他們從整體上看待準備工作這一事實。然而，即使在解決方案、人才和培訓方面進行投資，中小型企業也確實發現自己處於網路攻擊的錯誤終點。這只是行業的性質。隨著對網路事件對業務的潛在影響的日益了解以及法律影響的增加，中小型企業正在將網路資安保險作為關鍵投資領域。這為他們提供了一個保障，以緩衝任何此類事件可能對其業務造成的財務影響。



將以下因素視為提高網路資安彈性的障礙之百分比

	亞太市場	澳洲	中國	香港	印度	印尼	日本	馬來西亞	紐西蘭	菲律賓	新加坡	韓國	台灣	泰國	越南
與時俱進不斷發展的技術和資安需求	77%	82%	63%	73%	87%	53%	69%	84%	83%	89%	79%	75%	72%	71%	80%
努力跟上不斷變化的網絡威脅	76%	80%	59%	71%	87%	50%	66%	87%	81%	88%	82%	74%	74%	77%	81%
員工與其職責所面臨的挑戰	75%	76%	61%	65%	86%	55%	70%	81%	82%	81%	75%	67%	68%	73%	81%
行業太過複雜	75%	77%	61%	63%	85%	57%	65%	80%	87%	82%	82%	69%	65%	74%	79%

資安中小型企業的五個習慣

本報告揭示了中小型企業在應對不斷變化的網路資安環境時所面臨的常見挑戰。本節概述了各種規模的中小型企業可以用來改善網路資安狀況的五個習慣。

1 **討論的風氣**：網路資安環境在不斷發展，因此中小型企業需要隨時了解威脅及其對組織的潛在影響。安排高級領導和所有利益相關者之間頻繁的定期會議將確保將威脅形勢納入業務規劃。能夠應對網路資安事件的中小型企業經常談論這個問題。超過 90% 的人每週討論問題和風險，超過三分之二 (68%) 的人每天討論。面對威脅的組織不太好的中小型企業討論網路資安的頻率較低，大約三分之一 (31%) 討論問題的時間少於每月一次。

2 **簡化即關鍵**：處理網路資安的傳統方法是購買點資安產品和解決方案，以解決當時的特定問題。然而，這導致許多中小型企業在其基礎設施中擁有無數產品和解決方案，在許多情況下，這些產品和解決方案無法相互整合，從而在發生網路事件時造成營運複雜性和不必要的延遲。評估網路資安堆棧的各個部分如何協同工作對於處理攻擊的速度和結果至關重要。為了連接不同的產品和解決方案，SMB 需要一種整合的平台方法，以確保他們對整個資安基礎設施有清晰的可見性，並且當系統在現實世界中進行測試時，它可以無縫運行。

3 **錯誤準備便準備出錯**：確保中小型企業為現實世界做好準備的一種方法是模擬情況和結果在更受控制的環境中。這可以幫助中小型企業真實地了解可能存在的任何弱點，並提供解決這些問題的機會，並在發生這種情況時為實際情況做好更好的準備。事實上，我們的研究發現，準備充分的中小型企業的一個共同特徵是，超過 98% 的企業在過去 12 個月內進行了情景規劃或模擬。幾乎所有這些中小型企業，96%制定恢復計劃，以確保他們能夠盡快有效地啟動和運行業務。相比之下，在沒有有效規劃的中小型企業中，超過一半（58%）沒有進行情景規劃，近三分之二（63%）沒有恢復計劃。

4 **訓練再訓練**：了解在中小型企業可以部署的所有技術和解決方案中，人類往往是最薄弱的環節這一點至關重要。可以很好地判斷這一事實，即儘管該行業取得了所有進步，但網路釣魚（基本上是誘使人們點擊發送給他們的數位通訊中的連結）仍然是排名第一的威脅媒介。中小型企業需要確保每位員工，無論其角色如何，都對網路資安以及他們在確保業務資安方面可以發揮的作用有基本的了解。

我們在這方面的研究資料令人震驚。在準備好管理網路資安環境的中小型企業中，96% 同意或強烈同意員工了解網路資安的總體情況，95% 了解潛在攻擊的嚴重性及其角色。相比之下，那些對活動準備不足的人對其員工的信心要低得多，只有15%的人同意員工了解網路資安。

5 **一同攜手成就**：與合適的技術合作夥伴合作對於在網路資安方面取得整體成功至關重要。中小型企業應該記住一些事情。首先，與他們合作的合作夥伴應該有能力為他們的業務提供端到端的保護。在大多數情況下，需要將不同的產品和解決方案整合到一個平台中，以提供整個基礎架構的簡單性和可見性。其次，隨著中小型企業開始數位化之旅，他們的業務最終會增長，他們將擴大業務。他們選擇與之合作的合作夥伴應該有能力保護他們的營運，而不管其規模如何。最後，合作夥伴應該有能力就中小型企業想要如何部署技術提供不同的消費模型。

關於這項研究

3,748 受訪者 在 **14** 市場

市場

- 澳洲
- 中國
- 香港
- 印度
- 印尼
- 日本
- 馬來西亞
- 紐西蘭
- 菲律賓
- 新加坡
- 韓國
- 台灣
- 泰國
- 越南

受眾

負有網絡安全責任的 IT 和商業領袖

這些組織包括：

- 小型（1 至 249 名員工）
- 中等（250 至 999 名員工）

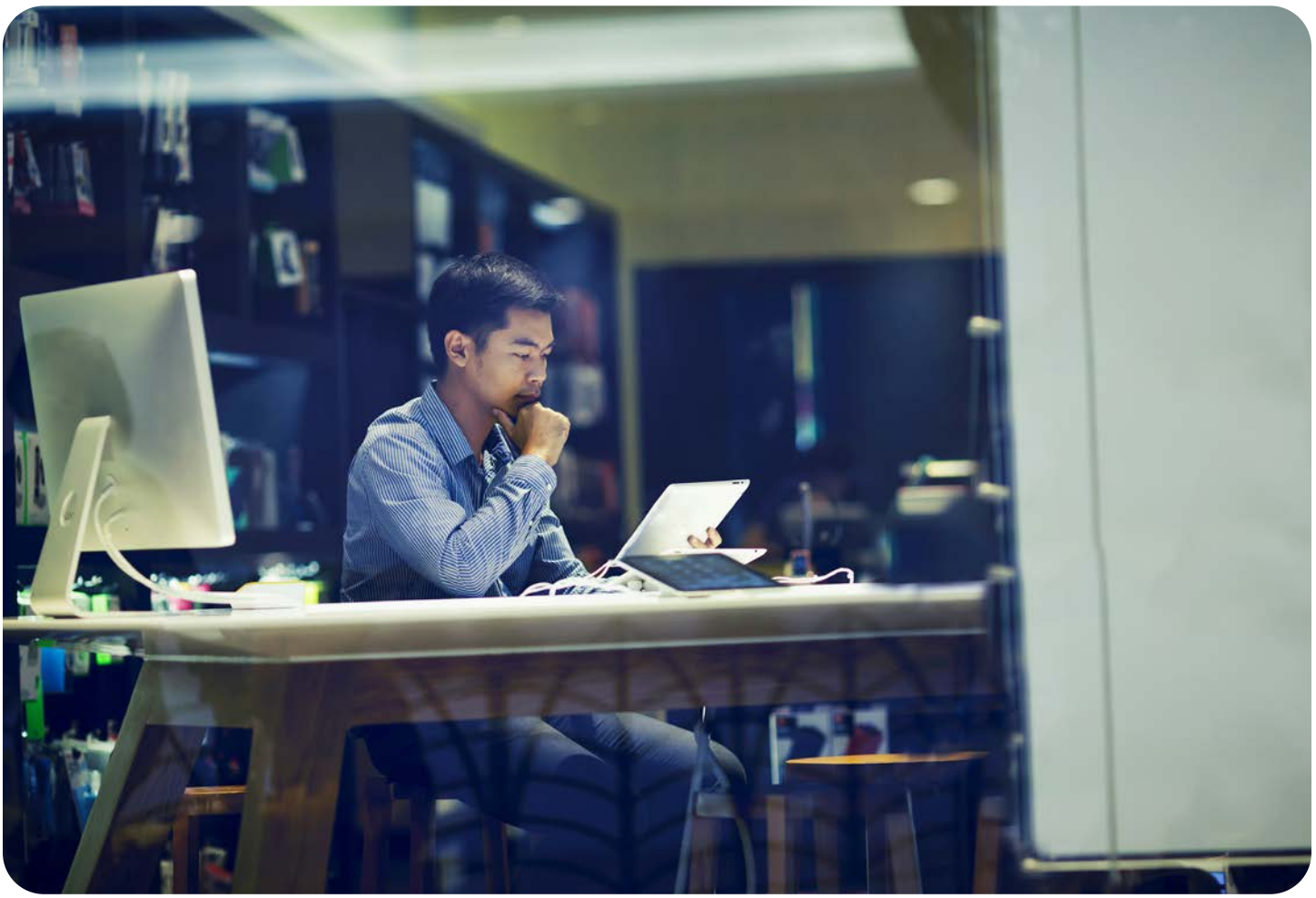
行業

- 廣告或市場研究
- 商業服務（例如會計、諮詢）
- 建造
- 教育
- 工程、設計或建築
- 金融服務
- 衛生保健
- 製造業
- 媒體與通訊
- 自然資源（例如石油、採礦、林業）
- 個人護理和服務
- 專業的服務
- 房地產
- 餐廳服務
- 零售
- 技術服務
- 運輸
- 旅遊服務
- 批發
- 其他

附錄 A

由於停機時間長，影響升級

	亞太市場	澳洲	中國	香港	印度	印尼	日本	馬來西亞	紐西蘭	菲律賓	新加坡	韓國	台灣	泰國	越南
在您的組織的營運受到嚴重影響之前的停機時間															
不到一小時	15%	10%	21%	11%	17%	18%	10%	13%	17%	16%	7%	10%	21%	18%	8%
一到兩個小時	29%	25%	28%	21%	32%	35%	18%	32%	39%	28%	23%	29%	28%	31%	30%
在您的收入受到嚴重影響之前的停機時間															
不到一小時	13%	8%	16%	12%	12%	25%	7%	16%	9%	15%	10%	14%	14%	14%	9%
一到兩個小時	24%	20%	26%	21%	24%	27%	17%	23%	19%	27%	20%	19%	34%	28%	20%
在您可能面臨監管或法律影響之前的停機時間															
不到一小時	13%	7%	16%	14%	13%	19%	6%	17%	8%	13%	11%	13%	18%	14%	12%
一到兩個小時	22%	19%	24%	18%	24%	32%	15%	23%	20%	19%	24%	21%	25%	22%	17%



關於思科資安

思科長期以來一直是網路領導者，同時在此過程中構建了開放、整合的網路資安解決方案組合。我們認為資安解決方案應該設計為一個團隊。他們應該互相學習。

他們應該作為一個協調單位來傾聽和回應。當這種情況發生時，資安變得更加系統且高效。多年來，我們的客戶一直信賴我們作為全球最大的 IT 基礎設施和網路服務提供商以及全球最大的 B2B 網路資安企業。

Cisco Secure 建立在更好的安全性原則之上，而不是更多。它提供了一種簡化的、以客戶為中心的資安方法，可確保它易於部署、易於管理和使用，並且可以協同工作。我們受到這樣一個事實的推動：人和我們的客戶是我們工作的核心。我們了解客戶希望消除複雜性和噪音，並對他們的資安充滿信心；注重結果。

這需要簡化而不是簡單化。我們的雲原生平台在這方面是一個巨大的飛躍。

我們賦予資安社區以可靠性和信心，他們現在和將來都可以免受威脅 思科 SecureX 平台。我們幫助 100% 的財富 100 強公司通過地球上最全面、最整合的網路資安平台保護現在和未來。詳細了解我們如何簡化體驗、加速成功並保護未來，請連接cisco.com/go/secure.

思科安全成果研究

為了更深入地潛水，我們邀請您閱讀2021年中小企業安全成果研究(SMB)，並訪問我們的專用頁面了解更多 Cisco Secure 思想領導力內容。

美洲總部
思科系統公司
加利福尼亞州聖何塞

亞太總部思科系統（美國）私人有限公司 新加坡有限公司

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

思科在全球擁有 200 多個辦事處。地址、電話號碼和傳真號碼列在 Cisco 網站上，網址為**https://www.cisco.com/go/offices**


CISCO