提升數位彈性：

台灣企業的安全自動化

全球網路安全領導者每天都在面臨多種挑戰。在逐漸複雜化的威脅形勢中，複雜的 IT 基礎架構環境與日益增加的安全周邊，對於維持資料安全有著極其重要的影響。

鑑於對技能的需求持續高漲，自動化安全工具對於支援安全專家的日常工作也變得至關重要。為了協助高階主管瞭解如何善用此機會，Omdia 與 Telstra 展開合作，以 250 名資深技術決策者作為調查對象，藉此評估北亞地區安全自動化策略的成熟度。透過來自不同規模企業與部門的洞見，本研究的結果可以協助高階主管有效地增強企業網路彈性。

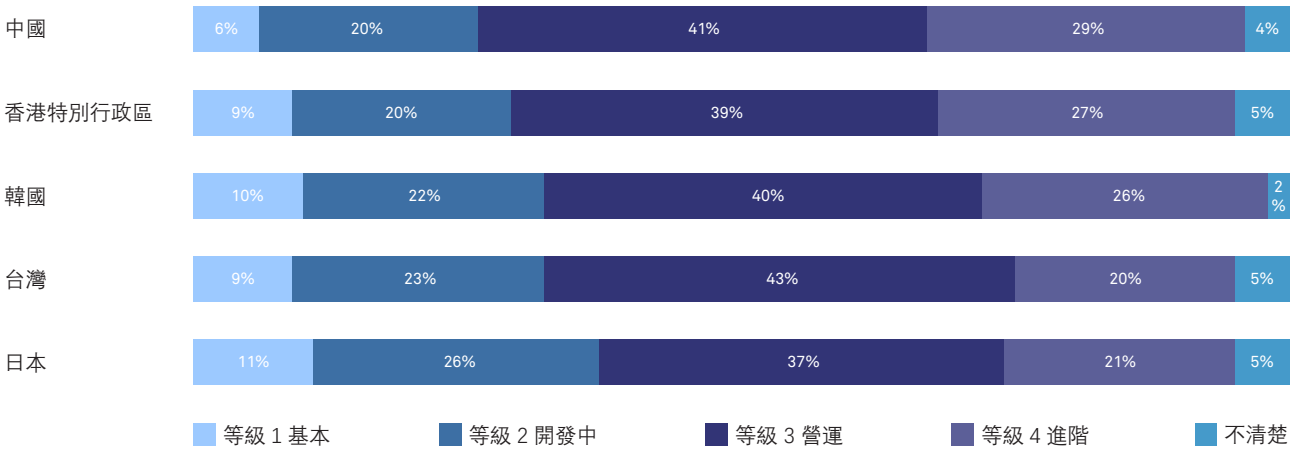
儘管目前企業遇到的挑戰都具有一定的共性，但各個地區之間仍呈現耐人尋味的差異性。以下是台灣企業在安全自動化方面所面臨的部分關鍵阻礙因素與驅動因素。

台灣企業的安全自動化狀態（成熟度）

對比其他北亞地區成員，台灣的安全自動化成熟程度是倒數第二。對比本研究中所有其他地區平均 64% 的成熟度，台灣僅有 63% 的企業報告等級 3（營運）或 4（進階）的成熟度。

同時在報告等級 1（基本）和 2（開發中）成熟度的企業方面，台灣的百分比 (32%) 也是第二高。

在貴企業的網路安全攻擊防禦框架中，使用安全自動化的成熟度為何，1 表示成熟度為基本，4 表示成熟度為進階？

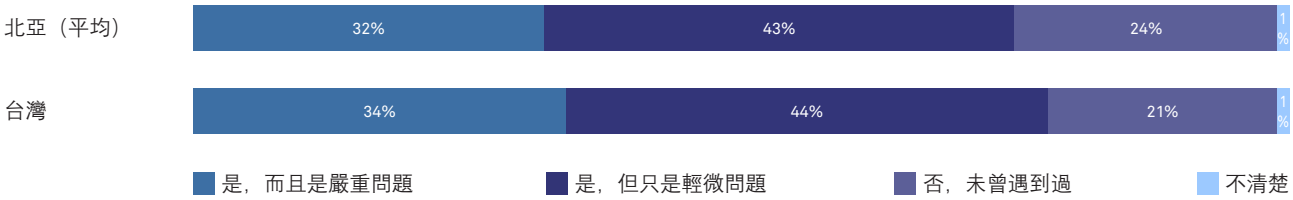


而在關注的 5 個產業中，報告指出台灣醫療保健企業擁有最高等級的安全自動化成熟度，然而運輸與物流企業的等級則最低。

安全問題的普遍程度

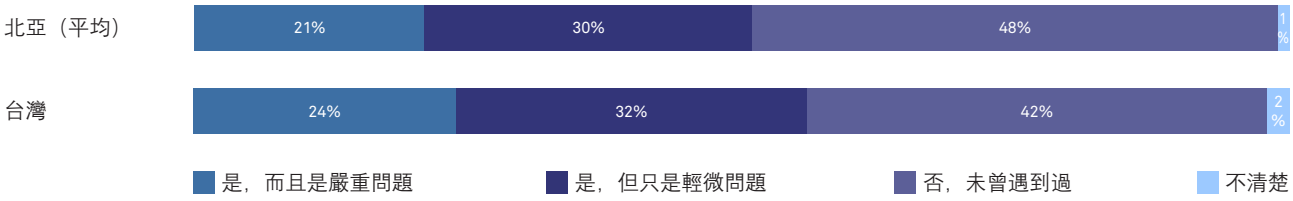
安全事件層出不窮，所有地區的企業都在持續因應隨之而來的各種挑戰。這在台灣受訪者之間也有所反映，有 34% 的公司在過去 12 個月內遭到「嚴重」攻擊的次數增加，這在北亞地區是第二高的。而台灣有 44% 的企業報告輕微安全事件的增加，另外 21% 則報告沒有增加。

針對重要資源受到攻擊的整體安全事件，貴企業在過去 12 個月是否遭遇此類事件顯著增加的情況？



至於實際的漏洞，有 24% 的台灣受訪者回應在過去 12 個月發生嚴重漏洞的情況顯著增加。另外，有 32% 的企業也回應了輕微漏洞的增加，而 42% 表示他們沒有遇到增加的情況。

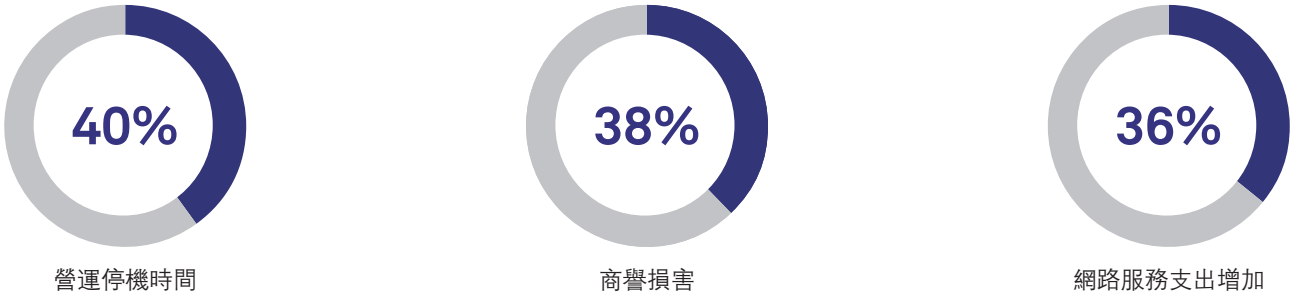
貴企業在過去 12 個月是否遭遇安全漏洞顯著增加的情況？



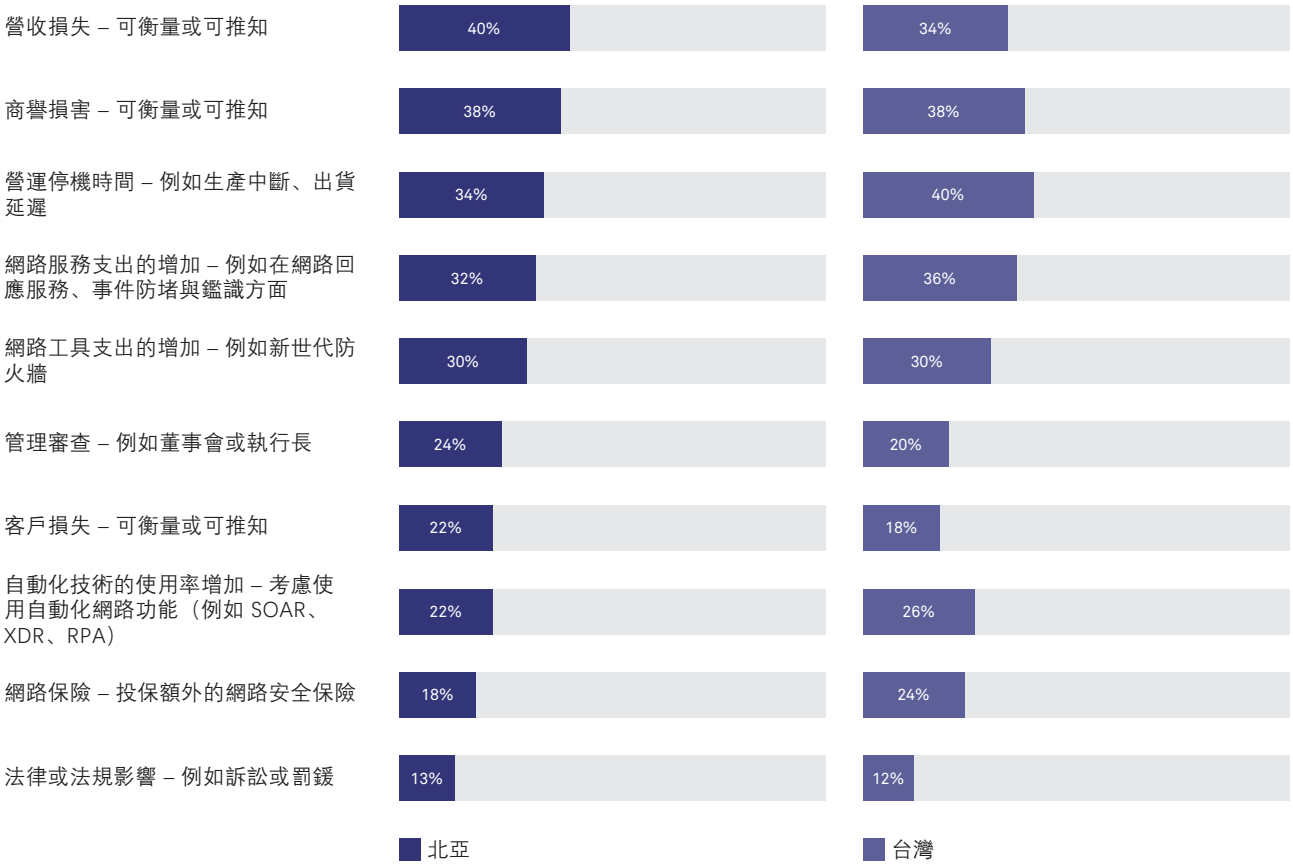
損害的影響

台灣公司報告了安全事件造成的各種重大影響。台灣公司遭遇的暫停營運時間百分比最高，有 40% 的受訪者認為這是一項不容忽視的問題。
所幸，有 26% 的台灣企業選擇啟用更為自動化的安全服務來因應影響最為重大的網路攻擊，這在北亞也是最高的比例。
在網路服務支出方面，台灣企業的投入增加比例 (36%) 也最高。

整體而言，對於台灣企業的前三大影響是:



在過去 12-18 個月，網路安全事件或漏洞對貴企業造成的最重大影響為何?

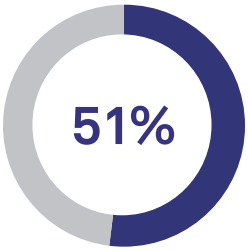


自動化的優勢

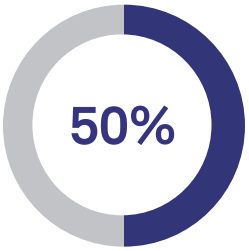
安全自動化可協助所有企業取得各種優勢，特別是加快處理重複性的低價值工作，以及減少處理誤報警示所花費的時間。儘管台灣呈現同樣最低的誤報警示比例 (41%)，但自動化仍有很大機會可協助消除此類「干擾」。

建置完善且妥善啟用的安全自動化可協助大幅降低發生嚴重漏洞的可能性與影響。台灣高階主管認為，有效的安全自動化可協助將安全事件和漏洞所導致的嚴重影響減少 50%。

在過去 12 個月，針對影響貴企業的「嚴重」網路安全事件或漏洞，其中可以使用最佳化安全自動化來減少的百分比有多少？



北亞



台灣

放眼台灣以至全世界，安全自動化均是一項極其重要的工具，可協助企業改善網路安全彈性並抵禦逐漸複雜化的威脅形勢。對於台灣的公司而言，至關重要的是識別公司的成熟度等級，並針對整個業務範圍擬定好策略，以建置世界級的自動化功能。

欲了解更多詳情，請聯絡您的 Telstra 業務代表。

telstra.com.hk telstraenquiry@team.telstra.com