FUJIFILM
Value from Innovation

減少資訊科技、數據和打印機的安全威脅

企業如何增強資訊科技安全韌性

推動轉型，茁壯成長：展開企業的數碼轉型之旅

我們的《從掙扎求存到茁壯成長：利用業務韌性建立競爭優勢》報告指出，企業如何在急速變化的環境中保持韌性，從而變得更強大並茁壯成長。公司憑藉清晰、有效率的工作流程及人手安排，展現更卓越的應對危機能力。

全球企業預計以下趨勢將推動從2023年至2027年之間的轉型。

- 新興技術的採用
- 環境、社會和治理（ESG）標準的實施加強
- 消費者的生活成本不斷上升
- 數碼科技越趨普及
- 全球經濟增長放緩

相比起步較慢的同業，較早推動數碼轉型的企業之增長速度快高達5倍。[1]

今時今日，關鍵在於敏捷。

無論是大型企業或中小企，具韌性和策略性的企業已推動數碼轉型，令混合辦公模式和遙距團隊更有效工作，確保業務取得成功，並進一步履行社會責任。

許多企業正在迎頭趕上，其中一些表現較佳。在科技採納和創新文化方面，起步較遲的企業現在可以把握第二波優勢，收窄與行業領袖的差距。他們可以借鑑較早採納創新科技者的經驗，加快數碼化流程，後發爭先。

長遠的數碼轉型有助提升韌性，並培養正確的組織文化思維。當中涉及塑造互聯互通的工作空間，加強混合辦公模式和遙距團隊的協作，透過業務工作流程自動化構想未來的工作，並提升員工技能，為創新做好準備。

透過本系列了解更多：

1

未來勞動力：簡化工作流程，提高團隊生產力

2

減少資訊科技、數據和打印機的安全威脅：企業如何增強資訊科技安全韌性

3

身處數碼時代，推動工作場所轉型，令業務茁壯成長：工作場所轉型的趨勢和策略

表現超乎預期的公司增長速度驚人，為最遲採納創新者的4倍之多[2]。這個比率甚至高於具領導地位的公司，表明企業可以在維持盈利的情況下，成功推動數碼轉型。

推動轉型，令業務茁壯成長——透過數碼轉型，加快發展步伐，提高生產力。

目錄

資訊科技安全：
亞太區企業日益關注的問題

加強資訊科技安全是亞太區企業目前最關注的問題，當中涉及網絡安全策略，保護機構資產（包括電腦、網絡和資料）免遭未經授權的存取。

網絡安全威脅是現今企業的一大挑戰，而這些攻擊所造成的後果亦越來越嚴重。除了蒙受經濟損失之外，企業還可能要付上數據流失、聲譽受損和業務中斷的沉重代價。

大勢所趨下，亞太區企業意識到加強資訊科技安全能力的逼切需要。

企業需要有效的安全策略。然而，建構過程是個旅程，而不是終點。人們常以為資訊科技安全需要大型解決方案，但其實即使是微小的改變，也有助加強公司的安全意識。

在本指南中，我們將深入探討亞太區的安全威脅形勢，並重點介紹企業面對的首要安全挑戰。我們希望幫助企業找出現有策略中的差距，以便執行改善資訊科技安全防衛的必要解決方案。

亞太區是面對全球網絡威脅數目最多的地區，佔全球已修復網絡安全事件的31%。[3]

2023年第一季，亞太區每週網絡攻擊按年增幅最高（每週1,835次攻擊）。

這數字比全球平均網絡攻擊（每週1,248次）高出47%。[4]

亞太區安全威脅概況

在電腦設置後門程式是網絡攻擊者最常見的行動，其次是勒索軟件和MalDocs。[5]

馬來西亞和菲律賓是最多企業遭受安全威脅的地區。[6]

澳洲是最多企業沒有事故應變計劃的地區，而香港則是最多企業設有應變計劃的地區。[7]

新加坡企業主要擔心業務中斷。[8]

企業應對資訊科技安全事故採取的五項主要措施[9]

68% 進行定期培訓或桌上演習

64% 制定事故應變手冊和計劃

62% 制定折衷的復原計劃

62% 委任一名數據保安專員

62% 外聘網絡安全專家服務

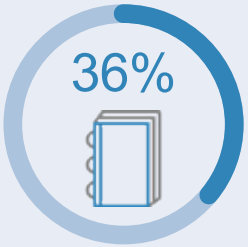
亞太區企業面臨的主要資訊科技安全挑戰

深入了解資訊科技安全挑戰有助企業避免營運中斷、收入損失及資料被盜的嚴重後果。

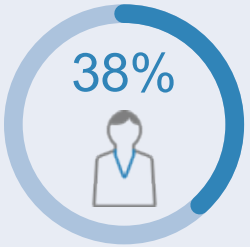
企業如能投資全面的業務策略，便可涵蓋各種資訊科技安全問題。深入了解重要挑戰，以便找出及堵塞資訊科技安全過程中的漏洞。

業務與資訊科技安全兩者的步調不一致

當資訊總監和業務主管目標不一致，可能會阻礙執行有效的安全措施，繼而導致資訊科技安全方面的投資不足。



亞太區企業在2022年仍未制定事故應變手冊、計劃和政策。



沒有委任數據保安員，也沒有常年外聘網絡安全專家。[10]

未能確定他們的資訊科技安全防衛是否能夠足以抵禦網絡攻擊者的最新攻勢。[11]

教育員工保護數據

人為錯誤是雲端數據外洩的首要原因。[12] 導致人為錯誤有幾個主要因素，包括機會、環境和缺乏意識。[13]

導致資料外洩的人為錯誤包括下載帶病毒的軟件、使用弱密碼或IP位址外洩。

導致人為錯誤的因素：

機會

出錯的機會越多，造成錯誤的可能性就越大。

環境

工作場所的實體環境和辦公室文化有機會導致人為錯誤。有時，員工知道要採取正確行動，但卻未能執行。

缺乏意識

使用者可能根本不知道要採取哪些正確行動。

解決資訊科技安全人才短缺問題

2022年，全球網絡安全人員短缺擴大了26.2%，達342萬人。[14]

亞太區面臨最嚴重的人才短缺，共欠216萬網絡安全人員。[15]

人才短缺原因包括缺乏資訊科技安全方面的高等教育課程[16]、對資訊科技安全行業的誤解，以及科技發展步伐急速。[17]

而這個問題亦顯示，企業必須尋找更好方法以保護敏感資料和數碼資產。

解決雲端應用的安全挑戰

隨著企業轉向雲端以滿足資訊科技需求，亞太區的雲端應用率亦迅速增長。

然而，雲端運算是一個複雜的過程，最重要是一開始便要考慮安全性。如果缺乏有效的雲端遷移策略，便可能會面對資料外洩、資料遺失和雲端配置錯誤的風險。

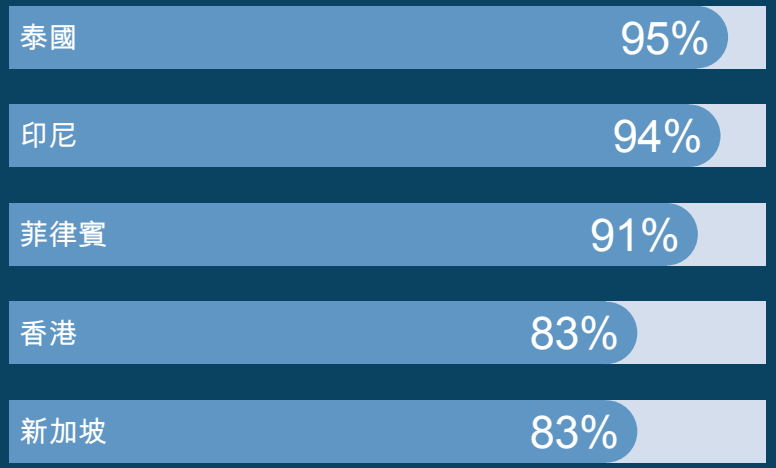
亞太區雲端應用現況

2024年，亞太區企業的雲端支出將達2,000億美元。[18]

已經使用雲端服務的企業也有望增加雲端投資。

每五間亞洲區企業就會有一間（84%）計劃在2024年全面遷移到雲端。

投資於雲端的增長很可能來自[19]：



防範網絡解密入侵

隨著企業將數據和運算遷移到雲端，資訊科技安全團隊必須使用加密流量來保護企業的數碼足跡。然而，網絡攻擊者有方法解密已加密的訊息，甚至洩露這些敏感資料、密碼和金鑰，並破壞這些系統。

隨著量子電腦的發展，系統一旦落入犯罪份子手中，便會對公司造成極大的威脅。

2023年，亞太地區企業面臨最大的網絡安全挑戰之一，就是利用量子運算進行網絡解密。

約60%亞太區企業視網絡解密為最令人擔憂的量子電腦運算安全威脅。[20]

保護數碼空間

隨著連網設備的數目與日俱增，要保護這些設備免受入侵的威脅越來越困難。這是由於：

1. 現在，員工擁有**比以往更多的連網設備**，他們通常使用一系列連網設備，包括桌上電腦、手提電腦、智能手機、平板電腦和多功能影印機，以執行日常職責。

2. 採用連網設備能擴大設備之間**所收集和傳送的資料量**，但卻擴大了網絡不法份子的可攻擊範圍。

3. **大多數連網設備的設計都沒有周全的安全考慮**，沒有足夠的安全控制措施來防止網絡攻擊，例如定期軟件更新或來自製造商或供應商的安全更新程式。

流動網絡安全威脅：

- 網絡釣魚攻擊、惡意應用程式、易受攻擊的網絡、中間人（MiTM）攻擊[21]

列印安全威脅：

- 內部威脅：其他使用者未經授權的操作、因疏忽大意導致的資料外洩
- 外來威脅：軟件被篡改、裝置上儲存的文件資料遭破壞、審核日誌被篡改、竊聽、通訊資料被篡改、未經授權存取管理功能

保護企業免受資訊科技安全威脅

企業必須制定合適的資訊科技安全措施，以克服已知的安全問題。

以下是保護企業免受安全威脅的建議。

挑戰	建議
業務與資訊科技安全的步調不一致	建立企業的網絡韌性
教育員工如何保護數據	提升職場網絡安全意識
解決資訊科技安全人才短缺問題	
解決雲端應用的安全挑戰	外聘資訊科技專家服務來支援內部的資訊科技團隊
防範網絡解密入侵	
保護數碼空間	制定企業設備安全措施

提升企業的網絡韌性

網絡韌性是指企業預測網絡攻擊、回應及回復正常的能力。

網絡攻擊類型日新月異，網絡韌性亦因此成為企業的首要任務。以往，入侵系統需要數天時間；但現時，這些惡意活動可能只需數小時。

為了迅速抵禦黑客攻擊，企業必須與專家合作建立現代化資訊科技安全計劃，並進行系統整合。[22]

提升網絡韌性的因素[23]

1

預計

了解企業的資產、漏洞和潛在威脅。

2

抵抗

採用系統、流程和工具來保護數據和連網設備。

3

復原

能夠及時恢復正常運作非常重要，因此企業必須制定事故應變計劃，盡量將安全事故的影響減至最低。

4

演變

從過去的事故中汲取教訓，透過分析和經驗來填補企業資訊科技安全措施的不足。

提升職場網絡安全意識

即使擁有頂尖的技術，但在資訊科技安全方面，員工往往是企業中最弱的一環。

進行網絡意識培訓有助解決這問題，加深員工對最新安全威脅、最佳實踐，以及行業特定法規和合規要求的認識。

這有助降低安全事件的風險，並促進企業遵守相關的行業法則，有助加強安全防禦力。

提升職場網絡安全意識的最佳實踐例子

網絡意識培訓需要企業上下齊心努力。

度身訂造培訓內容，以滿足主管和下屬的要求。

避免千篇一律的方法。

進行定期培訓能讓團隊了解最新的網絡威脅和攻擊手法。

定期進行網絡釣魚攻擊的模擬測試。

找出安全策略中較弱的部分，並透過模擬電郵測試員工的反應，讓他們在過程中了解網絡釣魚，避免事件發生。

外聘資訊科技專家服務以支援內部資訊科技團隊

鑑於大多數業務安全團隊無法應對新挑戰（例如準備大規模網絡解密或順利過渡至雲端系統），為資訊科技團隊提供經驗豐富、值得信賴的專家服務，有助預防和應對網絡攻擊。

例如，資訊科技專家能協助你對抗網絡解密，服務如下：

- 判斷敏感資料是否可以被輕易解密
- 持續為你提供加密技術的最新資料

在遷移到雲端系統方面，資訊科技專家可監督及引導企業完成遷移過程，針對合規工作、事故應變計劃、定期演習和模擬測試等方面為企業制定適當的程序。

透過外聘資訊科技專家服務，可解決企業潛在的問題和違規行為。專家會為企業作出頻密的評估和及時的技術升級，即使發生事故，企業仍可合規地化被動為主動。

為甚麼亞太區的企業會與託管和專業安全服務供應商合作[24]：

亞太區資料外洩事件不斷增加

數碼轉型措施令雲端項目不斷增加

克服資訊科技安全專業人才短缺的問題

對外來安全專業知識和合規見解的需求不斷上升

減少聘請內部安全專家的開支，同時獲得有效的安全管理方法

制定企業設備安全措施

企業必須採用能夠保護跨用戶端點裝置的安全解決方案，這些裝置包括桌上電腦、手提電腦、平板電腦、伺服器、智能手機及其他連接裝置。

此外，必須保護列印裝置免受網絡攻擊。文件列印是企業最常見的活動，大量頻繁的商業數據會透過打印機傳遞。

要建立安全列印策略，你需要：

- 確保連接到企業網絡的所有設備都是安全的。
- 確保企業內所有連接設備都遵循相同的安全標準和策略。
- 使用提供安全列印允許功能的解決方案，能保護打印機輸出。
- 利用管理列印服務提供最新保護，抵禦日漸複雜的網絡威脅。這對於經常依賴列印並使用分散式列印的企業來說是理想之選。

確保打印機安全的必要功能

安全列印

安全列印讓列印項目停留在安全的虛擬佇列中，直至使用者走到打印機前發出最終的列印指令才列印。在項目打印出來前，員工必須透過各種方法進行身份驗證，例如使用PIN碼、身份證、行動應用程式或掃描二維碼。

這能降低一般使用打印機的錯誤，讓用戶安心拿取列印文件，確保不會被他人看到或影印，以及減少敏感資料被他人拿去的機會。

安全流動列印

安全流動列印讓員工透過連網裝置安全地傳送列印項目，一般包括身份驗證、加密、使用者授權、日誌紀錄和審查等功能。

安全流動列印在某些工作環境中更為重要，例如當企業實施混合工作模式，並安排員工在遙距工作時使用他們的設備進行列印。而醫療保健和金融行業的企業都需要符合文件安全合規的要求，因此安全列印更是必須的。

360° 數據安全

360° 數據安全透過穩健的措施加強保護，包括安全掃描、停止未經授權的存取，或透過審查追蹤路線，即時監控連網設備。

主要功能包括一鍵式使用者身份驗證（讓你有效管理使用者和列印環境）、更嚴謹的審查功能，以及透過安全網絡進行點對點數據加密。

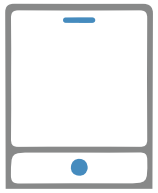
制定資訊科技策略清單

以下是針對資訊科技策略的建議：

評估企業的資訊安全能力

- ☐ 評估團隊成員的技能和專業知識。
- ☐ 評估資訊科技安全團隊的資源分配。評定預算是否符合企業的安全要求。
- ☐ 就團隊中需要改善的地方及技術不足的問題，制定相關計劃。
- ☐ 考慮有助於提升業務管理的解決方法，例如外聘資訊科技專家。

執行計劃以提升網絡韌性



- ☐ 針對企業的資產、漏洞和潛在威脅進行評估。
- ☐ 列出保護數據安全和連網設備所需系統、流程和工具。
- ☐ 訂立明確的事故應變計劃。透過桌上演習和模擬活動，定期測試和改良這些應變計劃。
- ☐ 監控資訊科技安全基礎建設，定期評估及更新相關策略。

進行網絡意識培訓

- ☐ 訂立網絡意識培訓目標，並準備好培訓計劃的內容。
- ☐ 安排員工參與培訓課程，確保他們輕易上課及取得相關的培訓資料。
- ☐ 監督及評估培訓計劃的有效性。
- ☐ 定期更新培訓資料和內容，確保計劃內容與網絡威脅形勢同步。

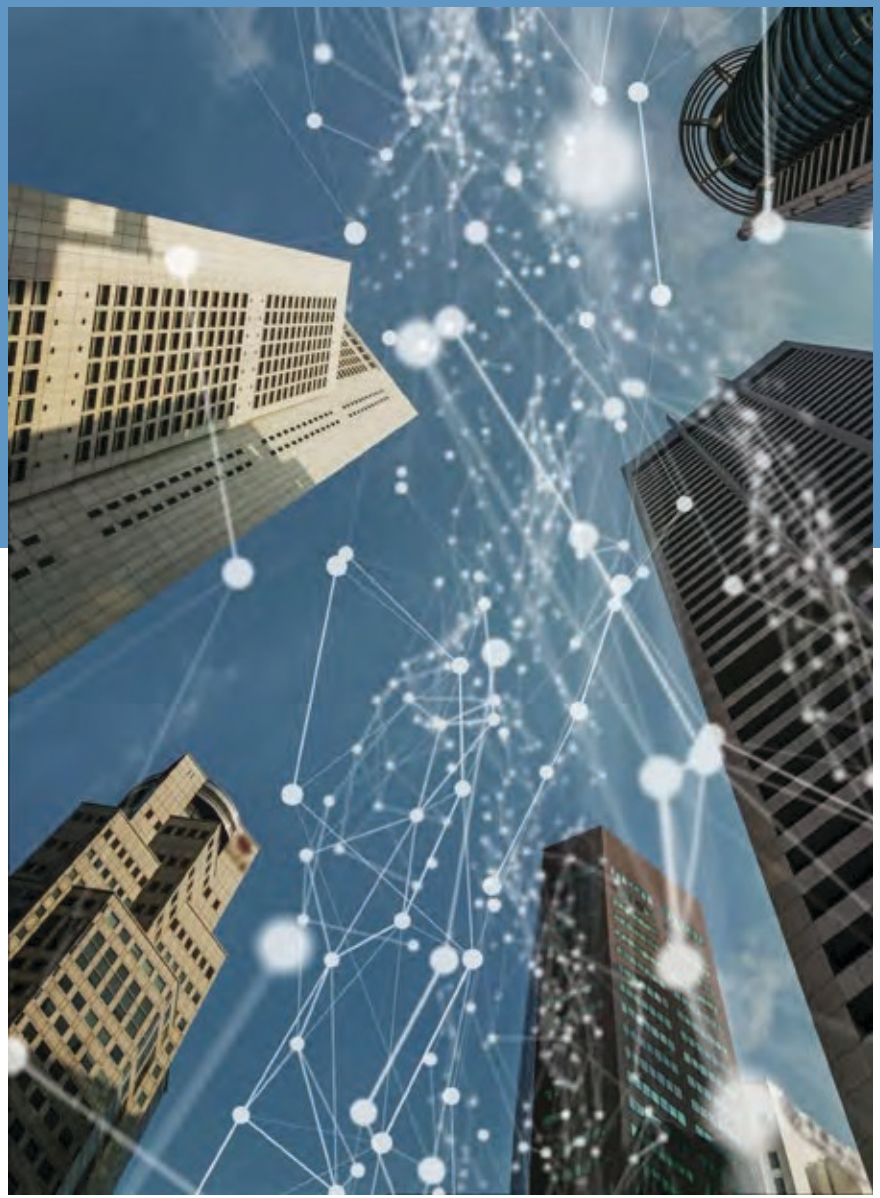
執行連網裝置計劃

- ☐ 保持一份企業打印機和連網設備的最新庫存紀錄。
- ☐ 在列印和連網裝置上進行使用者身份驗證，確保只有授權人員才能存取該裝置。
- ☐ 確保所有打印機和連網設備使用最新版的軟件。
- ☐ 查看每項設備的安全功能。利用能夠提供安全列印功能的解決方案，例如安全列印和安全流動列印等技術。
- ☐ 利用列印管理服務提供最新保護，抵禦不斷演變的列印安全威脅。
- ☐ 確保企業的網絡意識培訓課程涵蓋有關保護打印機和連網裝置的內容。

資訊科技網絡是保護企業安全的首要任務

由於全球網絡安全事故在亞太區愈發頻繁，企業必須優先關注資訊科技安全。安全威脅與日俱增，保護網絡、數據和裝置（包括打印機）已成為企業日益關注的議題。

為了有效應對不斷變化的網絡威脅，企業必須了解最新的資訊科技安全形勢和挑戰，並制定靈活彈性的計劃，以執行穩健的安全解決方案。透過這些策略和方法，能改善工作流程，加強資訊科技夥伴合作關係，進一步提升安全性。富士膠片商業創新為資訊科技團隊提供合適的解決方案和支援服務，是企業可靠的專業資訊科技安全合作夥伴。



與富士膠片商業創新一同茁壯成長

我們提供卓越的數碼科技和自動化解決方案，支援你的數碼轉型之旅。

ApeosWare Management Suite 2 是一款打印管理軟件，功能包括設備管理、整合式認證、安全列印輸出、用量總計、傳送文件、追蹤資訊外洩。以精簡流程全方位管理文件，為企業帶來價值。

IT Expert Services 針對中小型企業的綜合管理支援服務。透過資訊科技專家服務，中小企可獲得專家的協助，以專注於核心業務發展。

網絡安全管理服務是一項訂閱模式的人工智能網絡安全解決方案，由網絡安全專家提供24x7全天候支援。此方案不但簡化搜尋網絡威脅的工作，而且提供更快、更具行動力的回應，讓你持續監控易受攻擊的領域與環境。

安全MFP（多功能影印機）是一項安全列印解決方案，提供重要的列印安全功能，例如按需列印，協助企業塑造安全的列印環境，將常見的打印機用戶錯誤減至最低，同時減少列印開支及輸出成本。

MPS (Managed Print Services) Guardia 是富士膠片商業創新提供的新一代管理列印服務，可保護企業免受預算超支、資料外洩及生產力下降引致的損失。

PaperCut 是一款供打印機、影印機和多功能設備使用的嵌入式列印管理軟件，用於監控企業列印輸出。用戶可節省列印耗材，同時體驗輕鬆安全的列印。

Ysoft 是一款專門負責文件擷取及3D列印的列印管理軟件。模組化的列印管理解決方案靈活度高，能提升業務的擴展速度，並根據需求的改變而增設其他功能。

FUJIFILM IWpro 是一個安全的一站式平台解決方案，有助推動業務數碼化，提供協作空間、完善的工作流程、元數據（Metadata）和文件的高效文檔管理，以及雲端多種列印功能。

與富士膠片商業創新攜手推動轉型之旅

透過我們的解決方案和專業知識，企業可以推動轉型，成就長遠果效。細閱客戶分享，了解他們與富士膠片商業創新的合作關係。

以下是客戶意見調查的結果：

96%
認為與富士膠片商業創新合作很輕鬆

98%
認為我們是理想的創新合作夥伴，能夠滿足他們的各種需求

97%
很樂意推薦富士膠片商業創新，因為我們能涵蓋所有業務需求

FUJIFILM
Value from Innovation

讓我們協助你加強資訊科技安全。

隨著網絡威脅的規模和複雜性不斷演變，企業必須優先考慮資訊科技安全。富士膠片商業創新為你提供有效的解決方案，助你建立企業的網絡防禦系統。

我們以客為先，以提供出色的體驗予合作夥伴為榮。我們一直與客戶保持緊密的溝通，以確保有效且恰當的解決方案得以實施。

在瞬息萬變的網絡安全環境中，富士膠片商業創新是你可靠的合作夥伴，隨時助你發揮數碼轉型的潛力，並確保你的業務免受安全威脅。

為未來做好準備。

聯絡富士膠片商業創新

FUJIFILM
Value from Innovation

References

1,2. Accenture, Scaling Enterprise Digital Transformation, August 2021

3. IBM, IBM Security X-Force Threat Intelligence Index 2023, March 2023

4. Check Point Research, Global Cyberattacks Continue to Rise with Africa and APAC Suffering Most, April 2023

5,6,7. Kroll, State of Incident Response: APAC, October 2022

8. IBM, IBM Security X-Force Threat Intelligence Index 2023, March 2023

9,10. Kroll, State of Incident Response: APAC, October 2022

11. EY, Global Information Security Survey, July 2021

12. Thales, 2023 Thales Global Data Threat Report, June 2023

13. Usecure, The Role of Human Error in Successful Cyber Security Breaches, June 2022

14,15. ISC2, Revealing New Opportunities for the Cybersecurity Workforce, October 2022.

16. Deloitte, Finding cybersecurity talent in an altered world, February 2023

17. Advantis Global, The Cybersecurity Talent Shortage: Understanding the Urgency and Impact, July 2023

18. Boston Consulting Group and Cisco, The Future of Cloud in Asia Pacific, August 2021

19. Alibaba Cloud, A Majority of Asia Businesses Expect to Increase Cloud Investment in 2023, March 2023

20. Thales, 2023 Thales Global Data Threat Report, June 2023

21. Tech Target, Top 4 mobile security threats and challenges for businesses, May 2021

22. CNBC, Palo Alto Networks CEO warns companies need modern, integrated cybersecurity: 'The bad actors are moving faster', August 2023

23. IDC, Leadership in a Changing Digital World: Five Mandates, April 2023

24. Frost & Sullivan, Asia-Pacific (APAC) Managed and Professional Security Services Market: The Shortage of Cybersecurity Professionals is Driving MSS and PSS' Future Growth Potential, November 2022