

team+ newsletter

疫後新常態-混合式辦公
您的資安做好了嗎？

互動資通用戶成功中心

2021.07.30

前言

各位好，一切平安！

雖然是句簡單的問候，但我們衷心期盼疫情早日趨緩，生活回歸日常。

疫情糾纏著全世界超過一年半，即使各地開始施打疫苗，但一年多來的影響，也讓許多企業開始思考，如何將這段時間的經驗轉換成**迎接後疫情來臨的新動力**。

這一期team+ newsletter，我們想聊聊「**混合式辦公（Hybrid Working）**」，這已是企業認知回不去的工作新常態。因此，我們整理國際相關調查、遠距辦公於疫情間帶來的資安挑戰，以及該如何因應的建議，希冀大家都能對疫後新常態提早準備。

01

混合辦公成疫後共識
隨處工作(Work from Anywhere)是未來趨勢

02

遠距或混合辦公 應掌握潛在資安風險

03

打造具資安層級的混合辦公情境



01

混合辦公成疫後共識
隨處工作(Work from Anywhere)是未來趨勢

CISCO：混合式工作場所興起

以辦公室為基礎並保留靈活與彈性，將是企業於後疫情施行的策略。

混合工作模式，不是選擇在哪個地點工作，而是如何激發員工的潛力並將其極大化。

因此，企業應更加重視「工作目的」，而非「工作地點」。

CISCO在2020年底發布「全球工作團隊調查」，企業員工普遍對未來工作的期望



98%

預期未來開會將會有
更多WFH參與者



58%

期望未來一個月可
以WHF 8天或更多



94%

希望能有更好的居
家工作協作經驗

CISCO：86%台灣員工希望能自由選擇工作地點

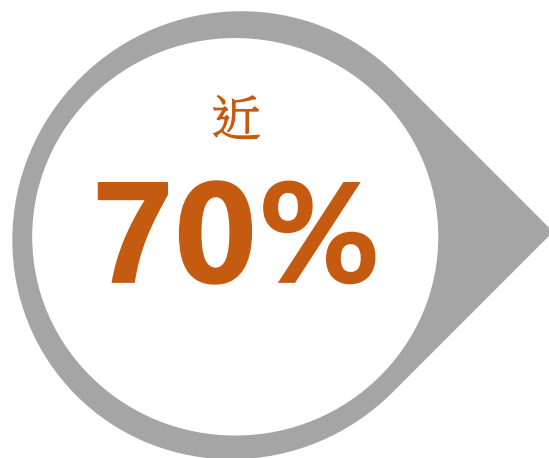
工作模式改變，也讓企業在人才晉用策略面臨調整。

人才是企業競爭力的關鍵，面對追求生活自由的Z世代及千禧世代，保持彈性靈活的工作模式將是未來企業吸引新技術人才的關鍵之一。

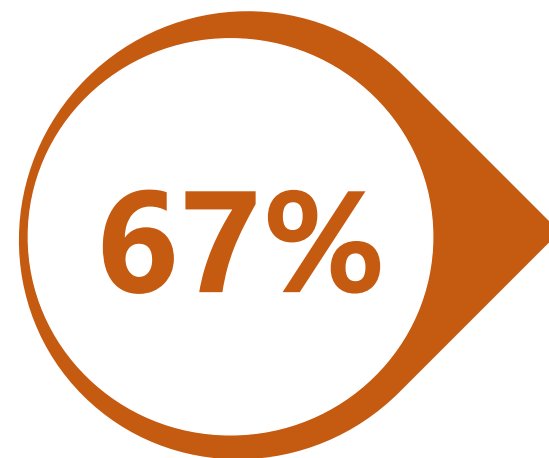
Cisco在《未來工作力研究報告(Workforce of the Future)》受訪的台灣員工調查



即使恢復正常，仍希望能自由地選擇在家或在辦公室工作及管理工作時間



遠距工作能夠讓他們有機會強化管理身心健康



希望繼續減少出勤，並認為對環境有益

資料來源：https://www.cisco.com/c/zh_tw/products/collaboration-endpoints/workforce-survey-2020.html

本簡報內容相關版權屬互動資通公司及各圖文引用來源機構所有

微軟：迎接職場環境的劇變

微軟發表「2021工作趨勢指數 (Work Trend Index)」調查結果，台灣部分



資料來源：<https://news.microsoft.com/zh-tw/>；ETToday新聞

Poly：混合式辦公是未來勢在必行的協作模式

企業要讓員工能在不同地點靈活工作，擁有沉浸且高效的工作空間，並且保障員工身心健康的工作模式。

Poly提出混合式新常態辦公的三大趨勢



新的工作模式

新的工作政策讓員工靈活選擇
辦公時間與辦公地點



成果導向型工作

企業不再將工作時間和地點視為
首要，更重視工作效率和成效



優化投資

跨越傳統辦公室思維，創建遠距協
作及技術支持型的個人工作空間



02

遠距或混合辦公 應掌握潛在資安風險

Thales：企業仍對遠距辦公網路安全問題感到擔憂

- 雖然許多企業已在評估混合辦公模式，但**82%的企業仍擔心員工遠距辦公存在安全風險**。
- 47%受訪者表示，在過去的一年裡，網路攻擊的數量、嚴重性與範圍都有增加。
- 在經歷過漏洞攻擊的企業中，有**41%是在2020年遭到攻擊**，與2019年相比，幾乎增加了一倍。
- 從全球調查來看：
 - 安全攻擊主要來自：**惡意軟件(54%)**，**勒索軟件(48%)**及**網路釣魚(41%)**。
 - 攻擊的發生原因：**內部威脅**和**人為錯誤**仍是關注的焦點。
 - 1/3的企業表示，惡意的內部人員(35%)和人為錯誤(31%)是面臨的最大風險，其次是**外部攻擊者(22%)**。
- 報告指出，在疫情期間，遠距辦公給企業帶來更大的風險，46%的企業報告指出，其安全基礎架構尚未準備好處理因疫情造成的風險。

混合辦公對企業的挑戰首要在「資安」

建置安全、靈活高效且在各環境間能無縫轉換的工作平台，是疫情帶給企業最大的挑戰

DO YOU KNOW

根據微軟亞太地區微軟數位犯罪防治中心(Microsoft Digital Crimes Unit, DCU)估計，
自Covid-19疫情爆發後，
網路駭客透過 網路釣魚(Phishing)和 勒索軟體(Ransomware) 的惡意攻擊
增加**五倍**

5月疫情爆發，防疫警戒升級，企業為了順利地維持營運，很多的措施是當下急就章決定。

因應居家上班的需求，企業必須讓員工從家裡連線到公司，存取工作上需要的資訊或連接重要的作業系統。為能即時溝通，也是使用一般社交IM軟體，並未有資安規畫或搭配解決方案，因此讓身為企業的資訊主管們十分擔憂。

微軟：台灣勒索軟體遭遇率位居亞太地區第5

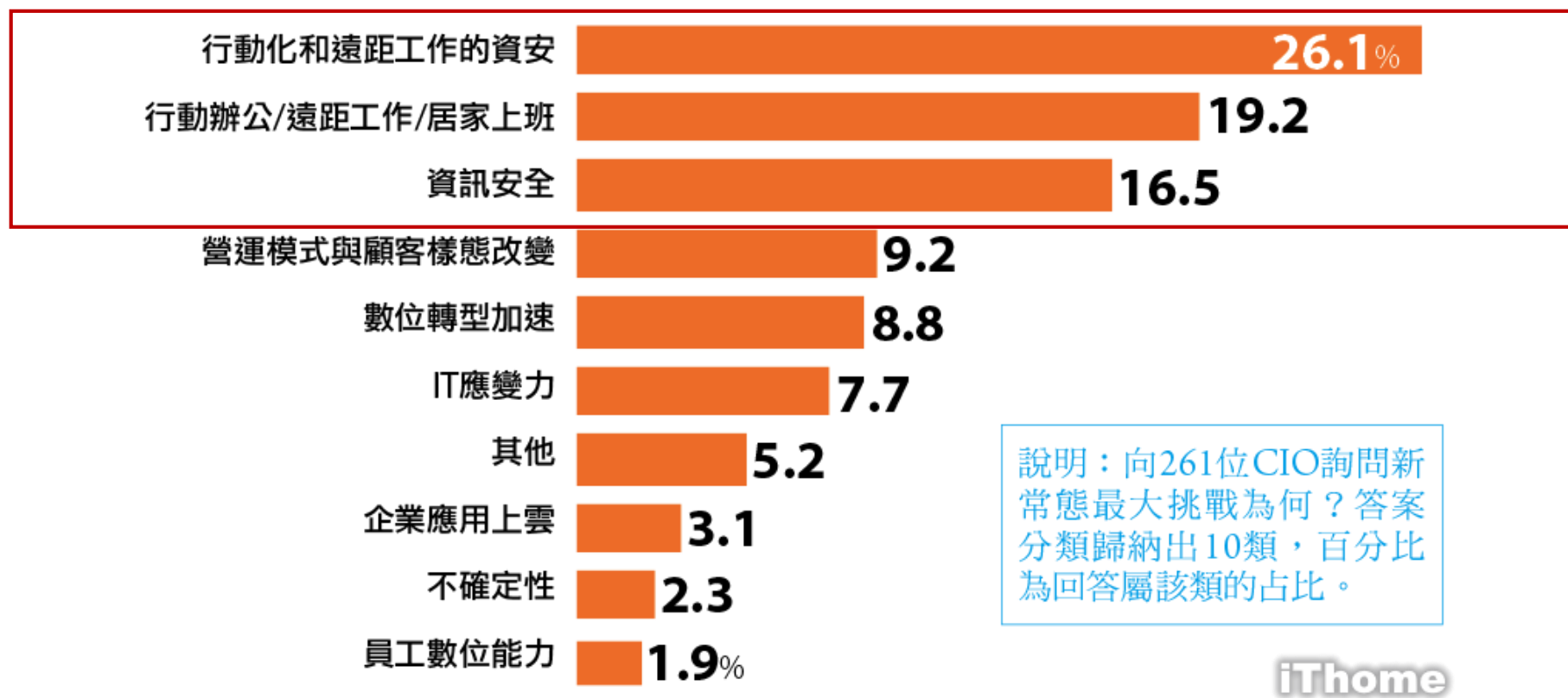
亞太地區包括台灣，有**超過98%是中小企業**，未必都有資安單位或人力。
企業宜盡速制訂資安防護策略，才能應變更彈性的混合辦公模式。

- 根據Microsoft Defender Antivirus 防毒軟體檢驗的資料顯示，亞太地區：
 - 遭受惡意程式攻擊的比率**比疫情之前平均提升19%**。
 - 遭受勒索軟體攻擊的比率平均則**比疫情之前提升240%（2.4倍）**。
- 其中，**台灣的惡意程式攻擊遭遇率增加了16%，勒索軟體更增加了407%**。
- **台灣勒索軟體遭遇率位居亞太地區排名第5**，僅次於紐西蘭（825%）、日本（541%）、中國（463%）及澳洲（453%）。

iThome：後疫新常態的資安是CIO最大的課題

iThome最新發布的2021年CIO大調查，疫後新常態的前三大挑戰都與行動化/遠距工作/居家上班及資訊安全相關。

近7成企業未來一年將準備強化 IT遠端工作能力。



資料來源：[iThome 2021CIO年大調查](#)



03

打造具資安層級的混合辦公情境

混合辦公迫使企業必須提高資安層級

除了內部溝通的訊息內容與視訊會議的加密保護外，更需強化員工在檔案資料的傳遞與存取上的安全性，**採用私有雲的地端架構，資料存放在客戶自行管理的伺服器中，是更加安全的考量。**

不僅考量提升營運效能、優化管理流程及加速數位化，更多的大型企業已將**資安防禦與產業專屬的客製需求**一併納入規劃，以因應混合辦公需求。



三大層面帶動企業尋找具資安防護的解決方案

不再依賴大眾IM
企業轉向尋找
高資安防護方案



互動資通觀察近一年半的變化，企業選擇溝通協作工具不只考慮便利性，更要求遠距辦公者與回辦公室上班者能有一致的操作經驗。

隨著攻擊不斷增加
企業轉向
安全的雲端服務



50%的企業表示超過40%資料儲存在外部雲端環境中。如何找尋安全雲端服務，成為一大資安考量。

不再只是添購設備
企業朝向全面
數位轉型建置



混合辦公不只是線上與實體工作場域交錯，企業需思考工作流程的改變、地端/雲端的IT環境、支援工作需要的數位資源及工具等的全面數位轉型。

您需要的資安防護 team+一應俱全

team+ 的資料儲存在企業專屬的私有雲伺服器，

還可以永久保存。即使團隊因任務完成而關閉，仍可以隨時查閱貼文、檔案與討論資料，業務交棒不漏接！



team+ 完整資安機制一覽

完善後臺管理機制

- 遠端刪除APP內容
- 帳號顯示版本資訊及最後時間
- 訊息稽核授權與查詢 (*)
- 操作日誌查詢(管理者)
- 團隊與交談室進階後台管理
- 大型交談室上限申請與管理(*進階資安)

登入/帳號 安全機制

- 企業員工身份驗證(AD同步) (*)
- 帳號權限分級(角色層級設定)
- 應用中心支援Single Sign-On
- APP安全密碼設定(可強制開啟)
- 企業代碼驗證功能
- 圖形驗證碼機制
- Web自動登出逾時未操作的使用者

(*)：為選配模組

檔案/訊息保護機制

【限制上傳】

- 限制上傳檔案格式
- 檔案發送限制
-(by平台/帳號 設定) (*進階資安)
- 支援整合防毒掃描、個資掃描系統(*)

【限制擷取/下載】

- 手機擷圖管理機制(*進階資安)
- 行動裝置檔案保護機制(*)
(手機檔案不落地)
- 影片串流化

【限制讀取】-企業成員

- TLS傳輸加密
- 限制使用APP
- 交談記錄-訊息查詢期限設定(*進階資安)
- 交談記錄-檔案查詢期限設定(*進階資安)
- 外網瀏覽檔案/通訊錄限制-by網路環境設定(*進階資安)
- 通訊錄查看限制-by帳號設定(*進階資安)
- 資料庫訊息加密儲存 (*)

【限制讀取】-外部人員(*)

- 邀請外部人員白名單權限管理
- 限制查看企業成員通訊錄
- 外部人員查檔限制(*進階資安)

【嚇阻與追蹤】

- 浮水印(*)
- 手機破解偵測裝置越獄(*進階資安)
- 檔案傳遞(上傳/下載)記錄(*進階資安)



智慧溝通 | 聰明工作
Working in a smarter way.

歡迎瀏覽互動資通官方網站，了解更多team+實用功能
www.teamplus.tech

