臺東縣政府
TAITUNG COUNTY GOVERNMENT

防疫期間異地或居家辦公資訊與網路風險態樣分析

臺東縣政府政風處

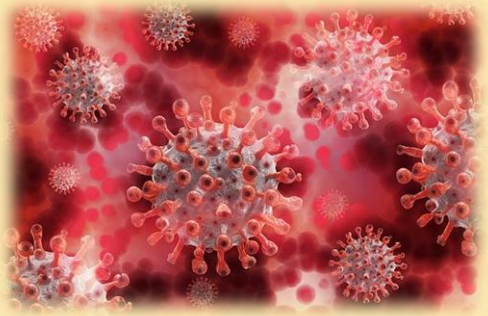
簡報大綱

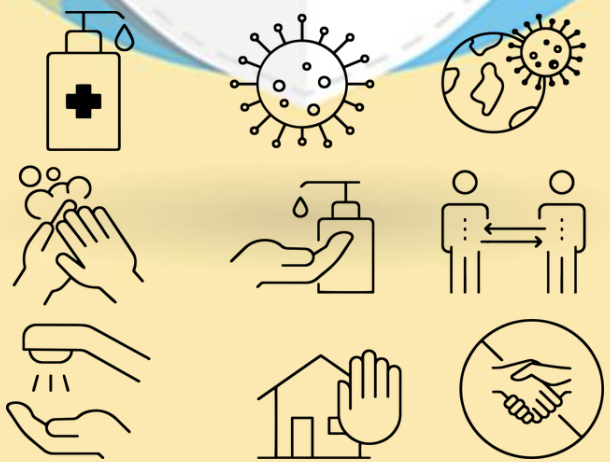
- 前言
- 異地或居家辦公之網路與資訊安全風險態樣
- 相應防範對策
- 結語

前言

自去（2020）年初新冠肺炎(COVID-19)爆發後蔓延至全球，至今雖因疫苗推出似見曙光，然疫情持續嚴峻仍未完全平息。疫情期間為避免對社會的衝擊擴大，各國政府皆視疫情發展，實施各種防疫管控措施，從自主管理、居家檢疫、社交距離甚至封城鎖國等，不僅打亂民眾生活步調，也影響民間企業與政府機關日常運作。

民間企業與政府機關為降低群聚與通勤的感染風險，實施遠距工作或居家上班措施，以期在防範員工感染之下，維持最大限度地正常運作。由於遠距工作或居家上班對各種通訊、線上會議軟體與網路之依賴程度更高，資安風險隨之升高。





異地或居家辦公之網路與資訊安全風險態樣

- **家庭網路未具備如民間企業或政府機關嚴密監控網路安全設施**

由於實施遠距或居家工作期間，一般會開放VPN(Virtual Private Network，虛擬專用網路，讓員工連線進入民間企業或政府機關內部網路，而家庭網路缺乏像民間企業或政府機關網路的嚴密防護管控機制，駭客可能會利用家庭網路漏洞當跳板對民間企業或政府機關網域發動攻擊，或找到VPN網路中具有民間企業或政府機關之關鍵數據作為目標，進一步竊取民間企業或政府機關機密資料。

備註：VPN(Virtual Private Network)是一個封閉的通道，把公司內各節點之網路連接起來，形成一個企業內部獨立且封閉安全的網路環境，且針對不同公司之資料，加裝特殊之封包資訊，避免無權限使用者或駭客無法進入該封閉的通道，達到通道內資料受到保護功能)。

異地或居家辦公之網路與資訊安全風險態樣

- **變臉詐騙**

在民間企業與公部門方面，趁全球眾多公司與政府機關持續遠距工作、居家辦公，而許多事務難以當面確認之際，駭客可能透過變臉詐騙（Business Email Compromise，簡稱BEC）手法，假冒供應商、公部門寄郵件給員工，謊稱要提供相關機敏檔案、變更銀行帳號或付款方式，誘使員工提供機敏檔案或逕行匯款。

異地或居家辦公之網路與資訊安全風險態樣

- **惡意郵件與網址釣魚**

在因疫情居家上班期間，以Coronavirus、COVID-19等為名的垃圾郵件、詐騙郵件，大量出現在個人的電子郵件信箱，相關的商業郵件詐騙、勒索軟體、惡意軟體、惡意網址等也隨之暴增。

趨勢科技公布的2020年第三季COVID-19相關威脅觀察報告指出，偵測到3千8百萬件電子郵件威脅，為最大的單一威脅類型，占比近8成。除依附在疫情相關議題之外，針對物聯網裝置、營運技術（Operational Technology，簡稱OT）層面的勒索軟體與攻擊亦呈現不減反增的狀況，顯示資安威脅在持續演變中，變得更加複雜且更具針對性。

異地或居家辦公之網路與資訊安全風險態樣

•頻繁使用即時通訊（IM）應用軟體易流洩公務或商業機敏資訊

常見的即時通訊軟體如LINE(日本與韓國)、WeChat(中國)、WhatsApp、Facebook、Instagram、Twitter(美國)等等，臺灣使用者數量龐大、使用頻率極高，對於IT預算有限的民間企業與政府機關，組織員工多會利用這些即時通訊（IM）應用軟體的免費、便捷性與分享性，當成居家(分區)辦公的的輔助工具；但相對來說，也就缺乏公私部門嚴密的管控機制，其開發者與伺服器若不在臺灣，而臺灣政府與企業無法進行監控，對於民眾日常溝通使用影響尚不明顯，但用在公務或商務溝通時，也等於是讓機關與企業的機密對話內容與重要文件等，全都存在國外伺服器紀錄軌跡上，不免產生資安外洩的疑慮，一旦發生資料外洩或安全事件時，亦增加監管單位調查與追蹤難度。

異地或居家辦公之網路與資訊安全風險態樣

- **不當視訊會議軟體資安疑慮及隱私侵犯**

以被美國政府機構、軍方單位、NASA、哈佛大學、部分企業如Google、臺灣行政機關與公立學校等相繼宣布停用之爭議視訊會議軟體ZOOM為例：

ZOOM預設會將會議設定為無密碼，使用者可以輕鬆登入，以致自己的視訊會議會莫名被陌生人「亂入」，發生會議流程被侵入、搗亂甚至掘取等資安危機。

知名的資安公司Sixgill就曾發現有多達352組的ZOOM帳號密碼，以及相關的會議ID、用戶姓名等個資，都被放上暗網出售的案例，其中更包括不少付費帳戶，在在突顯了ZOOM軟體「偏重使用方便性」而「降低資安管控層級」。

異地或居家辦公之網路與資訊安全風險態樣

- **不當視訊會議軟體資安疑慮及隱私侵犯**

Mac版ZOOM曾被爆出一項重大漏洞，於未經用戶同意就將用戶連結到特定的ZOOM視訊會議，並開啟Mac的鏡頭(後已被APPLE修正)；另外，Windows版ZOOM用戶如果在聊天室傳送特定字串，會產生一個特殊的Windows連結，可能讓電腦因此被遙控，其他缺失，還包括用戶可以輕易在 Google搜尋引擎，找到部分會議的視訊內容。

雖然ZOOM軟體所屬公司宣稱已在所有應用程式層面，加採256位元AES加密，但多倫多大學的研究員卻發現，其視訊會議其實只採用128位元的金鑰，來加密用戶的視訊會議或錄音檔；《The Intercept》也發現ZOOM的資安白皮書宣稱自家軟體支援了點對點加密(End-to-End Encryption)，但實際上點對點加密僅在聊天室上實現，最重要的視訊會議則沒有。

居家(分區)辦公之網路與資訊安全風險態樣

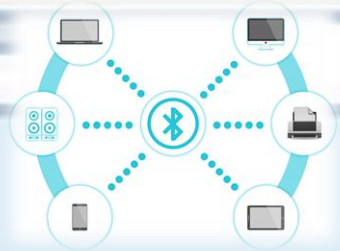
- 不當視訊會議軟體資安疑慮及隱私侵犯

相應防範對策

- **網路連線與伺服器開放方面**

由於VPN伺服器是常被駭客攻擊的對象，各機關資管人員須確認伺服器是否為最新版，而外部網域管理方面須落實VPN帳號盤點，全面開放或僅針對需要的員工開放，區分群組給予不同的權限與連線範圍，並透過內部網路的網路流量監控機制，確認VPN使用無異常狀況。此外，在內部資料管理方面亦須依照機密或重要性區分存放位置與取用權限，如移轉至雲端或伺服器，遠端取用管制，或存放在個人電腦端等。

網路連接方面，盡量不要使用公共Wi-Fi連接公司或機關網路，或公共電腦登入公司或機關系統，必要時可使用手機熱點或透過VPN連接網際網路，以免被側錄或竄改等；連線時，確認取得之內部網路或網際網路的IP位址是否正確無誤；在公共環境工作時，將電腦的藍牙等非必要連線管道關閉，可避免有心人士透過該管道攻擊個人裝置。



相應防範對策

- **訊息回覆與網址驗證方面**

請勿回覆不明來源提出的資訊要求，特別是提出與個人身分有關的資訊或密碼的要求，不肖分子會試圖假冒成當事人可能認識的親友或者同事來誘騙其分享機密資訊。要特別注意當事人將資訊分享給誰?即使認為這項要求是來自可信任的機關或公司亦須謹慎，無須立刻回覆，務必冷靜並保留充裕的時間來查證這項要求的來源、思索這項要求是否合適，再採取行動。

於分享機密資訊之前，請先驗證網址，不肖人士會創立一個非常擬真的詐騙網頁，不論是網址還是主頁面都看起來很像使用者所信任的網站，例如衛生所通知施打疫苗、銀行、或者電子郵件服務提供者，爰建議不要使用電子郵件中所附的連結，而係直接使用鍵盤輸入網址來連結信任的網站。此外，尚須確認所造訪的網頁網址當中含有HTTPS，這類的網站比網址中含有HTTP的網站更安全。

相應防範對策

- **電子郵件與網頁連結方面**

只在信任的網站或者郵件中點擊連結、開啟附件，或者下載軟體，大多數人都想要掌握最新的資訊，在疫情持續嚴重、變化多端的時期更是如此，而不肖人士會利用這一點，傳送夾帶似乎有用的資訊連結，誘使不知情的使用者點擊，進而透過惡意連結以取得個人、政府機關或民間企業的機敏資訊，甚至凍結使用者的電腦或網路，若對資訊來源有所疑慮，務請先查詢機關或公司主要網頁，因為重要訊息理應公告於官方網頁(Official Website)上。

針對釣魚郵件充斥的風險，政府機關或民間企業應設法提供具備郵件過濾機制的安全郵件使用環境，做好郵件安全防禦，再搭配定期的教育訓練與社交工程演練，提高員工的警覺性。

相應防範對策

- **設備監控與資料儲存方面**

政府機關或民間企業平時若未配置可攜式辦公設備給員工，面對緊急情況時須盤點設備是否充足，若設備不足，折衷於短期開放員工透過自有設備進行連線，因此須對非管控範圍內的設備進行安全檢核，並進行遠距工作行為監控，以免成為駭客攻擊的破口。

當員工將資料下載儲存在遠距工作的設備時，政府機關或民間企業將無法控管資料被上傳到雲端或未加密儲存的狀況，建議各機關(單位)應針對移動設備進行資安管控，降低資料未被及時刪除、設備遺失，所造成的資料或公務機密外洩風險。

相應防範對策

- **個人軟硬體設備保存使用方面**

員工個人設備使用方面，用來存取業務相關之政府機關或機關內部網路的電腦，須定期更換登入密碼，並嚴格遵守禁止將其作為非公務用途之原則，也應避免職員以外人士操作該電腦，若常於公共空間工作，可以為個人筆電安裝螢幕防窺片，或離開電腦時立即設定螢幕保護程式並鎖定，常須攜帶移動時，對於尋找、鎖定以及遠端清除資料等遺失因應機制須完整設定、定期備份保存，以避免因設備遺失導致資料外洩。

於居家(分區)辦公、遠距工作期間，個人處理公務所使用之通訊硬體設備、資料儲存設備，如桌上型電腦、筆記型電腦、平板電腦、智慧型手機、USB隨身碟、記憶卡、光碟片等等，應妥善保管避免失竊或毀損，且盡量不外借其他人員接觸使用，防範公務資料外洩；另外，上述設備，並請安裝與定期更新正版防毒軟體，並定期掃描，防止駭客利用病毒程式入侵並竊取個人資料。

相應防範對策

- **即時通訊軟體與會議室訊軟體方面**

疫情期間召開視訊會議，建議採用有端到端加密（End-to-End Encryption，簡稱E2EE），以確保機密內容只有內部人員才能解密。而期間若不幸發生資安事件，負責處理團隊、處理方式等標準作業流程，亦須事先規劃研擬，才能快速處理降低損失，目前行政院鼓勵中央與地方政府機關以及國內企業團體盡量使用國產通訊軟體，例如Juiker，相對安全保密且伺服器位於國內方便追蹤與控管。

進行線上會議時，視訊設備、軟體測試須事先準備與完成，並熟悉同時發言、分享檔案等遠端操控功能，以確保會議品質與效率。此外，會議軟體等是否加密等安全性也是須注意的環節。

因疫情持續，各機關(單位)遠距工作、居家(分區)辦公或成常態，為兼顧機敏資訊保密、網域安全保障，目前公部門常使用且相對安全之會議視訊軟體有Google Meet及Hangout、Microsoft Teams、Cisco Webex等。

結語

硬體設備保存完善，軟體資料使用謹慎，居家(分區)辦公、遠距工作資訊安全、網路安全與在辦公室同步監控不鬆懈：

一、正視網路環境安全問題

二、強化個人設備資安監控

三、提升外在設備資料保護

四、遠距工作平台機密保護

五、強化員工網路安全認知

臺東縣政府
TAITUNG COUNTY GOVERNMENT

資訊安全 人人有責
保密防駭 你我共進