淺談資安風險管理
以遠距視訊爲例

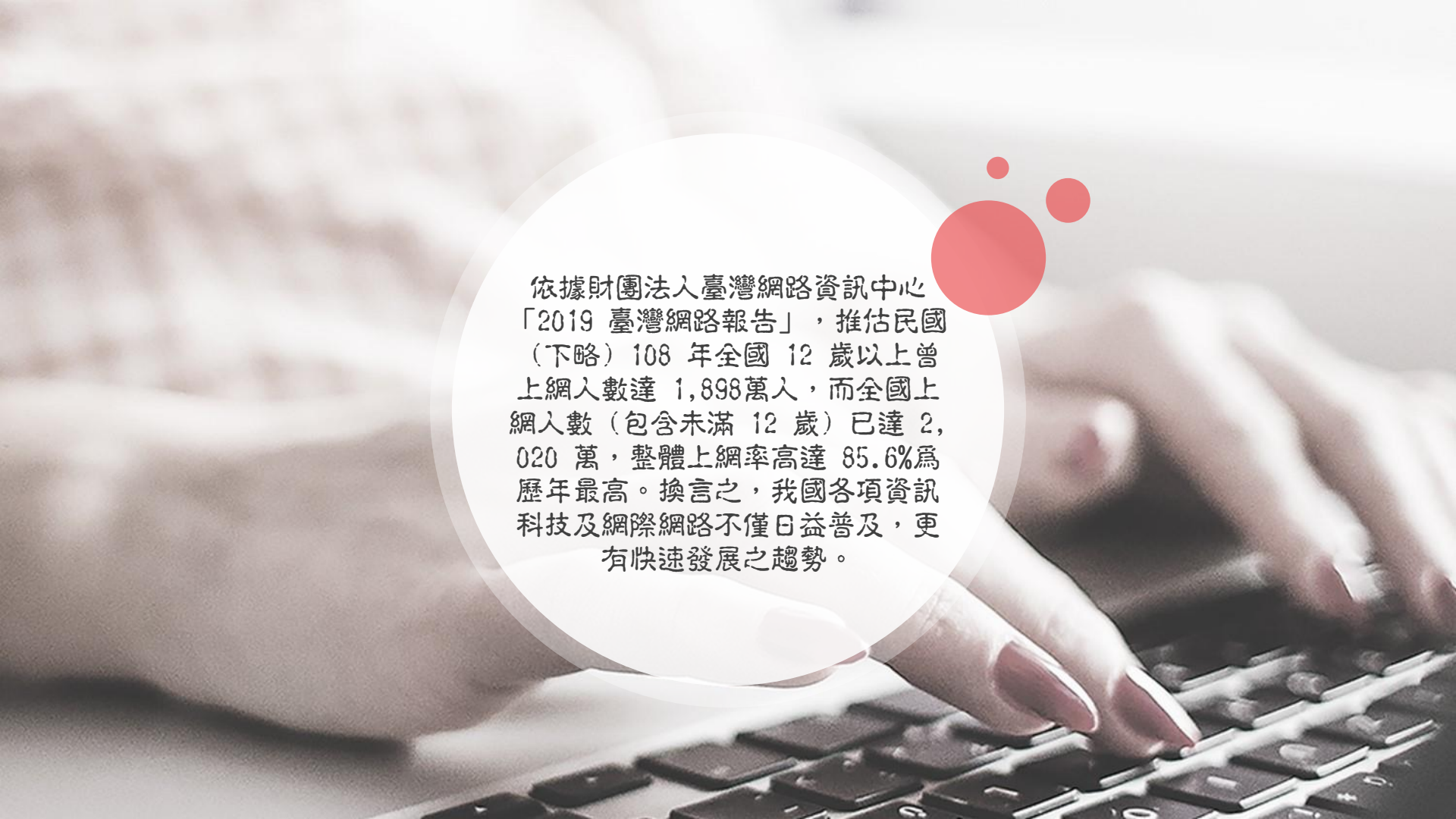
苗栗縣政府政風處
9月份公務機密維護宣導

資料來源：法務部調查局雙月刊2020年9月號

作者：金門縣政府政風處專員　陳大中

目錄

現況概述



依據財團法人臺灣網路資訊中心「2019 臺灣網路報告」，推估民國（下略）108 年全國 12 歲以上曾上網人數達 1,898萬人，而全國上網人數（包含未滿 12 歲）已達 2,020 萬，整體上網率高達 85.6%為歷年最高。換言之，我國各項資訊科技及網際網路不僅日益普及，更有快速發展之趨勢。

資安破口及損害

然隨著網際網路及其他資通科技之迅速發展，亦帶來資訊安全危機，如：銓敘部 108 年 6 月間經報導指出超過 24 萬筆個人資料遭外洩，台積電於 107 年 8 月初設備遭電腦病毒 WannaCry 感染，該次中毒事件影響台積電營收估計新臺幣 25.96億元（依台積電 107 年第三季財報據），足堪為我國史上損失最大的資安事件。今年 5 月間不僅國內多家重要能源及科技公司接連遭勒索軟體攻擊，甚至爆發位列資通安全責任等級最高級 A 級之總統府電腦也遭駭客入侵事件。

視訊軟體
Zoom之資安隱憂

全球因受新冠病毒蔓延影響，遠距視 訊軟體開始廣泛使用，其中 Zoom 視訊軟 體資安疑慮遭連環踢爆，先是該視訊軟體將加密金鑰存放位於中國大陸的伺服器，有 遭駭客竊聽之虞。隨後爆發英國金融時報 記者藉由竊聽其他報社運用 Zoom 視訊軟 體召開的會議，刺探其他報社之新聞訊息。 不僅如此，香港中文大學使用 Zoom 視訊軟體進行遠距考試，系統被不明人士駭入， 考試時透過該軟體分享個人電腦螢幕，播 放色情成人片、舞曲 MV 等，Zoom 的各種 資安事件接踵而來地發生。因此，電動車大 廠特斯拉、美國國家航太總署及英國國防 部等機構陸續宣布禁用 Zoom 軟體。

資安風險管理步驟

資安風險管理四步驟

識別風險因子

01

應對其本身及所屬部門之資安風險全面確實掌握。應審酌不同業務屬性，可能潛存的風險因子，做出可識別的異質性資安風險因子，此爲管理的基礎，亦爲最重要的步驟。

進行風險評估

02

針對可能存在的資安風險，逐一分析評估曝險係數、發生可能性、發生時之影響程度、損失預期範圍及處理之優先順序等，確實風險分析與評估，以爲後續有效之管理與因應。

檢視風險成因

03

深入檢視風險成因，瞭解可能之外在威脅與本身潛存之弱點，透過確實認識可能造成資訊設備、系統危害或威脅之外在影響因素，；以及掌握資訊系統或資訊設備本身可能存在的弱點，清楚分辨外在可能危害之威脅與內在潛存之弱點。

提出風險因應

04

提出最適切之風險因應，當風險經識別出來及評估後，須提出相應之處理計畫，處理方式大致上可區分爲避免風險、轉移風險、降低風險及接受風險。

結語

資訊安全不僅是安全與便利的取捨，更關係整體國家安全與國家利益，近年政府爲強化資安工作，陸續完成相關法制作業，然徒法不足以自行，若要達到有效資安防護，就須做好妥善之資安風險管理，並逐步落實資安環境的改善，減少風險的存在，並培養資通使用者之資安觀念及敏銳度，提升其資安防護之素養與能力，如此方能建構更臻完妥之資通安全防護網。


廉政專線：037-356639
苗栗縣政府政風處
關心您~