台灣資安發展面面觀

摘要

COVID-19 疫情催化企業加速數位轉型的腳步，但也帶來更多資安攻擊事件。從全球資安發展趨勢來看，連美國將網路安全視為國家安全領域的重中之重，另外資安事件帶來龐大商機，形成全球資安獨角獸公司，表示企業越來越多注重資安防護力。台灣原本就是駭客攻擊熱區，2020 年疫情期間每 4 家大型企業就有 1 家遭遇 50 次以上資安攻擊事件，從目前資安相關調查報告皆顯示，台灣企業在資安防護仍待加強，即便是資安標竿的金融業因金融網路犯罪利益巨大而面臨高度挑戰，不過，隨著企業對資安投資增加，也可為台灣資安產業發展帶來新的機會。因此，企業在面對資安議題所提出之建議，包括(1)企業更重視資安，將可為企業加速數位轉位奠定基礎；(2)從外洩個資來看，企業內部應加強員工資安教育，降低資安風險的發生；(3)資安產業化，首重人才養成，企業可採分潤機制，延續產學研協力合作模式，並將目光投射到全球市場，發展出屬於台灣的國際級資安產品與資安產業。

前言

COVID-19 疫情籠罩全球，不僅造成全球經濟嚴重衝擊，也替產業帶來不可逆的影響與轉變，遠距辦公、居家避疫已成為新的生活型態，線上連網及網路服務用量增加成為新常態，間接地為資訊安全帶來威脅，尤其企業在資訊安全環境缺乏保護，常面臨駭客攻擊，資安風險也比過往增加很多。依據微軟 2021 年 7 月 1 日公布《遙測分析報告(Microsoft Defender Antivirus)》指出，在疫情前至今的 18 個月內，駭客每天平均發動 5,000 萬次密碼攻擊，相當於每秒 579 次，光 2020 年一年內截獲 300 億封電子郵件威脅，2020 年疫情期間因網路駭客攻擊的受害者付出的贖金高達 3.5 億美元，年成長 311%，平均每個受害單位須支付 31.2 萬美元，以換取正常網路營運，並指出 2022 年網絡犯罪對全球經濟的影響將達到 240 兆台幣(8 兆美元成本)，顯示出疫情期間全球防駭更不可輕忽。

在台灣方面，2020 年 5 月中油、台塑 2 家石化廠商受到勒索軟體攻擊、11

月筆電代工大廠仁寶電腦(Compal)、工業電腦大廠研華科技（Advantech）也傳出類似遭勒索軟體攻擊資安事件等，海外分公司也沒例外，像臺灣銀行洛杉磯分行員工因疫情居家上班而遭到商業電郵詐騙千萬元、鴻海(Foxconn)墨西哥CTBG 工廠也遭勒索 3,400 萬美元等。美國網安諮詢公司「記錄未來」（Recorded Future）2021 年 7 月報告指出，疑似中國資助的團體正鎖定台灣電信組織，甚至有針對台灣半導體產業為主要的大型駭客行動，近期則以台灣技術研發、育成台灣科技公司的工研院為攻擊目標。

據國際數據資訊(International Data Corporation, IDC)統計，2019 年全球資安產業產值高達 1,066 億美元，每年並以 12%-15%速度持續成長，相關支出累計更已達 1 兆美元。再觀察全球資安指數(ISE Cyber Security Index)，自 2020 年 3 月 23 日最低點反彈至 2021 年 7 月 23 日已上漲 106.2%，強於道瓊指數漲幅 82.9%，顯示投資人也認同網路安全產業前景的成長性，資本市場對資安評價提升，資安將在全球疫情期間升級成為重要產業之一。

蔡總統也喊出「資安即國安 2.0」的政策方向，從過去的政府組織內部設置資安部門、到「資通安全管理法」等逐步建立基礎，而今宣示的 2.0 戰略，除了新設數位發展部外，也要利用台灣作為國際資安攻防熱區，將台灣資安挑戰轉換成第一線練兵場域，增進台灣資安產業的防衛優勢。從全球產業鏈分布來看，網路安全相關硬體設備有超過半數是由台灣 OEM，台灣既然在相關硬體製造處具有優勢，是否能讓資安產業在此立基下取得相似的商機？本文將從近期全球資安問題談起，瞭解資安議題走向，及台灣資安問題與產業發展契機，以提供業者參考。

近年全球資安發展

依據全球領先的企業軟體創新者 VMware 公布《2021 年全球安全洞察報

告[註[1]]（Global Security Insights Report）》指出，數位轉型加速迫使企業必須面對不斷演進的資安威脅，有 8 成企業表示疫情期間因員工居家辦公而遭受網路攻擊。81%受訪者表示過去 1 年中因網路攻擊而發生資料外洩事件，每家企業或組織遭受攻擊的平均次數由 2020 年 6 月調查的 2.17 次增加至 2.35 次，且 82%屬重大情節。56%受訪者擔心 2021 年仍會出現重大外洩事件，目前只有 41%受訪者是已更新資訊的安全政策及方法，來降低外洩的風險，此顯示，企業不僅低估重大外洩事件發生，即使資安事件大幅增加下，企業也缺乏緊急應變能力。

這個現象可從 2020 年年底美國爆發有史以來最大的資安事件看出，軟體公司 SolarWinds[註[2]]主要是供應政府和企業網路監控和管理軟體或服務的供應商之一，在 2020 年 2 月 SolarWinds Orion 平臺就被俄國駭客 Nobelium 植入木馬系統，直到 2020 年年底才東窗事發，不僅美國電信商、財政部、國土安全部、商務部（Department of Commerce）及國防部等受影響，受害者還遍及歐洲、亞洲和中東地區的政府、科技公司和電信公司等，且駭客動竊取美國政府機密，未來可能透過這些機密影響美俄政策，為此，美國在 2021 年 4 月 15 日宣布對俄羅斯實施一系列新制裁，以報復俄國涉嫌 SolarWinds 駭客攻擊事件及干涉大選等不當行為。另一個重大資安事件是 2021 年 5 月 7 日美國最大燃油管道系統 Colonial Pipeline[註[3]]遭到勒索軟體 DarkSide 攻擊，由於該公司負責美國東岸約 45%的燃料供應，並因攻擊事件而暫停所有的管道作業，此事讓美國政府在 5 月 9 日宣布美國進入緊急狀態（State of Emergency），也破例讓當地燃油業者透過一般道路運送燃油，以緩解燃油短缺問題。

微軟的《Microsoft Defender Antivirus 遙測數據》報告亦指出亞太地區 15 個市場遭受惡意軟體與勒索軟體的遭遇率，如表 1 所示，除了比疫情爆發前平均提升 2.4 倍外，其中台灣惡意程式攻擊遭遇率增加 16%，勒索軟體更增加 407%，台灣勒索軟體遭遇率位居亞太地區排名第五，僅次於紐西蘭(825%)、日本(541%)、中國(463%)及澳洲(453%)，同為亞太區勒索軟體攻擊的五大熱區。

表 1　亞太地區遭受資安攻擊增加率

單位:%

次序	亞太地區	惡意程式	勒索軟體
1	紐西蘭	↑19	↑825
2	日本	↑16	↑541
3	中國	↑80	↑463
4	澳洲	↑23	↑453
5	台灣	↑16	↑407
6	新加坡	↑43	↑296
7	香港	↑38	↑179
8	印度	↑15	↑100
9	斯里蘭卡	↑12	↑74
10	南韓	↑22	↑64
11	菲律賓	↑15	↑70
12	馬來西亞	↑ 2	↑72
13	印尼	↑24	↑31
14	越南	↑ 7	↑15
15	泰國	↑ 3	↑ 6

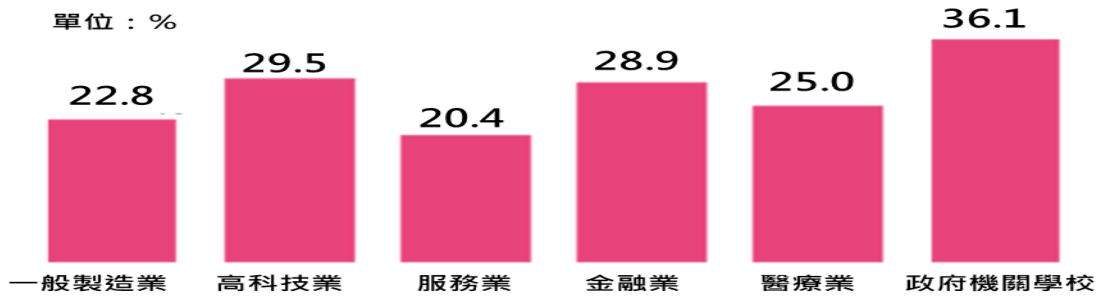
資料來源：https://news.microsoft.com/zh-tw/microsoft-info-security-hotspot-taiwan/

全球資安攻擊事件日益嚴重，像美國都已開始檢討既有網路安全政策及相關制度，包括整合公私部門的既有網路威脅情報，要求私部門必須有所作為對企業內的資安漏洞負起責任，確認使用第三方軟體供應鏈的網路安全，再則要強化政府部門間協作能力，建立整體網路安全戰略，另美國也對飽受駭客攻擊的歐洲各國，一改川普總統「美國優先」政策，反而積極倡議建構大西洋盟友共同網路防禦陣線，共享共同敵國的駭客威脅情報等。

另一方面，資安事件也帶來龐大商機，美國資安公司 Fortinet 的營收由 2018 年 18.04 億美元到 2020 年的 25.94 億美元，成長 43..8%，近三年股價漲幅超過 354%，2021 年全球有 19 間從事網路安全相關領域的企業進入獨角獸行列，其中以成立不到 15 年就擁有 90 億美元市值的網路安全和系統管理公司 Tanium 位列榜首，為當前網路安全巨頭，也是目前最成功的網路安全獨角獸公司。

台灣資安概況

台灣因地緣政治而長期處在駭客威脅中，2020 年更因疫情肆虐下，國內企業廣泛地應用雲服務、物聯網等新興科技，遠端工作、智慧生產及網購等行為達歷史高峰，台灣更成為資安攻擊的熱區。依據《iThome 2021 企業資安大調查》[註[4]]，2020 年每 4 家國內大型企業中，就有 1 家遭遇 50 次以上資安攻擊事件，如圖 1 ，其中政府機關學校最嚴重，每 3 間就有 1 間受到攻擊 50 次以上攻擊事件；高科技業與金融業次之，比率 29.5%及 28.9%。而能在一天內復原正常運作的企業，2020 年比例有 69.8%，比 2019 年的 65.9%與 2018 年的 63.1%高，但是也有 30.2%企業需要一周以上才能復原。今年企業能加速資安事件復原的主要原因是對強化數位韌性投入的企業比例大幅增加，從 2020 年 6.4%提升到 2021 年的 11.6%。

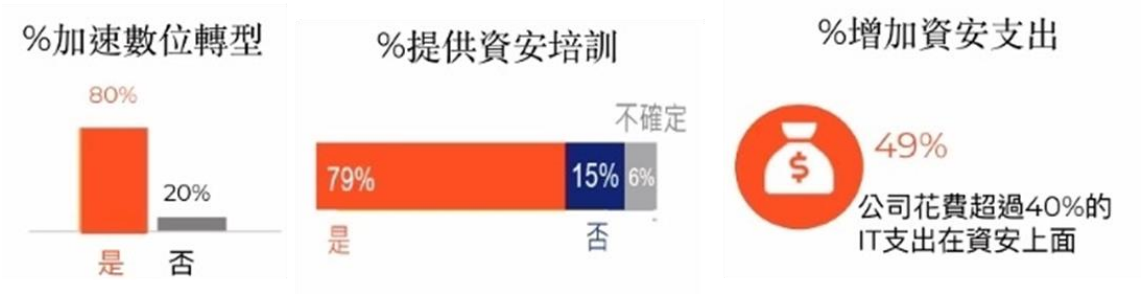


資料來源：iThome 2021 企業資安大調查

圖 1　台灣各產業遭受資安事件超過 50 次以上的占比

另一家資安公司 Palo Alto Networks 公布《2021 台灣資安現況報告》[註[5]]發現，多數的台灣企業認為疫情為遠端工作模式帶來更多資安上的挑戰。有 60%企業面臨雲端服務和應用程式帶來的新風險、有 59%企業認為居家工作期間難以監控和管理員工的「網路衛生」，有 57%企業認為面臨員工使用個人裝置和家庭網路訪問會對公司網路的風險。為因應疫情帶來的資安挑戰，有 66%的

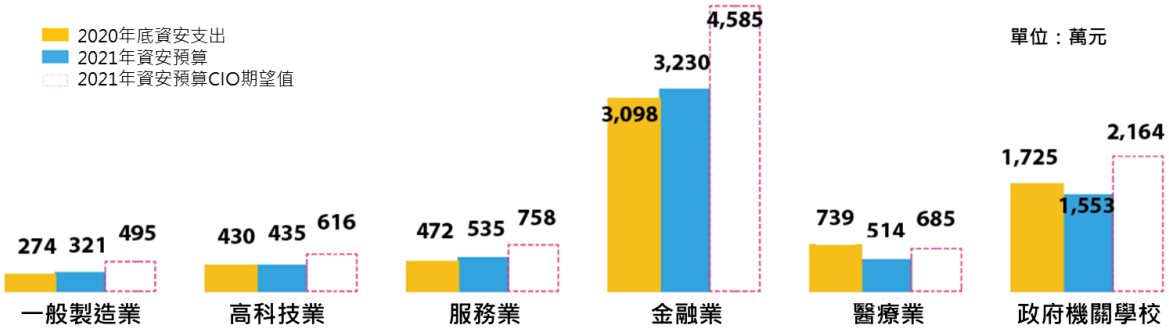
企業認為應強化內部的資安部署。因此，企業所採行措施，如圖 2 所示，有 80%企業是透過加速數位轉型，其中又以金融服務、醫療保健和電信產業最積極；有 79%企業提供資安培訓課程，以提升員工資安意識；有 49%企業願意在資安方面花費逾 40%的 IT 支出。



資料來源：陳映璇(2021.6.29)，《遠距辦公恐成攻擊破口？近 5 成企業增加資安支出、「零信任」五大原則防堵威脅》,數位時代

圖 2　台灣企業因應資安事件所採取的行動

台灣產業對資安投資情形，也可從《iThome 2021 企業資安大調查》獲知，2020 年因疫情關係，資安威脅變得更嚴峻，企業對異地備援與災難復原需求大增，平均資安支出為 789 萬元，2021 年平均資安預算雖下滑至 772 萬元，恢復到常態，但資安占 IT 支出的比重為 4.8%，高於 2020 年 4.2%及 2019 年的 4.9%，此意謂著企業對資安投資還是重視，並未隨著預算降低而減少。調查中亦指出，CIO 認為台灣資安投資應再增加，才能強化資安防衛能力，如圖 3 所示，包括金融業投資金額 2020 年支出額平均達 3,098 萬元，是所有產業中對資安投資最高者，2021 年雖編列 3,230 萬元，但 CIO 認為應增加到 4,585 萬元，另外是製造業，2021 年投資預算平均僅 321 萬元，雖較 2020 年成長 17%，CIO 也認為應成長 54%。



資料來源：如圖 1

圖 3 台灣各產業資安投資概況

安侯建業(KPMG)首次發表的《臺灣本土企業的資安曝險大調查》[註[6]]顯示，台灣企業平均網路防護分數為 78.68 分，在四大面向指標[註[7]]表現上，「安全性」成績明顯落後，調查中的 50 家大型企業中，就有 11 家企業的安全性分數不及格，若依產業別，除金融業外，電子零組件製造業、一般製造業、電腦及設備製造業、通訊業的平均安全性分數皆低於 75 分，其中電腦及週邊設備業最需加強網路防護，不僅平均網路防護分數墊底，更有高達 8 成企業排名墊底，網路防護亟待加強。金融業網路防護表現最佳，但仍面臨高度挑戰，主要是金融網路犯罪利益巨大，加上廣泛使用雲端儲存、資料分析工具並與多元的第三方合作而擴大曝險面積，至今仍是駭客集中攻擊的標的。

綜合前述，金融業因主管機關的高度監理及國際信評機構評比壓力，為了避免資安事件而觸法遭到重罰、信譽被降級等事件，造成營收重大損失，對資安投資要求相對其他產業高出許多，是台灣企業的資安標竿，即便如此，因豐富及高財富資產誘因，至今仍是駭客攻擊熱點。另外，電子零組件製造業、通訊業與電腦及周邊設備製造業被稱為「高科技產業」，在全球產業供應鏈扮演關鍵角色。因擁有關鍵技術等重要營業秘密而遭攻擊，近年也轉為更明目張膽地進行系統綁架與財務勒索、商業郵件詐騙等事件，更突顯台灣高科技產業的網路防護明顯落後，也提醒高科技業加強其資安防護的重要性。因此，面對未來資安挑戰必然更

加嚴峻，台灣企業應更看重「產業資安化」，要推動各產業落實資安，並期望讓企業更札實地一步步做好資安。在此同時，隨著資安防護量能增加，便可加速資安產業化發展的契機。

建議

從國際資安發展趨勢來看，連美國都將網路安全視為國家安全領域的重中之重，除了網域資安機制調整，亦朝向國際的合縱連橫，包括民間企業及政府間協力合作，以抵禦大型的惡意網路攻擊行動，另一方面也為資安產業化帶來發展商機。台灣企業除了要加強產業的資安防護力，隨著企業資安投資的增加，也可為台灣資安產業發展帶來新的機會。因此，對企業在面對資安議題所提出之建議：

(一)企業更重視資安，將可為企業加速數位轉位奠定基礎

疫情、5G 應用擴展加速企業數位轉型，也為企業帶來更多資安問題，尤其是大量關鍵設備採用連網方式，讓資料網路的資訊技術(IT)與工業控制系統的操作技術(OT)間的界線變得模糊，網節點的資安防護成為企業數位轉型時不得不正視問題，特別台灣智慧製造在全球供應鏈扮演重要角色，更應重新審視數位轉型下的如何部署完善的資安防護。像台積電為 2018 年 8 月機台中毒損失 26 億元事件，讓他們深切瞭解資安的重要性，於是 2019 年成立供應商資訊安全協會，結合半導體產業鏈與國際標準組織，推動全球第一個半導體資安國際標準，也促進半導體與資安跨域合作商機。產業透過供應鏈資安風險評鑑、資安實務合作與分享，持續強化供應鏈資安防衛，為加速企業數位轉型奠定更好的基礎。

(二)企業內部應加強員工資安教育

從趨勢科技 2021 年首度發表《台灣關鍵基礎設施網路曝險報告》[註[8]]，報告中指出外洩個資數量最大宗為高科技製造業，占總件數 7 成；以外洩資料數量加上企業員工數來看，通訊傳播業每名就有 1 位員工個資遭洩。再以員工資料外洩比例，依序為通訊傳播類比重最高，達 23.26%、緊急救援與醫院的 16.0%、

政府機關的 10.9%、能源產業的 9.0%及科學園區與工業區的 8.4%。而員工個資易外洩原因，除了企業系統或程式出現被攻擊弱點、還有員工的資安意識不高，在自身密碼建置或釣魚郵件等而資料外洩。尤其員工是企業資安防護最前線，若沒有足夠資安意識，可能易被駭客誤導，而造成惡意軟體感染與意外資料外洩的錯誤。因此，企業應更重視員工個資安全，並強化相對應的安全防護措施。認識資安威脅為起點，教育並確保員工了解資安漏洞對公司或組織的影響，降低資安風險的發生。

(三)資安產業化，首重人才養成

根據 MIC 及 IEK 研究，台灣的資安產業市場規模在 2021 年可超過 530 億元，但台灣有超過 400 家以上資安公司在 Y2020 年以前的營收低於新台幣 1 億的的比重約 96%，分析其原因表示，台灣資安產業看似蓬勃發展，但實際是受制人力規模與能力素質，只能以技術檢測或演練服務獲取營收，無法發展成為長久經營的商業模式。因此，台灣資安要產業化，首要在資安人才的養成，尤其現在的各種網路攻擊手法越來越複雜，無論是政府或是企業、產業對具備攻防實務的資安高階人才的需求更是殷切，目前政府推出《臺灣資安卓越深耕計畫 - 資安卓越中心計畫(2021～2025 年)》，從頂尖實戰人才養成、實習場域建置、國際合作及技術移轉創新育成等面向，著手資安人才培育計畫。企業方面則可更務實地透過產學合作機制，如採分潤機制回饋學研單位對相關資安的人才培育及研發，延續產學研協力合作模式，並將目光投射到全球市場，藉由這波 5G、大數據、人工智慧、物聯網等新興科技趨勢，發展出屬於台灣的國際級資安產品與資安產業。

[1] 係針對全球 3542 位企業資訊長(CIO)、數位技術長(CDO)及資安長(CISO)進行線上問卷調查，以瞭解網路攻擊與資料外洩事件對企業機構所帶來的衝擊

[2] 總部位於德州奧斯汀，全球市場規模為 115 億美元，擁有逾 3200 名員工

[3] 總部設於喬治亞州的 Colonial Pipeline 是美國最大的精煉油管道系統，每天運送多達 1 億加侖的汽油、柴油、航空媒油與家用燃料油，占美國東岸燃油供應的 45%，也負責美國 7 個機場的燃油供應

[4] 以台灣 2 千大規模的企業為主，針對 iThome 歷屆 CIO 大調查企業、政府一級機構、大專院校 IT 和資安主管，進行線上問卷調查。調查時間 2021 年 3 月 8 日到 4 月 5 日，有效問卷數 439 份。68.4%填答者是企業資安最高主管

[5] 於 2021 年 4 月線上訪問台灣金融服務、醫療保健、教育、製造、高科技、電信、零售和政府等 8 大產業的 300 名企業 IT 決策者和業務領導者。

[6] 係鎖定臺灣 50 家大型企業，調查期間為 2020 年 8 月-10 月，透過收集器、爬蟲技術取得外部多元大數據「情資」等客觀依據。

[7] 四大面向為隱私性(Privacy)、韌性(Resiliency)、聲譽(Reputation)、安全性(Safeguard)，資料來源：https://home.kpmg/tw/zh/home/insights/2021/02/tw-kpmg-cyber-risk-report.html

[8] 依能源、水資源、通訊傳播、交通、金融、緊急救援與醫院、政府機關、科學園區與工業區等八大分類；外洩比例是以外洩資料總數除以員工人數