資訊安全的趨勢與台灣資安新創的突破方向

2021 November

TAcc+計畫分析團隊

2020 年全球受到 COVID-19 疫情的衝擊，各行各業受迫於外在環境紛紛轉向不同的營運模式，也因此加速了企業的數位轉型，同時亦提高資安防範的意識。這也讓零信任趨勢成為資安的新常規，各組織都將要處於不間斷的防禦態勢，並釐清遠距用戶為保持安全而面臨的業務風險。由此可見，未來對資訊安全的需求，隨著數位轉型的驅動，也將水漲船高。

(1) 近年資安發展趨勢

2021 年 Gartner 的報告指出， COVID-19 大流行後，居家上班讓資安環境面臨重大的變化，防範策略也隨之改變，隨著疫情後新常態的形成，各組織都將需要更進一步的釐清遠距用戶的資訊安全需求，以及為保持安全而面臨的業務風險。Gartner 表示，今年的資安和風險趨勢凸顯了資安生態系統中正在進行的戰略轉變，長遠下來將對整個行業產生廣泛影響，並具有巨大的破壞潛力。趨勢觀察列舉如下：

- 網絡安全網格：使分佈式企業可以在最需要的地方部署和擴展安全性。
- 精通網絡的董事會：隨著公共安全漏洞和複雜安全設置的日益增多，董事會越來越重視網絡安全。
- 供應商整合：當今資安的現狀是資安領導者擁有太多工具，須進一步整合。
- 身份優先的安全性：疫情已將組織推向完全 (或大部分) 遠距，這種趨勢已變得至關重要。
- 將機器身份作為一項重要的資安功能進行管理：組織正看到越來越多的非人類實體，這意味著管理機器身份已成為資安策略的重要組成部分。舉電動車為例，如何追蹤車主很困難，以前可以憑引擎上的燒錄碼來辨識，因為引擎很貴不易變造，但電動車的電池不貴，如何辨識車主，除了人員辨識外，車體上的辨識裝置業界還在構思中，某些車

廠就在討論如何使用 PUF (Physically Unclonable Function) 來辨識，可見這是亟待解決的挑戰。

- 遠距工作常態化：64%的員工現在可以在家工作，五分之二的人實際上是在家工作。
- 破壞和攻擊模擬：在安全控制的有效性、配置問題和檢測功能方面，幫助發現問題。
- 增強隱私的計算技術：即使在不受信任的環境中，也可以實現安全的數據處理、共享、跨境傳輸和分析。

(2) COVID-19 疫情影響

台灣最具代表性的資安公司-趨勢科技在 2020 上半年總共攔截了超過 278 億次威脅，較去年同期增加 10 億，其中 93% 是經由電子郵件散布。另外，變臉詐騙 (Business Email Compromise, BEC) 偵測數量較 2019 下半年成長 19%，部分原因是因為詐騙集團試圖利用居家上班工作者更容易遭到社交工程詐騙的弱點嘗試發動攻擊。

McAfee Labs 的報告觀察到惡意軟體威脅數量平均為每分鐘 588 個威脅，到 2020 年第三季度每分鐘增加 169 個威脅 (40%)。第四季度平均數量為每分鐘 648 個威脅，每分鐘增加了 60 個威脅 (10%)。

2020 年 5 月 4 日，臺灣中油遭受勒索軟體攻擊，同年捷克第二大城布爾諾 (Brno) 的大學醫院遭受勒索軟體攻擊，使檢疫從原本的 1 天變成要好幾天才能完成，嚴重影響防疫工作。趨勢科技分析，勒索病毒犯罪集團瞄準最醒目、高價值的目標來攻擊。

來自美國的 Coveware，以及來自紐西蘭的 Emsisoft 於 2020 年 3 月宣布，在 COVID-19 全球大流行期間，攜手替受到勒索軟體攻擊的醫療院所提供免費的協助，包括協助分析勒索軟體、免費幫其開發解密工具，甚至是代為與駭客談判，並協助回復系統。

原預計於加拿大溫哥華的 Pwn2Own 漏洞發掘競賽，除了改為線上進行，參賽者利用漏洞的攻擊標的，特別聚集於三大電腦作業系統，突顯了大量員工在家工作，個人電腦也變成駭客鎖定的頭號目標，駭客將通過破壞防禦力弱的家庭電腦和家庭無線網絡，開發出滲透公司網絡的新方法。

疫情也左右了產品開發的步調，例如 Google 宣布 Chrome 與 Chrome OS 不再依循過去的快速發布策略，而集中於現行 80 版的安全漏洞處理，暫緩發表後續版本，原本表定於 3 月底推出的 81 版因此喊停，延後到 4 月推出。微軟也表示，5 月起推出軟體更新的策略，也打算取消提供選用功能的部分。

另從去年知名的 SolarWinds Orion 資安事件，可看出惡意組織利用軟體供應鏈漏洞進行攻擊的趨勢形成。

在線會議和團隊協作工具猛增，也吸引惡意的對手創造攻擊技術，以竊取憑據，在協作平台上立足並訪問用戶共享的機密數據。

(3) 資安領域新創與創投趨勢

CBInsights 整理了 14 個網路安全領域中的潛力新創企業，對於有心投入資安的臺灣創業家，可透過此整理來觀察別人切入哪些新興領域（參見表 1），例如從源頭防範假新聞、隱私權設計避免違反各國隱私規範、運用 AI 偵測使用行為的異常藉此找出攻擊案件，Patch protection 自動化防範軟體被入侵，Zero-trust Networking 以嚴謹的方式防患未然，Bot-Assisted Defense 使用 AI 等機器人協助資安防護，Multi-Cloud Security 也是近期投入大量資金與充滿挑戰的領域，尤其 5G 網絡已經是由軟體定義的網路 (SDN) 環境，透過軟體整合眾多的 5G 基地台，同樣的概念也會在未來，更多的使用軟體來整合資安防護，利用網路功能虛擬化 (VNFs)，將網路節點階層的功能，分割成幾個功能區塊，分別以軟體方式實作，不再拘限於硬體架構。Container Security 已經成為主流，還有 Medical Device Security 會要求蒐集個人生理資訊，也有很多資安防護需求。

表 1、有望改變網絡安全的新創企業

網絡安全領域	新創企業
Medical Device Security	ordr　MEDIGATE
Container Security	anchore　CAPSULE8
Outsourced Data Protection	evervault　VERY GOOD SECURITY
Multi-Cloud Security	CLOUDKNOX　orca security
Bot-Assisted Defense	SECURITI.ai　respond

Zero-Trust Networking	ZERO Networks / perimeter 81
Credential Stuffing Defense	kasada / Arkose Labs
Patch Protection	AUTOMOX / ForAllSecure
Third-Party Risk Management	axis security / SecZetta
Anomalous Behavior Detection	Abnormal Security / AWAKE
Privacy by Design	CONCENTRIC / TRANSCEND
Password-less Verification	passbase / BEYOND IDENTITY
Decentralized Digital Identities	evernym / bitkey
Disinformation Detection	yonder / Astroscreen

資料來源：CBInsights

Smart money 係指在此行業投資績效較好的 VC，透過觀察他們的投資標的與方向，從中瞭解募資市場看好的領域，這項指在矽谷已成為大企業與新創團隊必須持續關注與留意的指標。參考表 2 的 2020 年資安 Smart Money 投資分析，Cloud security 仍為近期最大領域，其次包含 Data protection、Identity-based security、Threat intelligence、Network security 都是 Smart money 非常關注的領域。

表 2、Smart Money 投資資安領域分析

資安領域	投資佔比
Cloud security	18%
Data protection	11%
Identity-based security	11%
Threat intelligence	10%
Network security	10%
Other	9%
Email security	8%
Website security	7%

Privacy	6%
Connected devices (IoT) security	5%
Endpoint security	5%

資料來源：CBInsights

(4) 資安領域政治環境

- 歐盟執委會於 2020 年 12 月 15 日提出「數位服務法」與「數位市場法」草案，前者旨在建立更安全的數位空間，保護數位服務用戶權益，後者則是維護數位市場公平競爭與創新環境。
- 歐盟資料保護法 GDPR (25 May 2018)，最高可處以 2,000 萬歐元或企業全球營收 4%的罰金。
- 行政院國發會將在 2020 年進行「個人資料保護法」修法作業，成立「個人資料保護專責機構」，希望能在 2020 年獲得歐盟 GDPR 適足性認定，讓臺灣境內企業能自由與歐盟進行個人資料跨境傳輸，降低企業的營運成本，提高競爭力。
- 美國食品與藥物管理局 (Food and Drug Administration, FDA) 於 2016 年 12 月 28 日，發布「醫療裝置上市後網路安全管理指南」(Postmarket Management of Cybersecurity in Medical Devices)，作為已上市醫療裝置管理的一部份。
- 美國加州（The California Consumer Privacy Act, CCPA）在 2020 年 1 月 1 日生效。
- 美國國防部 2020 年 1 月 31 日宣布，2020 年 9 月底前，該部將要求部分競標國防部合約之承包商具備網路安全驗證，此一驗證將奠基於 (Cybersecurity Maturity Model Certification, CMMC)，承包商必須依據專案之機密性，取得不同等級之安全驗證。
- 以色列 Check Point 公布 2019 年 6 月的統計數字，結果顯示，臺灣企業受惡意軟體攻擊的比率，可達全球的四倍到數十倍不等；尤其是貿易戰開打後，來自中國的攻擊明顯增加。
- 內政部計畫斥資 44 億，原預定於 2020 年 10 月全面換發 New eID

（晶片身分證），作為未來進行「數位身份識別」的工具。尚未有規範卡片的晶片內容、資料讀取、資料庫串接等狀況，有潛在隱私風險。

- 韓國國會 2020 年 3 月通過 (Act on Reporting and Use of Specific Financial Information Bill) 的修訂，要求虛擬資產營運商，包括加密貨幣交易平台、電子錢包廠商及 ICO 等業者，都必須取得資安管理系統 (Information Security Management System，ISMS) 認證。

1. 台灣資安新創突破方向

根據工研院的調查，台灣資安產業之產值，自 2016 至 2019 年依序為 351.7 → 393.5 → 439.4 → 493.4 億元新台幣，台灣資安產業起源於 2000 年網通產業起飛時的防火牆需求，發展至 2019 年，投入廠商達 324 家，從業人數約 8,800 人，業務類型可分為三大類，各類產值占比為模組與硬體占 51.4%、軟體占 9.7%、代理和資安服務占 38.9%。

硬體是臺灣具備優勢的領域，全球超過 80%的網路安全硬體平台由臺灣製造，另因本身國情因素，以及身為資通訊產業大國，臺灣也成為各國駭客挑戰、測試的對象，在與駭客攻防的實戰中累積了不少經驗與人才，加上國情需要，資安及國安，使得臺灣在資安產業的發展上，具備相較其他國家更為迫切的動機與資通訊背景上的優勢。

然而，臺灣本土市場太小，很難成為規格制定者，使得軟體占比很小，也讓臺灣資安產業的產值分布，與全球資安市場軟體占比較大的分布相差很多，取而代之的是資安服務的成長性較佳，服務範圍涵蓋營運監控、雲端資產管理、檢測鑑識與顧問、系統規劃與建置，加上企業的資安意識持續提升，本身資源不足之企業會採取委外方式，相關之營運管理服務商或系統整合商發展的比較健全。

(1) 台灣資安商機

IDC 估計臺灣資安市場規模將由 2019 年的 4 億 6 千萬美元成長至 2023 年的 8 億 2 千萬美元，其中資安服務 (Service) 市場快速成長，年複合增長率達 21%，資安軟體 (Software) 和資安設備 (Appliance) 市場則保持微幅成長。

iThome 針對臺灣企業進行之調查結果顯示，近 4 年企業對自己的資安防護信心水準依序是 2018 年 62.9 分、2019 年 61.4 分、2020 年 63.8 分、2021

年 62.4 分，長期維持在剛好及格的水準。當企業遭遇到資安事件，有 8.4%的企業表示可在 1 小時內完成復原，表示可在一天內完成的有 61.4%，可於一周內復原的佔 23.3%，其次依序為二周內佔 5.1%、一個月內 1%、三個月內 0.5%、半年內 0.3%。

Gartner 報告指出，全球資安市場規模約占全球 IT (Information Technology) 支出的 3.32%，且佔比有持續上升的趨勢，臺灣是 IT 設備製造大國，發展資安產業之挑戰在於本國市場太小，且在資安軟體的發展與領先國家相較有段落差，加上顧客看待資安業者如同看醫生，好醫生大家搶，且希望獲得一次購足的產品和服務保證，以利簡化管理複雜度，產業特性不利於單兵作戰的小型資安業者，因此在發展上必須採取較為迂迴與綜合性的方式。

(2) 台灣資安新創面臨之挑戰

A. 不同產業所面臨複雜的 IT 環境

每個產業都會有本身作業上相關的專業知識 (Domain knowledge)，IT 環境也是配合該產業實務運作上的需要所建置，各種 IT 裝置間的連結與整合應用方式也隱含了各產業的習慣作業流程，加上資安的防禦技術本就多元且與時俱進，使得想要切入資安的臺灣廠商，面臨各產業需要的解決方案不盡相同，且各種資安技術之間又必須有效串連整合，才能展現出良好防護效果的挑戰；舉醫療和零售產業為例，CBInsights 分別整理了與 Healthcare、Retail 相關的資安業者，並各自依其產業特性，分為下表中的 15 類。

表 3 CBinsights 對醫療與零售產業相關資安業者之分類

醫療 (Healthcare)	零售 (Retail)
Cloud Seucurity	Cloud Seucurity
Data Security	Data Security
Data Privacy (HIPAA)	Consumer Data Privacy
Endpoint Security	Endpoint Security
Human Element	Human Element
Managed Security	Managed Security
Network Security	Network Security
Secure Collaboration	Secure Collaboration

SIEM	SIEM
Third-Party Risk	Third-Party / Supply Chain Risk
Vulnerability Mgmt.	Vulnerability Mgmt.
Website Security	Website Security
IAM	Digital Brand Protection
Medical Device Security	E-Commerce Experience Fraud
Threat Intelligence	In-Store & Supply Chain IoT Security

資料來源：CBinsights

從表 3 可觀察出，醫療、零售的資安業者都被分成 15 類，其中名稱完全相同的有 10 類，在 Data Privacy (HIPAA)與 Consumer Data Privacy、Third-Party Risk 與 Third-Party / Supply Chain Risk 則屬於部分名稱相同。然而，配合產業特性設定名稱卻不一定有相同的規範，例如 Data Privacy 在醫療產業重視的是符合 HIPAA 的規範，但在零售產業，則重視對消費者的保護；零售業相較醫療產業，除了 Third-Party 風險，還特別重視 Supply Chain 風險；雙方各自有三種針對本身產業特性的分類。進一步比較，相同分類名稱下的醫療和零售資安業者也並不完全相同，且幾乎找不到能夠橫跨 15 類防護技術的業者，印證複雜的 IT 環境。

B. 資安創業者多是技術出身，在行銷或銷售能力上，並非其所擅長

鑒於資安面向複雜的 IT 環境、防護需求持續增長、競爭產品/服務眾多、企業高階主管對於資安防護的了解程度相對較低、信任度與信譽的建立需要時間、顧客需要大量的教育與加強防護意識、許多企業還未將資安納入整體策略或排在次要順位、顧客期望整合式解決方案、攻防技術的日新月異等挑戰，需要投入很多人力、時間、資源與潛在、現有顧客溝通，以及規劃出良好的商業模式，產業特性不適合單打獨鬥。然而，臺灣資安相關新創企業的核心成員許多是技術出身，對於如何與潛在顧客群、合作夥伴、產品/服務使用者、管理者、投資者等交流與互動，較為缺乏經驗。

C. 臺灣具有資安自主研發能力的業者，目前多數都是小公司。

依據國發會產業發展處資料，臺灣資安業者之分布狀況與規模如表 4 所示，從中可觀察出，臺灣資安業者的規模以資安營運管理服務、終端與行動裝置防

護業者為前二高，平均每家營收超過台幣 3 億元，資安支援服務、資安系統整合建置業者的平均每家營收則低於 1 億元，整體平均每家營收約為 1 億 5 千萬元，可見規模普遍不大，如僅靠自己單兵作戰，成長速度勢必受限。

表 4 臺灣資安產業廠商分布與平均規模

資安產業分布	營收(台幣億元)	家數	平均每家營收(台幣元)
終端與行動裝置防護	108	31	348,387,097
網路安全	139.5	53	263,207,547
資料與雲端應用安全	26.5	24	110,416,667
物聯網安全	20	13	153,846,154
資安營運管理服務	50.3	13	386,923,077
資安檢測鑑識顧問服務	61.7	48	128,541,667
資安系統整合建置	83.8	132	63,484,849
資安支援服務	3.3	12	27,500,000
整體	493.4	324	152,283,951

資料來源：國發會產業發展處

D. 臺灣創投希望投資較晚輪次，以規避風險

資策會資安科技研究所指出，全球資安新創的被併購機率持續增加；此現象背後顯示，資安大廠持續透過 CVC 投資或收購新創來充實本身的解決方案是重要原因之一。FINDIT 網站分析 2020 年 CVC 對於網路安全的投資相當熱絡，投資件數相較前年成長 13%至 140 件，投資總金額也大幅增長 31%至 38 億美元，其原因包括鉅額交易件數倍增至 12 件。臺灣的創投業者也習慣投較晚輪次，且對於回收時間點的期望也相較為短，身處此環境下的新創，將面臨做得不錯時容易被外國大廠買走、不接受 CVC 則可能需要更久的時間找到生存市場，想要透過 VC 募資來強化自主研發能量的企圖不易實踐，如何制定出最佳的成長策略需要審慎規劃。

綜整上述觀察，臺灣廠商於自主研發資安產品面臨諸多挑戰，在發展上必須採取較為迂迴與綜合性的方式，台灣的資安產業之發展相對遇到瓶頸，主要是因為多數人只認知到駭客與防毒軟體，以為兩者就是資安的全部，臺灣資安產業的相關統計，與主流國際的資安產業統計有落差，現因美中關係的對立與

競爭激烈化，使得歐美國家對於中國大陸製造的資安產品疑慮大幅增加，再加上臺灣本身國安上的考量，目前在客觀環境上造就了適合發展資安的環境，以色列就是臺灣最好的借鏡對象。