捍衛網域國境 腳步從不停歇

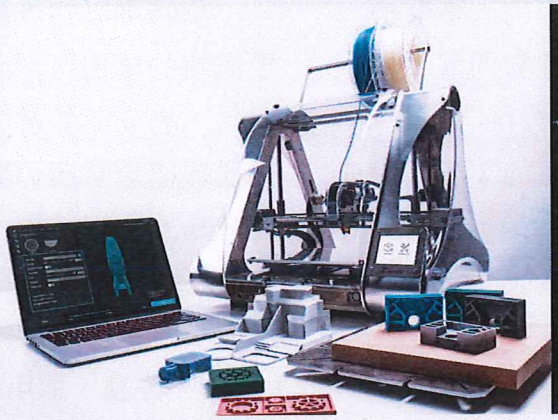
／調查局資通安全處　蘇　輦

資訊科技發展日新月異，多元資安威脅與日俱增，不法駭侵犯罪邁向產業化，調查局力抗駭侵狂瀾。

如果您佇立門外仔細聆聽，有個聲音在耳邊悄悄迴盪，彷若手法純熟的演奏家正此起彼落敲著琴鍵，奏鳴出未曾聽聞的旋律，您可能會疑惑，這篇樂章截至目前為何始終在細膩鋪陳著前奏，潛藏的思緒與情懷卻難以捕捉，是刻意按捺？是意境延伸？突然一聲動人心魄的重音，將樂章瞬間畫下句點，回歸瀰漫著詭異的寧靜。

如果您佇立門內睜大雙眼，原來有個人影在螢幕前映著藍光，彷若全神貫注的演奏家，敲的卻是鍵盤，在螢幕上奏出一行又一行的指令及程式碼，而非耳中輕快跳動的音符，您會驚覺方才的綿長鋪陳竟是潛伏的惡意，待萬事即將俱備、大功即將告成之際，眼前人影突然使勁敲下「Enter」鍵，螢幕中滿布駭侵而得的戰利品，嘴角的訕笑無情地諷刺著彼端的血淚。

或無能為力，或力不從心嗎？這般景象恐愈發頻繁地在世界各地上演，但大多數的人往往無所知覺已然受駭，資安技術與防護概念似如一扇高聳冷冽的大門，不得其門而入，今天就讓我們一起試著推開這扇門吧。


未來 5G 網路將全面布建，萬物皆可聯網，虛擬貨幣、自動駕駛、太空開拓、3D 列印生產技術等事物，流通串聯的是難以計數的資訊流，然而其中的黑暗面值得引起我們的思考與重視。

新資訊時代蓬勃發展

網路科技數十年來席捲了整個世代的變革，為人們的生活帶來無窮的便利與品質的提升，然而網路等資訊科技的影響真正開始從資訊業巨幅外溢、甚至更為深入地滲透人們生活中所行所為，則在近幾年來愈發顯著；根據 FRED 數據，資訊產業中數據儲存處理分析相關服務及其他新興資訊服務從業人數，在近十年來成長至少一倍以上；尤其在今年新冠肺炎疫情爆發以來的這段期間，實加速了諸多產業的數位轉型，甚至擴及農業、製造業、服務業。

與此同時，我們似乎已可望見未來世界的藍圖逐漸清晰，5G 網路的全面布建、萬物皆可聯網、區塊鏈技術帶來零信任交易基礎的智慧合約及虛擬貨幣、普及的自動駕駛車輛與飛行器、太空開拓與衛星網絡的建構、跳脫人力框架的 3D 列印生產技術、自線上愈趨落地的社群網絡；在不遠的未來，你會發現身處的世界、手邊之物，彼此緊密的串聯著，流通的是難以計數的資訊流，然而在與嶄新未來接軌的此時此刻，有些黑暗面令我們不得不開始思考與重視。

資安威脅與日俱增

一、全球發生資安事件之產業分布

根據 Statista 針對全球產業機構去（108）年發生資安事件之統計（來源：Verizon），3 萬 2 千餘件中即有約 6 成以

上，集中於資訊產業、公共部門、專業技術服務產業（如研究室、管理顧問等），均係科研技術密集、持有機敏資料之單位；大型規模之機構受駭案例則有約 7 成集中於公部門，而小型規模之機構受駭案例則有 5 成集中於金融、醫療、資訊、公部門等產業。

Incidents:	Total	Small	Large	Unknown
Total	32,002	407	8,666	22,929
Accommodation (72)	125	7	11	107
Administrative (56)	27	6	15	6
Agriculture (11)	31	1	3	27
Construction (23)	37	1	16	20
Education (61)	819	23	92	704
Entertainment (71)	194	7	3	184
Finance (52)	1,509	45	50	1,414
Healthcare (62)	798	58	71	669
Information (51)	5,471	64	51	5,356
Management (55)	28	0	26	2
Manufacturing (31–33)	922	12	469	441
Mining (21)	46	1	7	38
Other Services (81)	107	8	1	98
Professional (54)	7,463	23	73	7,367
Public (92)	6,843	41	6,030	772
Real Estate (53)	37	5	4	28
Retail (44–45)	287	12	45	230
Trade (42)	25	2	9	14
Transportation (48–49)	112	3	16	93
Utilities (22)	148	5	15	128
Unknown	6,973	83	1,659	5,231
Total	32,002	407	8,666	22,929

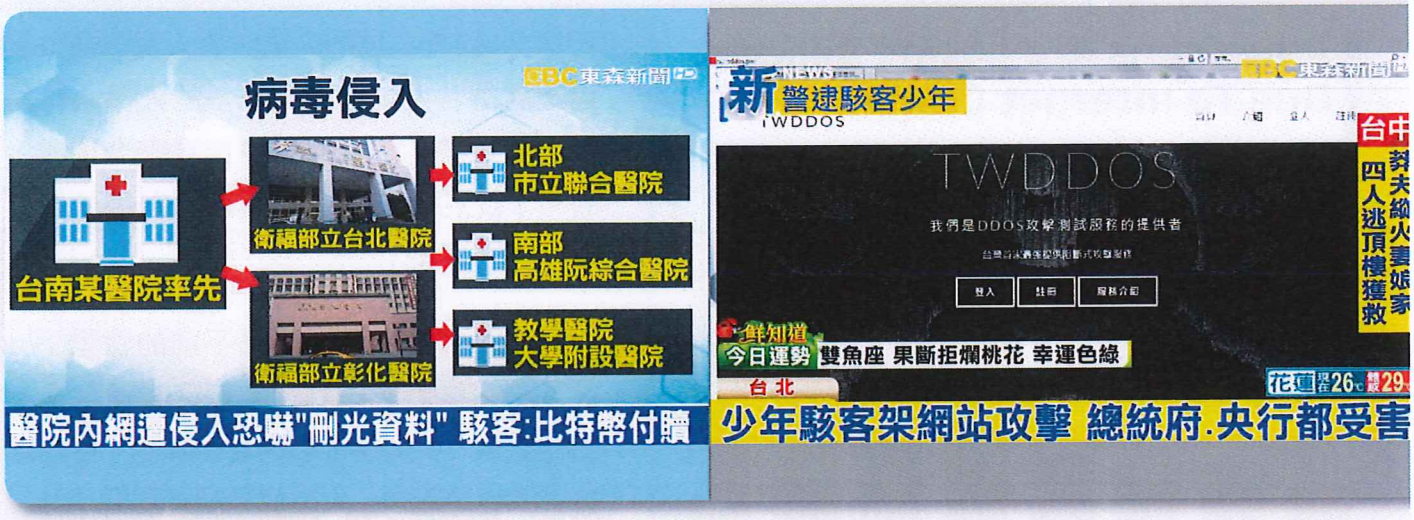
Table 1. Number of security incidents by victim industry and organization size

我們可以初步研判，小規模但提供重要服務的機構可能因資安防護的能量較為不足，易成為駭侵犯罪得手的目標；而大規模機構通常擁可觀預算及人力，能夠實施較高的資安防護水平，因此一般較不易成為駭侵目標；但是大規模的公部門機構，可能因內部資料較為機敏、資料結構品質完整、運用價值高，甚至可藉其獲利或以攻擊遂行政治上的訴求及目的，而遭到不法人士的鎖定。

二、 社會矚目案件

我們已可在新聞報章媒體上看到，電腦、網路的駭侵犯罪已經不僅止於資料遭竊，而是搭配服務阻斷及勒索、社交工程及詐騙等複合式攻擊手法，諸如「第一銀行詐領案」、「銓敘部個資遭駭案」、「臺大醫院病歷遭駭案」、「衛福部及醫療院所遭植入勒索病毒案」、「全球殭屍網路 Necurs 不法案」、「政府機關遭 DDoS 攻擊案」、「某

根據統計資料顯示，全球產業機構 108 年發生的資安事件中，3 萬 2 千餘件中即有約 6 成以上，集中於科研技術密集、持有機敏資料之單位；大型規模機構受駭案例則有約 7 成集中於公部門，而小型規模機構受駭案例則有 5 成集中於金融、醫療、資訊、公部門等產業。（Source: Statista, Verizon, https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf）



新聞上常見的電腦、網路駭侵犯罪不僅止於資料遭竊，還搭配服務阻斷及勒索、社交工程及詐騙等複合式攻擊手法，鎖定目標集中於擁有機敏資料、提供民眾關鍵服務的機構及企業。（圖片來源：截自東森新聞，https://youtu.be/sd1vugUHhqU，https://youtu.be/Z8RK5w2MmWw）

公司遭植入勒索病毒」、「某公司營業秘密遭竊」……等案例不勝枚舉。

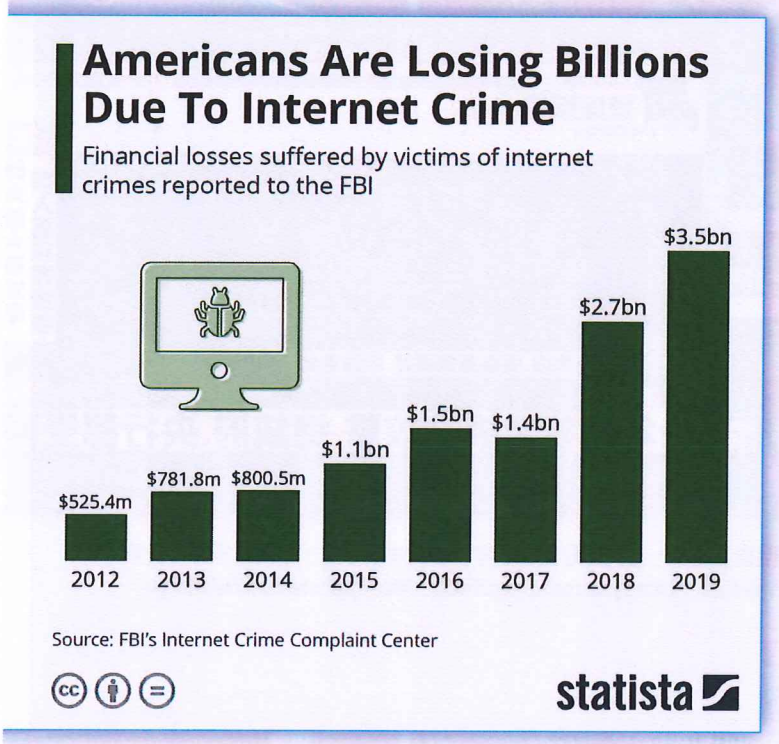
對於一般人或企業來說，最為迫切相關的大概就是個資遭竊、信用支付遭盜用、各種服務癱瘓、商業匯款郵件詐騙、勒索病毒損失等狀況，除影響生活所需及便利性外，更造成實質上的損害。同時我們也可以看到，惡意駭客鎖定的目標，確如統計所述的集中於擁有機敏資料、提供民眾關鍵服務的機構及企業。

三、駭侵犯罪規模及肇生損害顯著攀升

根據 Statista 針對近年來的網路犯罪（來源：FBI 所屬 IC3 的網路犯罪報告）損失金額統計，僅去（108）年即高達至少 35 億美元，相較於 8 年前水準竟有將近 6 倍之漲幅，且連年呈現高度成長的態勢。

經綜合多項統計資料，我們可以發現，近年來資安事件除數量顯著增加外，相應的損失更為驚人攀升，可見網路駭侵犯罪隨著時間的演進，其商業模式、產業鏈、獲利手法已然成形且組成龐然的分工結構，同時更具有針對性、目的性，只要有利可圖，不論是個人、法人、公部門均可能成為駭侵的目標。

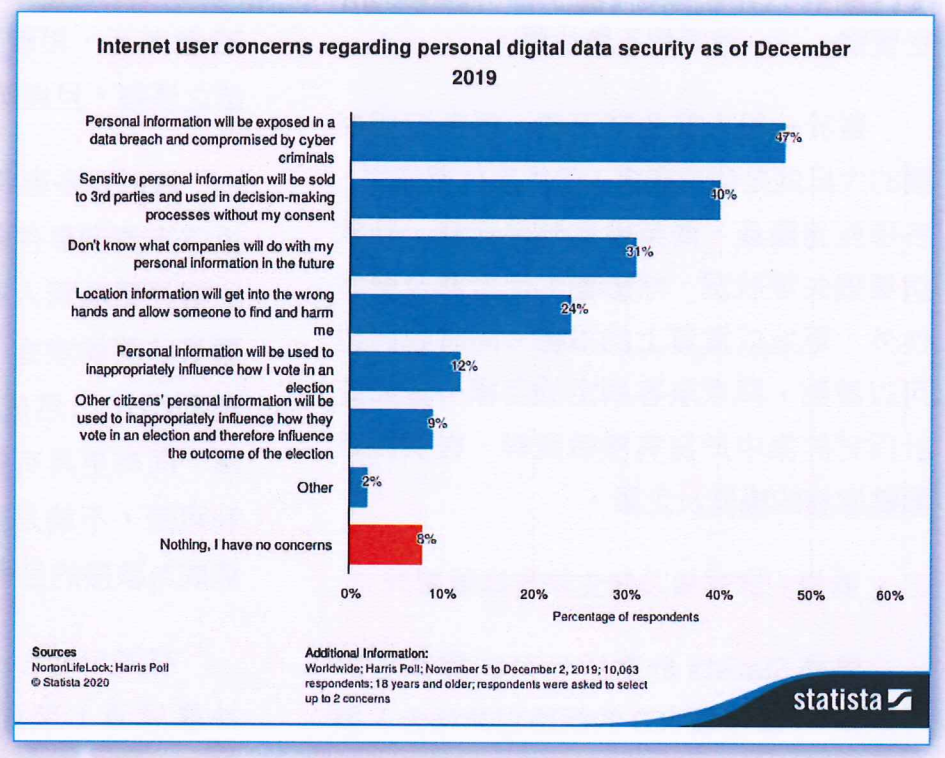
根據 Statista 針對全球網路使用者進行抽樣調查（來源：NortonLifeLock; Harris



Poll），約有 5 成的人擔心個人資訊遭駭客違法取得利用，約有 2 成多的人擔心位置遭暴露致遭人不當利用及出現安全疑慮，約有 1 成的人擔心個人資訊遭利用於影響政經決策傾向。

在現代資安事件層出不窮的背景下，民眾開始逐漸意識到，原來資訊安全是如此的重要，小則危害個人身家安全，中則影響企業經營運作，大則撼動政經體制平衡。

據 FBI 所屬 IC3 的報告統計，2019 年美國因網路犯罪損失的金額高達至少 35 億美元，相較於 8 年前水準竟有將近 6 倍之漲幅。（Photo Credit: Statista, https://www.statista.com/chart/20845/financial-losses-suffered-by-victims-of-internet-crimes）



由全球網路使用者抽樣調查來看，在現代資安事件層出不窮的背景下，民眾開始意識到資訊安全小則危害個人身家安全，中則影響企業經營運作，大則撼動政經體制平衡。（Photo Credit: Statista, https://www.statista.com/statistics/296700/personal-data-security-perception-online）

駭侵犯罪攻擊趨勢

近期的駭侵犯罪及攻擊的型態與未來趨勢將是如何呢？我們可以想像有一間賣餅乾的公司，專長就是做餅乾，在上市開賣前的第一步當然就是先調查看看消費者喜歡吃什麼口味，再針對能引發消費者食慾又難以抗拒的口味進行開發，除了巧妙精緻的包裝外，少不了專業的行銷宣傳，不論是廣發傳單、置入性行銷，甚至是強迫推銷都在所不惜，接著利用像是便利商店般的廣大通路送到每位消費者的手上，如果不夠還可以雇用狂熱的業務員，甚至租用攤販、自動販賣機 24 小時營業。

如果有人拒吃這家公司的餅乾，可能會被業務員盯上，以各種花言巧語騙稱吃了會瘦，同時為取信消費者自己還吃上一口……消費者荷包因此被掏空也就算了，但他們還可能在你停車的時候偷偷上車輪鎖，留下紙條表示不付錢就不解鎖，嚴重的話還可能被一群凶神惡煞包圍到無路可逃，最後只得被迫付錢買餅乾。

是不是覺得這間餅乾公司很惡質？讓我們換個情境，這間公司其實就是駭客不法集團，專長撰寫惡意程式，在做案之前，會先偵測檢閱看看哪些系統、軟體、機構有資安漏洞，再針對這些漏洞開發破解的駭侵手法，或將惡意程式碼巧妙包裝、隱匿於看似無害的文件或檔案裡，透過廣發垃圾郵件、惡意連結、包裹在民眾常用的網路服務裡，散播到大家的手機及電腦，有時更針對系統漏洞強行將惡意程式注入到設備中，如同強迫推銷一般；再者，還可以操控為數眾多的殭屍網路，不夠的話甚至還能找其他駭客租借，以各種通路散布出去，24 小時不間斷，若是有人具備不錯的資安觀念，拒病毒於門外，亦可能被駭客盯上以社交工程、假造郵件鎖定詐騙，一不留神恐損失慘重，還可能被注入勒索病毒，將電腦檔案加密無法使用，不付比特幣就無法解鎖，嚴重者可能還被 DDoS 阻斷式攻擊，癱瘓網路服務，甚至遭到鉅額勒索。

現在的電腦、網路駭侵犯罪已經形成穩固的地下產業結構，擁有清晰的商業模式及獲利方法，高度組織化、多層次分工，只要有利可圖，不論是販售個資、機敏政府資料，詐騙勒索，取得市場競爭優勢等，都能接受委託或主動出擊，即使目標資安防護固若金湯也無法阻擋其駭侵意圖，有些駭客不法團體背後甚至有國家那雙看不見的手，意圖撼動國際政經情勢。

調查局力抗惡意駭侵狂瀾

為了應對這場沒有煙硝的嚴峻戰爭，調查局在今（109）年成立資安工作站，集結資通專業人力、整合司法調查能量，在資安事件、駭侵犯罪發生之際，即能迅速發動偵辦，遏止犯罪行為持續擴散，有效減輕損害及後遺，發揮「主動偵查、打擊犯罪」的能力，為落實我國資通安全戰略立下一個新里程碑。

蔡總統在「國家資通安全戰略報告」提出「資安即國安」，甚至在今年公開表示「資安成為新政府重點核心戰略產業」，就是為了建立並完備「國家資安聯防架構」，在國安單位及政府各部會的合作下，提升「早期預警、緊急應變、持續維運」的能量及效率。

調查局將本於資安專業技術，成為我國資安執法先鋒，擔任我國網域國境安全

電腦、網路駭侵犯罪已形成穩固的地下產業結構，擁有清晰的商業模式及獲利方法，且高度組織化與多層次分工，有些駭客不法團體背後甚至有國家撐腰，意圖撼動國際政經情勢。

調查局在 109 年 4 月成立資安工作站，集結、整合資通專業人力與司法調查能量，有效遏止駭侵犯罪發生與擴散，為我國資通安全戰略立下新的里程碑。（圖片來源：總統府）

維護之「資安尖兵」！只要民眾、企業、公家機關察覺到有可疑駭客行為，不論是收到夾帶可疑檔案的電子郵件、商業匯款電郵詐騙、偵測到可疑來源駭侵攻擊，甚至是發現有大筆不法個資或政府機敏資料遭到販售及利用，都可以向調查局檢舉通報，共同協力杜絕不法駭客。

結語

大家平時除了須培養良好的資安觀念外，更要在生活與工作中實踐，注意使用的手機、電腦應用程式版本是否都有即時更新，網路連線（尤其使用 WIFI）時是否安全，點閱郵件及瀏覽網站時，是否有謹慎確認來源、排除可疑風險；企業及公部門亦要全面檢視自身的資安威脅，以風險為導向進行評估，建立符合需求的資安防護體制。

同時，本局的每一位成員必將竭盡所能，讓正義的輝芒照映駭客門內的黑暗，打擊惡意的潛伏、終止無情的訕笑，誓言劃下駭客不法樂章最後的句點。