109 年國家資通安全情勢報告

行政院

中華民國 110 年 6 月

目次

詞彙表

5G	5th Generation Mobile Networks，第五代行動通訊網路
AI	Artificial Intelligence,人工智慧
APT	Advanced Persistent Threat，進階持續性威脅攻擊
Botnet	RoBot Network，殭屍網路
DDoS	Distributed Denial of Service，分散式阻斷服務攻擊
DNS	Domain Name System，網域名稱系統
DoS	Denial of Service，阻斷服務攻擊
IoT	Internet of Things，物聯網
OT	Operational Technology，營運技術
UPnP	Universal Plug and Play，通用隨插即用協定
VPN	Virtual Private Network，虛擬私人網路

壹、依據及目的

資通安全管理法(以下簡稱資安法)業於 108 年 1 月 1 日正式施行，本院依據資安法第 5 條規定，定期公布「國家資通安全情勢報告」。

隨著新興科技與物聯網(Internet of Things, IoT)設備運用日漸普及，公私部門皆面臨更加嚴峻之資通安全威脅。本報告藉由研析 109 年全球資通安全威脅情勢及我國政府機關所面臨之資通安全威脅現況，研擬相關資安防護建議，俾利各界參考依循，以精進整體資安防護作為。本院期望藉由本報告之公布，持續加強公務機關資安防護意識，提升國家資安防護能量。

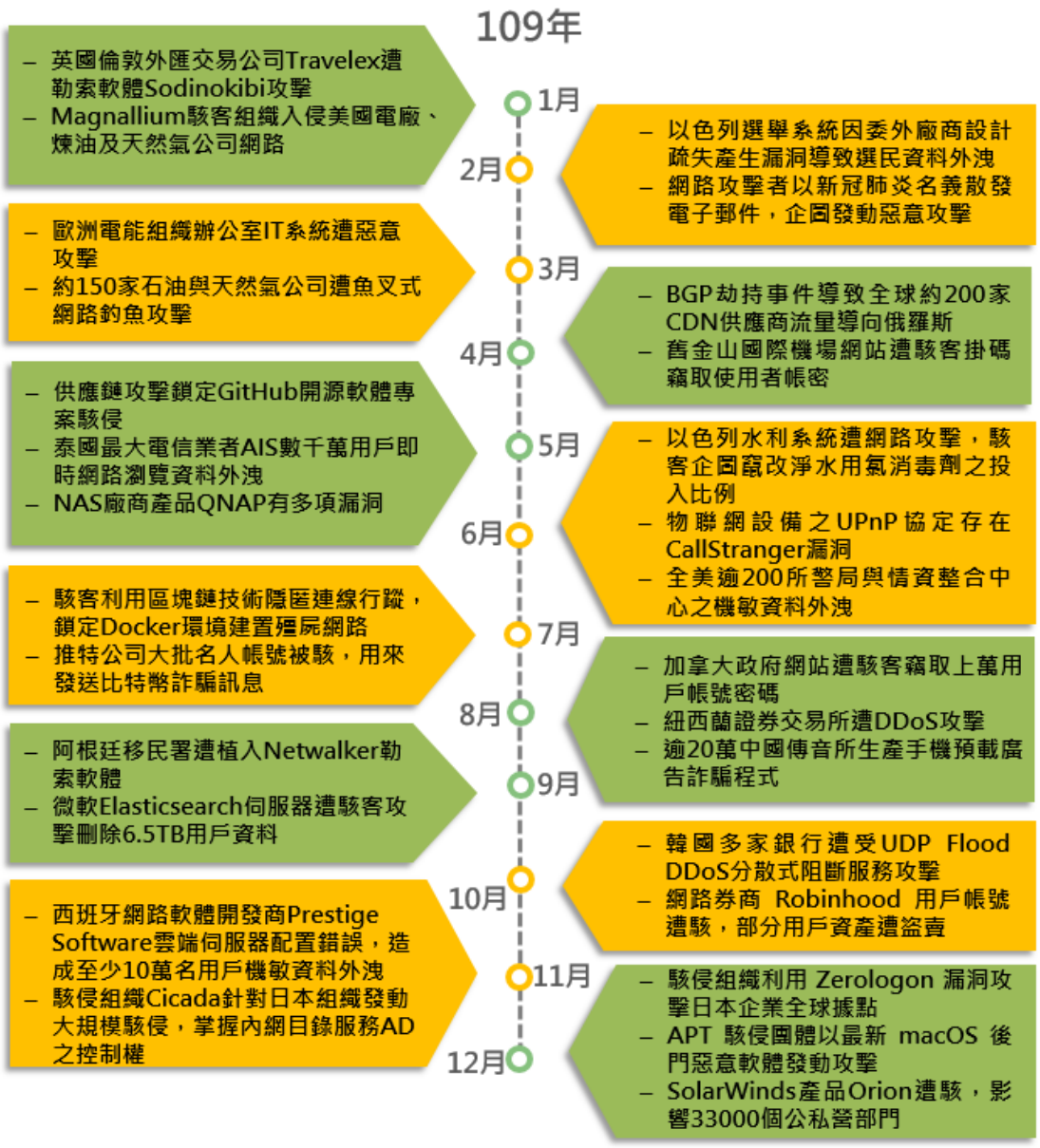
貳、109 年全球資安威脅情勢概要

根據世界經濟論壇(World Economic Forum， WEF)「109 年全球風險報告」,「網路攻擊」無論在影響(impact)風險或是可能性(likelihood)風險,已連續三年皆位於前 10 名之列,可見網路攻擊事件不但發生可能性高,且衝擊甚鉅,其衝擊範圍小則影響民眾日常生活,大則恐致危害國家安全。

面對層出不窮的網路攻擊,新興科技的資安議題亦面臨更為嚴峻挑戰，物聯網(Internet of Things, IoT)、第五代行動通訊網路(5th generation mobile networks, 5G)及人工智慧(Artificial Intelligence, AI)等科技應用，帶來科技便利的同時，亦伴隨著新的資安威脅與挑戰，為有效採取相關防護措施,國際資安機構正持續發展相關資安防護基準及參考指引,已見針對新興網路攻擊之防護已為現行資通安全顯學。

經檢視 109 年全球網路攻擊趨勢發現,駭客透過物聯網設備弱點、社交工程、廠商供應鏈攻擊及弱密碼等方式作為入侵途徑。另由於新冠肺炎(COVID-19)疫情之影響,發現社交工程亦多利用此類訊息,透過社群媒體及電子郵件散布惡意程式。各國關鍵資訊基礎設施之工業控制系統受網路攻擊事件仍持續發生,顯示隨著營運技術(Operational Technology, OT)環境逐漸連網與各種系統進行串聯，在管理及技術面向的資安防護更應與時俱進，加入縱深防禦之概念。此外，國際間對於中國品牌資通設備之資安疑慮，漸提高警覺採取因應措施。

經分析全球 109 年全球重大網路攻擊事件(詳見圖 1)，歸納出 6 大面向資安威脅趨勢，包含「個資與帳密頻遭大量竊取」、「社交工程郵件助長勒索軟體散布」、「物聯網設備資安漏洞擴大蔓延」、「進階持續性威脅攻擊鎖定能源產業」、「供應鏈資安威脅激增」及「關鍵基礎設施遭駭風險升高」,說明如下：



資料來源：本院國家資通安全會報技術服務中心整理

圖 1 109 年全球重大網路攻擊事件

一、個資與帳密頻遭大量竊取

依 IBM Security 於 109 年「資料外洩成本報告」指出，52%資料外洩是由於惡意攻擊，且其中 8 成之資料外洩包含個人資訊，其遭受洩露後所付出之成本也最高。使用者為求便利，習慣在不同服務上使用相同帳號與密碼，個人資料一旦遭駭客竊取而洩露，將招致源源不絕之網路攻擊。

例如 109 年 8 月加拿大政府網站遭駭客利用殭屍網路(Botnet)，以自動化方式，使用先前已外洩之登入帳號與密碼試圖登入網路服務，攻擊竊取上萬用戶帳號密碼之事件，駭客鎖定該國政府所提供之身分驗證服務帳號與稅務局帳號發動網路攻擊，估計約有 9 千多筆身分驗證服務帳號與 5 千多筆稅務局帳號遭破解並存取相關服務，為避免民眾個資遭洩漏，該國政府已緊急關閉受駭帳號，並要求用戶重新更換密碼。

二、社交工程郵件助長勒索軟體散布

國內外遭受勒索軟體攻擊之組織或機關不勝枚舉，其範圍涵蓋衛生醫療、教育、政府組織、科技及金融產業等，駭客利用社交工程散布含有惡意程式之釣魚郵件，誘導收件者點擊郵件中所夾帶之惡意勒索軟體，進而加密重要系統之資料，達到勒索贖金之目的。

例如 109 年 1 月英國倫敦之外匯交易公司 Travelex 遭勒索軟體攻擊事件，據媒體報導，Travelex 遭受勒索軟體 Sodinokibi 攻擊，108 年才現身之 Sodinokibi 迄今已是全球第五大勒索軟體，主要藉由惡意垃圾郵件來滲透企業網路進一步發動勒索軟體攻擊。媒體更取得駭客本身證實，以 Sodinokibi 攻擊加密 Travelex 重要系統之前，已預先備份系統之包含生日、社會安全碼及金融卡資訊等 5GB 個人檔案，以

此向 Travelex 勒索高達 300 萬美元贖金。

三、物聯網設備資安漏洞擴大蔓延

隨著物聯網時代來臨，越來越多物聯網設備被運用在組織內部作業，風險可能發生在任何物聯網設備上。若未做好網路區隔及資安防護等措施，任何物聯網設備受到駭侵，都可能擴大影響到組織正常運作。

109 年 6 月研究人員發現物聯網設備仰賴之通用隨插即用協定(UPnP)存有安全漏洞，駭客可藉此漏洞發動分散式阻斷服務攻擊及掃描探測連接埠，以挖掘潛在受害目標竊取資料。由於該協定之用途係讓物聯網設備得以探索區域網路中其他鄰近設備，並自動與之互相連接溝通，因此，駭客可利用漏洞繞過防火牆等網路安全機制，竊取機敏資料、掃描內網及利用各種連網設備，發動分散式阻斷服務攻擊(Distributed Denial of Service, DDoS)。

四、進階持續性威脅攻擊鎖定能源產業

駭客慣用進階持續性威脅(Advanced Persistent Threat, APT)攻擊手法來鎖定專一或特定族群為目標對象，經由針對性、持續性、隱密性策劃後，對目標對象進行入侵滲透攻擊。

資安業者 Bitdefender 研究人員即發現 109 年 3 月有針對能源產業之魚叉式網路釣魚攻擊(Spear-phishing Attack)事件，在一週內約有 150 家分別位於馬來西亞、美國、伊朗及南非等國之石油與天然氣公司均遭受到同樣之釣魚攻擊。駭客假冒埃及知名石油暨加工工程承包商之名義寄送釣魚郵件，透過寄送精心製作之釣魚郵件予收件人，請收件人對該承包商計畫設備與材料進行投標，誘騙收件人點擊郵件附

檔，以安裝 Agent Tesla 木馬程式，進而發動後續惡意攻擊行為。

五、供應鏈資安威脅激增

由於資安(訊)設備供應商所處環境對資安防禦程度相對較低，廠商人員不易凝聚針對威脅風險控管之資安意識，而形成了供應鏈安全遭受破壞之危險因子，容易成為駭客攻擊首要目標之一。供應鏈資安議題持續不斷發生，且隨著與供應商合作夥伴關係之密切度，所造成之衝擊與範圍亦逐漸擴大。

109 年 12 月即發生美國政府機構遭遇供應鏈攻擊案例，這場風暴核心源自一家網路監控軟體公司 SolarWinds，該公司為美國政府最大軟體供應商之一，駭客組織藉由入侵該公司 Orion 平台產品，進而攻擊使用該產品之目標企業及組織。由於使用該產品之用戶遍及全球，特別是包含美國數個重要政府機構及大型企業，估計有數千個政府機構和大型企業使用該產品，如美國國務院、國防部等重要部門，以及 Intel、NVIDIA、Cisco 等大型國際企業，已有美國財政部與商務部證實遭受駭侵。

六、關鍵基礎設施遭駭風險升高

關鍵基礎設施與民眾生活密不可分，直接涉及民生重要活動，其領域包含能源、水資源、通訊傳播、交通、金融、醫療、高科技園區及政府機關等皆是重要防護範圍，近年來各國關鍵基礎設施越來越容易遭到攻擊，已成為國家級駭客覬覦之主要目標。

109 年 6 月即發現以色列水利系統接連遭到網路攻擊，駭客入侵農業水泵與氯控制器，企圖竄改相關數據。以色列水利系統並非首次遭受攻擊，當年 4 月駭客已滲透到以色列水處理系統，並試圖竄改淨

水用氯消毒劑之投入比例，但相關攻擊活動被偵測且成功阻擋。當局評估若被成功竄改數據，可能造成供水區域中毒事件。此外，由於駭客注意到工廠端工業控制系統資安防護之脆弱性，便透過惡意軟體進行攻擊，資安廠商發現美國電網、煉油及天然氣公司，以及中東國家巴林煉油廠，先後遭到惡意駭侵，我國亦爆發石油公司遭到駭客利用勒索軟體惡意攻擊。

參、109 年政府資安威脅統計

一、聯防預警情資

為及時掌握政府機關之潛在資安威脅，國家資通安全防護中心定期彙整政府機關資安預警情資與事件，掌握資安威脅類別及趨勢，提供政府網路資安監測預警服務。經分析 109 年所彙整之情資，共分為系統服務、入侵攻擊、阻斷服務、惡意程式、政策規則、掃描刺探及經同意之攻防演練等 7 類。109 年資安威脅類型第 1 名為掃描刺探類(39.16%)，主要針對已知漏洞、遠端服務及密碼猜測之探測行為；其次為入侵攻擊類(32.35%)，主要針對系統攻擊以獲取非法權限；以及政策規則類(14.92%)，主要針對違反機關資安規範之使用者行為，各類資安威脅分布(詳見圖 2)。

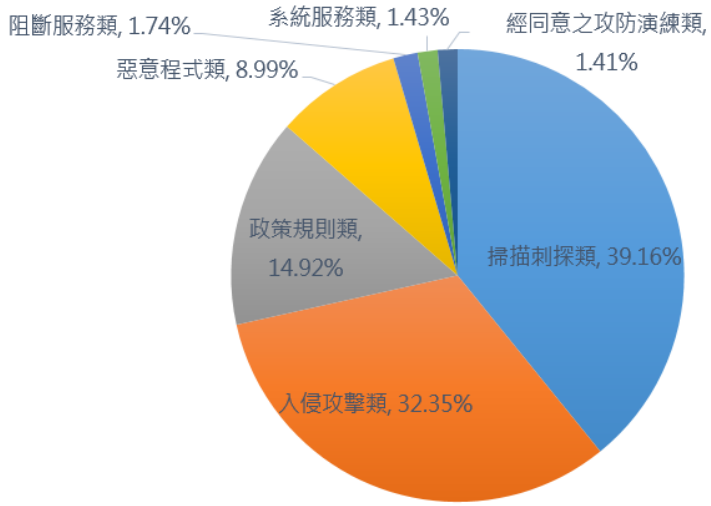


圖 2 各類資安威脅分布圖

二、惡意電子郵件分析

透過惡意電子郵件進行進階持續性威脅攻擊為組織型駭客常用之手法，有別於一般廣泛散播之惡意程式較容易被防毒軟體等偵測防護，組織型駭客持續發動魚叉式網路釣魚攻擊，做為入侵政府機關電

腦，以竊取公務、國防及商業機密並佈建情蒐網路之主要手段。109年政府領域攻擊趨勢主要可歸納為三波攻擊行動，第一波為年初利用COVID-19議題與政府機關採購主旨進行魚叉式網路釣魚攻擊；第二波則是年中利用520總統就職典禮一事，針對不同政府機關與重要人士寄送惡意電子郵件；最後一波則是雙十國慶期間，利用系統相關問題主旨對政府機關業務負責人發動攻擊。

為了解109年針對政府機關之惡意電子郵件攻擊趨勢，經蒐集相關惡意行為資訊進行分析，偵測發現惡意電子郵件數量約占整體電子郵件3.21%，每月惡意電子郵件偵測數量統計(詳見圖3)。109年8月與11月因有大量詐欺釣魚郵件散佈，造成惡意郵件偵測數量偏高。8月惡意郵件主要為偽冒安全通知相關郵件主旨，要求收件人繳付比特幣以避免機敏文件外洩，11月惡意郵件則是使用知名電商Amazon相似之網路域名詐騙使用者，以投資名義要求收件人回傳個人機敏資訊。

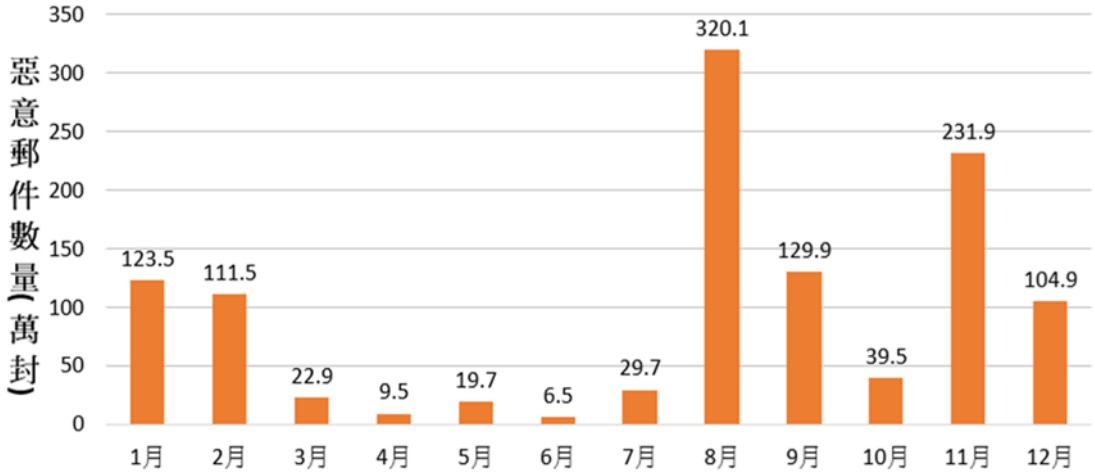


圖3 每月惡意電子郵件偵測數量

三、資安攻防演練

為有效提升政府機關在面對網路攻擊之應變處理能力，本院每年

皆針對政府機關辦理網路攻防演練，109 年共計 66 個機關參與演練，演練內容包括「資通系統實兵演練」及「社交工程演練」兩類，109 年演練結果說明如下：

(一)資通系統實兵演練

109 年網路攻防演練，共計針對 66 個演練機關 5,289 個對外資通系統進行演練，依其可能產生的衝擊性分為高衝擊性、低衝擊性及尚無衝擊性(簡稱 Info 衝擊性)3 種類型。

本次演練共發現 266 個弱點，其中高衝擊性弱點數量 72 個，占整體弱點數量 27.07%；低衝擊性弱點數量 99 個，占整體弱點數量 37.22%；Info 衝擊性弱點 95 個，占整體弱點數量 35.71%(詳見圖 4)。而 Info 衝擊性則包含非機敏資訊洩漏或低權限帳號被取得，惟該弱點尚無法被直接有效利用，其中有 44 個機關之系統發現至少 1 個 Info 衝擊性以上弱點，占演練機關總數之 66.67%(詳見圖 5)。依中央及地方機關區分存在弱點之資通系統比例，中央機關占 31.20% ，地方機關占 68.80% (詳見圖 6)。

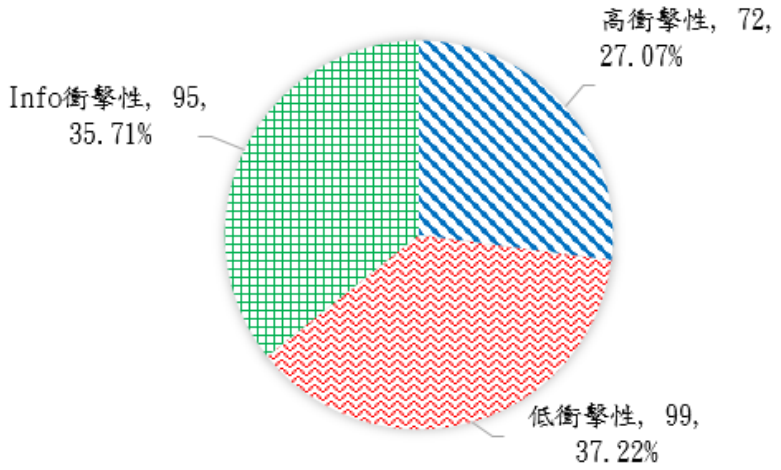


圖 4 弱點衝擊性比例分布圖

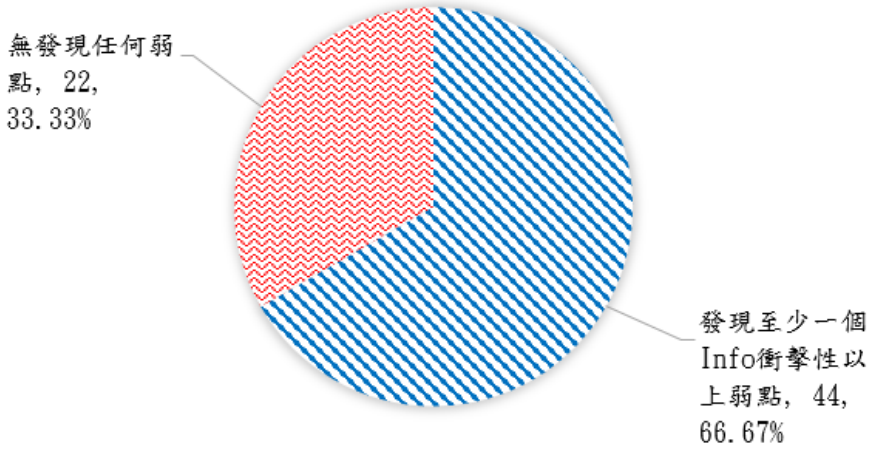


圖 5 發現弱點之機關比例圖

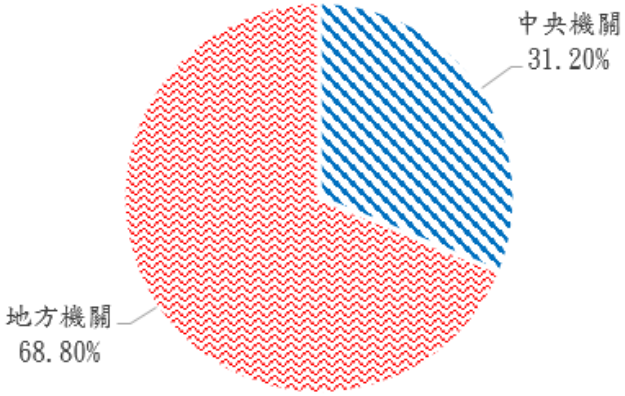


圖 6 存在弱點之資通系統比例圖

(二)社交工程演練

在參與演練的 66 個機關中，開啟社交工程郵件之機關有 48 個，占演練機關數量之 72.73%(詳見圖 7)，參演機關同仁開啟社交工程郵件比率為 6.53%(詳見圖 8)；點閱連結/附件之機關有 48 個，占演練機關數量之 72.73%(詳見圖 9)。此外，在 66 個機關中有 59 個機關配合參與社交工程簡訊演練，其中點閱簡訊連結之機關有 41 個，占演練

機關數量之 69.49%(詳見圖 10)。

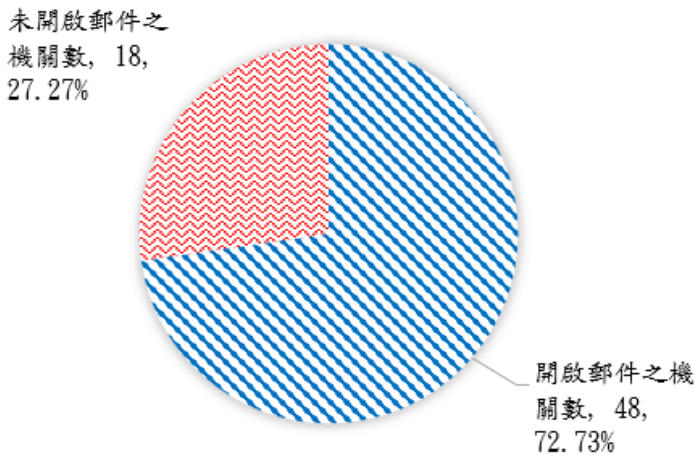


圖 7 開啟郵件機關比例圖

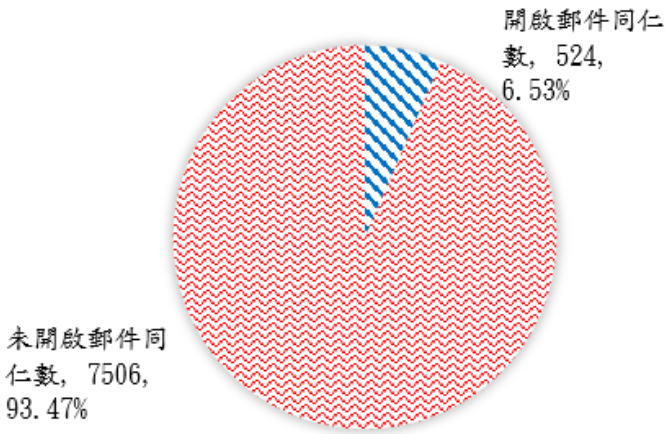


圖 8 機關同仁開啟郵件比例圖

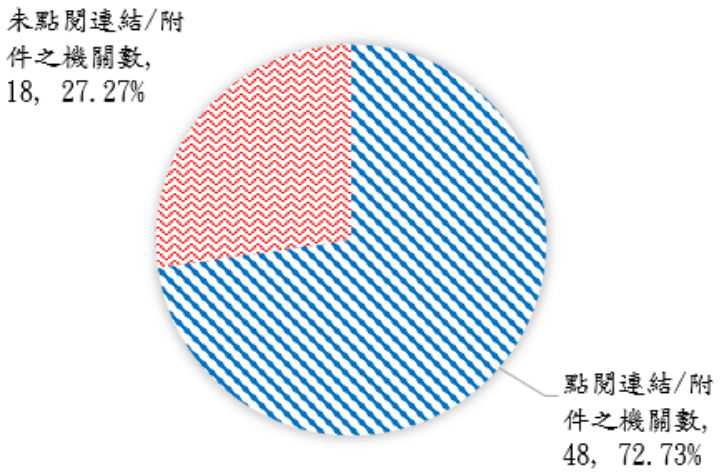


圖 9 點閱郵件連結/附件機關比例圖

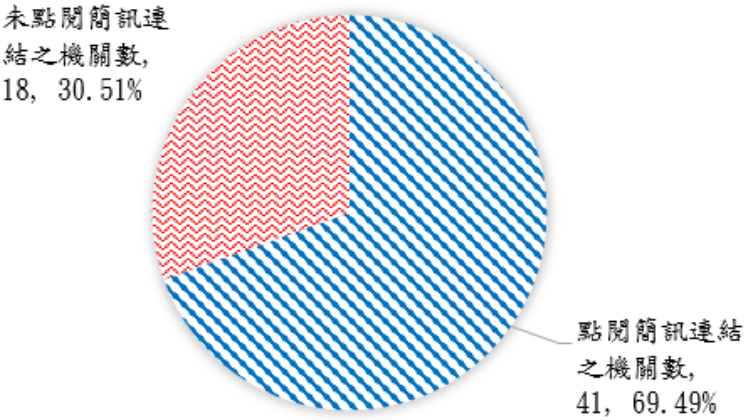


圖 10 點閱簡訊連結機關比例圖

四、資安稽核作業

為落實資安分層管理監督作業，109 年稽核對象以行政院所屬各部會行總處署為主，共選擇 15 個公務機關辦理稽核作業，辦理情形如下：

(一) 實地稽核

實地稽核作業分別依「策略面」、「管理面」及「技術面」3 個

構面進行，「策略面」稽核項目包括：「核心業務及其重要性」、「資通安全政策及推動組織」及「專責人力及經費配置」；「管理面」稽核項目包括：「資訊及資通系統盤點及風險評估」、「資通系統或服務委外辦理之管理措施」及「資通安全維護計畫與實施情形之持續精進及績效管理機制」；「技術面」稽核項目包括：「資通安全防護及控制措施」、「資通系統發展及維護安全」及「資通安全事件通報應變及情資評估因應」，共計 9 個稽核項目。109 年公務機關實地稽核各項目之成績分布(詳見圖 11)，其中成績較高為「資通安全維護計畫與實施情形之持續精進與績效管理機制」，顯示受稽機關已逐步重視推動及檢討資通安全維護計畫，並對其實施情形落實管控作為；另「核心業務及其重要性」成績相對較低，顯示受稽機關對機關核心業務及核心資通系統分級尚待加強。

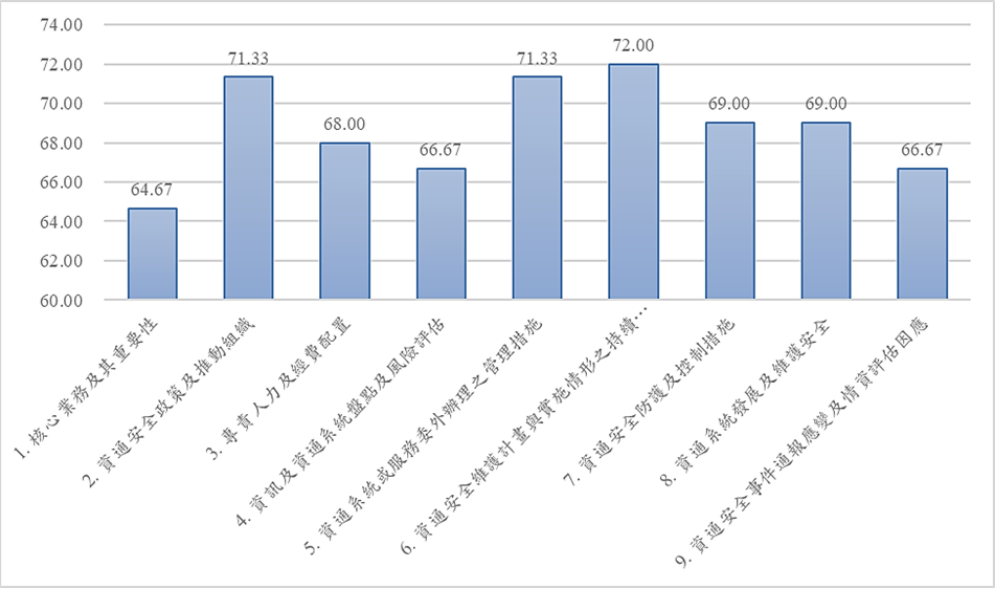


圖 11 公務機關實地稽核個別項目成績分布圖

(二)資安稽核共同發現事項

1. 策略面

(1) 未有效落實核心業務與核心資通系統之界定，且部分機關之資通安全維護計畫與實施情形之填報內容有所差異。

(2) 未完整建立機關內、外部利害關係人清單，並定期檢討其適宜性。

(3) 資通安全相關法遵、資安威脅趨勢及技術知能要求與日俱增，惟部分機關受限資安人力資源，未配置資安專職/責人力。

2. 管理面

(1) 已辦理資訊資產盤點並建立資產清冊，惟盤點範圍與內容完整性不足。

(2) 資訊委外作業未於合約或規範書明確規範防護基準需求，且未依法規定規劃與落實(如委外廠商選任要求、防護基準納入 RFP、安全檢測、通報程序等)。

(3) 已規劃並執行資通安全內部稽核作業，惟部分機關稽核對象未涵蓋全機關，且稽核項目未完整納入資安法應辦事項。

3. 技術面

(1) 部分機關網路架構安全性仍顯不足，如網段區隔與存取控管未確實。

(2) 已進行網站安全性檢測、滲透測試及資通安全健診等作業，惟未訂定相關作業程序進行後續追蹤。

(3) 資通系統安全開發程序未納入資通系統防護需求。

(4) 已辦理資安事件通報與應變演練，惟未納入事件通報環節，另建議將新興資安議題或事件納入演練情境。

五、政府機關資安事件通報

經彙整 109 年國家資通安全通報應變網站所接獲之政府機關通報事件共計 525 件，分別依事件所造成機密性、完整性及可用性之衝擊嚴重度區分，由輕至重分為 1 級、2 級、3 級及 4 級，109 年政府機關各級事件通報數量分布(詳見圖 12)。

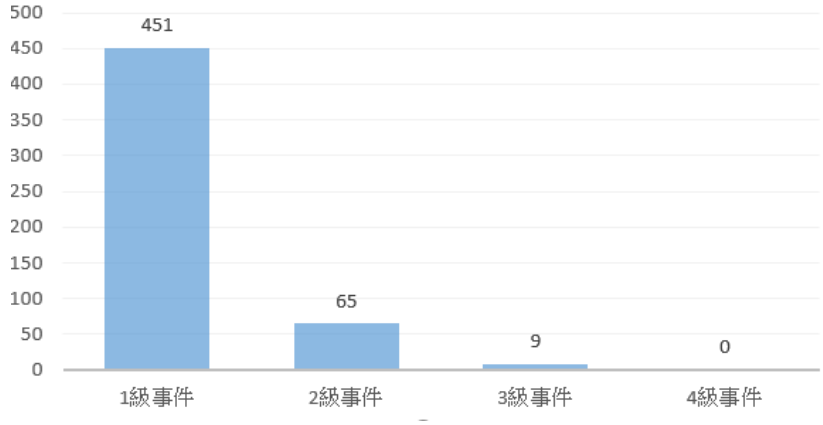


圖 12 109 年政府機關各級事件通報數量分布圖

依資安事件通報類型可分為非法入侵、網頁攻擊、設備問題、阻斷服務(DoS/DDoS)及其他，經統計 109 年政府機關通報類型比率(詳見圖 13)，其中「非法入侵」占事件通報類型 68.76%為最大宗，主要肇因於第三方產品套件漏洞、主機未啟用作業系統自動更新功能或遠端連線管理問題，相關案例包含政府機關遭駭客植入勒索軟體、政府機關監視器遭植入惡意程式、政府機關內部網路遭駭客潛伏及承包廠商成為駭客入侵政府機關之跳板等。「網頁攻擊」占事件通報類型 6.67%，主要肇因於網站未做好權限控管、檔案格式限制或第三方套件更新等作業，遭駭客利用而成為攻擊目標。分析 109 年通報事件分布情形，中央機關占整體 49.24%，地方機關則占 50.76%。

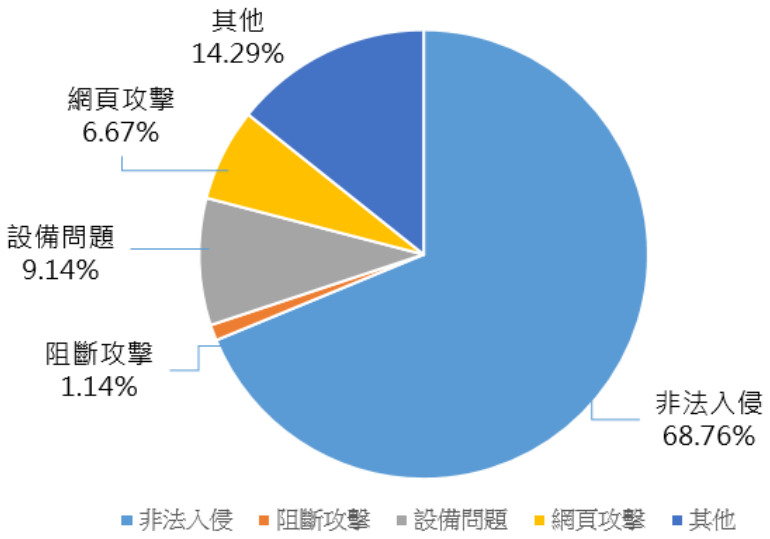


圖 13 109 年政府機關通報類型比率圖

肆、政府機關資安威脅情勢與防護建議

經綜整 109 年國內外資安威脅情資，歸納政府機關面臨之資安威脅及相關防護建議如下：

一、持續出現個資遭洩案例

個人資料保護議題日益受到重視，不法集團利用盜取之個人資料進行詐騙與身分盜用案件層出不窮，再加上暗網助長非法資料交易，個人資料一旦洩露，將導致源源不絕之攻擊。

109 年通報案例即發生某國立大學向校內學生寄出講座通知信時，誤夾帶學生個人資料作為附件，造成個人資料外洩。另發生某機關因辦理活動架設網站，廠商誤將未經遮罩之敏感資訊上傳網站，致民眾個人資料外洩。由此可見，個資外洩問題除外部駭客攻擊竊取因素外，亦可能肇因於人員操作或內部管控不當。

建議各機關應加強同仁對於個資管理之教育訓練，以提高個資保護意識，並定期檢視同仁存取個資及機敏資料之權限設定，建立資料上傳審核流程，對於敏感資料之檔案應加強防護。另因應疫情需求所蒐集之實名登錄個資，應指定專人辦理並善盡資料保護責任，落實管控與刪除銷毀作業。

二、勒索軟體阻斷系統服務運作

勒索軟體攻擊肆虐全球，我國公私機關部門亦難倖免於外，勒索軟體會藉由加密檔案，致使受害者無法正常使用電腦，影響業務運作，進而達到勒索贖金之目的。攻擊對象也從過往隨機攻擊，轉變成鎖定大型企業或政府關鍵基礎設施領域之目標式攻擊。

以某機關發現遭受勒索軟體攻擊為例，駭客經暴力破解設備維護廠商使用之帳號密碼，再橫向擴散至其他設備，利用勒索軟體加密資

料，致相關資通系統無法於可容忍中斷時間內恢復運作，造成三級資通安全事件。另在能源領域所發現勒索軟體攻擊之案例，則是駭客入侵公司系統長期潛伏及探測，最終利用勒索軟體加密重要檔案，以要脅鉅額贖金。面對勒索軟體攻擊成為常態，如何制定應變措施，以縮短災害復原耗費之時間將成為關鍵。

建議各機關應落實系統弱點修補及軟韌體更新作業，在設定系統登入密碼時應符合複雜性原則，網路架構上應有適當區隔及存取控制，重要資料應建立異地備份備援機制，定期辦理營運持續演練，降低資通系統遭受勒索軟體攻擊之風險，並強化機關成員之資安意識，避免點擊來路不明之檔案或連結。

三、物聯網設備因韌體未更新遭植入惡意程式

物聯網設備逐漸在政府機關被普遍使用，包括網路印表機、網路攝影機、無人機、無線網路基地台及無線路由器等，常因韌體或軟體未更新，導致漏洞被利用進行攻擊之風險大幅提升，對資安防護構成嚴峻挑戰。

以數個政府機關使用之某廠牌網路攝影機為例，該設備在短短半年間陸續遭揭露多個資安漏洞，其中包含因未強制變更預設密碼，使駭客可利用預設密碼登入，篡改網路介面設定，另駭客亦可利用其中一種漏洞，進行命令注入攻擊，執行任意指令。

建議各機關採購具備通過資安檢測之物聯網設備，使用前應變更設備預設帳號密碼，隨時注意原廠所提供之更新通知，落實即時更新作業，縮短漏洞被利用之空窗期。並妥善規劃物聯網設備之網路連線行為監控與加強存取控制。

四、進階持續性威脅攻擊竊取機敏資料

進階持續性威脅攻擊係採取針對性、持續性、隱密性並且經過精心策劃後，對目標對象進行入侵滲透攻擊，目標對象多鎖定政府機關及大型企業竊取公務及商業機密。

經發現駭客透過市面上常見的免費虛擬私人網路（Virtual Private Network，VPN）工具，將機關內部相關電腦連結成大內網，再利用 VPN 加密傳輸資料不易偵測之特性，長期潛伏於機關內部網路。另發現駭客除透過社交工程惡意電子郵件散布後門程式，亦使用 HTTPS 或 DNS 隧道通訊(DNS Tunnel)等加密技術，偽冒合法網站隱藏中繼站連線資訊，進行資料竊取。

建議各機關可於入侵偵測系統與入侵預防系統，部署進階持續性威脅攻擊之偵測規則及端點偵測系統，進行異常連線行為之即時偵測。並持續透過社交工程演練與教育訓練，加強人員資安意識，避免進階持續性威脅透過惡意電子郵件攻擊造成機敏公務資料外洩。

五、政府機關委外供應鏈遭駭侵

政府機關之資訊及資安業務多以委外方式由國內資訊服務業者承作，資訊服務業者對於資安的重視程度，影響政府機關之資安防護甚深，承包政府標案之供應鏈委外廠商如遭入侵，將成為駭客入侵政府機關之跳板。

以某機關提供委外廠商以 VPN 遠端連線方式進行資通系統維護為例，駭客透過入侵資安防護相對脆弱之委外廠商，間接利用 VPN 遠端連線存取方式，攻擊機關資通系統。另亦發現駭客利用入侵委外廠商雲端儲存服務之軟體更新服務，掩飾惡意行為，作為惡意程式下載之途徑，導致機關由正常管道更新軟體時遭植入惡意程式。

建議各機關開放機關內部同仁及委外廠商進行遠端維護資通系統，應採「原則禁止、例外允許」方式辦理，如機關因地理限制、處理時效及專案特性等因素例外允許時，應建立及落實異常行為管理機制，並於結束遠端存取期間後，應確實關閉網路連線，並更換遠端存取通道登入密碼。另為避免公務及機敏資料遭不當竊取，公務機關不得使用或採購大陸廠牌資通訊產品，並應就已使用或採購之大陸廠牌資通訊產品列冊管理，且不得與公務環境介接。

伍、結語

藉由檢視 109 年資安事件發現，個人資料保護、強化委外廠商資安管理、提升社交工程之資安意識及物聯網設備之資安管理，仍為政府機關當前重要之資安防護議題。

面對新興科技帶來之資安議題，本院將持續透過資安監控與威脅情蒐，即時發布資安警訊，並分析駭侵樣態及手法，研擬相關防護建議，提供機關作為早期預警與預為防範之參考。並要求各機關落實追蹤稽核作業及攻防演練之改善建議，及依規定時限內進行資安事件通報，以完成後續損害控制及復原作業。此外，本院將透過主動式防禦機制之建構，持續深化政府機關之資安縱深防護，並持續透過資安稽核與攻防演練，引導政府機關精進資安防護能量，落實資安防護作業。