資通安全網路月報（113年3月）

資通安全網路月報(113年3月)

<近期政策重點>

政府機關運用社群媒體作為政策溝通管道，雖社群平臺非政府機關自建之資通系統，但以機關名義推廣業務，仍須注意使用管理，倘社群平臺帳號遭盜用，進而影響機關服務或資料之機密性、完整性或可用性，亦屬應通報之資通安全事件。政府機關如使用社群平臺推動業務，應注意以下事項：

一、定期盤點及管理社群平臺維護帳號(含委外處理部分)，包含不共用帳號、不使用弱密碼及啟用多因子認證等，定期檢查帳號登入紀錄。

二、社群平臺上不應傳遞機密或敏感資訊，社群網站如已無經營需求，應予關閉。

<整體威脅趨勢>

事前聯防監控

本月蒐整政府機關資安聯防情資共5萬3,440件(較上月增加5,528件)，分析可辨識的威脅種類，第1名為資訊蒐集類(40%)，主要是透過掃描、探測及社交工程等攻擊手法取得資訊；其次為入侵嘗試類(20%)，主要係嘗試入侵未經授權的主機；以及入侵攻擊類(12%)，大多是系統遭未經授權存取或取得系統/使用者權限。統計近1年情資數量分布，詳見圖1。

經進一步分析聯防情資，發現近期駭客以資料外洩之時事新聞，寄送主旨為「某國政府雇傭黑客攻擊鄰國證據確鑿」之社交工程電子郵件，攻擊政府機關人員，相關情資已提供政府機關聯防監控防護建議。

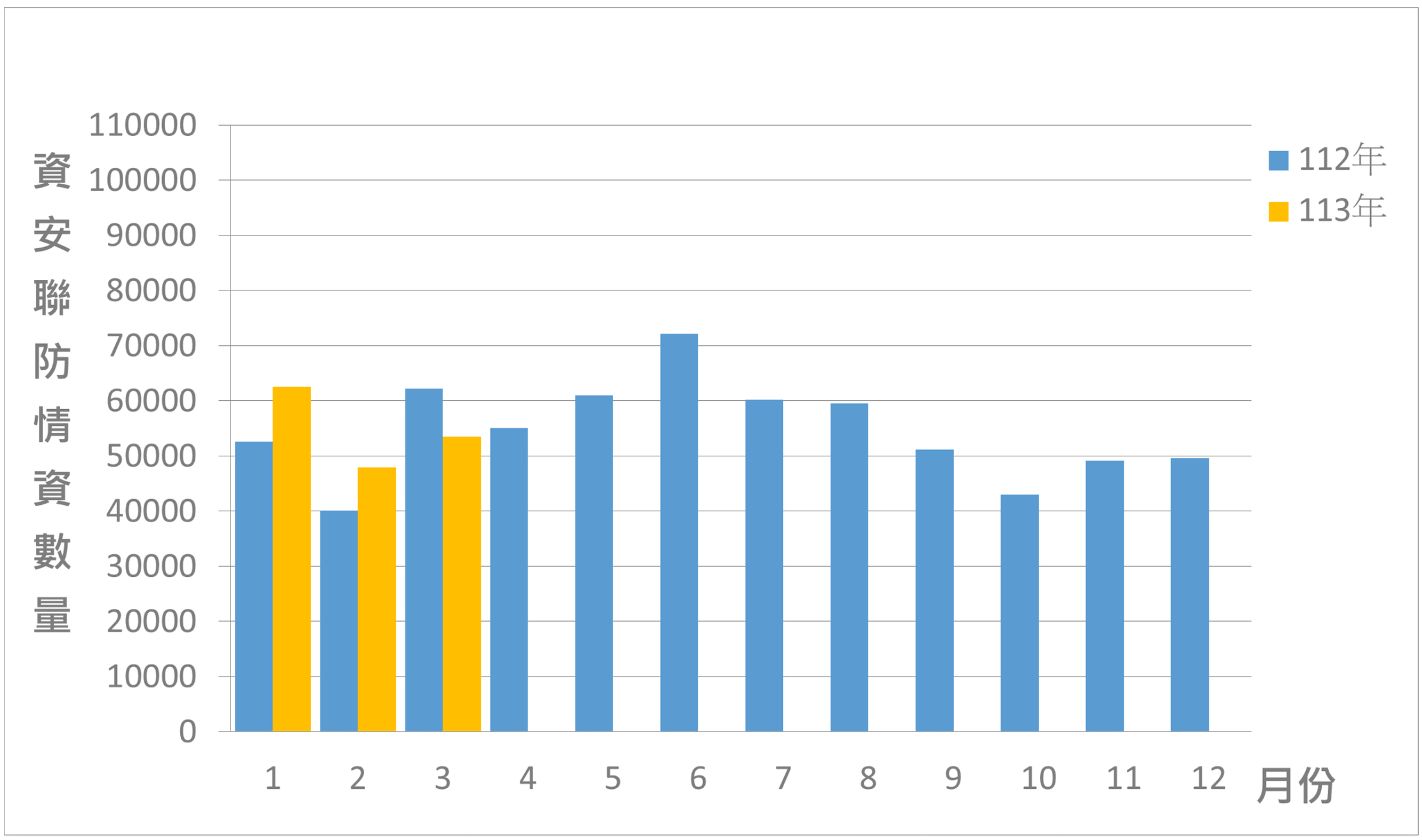

圖1 資安聯防監控資安監控情資統計

事中通報應變

本月資安事件通報數量共83件（較上月增加10件），與上個月相比，通報件數增加13.7%，部分機關因使用某機關所提供之共用行政系統具安全性漏洞，且機關未限制網際網路存取，遭駭客入侵成功並上傳惡意程式，該事件佔「非法入侵」事件類型之13.2%。近1年資安事件通報統計詳見圖2。

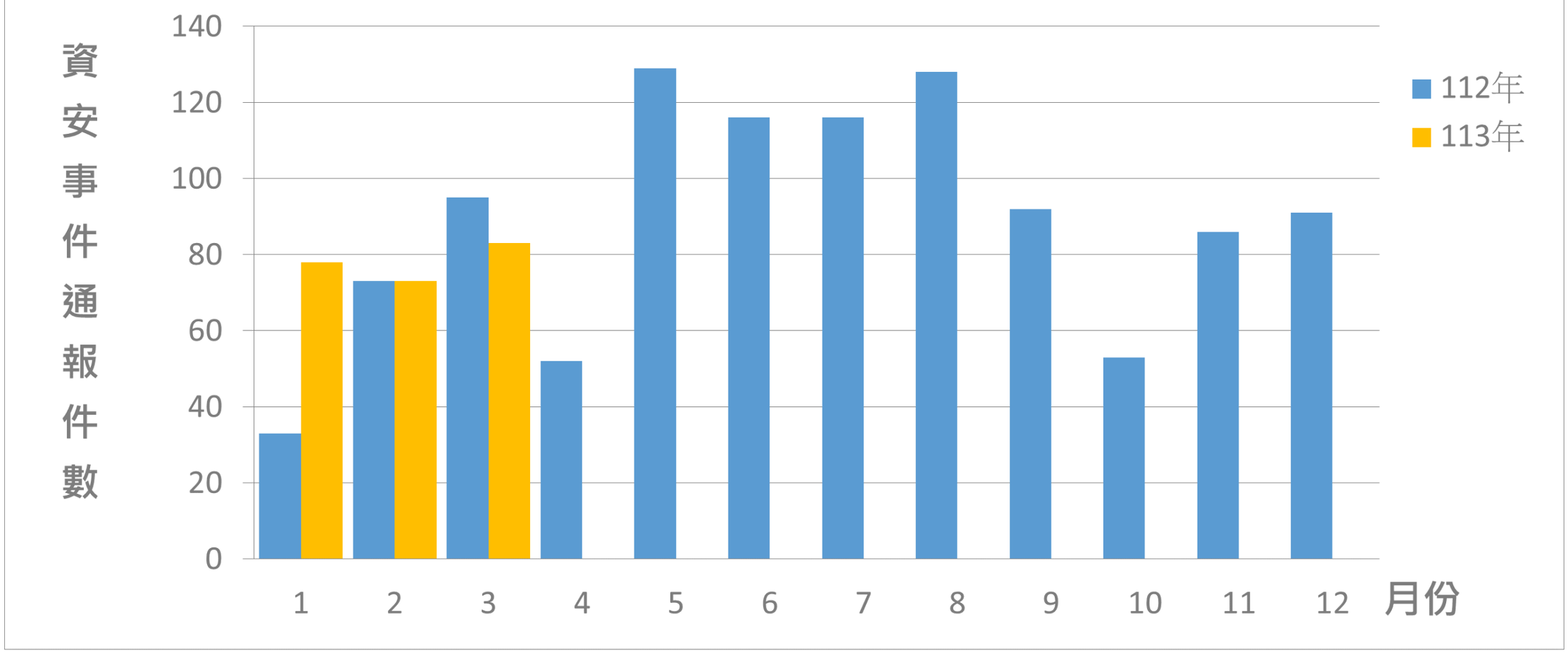

圖2 資安事件通報統計

事後資訊分享

某機關持續遭國家資通安全研究院偵測到符合偽冒通訊軟體Line之惡意程式持續連線中繼站，經查該機關自本年1月起即持續有連線行為，經洽機關皆表示已將受駭主機重置，機關系統亦已檢視更新，並向使用者宣導至官方網站下載正確版本，亦要求廠商協助於防火牆設定阻擋中繼站；惟後發現該機關僅口頭宣導，未確認使用者行為與廠商執行情形，導致持續連線至相同的中繼站。

足資借鏡：

發生資安事件時，應進行事件根因分析，據以提出有效的強化作為與改善措施，並落實執行；惟部分機關可能受限於人力與資源，僅以重建資訊環境進行事件處理，未確實釐清事件根因，施以有效管控作為，或未落實辦理改善作業，導致資安事件一再發生。為降低資安事件發生風險，針對使用者下載或安裝軟體應予限制或規範、確實檢視改善作業落實情形(含委託供應商部分)，資安事件如持續發生，更應審慎檢視根因及應處，以確實處理風險。

<國內外重點資安新聞>

一、數位發展部提3大策略 通傳關鍵基礎設施強化資安防護

數位發展部公布強化通訊韌性3大策略，持續推動建設海陸空應變通訊網路、強化通傳網路防護及普及通訊寬頻網路建設。並針對督導的通訊傳播領域關鍵基礎設施（CI），要求擬定防護計畫，進行資安演練與稽核，以強化資安防護，確保台灣通訊網路緊急狀況不斷訊。

(資料來源：中央社，聯合新聞網)

二、APT駭客組織鎖定多國進行攻擊

外媒報導，中國知名APT駭客組織「Earth Krahang」鎖定45個國家的116個單位為攻擊目標，攻擊地圖顯示包含台灣。

Earth Krahang熟練運用釣魚電郵散布木馬程式，另也擅長利用系統漏洞，使用開源工具來掃描公開的伺服器，尋找特定漏洞如CVE-2023-32315(Openfire)和CVE-2022-21587(Control Web Panel)。駭入後， Earth Krahang即在受害主機上建置VPN伺服器，進行日後長期控制與持續滲透其他內部系統。

(資料來源：資安人)

<近期重要資安會議及活動>

為推動政府機關資安人才培育機制，瞭解常見之駭客攻擊手法，數位發展部資通安全署於113年3月21日至3月23日辦理113年度「資安工作坊」。透過模擬環境實機練習及舉辦攻防演練活動，增加公務機關資安人員技術實戰經驗及機關間互動交流。

<資通安全長及資訊主管異動情形>

立法院資通安全長於113年3月13日起，原由高顧問明秋兼任，改由張裕榮副秘書長兼任。

發布單位：資通安全署　　建立日期：2024-04-15　　更新日期：2024-04-12