113年11月號

公務機密 資訊安全維護

林業及自然保育署
臺東分署

公務機密 資訊安全維護

目錄

2024年重大資安事件回顧 超過10億筆個資外洩

2024-10-15
編譯／Cynthia

2024年成為全球資料外洩事件的高峰期，超過10億筆資料遭駭客竊取，創下歷史新高。駭客手法日趨複雜，從網路釣魚到勒索軟體、憑證盜用，幾乎無孔不入，許多企業和機構的資安防護無法應對，導致頻繁的重大外洩事件，不論是科技大廠、通訊業者，還是醫療及金融機構，無一倖免，資料外洩對全球各行各業及個人安全產生重大影響，除了損害企業聲譽，更對個人隱私造成無法估量的損失。

通訊與科技業面臨嚴重資料外洩

通訊與科技業在2024年成為資料外洩的重災區，美國通訊供應商AT&T當年發生兩起嚴重的外洩事件，影響高達1.1億名客戶，洩露的資料包括電話號碼及通話記錄，甚至連非客戶的電話也受到波及，這些資料不是直接從AT&T系統中被竊取，而是透過數據公司Snowflake的帳號遭攻擊。此外，Snowflake也因資料工程師憑證遭盜用，導致數億筆客戶資料外洩，受影響企業包括Ticketmaster和Advance Auto Parts等知名公司。這些事件對高風險族群的隱私造成重大威脅。

醫療系統面臨嚴峻資料外洩危機

2024年，醫療產業也遭受多起資料外洩事件的重擊。醫療科技公司Change Healthcare遭到勒索軟體攻擊，被竊取大量醫療和帳單資料，影響美國約三分之一的人口，並使醫療體系大規模癱瘓，導致醫院、診所無法正常運作。同時，英國的Synnovis實驗室也被駭客入侵，300萬筆病患資料外洩，導致數千台手術延後，英國國民保健署（NHS）被迫宣布進入緊急狀態。此外，健康保險公司Kaiser意外洩露1,340萬名患者的健康資料，這些資料被廣告商利用，嚴重威脅患者隱私。

政府與金融機構資料外洩風波

2024年，政府與金融機構也頻頻遭受資料外洩攻擊。2月美國藥品公司Cencora遭駭客入侵，數百萬患者的醫療資料被竊，影響範圍廣泛。4月澳洲的MediSecure系統被勒索軟體攻擊，約1,300萬人的個資與健康資料被盜，相當於全國一半人口受到波及。10月數據公司National Public Data因洩露3億筆敏感資料，如社會安全號碼等，無法應對法律訴訟，最終申請破產保護，這起事件成為今年最大資料外洩事故之一，對企業和個人造成長期損害。

資料外洩事件顯示數位安全隱憂

2024年，多起重大資料外洩事件再次突顯數位安全的脆弱。不論是通訊、科技、醫療，還是政府與金融機構，這些外洩問題無所不在。每次事件都對個人隱私和企業形象造成嚴重損害，顯示出企業和機構在資料防護上的不足。這不僅是駭客技術的提升，更是安全措施的落後所致。面對日益嚴峻的趨勢，企業與政府必須採取更強的保護措施，避免未來類似事件再度發生。

資料來源：TechCrunch

卡西歐遭勒索軟體攻擊，攻擊者也曾駭入臺灣公司

文/林妍溱 | 2024-10-13發表

日本消費電子大廠卡西歐（Casio）上周證實，公司遭勒索軟體攻擊，造成公司多個系統一周無法使用，以及為數不詳的員工資料及部分客戶個資外洩。這個組織並在今年7月攻擊一家臺灣廠商。

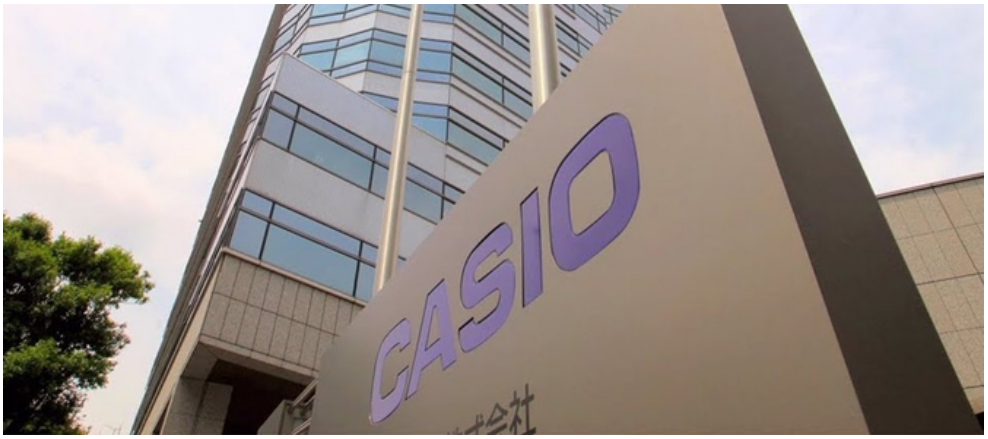
上周卡西歐透過官網公告，10月5日該公司確認遭網路攻擊，經過調查顯示，未經授權的存取，致使該公司部份伺服器故障，造成多個系統無法運作，並導致一些服務斷線迄今。10月11日卡西歐公布初步調查結果，該公司及其關聯公司部分個資和機密資訊已外洩。

Bleeping Computer報導，Underground背後的駭客組織宣稱犯案。駭客也在其網站公布其受害公司名單，以及一批卡西歐資料內容。

資安業者Fortinet說明，這個組織名為RomCom或Storm-0978，專門部署Underground。Fortinet分析，該駭客組織是濫用Microsoft Office和HTML RCE漏洞CVE-2023-36884以入侵受害者網路，也可能使用電子郵件、或從其他駭客購得存取資料。微軟已在8月份的Patch Tuesday予以修補。

根據Fortinet的研究，RomCom公布的受害名單光是從今年2月到7月就有十多家，包含一家臺灣公司。

作為最新的受害者，卡西歐說明，10月初的攻擊外洩的資訊包括員工（包括臨時和約聘員工）個資、關聯企業的部份員工的個資、合作夥伴個資，以及應徵者個資、使用過卡西歐服務的部份客戶資訊。此外，卡西歐也被竊走合作夥伴合約、發票、銷售，及其和關係企業的法務、財務、人事規劃、客服、銷售和技術資訊。



圖片來源:Casio

在網路上公布他人個資會違反個資法嗎？洩漏個資會有那些刑責？

個人資料定義

依照個人資料保護法第2條第1款規定：「個人資料是指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。」換言之，個人資料是指「自然人」的資料，且除了上開規定列出的項目外，還要特別留意「其他得以直接或間接方式識別該個人之資料」也屬之，像手機號碼就是一例。而在非公務機關蒐集、處理、利用他人個資時，原則上必須要在「特定目的必要範圍」內為之。

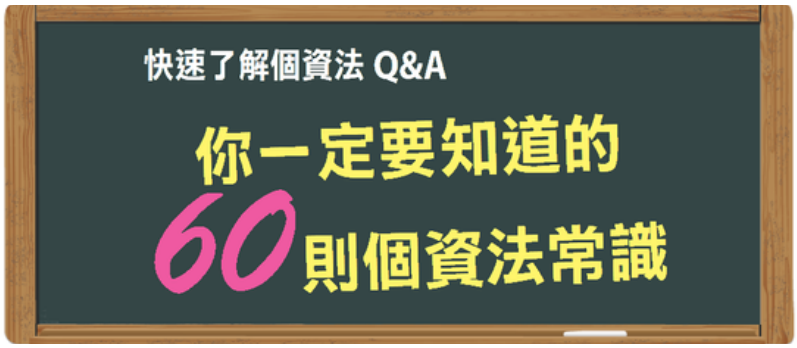
哪些行為會違反個資法？

1. 未經同意收集個人資料： 未經個人同意，擅自收集、處理或利用個人資料可能違反個資法，應通知資料主體有關其個人資料的收集、處理與利用，並提供其相應的權利，如：查詢、更正、刪除等。 但如果個人主動在社群網站上公開個人資料，並在使用該平台時同意了相關條款，那麼這可能被視為他們已經同意他人搜尋他們的資訊。
2. 資料用途不當： 收集的個人資料必須依照明確的目的使用，不得擅自改變或超越原定的使用範圍。如果網友進行肉搜是為了合法的目的，例如：尋找失踪人口、防止犯罪等，這可能被視為合法行為；但如果肉搜的行為涉及到騷擾、侵犯他人隱私或是用於非法目的，則可能違反個資法。
3. 資料安全不當： 對於敏感性較高的個人資料，例如：醫療紀錄、金融資訊等，處理時應該採取合理的安全措施，以避免資料外洩、損毀或被未經授權的人取得。
4. 跨境轉移個人資料不當： 如果需要將個人資料轉移到其他國家，可能需要得到當事人的同意，並確保轉移符合法律的要求。
5. 未成年人資料處理： 許多地區的法律都有針對未成年人的特殊隱私保護規定，在未經法定代理人同意的情況下，公開或搜尋未成年人的個人資料可能違反這些法律。

洩漏個資刑責

1. 刑事部分：有分告訴乃論或非告訴乃論之罪。
2. 依照個資法第41條規定：「意圖為自己或第三人不法之利益或損害他人之利益，而違反第六條第一項、第十五條、第十六條、第十九條、第二十條第一項規定，或中央目的事業主管機關依第二十一條限制國際傳輸之命令或處分，足生損害於他人者，處五年以下有期徒刑，得併科新臺幣一百萬元以下罰金。」，若意圖為自己或第三人不法利益或者有損害他人利益，足生損害於他人者（包含非財產上損害，且不以實際發生損害結果為必要），就可能會構成此項違反個資法的犯罪。
3. 個資法第45條規定：「本章之罪，須告訴乃論。但犯第四十一條之罪者，或對公務機關犯第四十二條之罪者，不在此限。」
4. 民事部分：
5. 個資法第28條：「公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。但損害因天災、事變或其他不可抗力所致者，不在此限。
6. 被害人雖非財產上之損害，亦得請求賠償相當之金額；其名譽被侵害者，並得請求為回復名譽之適當處分。
7. 依前二項情形，如被害人不易或不能證明其實際損害額時，得請求法院依侵害情節，以每人每一事件新臺幣五百元以上二萬元以下計算。
8. 對於同一原因事實造成多數當事人權利受侵害之事件，經當事人請求損害賠償者，其合計最高總額以新臺幣二億元為限。但因該原因事實所涉利益超過新臺幣二億元者，以該所涉利益為限。
9. 同一原因事實造成之損害總額逾前項金額時，被害人所受賠償金額，不受第三項所定每人每一事件最低賠償金額新臺幣五百元之限制。
10. 第二項請求權，不得讓與或繼承。但以金額賠償之請求權已依契約承諾或已起訴者，不在此限。」
11. 受害人也可依民法第184條、195條之規定向加害人提起侵權行為訴訟。 資料來源:黃建閔律師事務所

每月一常識



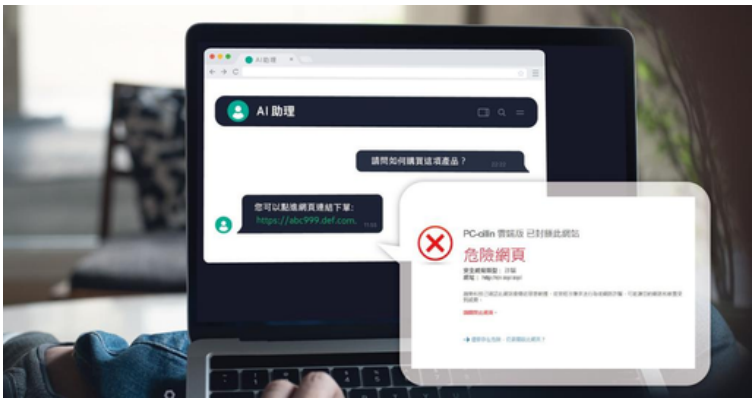
新版個人資料保護法與過去有很大的不同，新法進一步擴大了個人資料的保護範圍，並且讓所有產業一體適用；新法甚至首度增加團體訴訟，而且違法的罰則也加重了，企業老闆要負更大的責任。接下來，我們以60個Q&A，快速帶你認識新版個人資料保護法

Q7 往生者的個人資料是否受到保護？

A 個資法所稱的「個人」，是指擁有自主決定權的現生存自然人，因其隱私權可能受侵害，所以，往生者的個人資料不受個資法的保護。

文/iThome

網路資安3大隱憂不得不防 貪圖便利小心被駭



民眾使用AI助理時，切勿隨意提供機密資料，在點選外部連結前也務必再三確認。（趨勢科技提供）

2024.10.17 中時即時 古明弘

AI無所不在，提供快速便利的生活，但也衍生資安問題。趨勢科技剖析AI世代下，民眾使用AI助理、上社群、瀏覽網頁時的3大資安隱憂，呼籲民眾留心並重視網路身份安全。

1. AI助理是資訊傳送門，也可能成為駭客入侵的捷徑：

你是否對AI助理下達「請給我OO銀行連結」、「幫我找最便宜的班機並提供訂購連結」，若生成式AI的相關應用遭駭客植入病毒，或不慎讀取機密資料，可能導致AI助理提供錯誤資訊，甚至誤導用戶執行惡意指令或點入釣魚網址。趨勢科技提醒民眾使用AI助理、聊天機器人時，切勿隨意提供機密資料以保障個人隱私，同時務必審視其提供內容的合理性，在點選外部連結前也必須再三留意，以避免落入個資外洩或裝置中毒等風險當中。

2. 社群連動帳號好便利，當心被盜：

「我們注意到您從不同裝置和地點登入」，當遇到帳號要求在其他位址登入，民眾通常會收到社群官方通知以保障安全。而現今有許多民眾經常使用社群帳號授權登入第三方應用程式或使用相同帳密登入其他網站，若觀察到社群帳號有疑似被盜用的跡象，除了通報官方、刪除可疑的IP位址、告知親友勿點擊訊息連結或主動回覆外，也須儘速更換設定高強度的密碼，避免威脅持續蔓延至連動帳號或使用同一組帳密的第三方應用程式和網站。

3. cookie不定期清理恐引發隱私侵犯、個資外洩：

「你是否同意並繼續此網站使用cookies？」在進入許多網頁時，經常看到類似的通知。啟用Cookie能讓網路瀏覽更流暢，省去每次重複登入會員網站，但未定期管理則會導致運作速度變慢，甚至產生個人資料存取的隱私問題。趨勢科技建議民眾每月定期清理，並在登出某個網站時，清除該網站過去存取的所有cookie，以確保個人資訊安全與維持良好的網頁瀏覽體驗。

趨勢科技今年升級推出PC-cillin 2025雲端版與PC-cillin Pro版，整合AI智能防毒防詐的多層防護技術，全面守護裝置與個資安全。PC-cillin Pro版結合雲端版功能和世界級VPN加密技術，達到雙效隱私防護。