使用最完備的資安防護為什麼還會洩密？

◎楊柏青

近幾年，國內翻譯小說類有一部頗具人氣的瑞典犯罪小說—《千禧年三部曲》，故事中的主角，莉絲・莎蘭德是一位保全公司的非正式調查員。她對調查對象總是有敏銳的直覺，並擁有出色的邏輯推理能力以及極佳的分析技巧，能到處蒐集資料並找出所有與當事人有關的大小資訊。然而，這些突出的科學辦事能力或許能說明莎蘭德如何寫出一疊令人驚嘆、富有邏輯性且結構完整的分析報告，但無法解釋她如何挖出埋藏在她調查對象的資料庫中最機密，甚至是私密的情報。後來答案終於揭曉，莎蘭德有一個不為人知的業餘興趣，她其實是整個瑞典最頂尖的駭客之一。很顯然地，莎蘭德將她的興趣也應用於工作之中，而達成常人所無法完成的任務。

在閱讀這部暢銷著作時，讀者或許會覺得相當過癮，因為一家黑心跨國大企業的不法交易，在這位頂尖駭客的巧手運作下，其機密的信件資料與文件都因此曝光，終遭政府查緝而倒閉。然而，這部小說也揭露了現實生活中，企業與個人資料會被有心人士盜用的可能性，而千變萬化的駭客手法除了攻擊個人或企業電腦中的各種系統、防毒軟體或防火牆的漏洞外，也會利用人性的弱點，以社交工程的方式散布惡意郵件，或利用社交網路植入惡意程式，令人防不勝防。

在電腦設備及軟體上，我們可以運用各種防護措施以維護資訊安全，軍事單位及部分機關內部甚至使用封閉式的區域網路，以防國家機密經由外部網路遭到竊取。然而，即便使用了最新、最完備的防護系統，機密資訊仍然有可能洩漏。其根本原因即在於「人」，不論是蓄意或粗心，人的疏忽及非理性的行為所導致的機密流失，經常對所屬公司或單位造成極大的傷害。

為減少人為疏失及不法洩漏機密等行為，以下提供一些方法供參：一、定期宣導資訊安全防護教育，輔以案例，向所屬宣導最新的竊取機密手段及其因應辦法，使相關人員獲得正確認知並提升危機處理的能力。二、舉辦資訊教育訓練，使人員具有基本的電腦與網路知識，了解駭客入侵的各種機制；許多資料的外洩即肇因於人員不熟稔其洩密機制，如在區域網路內連接無線網路設備，即有可能使系統遭到外部攻擊。三、落實人員的安全調查，負責企業或單位重要機密業務之人員，在選任或任職期間均應做好安全調查，並追蹤其在外有無不良習慣或財務糾紛等，使其竊密謀利的可能性減至最低。

除了以上列舉的方法外，更重要的是將學得的各種知識以及處置方法銘記在心，並落實執行，使之成為日常生活的一部分。資安習慣一旦養成，那麼防護的動作甚至不需刻意去思考也能持續執行。在外部防範、內部習慣的雙層保護下，資訊安全自能達到最佳狀態。（文摘自法務部調查局-清流月刊 102 年 8 月號）

嘉義區監理所 關心您