工作效率與資訊安全間的兩難

◎魯明德

由於平板電腦及智慧型手機越來越普及，且功能越來越強大，很多企業剛開始為方便高階主管出差在外，處理公事不便，而開放高階主管可以使用手持式裝置登入公司電腦，以免耽誤公事；漸漸地，這股需求已經蔓延到員工了。公司的業務人員因為需要長期在外，常常乘著空檔利用自己的電腦就把工作完成，等回公司再複製到公司的電腦，導致公司的電腦常因此而中毒。在資訊部門工作的小潘，接到長官指示，要他研議如何提升公司的資訊安全。

小潘心想：如果把電腦的 USB 介面都封起來，不就可以解決了嗎？但是，資訊部門的工作應該不是防弊，而是積極興利才是；業務人員利用工作空檔整理資料，等回公司再複製到公司的電腦，可以提升工作效率，資訊人員要防止的應該是危安事件才是。

利用師生下午茶約會的時間，小潘把這個問題提出來跟司馬特老師討論，司馬特老師喝口咖啡後娓娓道來，讓員工使用自己熟悉的設備，是可以提高工作效率，且對企業主而言，還可以節省軟硬體設備的支出，以及另外花費時間和金錢安排教育訓練；但是，相對地也隱藏了一系列企業資料外洩與安全性的問題。

根據國際電腦安全協會報告:60%的洩密事件,是來自企業內部，只有 15%是來自外部入侵;表示企業對於自己內部資訊機密的保護作為，還不是很周全。商業管理協會的研究報告也指出：白領工作者平均每週處理 11 份機密營業文件，而且這些機密文件常常會在不必要的情況下曝光。另外，39%的工作者曾經將客戶資料寄出公司；52%的員工曾在離職時，將工作資料帶走；86%的員工坦承習慣性將郵件轉寄其他人；26%的員工甚至會使用免費信箱寄送工作資料。由以上的研究發現：企業的危安事件大部分來自內部。

以往企業對於資料外洩防護所做的資訊安全措施，不外乎是：檔案加密、可移除式媒體控管及網路監控。採用檔案加密的方式，需要額外的軟、硬體配合，初期有建置成本，執行中有維護成本。也有企業採用可移除式媒體控管的方式，它的主要做法是：要求人員出入辦公場所時，交出手機，或是在電腦的 USB 介面上貼封條，並由中央控管所有終端電腦的儲存裝置，需特定人士核准才能使用。此舉不但不夠人性化,還會造成工作上諸多不便。至於透過側錄、監控、記錄，或限制藉由網路流通的未加密文件檔案的方式，如 E-mail、Skype、http、ftp 等作業，防範機密文件透過網路而外洩的方式，除不夠人性外，這些管制行為，通常無實質控管功效，僅能在事後稽核時產生作用。

聽完司馬特老師的說明，小潘又問道：現在手持式裝置的功能強大，又可提升工作效率，應該如何管理才好呢？司馬特老師喝口咖啡繼續說：由於智慧手持裝置的規格接近 PC，包括大容量的儲存能力、各式各樣的應用軟體等，許多 PC 可能遭受的攻擊，包括詐騙網站、惡意軟體，一樣可能透過這些智慧手持裝置而入侵企業內部。此外，由於智慧手持裝置的體積小，又容易攜帶，遺失或失竊的風險大增，存放其中的客戶資料、公司機密或財務資訊，可能就會因此外流。

但由於它可以讓員工利用瑣碎的時間處理公事，提升工作效率，禁止或開放對企業而言是個兩難的問題。日本的 NTT 調查發現，超過 50%以上的員工會自行攜帶智慧型手機上班，但只有 20%左右是真正得到企業正式同意，顯示員工真的有此需求。

對於資訊安全的管理，應該是從需求面去疏導而不是一味地防堵。在硬體上，可以透過雲端服務、加密通信網路及多重身分驗證等機制，讓員工即使是使用自己的私人設備，也不會讓企業的重要資訊留存在裝置上，如此一來，如果員工的手持式裝置遺失或失竊，也不會造成企業的機密或客戶的資料外流，從而維護資料的安全。在管理上，也要訂定使用規範，讓員工知道自己的權利與義務，並時時稽核。唯有落實管理制度，才能維持資訊的安全。