電子郵件在隱私與資訊安全間的衡平

◎魯明德

Fortinet在2013年10月間做了一個全球性的網路資訊安全調查，有36%的受訪者表示：他們會違反公司禁止使用資訊媒體的規定，例如因工作關係而使用個人雲端硬碟。至於尚未普及的新科技，如Google眼鏡或智慧手錶，則幾乎有近半（48%）的受訪者表示，可能會違反上班禁止攜帶的規定，其中臺灣受訪者的調查結果為43%；這個結果顯示Y世代族群，違反公司資訊安全規定的潛在性大增。

在高科技公司負責資訊安全工作的小潘，看到這份調查報告後，很快就聯想到：現階段公司已經透過資訊科技，將雲端硬碟阻隔在外，讓員工在辦公室內無法透過網路連結到雲端硬碟，暫時解決這個可能的洩密管道。但是公司內、外很多的資訊交流，都是透過電子郵件，是不是有機密資料會經由電子郵件流出，則不得而知。

電子郵件可能傳遞的是不欲人知的隱私內容，但它又可以是公司用來傳達訊息的工具。對電子郵件的管理，是一件不易拿捏分寸的問題，動輒可能會被告侵害隱私，但不作為又可能造成機密資料的外洩。

小潘把這個問題提出來請教司馬特老師，老師也很認同這是組織在管理上兩難的問題。司馬特老師特別提出，在2001年Enron、Worldcom等公司的財務欺詐行為，所引爆的一連串惡意破產事件，美國證管會在調查過程中，發現許多與案情相關的電子郵件，都被有心人士惡意刪除，因此制訂「沙賓法案」（Sarbanes-Oxley Act），規定上市公司針對與公司業務有關的電子郵件，必須至少保存7年，這又另外引發一個電子郵件的管理問題。

小潘聽完後心想：在巨量資料（Big Data）的時代中，組織要存放的資料與日俱增，再加上電子郵件，光是儲存就是一個大問題，如何還能確保不會洩密？巨量郵件資料分析與稽核的技術，是對企業郵件及智財管理者新的挑戰。

當電子郵件可能成為洩漏公司機密的管道時，雖然很多企業透過流程設計、行為監控、郵件稽核、加解密等方式，來確保資訊的安全，但是任何複雜的資料加密措施，都只是相對的安全，仍然可能發生檔案外流之後會被破解的風險；所以如果能在重要資料外洩之前便攔阻下來，自然可以避免對企業的營收或商譽造成傷害。

司馬特老師喝完咖啡後，接著說下去。其實管理要善用科技，坊間已有商品化的郵件稽核設備，通常會提供事前稽核與事後審查兩種功能，若從防止機密外洩的角度來看，企業應採事前稽核的作法，也就是在郵件送出之前，先經過完整的比對與查詢之後，才允許郵件伺服器將資料送出。不過，事前稽核執行時會遇到很大的困難，主要是郵件稽核設備必須逐一去拆解每封郵件，若郵件本身有附加檔案，還必須解開比對，若待處理的郵件過多，輕則影響業務的延遲，重則會導致設備當機，造成重要資料遺失的風險。

事後稽核的作法則是郵件伺服器在收、發信時，郵件稽核設備會同步抄錄一份資料，再依照管理者事先輸入的資料，逐一去比對各種關鍵字與欄位，當有發生異常狀況時，便即刻發出警告信給管理員，不會影響原來的工作流程。小潘聽完心想科技真是來自人性啊！但是要怎麼去比對呢？司馬特老師繼續解釋，電腦其實是很笨的，只能一個命令一個動作，比對的邏輯當然要由人給啦！我們要先定義出一些異常的行為，例如：員工把附件壓縮加密外寄到免費信箱，而沒有副知主管、在單一信件中同時出現客戶與供應商、外寄加密信件，而未副知公司內部人員等狀況，供系統進行監控、比對，才能發現異常的危安因子，避免洩密事件發生。公司的電子郵件雖然是為公務使用，

但難免會有私人訊息透過它來傳遞，這對於電子郵件的管理就變複雜了，然而透過資訊科技，仍可以在隱私與資訊安全間找到衡平點，讓企業與員工雙贏。