清流月刊中華民國一百零三年一月號

公司組織可以善用事前稽核與事後審查兩種管理機制，讓電子郵件的使用在隱私與資訊安全間平衡雙贏。

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。

（作者為科技大學資訊管理系講師）

▲Top

清流月刊中華民國一百零三年一月號
使用智慧型手機如同使用個人電腦一般，下載軟體或登錄社群網站，皆應時時保持戒心。

你使用的APP安全嗎？

◎陳婠綺

隨著智慧型手機的普及與其功能越來越強大，如同一台隨身電腦，加上使用者將許多檔案、照片也存放於手機內，因此智慧型手機延伸出的資安問題已成為國人的重要議題。

現在隨處可見的「低頭族」，人手一支智慧型手機，想要下載各種APP軟體只要手指輕輕一按就能搞定。APP市場競爭激烈，不少業者紛紛祭出「免費」軟體吸引消費者，但看似免費的背後，付出的可能是親朋好友的隱私。目前免費的APP資安軟體與付費版本最大的差異主要是功能上的不同，免費版本主要是提供基礎的偵測與防護，進階功能則必須購買付費版本。甚至有些APP本來是付費軟體，卻在重新上傳後，成為免費軟體，許多人不疑有他，還以為撿到便宜，就在不知不覺中掉入陷阱。Google雖然在Android Police回報後，５分鐘內就將這些軟體下架，但下載數可能已經超過五萬次。更可怕的是，Google本來還特別提供了名為Android Market Security Tool的工具，用以清除那些惡意軟體對手機所做的修改，從而防止手機在感染惡意軟體後，將手機中的重要資訊上傳給不法分子；結果這些歹徒居然也將Google開發的反木馬工具，改變成木馬化應用程式。這個軟體不但會蒐集手機中的相關資訊，傳送到遠端的網站，還會不經使用者允許就執行某些功能和動作，包括修改通話紀錄、攔截或監控訊息，以及下載影片等，可見手機惡意軟體的可怕程度，絕對不輸給個人電腦的惡意軟體。

事實上，相較於個人電腦用戶對下載軟體已有基本戒心，而智慧型手機用戶尚未建立起相同習慣，讓中毒的可能性大增。手機資安的問題，因為越來越多的社交網站都已推出多平台移動設備用戶端，而變得更加嚴重。這些行動裝置端的安全防禦，也比個人電腦端要差很多，加上咖啡廳、機場、旅館等公共場所提供的無線網路安全問題，讓網路犯罪分子可以利用的攻擊管道，變得越來越多。

現今網路正熱門的社群網站Facebook，也可能成為駭客釣魚的釣餌；駭客假冒Facebook名義，發送假警告信件給使用者，但使用者卻不知道其內含釣魚網頁連結，讓使用者誤信帳號已遭檢舉為垃圾帳號，需於24小時內立即點選email內的連結進行帳號安全性確認，否則帳號將可能遭永久停用。使用者一旦點選該網址後，使用者將被導向特定網頁，該網頁貌似Facebook的安全檢測系統，要求使用者輸入註冊Facebook的email帳號、密碼及生日等個人資料；輸入該網頁所要求的訊息後，使用者將再被導向另一個網頁，並被要求提供信用卡等相關資訊，最後導致個資外洩。

近來人手一支智慧型手機，使用者個人的隱私風險，也經常暴露在各種惡意程式攻擊的威脅中，智慧型手機的資安問題逐漸浮現。由於現代人將許多重要的資料、照片、訊息都存放在智慧型手機中，手機一旦遺失就可能造成重大的個資外洩問題。現今的手機未必只是一支電話，它還可能成為個人的錢包、身分證、電話簿及家庭相薄，當我們的行動裝置具有以上用途，若遭遺失或被盜，便會造成敏感資料外洩風險。再加上使用者十分依賴各項APP程式的功能，根據國外媒體報導顯示，許多手機應用程式的使用條款中，允許手機程式開發商可以查閱手機用戶的個人資料，甚至查看照片、通話對象等，個人資料就在不知不覺中外洩。許多手機用戶在下載付費或是免費的APP程式時，未詳閱程式使用條款即按下同意，此舉可能讓手機應用程式開發商有權搜尋手機內的相片，或是手機用戶的所在位置。社群網站Facebook、Badoo、雅虎公司和照片分享網站Flickr，皆坦承透過搭載Android系統的智慧型手機應用程式，可讀取手機用戶的簡訊。其餘不知名、免費下載的應用程式，大多在使用條款及條件中，也明確寫到有權取得用戶的個人資料。

程式開發商看準個人資訊能讓社群網站的定位更明確，若能提供更貼近使用者的服務則能增添網站的魅力，因此「個資」儼然成了所有業者最垂涎的商品。一項由臉書技術支援的雅虎公司服務，要求使用者提供宗教信仰、政治傾向才能進入；網路電話Skype也透過使用者拿到他們朋友的臉書照片和個資。雖然臉書要求APP在取得使用者的個資前，必須徵求使用者的許可，但若是朋友資料遭外流，當事人也不會收到任何通知。不少人開始擔心，這些看似免費的服務，實則賠上隱私代價，反倒是握有這些籌碼的業者，能吸引廣告主、APP開發商或是更大的商機。

隨著手持行動網路的普及，資訊安全已從傳統電腦作業系統，擴展到手持裝置系統，部分消費者也開始建立智慧手機和平板電腦的防毒功能。但資安業者還是提醒民眾，除了安裝適當的防毒軟體之外，更應養成良好的手機使用習慣，以保護自身的資料安全。

面對日益氾濫的手機病毒，手機用戶也不是沒有預防之道，只要遵守下列防毒程序，還是可以將手機病毒有效隔離：

一、慎用藍芽裝置。就像流行性感冒一樣，病毒肆虐期間，如果到公眾場合，最好暫時關閉手機上的藍芽接收功能。如果有陌生的手機，或任何擁有藍芽裝置的機器請求連接，最好不要接受；就算是收到朋友傳送的多媒體簡訊，對於來路不明的手機程式，還是不要任意安裝。

二、接收到亂碼顯示的文字簡訊和多媒體簡訊時，最好立即刪除，因為這些亂碼簡訊，很有可能暗藏惡意的程式碼。

三、確認手機下載網站的安全性。許多智慧型手機的用戶喜歡到網路上找尋免費的軟體下載，不過這些網站卻可能是暗藏手機病毒的大毒窟。為了要遠離手機病毒，最好不要到來路不明的網站下載軟體程式。

四、如同電腦一樣，安裝防毒軟體，定期掃毒，能夠減少手機遭到數位病毒感染的機率。

由於智慧型手機的普及，導致手機資訊外洩的案例屢見不鮮，加上雲端運算和虛擬化，外洩的個資無論是關於個人品德缺陷或遭敵威脅利誘，都已對國家安全造成嚴重的影響；身為基層的我們雖沒有接觸國家安全的重大機密，也不具有決定國家指導方針的權力，但我們每一個人都是組成捍衛國土的堅實分子，所以我們必須從自身做起，並應該戒慎恐懼，攜手共同面對這項威脅，體認國家安全、匹夫有責的觀念。唯有每個人都自我要求，恪遵規定，才能建構一個堅若磐石的安全網。

▲Top

清流月刊中華民國一百零三年一月號

資安最關鍵因素在於每位使用者是否具有一定的「資安意識」，如何攻防抵禦，相信是當前最重要的資安課題。

從駭客觀點反思資訊安全

◎吳帝瑩

民國102年是一個網路動盪不安的年份。３月20日，韓國數家銀行、保險公司及電視台的電腦因為駭客攻擊，近五萬台電腦同時當機，造成ATM故障、金融服務停擺、網站癱瘓。有人懷疑這是北韓駭客所為，韓國政府也宣布這次攻擊視為國家級的戰爭行為。在此之前的３月２號，知名軟體Evernote遭到駭客入侵，五千萬用戶必須因此重設密碼；而在那之前，包括Facebook、Twitter等知名科技公司也屢屢傳出駭客入侵、個資外洩的消息，讓這些大企業的信譽遭到極大挑戰。這些或許與我們沒有直接關係，不過大家應該都記得５月13日廣大興號事件，臺灣駭客侵入菲律賓政府的DNS主機，癱瘓菲律賓政府網站。此事曾被新聞廣泛報導，「駭客」這個詞彙也從黑暗中漸漸浮上檯面。事實上不管有沒有報導，世上每日都有大大小小的網路攻擊與盜竊發生在你我周遭，在我們不知道或不注意的時候深深地影響這個世界。

駭客，在一般人想像中是神秘且深不可測，但他們即有可能是你周遭任何一個外表看似平凡、內地裡卻擁有高超專業網路技術和知識的傢伙。駭客的存在看似與我們的生活無直接關係，事實上只要我們連線上網際網路，就隨時可能與他們接觸。

筆者在臺灣大學住宿的時侯，旁邊寢室就住著一個駭客。他是我念電機系室友的朋友，平常看起來是一個再普通不過的人，然而當有一天學校的選課系統結束我卻忘記選課時，他突然出現並幫我解決選課的問題。後來才知道他高中時就熱愛程式語言，大學時更買了許多艱澀的書籍來研究，其撰寫程式的實力早已遠遠超越同儕。但當時我以為他只是一個熱愛程式的同學，直到有一天他說他參加了駭客年會，才讓我驚覺原來我身邊就有一位活生生的「駭客」，也讓我逐漸揭開駭客這隱晦神秘的面紗。

在一般人的印象中，駭客似乎總是搗亂正常的電腦運作、破壞網路安寧的那群人，但實際上這個詞彙與身分並沒有善惡之分，駭客是中性的詞彙，代表著一種精神，亦即擁有高超的技術，想要去挑戰任何「加密」的東西。雖然這樣的舉動並不全然合法，但也不代表每個駭客都會去從事非法行為。有鑑於網路的普及和重要性與日俱增，在跨國網路攻防交戰日趨頻繁的現今，各國無不積極培養「網軍」，並將網路安全視為國防能力的重要元素。但在臺灣，不僅缺乏培養戰技等級資安能力的意識，甚至整個社會普遍缺乏資安的警覺性，使臺灣社會從上到下處於暴露在危險之中而不自知。

而所謂「駭客年會」的舉辦在世界早已實施有年，而臺灣也早在94年便舉辦了第一場臺灣駭客年會（HITCON, Hacks In Taiwan Conference），性質類似各國舉辦的資安研討會。在這個會議中集結了臺灣最有名、最厲害的駭客與資安研究人員，一起分享與探討最新的資安議題、網路漏洞和駭客攻擊事件。參加者除了駭客，更有國防部、國安局、調查局等政府單位的人，甚至有來自不同國家的與會者共同分享經驗；而微軟總部MSRC更長期贊助並派人參與，就可知道全世界無論是公部門或私人企業對資安都非常重視。

「駭客年會」把臺灣的資安漏洞攤在陽光下討論，就是希望能經由公開透明的論述，找到更好的資訊防護措施。承如上述可知，國防部與政府相關單位也開始借重駭客們的力量，積極設法為國人建立一套免受攻擊的防護網。但僅依賴政府的力量是很難將資訊安全做到滴水不漏，因此筆者以為資訊安全最關鍵的因素在於每位網路的使用者是否具有一定的「資安意識」，也就是在享用網路便利性的同時，要能同時意識到資訊安全的重要性。如果每個人在使用電腦時都存有這種危機意識，那麼在資訊安全的防護上必能產生很大的助益。

在數位的世界裡，每天都有很多看不見的資訊戰爭正無聲而激烈地進行著，特別是中國大陸積極培育的「網軍」，儼然成為全球網路安全的最大威脅。如何攻防抵禦、防患未然，進而待勢出擊，相信會是臺灣當前最重要的資安課題。

▲Top