防止個資外洩，從源頭做起

Openfind PM Team

新版個資法已於今年 10 月 1 日正式上路，各機關與組織面對法規遵循及捍衛企業商譽的雙重壓力，無不嚴陣以待。根據最新統計報告指出，目前平均每台電腦擁有超過 14 萬筆個資，加上近來國內個資外洩事件層出不窮，其中有幾個案例更是透過電子郵件而將個資流洩出去，例如曾被判賠罰緩的某知名網路書店，就因為員工在處理會員註冊資料、發送註冊通知信的同時，一時疏忽，不小心將「會員資料名冊」夾帶於信件附加檔案一同寄出，這份名冊內包含了 400 多位會員的註冊資料，會員的帳號、姓名、地址、電話、手機、電子信箱等資料因此外流，造成會員個人權益相當嚴重的影響，若這些資料遭到不法人士利用，冒用他人身分從事簽約、買賣，甚至是詐騙等犯罪行為，所造成的損害更是難以估計。

美國 1974 年開始施行的「The Privacy Act」、英國 1998 年開始施行的「Data Protection Act」、日本 2005 年施行的「個人情報保護法」到台灣 2012 年 10 月 1 日正式施行上路的新版「個人資料保護法」，都是在倡導個人資料隱私的重要性。台灣新版個資法規定，企業必須善盡資料保護與舉證的責任，若是企業違反個資法規定，導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，企業需要負損害賠償之責任。並且，民眾可以要求民事損害賠償，民事賠償的金額每人每一事件可以要求 500 到 2 萬元不等，罰鍰總金額最高達 2 億元。並且新法也導入了團體訴訟的機制，單一案件當事人二十人以上即可以書面授與訴訟實施權者，提起團體訴訟。

因此，以台灣發布的新版個資法規範來粗估算，上述所發生的某知名網路書店案例，企業可能會因為單一員工的疏忽，而承擔民事損害賠償總金額高達 8 百到 9 百萬之多。

無所不在的隱藏風險

隨著個資法正式頒布施行，從金融業、電子商務業到政府單位無不上緊發條、戒慎應戰，而超過九成企業用來做為主要對外溝通橋樑的電子郵件系統，自然成為有心人士意圖竊取資料的目標。許多重視內部系統的安全性的企業，為此添購了很多防毒防駭的網路閘道、防火牆等設備，期望透過硬體設備來阻擋外部攻擊或內部資料外洩，但是，這些機敏資料的外洩，常常不是透過技巧高超的駭客行為所造成的，反而是內部員工對外發送電子郵件時洩漏的，加上日益頻繁的行動商務，資訊處理平台已從傳統電腦轉移到智慧型手機或平板，智慧型裝置上的偵測也是要被重視的趨勢。儘管企業可能要求每位員工，小心謹慎地處理每一道作業流程，這樣的人為疏漏仍然防不勝防，不可能完全避免疏失。然而，針對電子郵件防範外洩的機制並不多，能真正達到偵測效果的更少，要讓電子郵件系統同時要肩負個資檢測的角色，在評估時必須注意以下重點：

從源頭阻擋，防止個資外洩

現行的電子郵件系統，皆沒有可以保護郵件個人資料的機制，為了避免企業與外部溝通的過程中，造成個人資料外洩的情況發生，一定要從源頭阻擋做起，無論是從電腦瀏覽器，或是智慧型裝置專用操作介面寄送信件，都要能偵測郵件內文是否個資，檢核可疑的附加檔案或內容，保護企業所寄出的每一封信，遠離個資外洩的風險。

根據不同的組織政策，設定不同程度的風險以及對應的等級控管，管理者只需要透過幾個簡單步驟設定，便可以輕鬆的協助使用者，判斷即將寄出的郵件標題、內文或是附加檔案內，是否包含機敏個資，由系統主動提醒或是禁止寄送，並提示所包含的個資數量，避免可能造成的風險與危害。

【管理者設定畫面】

【使用者寄信偵測畫面】

從大處著眼，提防大量收件人資訊外洩

除了擔心個資經由附檔或內文洩漏外，收件人資訊也是可能洩漏隱私的一個脆弱環節，身為單位溝通的重要窗口，常常需傳送資料給協力廠商或是不同的部門單位。若一時不察，將大量的收件者加入寄送郵件的收件人欄位，意外將資料寄送給無關聯的收件人，或因隱私觀念不足，未將收件人保密以密件副本寄送，而不經意地透漏信件收件人資訊，包含大量姓名和電子郵件信箱，就已經構成個資外洩的條件，若是郵件再被轉寄，那麼取得資訊者將會無以計數，嚴重者可能引發團體訴訟，造成難以預估的個資外洩賠償。

為了避免這種情況的發生，「大量收件人偵測」的機制也變得相當重要，由電腦到智慧型裝置，都要能完善地協助管理者滴水不露預防大量收件人資訊外洩，同時也要考量到組織內外不同政策規範，針對不同信件流向也要能設定不同規則，當使用者在發送信件時，系統可以主動偵測是否包含大量收件人，依據規範禁止寄送，或提示使用者是否將大量的收件者轉換為密件副本（Bcc）後寄出，減低因人為疏失所帶來的訴訟紛爭。

【管理者設定畫面】

從小處著手，避免釣魚陷阱

上述提到兩種常見的個資外洩管道與防範方式，這邊我們在提出一個一般企業較少注意到管道--「公告信件」，由於員工長久以來信任管理者所發送的信件是安全無虞的，攻擊者很可能就會利用這樣人性的弱點，仿冒公告信件來釣魚，突破多重防護設備長驅直入。為預防企業員工郵件遭仿冒，開始有電子郵件系統提供具有特殊識別圖示的公告信件，協助使用者有效區別公告郵件和一般郵件，不僅能達到重要通知不漏接，也可以讓使用者免於惡意釣魚信的迫害，透過這樣特殊的公告信標記，可以更清楚識別寄件來源，對管理者和使用者都是保障。

坐而言不如起而行，現在就開始防範

在這麼多偵測及提醒下，相信管理者已有一套方法可以避免使用者洩漏個資，以免連帶受到個資法規範罰緩，但若管理者只聽聞雷聲而不實踐防範，被動地等待與觀望同業動作，很可能讓組織環境疏於防備，讓個資輕鬆暴露在外。Mail2000 除了提供安全及穩固的郵件系統外，也貼心的站在使用者的角度，主動的提醒或是阻止個資外洩的形況發生。我們將會不斷的精進，推出新功能為使用者把關，致力於捍衛企業郵件安全而努力。