法律規範與郵件稽核

叡揚資訊 系統工程師 陳銘峰

郵件資料外洩

隨著資訊和網路科技的進步，使用電腦處理個人資料之情況日益增加，不管是政府行政機關與民間工商企業亦是使用電腦與網際網路來收集、處理大量個人資料，外加上電子郵件應用普及，使得電子郵件已成為現今企業廣泛用於溝通、寄送檔案及發佈資訊最常見的工具，其主要的原因在於郵件傳遞相關協定制定之初的概念就是簡單方便，因此電子郵件在附加檔案上並沒有什麼特殊限制，就像是個 Box 容器，任何東西都可以放進去。然而也因為這樣方便的特性，讓使用者在不經意的情況下，就輕易的將個人或機密資料，透過電子郵件一下子送出而不自知，所以說資料外洩最主要的管道是電子郵件一點也不為過。

近年來詐騙案件層出不窮，手法亦不斷翻新，輕則擾民作息，中則損失金錢財產，重則威脅生命安全。想必大家都會有所疑惑，為何詐騙集團會對其個人家庭狀況能瞭若指掌，詐騙集團是如何得知這些個人資料呢？除了詐騙案件外，資料外洩事件也是不斷再發生，一旦個人資料透過詐騙行為，轉變成一種有價值的物品，即可預期會有惡意人士，將藉由各種管道企圖取得這些資料，再利用它從事違法的犯罪行為。有鑑於詐騙集團日益猖獗，集體個資遭外洩事件層出不窮，個人資料氾濫的問題是越來越顯見。

法規規範不足與改善

台灣於 1995 年 8 月所訂定公布的「電腦處理個人資料保護法」(註 1)，保護的範圍僅限於公務機關和徵信業、醫院、學校、電信業、金融業、證卷業、保險業及大眾傳播業等「八大行業」，一般行業及個人均不受規範，保護之客體亦只限於經電腦處理之個人資料，不包括非經電腦處理之個人資料，對於保護個人資料隱私權議之規範顯有不足，而且屬於「告訴乃論」，因此近年來屢屢發生重大的個人資料大量外洩事件，卻未見應負責任的機構依照個資法的規定負起各種法律責任，究其原因，主要是因為社會上對於個資法的規定並沒有普遍的認識，並且缺乏外部的監督機制，另外也因為科技進步，現行法律有諸多不合時宜之處，包括應受保護個人資料的種類狹隘、損害賠償機制的不便、監理機制的欠缺等等，所以並沒有真正保障所有受害民眾的權益。

針對法規規範不足部分，法務部於 2001 年擬定修法計畫，積極推動研修個資法工作，終於提出「電腦處理個人資料保護法修正草案初稿條文」(註 2)，修法內容重點包括擴大保護客體、普遍適用主體、增修行為規範、強化行政監督、促進民眾參與、妥適調整罰責、配合增修條文，現行法之諸多缺失與漏洞均已作適度

之改進。將電腦處理個人資料保護法擴大範圍到各種形式的個人資料，亦將非公務機關擴大適用主體，讓各行各業皆可納入規範。

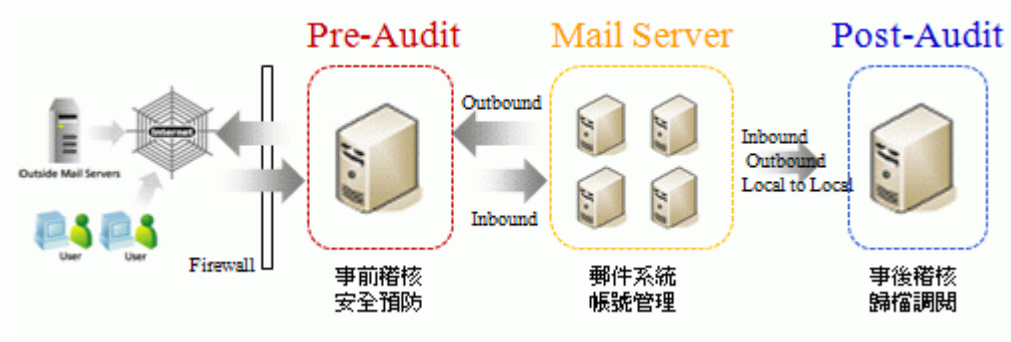
經過漫長的時間，「個人資料保護法」(註 3)終於在 2010 年初，快速地通過二讀、三讀，並於 2010/05/26 由總統公布。個人資料保護法不但將個人資料保護的責任歸屬範圍擴大，同時也賦予消費者可以向洩露個人資料的企業，提起團體訴訟及損害賠償。對於企業來說，即使是遭遇到駭客入侵而資料外漏，也必須擔負起責任。

前述提及電子郵件為資料外洩最主要的管道，而今法規也已訂定，如何做到遵循法，並且防範郵件資料外洩問題，「工欲善其事，必先利其器」，我們需要的一套的郵件稽核系統來協助我們做好防範。

郵件稽核系統架構建議

稽核的主要目的是確保所有運作按造既定安全政策執行，同時也能夠確認所有存取資料皆獲得授權，資料並經適當處理及其正確性。安全稽核可依時間點區分為事前稽核（Pre-Audit）與事後稽核（Post-Audit），主要規範內容如下：

事前稽核：即時資料的稽核，確保內部資料安全性與正確性。
事後稽核：歷史資料的稽核，發覺或追查可疑的事件及人員。
而在郵件安全架構設計上，完整郵件稽核也要能夠符合事前與事後稽核的規範。系統建議架構圖如下：



【郵件稽核系統架構圖】

兩者間的差異在於，事前稽核（Pre-Audit）是做好事前預防，就可以確保一定程度上的安全；事後稽核（Post-Audit）則是先訂好規範準則，事後告訴你稽查結果，再要求改善。若是採用閘道方式（Gateway）進行郵件的過濾與攔截封包的事前稽核方式，此作法未能兼顧到內對內的信件稽核，難免會發生系統誤判或漏信問題。相對的，僅做事後稽核，缺少事前的預防，當發生問題時，損失已造成。因此，建議除完成事前稽核工作，也能納入事後稽核的機制，完整郵件稽核與歸

檔管理，才能確保郵件安全百密不漏。

郵件安全稽核可保護資訊不受各種威脅，確保持續營運，將可能的風險損失降到最低。郵件對企業組織而言就是一種資產，和其它重要的營運資產一樣有價值，因此需要持續給予妥善保護。只要事先做好郵件稽核妥善規劃，未來將可以順利建構完整的機制，相信在此機制建立完成之後，對企業整體的營運效率及資訊安全的提升，會有一定程度的幫助。

註 1:電腦處理個人資料保護法：http://law.moj.gov.tw/LawClass/LawContent.aspx?pcode=I0050031

註 2: 電腦處理個人資料保護法修正草案：http://thinktank.nat.gov.tw/ct.asp?xItem=465&ctNode=78&mp=1

註 3:個人資料保護法：http://law.moj.gov.tw/LawClass/LawContent.aspx?Pcode=I0050021