個人資料要盤點時，究竟要如何盤點才算正確且不會造成遺漏？

個人資料保護實務與稽核準備(上)

◎黃小玲

壹、前言

小王跟隔壁小張抱怨：又要開始個人資料盤點了。小張：怎麼說「又要」？小王：上次不是才說請各部門對所擁有之個資進行盤點嗎？現在高層又請了號稱經驗豐富的專業顧問設計個資盤點表格，所以又得重來一次。小張：那你預估我們個人資料盤點到底要做幾遍才能算完成？小王：我猜應該是直到高層知道如何做下一步時才會完成吧！先別聊天，你幫我看看這兒有一筆個人資料是紀錄小明曾經感染B型肝炎而請病假休養的紀錄，是應該歸屬到「病歷」還是「醫療」這一欄？小張驚呼：這麼多欄位都要填哦！而且醫療列為特種資料，病歷是一般個資，那差別在那呢？小王：…

以上小故事，反映現在個資擁有者或管理者的問題，當大家都知道個人資料要盤點時，究竟要如何盤點才算正確且不會造成遺漏？是對照到個人資料保護法的個人資料定義一一盤點勾選，或是只分一般與特種資料即可？

第二個問題則是完成個資盤點後，下一步呢？按部就班，了解且依據法令或主管機關要求，可以是在施行細則公告之前的解決方案。

本文將從分析個人資料保護法的要求、個資管理實務及後續維護時之稽核要點，提供組織日後維護管理或稽核時參考。

貳、個資稽核計畫準備

個人資料保護法不論是針對公務機關或非公務機關，都有類似的一條規定：…應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏。[2]

所謂適當之安全措施，應從組織所擁有之個人資料屬性進行評估，包括個人資料之特性（一般與特種資料）、個人資料敏感程度及擁有之個人資料數量。特種個資在一般情況下，是不得蒐集、處理及利用，當然有少數情況是例外的；而擁有之個人資料數量則是考量日後若真有個資事件發生時，所涉及之損害賠償及訴訟等問題。

依據英國個人資訊保護標準（Data protection：Specification for a personal information management system）[1]中提到個人資料的稽核應排定稽核週期，以俾（１）檢視個人資料保護制度是否跟既定政策或程序相符；（２）建置與維護上是否符合技術要求。從以上可以知道稽核要求應兼顧流程與技術。以下將從管理流程與技術方案角度，分別概述個人資料保護實務與進行後續稽核時應有之準備。

參、管理流程稽核

個人資料之主要活動包括：蒐集、處理、利用及國際傳輸[2]，而僅是處理活動就涵蓋資料之記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送。管理流程稽核之規劃重點，建議可從主要個資管理流程中，參考BS 10012個人資料管理標準，依管理稽核流程之文件藍圖，詳見圖１，以規劃或執行個人資料管理機制之系列稽核。接續將整理關鍵管理流程主題，並分述稽核要點。

資料來源：本文自行整理 / 圖 1: 管理稽核流程之文件藍圖

一、政策與保護要點

為使組織有既定之個人資料保護策略與方向，首要工作為訂定及公布組織之個人資料保護政策與要點，清楚定義組織內部一致之保護政策，同時提供個資當事人了解自身之相關權利與義務。稽核要點如下：

（一）個人資料之蒐集、處理或利用，是否有法源依據或符合特定目的？

（二）是否訂定個人資料保護政策及管理要點？此政策應涵蓋與適用之範圍及對於個人資料保護之管理方向。

（三）是否準備個人資料提供同意書以請求當事人之意向？同意書應載明個資當事人所有法律賦予之權利及組織保密之責任等等。

二、角色與管理責任

公務機關保有個人資料檔案者，應指定專人辦理安全維護事項…[2]；國外盛行之隱私長角色，可供國內組織參考，同時再由隱私長發展個資保護組織架構。在角色與管理責任可能出現的爭議點是：個人資料保護應由資訊人員主責或其他專責人員負責？會出現這個議題也是因為現行個人資料大多透過電腦記錄、儲存及傳送，建議組織可依業務特性，分析及決定個資管理角色與責任。稽核要點如下：

（一）個資保護組織架構是否包括管理階層人員？檢視個人資料管理由上至下（Top down）的管理方式。

（二）是否提供合宜之聯絡方式予個資當事人？以利個資當事人行使其權利。

（三）個資保護組織架構之人員是否清楚應盡之權責事項？測試相關人員對個人資料之認識與管理能力。

（四）是否建立個人資料防護之教育訓練程序？藉由檢視訓練內容及紀錄確認人員之認知與技能，了解組織內所有人是否皆完成基本之認知課程。另外針對個人資料管理，組織應特別再提供進階訓練。

三、通知與應變程序

對組織而言，最讓人擔心害怕的事，恐怕是個資事件發生時，通報者是外部人員或是受害者直接告知。組織違反個人資料保護法時，應在查明個資事件後，以適當方式通知當事人。[2]稽核要點如下：

（一）是否建立個人資料審視管理程序，定期檢視違反個資保護之徵兆與可能之趨勢？

（二）檢視通知與應變程序是否排定測試計畫，並確認其可行性。

（三）個資事件發生後，是否視應變需要重新調整管理計畫？同時得確認後續管理計畫之有效性。

（四）是否留存所有通知與應變程序之紀錄，做為日後分析與處理經驗分享使用？

四、委外管理

受公務機關或非公務機關委託蒐集、處理或利用個人資料者，於本法適用範圍內，視同委託機關。[2]第４條。委外管理之所以重要，是因為不論公務機關或非公務機關個人資料蒐集、處理及利用等程序委外皆有相當高的機會與比例，委外管理不可不慎。稽核要點如下：

（一）是否於合約中載明應遵循組織之個人資料保護管理原則？

（二）是否具備對個資事項之稽核權？確認組織是否派員執行稽核、稽核頻率及稽核紀錄等。確認委託機關之防護要求等級應與組織相同，以確保風險發生之可能性。

（三）委外機關管理受委託之個人資料是否與組織之管理等級相同？

五、其他管理稽核事項

（一）檢視當事人行使個人資料保護法所賦予之權利時，組織回應之程序與方法，可確認組織能否於限定期間內回覆？依[2]第13條規定，得依當事人不同之請求權利於15日或30日內完成准駁之決定。能否設計妥適回應流程，且即時回覆個資當事人，應列為稽核要點之一。

（二）可攜式媒體是否訂定個人資料儲存、傳送之管理程序？隨身碟、平版式電腦及智慧型手機之盛行，相對地也提高資安事件之風險程度；若這些裝置未納入資料保護與控管的範圍，則未來可能成為風險發生之最大來源。

（三）是否訂定銷毀程序，包括紙本資料及電子檔案等不同之處置程序？確定銷毀過程皆留下紀錄，並可被再次顯現？

（四）是否定期進行管理階層審查，以確認個人資料保護政策之合宜性、個資事件趨勢及處理之有效性，甚至是因為內在或外在環境的改變而需要調整的管理程序？

（五）個人資料是否有國際傳輸行為？除考量是否符合本國法律外，亦應考量雙方管理程序與交換技術之操作安全？

個人資料保護需兼顧管理與技術兩方面，以周全個資之防護機制。下期文章將從個人資料保護法要求之「安全維護事項」，分析如何從技術觀點進行稽核準備。

肆、參考文獻

[1] BS 10012:2009
[2] 個人資料保護法

▲Top

請神容易送神難，是每個公司管理者最怕遇到的問題。

從人力資源管理角度談資訊安全如何維護

◎魯明德、魯晏汝

壹、前言

近日新聞報導，有一位華裔工程師，因任職期間被指控濫用員工折扣購買商品，並轉售圖利而被解僱，於是基於報復及炫耀技能的心態，開始入侵前公司的電腦，不僅刪除多個伺服器，並關閉一個內部系統，同時刪掉大多數的檔案及E-Mail信箱；此舉不僅讓該公司員工無法登入，更影響所有的分店及電子商務部門。據了解，該員是利用受僱期間職務之便，用虛假的員工資料設立帳號，以方便自己登入公司系統。被解僱後更多次以該帳號入侵公司的網站進行破壞，造成公司嚴重的損失。

除了上述案例外，離職員工可能帶來的問題也包括帶走公司的營業秘密或客戶資料、離職後惡意中傷前公司或主管等。為避免類似狀況的發生，我們可以從員工在職的管理及離職的管理兩部分進行探討。

貳、員工在職期間的管理

在平日例行的工作中，其實潛藏著許多可能危及公司的危機。例如：業務人員在日常工作中因職務之需，有時會將客戶資料攜出；行銷人員及研發人員因工作的連續性和時效性，而將工作帶回家繼續完成。這些當下看似不怎麼樣的行為，在未來的某一天也許就可能侵害到公司的權益。有鑑於此，身為公司的管理者，可從下面幾個方向著手進行規範：

一、禁止攜帶私人的電腦進入公司，或是在公司使用私人的電腦：有些公司並未禁止員工在工作時間使用私人的電腦，甚至公司一開始用人時，為了節省成本，不發放電腦給新進人員，請他們使用自己的Notebook。眼前看來的確可為公司節省一筆開銷，但長遠來說，員工等於隨時可將公司的機密文件（系統開發程式、客戶及訂單資料等等）存放在個人電腦中攜出，離職時也無法管控員工到底帶走了多少公司內部資料。所以員工新進時配置一台電腦，並且禁止員工攜帶私人的電腦進出公司，絕對有其必要性。

二、禁止使用外部存取裝置：相較於厚重的紙本資料，使用輕巧的外部存取裝置將資料攜出公司是很容易的事，所以平時就應規範外部存取裝置的使用，以避免員工隨意將重要文件攜出。

三、重要或機密文件禁止列印及另存複本檔案。

除以上規範外，公司更應定期檢核各單位人員的作業流程。以上述案子為例，當有新人報到時，人資單位理應通知各相關部門建立資料。稽核單位也可以定期依人資單位所提供的在職名單去檢核系統裡的帳號，是否有離職未關閉的，或是存在虛假的帳號，以避免員工離職後還可以隨意入侵公司的系統。

參、員工離職的管理

員工離職的原因有很多，例如：工作壓力太大、待遇不理想、沒有發展性、不滿人際關係、遭到解僱等等。離職原因雖有千百種，但不論是哪種理由都有侵害公司權益的可能，所以當員工提離職時，身為公司的管理者或是該員工的直屬主管，除了要煩惱工作該如何交接、要不要找新人進來之外，了解員工離職的原因更是件重要的事。

此時可以透過離職面談的方式跟員工一對一地進行面談，大部分要離職的人，會比較願意說出真心話，或許有些人不會毫無保留地說出離職的原因，但經由同理心的談話，或許較能旁敲側擊地問出離職的原因。此外，如果離職原因是由於對公司的政策或管理方針不滿時，也可以藉此提出修正，以降低其他員工的離職率。離職面談除可探究離職的原因外，也可在此過程中提醒離職員工須將公司的資料完全交接，不可私自夾帶出去，尤其是研發或管理級人員，更不可將公司的營業秘密帶至新公司，以免觸及競業禁止的規定。

一般管理嚴謹的公司，人資單位會在員工離職當天，通知各系統相關負責人把該員工所有帳號、網域及門禁設定都關閉，以免發生像案例一樣的狀況。有些公司竟在員工離職兩三個月後，仍未將其相關的設定關閉，以致離職員工依然可以用原帳號密碼登入並使用系統。這種管理上的漏洞很容易讓心懷不軌的員工有機可乘，這點在離職員工的管理上不得不注意！

肆、結論

「請神容易送神難」是每個公司管理者最怕遇到的問題，為避免發生這樣的問題，除了在一開始招募新人時就要做好謹慎評估外，在員工平日管理上更應落實做好各項資訊安全的防範措施，以避免真的發生問題時，造成公司無法彌補的損失。

（作者任職於特力股份有限公司、華創車電技術中心股份有限公司）

▲Top