機密維護常識彙編（102 年 11 月份）

＊離職員工的保密責任

「山中傳奇」是一家貿易公司，因能掌握關鍵客戶，所以在高科技產業的市占率很高。但該公司最近發現業績嚴重衰退，經公司內部調查發現，原來是去年底由於業務人員的離職，致使隔年客戶流失很多；再經派員訪查，發現那些流失的客戶，都轉移到去年離職那位業務員所任職的公司。

小潘看到這則報導後，心想這個現象顯然是那位離職員工把客戶資料攜出，進而讓這些客戶到自己新任職的公司。然而，員工離職是企業常態，要如何確保員工的流動，不會造成公司機密資料的外洩呢？

趁著下午茶的約會，小潘把這個問題提出來，司馬特老師喝口咖啡，把問題分成２個部分來說明。員工離職把機密資料帶走，是不容易防範的；但是，企業不能因為不易防範而不作為，任由洩密事件造成公司的危機。業務員在離職時所攜出的客戶資料，可分為自然人的資料及法人的資料，自然人的資料洩漏，除涉及個人資料保護的問題外，由於這是公司營運上的資訊，不是一般人可輕易獲得，因此，也有侵害營業秘密的問題；法人的資料遭洩漏，則是侵害營業秘密的行為，該行為在營業秘密法修法後，已有刑責，不可不慎！

自然人的資料外洩涉及個人資料保護的問題，容易理解，但自然人的資料也是營業秘密，小潘就感到迷惑了。司馬特老師接著從法律面加以說明，指出營業秘密所保護的標的，係指方法、技術、製程、配方、程式、設計，或其他可用於生產、銷售或經營之資訊；客戶的個人資料，顯然屬於可用於銷售或經營之資訊，如果這個資訊符合：非一般涉及該類資訊之人所知、因其秘密性而具有實際或潛在之經濟價值，以及已採取合理之保密措施等要件，就成了營業秘密法所保護的對象。

小潘聽完後恍然大悟，但他又想到：如果客戶的資料，是該業務員所開發來的，這個資料業務員為何不能帶走到新公司運用？司馬特老師喝口咖啡，問了個問題：公司業務員的工作是什麼？小潘心想老師問這問題實在太簡單了，業務員的工作當然是找到客戶、銷售產品。

司馬特老師聽了點點頭，開發客戶、銷售產品所得到的資訊，顯然是可用於銷售的資訊，即係營業秘密保護的標的，而受僱人於職務上研究或開發之營業秘密，依營業秘密法規定，是歸僱用人所有；因此，業務人員開發來的客戶資料，當然是公司的財產。

小潘聽完司馬特老師的分析，對於銷售資料洩漏的問題，已有初步認識。接著又問老師，企業有什麼方法可以防止這類機密資料的外洩？司馬特老師把問題分成 3 個部分繼續說明。

第一、在人員到職時，人力資源部門應該跟員工簽訂一份保密合約，合約中除了明確定義公司的營業秘密範圍外，也要把保密責任與違約罰則條列在合約中，要求員工除在任職期間要遵守外，離職後亦需負擔保密責任。

第二、企業的管理部門，應該要對機密資料的產生、保管、借閱等，訂定相關作業規定，並定期清點，以免遺失。對於屬於營業秘密的資料，除了要律定標示符號，要求保管人員確實標示外，保管的地方也要特別規劃，有一定的門禁管制措施，以防閒雜人等接觸。另外，現今企業許多機密資料都是數位資訊，自然不能忽略數位資訊安全，所以企業的資訊部門在規劃網路安全時，除要防止外部駭客入侵外，也要管制內部人員的使用，避免機密資料經由內部管道外洩。

第三、離職面談一向被大家忽視，卻是資訊安全重要的防線。當人員離職時，人力資源部門一定要做好離職面談，除了要求離職員工遵守到職時所簽訂的保密合約外，也要提醒不得把本公司的客戶資料運用到新公司。如有可能，最好列出客戶清單，以免對簿公堂時各說各話。

小潘聽完司馬特老師一席話，發現不只資訊安全涉及的層面廣泛，連客戶資料都是企業的營業秘密。離職員工的洩密不是不能防止，只要妥善利用法律規範搭配管理措施，即能防患於未然！（作者為科技大學資訊管理系講師/魯明德）

＊資訊安全的四項提「防」

隨著電腦應用的普及和網際網路的急遽發展，不僅改變了人類的生活模式，也帶來令人憂慮的資訊安全問題。因此，建立完善的資訊安全防護措施已是當務之急，唯有在安全無慮的前提下享用網路資訊帶來的便利，才是面對科技發展的正確態度。

資訊安全的種類可分為三個面向：一、硬體的安全，包含對於硬體環境的掌握以及設備管理；二、軟體的安全，包含資料軟體安全和通訊管道的安全性；三、個資的安全，包含個人資料保密，隱私性等。

如何做到上述資訊安全的保護措施呢？首先我們要了解影響資訊安全的因素，包括：未經授權侵入使用者帳戶，進行竊取或是更動系統設定；資料在傳輸過程中被擷取，或被變更內容；透過感染電腦病毒與傳播惡意程式。諸如此類的資訊安全問題層出不窮，且手法日新月異，然而注意下面幾點防護措施，可在面對大部分的狀況時，具備基礎的防護手段。

一、防毒：當一隻病毒被製造出來之後，開始於電腦與網路設備中擴散，透過網絡無遠弗屆的傳遞，變成所有電腦使用者的夢魘，隨之而來的系統崩潰甚至硬體損壞，將損毀寶貴的資料。使用者防治的積極手段就是安裝來源合法的防毒軟體，並且定時更新病毒碼，以保持作業系統處於健全的防護程度。

二、防駭：隨著社群網絡和各式資訊系統的應用，駭客由開始時半開玩笑地更動系統設定，演變到後來的蓄意破壞、資料竊取，也因此發展出了各式的系統安全通行證，包含使用者密碼、身分驗證、通訊鎖、晶片卡等設置，普遍使用於各層面。除了定期變更驗證方式以及使用多種防護作為外，也需隨時保持資安的警覺性。

三、防治天災：這是容易忽略的一個項目，電腦硬體從來就屬於耗損型的設備，隨著時間、溫度、濕度、跳電等，甚至震動都可能導致硬體的受損；因此使用者應該以嚴肅的態度準備更完整的防治計畫，例如定期更新易耗損的硬體設備，備份重要資料，以及安裝備用電源，預防斷電造成的資料損失等。

四、資料防竊：隨著智慧型手機的流行，現在低頭族已成為一種社會現象。而資訊的氾濫成為眾多使用者頭痛的問題，許多不同的應用程式都會記錄使用者的個人資

訊，但設計這些應用程式的公司是否確實做好保護我們的個人資料？值得存疑！許多應用程式的分享與協同編輯功能權限設置不明，更是成為資料安全上的一大隱憂。因此，我們對於自身的資料處理應該抱著更謹慎的態度，切勿在網路上分享或是儲放機密資料。

我們若能認真地思考資安問題，完善規劃這些資訊系統與網路設備，定期保養與維護個人資安，便可長保資料的可用性及可靠性了。（本資料摘自於清流月刊/蔣衡）

＊莫讓網路成為洩密的公路

近期紐約時報大篇幅報導，美國網路安全公司 Mandiant 的最新研究指出，近年對美國公司、機構和政府單位大規模的網路攻擊行動，極可能源自中共位於上海的 61398 部隊。消息傳出後，中共方面當然拒不承認，並公開表示自己才是網路駭客活動中最大的受害者，其反應雖早在各國意料之內，但也對中共的圖謀有更深一層的認識。網路攻擊每次造成的損害皆視種類及規模而定，較嚴重時往往不下於一次傳統戰爭失利所帶來的損失，這鍵盤上廝殺的代價甚至非金錢所能衡量。在中共官方的扶植下，軍方與民間的駭客活動日益頻繁，且越發老練兇狠，並擅長以惡意程式或破解安全機制等方式，針對他國企業、科技、軍事、政治與經濟等重要資訊進行破壞或竊取，中共駭客甚至常利用臺灣及其他國家的伺服器作為中繼站執行所謂的「跳島戰術」，使受害者難以追蹤來源。所謂道高一尺、魔高一丈，即令美國作為網路的先驅亦是防不勝防，數十億美元及長期的研發結晶瞬間為他人所用，國際間亦合理懷疑中共近年來各項科技的突飛猛進多半是源於此道。

由於損害非同小可，美國政府除積極進行各項防堵作為外，更針對駭客入侵時所留下的網路足跡進行追查，如登入時慣用的英文拼音方式、獨特的簡體輸入法，以及駭客個人使用的社群網站 Facebook 和 Twitter 等，才得以反推追查真正的元兇就是中共。我們亦可以藉此了解一件事，亦即精明如駭客都因忽略資訊安全而洩漏行蹤，可見我們平日在使用網路時又豈能不謹慎小心，尤其在資訊媒體裝置不斷微型化、普及化及功能多元化的今天，各種資訊傳遞快速且便捷，在 Facebook 等社群網站或部落格內公開暢談生活瑣事已是現代人的家常便飯，但往往就在談天說地中洩密而不自

覺。例如最近就有網路部落客貼出一則文章，內容係針對國軍飛彈指揮車偽裝成物流車輛的創意及技巧表示稱讚，接著更有其他網友回文，聲稱在何地、何時看過此等裝備，甚至有人連單位全銜也一併寫上。這些軍事迷看似交換心得的文章，無疑幫敵人情蒐單位一個大忙，有心者只要付網路費用再敲敲鍵盤就可以蒐集到我方的軍事部署與動態。然而，洩漏的軍情卻會對國家造成難以估算的傷害。在平時，部隊就必須要另行調整部署或計畫，額外花費大量的人力物力來彌補；在戰時，國軍可能就要付出十倍百倍的代價及犧牲，卻因為那無知的隻字片語。

近幾年在馬總統的領導下，兩岸情勢雖趨於和緩，有部分國人亦因此鬆懈應有的保密警覺，其實只要多留心相關訊息，就會發現中共的各種情蒐與滲透仍是暗潮洶湧，不曾停歇；其中又屬網路攻擊最難防範。因此，凡我國民均需培養一個觀念，在網路上留下的各種訊息無遠弗屆，在電腦中存放的公務資料，只要連上網際網路，駭客就可以利用各種意想不到的方式對其進行存取，再藉由各種零碎的資訊，拼湊出「點」、「線」乃至於「面」的情報全貌；例如最近某大陸網民就利用 Google 衛星空照圖，標定了大量的臺灣防空部署位置並於網路發表，這些名稱與訊息都是藉由各種來源的資訊組合而成，姑且不論其可信度有多少，僅是圖上密密麻麻的陣地與裝備名稱已夠令人怵目驚心。希望能國人對於國防秘密能深切重視，明白「保密是國家安全的基礎」，切勿為了自己的一時大意而為國家帶來難以估計的危害，尤其國軍弟兄身為表率，更應恪遵「不公務家辦」與「不記述軍中事務於網路及個人電腦」等重要原則，牢記保密是國家的根本，唯有「樹根站得穩、才不怕樹梢颳颱風」。

（本資料摘自於清流月刊/陳韋志）