機密維護常識彙編（102 年 9 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）

＊殭屍網路與進階持續性滲透攻擊趨勢

資訊安全的發展歷程中，網路攻擊的手法目前已朝向組織化、精緻化發展，大規模的攻擊行為已不多見，取而代之的是經過精心設計的網路攻擊，其中利用各種惡意程式感染受害者為當下最常見的手法之一；而殭屍網路（Botnet）是目前最嚴重的資訊安全威脅之一；進階持續性滲透攻擊（APT, Advanced Persistent Threat）則為近來最熱門的資安議題。在針對性的攻擊行動中，常可見到透過殭屍網路進行資訊的竊取或是大規模的攻擊活動，當攻擊者選定攻擊的對象或目標後，將會採用多種不同的攻擊手法，針對特定目標進行長期且持續性的攻擊，不擇手段以達成攻擊的目的。許多受駭的電腦在不自覺的情況下，參與了駭客所發起的攻擊行動，而殭屍網路所使用的惡意程式，大多針對該目標被發掘的弱點進行客製化的開發；此「特殊」用途的惡意程式，在潛伏與感染的階段很難被發現，除非掌握其行為模式，否則也不容易由特徵比對的方式進行偵測，再加上惡意程式的變種速度快，系統一旦被感染，防毒軟體恐不易偵測與清除。

殭屍電腦為了能穿透防火牆等資訊安全設備的防禦，大多採用一些在防火牆上允許通過的協定與通訊埠，也改變了傳統的資訊安全防護機制。以往大多將內部的網路視為安全等級較高的區域，而外部的網路則是安全等級較低的區域，在存取的管制上，較高安全等級的區域預設就能夠連線到較低安全等級的區域，因此許多受到惡意程式感染的殭屍電腦，能夠自由地進出防火牆等資安設備，而不會受到阻擋，這也是造成殭屍網路大規模擴散與感染大量電腦主機的原因之一。目前殭屍網路經常使用的通訊協定，包括 http、ftp、tftp、irc 等，而這些通訊協定廣泛地使用在許多的應用程式上，因此當殭屍網路透過這些常見的通訊協定進行通訊時，網管單位或是遭到惡意程式感染的系統，往往很難察覺這些通訊行為的存在；尤其當殭屍網路仍在潛伏期，除了與中繼站或駭客的控制平台保持微量的通訊外，在傳統網路流量的統計方式上，並無法有效掌握這些微量的通訊行為。

殭屍網路與傳統電腦病毒、木馬程式或是網路蠕蟲最大的差別在於前者除了對我們的系統造成影響之外，也配合中繼站或是中央控制站角色，提供了殭屍網路更有效的管理方式，受害的殭屍電腦會主動與這些中繼站或中央控制站進行連線，並隨時等

待來自攻擊者所下達的指令，一旦接獲攻擊的指令，便能在最短的時間內依據指令的內容進行惡意攻擊，改變傳統攻擊者必須自行下達指令予分散各地的受駭主機模式，除了更有效率的管理外，也能在較短的時間內進行針對式的攻擊活動。

目前地下的經濟活動，大多配合殭屍網路進行相關的非法活動，例如：個人機敏資料的竊取，及網站帳號密碼、鍵盤或系統畫面的側錄等，或是參與殭屍網路所進行的惡意攻擊行為，這些都是造成資訊安全事件的主要原因。加上惡意程式的變形工具或是原始碼在網路上流傳，更造成惡意程式偵測上的困難。如今資訊匯流及數位經濟的發展，促使資訊安全應用遍及各個領域，而雲端應用技術及行動商務模式的興起，更讓資訊安全防護有更多的考量。在新環境、新技術的考驗下，行動及寬頻終端、網路、服務、應用平台、資料中心、犯罪調查、國家安全各領域，亦需面對功力高深的駭客攻擊、惡意程式植入等相關挑戰。

2012 年可稱得上是進階持續性滲透攻擊（APT）相當活躍的一年，多起資訊安全事件都與此種攻擊的手法有關。APT 不是一種新的攻擊，而是同時採用多種不同類型的攻擊手法，使用多種不同類型的攻擊方式以因應攻擊目標的環境。整個攻擊的流程可分為多個不同的階段，包括資料的收集與分析、系統與應用程式弱點的掃瞄、Rootkit 的使用、針對 Web Application 的安全弱點運用等。除了知名的 RSA、HBGary 等以資安設備或服務為主的公司皆遭到此類型的攻擊，後續衍生出其客戶的資安風險，或是由於所使用的資安設備或服務遭到破解造成的資訊安全事件，皆造成不小的影響；這類型的攻擊同樣發生在 Sony 的遊戲社群平台、花旗銀行、Google、VISA 信用卡國際組織等，這些針對特定目標與目的所進行的多起攻擊事件仍時有所聞。由此攻擊趨勢觀察，駭客的攻擊對象，除了由一般使用者的電腦竊取資料之外，也對重要且有指標性的目標逐漸感到興趣，且有長時間準備發動攻擊行為的規劃，透過社交工程、網路探勘與偵測等細緻的攻擊手法，針對特定的目標與目的，客製成為獨特的攻擊手法，以達到目的為最終的目標，未達成目的前決不輕言放棄；此類型的攻擊行為，往往長達數個月或一年以上。攻擊者經常使用或發送一些看似正常的網路服務或是文件，透過其中夾帶惡意程式發動零時差的攻擊，並針對尚未發布的系統或應用程式的弱點進

行攻擊。至於遭受攻擊的目標，往往受駭者並不會察覺，當殭屍網路與持續進階滲透的攻擊相互結合時，攻擊者能有效地運用龐大的殭屍網路做為幫手，針對該目標進行多類型的攻擊，並利用多種管道將惡意程式植入特定目標的系統中，以達成攻擊者的目的。

目前我們正處在一個不斷演變的網路環境，對於結合多種攻擊手法，運用殭屍網路進行資訊的蒐集或是攻擊的活動，每隔一段時間就有新的技術問世。而在資訊安全的趨勢分析上，往往會因不同的應用而有新的風險產生，因此隨時掌握資訊安全的發展趨勢以及相關攻擊手法的演變，為當下至為重要的課題。唯有掌握最新的資訊安全趨勢，了解常見的攻擊手法，並對本身系統或應用程式的保護，避免風險的發生以及曝露在不安全的環境中，才是提升本身安全性的不二法門。

（本資料摘自於清流月刊 / 蔡一郎）

＊雲端與資安交互的火花–雲端資安效應初探

雲端科技近年來已成為國際通訊及科技市場上重點發展的領域，包括 Google、Amazon、IBM、Microsoft 等大廠，甚至是各國政府組織，均積極投入大量資源發展相關技術與產業，未來人們就能以低成本、高效率的方式，快速連結到網際網路上處理資訊資料，進而根據個人或公司的需求，發展資訊服務平台並快速地部署在網路上供顧客使用。但是，到底什麼是「雲端」？又分享在雲端上的資訊是否能保護我們的隱私，讓我們在便利使用各項資訊應用的過程中，不至於擔心「雲」會讓我們個人或企業的重要資料曝露在不安全的環境中，而讓不法之徒有機可乘？這是目前許多人最想確認與了解的課題。

本篇文章首先期望從雲端架構進行探討，讓讀者了解雲端如何服務大眾，進一步從中點出資訊安全議題，並提出此類資訊問題該如何解決；最後希望給大家省思，當進步的科技帶來幸福的果實讓大眾享用時，相對而言大眾所能保有的隱私是否也逐漸降低？這兩者間是否有一平衡機制？身為個人該如何防範？

探討雲端架構之前勢必要解釋何謂「雲端」？基本上所謂的「雲端」，其實就是泛指「網路」，會稱為雲端是因為早期工程師繪製網路示意圖時，習慣用「雲」來代

表網路，因此雲端科技簡單而言，可說是網路科技之延續。坦白說，雲端科技並不是一項創新的科技，因為其概念及技術均來自於更早期的「分散式運算」（Distributed Computing）以及「網格運算」（Grid Computing）這兩種概念，但不同於此兩種運算技術，故雲端科技可簡稱為此兩者之整合應用與服務。原本此兩種技術受限於硬體及軟體，所能服務之對象均有限，但透過整合兩者的優勢與特長，雲端運算能讓更多人享受到分散式及網格運算技術的強大效益，同時，也伴生及結合出更多更新的應用概念與新興技術。

而雲端到底包含哪些架構？這些架構需要如何定義？這個問題最早是由 CSA（Cloud Security Alliance）在 2009 年發表的報告中，以服務的角度切入雲端並進一步區分為三大類，即 IaaS（Infrastructure as a Service）、PaaS（Platform as a Service）與 SaaS（Software as a Service）。從各類服務的內容與特質來看，三種服務分別針對基礎設施（硬體、網路連線）、系統平台（系統環境、開發工具）、應用系統（軟體、服務平台）作為雲端架構的檢視；並進一步從中針對雲端技術如何支援此三種服務進行討論。

隨著雲端科技越趨火熱，市場上相關的應用相繼出籠，單純從 CSA 提出的服務架構來看雲端發展，也變得有些不足。因此，許多專家學者紛紛提出自己的雲端應用架構。我們認為，應該將支援輔助的角色含括進來共同討論，才能算是完整的雲端服務架構。所以，架構的核心仍然是 CSA 的三層服務類型，而相關服務的提供者就稱為雲端內容服務商，協助設計、規劃與布建的提供者稱為稽核顧問商，尚包括其他周邊的支援性產品提供者。在稽核顧問商這部分，必須隨時關注各國相關政策與法令規章，這會影響到雲端服務商在服務架構上的設計要求；這部分也會連帶影響雲端應用系統與服務平台關於設計開發規範與營運管理的要求，進而影響後端其他支援性產品的開發與設計。

至於資訊安全在這一架構中，到底扮演何種角色？若從服務的角度切入，那麼資訊安全的需求勢必成為最被關注的問題。尤其在內容服務商這部分，對任何一個選擇雲端作為解決方案的個人或企業，資訊安全一定是其最為擔心的問題；畢竟，資料都

存在「雲」上，廠商怎麼保證其實體資料不會遭受駭客、敵對廠商之竊取與入侵？因此，雲端必須加重其資訊安全之重要性。至於如何規劃布建出一個符合需求的雲端資訊安全架構與環境，則是雲端與資訊安全廠商必須積極努力的課題。

現階段 ISO27001 針對資訊安全構面，已有詳盡的管理規範，從硬體、軟體，甚至接觸者，均有稽核時應注意的重點與要求。但這是否已足夠應付雲端服務可能遭遇的資訊安全問題？其實，整個雲端資訊的安全，必須從內容服務加以拓展出去，針對各種可能出現的資訊安全狀況進行分析，並進一步思考制定適當的法規；稽核顧問商也應重新思考如何加進法規，進行一系列雲端內容商的認證；同理，支援商也必須符合技術及法規規範，提出相對應之服務、軟體或設備。

概括而言，真正影響雲端發展之問題，並不是技術與服務項目的多寡，恐怕還是資訊安全上的保障與相關技術，是否足以讓使用者在享受方便之資訊服務的同時，能安心使用，達到「免於恐懼的自由」，這將是雲端與資安廠商最應注重的問題。

（本資料摘自於清流月刊 / 樊晉源）