淺析企業網路安全的潛在風險

企業營運由於具備開放結構的特性，在導入網路應用的同時，如何維護資訊設備與資料的安全性也備受考驗 (張玉龍等人，2006)。基本上，會對企業網路安全造成潛在風險的來源有「人」、「物」與「環境」三者，如下所述：

一、人的風險

主要來自於操作或管理上的錯誤與疏失，例如 PROXY 或 ROUTER 安全政策設定不當產生漏洞、密碼過於簡單使人容易猜測，或是 AD 管理者對人員權限控制不當。另外，就是惡意的攻擊行爲，這不僅僅指企業外部的駭客，還包括了內部員工所引起的攻擊，例如主動性攻擊如惡意中斷網路連線 (賴明豐與李駿翔，2007)，或是被動地在網路中實施訊框側聽或攔截的動作 (賴明豐與呂芬蘭，2007)。

二、物的風險

主要來自於軟體、TCP/IP 協定與網路規劃及設計上的缺陷 (張玉龍等人，2006)。對駭客來說，軟體的缺陷 (又叫做系統漏洞) 就像開了一扇可以隨時供人進出電腦的後門，攻擊者可以透過寄生在特定的埠上捕捉流通在企業網路中的訊框，或是直接刪除 SAM 文件取得系統使用權。而 TCP/IP 的缺陷則是肇因於連結建立的三次握手過程 (賴明豐與李駿翔，2007)。許多 TCP 攻擊方法就是抓住這種特性設計出來的，常見的手法包括 IP Spoofing、TCP session hijacking、RST/FIN DoS、Ping O’ Death，以及 ISN/SYN FLOODING。網路規劃與設計的缺陷，則包括用來連結電腦的網路設備不佳或是不當的拓樸結構 (topology structure) 造成的問題。

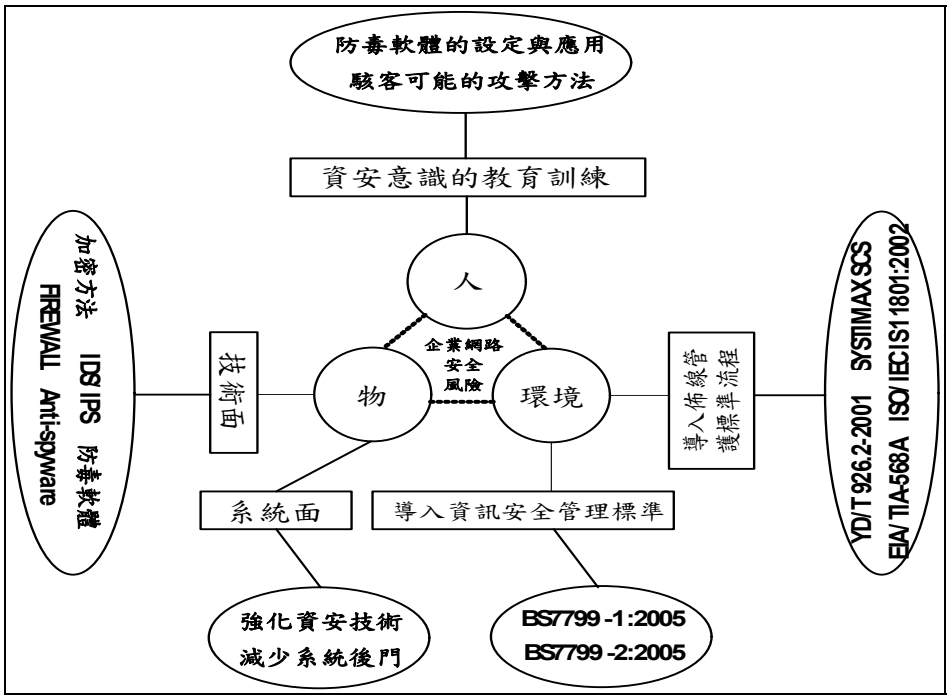
基本上，網路設備除了包含用來連結電腦的設備 (如 ROUTER、MODEM 或是 GATEWAY) 之外，還有電腦與電腦之間用來傳遞資料的載體 (如雙絞線、同軸電纜或是光纖)。如果這些設備的可靠性或穩定性不佳，可能會導致訊框遺失或位元失真的問題；網路拓樸則包括拓樸結構、ISP，或是系統軟體選擇不當的問題。另外，企業在整個網路拓樸中所部署的資安結構，也會對企業網路或系統安全造成影響。

三、環境的風險

主要來自於自然災害與資訊設備放置的環境所產生的安全風險。由自然災害所導致的資安事件往往很難恢復，像地震、水災與雷擊都會對資訊設備造成損壞 (張玉龍等人，2006)。資訊設備放置的環境，一般來說是機房，因素包括溫度、濕度、電力品質與磁場都會對資訊設備的使用壽命與通訊品質都有直接的影響。

整體來看，網路安全風險是一個牽涉很多面向的問題。對企業而言，除了資訊相關技術需要考慮之外，其中還包含了人與環境的管理問題，因此，必須再加入相當多管理面的配合才算完整。因此，本文針對上述人、物與環境等因素分別提出可行的因應架構，如圖一所示，

提供給管理者參考：



圖一　企業網路安全風險與因應架構

一、由「人」所造成的問題，大部份的原因都是人員資安意識過於薄弱 (林怡辰，2006)。因此，「不光是作業系統，人腦也應該上 patch」(李倫銓，2006)。企業可以定期舉辦用戶資安意識的訓練，目的在提高人員對資訊安全的認識。尤其，自從微軟作業系統內建防火牆之後，許多駭客開始轉向研究應用程式漏洞，所以，不僅要訓練使用者防範新型態攻擊手法，也需要教育使用者如何設定防毒軟體。

二、由「物」所造成的問題，基本上，這是由作業系統、應用軟體或是承襲由過去前人設計的拓樸架構等原因所造成，很難去完全的改變它。因此，企業只能把防線退到加密技術、FIREWALL、IDS/IPS、防毒軟體與 Anti-spyware 技術等達成防範的目的(李倫銓，2006)。不過，歸根究底，作業系統廠商如果可以在資訊安全技術上更加完善，減少系統出現「後門」的可能性，或許才是有效減少企業網路安全風險最基本也是最有效的方法。

三、由「環境」所造成的問題，必須透過完整、全面的管理制度降低其風險，像 SYSTIMAX SCS、ISO/IEC IS 11801:2002、EIA/TIA-568A 與 YD/T 926.2- 2001 都是可以參考的佈線管護標準，透過這些結構化的架構，企業資訊人員可以按照一定的實施步驟、參考既有的地理關係與組織結構去連結一幢建築物內或建築群體中的資訊傳輸媒介系統。另外，也必須針對人與環境或物與環境間的關係進行明確的定義，以便進一步規範與管理，像英國的 BS7799-1:2005 (即 ISO/IEC 17799) 或是它的進階版 BS7799-2:2005 (即 ISO27001: 2005) 都是管理者可以參考的管理規範 (彭俊妤，2006)。它是以 PDCA 流程模型爲基礎，透過組織整體安全政策、資產管理、人力資源安全、實體環境安全、通

訊與操作安全、權限審查、資訊系統的開發…等多個控制要項協助企業內部的資訊資產，有效控管機房可能發生的安全風險。

【參考文獻】

- 李倫銓 (2006)。免殺木馬兵臨城下 資安防線節節敗退。資安人科技網。
- 林怡辰 (2007)。資安意識低落 使台灣企業成垃圾郵件幫兇。Taiwan.CNET.com。
- 張玉龍、張彥珍與王大龍 (2006)。*計算機網絡的風險分析與對策*。網絡安全技術與應用，1 月，87-89。
- 彭俊妤 (2006)。信息安全風險評估方法綜述。網絡安全技術與應用，1 月，84-86。
- 賴明豐與呂芬蘭 (2007)。*淺談殭屍電腦的影響與防治之道*。科技政策智庫。
- 賴明豐與李駿翔 (2007)。*淺談 ISN/SYN FLOODING 攻擊方法與可能的因應對策*。科技政策智庫。

（本文由國家實驗研究院科技政策研究與資訊中心副技術師賴明豐、李樹民助理技術師 提供）