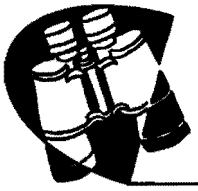


資安管理

組織資訊安全管理策略之探討

洪國興・季延平・趙榮耀

由於資訊科技的無遠弗屆，隨著Internet的崛起與EC的盛行，不論個人或組織對資訊科技的依賴日深，益突顯組織資訊安全的重要性與急迫性；因此，本文透過資安管理的深入調查、研究，歸納出實務上對資安管理面、產品面與委外面應有的解決策略，期望能提供各界研參…

隨著資訊科技(Information Technology)廣泛的被應用在各行各業，組織對資訊系統(Information System)的依賴也日益加深，使得現今社會對於資訊科技已到了不可或缺的地步。網際網路(Internet)應用的崛起，電子商務(EC)的日漸盛行，堪稱係繼農業革命、工業革命、資訊革命之後，又一次影響人類生活型態的革命，其影響的廣度及深度尚在持續擴大之中。在網路運算(Web Computing)時代，資訊系統的使用者，已是不限於組織內部，也不限於與企業有往來的上下游廠商，而是遍佈於世界各地不特定的組織或個人。由於組織面臨的是一個對資訊科技依賴日深，網路運算影響日益深遠，使用者無所不在的環境，使得組織的資訊安全面臨前所未有的挑戰（Schultz等，2001；Eloff & Solms, 2000）。

本文的目的，希望藉由對組織資訊安全管理的調查，來了解實務上解決組織資訊安全的策略，包括管理面、產品面與委外面，以作爲組織制定資訊安全解決方案的參考。

對組織而言，資訊是一種具有價值的重要商業資產，需要善加以保護，以免受到各種威脅的攻擊，而維持組織營運的持續性，即使發生安全事故，亦可使其可能發生損失降至最低。

資訊安全與管理

資訊安全係在處理電腦系統的使用者之非授權行爲的預防與發現(Gollmann, 1999)。任何資訊安全政策之廣義目標，必需能保護儲存於資訊系統中資料之機密性(Confidentiality)、完整性(Integrity)與可用性(Availability)，即所謂「C.I.A.」（Smith, 1989；Schultz, 2001；ISO/IEC 17799-1, 2000；Chapma, 1995；鄭信一，1999）：

（一）機密性(Confidentiality)：

確保「資訊」只能被經過授權的人，才能存取。

（二）完整性(Integrity)：

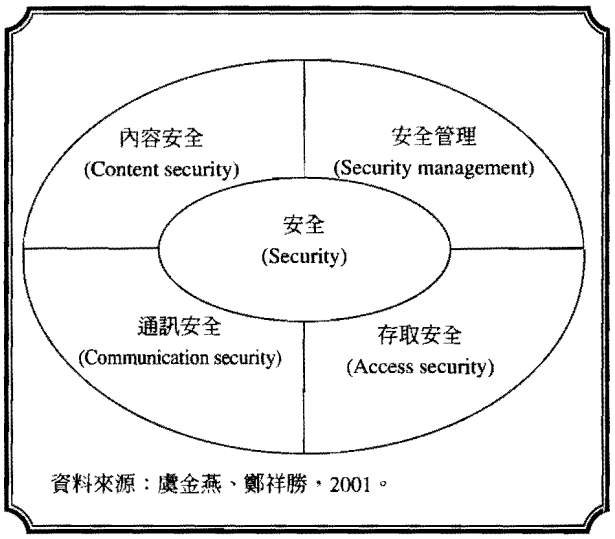
保證「資訊」和其「處理方法」的準確性與完整性。

（三）可用性(Availability)：

確保經過授權的使用者，能存取「資訊」，並使用相關「資訊資產」。

資訊安全就是保護任何與電腦有關的事務之安全，將管理程序與安全防護技術運用在硬體、軟體與資料之中(Rusell & Gangemi, 1992)。對組織而言，資訊是一種具有價值的重要商業資產，需妥善加以保護，以免受到各種威脅的攻擊，而維持組織營運的持續性，即使發生安全事故，亦可使其可能發生損失降至最低(ISO/IEC 17799-1, 2000)。「資訊系統安全」乃指一切保護資訊系統資源，包括：硬體、軟體、資料庫，以防止遭受變更、破壞及未授權使用資訊系統資源之控制措施，其範圍包括技術面與組織管理面（吳琮璠，1996）。

圖1 組織的資訊安全需求



資料來源：虞金燕、鄭祥勝，2001。

組織之資訊安全策略

Ovum研究機構認爲組織資訊安全的需求分爲以下四類，如圖1所示（虞金燕、鄭祥勝，2001）。

1.內容(Content)安全：

保護企業或組織資訊內容，免於天然或人爲的破壞或竊取。

2.存取(Access)安全：

控制使用者的權限，即特定人在特定時間及

地點內對特定資料的存取。

3.通訊(Communication)安全：

保護傳遞中的訊息及交易。

4.安全管理(Security management)：

控制及管理安全過程，監督其執行，與對安全侵害的反應。

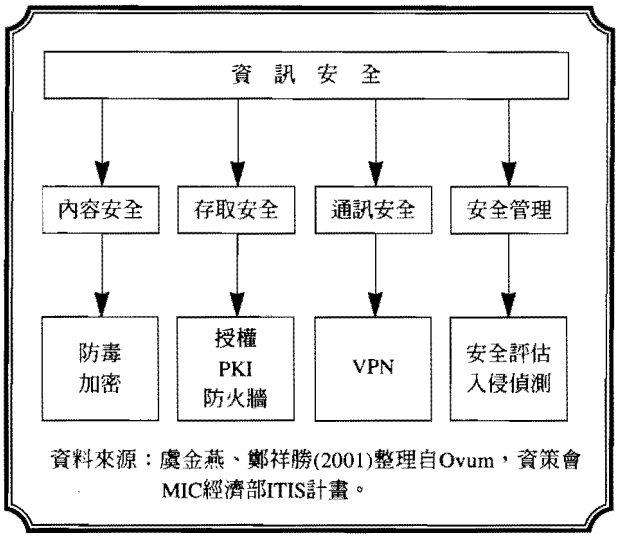
本文依據相關文獻共列舉資訊安全管理面之實施項目共14項進行調查，已／曾實施比例最高的前三名，分別是系統與資料之存取控制(94.2%)、網路安全控制(92.9%)以及系統安全控制(90.9%)，顯示此三項受到組織極大的重視。

在實務上，組織爲解決資訊安全的問題，具體作法可以分別從安全管理(Security Management)、產品與工具(Products and Tools)，與委外服務(Outsourcing)等三個層面進行。本文據以設計問卷，對中華民國資訊經理人協會、中華民國資訊應用發展協會之會員，及政府資訊資訊主管聯席會議成員等，除重複部份外，進行調查，於2002年11月間以E-mail寄出問卷650份，填寫問卷159份，扣除無效問卷5份，有效問卷154份，有效填答率23.69%。

(一) 安全管理策略

本文依據相關文獻共列舉資訊安全管理面之實施項目共14項進行調查，已／曾實施比例最高的前三名，分別是：「系統與資料之存取控制」(94.2%)、「網路安全控制」(92.9%)、「系統安全控制」(90.9%)等，顯示「存取控制」、「網路安全」及「系統安全」受到組織極大的重視。最低的前三名，分別是：「進行風險管理」(33.1%)、「進行風險分析（威脅、弱點等）」(36.4%)、「異地備援機制」(39.6%)等，顯示組織以「風險管理」、「異地備援機制」來達成資訊安全的目標之作法尚未普及。

圖2 支援組織資訊安全的產品



資料來源：盧金燕、鄭祥勝(2001)整理自Ovum，資策會MIC經濟部ITIS計畫。

整體而言，對於14項資訊安全管理面之實施項目，已／曾實施者爲71.9%，未來將實施爲21.2%，不知道者爲6.9%。顯示組織運用資訊安全管理策略，實施安全控制措施已受到極大的重視，其不知道者應有兩種可能，其一是被調查者，對該項措施不了解；其二是不知組織是否已實施，且不知未來是否會實施，其比例甚低，尚屬合理。

(二) 安全產品工具策略

組織對不同的資訊安全需求，使用不同的資訊安全產品與工具，如圖2所示。

本文共列舉資訊安全產品或技術9項，進行調查，已／曾實施比例最高的前三名，分別爲：「電腦防毒」(Anti-Virus)(98.1%)、「防火牆」(Firewall)(96.8%)與「虛擬私有網路」(Virtual Private Network, VPN)(67.5%)。顯示

「電腦防毒」與「防火牆」兩者幾乎成爲資訊安全的代名詞，是其來有自，是現今組織用於資訊安全的兩大利器（陳長榮與葉長偉，2002），VPN也正急起直追。

整體而言，對於九項資訊安全產品面的實施項目，已／曾實施者爲61.5%，未來將實施者爲28.1%，不知道者爲10.4%。顯示資訊安全產品與工具，仍是組織用以達成資訊安全目標的重要策略，尤其未來將實施者約接近三成，顯示資訊安全產品的市場潛力雄厚，值得資訊安全軟硬體供應廠商的重視。

（三）安全委外服務策略

由於資訊安全的專業及技術層次不斷提昇，使得組織內部較難以有足夠水平的人才，因此資訊安全委外服務應運而生。資訊安全委外服務廠商所提供的服務種類有（Fenn等，2002；立駭科技，2002）：

1.防火牆監控與管理服務(Fire Monitoring)。
2.入侵偵測系統監控與管理服務(Intrusion Detection Monitoring)。
3.防禦性安全弱點掃瞄服務(Vulnerability Assessment)。
4.滲透測試服務(Penetration Testing)。
5.病毒掃瞄服務(Anti-Virus)。
6.VPN管理服務。
7.網頁監控與即時復原服務(WebPage Monitoring & Recovery)。
8.網址過濾服務(URL Filtering)。
9.安全警訊通報服務(Security Intelligence Alert)。
10.報表分析服務(Reporting & Analysis)。
11.安全事件回應、調查與蒐証服務(Incident Response & Forensics)。
12.資訊安全政策制訂服務(Security Policy Development)。
13.資訊安全教育服務(Security Education and Training)。
14.修補管理(Patch Management)。

本文將資訊安全委外歸納整合成三項實施項目進行調查，其中已／曾實施比例最高者爲「諮詢顧問服務」(20.1%)、未來將實施比例最高者爲「認證服務」(56.5%)。整體而言，已／曾實施者的比例爲17.3%，未來將實施的比例爲52.8%，不知道的比例爲29.9%，目前組織普遍未運用資訊安全委外服務的策略，但未來將實施的比例都高達五成以上，顯示資訊安全委外服務未來有極大的市場開拓空間，值得委外服務廠商的重視。

（四）資訊安全策略之執行績效

組織在實施資訊安全管理措施，建置資訊安全軟硬體產品或工具，或資訊安全委外服務等之後，對組織資訊安全的影響，經問卷調查，以7尺度表示非常不同意到非常同意，經評估最高的爲「整體資訊安全績效提升」(5.86)，其次爲「因資訊安全事故而造成的損失降低」(5.84)，再次爲「資訊安全事故之後的復原時間縮短」(5.82)，評估爲最低者爲「資訊安全事故的次數減少」(5.74)，最高與最低僅相差0.12，顯示整體而言，無論係安全管理面、產品工具面或委外服務面的資訊安全管理作爲，對提升資訊安全績效應係有正面的幫助。

結論

組織可採用之資訊安全策略可分爲三個層

面，包括：安全管理、產品與工具、委外服務等。經本文之調查，其中以資安產品與工具策略被採用的比例最高，顯示組織較重視資訊安全產品與工具的應用，這與廠商之大力促銷，快速喚醒組織之資訊安全意識的作法不無關係。其次係安全管理策略，安全管理策略漸受到重視，係導源於英國標準協會(BSI)對BS 7799的制定與國際標準組織(ISO)對ISO/IEC 17799的公佈，並經國內著名的會計師事務所的大力引進，尤其政府的強力介入與催化，使得組織對資訊安全管理的更加重視。資安委外服務策略尚在萌芽階段，近年來在政府的大力鼓吹之下，後勢看好。對於資訊安全策略執行之績效，大多數的組織均持正面的看法，相信與事實相去不遠，值得尚未重視資訊安全策略的組織借鏡，也可作爲組織制定資訊安全策略的參考。

（作者分別爲監察院綜合規劃室主任、政治大學資訊管理學系副教授以及淡江大學管理科學研究所教授）

■參考文獻

1.Chapman, D.B. and Zwicky, E.D.(1995), Building Internet Firewalls, O'Reilly & Associates.

2.Eloff, M.M. & Solms, S.H.V.(2000), "Information Security Management：An Approach to Combine Process Certification And Product Evaluation", Computers & Security, Vol.19, NO.8 , PP.698-709.

3.Fenn, C.& Shooter, R(2002),"IT Security Outsourcing", Computer Law Security Report, Vol.18, No.2, PP.109-111.

4.Gollmann, D.(1999) Computer Security, John Wiley& Sons Ltd, 1999.

5.ISO/IEC 17799-1(2000), Information technology-code of practice for information security management, 2000.

6.Rusell, D. & Gangemi, G.T.(1992), Computer Security Basics, California, U.S.A., O'Reilly & Associates Inc, 1992.

7.Schultz, E.E., Proctor, R.W., Lien, M.C.(2001),"Usability and Security An Appraisal of Usability Issues in Information Security Methods", Computer & Security, V.20, NO.7, PP.620-634.

8.Smith, M.(1989), "Computer Security-Threats, Vulnerabilities and Countermeasures", Information Age, October, PP.205-210.

9.立駿科技(2002)，“資訊安全委外服務研究”，資訊與電腦，12月，PP.33-38。

10.吳琮璠(1996)，“國外政府機構資訊系統安全稽核制度”，存款保險資訊季刊，10卷2期，PP.21-40。

11.陳長榮、葉長偉(2002)，“防火牆安全管理之實施”，資訊與電腦，200.10, PP.94-97。

12.虞金燕、鄭祥勝(2001)，資訊安全發展趨勢與科專研發方向建議，財團法人資訊工業策進會。

13.鄭信一(1999)，現代企業資訊安全之個案研究，銘傳大學管理科學研究所碩士論文。