組織制定資訊安全政策對資訊安全影響之研究

A Study of the Effect of Defining Information Policy on Information Security in an Organization

洪國興 季延平 趙榮耀

Kwo-shing Hong Yen-ping Chi Louis R. Chao

監察院綜合規劃室主任 政治大學資訊管理學系副教授 淡江大學管理科學研究所教授

摘 要

在網際運算及電子商務的 e 化時代，「資訊安全」已是組織的重要目標之一，組織經由資訊安全政策之制定、實施與維護之程序，來達成提昇資訊安全的目標，因此，資訊安全政策之制定是組織資訊安全的基礎建設。本研究係以資訊「安全政策理論」（Security Policy Theory）為基礎，提出資訊安全政策模式（Information Security Policy Model），並發展本研究之研究架構，就「組織特性」、「資訊安全政策」與「資訊安全之提昇」等三個構念進行研究，以假說檢定其構念之間是否有影響，並對其因徑函數加以驗証，以知其構念之間的因果關係。本研究除首開以實証研究驗証資訊安全管理理論外，亦可提供組織資訊安全在管理策略上的參考。

關鍵字：資訊安全、資訊安全政策、安全政策理論、資訊安全政策模式、因徑分析

Abstract

In the e-era of internet computing and electric commerce, "Information Security" has become an important goal of an organization. The organization achieves its target of promoting information security through the establishment, implementation and maintenance procedure of an information security policy. The establishment of information security policy is therefore the infrastructure of information security of an organization. This Study is based on the "Security Policy Theory" to propose the "Information Security Policy Model" and develop the research structure of the Study. Its research is further developed by three constructs－"characteristics of organization", "information security policy" and "improvement of information security". Hypothesis theory is used to examine the possible effects among its constructs. The Study also examines its path functions to derive the causality of each construct. It would not only be the first one to examine the theory of information security management by empirical research but also a useful reference to the information security management policy of an organization.

Keyword: information security, information security policy, information security policy theory, information security policy model, path analysis.

壹、緒論

身處在今天網路運算及電子商務的 e 化時代，追求「資訊安全」是每一個組織的目標，對於依賴資訊系統始能營運的組織，資訊安全更突顯其重要性。然而不同的行業，不同性質的組織，使用不同的資訊技術，在不同的風險程度，不同的成本效益考量下，其資訊安全要求的程度，使用的資訊安全技術及內部控制的策略均有所不同，故組織應從策略、管理、技術等層面來建立適合於組織的「資訊安全政策」（Information Security Policy），以作為組織資訊安全管理的指導方針與執行依據，也是組織將資訊安全融入企業策略規劃的必要途徑。當組織擁有一份適當而周延的安全政策，它能為組織帶來隱含的價值，為企業提昇其信用與商譽，使投資人及社會大眾對企業更有信心，為企業帶來策略上的優勢（林進財等，民 88 年；李正源與簡崑鎰，民 89 年；Hinde,2002；Kühnhauser, 1999）。

「資訊安全政策」是指導組織資訊安全的最高原則及指導方針，一個組織若欠缺資訊安全政策，亦可顯示其管理高層欠缺資訊安全意識，對資訊安全的警覺不足；一個欠缺資訊安全政策的組織，其資訊安全措施再完善，恐怕也只是個別的資訊安全技術或產品的使用，難有整體、周延的資訊安全保護，

畢竟要提昇組織的整體資訊安全，是有賴於完整的資訊安全管理制度與資訊安全防護技術，二者相輔相成，而資訊安全政策乃是建構此二者的基礎建設，也是組織建立安全環境的首要工作。資訊安全政策必須由高階管理人員支持，並領導實行，這也是組織長期的資訊安全建設中，最重要的一項基礎建設（鄭信一，民 88 年；李正源與簡崑鎰，民 89 年；Osborne, 1998；文茂平與余俊賢，民 89 年；Dellecave, 1996）。

根據國際電腦安全協會（ICSA）在 1999 年公布的研究報告指出，超過 80%的受訪者，其組織的資訊安全政策有明顯的缺失，國內較少此方面的調查研究，相信仍有相當大的「進步空間」（黃承聖，民 89 年）。Blacharski 也指出：大多數的經理人都宣稱對資訊安全的重視，但有接近一半的美國企業並沒有資訊安全政策，1980 年代也只有美國的軍方與政府網路有資訊安全政策，尤其對於分散式系統環境的興起，更缺乏可滿足分散式系統環境所面臨的資訊安全管理所需之資訊安全政策，以致資訊安全軟硬體的引進毫無策略可言，顯示資訊安全的基礎薄弱（李正源與簡崑鎰，民 89 年；Lindup, 1995；Ward & Smith, 2002）。在林進財等個案研究中，亦指出：組織的資訊安全政策不夠明確，且組織的資訊安全規定，與實際的資訊安全管制之間，存有相當落差，其原因導源於組織的資訊安全需求不明確所致。因此，資訊安全政策之制定，對於組織資訊安全需求之規劃，是其中重要的一環（林進財等，民 88 年；Lindup, 1995）。

本研究將資訊安全政策文獻整理歸納為資訊「安全政策理論」（Security Policy Theory），以作為本研究之理論基礎，進而提出資訊安全政策模式（Information Security Policy Model），並發展本研究之研究架構，對「組織特性」、「資訊安全政策」與「資訊安全之提昇」加以驗証，以了解「組織特性」對「資訊安全政策」的影響，「資訊安全政策」對「資訊安全之提昇」的影響，以及之間之因果關係。

本文首先對資訊安全政策的背景加以說明。第二部分探討資訊安全政策的意義、目的與功能，進而討論政策之制定、實施內容、評估與維護。第三部分為研究模式之建構與研究假說之擬訂。第四部分說明研究方法，包括：問卷設計、資料蒐集、研究工具等。第五部分為資料分析與研究結果。最後為結論與建議。

貳、文獻探討

本研究之文獻探討，在對資訊安全政策過去的研究進行瞭解、整理、分析，並歸納找出共同特性，形成資訊「安全政策理論」（Security Policy Theory），以作為本研究之理論基礎。

真正研究資訊安全政策的文獻不多，實證研究更少，但仍有部分資訊安全的研究，包含有資訊安全政策的議題。綜觀資訊安全政策的有關文獻，國外以探討資訊安全政策之制定、實施內容、評估等較多，國內近年的資訊安全稽核實證研究中，頗多出現資訊安全政策的調查，頗值得參考。

曾淑惠（民 91 年）的調查研究指出：有 80.4%的銀行有定期修正資訊安全政策，顯示銀行對於資訊安全政策的重視程度頗高；該研究係以 BS 7799-1（1999）為基礎評估銀行業的資訊安全環境，其中「安全政策」41.2%完全達成，29.4%部分達成，14.7%尚在建置中，11.8%尚在規劃中，2.9%尚未考慮，顯示仍約有三成的銀行，尚無資訊安全政策，其中外商銀行在安全政策的表現優於本國銀行，資訊安全政策的重要性在本國銀行較被忽視，故仍有進步的空間。

在黃姮儀（民 89 年）的研究中指出：金融機構已制定網路安全政策者佔 44.8%，未制定者 55.2%，在未制定網路安全政策的金融機構中，大部分預定於一年以內制定，顯示網路安全政策漸漸受到重視。對於安全政策的修正頻率，平均每 8 個月修正一次，最長者為 2 年。若是修正頻率過於頻繁，缺乏政策的穩定性，也會為使用者帶來不便，顯非妥適的做法（Höne & Eloff, 2002b）。

政府首次對政府部門及民間企業所做的資訊安全稽核，在受稽核的 76 個組織中，資訊安全政策非常完整者佔 59%，尚屬完整者佔 33%，是國內歷來所有調查中最好的一次，由於調查對象係經過挑選，其中政府機關均係資訊應用有相當歷史，民間企業均為具有相當規模，且資訊科技對其業務營運具有不可忽視的重要性，故調查結果尚不能推論為整體的現象（行政院主計處電子處理資料中心；民 91 年）。

另一項調查指出：85%的受訪者，聲稱他們的公司已投入在資訊安全政策的建置，但對照另一項由 KPMG 所做的調查，卻指出僅有 27%的受訪者已制定文件化的資訊安全政策，大型企業則提高到 59%。但在 Ernst & Young 的調查，其受訪者都認為他們已有資訊安全策略（Hinde, 2002）。

以下將文獻探討的內容分類整理為：資

訊安全政策的意義、目的與功能、政策之制定、實施內容、評估與維護等五個部分，分別加以陳述。

一、資訊安全政策的意義

據 Starling（1988）所指：「政策是目標或目的的一般性陳述，而計劃則是為達成政策目標的一種特定的方法（A Policy is a general statement of aims or goals. It's not quite the same thing as a plan, which is best thought of as specialized means for achieving the goals of policy)。」陳世賢等進一步指出：「政策（Policy)」一字，其意涵不論公或私部門，亦不論原則或細節，只要是處理或解決問題的方針、原則、策略、措施、辦法均屬之（陳世賢與陳恆鈞，民 90 年)。

資訊安全政策定義為：組織為了確保其資訊資產的機密性（Confidentiality)、完整性（Integrity)、可用性（Availability)，依據組織發展需要，衡量資訊資產之風險，符合組織營運目標，所制定之管理策略與制度規範（黃承聖，民 89 年)。從另一角度來看，「資訊安全政策」係規範組織的成員存取組織的資訊科技與資訊資產（Information Technology and Information Assets）所應遵守的規則之正式文件（欒志宏，民 91 年)。此一文件的名稱可能是：辦法、規範、規定、或要點等等。

組織的「資訊安全政策」是什麼呢？萬幼筠（民 90 年）認為是：

1、有體系之資訊安全管理體系的象徵。
2、組織對資訊安全需求的企圖聲明（Intension)。
3、賦予組織相關部門執行資訊安全的權責（Authorities)。
4、建立組織內部溝通資訊安全需求的基準（Baseline)。
5、建立組織資訊安全管理機制（Mechanism)。
6、與組織的整體策略及營運目標相結合（Business)。
7、由多階層的資訊安全管理體系所構成。
8、建立組織資訊安全一般性原則，但反應風險管理的必要性。

總之組織的「資訊安全政策」，係建立在組織的總體目標和優先順序的基礎之上，一般定義如下，亦作為本

研究之定義。

1、為組織設定如何安全的使用資訊，以及安全的優先順序，以達成組織目標。
2、在符合組織的目標下，規範「資訊安全」的範圍。
3、以資訊安全為基礎的資訊管理與資源使用原則。
4、係支援資訊安全技術，以建立資訊安全成本效益的原則。

二、資訊安全政策之目的與功能

資訊安全政策的主要目標在於定義組織資訊資源的使用者之權利與責任。而有效的資訊安全政策是要幫助使用者瞭解其處理日常事物時，在確保資訊資源與處理資訊的安全下，所可以接受與負責任的行為（Höne & Eloff,2002b）。

資訊安全政策的目的與功能在於（Ward & Smith , 2002；林勤經等，民 90 年；李正源與簡崑鎰，民 89 年）：

1、對組織資訊資產安全的需求，提供指導方針與規範，並具體表現高層管理者對資訊安全的支持與承諾，以善盡企業責任與義務。
2、定義組織內有關部門與人員對資訊安全管理的角色與責任，為資訊安全的基礎建設。
3、對於資訊系統的存取，建立安全標準與控制的基準，促使組織建置一致性的控制制度，以達成企業目標。
4、資訊安全是技術，也是策略，因此，資訊安全政策可指引資訊安全產品的選擇與技術的引進。
5、將資訊安全控制需求加以正式化與文件化，以支援組織內部與外部檢視對維護資訊安全的規劃與執行，是否充份足夠，以作為資訊安全溝通的平台。
6、確保合法的使用者可以存取檔案與資訊資源，防止未經許可的使用資訊資源，以維護資料的完整性。
7、對存取機密資料的限制，以防止意外或蓄意破壞，致危害硬體、軟體及其他資訊資源。

三、資訊安全政策之制定

資訊安全政策的核心在於界定組織資訊安全的核心價值，以符合組織的整體目標。組織性質的不同，其資訊安全的核心價值自然不同，如軍事單位的資訊安全核心價值可能是國防

機密的維護與資訊戰的存活，政府部門資訊安全的核心價值是人民隱私的保護與公共服務，對企業而言，其資訊安全的核心價值是營業利益的維護。由於核心價值的不同，其資訊安全政策應係符合其核心價值的策略方針，亦據於釐清資訊資產的價值，使資訊安全政策得以具體可行（黃承聖，民 89 年）。

國際間對資訊安全，已意識到安全政策的重要，在國際標準之中對於資訊安全政策提出一些制定的指導與規範，普遍受到重視，如表一所示（Höne & Eloff, 2002a），可以作為組織制定資訊安全政策的參考。

資訊安全政策制定的策略與步驟為（Kabay, 1996；Lindup, 1995；Word & Smith, 2002）：

1、專案開始（Project Initiation）：對組織資訊安全初步評估（Preliminary Evaluation），說服高層主管，促使其對資訊安全提昇其敏感度（Management Sensitization）。

表一　國際標準對資訊安全政策的規範

國際標準	對資訊安全政策的規範
BS 7799 （Code of practice for Information Security Management） ISO/IEC17799	・列出資訊安全政策至少應包含的內容。 ・說明組織應如何執行資訊安全政策。 ・資訊安全政策應經由組織負責人核定，並公布與溝通。 ・資訊安全政策應定期檢討與評估。
BSI IT Baseline protection manual German Bandesamt für Sicherheit in der Informationstechnik（BSI）制定	・如何草擬資訊安全政策。 ・資訊安全政策涵蓋的內容項目，如：管理責任，政策發展的職責，內容、政策的宣達等。 ・資訊安全政策至少應包括的內容。 ・資訊安全政策的檢討。

COBIT 由資訊系統稽核與控制協會（the Information System Audit and Control Association & Foundation）（ISACAF）所發展	・執行資訊安全政策的程序與控制需求。 ・簡要說明安全與內部控制的架構政策。 ・介紹各種文件的建立與維護。
GASSP （Generally Accepted System Security Principles）由美國國家研究會議（the Untied States of America's National Research Council）所出版	・提出資訊安全政策最低的需求及政策的原理。 ・資訊安全政策的定義、維護與建置。 ・資訊安全政策的層次概念，並探討其深度。
GMITS （ISO/IEC PDTR13335-1）	・對資訊安全的規劃、管理與建置，提供綜合性的指導。
ISFs Standard of Good Practice 來自全球化資訊安全論壇（the globally representation Information Security Forum, ISF）	・資訊安全管理的績效衡量。 ・列出資訊安全政策的內容。 ・資訊安全政策的特性。 ・說明可接受的使用者行為。

資料來源：本研究整理自 Höne & Eloff, 2002a.

2、資訊安全政策之發展（Security Policy Development）：進行資訊安全需求分析（Needs Analysis），草擬政策草案，經由內部討論與溝通，並由資訊安全主管（Information Security Officer, ISO）初步決定。

3、諮詢與核定（Consultation and Approval）：諮詢資訊安全專家或顧問的意見，再由組織負責人（CEO）對資訊安全政策的接受、承諾與核定的程序，形成正式的資訊安全政策，並正式發布。

4、安全意識與政策教育（Security Awareness and Policy Education）：對

組織各層級實施資訊安全政策之教育與訓練，以建立安全意識。

5、政策宣導（Disseminate Policies）：對組織內宣導資訊安全政策，作為組織資訊安全的基礎建設，對外宣導，以建立上下游產業、及消費者對組織資訊安全的信賴。

四、資訊安全政策之實施內容

管理階層應制定一個明確的安全政策方向，在整個組織中發布，並定期維護資訊安全政策，宣示管理高層對資訊安全的支持和保護的責任（ISO/IEC 17799, 2000）。

資訊安全政策的實施內容，係組織建立資訊安全的重要核心，其內容應包括：資訊安全組織與任務、角色與責任（Roles and Responsibilities）、資訊分類與控制（Information Classification and Control）、資訊風險評估（Information Risk Assessment）、資訊安全教育訓練、存取控制（Access Control）、實體及環境安全（Physical and Environment Security）、病毒防護與管理、資訊安全事故之緊急處理程序、業務持續運作管理（Business Continuity Management）、違反資訊安全政策的懲處（Information Security Policy Violations and Disciplinary Action）、法令規定的遵行（吳琮璠，民 91 年；林宗瀛，民 91 年；欒志宏，民 91 年；ISO/IEC 17799, 2000；Osborne, 1998；Höne & Eloff, 2002a&b；Ward & Smith, 2002；Flynn, 2001）：

國際間的資訊安全標準對於資訊安全政策的內容也有不同的規定，在組織內不同的職位，對於資訊安全政策的角色與責任格外令人重視，所有的標準均認為是資訊安全政策必須列入的重要內容，彙整如表二所示，可作為組織制定資訊安全政策之參考（Höne & Eloff, 2002a）。

表二　國際間資訊安全標準對資訊安全政策內容規範之彙總

要素與特性	BS7799	BSI	COBIT	GASSP	GMITS	ISF's Standard of Good Practice
資訊安全範圍與需求	v	v	v	v		v
資訊安全目標	v	v				
資訊安全定義	v					
管理高層對資訊安全之承諾	v	v		v		v
資訊安全政策的核定						
資訊安全政策的目的						
資訊安全原則	v	v				v
－遵守法律、規定與契約	v				v	v
－使用資訊安全意識與教育	v	v			v	
－病毒預防與偵測	v					
－永續經營計畫	v				v	
－系統開發與購置					v	
－風險管理					v	v
－人事議題					v	v
－委外管理					v	
－安全事故處理					v	
－資訊分類		v				v
－存取控制		v				
角色與責任	v	v	v	v	v	v
違反資訊安全政策的懲處規定	v	v	v		v	v
監督與檢討		v				
宣達與承諾						
參考附錄	v					
一般要項						
－作者						
－核定日期						
－修正日期						
長度		v				
型態		v				
格式	v	v				v
修正	v	v				v
分發	v	v				v

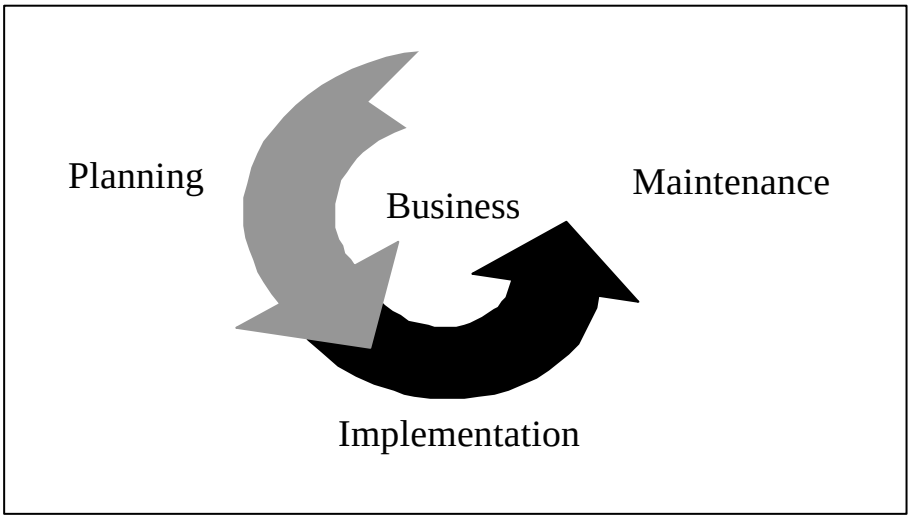
資料來源：Höne & Eloff, 2002a

五、資訊安全政策之評估與維護

組織之資訊安全政策，應定期進行獨立及客觀的評估，始能將政府資訊安全管理政策、法令、技術及組織業務之最新狀況反映於資訊安全政策之中，以確保資訊安全之實際作業與資訊安全政策之吻合，使資訊安全管理能可行而有效。組織應對資訊單位、人員、資訊系統之安全加以評估與稽核，以確保資訊安全政策與規定之貫徹執行（行政院，民 88 年）。

資訊安全政策是一個管理循環，從制定、實施到評估，是一種持續不斷的改善工作，如圖一所示（黃承聖，民 89 年）。

資訊安全政策的評估係按評估的程序進行，可以是定期性的，也可能是非定期的評估。定期性的評估係按資訊安全政策中所定的評估週期定期評估；非定期性的評估其時機為：當發生重大的資訊安全事故時、出現新的資訊安全弱點或漏洞時、組織變動或組織文化改變時、資訊技術或資訊安全技術的基礎建設發生變化時、資訊或控制的需求改變時等（欒志宏，民 91 年；Osborne, 1998）。



圖一　資訊安全政策的管理循環（資料來源：黃承聖，民 89 年）

參、研究模式與假說

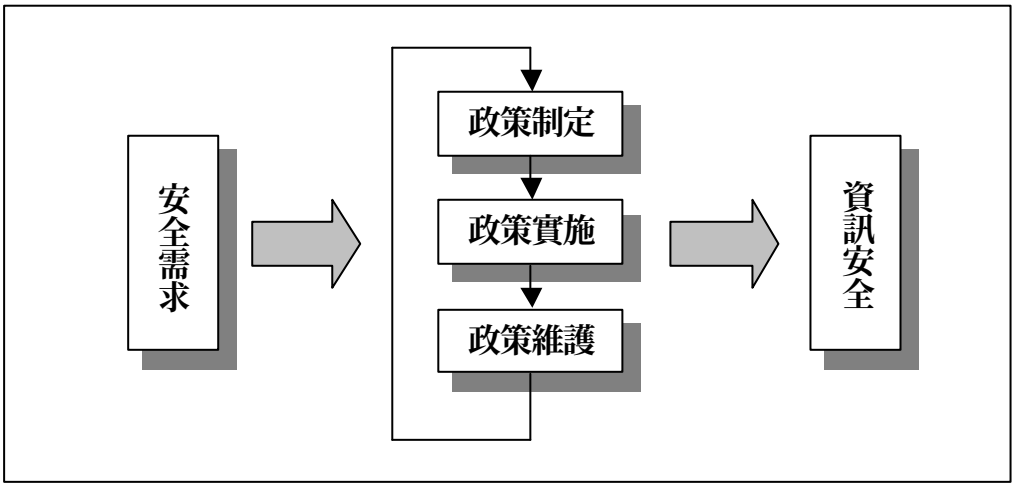
一、研究模式與架構

所謂資訊「安全政策理論」（Security Policy Theory）係指組織透過資訊安全政策（Information Security Policy）之制定、實施與維護的程序，以資訊安全政策為核心，形成資訊安全管理循環（Information Security Management Cycle），經由資訊安全政策的落實執行，來實現資訊安全之目標（Kabay, 1996；黃承聖，民 89 年；Gupta 等，2001；Flynn, 2001）。該理論所闡述的要旨為：資訊安全政策即在規劃資訊安全需求，於組織內形成共識，制定政策，付諸實施，並定期對實施效果加以檢討修正，以滿足組織的最新安全需求，而促進資訊安全的管理程序，示意如圖二所示。其資訊安全的決定則形成下列的函數關係：

資訊安全＝f（資訊安全政策）

資訊安全政策＝f（資訊安全政策制定，資訊安全政策實施，資訊安全政策維護）

資訊安全政策制定＝f（安全需求）



圖二　資訊「安全政策理論」示意圖（資料來源：本研究）

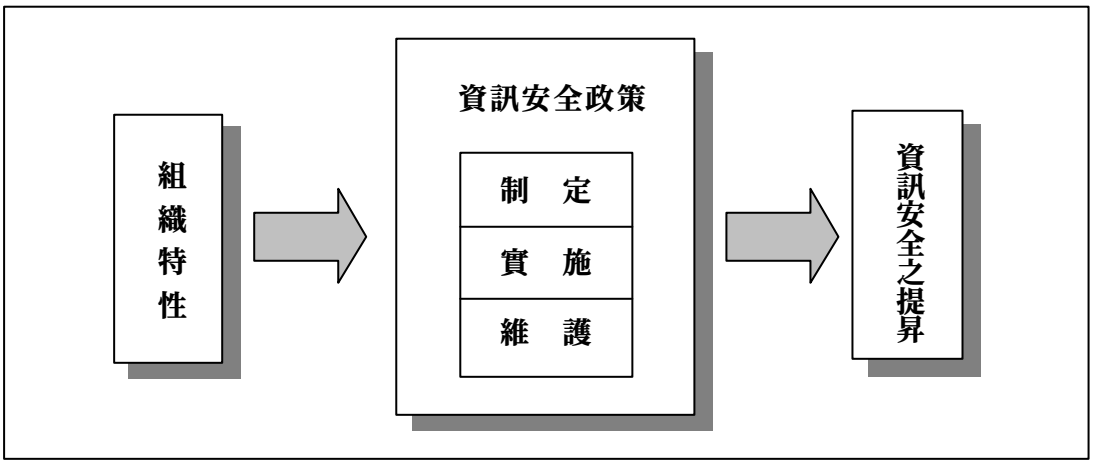
因此，本研究依據資訊安全管理之「安全政策理論」（Security Policy Theory），提出「資訊安全政策模式」（Information Security Policy Model），此一模式基本組成為：組織特性、資訊安全政策之制定、實施與維護、資訊安全之提昇。其關係為：組織特性表達資訊安全需求，組織特性影響資訊安全政策，資訊安全政策影響資訊安全之提昇。如圖三所示。

本研究再依據資訊「安全政策理論」（Security Policy Theory）與資訊「安全政策模式」（Security Policy Model），發展本研究之研究架構，如圖四所示。其函數關係為：

資訊安全政策制定時間＝f（組織特性）

資訊安全之提昇＝f（資訊安全政策-制定、實施、維護）

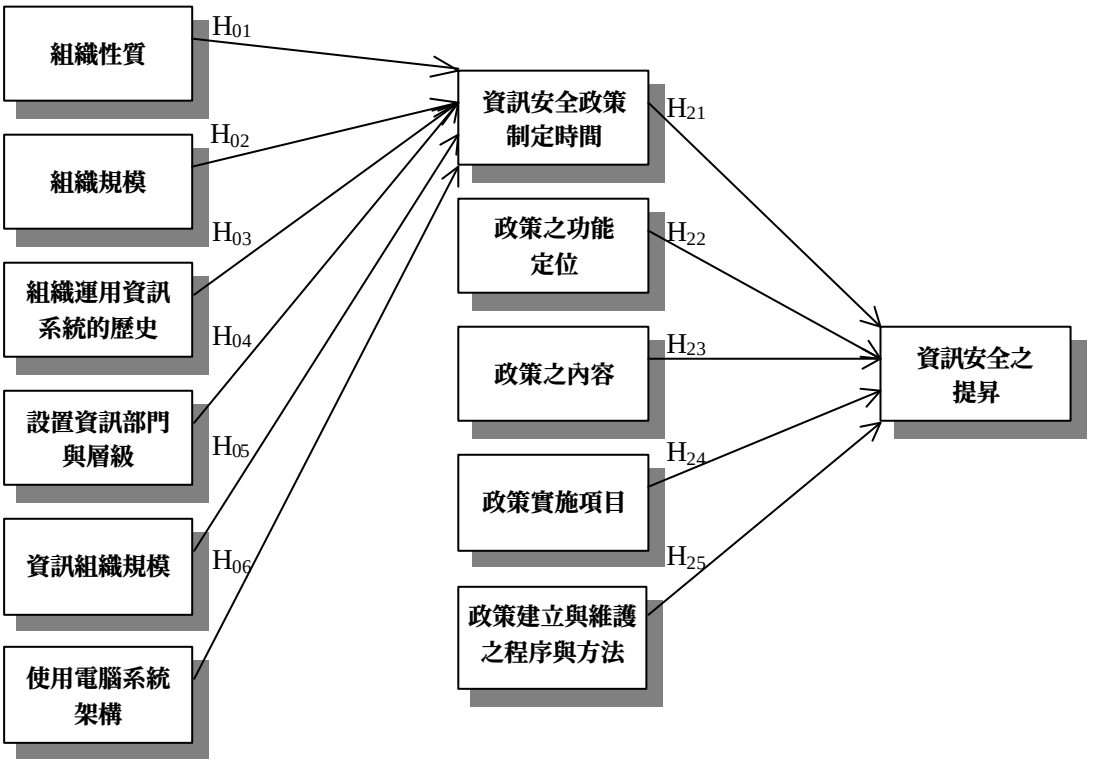
本研究在探討：組織的安全需求影響組織資訊安全政策之制定，資訊安全政策之制定、實施與維護影響資訊安全之提昇，亦即組織的資訊安全需求經由資訊安全政策影響資訊安全之提昇。組織資訊安全需求表現在「組織特性」，包括：組織性質、組織規模、組織應用資訊系統的歷史、設置資訊部門與層級、資訊組織規模及使用電腦系統架構等六個構念（Constructs）；「資訊安全政策之制定、實施與維護」包括：資訊安全政策制



圖三　資訊安全政策模式（資料來源：本研究）

定時間、資訊安全政策之功能定位、資訊安全政策之內容、資訊安全政策實施項目、及資訊安全政策建立與維護之程序與方法等五個構念，而「資訊安全之提昇」自成一個構念。各構念的定義如下：

1. 組織性質：係指組織設立的目的與性質。
2. 組織規模：係指組織成員的多寡，即員工人數的多少。
3. 組織運用資訊系統的歷史：係指組織開始建置資訊系統以直接間接支援各項企業活動，而達成企業目標迄今時間的長短。
4. 設置資訊部門與層級：係指是否設置資訊部門及其部門在組織的層級。
5. 資訊組織規模：係指資訊部門或資訊人員的多寡，即組織投入資訊技術的人力資源。



圖四　資訊安全政策研究架構（資料來源：本研究）

6. 使用電腦系統架構：係指組織主要使用何種形式的電腦系統架構。
7. 資訊安全政策制定時間：係指自組織制定資訊安全政策迄今時間之長短。
8. 政策之功能定位：係指組織制定資訊安全政策，所期待其應具備的功能，及扮演之角色。
9. 政策之內容：係指資訊安全政策所包含的主要內容。
10. 政策實施項目：係指資訊安全政策包含的項目，也就是那些安全子政策。
11. 政策建立與維護之程序與方法：係指資訊安全政策之制定、評估、維護，所經過之程序與使用之方法。
12. 資訊安全之提昇：係指對組織資訊安全的幫助，也就是威脅或弱點的降低、安全事故次數的減少或安全事故損失的降低等。

二、研究假設

由實務上的觀察與文獻探討得知，不同的組織，有不同的資訊安全需求，對於制定資訊安全政策通常有不同的看法與作法，亦即不同的組織特性，對於資訊安全政策制定時間之早晚，以及政策制定的相關決策均有所不同。換言之，由於組織設立宗旨不同，其組織規模的大小、組織運用資訊系統的歷史、設置資訊部門與層級、資訊組織規模的大小、主要使用電腦系統架構的不同，均會影響組織制定資訊安全政策的決策（黃承聖，民 89 年；李東峰與林子銘，民 90 年；Fisch & White, 1999；Ryan & Bordoloi, 1997；Loch 等，1992；李正源與簡崑鎰，民 89 年）。因此，在資訊安全管理的決策中，本研究主張組織特性將會影響組織資訊安全政策制定時間之早晚（Hitchings, 1995）。

H01 不同性質的組織，對於資訊安全政策制定時間會有影響。

H02 組織規模愈大，愈早制定資訊安全政策。

H03 組織運用資訊系統的歷史愈久，愈早制定資訊安全政策。

H04 組織設置資訊部門且層級愈高，愈早制定資訊安全政策。

H05 資訊組織規模愈大，愈早制定資訊安全政策。

H06 使用電腦系統架構，對於資訊安全政策制定時間會有影響。

「資訊安全政策」是組織資訊安全的最高指導原則，也是資訊安全的基礎建設，組織通常係透過「資訊安全政策」的建立來形成組織內外對資訊安全的共識，也是組織訂定資訊安全的基線水準（Baseline Level），成為組織對資訊安全的共同目標。因此，組織資訊安全政策制定時間之早晚，資訊安全政策的功能定位，包括：資訊安全範圍的定義、資訊安全目標與策略的訂定、各階層對資訊安全責任的規範、監督遵守資訊安全的機制、及宣示未遵守資訊安全規章的後果等，均足以影響組織之資訊安全（鄭信一，民 88 年;Höne & Eloff, 2002a ; Flynn, 2001）。因此，本研究主張組織資訊安全政策制定時間之早晚，資訊安全政策之功能定位，都將影響到組織資訊安全之提昇。

H21 組織資訊安全政策制定時間，對資訊安全之提昇會有影響。

H22 組織對資訊安全政策之功能定位，對資訊安全之提昇會有影響。

資訊安全政策的重心在於其執行，也就是將資訊安全政策所訂定的內容付諸實施。資訊安全政策的內容包括：政策目標、資訊安全標準、作業程序之建立與管控，資訊安全與企業營運的結合、安全意識的建立與增進、協調與整合、適用範圍、執行方法，這些都是資訊安全政策的重要內容，均足以影響資訊安全（Kabay, 1996; ISO/IEC 17799, 2000 ; Höne & Eloff, 2002a &b ; Ward & Smith, 2002 ; 李正源與簡崑鎰，民 89 年）。因此，本研究主張資訊安全政策之內容，將影響到組織資訊安全之提昇。

H23 資訊安全政策之內容，對資訊安全之提昇會有影響。

資訊安全政策的實施項目，或稱為子政策，此部分為資訊安全政策最核心的部分，在 ISO/IEC 17799 之中，有詳盡的規範，包括：政策之制定、安全組織與職責、人員安全、資訊資產分類、實體及環境安全、系統規劃與操作安全、資料與媒體安全，通訊與網路安全、存取控制、系統開發與維護、業務持續運作管理、執行與遵守、及資訊稽核等政策，對資訊安全之影響當既深且遠（ISO/IEC 17799,

2000；欒志宏，民91年; Ward & Smith, 2002; Höne & Eloff, 2002b ;吳琮璠，民91年)。因此，本研究主張資訊安全政策的實施項目，都將影響到組織資訊安全的提昇。

H24 資訊安全政策實施項目，對資訊安全之提昇會有影響。

按資訊安全管理「安全政策理論」(Security Policy Theory)，資訊安全係經由資訊安全政策之制定、實施與維護來實現，因此資訊安全政策之建立與評估維護係此一理論的重要環節，在管理程序中為規劃（Planning）與考核（Evaluation）的角色，對資訊安全自然有其貢獻（黃承聖，民 89 年; Höne & Eloff, 2002a；欒志宏，民91年；Gupta, 2001)。因此，本研究主張，資訊安全政策建立與維護之程序與方法，都將影響到組織資訊安全的提昇。

H25 資訊安全政策建立與維護之程序與方法，都將影響到組織資訊安全之提昇。

肆、研究方法

一、問卷設計

本研究採問卷調查法，問卷之設計，除參考資訊安全相關文獻外，並觀察實務上的情況，據以發展而成。初稿完成後，經分別送請有關學者與實務界人士試填，並提供修正意見，經整理分為三部分：

(一) 第一部分：資訊安全與政策基本資料調查。以蒐集組織資訊安全政策之制定，負責資訊安全的部門及人員之資料。

(二) 第二部分：資訊安全政策調查。以蒐集資訊安全政策之功能、政策內容、實施項目、建立維護之程序與方法，及資訊安全績效等資料。

(三) 第三部分：背景資料調查。以蒐集組織特性有關資料。

二、資料蒐集

本研究問卷調查對象為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，及政府資訊主管聯席會議成員等，扣除重複部分，於 2002 年 6 月間以 E-mail 寄出問卷 645 份，

填寫問卷 165 份，扣除無效問卷 8 份，有效問卷為 157 份，有效填答率 24.34%。

三、研究工具

利用 SPSS 統計工具軟體進行各項統計分析。

（一）次數分配：就樣本資料，進行敘述統計。

（二）信度衡量：本研究以 Cronbach's α 來衡量同一構面所有問項之內部一致性，以測試問卷所有問項在某特定構面的一致性程度。

（三）迴歸分析：本研究之研究架構的函數關係模式，係在探討「預測變數」與「依變量」間之因果關係，亦即在檢定：1、「組織特性」（預測變數）對「資訊安全政策」（依變量）的影響是否顯著；2、「資訊安全政策」（預測變數）對「資訊安全績效」（依變量）的影響是否顯著。因此採用「迴歸分析」以期探討兩者間之因果關係，並經由「組織特性」預測「組織資訊安全政策制定時間」，及由「資訊安全政策」預測「資訊安全績效」（Hair 等，1995；周文賢，民 89 年）。

（四）因徑分析：採用因徑分析，用以了解「組織特性」、「資訊安全政策」與「資訊安全之提昇」之間的關係。並以「單向模式」來探討對「組織特性」透過「資訊安全政策之制定、實施與維護」，來解釋「資訊安全之提昇」的效果（周文賢，民 89 年；葉啟政，民 72 年；林清山，民 72 年）。

伍、資料分析與研究結果

一、樣本基本資料分析

有效樣本共 157 份，分析如次：

（一）按組織性質：以政府行政機關 67（42.7%）及民間企業 41（26.1%）較多，其餘如表三所示。

表三　組織性質統計

行業別	次數	百分比
民 間 企 業	41	26.1
政府行政機關	67	42.7
公營事業機構	19	12.1
學校及研究機構	23	14.6
其　　他	7	4.5

資料來源：本研究

（二）員工人數：以員工人數 200-499 人的組織 45（28.7%）及 1000 人以上的組織 38（24.2%）較多，其餘如表四所示。

表四　員工人數統計

人數	次數	百分比
< 5	1	0.6
5~9	5	3.2
10~29	15	9.6
30~49	4	2.5
50~99	11	7.0
100~199	21	13.4
200~499	45	28.7
500~999	17	10.8
> 1000	38	24.2
合計	157	100

資料來源：本研究

（三）組織應用資訊系統的時間：以 10-19 年的 72（45.9%）及 20 年以上的 49（31.2%）較多，其餘如表五所示。

表五　組織應用資訊系統的時間統計

應用時間/年	次數	百分比
<= 2	5	3.2
3~5	9	5.7
6~9	22	14.0
10~19	72	45.9
>= 20	49	31.2
合計	157	100.0

資料來源：本研究

（四）是否有資訊部門：設有資訊部門的為 134（85.4%），未設資訊部門的為 23（14.6%），如表六所示。

表六　是否有資訊部門統計

是/否	次數	百分比
是	134	85.4
否	23	14.6
合計	157	100.0

資料來源：本研究

表七　資訊部門層級統計

層級	次數	百分比
一級單位	100	63.7
二級單位	27	17.2
三級單位	6	3.8
其他	9	5.7
總數	142	90.4
未填	15	9.6
合計	157	100.0

資料來源：本研究

（五）資訊部門的層級：資訊部門為一級單位者有 100（63.7%），為二級單位者有 27（17.2%），如表七所示。

（六）資訊人員人數：人數在 20-49 人者有 35（22.3%），及 10-19 人者有 32（20.4 %）較多，其餘如表八所示。

八　資訊人員人數統計

人數	次數	百分比
1　2	14	8.9
3　5	23	14.6
6　9	29	18.5
10　19	32	20.4
20　49	35	22.3
50　99	13	8.3
> 100	11	7.0
合計	157	100.0

資料來源：本研究

（七）主要使用何種形式之電腦系統架構：以多使用者之個人電腦區域網路（multi-user PC-LAN）者有 72（45.9%），及大型電腦主機有 36（22.9%）較多，其餘如表九所示。

（八）網際網路連線情形：已建置者 156（99.4%），未建置者 1（0.6 %），如表十所示。

（九）是否有負責資訊安全的部門：是為 103（65.6%），否為 54（34.4%），如表十一所示。

（十）是否有負責資訊安全的人員：是為 129（82.2%），否為 28（17.8%），如表十二所示。

表九　主要使用何種形式之電腦系統架構統計表

系統架構	次數	百分比
大型電腦主機	36	22.9
迷你級電腦	28	17.8
工作站	11	7.0
Multi-user PC-LAN	72	45.9
Single-user PC	10	6.4
合計	157	100.0

資料來源：本研究

表十　網際網路連線情形統計

建置情形	次數	百分比
已建置	156	99.4
未建置	1	.6
合計	157	100.0

資料來源：本研究

表十一　是否有負責資訊安全的部門統計

是/否	次數	百分比
是	103	65.6
否	54	34.4
合計	157	100.0

資料來源：本研究

表十二　是否有負責資訊安全的人員統計

是/否	次數	百分比
是	129	82.2
否	28	17.8
合計	157	100.0

資料來源：本研究

為了解同一構面所有問題之一致性的高低，本研究以 Cronbach's α係數來衡量內部之一致性，其 Cronbach's α係數整理如表十三所示，由該表可知，Cronbach's α值都在 0.8 或 0.9 以上，且均符合信度標準。故各構面之解釋變異差誤的比例能力非常好，表示內部一致性相當不錯，具有高的信度，甚至達到甚佳的程度（Bryman & Cramer , 1997；Gay, 1992）。

二、信度分析

表十三　信度分析表

變　　數	題數	Cronbach's α值
政策之功能定位	5	0.8252
政策之內容	7	0.8722
政策實施項目	13	0.9446
政策建立與維護之程序與方法	13	0.9139
資訊安全的提升	6	0.9317

資料來源：本研究

三、假說檢定

（一）組織特性對資訊安全政策的影響

本研究有關組織特性對資訊安全政策的影響之假說共有六個，其中 H01 組織性質，會影響組織資訊安全政策制定時間，與 H05 資訊組織規模大小，會影響組織是否制定資訊安全政策等兩假說，經檢定結果獲得支持，其餘 H02、H03、H04、H06 等四假說未獲得支持，如表十四所示。

（二）資訊安全政策對資訊安全提昇的影響

本研究有關組織資訊安全政策對資訊安全提昇的影響之假說共有五個，其中 H22 資訊安全政策之功能定位，會影響組織資訊安全之提昇，H23 資訊安全政策之內容，會影響組織資訊安全之提昇，H24 資訊安全政策實施項目，會影響組織資訊安全之提昇，H25 資訊安全政策建立與維護之程序與方法，會影響資訊安全政策之提昇等四假說，經檢定結果獲得支持，

表十四　研究假說之檢定結果摘要表

研　究　假　說	迴歸係數 β	假說檢定結果
H01 組織性質會影響組織資訊安全政策制定時間	0.163*	獲得支持
H02 組織規模會影響組織資訊安全政策制定時間	0.146	未獲支持
H03 組織應用資訊系統的歷史會影響組織資訊安全政策制定時間	0.106	未獲支持
H04 設置資訊部門與層級會影響組織資訊安全政策制定時間	0.122	未獲支持
H05 資訊組織規模小大會影響組織資訊安全政策制定時間	0.181*	獲得支持
H06 使用電腦系統的架構會影響組織資訊安全政策制定時間	0.105	未獲支持
H21 組織資訊安全政策制定時間會影響組織資訊安全之提昇	0.006	未獲支持
H22 資訊安全政策之功能定位會影響組織資訊安全之提昇	0.506***	獲得支持
H23 資訊安全政策之內容會影響組織資訊安全之提昇	0.273***	獲得支持
H24 資訊安全政策實施項目會影響組織資訊安全之提昇	0.443***	獲得支持
H25 資訊安全政策建立與維護之程序與方法會影響組織資訊安全之提昇	0.482***	獲得支持

＊：P<0.05

＊＊＊：P<0.001　　資料來源：本研究

其餘 H21 假說未獲得支持，如表十四所示。

四、因徑分析：

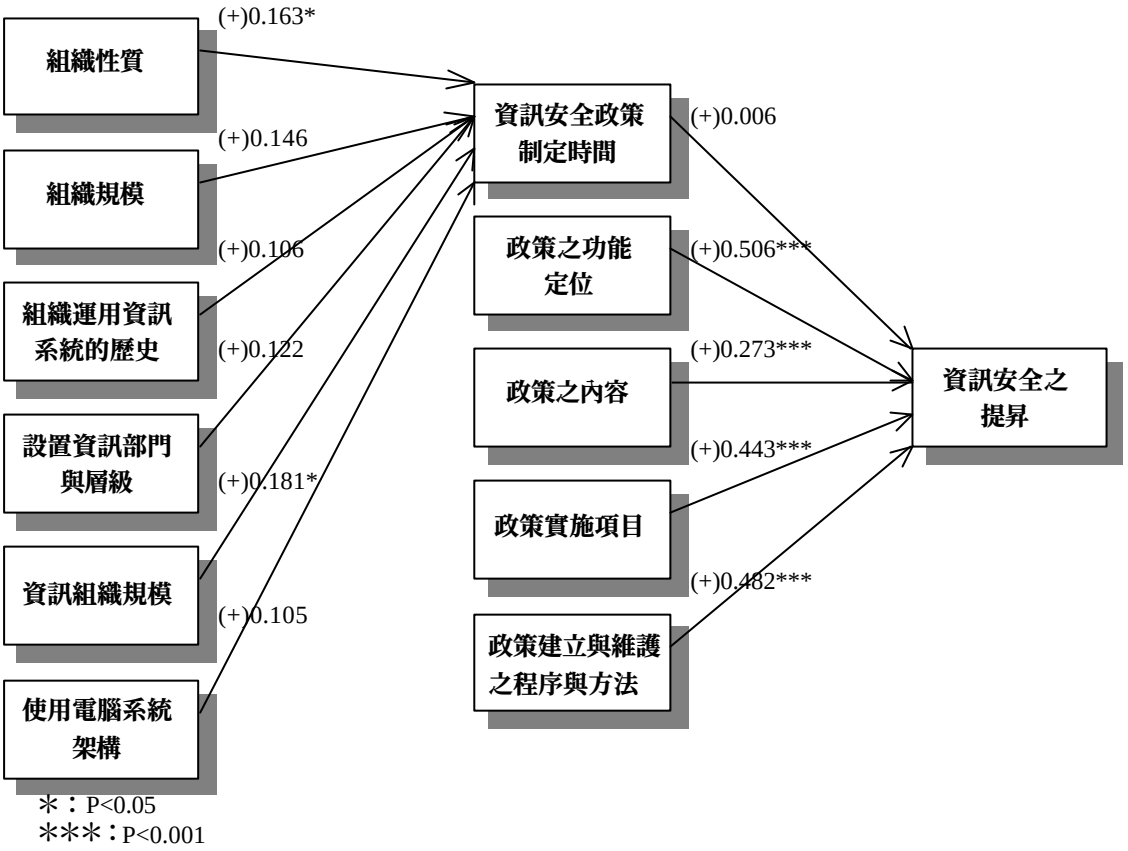
本研究以因徑分析的限制模式（Restricted Model），來分析「組織特性」、「資訊安全政策」與「資訊安全之提昇」各構念之間的關係，其結果如圖五及表十五所示，分別說明如下：

表十五　預測因徑關係的迴歸結果：直接推論條件

預測變數	依變量	R^2	F	b	t
組織性質	資訊安全政策制定時間	0.026	4.189*	-0.163	-2.047*
組織規模	資訊安全政策制定時間	—	—	—	—
組織應用資訊系統的歷史	資訊安全政策制定時間	—	—	—	—
設置資訊部門與層級	資訊安全政策制定時間	—	—	—	—
資訊組織規模	資訊安全政策制定時間	0.033	5.204*	0.181	2.281*
使用電腦系統架構	資訊安全政策制定時間	—	—	—	—
資訊安全政策制定時間	資訊安全之提升	—	—	—	—
政策之功能定位	資訊安全之提升	0.256	53.454***	0.506	7.311***
政策之內容	資訊安全之提升	0.075	12.494***	-0.273	3.535***
政策實施項目	資訊安全之提升	0.196	37.871***	0.443	6.154***
政策建立與維護之程序與方法	資訊安全之提升	0.233	46.425***	0.482	6.814***

＊：P<0.05
＊＊＊：P<0.001

資料來源：本研究



圖五　資訊安全政策因徑模式（資料來源：本研究）

（一）組織性質

分析結果「組織性質」對「資訊安全政策制定時間」有因果效應。換言之，「組織性質」之不同，有政府行政機關、民間企業、公營事業機構、學校及研究機構或其他性質的組織，與「資訊安全政策制定時間」之間有因果關係，亦即因組織性質之不同，而影響該組識資訊安全政策制定時間的早晚。兩者經χ^2檢定結果，亦達顯著水準（P<0.05），顯示政府行政機關已制定資訊安全政策，且制定時間較早之傾向最高，其次為公營事業機構，再次為學校及研究機構，最低者為民間企業，顯示此一結果與政府重視資訊安全，公布資訊安全管理規範，

明文要求各級機關應制定資訊安全政策（行政院，民 88 年），有極密切關係，而民間企業對資訊安全之重視，起步相對較晚。

（二）組織規模

分析結果「組織規模」對「資訊安全政策制定時間」無因果效應。換言之，「組織規模」的大小，與該組織「資訊安全政策制定時間」之間無因果關係，概因「組織規模」的大小，人數之多寡，與組織所面臨的資訊安全威脅程度或資訊風險之高低，未成正相關，與組織「資訊安全政策制定時間」之早晚無因果關係，因此，不會因為「組織規模」的大小而影響組織「資訊安全政策制定時間」。

（三）組織應用資訊系統的歷史

分析結果「組織應用資訊系統的歷史」對「資訊安全政策制定時間」無因果效應。換言之，「組織應用資訊系統的歷史」與組織「資訊安全政策制定時間」之間無因果關係，概因組織應用資訊系統時間的長短，與資訊系統的複雜度，或資訊風險高低未成正相關，因此，不會因組織應用資訊系統歷史的不同，而影響到組織資訊安全政策制定時間的早晚。

（四）設置資訊部門與層級

分析結果「設置資訊部門與層級」對「資訊安全政策制定時間」無因果效應。換言之，「設置資訊部門與層級」與「資訊安全政策制定時間」之間無因果關係。概因，組織設置資訊部門與其層級的高低，與組織所面臨的資訊安全風險未必有關係，因此不會因為組織是否設置資訊部門與資訊部門之層級高低之不同，而影響組織資訊安全政策制定時間的早晚。

（五）資訊組織規模

分析結果「資訊組織規模」對「資訊安全政策制定時間」有因果效應。換言之，「組織資訊人力的多寡」，與組織「資訊安全政策制定時間」之間有因果關係。兩者經 χ^2 檢定結果，亦達顯著水準（$P<0.001$），顯示由於資訊安全威脅許多係來自於組織內部，資訊人員也是最有能力危害資訊安全的人，在許多的研究中均顯示，非授權存取大部分都是來自於組織內部，而資訊人員又擁有比一般的使用者更高的權限及資訊技術能力，也更有機會接觸到敏感性、機密性的資訊，

因此，資訊人員愈多，內部控制制度亦應愈嚴密，對於資訊安全政策之制定愈有需要，則組織愈會儘早制定資訊安全政策，據以實施，以提昇組織的資訊安全水準。

（六）使用電腦系統架構

分析結果，「使用電腦系統架構」對「資訊安全政策制定時間」無因果效應。換言之，「使用電腦系統架構」與「資訊安全政策制定時間」之間無因果關係。亦即不會因為使用大型電腦主機（Mainframe Computer），迷你級電腦（Mini Computer）、Multi-user CP-LAN 或其他電腦系統架構之不同，而影響組織「資訊安全政策制定時間」的早晚。以今日資訊科技環境，任何資訊系統架構都有資訊安全的問題，其組織「資訊安全政策制定時間」之早晚，顯然與其「使用電腦系統架構」為何無關。

（七）制定資訊安全政策時間

分析結果，組織「資訊安全政策制定時間」對組織「資訊安全之提昇」無因果效應。換言之，組織「資訊安全政策制定時間」與組織「資訊安全之提昇」之間無因果關係。此結果與常理判斷似有不同，總認為組織「制定資訊安全政策」，必有助於「資訊安全的提昇」，然而若從以下四項有關資訊安全政策之功能、內容、實施與維護等對「資訊安全之提昇」的因果效應來看，即可知組織徒有「資訊安全政策」，也就是組織制定「資訊安全政策」雖甚早，而未能有效的付諸實施，其內容與程序未能真正符合組織資訊安全所需，恐未必真能促進資訊安全，亦即資訊安全政策「實質上的內容」重於「形式上的有無」與「制定時間的早晚」。

（八）政策之功能定位

分析結果，資訊安全「政策之功能定位」對組織「資訊安全之提昇」有因果效應。換言之，資訊安全「政策之功能定位」與組織「資訊安全之提昇」之間有因果關係。資訊安全政策愈能具備：規範資訊安全範圍、訂定目標與策略、規範各階層之安全責任、宣示未遵守規章的後果、監督執行政策的機制等功能者，對組織「資訊安全之提昇」愈有幫助。

（九）政策之內容

分析結果，資訊安全「政策之內

容」對組織「資訊安全之提昇」有因果效應。換言之，資訊安全「政策之內容」與組織「資訊安全之提昇」之間有因果關係。資訊安全「政策之內容」愈能包含：安全政策目標，安全標準、作業程序之建立與管制，資訊安全與企業營運的結合，資訊安全認知的建立與增進，資訊安全協調與整合，資訊安全政策適用範圍，及資訊安全執行等，對組織「資訊安全之提昇」愈有幫助。

（十）政策實施項目

分析結果，資訊安全「政策實施項目」對組織「資訊安全之提昇」有因果效應。換言之，資訊安全「政策實施項目」與組織「資訊安全之提昇」之間有因果關係。資訊安全「政策實施項目」愈完整，其項目包括：資訊安全政策之制定與修正，資訊安全組織與權責，人員安全管理與教育訓練，資訊資產分類，實體及環境安全，系統規劃與操作安全，資料與媒體安全，通訊與網路安全，存取控制，系統開發與維護安全，業務持續運作管理，資訊安全執行與遵守，資訊稽核等，對組織「資訊安全之提昇」愈有幫助。

（十一）政策建立與維護之程序與方法

分析結果，資訊安全「政策建立與維護之程序與方法」對組織「資訊安全之提昇」有因果效應。換言之，資訊安全「政策建立與維護之程序與方法」與組織「資訊安全之提昇」之間有因果關係。資訊安全「政策建立與維護之程序與方法」愈完整周延，包括：嚴格定義其範圍，高階管理者的支持與核定，進行風險評估或衝擊分析，組織內部各階層的有效溝通及建立安全意識，政策內容的周延與完整，與業務主管部門的溝通與協調，政策的落實執行，政策之定期檢討與修正，當發生重大安全事故的檢討修正，當組織出現新的安全漏洞的檢討修正，當組織或技術基礎結構發生變化時之檢討修正，對資訊安全與工作效率、成本與效益求取平衡等，對組織「資訊安全之提昇」愈有幫助。

陸、結論與建議

本研究係以資訊「安全政策理論（Security Policy Theory)」為基礎，認為組織

透過資訊安全政策（Information Security Policy）之制定、實施與維護的程序，以資訊安全政策為核心，形成資訊安全管理循環，經由資訊安全政策的落實執行，來實現資訊安全之目標。據以建構資訊安全政策模式（Information Security Policy Model），提出十一個研究假說，其中六個假說獲得支持，即企業「組織性質」與「資訊組織規模」大小會影響組織「資訊安全政策制定時間」之早晚（H01，H05）；組織資訊安全「政策之功能定位」、「政策之內容」、「政策實施項目」及「政策建立維護之程序與方法」均會影響組織「資訊安全之提昇」（H22，H23，H24，H25）；但組織「資訊安全政策制定時間」早晚，並不會影響組織「資訊安全之提昇」，顯示資訊安全政策應「重實質」，而「輕形式」。

本研究以資訊「安全政策理論」為基礎，提出安全政策模式，經驗証結果，「組織性質」與「資訊組織規模」兩構念分別與組織「資訊安全政策制定時間」之間有因果關係；資訊安全「政策之功能定位」、「政策之內容」、「政策實施項目」與「政策建立與維護之程序與方法」等分別與組織「資訊安全之提昇」之間有因果關係。因此，組織性質之不同，政府行政機關、公營事業機構，資訊部門規模愈大，愈較早制定資訊安全政策，而組織欲求「資訊安全之提昇」，也應從強化資訊安全「政策之功能定位」、「政策之內容」、「政策實施項目」與「政策建立與維護之程序與方法」等資訊安全政策實質面下工夫，才能見效。

本研究雖力求嚴謹、客觀與周延，然而受限於人力、物力及時間等因素，仍不免有些限制。例如樣本的選擇，本研究直接調查中華民國資訊經理人協會、中華民國資訊應用發展協會的會員，及政府機關資訊主管聯席會議的成員，而未能進行隨機抽樣，因此，可能造成外部效度的降低，進而導致推論能力受到一些影響。

在往後研究方面，本研究建議：

一、在樣本的取得方面，予以採用隨機抽樣，或分層隨機抽樣，以強化研究的外部效度，進而提昇研究的推論能力。

二、在資訊「安全政策理論」的基礎下，擴大研究構念，考量組織行為或領導行為對資訊安全政策的影響，發展更完備的資訊安全政策研究模式，據予進行實証研究，相信會有更多的發現

三、資訊安全尚有「風險管理理論」、「控制與稽核理論」、「管理系統理論」、「權變理論」與「整合系統理論」，可繼續發

展研究模式，據予進行實証研究，對資訊安全管理理論與實務的發展，將會有更大的貢獻。

對實務界的建議：

一、組織為達成資訊安全的目標，應建立資訊安全政策，並經資訊安全政策的制定、實施與評估維護，以提昇組織的資訊安全。

二、資訊安全政策之制定，應重視其政策的實質內容，形式可不必過於計較。

三、組織規模愈大，資訊人員愈多，愈有必要制定資訊安全政策。

參考文獻：.

1. 文茂平、余俊賢「從 Y2K 與供應鏈角度看企業 IT 人員如何推廣資訊安全實例探討」，資訊系統可信賴作業體制研討會論文集，民國 90 年，PP.58-79。
2. 行政院，「行政院及所屬各機關資訊安全管理規範」，民國 88 年。
3. 行政院主計處電子處理資料中心，「九十年度資訊安全稽核報告」，民國 91 年。
4. 李東峰與林子銘，「風險評估觀點的資訊安全規劃架構」，臺灣大學資訊管理學系第十二屆國際資訊管理學術研討會，民國 90 年。
5. 李正源、簡崑鎰譯，「網路安全：在多環境下（Blacharski,D.原著）」，文魁資訊股份有限公司，民國 91 年
6. 吳琮璠，「會計財務資訊系統」，智勝文化事業，民國 91 年。
7. 周文賢，「多變量統計分析：SAS/STAT 使用方法」，待出版書稿，民國 89 年。
8. 林宗瀛，「如何制定企業安全政策」，http://www.sysware.com.tw，民國 91 年。
9. 林清山，「多變項分析統計法」，東華書局，民國 72 年。
10. 林進財、黃旭男、陳　斌，「現代企業資訊安全之研究」，民國 89 年。
11. 林勤經、樊國楨與方仁威，「資訊安全認證與電子化網路社會」，建立我國通資訊基礎建設安全機制標準規範實作芻議研究報告書，經濟部標準檢驗局委託計畫，民國 90 年，PP.80-104。
12. 陳世賢、陳恆鈞，「公共政策」，高鼎文化出版社，民國 90 年。
13. 曾淑惠，「以 BS 7799 為基礎評估銀行業的資訊安全環境」，淡江大學資訊管理學系碩士論文，民國 91 年。
14. 黃承聖，「企業資訊安全的起點－資訊安全政策」，網路通訊，民國 89 年，8

月。

15. 黃姮儀，「台灣地區不同類型金融機構在全球資訊網路安全考量因素之研究」，國立中正大學資訊管理研究所碩士論文，民國 89 年。
16. 萬幼筠，「企業的網路安全控管與風險評估」，會計研究，第 184 期，民國 90 年。
17. 葉啟政，「因徑分析」，社會及行為科學研究法（下冊）－楊國樞等編，東華書局，民國 72 年，PP.859-905。
18. 鄭信一，「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，民國 88 年。
19. Bryman, A. & Cramer, D., *Quantitative Data Analysis with SPSS for windows*, London: Routledge, 1997.
20. BS 7799-1, *Information Security Management-Part1: Code of Practice for Information Security Management , BS 7799-1:1999* , BSI（British Standards Institution）, 1997.
21. Dellecave, T. Jr., "Insecurity: Is Technology Putting Your Company's Primary Asset-It's Information－At Risk? ", *Sales & Marketing Management*, Apr. 1996, PP. 39-50.
22. Fisch, E.A. & White, G.B., *Secure Computers and Networks: Analysis Design, and Implementation*, CRC Press LLC, New York, USA, 1999.
23. Flynn, N.L, *The e Policy Handbook: Designing and Implementing Effective E-Mail, Internet, and Software Policies*, American Management Association New York, USA, 2001.
24. Gay, L.R., *Educational Research Competencies for Analysis and Application*, New York: Macmillan, 1992.
25. Gupta, M., Chaturvedi, A.R., Mehta, S. & Valeri, L., *The Experimental Analysis of Information Security Management Issues For Online Financial Services*, 2001.
26. Hair, Jr. J. F., Anderson, R. E. Tatham, R. L., & Black, W. C., *Multivariate Date Analysis with Reading*, 4thed, Prentice Hall, Englewood Cliffs, New Jersey, USA, 1995.
27. Hinde, S., " Security Survey Spring Corp", *Computer & Security*, Vol.21, Issue: 4, 2002, PP. 310-321.
28. Hitchings, J., "Deficiencies of the Traditional Approach to Information

Security and the Requirement for a New Methodology", *Computer & Security*, Vol.14, No.5, 1995, PP.377-383.

29. Höne, K. & Eloff, J.H.P., "Information Security Policy－What do International Information Security Standards Say? ", *Computer & Security*, Vol.21, Issue: 5, 2002A, PP. 402-409.
30. Höne, K. & Eloff, J.H.P., " What Makes an Effective Information Security Policy", *Network Security*, Vol. 2002 (6), June 2002B, PP. 14-16.
31. ISO/IEC 17799, *Information Technology-Code of Practice for Information Security Management*, 2000.
32. Kabay, M.E., *The NCSA Guide to Enterprise Security*, McGraw-Hill, 1996.
33. Kühnhauser, W.E., "Policy Groups ", *Computer & Security*, Vol.18, No.4, 1999, PP.351 -363.
34. Lindup, K.R., "A New Model for Information Security Policies ", *Computers & Security*, Vol.14, 1995, PP.691-695.
35. Loch, K.D., Carr, H.H. & Warkentin, M.E., "Threats to Information Systems: Today' s Reality, Yesterday' s Understanding", *MIS Quarterly*, June 1992, PP.173-186.
36. Osborne, K., "Auditing the IT Security Function", *Computer & Security*, Vol.17, No.1, 1998,PP. 34-41.
37. Ryan, S.D. & Bordoloi, B. "Evaluating Security Threats in Mainframe and Client/Server Environments", *Information & Management*, 1997, 32, PP.137-146.
38. Starling, G., *Strategies for Policy Marking*, Homewood. IL: The Dorsey Press, 1998.
39. Ward, P. & Smith, C.L., "The Development of Access Control Policies for Information Technology Systems ", *Computers & Security*, Vol.21, No.4, 2002, PP.356-371.
40. **欒志宏，** *How to develop Information Security Policy* **講義**, 2002.

作者簡介

洪 國 興

民國四十三年生，畢業於交通大學管理科學研究所碩士，政治大學資訊管理學系博士班研究，曾任中華民國資訊應用發展協會會長、副會長與資訊經理人協會常務理事，曾任台北市監理處、

台北市政府捷運工程局、考試院等機關之資訊主管、監察院副處長、委員會主任秘書等職務，現任監察院綜合規劃室主任。研究領域為資訊委外、資訊安全。

季 延 平

民國四十一年生，畢業於交通大學海洋運輸學系，政治大學企業管理研究所碩士、美國馬里蘭大學管理博士，現任國立政治大學資訊管理系專任副教授、中華民國資訊應用發展協會理事長、中華民國資訊管理學會與中華 ERP 學會理事。研究領域為資訊策略規劃、企業資源規劃、知識管理等。

趙 榮 耀

民國三十二年生，畢業於台灣大學電機工程學碩士，美國杜克大學電機工程博士，學成返國後任教於淡江大學，經歷工學院教授、院長、副校長、校長等職務，自民國八十二年二月擔任監察委員至今，歷任監察院教育、交通、經濟、外交、等委員會及國際事務、公共工程等小組召集委員。