資訊安全政策實施對資訊安全文化與資訊安全有效性影響之研究

蘇建源
國立中正大學資訊管理學系

江琬瑠
國立中正大學資訊管理學系

阮金聲
國立中正大學資訊管理學系

摘要

隨著組織對資訊化依賴程度愈深，所面對的資訊安全威脅就愈多。組織除了擁有資訊安全技術外更須要一套資訊安全政策供組織有一致的管理標準來遵循。然而許多組織已建立資訊安全政策，還是難以避免許多資訊安全事件發生，究其原因是輕忽安全管理重要性的組織文化。本研究將探討資訊安全政策實施的管理活動與建立資訊安全文化之關係與影響性。針對國內大型企業的資訊主管進行問卷調查並使用結構方程模型進行資料分析。研究結果顯示：

1. 資訊安全教育與宣導、高階主管支持、違反資訊安全規範懲處對資訊安全文化有正向顯著的影響。
2. 資訊安全文化對知覺資訊安全有效性有正向顯著影響。
3. 資訊安全政策維護對制訂資訊安全政策文件有顯著的影響。

關鍵字：資訊安全政策、資訊安全文化、資訊安全有效性

A Study of the Effect of Implementing Information Security Policy on Information Security Culture and Information Security Effectiveness in an Organization

Chien-Yuan Su
Department of Information Management, National Chung Cheng University

Wan-Mei Chiang
Department of Information Management, National Chung Cheng University

Jin-Sheng Roan
Department of Information Management, National Chung Cheng University

Abstract

Organizations nowadays rely highly on the information technology to achieve its daily operation demand. Due to the continual occurrence of many information security incidents, the protection of information systems is a major problem faced by organization. For an organization's information security, it is not only a technical issue but also a management issue. The application of an IS security policy is one of the major mechanisms employed by IS security management.

The purpose of this study is to explore the effect of implementing an information security policy on information security culture and information security effectiveness in promoting the activities about information security policy. According to the large business ranking of top 1000 by China Credit Information Service, Ltd., we conducted a questionnaire survey of the MIS department manager. Structural Equations Modeling (SEM) was applied to analyze the data and the main findings of the study are as follows.

1. The implementation of an information security policy has positive impacts on information security culture.
2. Information security culture has positive impacts on perceived information security effectiveness.
3. The maintenance of an information security policy has positive impacts on making the documents of information security policy.

Key words: Information Security Policy, Information Security Culture, Information Security Effectiveness

壹、緒論

一、研究背景與動機

許多企業為了因應外部競爭與提升其營運績效，紛紛投入大筆資金導入資訊科技於營運流程上。然而，當組織對資訊科技的依賴程度愈深，所面對的威脅就愈多。CSO雜誌、美國密勤局與卡內基美隆大學軟體工程學院的電腦安全應變中心，在2005年針對安全執行者與執法人員進行的調查，結果顯示有88%的受查者認為遭遇到電子犯罪事件增加；而遭遇到電子犯罪事件的受查者中，有55%認為有作業上的損失，28%認為有財務上的損失，12%宣稱有商譽上損失。這意味著組織的資訊安全仍然面臨許多重大考驗，故資訊安全維護已成為當今組織最迫切的課題。

在資訊安全的提倡下，企業紛紛著手建構資訊安全防護網，如：防火牆、入侵偵測系統、防毒軟體等資訊安全技術與設備，來保護組織敏感性資料，然而實際上資訊危安事件仍層出不窮地發生。此外，許多企業投資大筆資金在資訊安全技術與設備上，卻不知如何正確規劃部署與運用並提出一套良好的資訊安全體系與控管機制。美國電腦安全局及聯邦調查局對於電腦犯罪與安全所做的調查發現多數資訊危安事件是由組織內部人員造成。故技術無法解決所有資訊安全問題，組織除了要建構良好的資訊安全技術外，資訊安全管理也是非常重要的一環。資訊安全政策是資訊安全管理中最主要的機制，其提供組織內資訊安全部門與資訊使用部門一套管理標準來引導組織內安全策略的部署方式與可依循的安全策略之作業程序(Höne & Eloff 2002; Kemp 2005)。因此，近年來許多組織大多致力於訂定完備的安全政策且建立良好的安全規範程序與實施資訊安全管理系統。

根據Datapro Research Corporation所做的資通安全發生原因調查發現，完備的安全政策、良好的安全規範程序和資訊安全管理系統的績效並不顯著。究其原因，有52%的事件是由不正確的個人習慣、未遵守相關安全程序以及人為失誤等資訊安全認知不足所產生。故組織在致力在資訊安全政策同時，可經由安全政策建置過程來逐漸形成組織的資訊安全文化來加強人員的資訊安全認知(Karyda et al. 2005)。整體而言，資訊安全文化是組織全體的安全核心價值，以資訊安全政策與上層領導為開端，文化逐漸成形且根植於組織每一個成員的心中並養成安全行為習慣，以達成組織永續經營目標。

在國內外資訊安全的學術研究，資訊安全政策相關文獻多以探討資訊安全政策之制訂、實施內容、評估，但少有關資訊安全政策與文化的實證研究。故本研究欲以實證方式探討組織採行資訊安全政策對資訊安全的影響，包含對於組織資訊安全文化形成與資訊安全有效性的影響。寄望能填補資訊安全政策相關文獻中，組織實施政策後的相關影響探討不足之處。

二、研究目的與問題

根據上述的研究動機，本研究認為組織資訊安全政策的落實是安全管理上的重要議

題，而組織透過何種安全政策之相關管理活動，來形成特定的組織資訊安全文化是探討的重點；並將組織內部推行以增進安全行為的所有管理活動統稱為「資訊安全政策」。因此，本研究希望聚焦於組織導入資訊安全政策與資訊安全文化形成之間的關係與影響性，最後藉由資訊安全文化來探討其對組織的資訊安全有效性具有何影響，以確立文化能夠影響產生正向的安全態度與行為，並有助於資訊安全的成效。此外本研究試圖藉由實證的方式，釐清與瞭解資訊安全政策、資訊安全文化、資訊安全有效性的關係，藉以作為日後組織在推動資訊安全管理制度與發展資訊安全文化之參考依據。故本研究目的為：

（一）探討組織要達成健全的資訊安全管理之要件，以及資訊安全政策對資訊安全管理的重要性及其扮演的角色。

（二）瞭解資訊安全政策目前在國內的發展與意涵。

（三）瞭解資訊安全政策的實施對組織資訊安全文化與資訊安全有效性之間的影響關係。

（四）藉由實證方式對組織資訊安全政策議題的探討，期盼能對國內資訊安全政策後續研究與實務界運作有些許助益。

基於上述研究目的，本研究欲探討的問題如下：

（一）資訊安全政策內涵為何？

（二）探討資訊安全文化的重要性為何？

（三）瞭解資訊安全政策是否會影響資訊安全文化的產生？

（四）瞭解資訊安全文化是否會影響資訊安全有效性？

（五）資訊安全政策是否會間接透過資訊安全文化對資訊安全有效性產生影響？

貳、文獻探討

一、資訊安全政策

Hong et al. (2006)彙集過去有關安全政策的文獻，歸納出安全政策的共同概念而形成了「安全政策理論」(Security Policy Theory)。所謂資訊「安全政策理論」是透過資訊安全政策(Information Security Policy)制定、實施與維護程序並以資訊安全政策為核心所形成的資訊安全管理循環(Information Security Management Cycle)，經由政策的執行以實現資訊安全目標。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並在組織內形成安全共識，政策之制定與實施，之後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之資訊安全的管理程序，如圖1所示。

Wood (1995)認為資訊安全政策是組織高層次的安全目標與策略之一般性宣示。其描繪組織總體性的資訊安全之最高管理方針，並指出組織在整體安全上所要依循的方向，其不涉及如何達成目標之具體實施手段、方法與步驟。資訊安全政策只須對於特殊問題，陳述其概念而不須做太過詳細或冗長的描述(Rees et al. 2003)。資訊安全政策可定義為組織如何管理與保護資訊資源以達到安全目的之規則，並將予以書面化且發佈廣為使

用者所知(Allen 1968)。綜合上述定義，本研究認為資訊安全政策除了是依據組織目標、策略或需求，所形成的資訊安全管理方針外，它也是安全目標與方法的一般性陳述之書面化文件。故凡是可促進資訊安全政策順利推行並使其發揮成效的相關管理活動或實務，例如安全政策宣導、安全教育訓練等，這些為維護資訊安全所採取的控管對策皆為『資訊安全政策』。

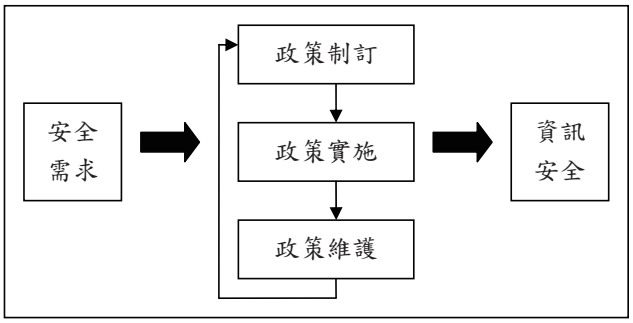

圖1：「安全政策理論」示意圖

(資料來源：Hong et al. 2006)

但如何達成有效實施資訊安全政策，是資訊安全政策研究與實務上重要課題。本研究整理過去學者們曾提及的資訊安全政策，將歸納以下四點，茲說明如下：

（一）制訂資訊安全政策相關文件

資訊安全政策是有關組織資訊安全管理的方針與實作方法之大略性描述。因此組織必須進一步將屬於高層次的資訊安全政策轉為較具體且可被使用與遵循的書面化文件，如制定相關資訊安全規範與資訊安全作業程序手冊等。藉以強力說服員工並建立安全意識，更重要的是能讓員工運用於日常工作實務，作為事務上採取正確的安全行為之判斷根據。Höne 與 Eloff (2002)及Tudor (2001)認為一個有效的資訊安全政策係規範組織成員在存取組織資訊資產所應遵守的規則之正式文件，而在資訊安全政策下則應細訂一套標準的文件集，即資訊安全規範及作業程序，並建立組織對安全行為的明確要求，使組織及其成員有一個安全行為的遵行方向。

（二）實施資訊安全教育與宣傳

Siponen (2000)提出資訊安全政策的成功實施，主要繫於組織是否提供的足夠及適當資訊安全教育訓練，讓成員了解安全政策對組織資訊安全的重要性也強化成員的安全認知，而主動將資訊安全政策規範及規則落實於工作中。Karyda et al. (2005)及Gaunt (1998)的研究中亦指出資訊安全教育與宣導的重要影響，其結果發現有配合資訊安全政策宣導及訓練的組織，其整體成員具備有較高的資訊安全認知，而能遵循相關之安全政策規範，展現正向的安全態度、行為；反之在缺乏相關資訊安全教育訓練的組織，由於組織全體缺乏正確的安全認知，造成政策日後被採用與執行成效有限，也阻礙資訊安全文化的發展。此外Horrocks (2001)和Siponen (2000)指出資訊安全政策推行通常比政策的制

定還因難，由於資訊安全政策的導入對組織而言是一項新項的規則，為了降低可能的衝擊與抗拒，充沛的資訊安全訓練可提供員工對安全政策規範細部的認識與對安全上的認知，有助日後員工辨識潛在安全問題，進一步運用安全法則且降低安全問題所帶來的風險，並形成安全行為與態度並將其融入工作中。

（三）實行違反資訊安全規範的懲處

為了讓組織成員確實遵循資訊安全規範，管理當局應該處分違反資訊安全規範的員工，使其在面臨是否採取安全行為的抉擇時，有所警覺而能採取適當的安全行為，促使員工形成良好的遵循安全規範之風氣。Ford 與 Richardson (1994)指出組織藉由倫理共同規範與獎懲制度來執行，在個人道德決策上有明顯的影響。而Loe et al. (2000)的研究亦發現嚴格的懲處制度會造成員工降低不道德行為。Straub (1990)隨機調查1121個組織發現在建置有效的安全控制措施中，能確實讓所有使用者明瞭違反資訊安全規範可能產生的後果及受到的懲處，能更加提升組織資訊安全的成效。Thomson 與 Von Solms (2005)表示高階主管若體認資訊安全的重要性，便會強力制止可能危害資訊安全之行為，並表明對違反資訊安全規範採取嚴格懲處的安全態度，為組織樹立明確可見的行為準則。雖然組織除訂定明確的違反資訊安全規範懲處條文，但懲處條文的效用乃在管理階層對相關懲處制度的真正落實，方使員工有所警覺，發揮強制約束力，促進組織全體遵循相關安全規範、程序，並塑成員工的安全行為與正確的安全習慣，而有助組織資訊安全文化之形成。

（四）資訊安全政策維護

根據ISO 27001(2005)所公佈的資訊安全管理規範，說明資訊安全政策實行後，應定期檢視與評估現行的安全政策，特別是在組織或資訊系統運作改變，更須注意安全政策是否符合現況而須進行更新。Gupta (1991)和Flynn (2001)指出資訊安全政策即在規劃資訊安全需求，於組織內形成共識並制定與實施政策，之後定期對實施效果加以檢討修正以滿足組織最新安全需求，促進資訊安全的管理程序。資訊安全政策的維護與評估是一個回饋的機制，透過相關的評估維護，來驗證現有安全政策內容是否反映政府法令、外部環境及技術之最新狀況且符合組織目前需求，以確保資訊安全政策與組織實際作業之吻合且合乎時宜。同時，瞭解現有安全政策的使用狀況，發掘安全政策的缺失，作為安全政策修改與改善的依據，並重新形成適合的組織使用的資訊安全政策，讓資訊安全政策更可行而能有效推行(Karyda et al. 2005; Hong et al. 2006)。

綜上所述，本研究認為資訊安全政策包括資訊安全政策相關文件的制定、資訊安全教育訓練與宣導的實施、違反資訊安全規範之懲處以及資訊安全政策維護等四個變數。

二、資訊安全文化

隨著資訊科技普及應用，使得資訊安全成為組織安全上重要的一環，故近年來國外學者開始逐漸探討「資訊安全文化」一詞。Chau (2005)、Kuusisto et al. (2004)和Martins 與 Eloff (2002)皆認為資訊安全文化為組織文化的一環，它指引個人、工作與組織特徵對

組織的安全的影響，故資訊安全文化的發展可以視為如同組織文化產生的過程。上述的定義對於資訊安全文化要素著墨不多，故對資訊安全文化較難有具體的體認而導致難以衡量，但卻指引出資訊安全文化是組織在資訊安全上的共同的觀念也是組織文化的一部份。因此，本研究將整合組織文化以及安全文化的定義來探討資訊安全文化。

Pettigrew (1979)和Ouchi (1981)認為組織文化乃藉由符號、語言、信念、意識型態等形式來影響組織成員的價值觀與行為模式並轉換為成員日常生活中共同的感受與意識。而在安全文化的部分，Glendon 與 Stanton (2000)及Richter 與 Koch (2004)則認為安全文化是成員間彼此共享安全態度、安全價值、安全信念、安全規範及安全實務並引領人們的行為朝向風險與事故之預防。蔡永銘 (2003)則認為安全文化是組織與個人共同建構一個以安全為一切作業核心價值的態度、行為特質與習性。本研究從組織文化與安全文化定義之相關文獻整理出主要元素於表1所示。

表1：組織/安全文化要素表

領域	文獻來源	主要元素					
		信念/意識型態	態度	價值觀	規範	行為	信任與共識的建立
組織文化	Pettigrew (1979); Ouchi (1981)	●		●		●	
	Martin (1992)	●	●	●	●	●	
	林妙雀 (2005)	●		●	●	●	●
	Richard et al. (2009)	●		●	●		
安全文化	Glendon與Stanton (2000)；Richter與Koch (2004)	●	●	●	●	●	
	黃清賢 (2002);蔡永銘 (2003)		●	●	●	●	●
	Fang et al. (2006)	●		●	●		

本研究根據上述多位學者對組織與安全文化定義上之共同要素以及資訊安全文化的定義，整合為本研究對資訊安全文化定義為：「組織成員所共享的資訊安全態度、價值、規範及實務，使資訊安全成為員工日常活動中自然的一面，以此支援所有的活動，建立內外部參與者間之信任」。

在資訊安全文化衡量方，過去有關探討資訊安全文化的文獻中，尚無一致標準的模式與衡量構面，但仍可從部分研究歸納出一些共同構面。Chia et al. (2003)採用了Detert et al. (2000)組織文化模式的概念，試圖以此為基礎來探討組織的資訊安全文化，而整理Andress (2000)、Breidenbach (2000)、Borck (2000)、Conolly (2000)、Hartley (1998)等學者將資訊安全文化歸納為安全政策、風險評估、安全管理、安全認知、安全稽核、人員安全、實體存取控制等構面進行評估。Chaula (2006)則將資訊安全文化分為管理承諾、安全認知、人員管理、風險評估、隱私、倫理、資訊分類、安全保證、未來安全規劃、不確定性避免等構面。Martins 與 Eloff (2002)為了將組織行為融入資訊安全文化概念，使用了Robbins (2001)的組織行為模式，進而建構其資訊安全文化模式，而將資訊安全文化分為組織、群體及個體三個層面，在組織層面包含政策與程序、風險評估以及預算，群體層面包含了管理與信任，個人層面則包含安全認知與倫理規範。

最後，一個不健全的資訊安全文化易產生不良的資訊安全價值，進而導致組織將面臨更多潛在的資訊安全威脅。Vroom 與 Von Solms (2004)認為藉由安全政策規範與程序的落實並建立具體的安全管理制度，方能讓相關作業的資訊安全井然有序且能有效的稽核，並讓員工更能融入安全態度與習慣，進而形成一個對組織與個人有價值的資訊安全文化。因此，提升資訊安全文化的價值之最佳方法就是組織確實實施資訊安全政策。

三、資訊安全有效性

ISO 27001(2005)提到資訊安全的特性是維護資訊的機密性、完整性及可用性。機密性是確保資訊只在被授權的使用者或使用情況下進行存取；完整性是保護資訊與處理方式的正確性與完整性；可用性是指在需要時被授權的使用者能立即取得資訊及相關資產。而這三項攸關組織能否保持競爭優勢與獲利率的重要關鍵。Pfleeger (1996)認為要能達成企業資訊安全控管的目標，必須努力維持企業資訊處理活動及專屬資訊資產的機密性、完整性與可用性。Dhillon 與 Backhouse (2000)認為在人員管理方面，為確保使用者的責任、品德與倫理，以達成相關人士和社會大眾的信任要求，故提出機密性、完整性、可用性、責任、品德、倫理與信任等七項資訊安全主要的控管目標。綜合以上文獻對資訊安全控管目標的探討，本研究認為企業的資訊安全控管目標，是為了維護資訊資產的安全與資訊使用者的正當使用行為，以保障企業與客戶、供應商與社會大眾的權益，不致因為企業管理上的疏忽而受損，同時更是為了建立及維護使用者或客戶對企業的信任關係。

以往在資訊安全研究主要著重在以軟體來偵測資訊安全誤用、預防資訊安全誤用的衡量、資訊安全適當程度的知覺衡量(Goodhue & Straub 1991)以及管理決策制定下的資訊安全規劃模式(Straub & Welke 1998)。除了少數的解釋性研究外(Baskerville & Siponen 2002)，其餘研究大多忽略組織因素。Straub 與 Welke (1998)指出上述研究所採取的客觀衡量可能有失精確性，因為受測對象通常較不願意直接提供實際發生於公司內的資訊安全事件之資料，由於資訊安全對公司企業而言，是具敏感性的問題。許多公司對於提供電腦濫用或資訊安全成效之相關實際數據資料，大多持保留及遲疑的態度，因對其而言，資訊安全是極具敏感性的議題，調查中可能會顯露公司企業內部的資訊安全弱點或漏洞，成為有心人攻擊的目標或影響外部對企業的信任感(Kotulic & Clark 2004; Straub & Welke 1998)。另外，資訊安全相關的實際數據資料如資訊安全事件發生的次數、造成的財務損失等，有些情況是因沒偵測到或沒確實回報發生的安全事件，而無法確保所收集的資料是正確而完整，而造成的損失包含有形及無形亦難以精確地計算，因此，實際上資訊安全數據資料的收集是困難且難以獲得完整而精確之數據(Richardson 2003)。故 Goodhue 與 Straub (1991)則建議採用使用者對資訊安全有效性的主觀判斷及感受等知覺來進行衡量，以取代較不精確的電腦濫用之客觀數據計算。

綜上所述，為了衡量企業的資訊安全控管措施是否有效，本研究將從三項資訊安全目標：機密性、完整性、可用性，來對知覺資訊安全有效性進行操作化的定義，為使用者知覺到組織保護資訊資產不受未授權或蓄意誤用的能力程度。

參、研究方法

一、研究架構推導

本研究根據前述之研究目的與文獻探討中各變數間關係的整理，對各變數間的關係提出以下的研究假說。

（一）資訊安全政策各構面之關係

在資訊安全政策維護與評估方面，其主要為一個回饋的機制。為了解現有資訊安全政策的使用狀況，以發掘安全政策及相關安全作業上的缺失並確定目前的安全政策是否合乎時宜以作為安全政策修改與改善的依據，進而重新形成適合的組織使用的資訊安全政策(Hong et al. 2006; Karyda et al. 2005)。故資訊安全政策的評估與維護是一種持續不斷的改善活動，透過政策的維護可監控組織現有的安全政策是否能因應不斷產生的威脅與漏洞、組織內外部法令變化、環境或技術上的變動，而提供政策檢討與修正的方向以及未來改善的依據。同時，亦可清楚知曉組織所制定之資安全政策文件其不足之處與問題所在且瞭解目前在政策實施上的問題，評估政策及相關安全作業程序能否符合人員實際的工作運作，調整安全政策到最佳可用的狀態，進而提升人員對安全政策的接受度及採用的意願。因此，資訊安全政策的維護對整體資訊安全政策相關文件的完善性有相當的影響。故本研究提出以下假設：

H1：資訊安全政策維護對制定資訊安全政策文件有正向顯著的影響。

（二）資訊安全政策與資訊安全文化

國際間資訊安全管理標準ISO 27001 (2005)對資訊安全政策內容規範，應包含違反資訊安全政策的懲處規定，藉以加強規範員工採取適當的安全行為，養成良好的安全風氣，而進一步塑造出組織的安全文化。Gaunt (1998)、Hancock (2001)、Leach (2003)和Kemp (2005)都認為這些相關的資訊安全政策活動，對於提升員工安全認知是有很大助益，有效促進其在每日工作中落實安全政策規範、安全程序與方法，逐漸營造成組織的資訊安全文化。Hegarty 與 Sims (1979)指出不論是正式或非正式的倫理政策皆會強而有力的影響道德行為。Sims 與 Keon (1999)認為提倡倫理規範，將有助於降低不道德的行為。Loe et al. (2000)的實証研究結果顯示，公司若存有倫理規範並配合懲處制度執行，將有助於增加其員工之道德行為。而Adams et al. (2001)、Farrell 與 Farrell (1998)研究也發現倫理政策下之倫理規範的提倡將會有助於創造企業倫理的文化及增進員工的道德感。因此，組織的政策對文化的形成有一定的影響。

本研究認為資訊安全政策的建置，可為組織提供一套明確可視的資訊安全準則，讓組織所有成員有依循的方向，規範員工形成安全的行為，培養其安全習慣。而藉由與資訊安全政策實施有關之活動，不但強化員工的安全價值，亦驅使員工自然落實安全於日常工作，養成全體具共同的安全意識與展現一致的安全行為之資訊安全文化。因此，本研究認為資訊安全政策長期之下，有利於組織形成與塑造其資訊安全文化。故本研究提出以下假設：

H2：制定資訊安全政策相關文件對資訊安全文化有正向顯著的影響。

H3：實施資訊安全教育與宣傳對資訊安全文化有正向顯著的影響。

H4：施行違反資訊安全規範之懲處對資訊安全文化有正向顯著的影響。

H5：資訊安全政策維護對資訊安全文化有正向顯著的影響。

(三) 資訊安全文化與知覺資訊安全有效性

在組織整體績效或各項資訊活動的成效上，文化具有其一定且的深遠影響力。在IS文獻中亦發現組織文化對新科技的成功採納、資訊政策及管理的有效性、以及資訊系統的成效有所影響(Beachboard 2004; Claver et al. 2001; Tolsby 1998)。Thomson 與 Von Solms (2005)和Vroom 與 Von Solms (2004)也指組織文化會正面影響員工的安全行為，而組織的資訊安全相當依賴員工日常所展現的行為，因此必須明確建立對資訊安全信念及價值認同的文化，以確保員工能採取較適當正確的安全行為。Schein (1992)提出組織文化其功能為型塑成員的共享價值、規範、信念或期待，以確認規範、重要事項、行為與態度及其指導原則，提供成員相似的知覺與認知模式並使其產生同質性的思想與行動，進而提升組織的資訊安全成效。故本研究提出以下假設：

H6：資訊安全文化對知覺資訊安全有效性有正向顯著的影響。

二、研究對象

本研究主要係探討組織資訊安全政策實施後所產生的影響，為達成此研究目的，故本研究將以國內有實行資訊安全政策的企業為對象進行調查。由於國內並無具有資訊安全政策的企業名單可供使用，因此，對象選擇主要針對資訊科技重要程度高的企業，對其而言資訊安全控管為重要的管理議題且這類型企業較可能具備完整的資訊安全政策協助其達成安全控管目標。一般而言，大型企業普遍資訊化程度深，自然對資訊安全的需求及重視程度較高，也較有足夠的資源、金錢、人力來作為資訊安全方面的投資及投入，而調查其相關的資訊安全政策與政策實行的影響也較具可行。有鑑於此，本研究將研究範圍設定為國內的大型企業，並依據中華徵信所出版的國內大型企業名錄，以其2007年所調查的各產業排名為準，依產業別選取製造業排名前500家，服務業排名前500家，及金融業132家，共1132家國內大型公民機構、企業做為研究樣本。

本研究所關注為企業整體的資訊安全政策議題，是屬於組織層級的議題，而資訊部門為資訊安全政策推動及實施的必要參與者，其中資訊主管負責資訊安全政策活動協調規劃，較為熟悉資訊安全政策的運作。由於本問卷的填答者必須要對企業資訊安全政策具有相當的瞭解與認知，因此，將以各企業資訊部門主管為調查對象，並以郵寄的方式，分別對名單中每家企業寄發一份問卷予其資訊主管，進行資料蒐集。

三、問卷設計

本研究之研究變數包括：(1)資訊安全政策；(2)資訊安全文化；(3)知覺資訊安全有效性，依文獻探討，茲將研究變數予以操作性定義並根據過去相關文獻對研究變數之衡

量問項進行設計。本研究問卷之衡量尺度將採用Likert七點尺度由「非常不同意」(1) 到「非常同意」(7)。本研究每一個研究變數的操作性定義、問項數與問項參考來源整理於表2。

表2：研究變數的操作性定義、問項數、問項參考來源

研究變數	操作型定義	問項數	問項參考來源
制訂資訊安全政策相關文件	依據資訊安全政策，進一步細訂清楚且易於了解的資訊安全政策相關說明文件，如使用者應遵守的安全規範或規則、安全作業程序等	4	Glendon 與 Litherland (2001)
資訊安全教育與宣傳	針對組織資訊安全議題所舉辦的相關訓練活動，以宣導資訊安全政策及規範事項，並教導資訊安全工作實務，加強全體之資訊安全意識	8	Knapp (2005)
違反資訊安全規範的懲處	管理當局依據組織所明訂之違反資訊安全規範懲處條文，對違反規定之員工所施予的懲處	4	Knapp et al. (2006)
資訊安全政策維護	為反應環境、技術之變動及符合組織目前的安全需求，而對資訊安全政策、規範及程序所進行的相關檢討評估與更新之工作	6	Knapp (2005)
資訊安全文化	組織成員所共享的資訊安全態度、價值、規範及實務，使資訊安全成為員工日常活動的自然的一面，以此支援所有的活動，建立內外部參與者間之信任	6	Knapp et al. (2006)
資訊安全有效性	使用者知覺到組織保護資訊資產不受未授權或蓄意誤用的能力程度	5	Knapp (2005)

本研究問卷題項發展是由國內外相關研究文獻及學者發展之問卷加以翻譯修訂而成，其翻譯後可能會有語意表達上不符合國內慣用方式或語意不清楚之處，為求嚴謹及確保研究對象瞭解問項意涵，問卷初稿設計完成後，並針對問卷題目的語意、代表性、完整性與相關專家學者討論和審查，以檢驗問卷語意是否完整、清楚、問題是否恰當，是否具代表性。經由反覆修改過後，再進行先導測試，依據前測結果再次修正潤飾問卷問項，確認問卷題意是否清楚且適合受測者填答，並檢驗問卷的信度是否達到Nunnally (1978)所建議的Cronbach's α值需在0.7以上的標準。經由上述的實施過程，其問卷之Cronbach's α值皆大於0.7，故可做為正式問卷之使用。

肆、資料分析

一、回收問卷與樣本結構分析

本研究以中華徵信所2007年出版的國內大型企業名錄為主，分別針對製造業、服務業各選取其排名為前500家之企業，而金融業則選取其全部的132家，以每家企業的資訊主管作為問卷調查研究的對象，共發出1132份。問卷發放一個月之後進行電話催收以增

加問卷回收率，回收共186份，總回收率為16.43%，扣除不願意填寫、填答有遺漏值與明顯亂填的問卷11份，有效問卷為175份，有效問卷回收率為15.46%。由於本研究之研究對象為資訊部門主管，因此在問卷回收方面，本屬不易。目前國內相關之類似研究的郵寄問卷回收率約在15%左右，因此本研究之問卷回收率尚可接受。詳細樣本的敘述性統計如表3所示。

表3：所有樣本基本資料分析

資料項目		樣本	
		人數	百分比
性別	男生	155	88.57
	女生	20	11.43
年齡	30歲（含）以下	10	5.71
	31-35歲	25	14.29
	36-40歲	29	16.57
	41-45歲	56	32.00
	46-50歲	33	18.86
	51歲（含）以上	22	12.57
教育程度	高中職（含）以下	1	0.57
	專科	28	16.00
	大學	86	49.14
	研究所（含）以上	60	34.29
職業	協理/副總	19	10.86
	資訊部門經理/主任/課長/處長/專案經理	93	53.14
	資訊副理/組長	30	17.14
	系統工程師/系統分析師/資料庫管理師	24	13.71
	其它	9	5.14
目前職位年資	1年（含）以下	5	2.86
	2-5年	64	36.57
	6-10年	36	20.57
	11-15年	18	16.00
	16-20年	24	13.71
	21年（含）以上	18	10.29
產業別	製造業	73	41.71
	服務業	66	37.71
	金融業	36	20.57

本研究利用卡方同質性檢定來確定催收前後樣本間是否存有顯著差異，分析結果發現：以產業別而言，結果顯示p值大於0.05，因此在0.05的顯著水準下，表示沒有證據證明有顯著差異存在，故本研究樣本在催收前後並無不同，故具有一定之同質性。同樣的再以各產業之營業額來比較催收前與催收後回收樣本之間是否有顯著差異而結果顯示

對製造業、服務業及金融業三個產業之營業額而言，在0.05的顯著水準下，p值均大於0.05，表示催收前後兩個樣本群體並無顯著差異，而具有一定之同質性，故本研究所回收的樣本有一定程度的代表性。此外，本研究依據研究問卷中的問項，經由獨立樣本T檢定來比較填答內容在前後期的問卷回收的填答差異，藉以瞭解未回收的問卷誤差，以確保回收的問卷具有充分且有效的母體代表性。在0.05的顯著水準下，p值均大於0.05，顯示第一次回收與第二次回收的樣本在每題問項的填答上並無顯著的差異，所以在這二次所回收的樣本，具有一定程度的同質性，可以說是屬於同一個母體中的個體樣本，故本研究所回收的樣本是具有母體代表性。

二、信度與效度分析

在信度方面，本研究採用內部一致性法Cronbach's α作為問卷信度的檢測。本研究量表之信度檢定各構面Cronbach's α係數均達0.9以上，符Guilford (1973)及Nunnally (1978)對Cronbach's α值應大於0.7以上之建議值。顯示本研究量表內部一致性良好，應具有良好之信度。

在效度方面，本研究以收斂效度(Convergent validity)與區別效度(Discriminatory validity)為主要的效度檢測項目。在區別效度方面，根據Fornell 與 Larcker (1981)的建議，研究構面的AVE平方根必須大於該構面與其他構面間的相關係數(Hair et al. 1998)。本研究整理出各構面之AVE平方根和相關係數於表4所示。由表中各構面之AVE平方根均大於該構面和其他構面間的相關係數，故本研究之構面具有良好的區別效度。

表4：區別效度分析表

構面	制定資訊安全政策文件(F1)	資訊安全教育與宣導(F2)	違反資訊安全規範懲處(F4)	資訊安全政策維護(F5)	資訊安全文化(F6)	知覺資訊安全有效性(F7)
F1	0.896					
F2	0.815	0.827				
F4	0.620	0.655	0.910			
F5	0.803	0.807	0.716	0.915		
F6	0.647	0.713	0.743	0.716	0.916	
F7	0.684	0.697	0.635	0.709	0.764	0.910

在收斂效度方面，本研究運用驗證性因素分析 (Comfirmatory Factor Analysis; CFA)來檢驗衡量所有量測問項彼此間的一致性程度。根據Fornell 與 Larcker (1981)、Bagozzi與 Yi (1988)等學者的建議，挑選三項最常用的指標，各指標分述如下：

（一）個別項目的信度(Individual Item Reliability)：考慮每個項目的信度，即每個觀察變數的變異量能被潛在構面所解釋的程度，也就是Loading係數的平方。依據Hair et al. (1998)等學者的建議值，其值應該都在0.5以上。運用Amos進行模式分析時，各觀察變項的信度指標即為R-Square值，分析時以多元相關平方(Squared Multiple

Correlations; SMC)來判斷。SMC值相當於個別變數的信度，本研究中所有觀察變項之SMC值，除了資訊安全教育與宣傳有兩題問項，分別為『貴公司中許多員工尚不知重要的資訊安全政策』與『貴公司員工可以直接在網路上取得資訊安全政策』小於0.5，其餘皆大於0.5，而Bagozzi 與 Yi (1988)認為最佳的SMC值為0.5以上，因此若不足0.5者考慮刪除。故本研究除去這兩題問項後，運用Amos再次進行分析。

（二）潛在變項的組成信度(Composit Reliability; CR)：CR是其所有觀察變項之信度的組成，若CR值愈高，則表示其觀察變項愈能測出該潛在變項。依Fornell 與 Larcker (1981)之建議，如果CR值在0.6以上，則表示衡量指標具有良好的內部一致性。一般而言，其值須大於0.8(Hair et al. 1998)。結果顯示，研究模式各變數的組成信度介於0.928～0.969，都在0.8標準值以上。

（三）潛在變項的平均變異萃取量 (Average Variance Extracted; AVE) ：此乃計算潛在變項之各觀察變項對該潛在變項的平均變異解釋力，若AVE愈高，即表示潛在變項具有愈高信度與收斂效度，依Fornell 與 Larcker (1981)之建議，如果AVE達到0.5以上，則稱為具有收斂效度。結果顯示，本研究各變項之AVE值介於0.684～0.838，皆達0.5以上，表示本研究變項的變異均可由其對應的構面所解釋。

三、研究假說檢測

本研究採用結構方程模式(Structure Equation Modeling; SEM)來檢測研究假說。首先，在模式適配度檢測部分，本研究參照Hair et al. (1998)的建議，挑選適配度標進行研究模式的適配度評估，而評估結果: χ^2/df = 1.94(<3); GFI=0.75(>0.8); NFI=0.87(>0.9); SRMR=0.08(<0.08); RMSEA=0.07(<0.08); NNFI=0.93(>0.9); CFI=0.93(>0.9); IFI=0.93(>0.9); RMR=0.19(>0.08); PNFI=0.81(>0.5); PGFI=0.65(>0.5)，整體而言，綜合各項指標的判斷，雖然部份指標未達良好的程度，但大多接近良好模式的範圍內，顯示本研究模式的整體適配度尚可被接受。

透過前述構面測量模型之收斂效度、區別效度、信度之檢測後，本研究已能確認各研究構面具有一定程度之信度與效度。而通過檢驗模式的整體適合度後，可進一步針對各個構面間的實質關係進行檢測。本研究模式經過驗證性因素分析後，修正模式並利用剩下之測量問項以Amos的路徑分析來進行「制定資訊安全政策文件」、「資訊安全教育與宣導」、「違反資訊安全規範懲處」、「資訊安全政策維護」、「資訊安全文化」、「知覺資訊安全有效性」等六個潛在變項間的關係檢測。

圖2為本研究模式的路徑分析結果，顯示結構模式及構面間之標準化因徑係數，其中R^2則說明了該潛在變項的解釋能力；虛線代表未達顯著水準，實線代表達顯著水準。並經由表5顯示路徑分析結果，以t-value 檢定各因徑係數的顯著性，推論本研究假設是否成立。

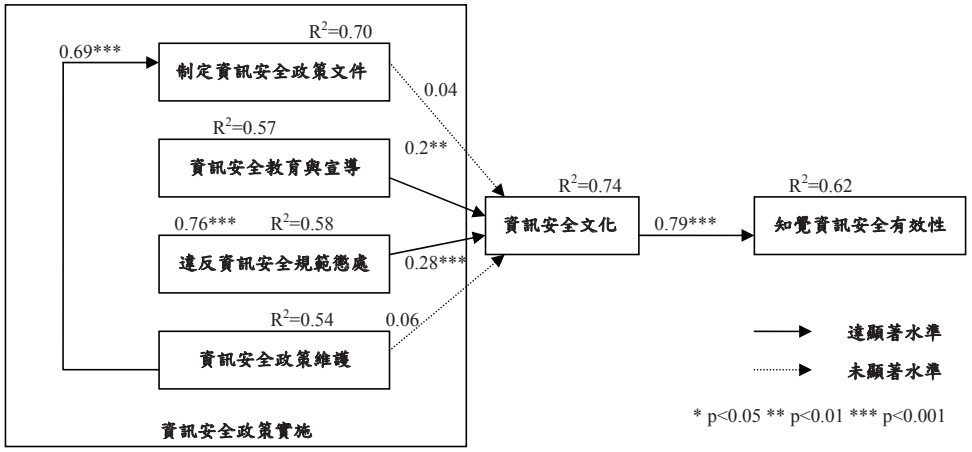

圖2：研究模式因徑分析

表5：假說檢定結果

研究假說	標準化路徑係數	t值	檢定結果
H1：資訊安全政策維護對制定資訊安全政策文件有正向顯著的影響	0.69	8.78***	支持
H2：制定資訊安全政策文件對資訊安全文化有正向顯著的影響	0.04	0.42	不支持
H3：資訊安全教育與宣導對資訊安全文化有正向顯著的影響	0.20	2.27**	支持
H4：違反資訊安全規範懲處對資訊安全文化有正向顯著的影響	0.28	4.06***	支持
H5：資訊安全政策維護對資訊安全文化有正向顯著的影響	0.06	0.68	不支持
H6：資訊安全文化對知覺資訊安全有效性有正向顯著的影響	0.79	13.11***	支持

四、研究結果分析

以下即針對本研究所提出的假設進行檢定後的結果，說明與探討如下：

（一）H1-資訊安全政策維護對制定資訊安全政策文件有正向顯著的影響：

由表5得知資訊安全政策維護對制定資訊安全政策文件間的標準化因徑係數為0.69，t 值為8.78 達到顯著(p<0.001)的統計水準。顯示資訊安全政策維護對組織制定資訊安全政策文件有正向顯著的影響，因此H1獲得支持。此檢定結果與國際資訊安全管標準ISO 27001 的規範是一致。規範明確列示應對資訊安全政策進行維護且資訊安全政策維護的執行愈確實愈能發現組織現存安全政策的問題，並能更瞭解與掌握問題的要點來制定出更適宜組織的資訊安全文件內容。

（二）H2-制定資訊安全政策文件對資訊安全文化有正向顯著的影響：

由表5得知制定資訊安全政策文件對組織內的資訊安全文化間的標準化因徑係數為0.04，t值為0.42未達到顯著(p<0.05)的統計水準，因此研究H2未獲支持。可能原因是資訊安全政策欲發揮效果，首先須仰賴員工對政策的接受及採納。因此，可能還須其他相關

措施的配合，才能強化資訊安全政策文件的作用，如高階主管必須身體力行，表達其實際支持並塑立典範，以激勵員工遵守資訊安全政策的意願。而安全政策訓練與宣導則是增進全體員工的安全意識，協助員工對資訊安全政策之理解，減緩員工對政策實施的衝擊與抗拒感，以避免影響政策日後之採用，造成執行成效有限，而阻礙資訊安全文化的發展。此外，文化的形成是要靠長時間的累積，而資訊安全政策相關文件從制定，中間透過不斷地調整改善，到最後真正被人員所接受採用，而形成組織全體共同的安全規範及行事準則，其中過程是漫長且需時間的蘊釀才能展現其效果，而當中若發展的時間不夠長或不夠成熟，可能使產生的效果有限而不足以對資訊安全文化有所影響。

（三）H3-資訊安全教育與宣導對資訊安全文化有正向顯著的影響：

由表5得知資訊安全教育與宣導對組織內的資訊安全文化間的標準化因徑係數為0.20，t 值為2.27 達到顯著($p<0.01$)的統計水準。顯示組織實施資訊安全教育與宣導對資訊安全文化有正向顯著的影響，因此H3獲得支持。員工的教育訓練是重要的因素，其影響成員對資訊科技的採用態度及資訊科技的建置成效。而運用於資訊安全上，訓練有關的議題主要與提升組織成員的資訊安全意識有相當大的關聯性，係改變員工對資訊安全議題的看法及態度，促使其自然落實安全相關程序、措施於每日工作實務，養成全體具共同的安全意識與展現一致的安全行為之資訊安全文化。

（四）H4-違反資訊安全規範懲處對資訊安全文化有正向顯著的影響：

由表5得知違反資訊安全規範懲處對組織內的資訊安全文化間的標準化因徑係數為0.28，t 值為4.06 達到顯著($p<0.001$)的統計水準。顯示組織施行違反資訊安全規範懲處對資訊安全文化有正向顯著的影響，因此H4獲得支持。施行懲處的主要目的即在使員工明瞭違反規定其後果的嚴重性並導正員工其不適當的安全行為，以強力制止可能危害資訊安全之行為，故為組織建立明確的安全行為準則，形塑員工正確的安全習慣，促進組織全體遵循資訊安全規範之風氣。

（五）H5-資訊安全政策維護對資訊安全文化有正向顯著的影響：

由表5得知資訊安全政策維護對組織內的資訊安全文化間的標準化因徑係數為0.06，t 值為0.68 未達到顯著($p<0.05$)的統計水準，因此H5未獲支持。可能的原因為組織藉由資訊安全政策維護反覆的循環，已能逐漸降低資訊安全政策的缺失並使資訊安全政策相關文件具有一定程度品質。但要使制度有所作用關鍵仍在於全體人員的遵循程度，因此可能需要更多的相關訓練以及上層的推動與監督等多方面配合，以強化組織的安全政策與相關規章的引導與作用力。此外，資訊安全政策維護的循環與調整過程是必須經由長期運行才能顯現其效果。而可能在實行時間還不夠長的情形下，不足以產生明顯的效果，因而可能對於資訊安全文化的影響力亦有所限。

（六）H6-資訊安全文化對知覺資訊安全有效性有正向顯著的影響：

由表5得知違反資訊安全規範懲處對組織內的資訊安全文化間的標準化因徑係數為0.79，t 值為13.11達到顯著($p<0.001$)的統計水準。顯示組織的資訊安全文化對知覺資訊

安全有效性有正向顯著的影響，因此H6獲得支持。資訊安全事件的發生通常是員工缺乏資訊安全意識下與不當的安全行為及習慣所致，因此，資訊安全文化扮演著很重要的角色，其傳遞了組織的資訊安全價值觀及共同的資訊安全行事準則，並影響個人對資訊安全價值的認同。當組織資訊安全文化愈強勢，接受其核心價值觀的成員愈多，其對核心價值觀的承諾也愈高，說明資訊安全文化會影響個人對於資訊安全的看法及表現態度，進一步影響個人對各項資訊安全措施及程度的落實程度，這也關係著組織在的資訊安全所能獲的成效。

伍、結論與建議

一、研究結論與說明

本研究係參考過去資訊安全及管理學相關文獻，整理歸納出資訊安全政策之影響構面並建構資訊安全政策對資訊安全文化與資訊安全有效性影響模式以探討組織實施資訊安全政策後的相關影響。研究對象是以台灣大型企業的資訊主管為問卷實證對象，本研究經由分析與整理後，歸納出以下之結論：

（一）資訊安全政策維護對制訂資訊安全文件方面

本研究的驗證結果，發現資訊安全政策維護對制定資訊安全政策文件有正向顯著影響，當組織內資訊安全政策維護的執行程度愈高，則組織所制定資訊安全政策文件的完善度越高。本研究結果與學者Hong et al. (2006)和Karyda et al. (2005)研究結果相符。資訊安全政策的維護是一個回饋的機制，其反應組織所制定之資安全政策文件中的不足及不合宜之處並進行檢討修正。對於組織在制定資訊安全文件內容，能掌握並瞭解問題的要點，制定出更適合組織全體人員所使用且可接受的資訊安全文件。經由如此不斷地循環改善，能增進組織資訊安全政策相關文件的品質，讓資訊安全政策文件更趨完備，因而資訊安全政策的維護工作對整體資訊安全政策相關文件的完善性有相當的影響。

（二）制訂資訊安全政策文件對資訊安全文化方面

本研究發現制定資訊安全政策文件對資訊安全文化的正面影響，並無達到統計上顯著的支持。本研究結果與Höne 與 Eloff (2002)和Wood (2000)的結果並不一致。Siponen (2000)認為採用資訊安全政策的前提，是伴隨著成功的資訊安全政策實施過程而來的，即透過高階管理實際支持、資訊安全教育與宣傳，來喚起全體對資訊安全瞭解與重視，促使組織成員逐漸形成安全態度與行為，並將資訊安全政策規範落實於工作中。因此，增加員工對相關政策文件的採用度，可能還須高階主管必須表達實際支持及塑立典範、安全政策訓練與宣導等相關措施的同時配合，才能強化資訊安全政策文件的作用。另一方面，增進全體員工的安全意識並減緩員工對政策實施的衝擊與抗拒感，以避免限制日後相關政策文件的採用與執行成效以及阻礙資訊安全文化的發展。此外，資訊安全文化的發展是由資訊安全政策相關文件制定之後，不斷地調整改善到最後真正被人員所接受採用，進而形成組織全體共同的安全規範及行事準則。但由於各個組織的資訊安全政策

實施情況不同，若其是處在初始的階段，可能由於發展的時間不夠長或不夠成熟，其產生的效果有限而不足以對資訊安全文化有所影響。

（三）資訊安全教育與宣導對資訊安全文化方面

在影響資訊安全文化的構面中，資訊安全教育與宣導的正面影響在本研究是獲得驗證的。當組織內的資訊安全教育與宣導實施度愈高，則組織展現的資訊安全文化愈強勢。本研究結果與學者Knapp et al. (2006)所提出之研究結果一致。Simon (1957)將教育歸為是影響組織的一個機制，意即透過相關教育訓練以協助員工將資訊安全工作所需的知識與技巧吸收內化，增進其實際業務的執行並作正確的安全判斷及決策，以達成組織期望的目標。另一方面透過教育訓練的方式，不斷地向員工宣導，使員工了解保護組織資訊的重要性。資訊安全訓練與宣導可以建立員工正確的安全觀念，提升全體員工的安全意識，並協助及促使其確實落實相關的安全控制程序，因而有助組織形成全體注重資訊安全且具備共同的安全之行為、習慣及做事方式，方為組織的資訊安全文化帶來正面的影響。

（四）違反資訊安全規範懲處對資訊安全文化方面

在影響資訊安全文化的構面中，違反資訊安全規範懲處的正面影響在本研究是獲得驗證的，當組織內的違反資訊安全規範之懲處愈確實，則組織所展現出資訊安全文化愈強勢。本研究結果與學者Adams et al. (2001)和Loe et al. (2000)研究結果相同。組織所訂定之違反資訊安全規範懲處條文，可作為規範員工行為的準則，但懲處條文必須透過實際實行才能發揮其作用，因此管理階層應監控、留意員工所發生之錯誤行為，並立即予以糾正並視情況給予適當之懲處，讓全體員工瞭解違反資訊安全規範可能導致的後果而有所警惕，進而能強力約束員工於工作實務中採取適當正確的安全行為。因此，透過施行懲處的方式，能為組織樹立明確可見的行為準則，並規範員工陪養好的安全習慣，而促進組織全體遵循相關安全規範、程序及養成良好安全行為之風氣，有助提升資訊安全文化之價值。

（五）資訊安全政策維護對資訊安全文化方面

本研究發現資訊安全政策維護對資訊安全文化的正面影響，並無達到統計上顯著的支持。本研究結果與Hong et al. (2006)和Karyda et al. (2005)的結果並不一致。資訊安全政策維護的主要作用係藉由持續不斷地由政策制定、實施至維護而形成的完整回饋機制並改善，促使資訊安全政策及相關文件更完善，確保與組織實際運作相符，更為全體人員所適用。Wood (2000)認為即使使用者認知安全政策的存在，卻常常無法以他們想要的方式去應用這些政策。故組織全體對政策、相關文件的採納遵循程度是決定資訊安全制度可否發生效用的因素。因此可能還需要多方面的配合，如提供有關之資訊安全訓練、透過高階管理對資訊安全議題的重視、監督與參與，讓全體人員瞭解資訊安全政策推動及相關文件採行的必要性，亦能使其具備足夠的實行能力協助安全實務的運作並建立起共同資訊安全制度及文化。此外資訊安全政策維護是持續性的工作，藉由不斷的評估、改善、再實施，逐漸降低策上缺失，因此是需要長期運行才能顯現其效果，可能在實行時

間還不夠長的情形下，產生的效果及影響力尚不明顯，而在影響力不夠明顯的情況下，可能無法造成資訊安全政策維護的影響達至顯著。

（六）資訊安全文化對之決資訊安全有效性方面

經由本研究的驗證結果，發現資訊安全文化對知覺資訊安全有效性有正向顯著影響，此結果與學者Knapp (2005)研究結果一致。資訊安全文化是組織全體員工所共用的資訊安全價值觀念和行為準則且為員工思考、採取安全行動的判斷依據。其可引導員工並協助學習，同時亦影響著員工的資訊安全價值與認知，進而能對資訊安全的重要性產生較高的認同感。當員工有較強的信念與價值去達成組織期望的資訊安全目標時，員工會努力落實組織的各項資訊安全措施，故有助組織的資訊安全績效之提升。資訊安全文化雖無形但卻為組織的資訊安全提供一個明確方向，因此企業必須先明確建立對資訊安全信念及價值認同的文化並凝聚更多的資訊安全力量，當組織內所展現出的資訊安全文化愈強勢，則愈能提升組織其資訊安全的有效性。

二、研究貢獻

研究貢獻分成學術研究上的貢獻以及實務上的貢獻，分別描述如下：

（一）學術貢獻

1. 在資訊安全的學術研究多以技術面的研究為主，管理面的研究則少，而就真正研究資訊安全政策的文獻不多，實證研究更少。故本研究可望填補資訊安全政策相關研究之不足，並改善過去資訊安全方面議題大都偏向於技術面之研究，而能增加有關資訊安全管理方面之研究。
2. 在資訊安全政策的文獻大都偏重觀念及概念論述，尚乏實證的研究。因此，經由此實證的方式，能對於組織實施資訊安全政策後可能產生的影響。故對於組織的資訊安全文化或資訊安全有效性之影響，有更清楚的瞭解。同時，對於組織文化影響資訊安全管理成效的原因有更進一步的瞭解。
3. 由於過去的國內研究並沒有對資訊安全政策、資訊安全文化及資訊安全有效性之間的關係進行探討。因此，本研究實證結果的深入探討並提出相關建議，以作為未來相關研究之參考，讓資管領域能有更多人參與此方面議題的探討與研究。

（二）實務貢獻

近幾年的調查研究中發現組織內部的人為因素所造成的資訊安全事件與危害有越來越嚴重的趨勢。而歸咎其中的原因主要係與組織內具有不正確的資訊安全觀念，如認為資訊安全就是資訊安全產品、技術及設備的建置，並未瞭解這些產品技術或設備只是做好資訊安全的其中部分防護，而忽略建立一個良好的資訊安全管理體系及控管機制。因此，透過本研究的實證結果分析與建議，讓企業對資訊安全觀念有更正確的認識進而在資訊安全管理改善及提升上有參考依據。此外，協助企業在資訊安全管理上發展其應著重之目標，即實施資訊安全政策以建構健全的資訊安全管理制度，塑造出成熟的資訊安

全文化且能將安全深植於全體人員心中，成為全體共同一致的安全習慣、共識及準則，進而能有效提升安全意識、持續改進資訊安全管理並達成永續經營之目標。

三、研究限制

本研究雖然力求周延，但受到一些環境、時間和工具的影響，而有未能涵蓋之處。因此，針對本研究不足的地方，提供以下的研究限制，以作為後續研究者未來之探討方向。

（一）衡量工具的限制

由於研究量表係由國外文獻所發展具信效度之量表加以修正發展而來，但基於翻譯過程語意的差異，雖然已求意義完善，但填答者仍可能發生誤解而產生誤答，致使未能反應填答者的真正情況，使結果產生偏差。

（二）研究議題的敏感性

資訊安全在企業中目前還是一個相當敏感的議題，這也可能造成問卷填答上面無法真實反應現況的情形出現。此外，在進行電話催收與許多企業接觸的過程中，由於許多企業認為本研究為資訊安全議題，可能涉及企業的機密資料且恐有外洩之疑慮，因此不願意填答，而致使問卷回收的情況不甚良好。

（三）問卷回收率的限制

本研究礙於研究對象之問卷回收不易以及研究議題敏感性等因素影響下，所回收的研究樣本稍顯不足。由於本研究所提出的結構模式所需的估計參數不少，所以在進行研究模式分析時，少部份的模式適配度未達到要求標準值。如果能多增加問卷回收數，將可使研究模式適配度指標更加完善。而本研究以製造、服務及金融產業作為研究對象，但樣本數目仍未達到可以研究三種產業之規模，使本研究無法就個別產業來建立分析模型進行比較，以瞭解個別產業對於整體模式是否有差異。

（四）時問縱斷面的改變

企業的資訊安全並非一夕能達成，但在實證研究上，受到時間上的限制，無法以縱斷面(Longitudinal)的研究方式來收集資料以探討變項間的因果關係，因此只能針對企業目前的實際情況來進行觀察、分析與討論，屬於單一時點的橫斷面(Cross Section)研究，而無法瞭解長時間過程中各個變項的變化，也不能比較出企業在實施資訊安全政策控管活動前後在資訊安全文化及資訊安全有效性上的差異，因此本研究的資料可能產生在時間上的偏差。

（五）研究一般化的限制

由於本研究的樣本主要是針對台灣地區的大型企業，若是要將本研究結果一般化至其他中小型企業，可能會有因企業規模不同而產生不易推論的情況。此外，本研究對象是大型企業之資訊主管，若主管不願配合時，樣本將無法取得，因此可能導致企業的產

業類別並未平均分佈，對於研究結果推論至所有產業類別的一般化能力可能會有所限制。

四、未來研究方向與建議

對後續學術研究與業界實務上，本研究提出在研究上方向與實務上建議：

（一）學術研究上的建議

1. 探討其他可能的影響因素：本研究實證結果雖然發現各構念間幾乎都具有顯著之相關影響結果，但仍有一些殘餘解釋空間，顯示可能有其它因素會對這些構念產生影響。例如，考量組織行為或領導行為對資訊安全政策的影響等。另外，也可能尚有其他因素影響資訊安全的有效性，如產業類型、組織規模或者資訊系統類型等，值得後續研究者更深入去探討。而目前資訊安全管理相關文獻相較於其他研究領域稍顯不足，未來的研究可依此為基礎據予進行更多相關的實證研究，致使本研究模式能更趨於完整。
2. 配合個案研究：由於受到時間及對象的限制，本研究只進行了實證性的研究，雖然可以藉由資料分析來推論出相關結論，但並無針對公司內部的實際狀況作一對照，所以在理論與實證結果的印證上略嫌薄弱，因此後續研究者，可以搭配「質性研究」作為結果相互應證工具，例如：實地深度訪談，來使研究內容更為完整並使研究結果更具說服力。
3. 採用更佳的衡量方式：本研究對各構面所採用的衡量方式係採用對象的主觀知覺程度為依據，而後續的研究，對於資訊安全有效性構面，在有良好的研究條件許可下，可採用實際客觀的資訊安全績效數據。例如，資訊安全事故發生次數、資訊安全事故損失等，以減少因為事後回溯造成的偏差或對象主觀判斷的影響。
4. 進行縱斷面研究：本研究僅就現階段採橫斷面的研究，所獲得的資料僅能瞭解各變項在某一時期的影響情形，因此建議後續研究者可採縱斷面的研究方法。針對企業進行長期的研究觀察其資訊安全政策活動落實及發展程度以及實施前後其資訊安全文化及資訊安全有效性的變化。因此由資訊安全政策實施前後分別進行施測或訪談，以獲取各變項的變化趨勢並進一步瞭解驗證變項間的真正因果關係。

（二）實務管理上的建議

1. 實施資訊安全教育訓練與宣傳：隨著企業組織的資訊化，參與和涉及企業資訊的人也增多，故突顯出人員安全管制的重要。雖然資訊安全政策文件是管理人們的最佳工具，但不應該讓政策文件只是形式上的條約。企業應須多辦理資訊安全相關的教育訓練與宣傳，使員工瞭解資訊安全的概念及重要性、培養及加強員工的資訊安全意識、協助員工如何於未來工作業務中確實執行相關安全程序與措施。因此，良好的安全訓練不僅能提升員工的資訊安全價值及水準，更能使員工有強烈的意願去落實組織的資訊安全。
2. 確立組織資訊安全之相關罰則：資訊安全事件的發生通常是員工缺乏資訊安全意

識，而未遵守資訊安全政策及採取適當安全程序與措施所致。許多企業雖已訂定違反資訊安全規範之懲處條文以作為員工行為的規範，但僅止於此是不夠的。員工通常都被動的，最有效的方式還是須仰賴管理階層確實執行這些相關罰則，否則這些懲處條文可能如同虛設。如果管理階層能監督員工行為，在錯誤發生時能立即糾正並施予適當之懲處，則全體員工才能真正瞭解違反資訊安全規範的後果，並促使員工採行適當的安全行為，為組織樹立明確可見的行為準則。

參考文獻

1. 林妙雀，2005，『企業之智慧資本與分享組織文化對組織管理績效影響之實證研究』，管理評論，第24卷．第一期：55～81頁。
2. 黃清賢，2002，職業安全管理，台北：新文京開發出版社公司。
3. 蔡永銘，2003，現代安全管理，台北：揚智文化事業公司。
4. Adams, J. S., Tashchian, A., and Shore, T. H.“Codes of Ethics as Signals for Ethical Behavior,”*Journal of Business Ethics* (29:3), 2001, pp. 199-211.
5. Allen, B.“Danger Ahead! Safeguard Your Computer,”*Harvard Business Review* (46:6), 1968, pp. 97-101.
6. Andress, M., and Fonseca, B.“Manage People to Protect Data,”*InfoWorld* (22:46), November 2000, p. 48.
7. Bagozzi, R. P., and Yi, Y.“On the Evaluation of Structural Equation Models,”*Journal of the Academy of Marketing Science* (16:1), 1988, pp. 74-94.
8. Baskerville, R., and Siponen, M.“An Information Security Meta-Policy for Emergent Organizations,”*Logistics Information Management* (15:5), 2002, pp. 337-346.
9. Beachboard, J. C.“Conceptualizing IT Management: Testing a Competing Values Model of Policy Compliance,”in *Proceedings of the Tenth Americas Conference on Information Systems*, New York, 2004.
10. Borck, J. R.“Advice for a Secure Enterprise: Implement the Basics and See that Everyone Uses Them,”InfoWorld (22:46), November 2000, p. 90.
11. Breidenbach, S.“How Secure Are You?”*InformationWeek* (800), August 2000, pp. 71-78.
12. Chau, J.“Skimming the Technical and Legal Aspects of BS7799 Can Give a False Sense of Security,”*Computer Fraud & Security*, September 2005, pp. 8-10.
13. Chaula, A. J.“A Socio-Technical Analysis of Information Systems Security Assurance: A Case Study for Effective Assurance,”Doctoral Dissertation, Department of Computer and Systems Sciences, Stockholm University, 2006.
14. Chia, P. A., Maynard, S. B., and Ruighaver, A. B.“Understanding Organizational Security Culture,”*Information Systems: The Challenges of Theory and Practice*, Information

Institute, United States of America, 2003, pp. 335-365.
15. Claver, E., Llopis, J., Gonzalez, M. R., and Gasco, J. L. "The Performance of Information Systems through Organizational Culture," *Information Technology & People* (14:3), 2001, pp. 247-260.
16. Conolly, P. J. "Security Starts from Within," *InfoWorld* (22:28), July 2000, pp. 39-40.
17. Detert, J. R., Schroeder, R. G., and Mauriel, J. J. "A Framework for Linking Culture and Improvement Initiatives in Organizations," *The Academy of Management Review* (25:4), 2000, pp. 850-863.
18. Dhillon, G., and Backhouse, J. "Information System Security Management in the New Millennium," *Communication of the ACM* (43:7), 2000, pp. 125-128.
19. Fang, D.P., Chen, Y., and Louisa, W. "Safety Climate in Construction Industry: A Case Study in Hong Kong," *Journal of Construction Engineering and Management* (132: 6), 2006, pp. 573-584.
20. Farrell, H., and Farrell, B. J. "The Language of Business Codes of Ethics- Implications of Knowledge and Power," *Journal of Business Ethics* (17:6), 1998, pp. 587-601.
21. Flynn, N. L. *The E-Policy Handbook: Designing and Implementing Effective E-Mail, Internet, and Software Policies*, American Management Association, New York, 2001.
22. Ford, R. C., and Richardson, W. D. "Ethical Decision Making: A Review of the Empirical Literature," *Journal of business ethics* (13:3), 1994, pp. 205-221.
23. Fornell, C., and Larcker, D. F. "Structural Equation Models with Unobservable Variables and Measurement Error," *Journal of Marketing Research* (18:3), 1981, pp. 382-388.
24. Gaunt, N. "Installing an Appropriate Information Security Policy," *International Journal of Medical Informatics* (49:1), 1998, pp. 131-134.
25. Glendon, A. I., and Litherland, D. K. "Safety Climate Factors, Group Differences and Safety Behavior in Road Construction," *Safety Science* (39:3), 2001, pp. 157-188.
26. Glendon, A. I., and Stanton, N. A. "Perspectives on Safety Culture," *Safety Science* (34:1-3), 2000, pp. 193-214.
27. Goodhue, D. L., and Straub, D. W. "Security Concerns of System Users: A Study of Perceptions of the Adequacy of Security," *Information & Management* (20:1), 1991, pp. 13-27.
28. Guilford, J. P. *Fundamental Statistics in Psychology and Education* (5th ed.), McGraw-Hill, New York, 1973.
29. Gupta, Y. P. "The Chief Executive Officer and the Chief Information Officer: The Strategic Partnership," *Journal of Information Technology* (6:3-4), 1991, pp. 128-139.
30. Hair, J. F., Anderson, R. E., Tatham, R. L., and Black, W. C. *Multivariate Data Analysis* (5th ed.), Prentice Hall, Englewood Cliffs, 1998.
31. Hancock, B. "The Chief Security Officer's Top Ten List for 2001," *Computers & Security* (20:1), 2001, pp. 10-14.

32. Hartley, B.“Ensure the Security of Your Corporate Systems (Developing a Security Policy),”*E-Business Advisor* (16:6), 1998, pp. 30-32.
33. Hegarty, W. H., and Sims, H. P.“Organizational Philosophy, Policies, and Objectives Related to Unethical Decision Behavior: A Laboratory Experiment,”*Journal of Applied Psychology* (64:3), 1979, pp. 331-338.
34. Höne, K., and Eloff, J. H. P.“Information Security Policy－What Do International Information Security Standards Say?”*Computers & Security* (21:5), 2002, pp. 402-409.
35. Hong, K.S., Chi, Y.P., Chao, L.R., and Tang, J.H.“An Empirical Study of Information Security Policy on Information Security Elevation in Taiwan,”*Information Management & Computer Security* (14:2), 2006, pp. 104-115.
36. Horrocks, I.“Security Training: Education for an Emerging Profession?”*Computers & Security* (20:3), 2001, pp. 219-226.
37. ISO ISO/IEC 27001:2005, International Organization for Standardization, Switzerland, 2005.
38. Karyda, M., Kiountouzis, E., and Kokolakis, S.“Information Systems Security Policies: A Contextual Perspective,”*Computers & Security* (24:3), 2005, pp. 246-260.
39. Kemp, M.“Beyond Trust: Security Policies and Defence-in-Depth,”*Network Security* (8), 2005, pp. 14-16.
40. Knapp, K. J.“A Model of Managerial Effectiveness in Information Security: From Grounded Theory to Empirical Test,”Doctoral Dissertation, Auburn University, 2005.
41. Knapp, K. J., Marshall, T. E., Rainer, R. K., and Ford, F. N.“Information Security: Management's Effect on Culture and Policy,”*Information Management & Computer Security* (14:1), 2006, pp. 24-36.
42. Kotulic, A. G., and Clark, J. G.“Why There Aren't More Information Security Research Studies,”*Information & Management* (41:5), 2004, pp. 597-607.
43. Kuusisto, R., Nyberg, K., and Virtanen, T.“Unite Security Culture: May a Unified Security Culture be Plausible?”in *Proceedings of the Third European Conference on Information Warfare and Security*, United Kingdom, 2004, pp. 221-229.
44. Leach, J.“Improving User Security Behaviour,”*Computers & Security* (22:8), 2003, pp. 685-692.
45. Loe, T. W., Ferrell, L., and Mansfield, P.“A Review of Empirical Studies Assessing Ethical Decision Making in Business,”*Journal of business ethics* (25:3), 2000, pp. 185-204.
46. Martins, A., and Eloff, J.“Promoting Information Security Culture through an Information Security Culture Model,”in *Proceedings of South Africa: Information Security South Africa*, 2002.
47. Martin, J. *Cultures in Organizations: Three Perspectives*, Oxford University Press, New York, 1992.

48. Nunnally, J. C. Psychometric Theory (2th ed.), McGraw-Hill, New York, 1978.
49. Ouchi, W. G. *Theory Z: How American Business Can Meet the Japanese Challenge*, Addison-Wesley, 1981.
50. Rees, J., Bandyopadhyay, S., and Spafford, E. H. "PFIRES: A Policy Framework for Information Security," *Communications of the ACM* (46:7), 2003, pp. 101-106.
51. Pettigrew, A. M. "On Studying Organizational Culture," *Administrative Science Quarterly* (24:4), 1979, pp. 570-586.
52. Pfleeger, C. P. *Security in Computing* (2nd ed.), Prentice Hall, New Jersey, 1996.
53. Richard, O. C., McMillan-Capehart, A., Bhuian, S. N., and Taylor, E. C. "Antecedents and Consequences of Psychological Contracts: Does Organizational Culture Really Matter?" *Journal of Business Research* (62:8), 2009, pp. 818-825.
54. Richardson, R. *Eighth Annual Computer Security Institute (CSI) and Federal Bureau of Investigation (FBI) Computer Crime and Security Survey*, Computer Security Institute, San Francisco, 2003.
55. Richter, A., and Koch, C. "Integration, Differentiation and Ambiguity in Safety Cultures," *Safety Science* (42:8), 2004, pp. 703-722.
56. Robbins, S. P. *Organizational Behavior: Concepts, Controversies, Applications* (9th ed.), Prentice Hall, New Jersey, 2001.
57. Schein, E. H. *Organizational Culture and Leadership* (2nd ed.), Jossey-Bass, San Francisco, 1992.
58. Simon, H. A. "Amounts of Fixation and Discovery in Maze Learning Behavior," *Psychometrika* (22:3), 1957, pp. 261-268.
59. Sims, R. L., and Keon, T. L. "Determinants of Ethical Decision Making: The Relationship of the Perceived Organizational Environment," *Journal of Business Ethics* (19:4), 1999, pp. 393-401.
60. Siponen, M. T. "A Conceptual Foundation for Organizational Information Security Awareness," *Information Management & Computer Security* (8:1), 2000, pp. 31-41.
61. Straub, D. W., and Welke, R. J. "Coping with Systems Risk: Security Planning Models for Management Decision Making," *MIS Quarterly* (22:4), 1998, pp. 441-469.
62. Straub, D. W. "Effective IS Security: An Empirical Study," *Information Systems Research* (1:3), 1990, pp. 255-276.
63. Thomson, K. L., and Von Solms, R. "Information Security Obedience: A Definition," *Computer & Security* (24:1), 2005, pp. 69-75.
64. Tolsby, J. "Effects of Organizational Culture on a Large Scale IT Introduction Effort: A Case Study of the Norwegian Army's EDBLF Project," *European Journal of Information Systems* (7:2), 1998, pp. 108-114.
65. Tudor, J. K. *Information Security Architecture: An Integrated Approach to Security in the Organization*, CRC Press, Boca Raton, 2001.

66. Vroom, C., and Von Solms, R. "Towards Information Security Behavioral Compliance," *Computers & Security* (23:3), 2004, pp. 191-198.
67. Wood, C. C. "An Unappreciated Reason Why Information Security Policies Fail," *Computer Fraud & Security* (2000:10), 2000, pp. 13-14.
68. Wood, C. C. "Writing InfoSec Policies," *Computers & Security* (14:8), 1995, pp. 667-674.