企業之資訊安全策略與其產業別及資訊化程度關係探討

葉桂珍
成功大學企業管理學系

張榮庭
成功大學企業管理學系

摘要

資訊系統的複雜化雖然為企業帶來可觀的效益，同時也帶來風險。有鑑於此，許多學者紛紛提出維護企業資訊安全的方法及相對因應策略(如 Rainer et al.1991; Straub & Welke 1998; von Solms et al. 1994; Ølnes 1994)。這些理論與方法雖然提供企業不少資訊安全解決之道，但多數未考慮企業自身屬性，如產業別或資訊化程度等，在擬定資訊安全策略上之重要性。然而，針對企業屬性適當地制定經營策略，是企業經營上不可避免的要點。本研究目的即在探討不同產業型態及資訊化程度之企業對資訊風險的看法，包括資訊風險對目前及未來產業之可能威脅，以及這些產業所採取之相對防護策略與措施等，以瞭解台灣不同產業間在擬定資訊安全策略上之適當性。

關鍵字：資訊安全、資訊風險、資訊安全策略、資訊化程度

Information Security Strategy to Businesses in Different Sectors and Computerization Levels

Quey-Jen Yeh
Department of Business Administration, National Cheng Kung University

Arthur Jung-Ting Chang
Department of Business Administration, National Cheng Kung University

Abstract

As businesses become increasingly dependent on information systems for strategic operations, the issues of information security emerge. Many MIS researchers (e.g., Rainer et al. 1991; Straub & Welke 1998; Von Solms et al. 1994; and Ølnes 1994) have proposed theories and practices against information risks. While useful solutions were provided, seldom have considered associations of business information security strategy with the industrial sector and the computerization level. The purpose of this paper is to construct the feasible information security strategy that identify the protections required to avoid the information risks. Through comparing the perceived seriousness of the potential information risks with the degree of preparation against them, and with the perceived trend of information risk in the future, main information risks are inferred for businesses in different sectors and computerization levels. Organizations must become aware of these critical areas and ensure that the appropriate security measures are implemented to reduce the possibility of loss.

Keywords:Information Security, Information Risk, Information Security Strategy, Level of computerization

壹、緒論

企業對資訊科技的應用有愈來愈依賴的趨勢，從早期作業流程自動化、支援管理活動及決策活動，一直到目前支援各種企業策略的資訊系統。系統的複雜化雖然為企業帶來可觀的效益，但同時也提高資訊風險(Information Risk)。所謂資訊風險乃指「資訊資產可能遭受的威脅」，這些資訊資產包括資料、硬體、軟體、人員、及設備等(Rainer et al. 1991)。Loch et al.(1992)曾指出，MIS 主管雖不斷引用新的資訊科技，但對新資訊科技與資訊安全的間隙卻沒有採用相對應措施，以致造成企業更大威脅。Vermeulen & von Solms (2002)則強調今日的電腦安全問題已迥異於以往；「資訊」(Information)，尤其是對企業經營有用的資訊，已躍升為企業資訊安全(Information Security)上之主角。就如 von Solms (1996)所言，過去的資訊安全強調的是實體安全、資料備份，但是在今日，企業之資訊安全重點已移轉到資訊安全之認知、資訊安全標準之遵循、以及資訊安全策略與政策之制定等非實體面問題。

不少學者，如 Goodhue & Straub(1991)、Kankanhalli et al.(2003)、Jung et al.(2001)等，曾指出組織及產業特性是影響資訊安全的重要因素。不同的產業有不同的資訊需求，比如傳統製造業、流通服務業等通常較重視資訊之可用性(Availability)，高科技產業較重視資訊之機密性(Confidentiality)，而金融服務業則較重視資料之完整性(Integrity)(Jung et al. 2001)。資訊可用性僅須確保資料不遺失，能維持系統的運作即可，其風險性較低；然而資訊機密性及完整性須分別確保資料不被揭露、不被篡改，其風險相對較高。換言之，不管風險是來自系統面(如軟硬體、資料、網路)或管理面(如實體、人為、法律)，企業之資訊風險會因其產業之特性而異。

企業之資訊化程度亦是一企業考量其資訊安全方向的重要因素。一直以來，組織之資訊化程度即隨著資訊科技之成長及其資訊應用層次，如作業、管理、決策、及策略等層次，之提升而改變。許多學者(如 Nolan 1979; Earl 1989; Galliers 1989; Galliers & Sutherland 1991 等)即曾提出資訊科技階段性成長之相關理論及實證研究，並描述組織在不同資訊化程度下的資訊特徵。其中，Galliers & Sutherland(1991)從 7 個 S 角度來闡述資訊科技之成長模式，他們認為企業之資訊化會隨著資訊策略、資訊部門結構、資訊系統架構、以及資訊應用領域而改變。可預期的是，此四項資訊應用特徵之改變，將直接或間接影響資訊風險的變化。另外，Loch et al.(1992)及 Ryan & Bordoloi(1997)等學者的研究亦顯示，資訊風險會隨著資訊系統架構而變化；他們分別以問卷調查不同資訊系統架構下之各項資訊風險，其研究結果雖有不同，共同的結論是，企業的風險與威脅會因其資訊化程度而異；其並建議組織在擬定資訊防護重點或方向時，應隨著其資訊科技之成長而不斷調適。

多位資訊學者紛紛提出不同之理論模式以解決組織之資訊風險問題，例如 Rainer et al.(1991)、Straub & Welke(1998)、以及 Birch & Mcevoy(1992)等學者，分別提出不同的資訊風險分析程序，協助組織了解其內部資訊風險；von Solms et al.(1994)發展資訊安全管理模式(ISM^2)，將資訊安全作業分為五個高低層次，提供組織執行資訊安全依

據；Ølnes(1994)亦提出資訊安全策略與政策制定的方法，協助組織如何有系統地建立其可行資訊安全政策；Fitzgerald(1995)、Kwok & Longley(1999)、von Solms(1999)、Eloff & von Solms(2000)、以及 Siponen(2002)等學者，則強調應藉由資訊安全國際標準發展組織內部資訊安全標竿，或協助組織擬定資訊安全政策。上述研究雖然提出不少解決企業資訊安全之途，但並未針對企業產業特性與資訊化程度提出適當之相對因應策略。所謂「資訊安全策略」是組織資訊安全的著重方向及指導原則(Pipkin 2000)。本文的目的即在以問卷調查方式，探討不同產業型態及資訊化程度之企業對目前及未來資訊風險之看法，以及其所採取或擬採取之相對防護措施；透過專家認知與現況差距分析，擬出組織之可行資訊安全策略方向。主要研究包括—

(一) 探討「產業型態」與組織資訊安全之關聯性—主要擬驗證產業間之特性與差異性對企業資訊安全策略之影響。理論上，不同產業別企業強調相異之資訊需求，對資訊可用性、機密性、及完整性三項安全需求的重視比例不同，這些差異同時造成組織資訊風險組合有所區別，進而影響資訊安全的策略規劃。

(二) 探討「資訊化程度」與組織資訊安全之關聯性—主要擬驗證資訊化程度對企業資訊安全策略之影響，包括不同資訊化程度者間應強調之方向，比如資訊化程度較低者是否應較強調基本面或作業面，如網路風險之防護；資訊化程度較高者是否除提高基本防護外，亦應深思資訊安全政策與風險轉嫁等高階資訊風險策略等。

(三) 由「產業型態」及「資訊化程度」兩個角度，擬出組織可行資訊安全之策略方向—主要透過問卷調查結果，擬出不同「產業型態」及「資訊化程度」企業的資訊需求特色、主要威脅來源的資訊風險、資訊安全防護現況、未來資訊風險趨勢的移轉、以及資訊安全策略的重點方向。

貳、文獻探討

一、何謂「資訊風險」？

如前述，「資訊風險」指資訊系統運作時的不可靠程度，亦即組織運用資訊科技時的不確定性或負面威脅。Rainer et al.(1991)將資訊風險定義為「易受外力威脅的資訊資產」，亦即一資訊資產的弱點所可能引發的各種威脅(Vulnerabilities to Threat)；因此，資訊風險分析必須同時兼顧資訊資產價值、資訊資產的弱點、以及資訊承受威脅三者之確認及分析。過去很多學者對「資訊風險」有不同的分類標準。Icove et al.(1999)由資訊資產保護的角度解釋資訊風險，他認為常見的「資訊風險」包括實體風險、軟體風險、硬體風險、資料風險、通訊風險、人為風險、管理相關風險等。Fitzgerald(1995)歸納出 15 項資訊風險，包括資料處理錯誤、資料／網路損壞、資訊設備偷竊、軟體錯誤、電腦詐欺、未受權的存取、電腦元件故障、蓄意破壞電腦資源、自然環境災害、

電腦設備誤用、核心人員之損失、資訊偷竊、病毒及木馬程式、軟體盜用、資訊服務暫停等。Fitzgerald 所歸納的 15 項風險雖有部份重疊，但與日後英國標準協會(BSI)所扮訂的資訊安全管理系統「BS7799 標準」相呼應。另外，Loch et al. (1992)從來源(Sources)、人員(Perpetrators)、動機(Intent)、及結果(Consequences)等四個維度探討不同類型的資訊系統風險；其中，「來源」乃來自企業內部(Internal)及外部(External)，「人員」分為人為與非人為風險，「動機」分為非意圖(Accidental)或意圖(Intentional)事件，造成之「結果」則有資料揭露(Disclosure)、篡改(Modification)、破壞(Destruction)與暫停使用(Denial of service)四種。

雖然上述文獻有多種資訊風險分類方式，不過這些風險可歸納成系統面風險及管理面風險兩部份。比如，就 Icove et al.(1999)分類方式而言，系統風險包含軟體、硬體、資料、網路四 部份的風險，而管理面風險是指實體、人為、及其它管理相關風險等。軟體風險中的「軟體」係指系統程式及應用軟體，而使用者的進出狀況記錄、購買並使用防毒軟體、回復系統功能(使用再生卡)、多重存取的控制、安全診斷系統、除錯程式、測試程式、及開發程式的版本控制等，則是常見的軟體保護措施。硬體風險中之「硬體」係指組織內部資訊系統主電腦及相關週邊或通訊設備，備用電腦、虛擬監視裝置、門禁管制措施與不斷電系統則是常見的硬體安全保護措施。資料風險則指組織資料之不完整或未達可靠度，保護組織資料安全之措施包括資料備份、登入身份確認、資料存取權設定、資料分級制、資訊異動記錄、定期磁碟整理、資料修改程序訂定、及資料稽核授權等。而通訊風險則是資訊傳遞過程的不確定性問題，包括組織內部及外部的資訊傳遞，其安全措施含概資料加密、簽章認證、第三者入侵偵測、防火牆的建立、及替代線路建立等。

管理面風險乃是包含系統之外部風險或其它因管理不當所造成的資訊風險。實體風險則泛指系統以外的硬體設備風險，如避雷裝置設立、空調設備、防火、防水、與防震保險措施。人為風險則是員工所造成的風險，這類議題包含離職員工帳號徹銷、資訊安全顧問聘任、不定期系統稽核、電腦安全訓練、員工操作訓練、錯誤處理程序、及員工保密契約等。在其它管理相關風險安全議題上則包括法律風險、自行承擔風險的威脅，而防護措施則涵蓋隱私權政策、智慧權保護、系統保全或診斷、資訊安全外包、資訊保險策略與資訊相關的第三責任避險等。

二、產業在資訊安全上之需求差異

King (1994)曾指出不同之產業通常會有不同的資訊需求。一般而言，財務或金融產業有較高之資訊需求。比如，Jarvenpaa et al.(1990)曾建議財務機構的資訊系統應扮演更多的策略性的角色，其對資訊系統的需求亦高於其它產業。值得注意的是，資訊需求較大的產業通常也同時會較重視資訊安全。Kankanhalli et al.(2003)的實證結果就發現，財務機構比較關心資訊安全課題；Goodhue & Straub(1991)亦提出財務組織比其它組織更應該重視資訊安全之三個理由：(一)財務組織投資在資訊系統的資源相對其它產業組織多，且依賴資訊系統的作業或管理活動亦廣泛；(二)財務組織是資訊密集

產業，電腦誤用的傷害比其它產業大；(三)資訊安全維護及其可靠度關係到財務組織的信譽，因此資訊系統誤用影響財務組織形象甚鉅。

Jung et al.(2001)分別從四種產業探討資料安全的三個需求—機密性(Confidentiality)、完整性(Integrity)與可用性(Availability)。機密性是指敏感性資料的保護，這些資料包括國家安全、法律、競爭優勢、及個人隱私；製造業通常比較重視資料隱密性，且隱密性會隨著資料之揭露而降低其重要性。完整性則是確保資料的正確性及可靠性，資料僅能被有授權者更改；金融業由於以交易記錄為主，如金額轉帳與個人信用史等，這些資料是不容許被外部人員隨意修改的，故金融業者比較重視資料完整性。資料可用性則指資料的需求乃在確保系統作業或服務不中斷，使用者可依自己需求去取得必要資料，只要確保資料被保護或可復原即可；零售及服務業之電腦運用屬性乃在確保功能之不中斷，故其資料安全需求較傾向資料的可用性。Jung et al.也同時說明「研究」是大學或研究單位之主要的產品，故也較傾向資料機密性的需求。

三、資訊化程度對資訊安全需求之差異性

McFarlan & McKenney(1983)從目前及未來對企業策略之影響兩個角度，將企業資訊系統分為支援型(Support)、工廠型(Factory)、扭轉型(Turnaround)、及策略型(Strategic)四種。支援型資訊系統支援之組織活動通常是傳統資料之處理與應用，並非關鍵性作業，也不是策略的一部份；策略型資訊系統則可能影響目前及未來企業競爭策略的角色，是企業策略的一部份；工廠型與扭轉型之資訊系統則介於支援型與策略型之間的過度型資訊系統。McFarlan & McKenney 的理論說明企業之資訊系統有應用層次上的差別，包括如協助作業、管理、或決策活動等功能性應用，以及策略性層次之決策應用。這些應用上的差異會造成企業資訊化程度之別，該差別則可由一些資訊應用特徵看出端倪。Nolan 於 1979 年所提出的「資訊處理六階段成長理論」即在說明企業資訊化過程中之類似特徵。最主要，Nolan 將企業之資料處理過程分為初始期、擴散期、控制期、整合期、資料管制期、及成熟期六個成長階段；位於各階段內的企業，都有類似的資料處理模式，因此亦皆有類似的資訊管理方法。其亦指出，前三個階段較偏向資訊技術的管理，後三個階段則著重在資訊資源管理(Information Resource Management)的議題上。其後，Earl(1989)亦由「資訊系統規劃」的角度，說明組織各成長階段之資訊特徵。Galliers (1991)則將 Nolan 與 Earl 的資訊處理六階段成長理論擴大修正，從科技面、管理面、組織面去探討資訊部門的 7S 特色。Galliers 提出各成長階段中企業之資訊策略(Strategic)、結構(Structure)、系統(Systems)、資訊部門成員(Staff)、資訊人員態度(Style)、目標(Superordinate goals)與使用者認知(Skills)之相似特徵。雖然 Nolan(1979)及 Galliers(1991)所發展的六階段成長理論非常具體，但皆未考慮資訊風險及安全特徵，企業並無法由該兩學者之成長階段論得知相對資訊風險，故亦無法由其論點擬出適切的資訊安全策略。

上述 Nolan(1979)、Earl(1989)、及 Galliers & Sutherland (1991)等人之組織資訊階段性成長理論，可以從資訊系統架構、資訊部門策略、資訊部門組織與資訊應用領域

四項特徵來衡量(Galliers & Sutherland 1991)。雖然過去文獻並沒有直接說明資訊安全與資訊化程度間之關係，然而有不少學者直接或間接提示資訊安全受資訊化四個特徵影響。比如 Loch et al.(1992)、 Ryan & Bordoloi(1997)、von Solms(1996)、及 Aivazian(1998)等人之研究即顯示，組織資訊系統架構之演變是影響資訊風險組合重要因素。其中，Loch et al.(1992) 比較個人電腦(Microcomputer)、主機電腦(Mainframe)、與網路式系統(Network)三種資訊系統架構之資訊威脅程度，並發現此三種系統架構對資訊之威脅差別很大，前二種架構之資訊威脅主要是員工意外損毀資料、或輸入錯誤，而網路式架構資訊威脅之主要來源則是環境因素及駭客。Ryan & Bordoloi(1997)則比較當時之主機電腦(mainframe)與主從式架構(Client server architecture)的潛在威脅項目及相對防護程度，亦發現類似的結果。此外，李東峰和林子銘(2001)以兩個台灣案例所進行之研究則發現，資訊策略是影響資訊安全之一項因子。另外，組織大小與資訊部門結構亦是影響資訊安全之因素(Straub 1986; Hoffer & Straub 1994)，較大或有專職資訊部門的組織通常會花更多的資源防治資訊風險。換言之，組織之資訊安全策略應考慮組織資訊化程度。

參、研究方法

一、研究架構

Smits et al.(1997)認為影響組織「資訊策略」的因素，主要來自組織資訊環境的四個面項，分別是組織資訊內部環境的資訊資源(IT resources)與組織特性(Nature of the organization)，以及外部環境的資訊科技機會(IT opportunities)與組織產業地位(Position in industry)。就本研究目的而言，組織「資訊安全策略」亦被預期受組織資訊內部環境差異所影響。換言之，組織特性中的「產業型態」及衡量資訊資源多寡的「資訊化程度」，將造成企業不同的資訊風險組合，而該風險組合差異終將影響企業的「資訊安全策略」。利用這樣的關係以及前述產業型態與資訊化程度對企業資訊安全需求之差異性探討，本研究之觀念性架構，可以圖 1 表示。圖 1 中，「資訊化程度」與企業之資訊策略、資訊部門結構、資訊系統架構、以及資訊應用領域四個資訊特徵息息相關；「資訊風險組合」同時包括軟體、硬體、資料、及網路等系統面風險，以及實體、人為、及其它與管理相關之風險。至於「資訊安全策略」則包含風險降低(Risk reduction)、風險規避(Risk avoidance)、風險自承(Risk acceptance)、以及風險轉嫁(Risk transferring)四項；前三項策略主要在增加各項風險防護措施(safeguards)以降低風險或承擔較小風險；風險轉嫁則是透過資訊保全、保險、及外包手段將組織資訊風險移轉給其它組織(Birch & Mcevoy 1992; Pipkin 2000)。詳細定義請見下節說明。

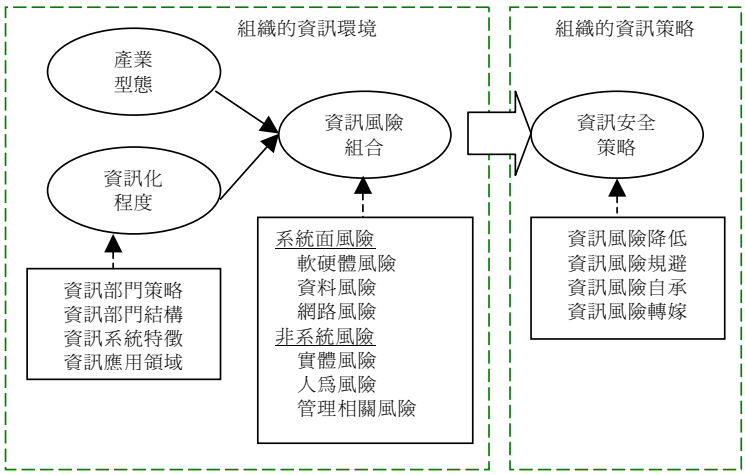

圖 1：觀念性研究架構

二、變數之操作型定義

本研究以問卷調查方式為之，問卷內容除了企業背景資料外，主要分為三部份—資訊化程度、資訊風險防護程度、及資訊風險威脅性，其內涵說明如下。詳細問卷內容如附件 A 所顯示。

(一)資訊化程度

本研究綜合 Galliers & Sutherland (1989; 1991) 所修正之階段成長理論來判別企業資訊化程度高低，主要採用四個資訊應用特徵：

- 資訊策略層次—即資訊部門面對企業資訊需求所採取的策略。當資訊部門策略若僅協助各部門取得必要之軟硬體、或依使用者需求開發各部門之軟體時，是屬於較低層次策略；當資訊策略為考量組織整體資訊需求，開發跨部門之資訊系統、或協調各部門資訊資源分配以整合組織內部整體資訊資源時，是屬於較中間層次策略；而資訊策略若為檢視組織外部環境，以尋找資訊科技可能帶來的新機會、或利用現有資訊技術以維持企業之領導地位與優勢時，是屬於較高層次策略。
- 資訊部門結構層次—即組織的資訊業務的職掌單位及該單位對企業策略的影響程度。倘若組織內尚無資訊部門，資訊業務由各功能部門自行控制、或是集中於總經理室、財務部門或其它某個部門控制，屬於較低層次部門結構；若組織內部有資訊或資料處理部門，並集中處理各部門資訊業務、或是成立資訊中心提供使用者自行開發系統時的諮詢服務時，是屬於中間層次部門結構；而資訊部門已協助組織策略單位共同研擬組織策略，即資訊單位影響策略單位之決策、或是成為主導組織未來發展之策略單位時，是屬於最高層次部門結構。
- 資訊系統架構層次—即透過資訊系統架構大小、集中式或非集中式處理、及組織內部或延伸至組織外部的資料處理狀況。當組織內部存在多個未整合的

小型資訊系統、或組織嘗試整合內部各資訊系統，但系統間仍存在相同或重複的功能時，屬於較低層次系統架構；若資訊系統是整合所有功能的「集中化系統」，由總公司集中控制，是屬於較中間層次系統架構；若組織之資訊系統屬「非集中式系統」或「分散式系統」，總公司能有效控制分散在外的資源時，是屬於較高層次的系統架構；而當組織之資訊系統已結合上下游夥伴廠商外部資料的資訊系統時，是最高層次系統架構。

- 資訊應用領域層次—即藉由資訊系統應用領域來判斷資訊化程度。Gibson & Nolan (1976)認為最早期資訊系統應用領域僅限於「財務」或「會計」方面的應用，然後才擴及其它功能；而就支援組織內部活動方面之應用層次而言，由低至高分別是人工作業流程自動化、管理活動支援、決策過程支援與策略規劃。在策略規劃方面，Galliers & Sutherland(1991)認為客戶關係管理、以及產製資訊導向產品與服務，是最高層次之應用領域。

利用上述四個資訊應用特徵，本研究建立一資訊應用層次的綜合指標，藉以判斷樣本企業之資訊化程度，並作為資訊化之分群依據。

(二)各項資訊風險的防護程度

本研究採用 Icove et al.(1999)之理論，由資產面來認定常見的「資訊風險」，包括軟體風險、硬體風險、資料風險、通訊風險、實體風險、人為風險、及管理相關風險等七項。這些風險的防護措施，則整理自 Icove et al.(1999)、Peltier(2001)、Pipkin(2000)、Siegel(2002)、及 Richardson(2003)等文獻。其中，Siegel(2002)所提之防護措施主要是參考 ISO17799 及 InfoSec 國際標準；而 Richardson(2003)是美國電腦安全協會(CSI)針對網路風險威脅所提出之防護措施，這些措施同時作為每年 CSI 電腦犯罪及安全調查依據。除了上述文獻外，本研究也透過專家訪談增列五個台灣實務界常用之措施，並再參酌英國標準協會(BSI)擬訂之資訊安全管理系統內部稽核標準 BS7799 (BSI 2002)，合併作為本研究設計組織資訊安全防護現況問項的依據。總計本研究得出七大資訊風險領域及 50 個風險防護項目，詳細內容見表 1。問卷中，表 1 列成一個查核表(checklist)(請見附錄 A 問卷)，藉由受訪者企業勾選每個防護措施的執行與否，來決定各受訪企業在七個資訊風險領域的防護程度。衡量方式是計算每個資訊風險領域內防護措施的執行比例，執行比例高則表示該項風險防護程度高，反之則低。

表 1 ：資訊風險防護措施整理一覽表

系統風險措施	參考文獻[a]	BS7799-2[b] (CNS17800)	依據[c]
軟體風險防護措施			
使用者進出日誌	[1] [2] [4] [5]	A.8.4.2	✓
防毒軟體	[1] [2] [4] [5]	A.8.3.1	✓
系統回復	[4]	A.8.4.1	✓
多人使用系統	[1]		✓
掃描軟體	[1]		✓
除錯及自我測試	[1]		✓
系統修正認可	[1] [2] [4]	A.10.4.3	×
系統修正驗證	[1] [2] [4]	A.8.2.2	×
軟體取得安全	[4]	A.10.5.4	
硬體風險防護措施			
異地備援	[1]		✓
監視裝置	[1] [4]	A.7.1.3	✓
門禁刷卡管制	[1] [4]	A.7.1.2	✓
不斷電系統	[1] [4]	A.7.2.3	✓
定期磁碟檢查	[1] [4]	A.7.2.1	✓
資料風險防護措施			
定期備份資料	[2] [4]	A.8.4.1	✓
登入電腦密碼	[2] [4]	A.9.1.1	✓
存取權限設定	[2] [4]	A.9.1.4	✓
強迫路徑設定	[2] [4]	A.9.4.2	✓
異動記錄(日誌)	[1] [4]	A.9.7.1	✓
資料庫修改程序	[2] [4]	A.8.6.3	×
儲存媒體控管	[4]	A.8.6.1	×
媒體報廢處理	[4]	A.8.6.2	
網路風險防護措施			
密文方式傳送	[1] [2] [4] [5]	A.10.3.2	✓
網路身份確認	[1] [2] [4] [5]	A.9.4.3	✓
入侵偵測	[1] [2] [4] [5]	A.9.7.2	✓
防火牆	[1] [2] [4] [5]	A.9.4.6	✓
線路備援	[1]		✓
數位簽章	[4]	A.10.3.3	
連線時間限制	[4]	A.9.5.8	

管理面風險措施	參考文獻[a]	BS7799-2[b] (CNS17800)	依據[c]
實體環境風險防護措施			
避雷裝置	[1] [4]	A.7.2.1	✓
空調設備	[1] [4]	A.7.2.1	✓
防火措施或火險	[1] [4]	A.7.2.1	✓
防水措施或水險	[1] [4]	A.7.2.1	✓
防震措施或震險	[4]	A.7.2.1	✓
人為風險防護措施			
員工保密契約	[4]	A.6.1.3	×
離職帳號撤銷	[1]		✓
資訊安全顧問	[2] [4]	A.4.1.5	✓
不定期系統稽核	[1] [2] [4]	A.4.1.7	✓
資訊安全課程	[1] [2] [4]	A.6.2.1	✓
系統操作訓練	[1] [2] [4]	A.6.2.1	✓
操作及應變程序	[2] [4]	A.6.3.1	✓
管理相關風險防護			
資訊安全政策			
資訊安全政策	[4]	A.3.1.1	
員工安全職責	[1] [4]	A.6.1.1	
營運持續計劃	[2] [4]	A11.1.1	
法律風險防範			
隱私權保護政策	[4]	A.12.1.4	✓
智慧財保護政策	[4]	A.12.1.2	✓
風險轉嫁措施			
資訊安全保全	[3] [4]		✓
系統安全外包	[3] [4]		✓
第一責任險	[3] [4]		✓
第三責任險	[3] [4]		✓

[a][1] Icove(1999); [2] Peltier(2001); [3] Pipkin(2000); [4] Siegel(2002); [5] Richardson(2003); [c]✓文獻整理; ×訪談新增

[b]BS7799-2 即 BS7799 第二版，同時為經濟部標準 CNS17800 資訊安全標準內容，表格內容為 BS7799-2 附錄 A 的稽核條文

(三)資訊風險威脅程度及趨勢

為了瞭解不同產業型態及資訊化程度企業的資訊風險組合、威脅程度與趨勢，本研究擬藉由組織之資訊主管對自身企業過去、目前及未來各項資訊風險威脅程度之認知進行統計分析。此部份問項採用 Likert 七點量表衡量風險高低，7 表示該項風險認知威脅性最高，1 表示該項風險認知威脅性最低，依此類推。由於採用 Likert 七點量表為衡量工具，可以認定平均威脅值大於 4 的風險項目，是資訊主管們認為相對較重要的資訊風險威脅來源。可以預期的，若樣本企業依產業型態或資訊化程度事先分群，可藉由各群風險威脅平均值衡量各群(不同產業或資訊化程度企業)目前及未來之主要資訊風險組合及主要風險威脅項目。

此外，本研究也進一步探討台灣企業對 [過去、目前] 及 [目前、未來] 兩種資訊風險威脅之趨勢認知，其方法乃以平均值做差異檢定，透過此兩種檢定來瞭解不同產業間或不同資訊化程度企業的資訊風險移轉趨勢。亦即，瞭解資訊風險對企業經營之威脅，在未來是否會比過去更提高，並分析這種趨勢認知與產業別及資訊化程度之相關性。

二、問卷前測與效度

問卷之設計除依文獻與專家意見發展外，亦利用內容分析法修正問卷項目。問卷之定稿則經由五位具資訊安全經驗的資訊主管審訂，目的要確認(1)資訊化程度及資訊風險防護措施的衡量項目；(2)題目的語譯及難易程度適當性；(3)受測時間長短。為了確保研究效度及信度，本研究並進行前測，前測乃委託資訊經理人協會發放 500 份問卷，目的在(1)確認填答內容符合預期；(2)每個資訊化程度及資訊風險防護構面提供「其它」欄位，供填答者增加其它項目用；(3)問卷最後留空白欄提供適當研究意見。最後回收問卷 66 份，填答選項及內容均符合本研究的預期，至於部分「其它」或「研究意見」有填答者，都斟酌修正。

三、問卷發放與回收

(一)研究對象

本研究主要探討企業的資訊風險及安全策略，故研究對象以企業個體為主。由於企業內部資訊安全相關業務以資訊主管及負責資訊安全人員最熟悉，且 Straub(1986)認為較大型組織會投入較多時間及金錢在資訊安全及系統稽核，因此問卷發放對象選擇台灣 1000 大企業資訊主管或負責資訊安全人員為樣本。

(二)問卷發放與回收

由於資訊安全研究涉及組織內部資訊業務或經營可靠度之資料，為了確保資料隱密性，本研究在正式的問卷調查過程中，備有回郵郵資，受訪者可以在填完後密封直寄回，以增加受訪者填答意願。本研究於民國 92 年 11 月發出問卷 1000 份(中華徵信

所認定之台灣 1000 大企業)，回收及有效問卷計 111 份，有效問卷之回收率達 11%。此回收率與同領域之研究差異不大。就 Kotulic and Clark(2004)實證探討「資訊安全問卷回收率偏低的原因」結論顯示，資訊安全研究因涉及公司的敏感性資料，未回覆之受訪者約有 23%不對外透露組織內部資訊安全相關訊息。此外，本研究進一步利用排名變項(以營業額排名)進行回收問卷與未回收問卷之無反應偏差檢定，以 $p<0.05$ 顯著水準檢驗，結果顯示兩者並無顯著差別($t=-1.098$; $p=0.273$)，亦即回收樣本所得之研究結論並不會造成太大的偏誤。

肆、研究結果

一、樣本特性分析

表 2 是本研究整理回收問卷填答者的基本資料。資料顯示有 99%填答者直接或間接參與企業資訊安全相關業務，包括規劃及制定資訊安全策略(61%)、執行安全策略(23%)、風險稽核(4%)、及系統工程師(11%)等工作。此外，有 66%填答者為資訊部門主管以上之職位。這個結果表示所回收資料皆來自專業人員，具有一定的效度。另外，有 77%(=49%+27%+1%)及 95%(=43%+45%+7%)填答者年資超過 10 年以上或年齡超過 30 歲，98%(=18%+62%+18%)填答者具備專科以上學歷。

表 2：填答者個人資料(N=111)

	個數	比例		個數	比例
工作總年資			**職位**		
10 年以下	26	23%	總經理或副總經理	2	2%
10~19 年	54	49%	資訊部門主管	68	62%
20~29 年	30	27%	負責資安之其他主管	2	2%
30 年以上	1	1%	專案經理	3	3%
年齡			一般工程師	14	13%
26~30 歲	5	5%	負責資安之工程師	15	14%
31~40 歲	48	43%			
41~50 歲	50	45%	**資訊安全業務之涉獵程度**		
51 歲以上	8	7%	規劃及制定策略	68	61%
學歷			執行策略及措施	26	23%
專科	20	18%	分析及稽核風險	4	4%
學士	69	62%	一般系統工程師	12	11%
碩士以上	20	18%	其它	1	1%

表 3 則顯示受訪公司之特性。由於研究對象是台灣前 1000 大企業，故樣本企業不管是公司歷史、員工數、或營業額各項特徵值都偏高，有 86%(=25%+61%)公司歷史超過 10 年、85% (=20%+23%+19%+16%+7%)樣本企業為中大型企業(員工數大於 200 人)、及 96% (=44%+21%+30%)樣本企業營收超過 10 億以上。就產業別而言，四種產

業回收個數差不多，有助於資料分析。值得一提的是，各產業之回收率並不相同，金融業回收率高達 26%(=24/93)，而其它產業平均回收率僅接近 10%(=87/907)，間接顯示金融業重視資訊安全程度較其它產業來得高。

表 3：樣本企業資料(N=111)

	個數	比例		個數	比例
公司歷史			**營業額**		
10 年以下	16	15%	10 億以下	6	5%
11~20 年	27	25%	10 億~50 億	49	44%
20 年以上	68	61%	50 億~100 億	23	21%
			100 億以上	33	30%
員工數			**產業別**		
200 人以下	17	15%	傳統製造業	30	27%
201~500 人	22	20%	電子製造業	26	23%
501~1000 人	25	23%	金融保險業	24	22%
1001~2000 人	21	19%	流通及服務業	29	26%
2001~5000 人	18	16%	其它	2	2%
5001 人以上	8	7%			

二、樣本企業之資訊化特性分析

(一)企業資訊化程度指標式—主成份(Principal Component)分析結果

綜合 Nolan(1979)、Galliers & Sutherland (1991)等學者之理論，企業資訊應用成熟度可以由資訊策略層次、資訊部門結構層次、資訊系統架構層次、及資訊系統應用領域層次等四個企業資訊應用特徵來判斷。由表 4 可以發現該四個資訊應用層次為高度相關，故適合使用主成份分析法將此四個特徵層次匯總成一個綜合指標—「資訊化程度」。Sharma (1996)認為主成份分析法可將相關性很高的變數合成一個變數，以減少變數個數。不但有簡化變數的功能，而且同時考慮原變數的平均數及變異。所得出之「資訊化程度」指標公式為：

PRIN (資訊化程度)=0.5598(資訊策略層次) + 0.3714*(資訊部門結構層次)*
+0.3591(資訊系統架構層次) + 0.6479*(資訊系統應用層次)*

表 4：四項資訊應用特徵兩兩相關程度

相關係數	資訊策略層次	資訊部門結構層次	資訊系統架構層次
資訊部門結構層次	0.58**	—	—
資訊系統架構層次	0.24*	0.23*	—
資訊應用領域層次	0.54**	0.38**	0.30**

顯著性 **p ≤0.05 **p ≤0.01

此指標可解釋原來四個資訊應用特徵 55% 的總變異量，且指標數值介於(1.938, 11.629)之間。因為 Galliers 所提之修正後階段性成長理論將資訊成長分為六個階段，故本研究亦將「資訊化程度」指標值線性切割成六等分。所有回收樣本企業皆依此四項資訊應用特徵，透過上述主成份指標，劃分成六個不同資訊化程度。表 5 顯示樣本企業在該六個資訊化階段之主成份指標值及四項資訊化特徵上之平均值。整體而言，「資訊化程度」指標平均值愈高者，其四項「資訊化特徵」平均值亦顯著較高，亦即其資訊化程度越高。依據該四項特徵值之高低(一至六)所分割出之六階段分別具下列特色：第一及第二階段企業之資訊策略為各部門軟體取得，資訊業務開始集中運作、且企業間存在多個未整合系統，系統之主要目的為協助例行性作業活動。第三階段企業之資訊策略為整合性、跨部門資訊系統之開發，以及資訊部門之成立；另一方面，雖然仍有系統未能整合問題，但已可協助部份之管理活動。第四階段企業之資訊策略為資訊資源之控制與協調、以及集中式資訊系統之使用，此外，系統已有部份決策功能。第五階段企業之資訊策略則在運用資訊科技尋找新機會、成立資訊中心提供諮詢服務、且已有少部份分散式系統功能，並支援客戶關係管理。第六階段企業之資訊策略則主要是利用資訊科技維持企業之競爭優勢，此時資訊部門已能協助企業研擬策略，而在系統架構上則是集中式與分散式系統並存，並能提供行銷面或資訊導向之產品與服務。

表 5：各資訊化階段企業之主成份指標值及四項資訊化特徵比較

階段	樣本個數	資訊化程度指標	資訊化特徵 [a]			
			資訊策略層次	資訊部門結構	資訊系統架構	資訊應用領域
第一階段	1	3.24	2.00	3.00	1.00	1.00
第二階段	7	4.78	2.57	2.71	2.57	2.14
第三階段	29	6.15	3.72	3.31	2.79	2.82
第四階段	33	7.57	4.51	3.51	3.45	3.85
第五階段	29	9.09	5.38	4.31	3.58	4.93
第六階段	12	10.64	5.92	5.25	4.75	5.67

[a]1 至 6 點量表之平均值

(二)資訊化程度與產業型態

所有企業樣本依產業型態及資訊化程度兩個維度分類結果如表 6 所示。就資訊化程度而言，台灣一千大企業大多集中在第三至第六階段，即中高資訊化程度，占所有產業 92.8%(=(29+33+29+12)/111)。若再依產業別細分，可發現企業資訊化程度會因產業別而有差異。高科技製造業、金融保險業及流通服務業對資訊需求似乎較依賴，分別有 75% (=41%+19%+15%)、67%(=29%+33%+4%)及 76%(=19%+42%+15%)企業落於第四至第六階段，屬中高資訊化程度。金融保險業資訊化程度高主要受資訊化產品與服務有關，如同 Jarvenpaa et al.(1990)所探討，財務機構較會引用資訊科技於策略面。而台灣高科技產業資訊化程度高可能原因有幾項：財務上較其它產業優渥、上下游夥

伴關係密切、產品生產需較高資訊科技配合、以及研發的需求等。至於流通及服務業，資訊科技通常用於產品或客戶本身，且作為企業競爭優勢的基礎，如銷售時點系統(POS)、分散式系統等，此類資訊應用層次亦較高。較相較之下，傳統產業之資訊化相對較低，有 75%(=9%+34%+31%)傳統製造業者屬中低資訊化程度。主要理由除產品非資訊化產品外，亦無高科技產業資訊需求的嚴苛條件。

表 6：樣本個數分析—依產業型態與資訊化程度

資訊化程度	產業										
	傳統製造業		高科技產業		金融保險業		流通服務業		其它產業		合計
第一階段	0	(0%)	0	(0%)	0	(0%)	1	(4%)	0	(0%)	1
第二階段	3	(9%)	1	(4%)	1	(4%)	1	(4%)	1	(50%)	7
第三階段	11	(34%)	6	(22%)	7	(29%)	4	(15%)	1	(50%)	29
第四階段	10	(31%)	11	(41%)	7	(29%)	5	(19%)	0	(0%)	33
第五階段	5	(16%)	5	(19%)	8	(33%)	11	(42%)	0	(0%)	29
第六階段	3	(9%)	4	(15%)	1	(4%)	4	(15%)	0	(0%)	12
合計個數	32	(100%)	27	(100%)	24	(100%)	26	(100%)	2	(100%)	111

三、樣本企業之資訊安全現況分析

(一)企業之資訊安全防護與其產業型態及資訊化程度之關係

為探討企業之資訊安全防護現況與其產業別及資訊化程度之關係，本研究利用多變量線性模式進行實證分析。模式之自變項包含「產業型態」(分成傳統製造業、高科技產業、金融保險業、及流通與服務業四種產業)、「資訊化程度」(分高、中、低三個水準；第一至三階段為低、第四階段為中、第五至六階段為高)、「員工數」及「營業額」；後兩者代表樣本企業的規模，在此視為共變項。依變項是前述表 1 中之七項「資訊風險防護程度」。資料分析結果如表 7 所示。

表 7：各項資訊風險安全措施皆受企業產業型態及資訊化程度影響

F 值	軟體防護	硬體防護	資料防護	實體防護	網路防護	人為防護	管理防護	Wilks' λ
產業型態	1.42	5.22**	3.26*	2.61	7.57**	6.20**	7.21**	2.24**
資訊化程度	4.64*	7.05**	4.72*	1.74	7.92**	3.77*	5.33**	2.20**
產業型態×資訊化程度	0.35	1.11	0.42	0.87	0.88	1.27	0.62	0.93
共變項								
員工數	0.63	0.51	1.31	10.13**	8.45**	4.84*	0.32	2.42*
營業額	0.32	0.18	0.44	0.86	0.00	0.63	2.82	0.78

顯著性 *p ≤0.05 **p ≤0.01

表 7 之 Wilks' λ 值顯示，「產業型態」、「資訊化程度」及「員工數」三者顯著影

響「資訊風險防護程度」，但「產業型態」與「資訊化程度」之交互作用則不顯著。表 7 亦顯示個別風險防護與自變數間之關係，除了實體風險外，其它軟體、硬體、資料、網路、人為與管理相關風險之防護程度皆受「產業型態」及「資訊化程度」所影響。另外，企業之員工數亦在實體、網路與人為風險上有顯著效果。上述防護現況分析結果亦顯示後續須針對產業型態與資訊化程度兩個主要研究變項作深入探討。

(二)產業間在資訊風險防護現況上之差異分析

前一節驗證產業差別會影響組織資訊安全，然而造成不同的防護差異那裡？那方面防範較好？本研究繼續透過 Fisher 最小顯著差異法(LSD)進行事後分析(post hoc test)，結果如表 8 所顯示。表 8 第一欄為七項風險防護措施之總平均執行率；而後三欄為兩兩產業平均執行率之差值(=行-列)。由表 8 數據顯示下列訊息：

表 8：產業間在資訊風險防護程度上之差異分析

產業型態	平均執行率(%)	產業間差異百分比(%) 傳統製造	高科技產	金融保險	產業型態	平均執行率(%)	產業間差異百分比(%) 傳統製造	高科技產	金融保險
A.整體風險防護					4.網路風險防護				
傳統製造業	52.6	—	—	—	傳統製造業	40.0	—	—	—
高科技產業	61.0	-8.4*	—	—	高科技產業	50.8	-10.8*	—	—
金融保險業	70.0	-17.4**	-9.0*	—	金融保險業	65.5	-25.5**	-14.7**	—
流通與服務業	53.4	-0.8	7.6*	16.6**	流通與服務業	41.1	-1.14	9.65	24.3**
1.軟體風險防護					5.實體風險防護				
傳統製造業	66.3	—	—	—	傳統製造業	63.3	—	—	—
高科技產業	73.2	-7.0	—	—	高科技產業	63.0	0.4	—	—
金融保險業	75.0	-8.7	-1.8	—	金融保險業	76.7	-13.3*	-13.7*	—
流通與服務業	66.2	0.1	7.0	8.8	流通與服務業	59.2	4.13	3.8	17.5*
2.硬體風險防護					6.人為風險防護				
傳統製造業	63.3	—	—	—	傳統製造業	52.4	—	—	—
高科技產業	67.4	-4.1	—	—	高科技產業	58.2	-5.8	—	—
金融保險業	80.8	-17.5**	-13.4**	—	金融保險業	69.1	-16.7**	-10.9	—
流通與服務業	65.6	-2.3	1.8	15.2**	流通與服務業	46.3	6.1	11.9	22.8**
3.資料風險防護					7.管理風險防護				
傳統製造業	62.1	—	—	—	傳統製造業	28.5	—	—	—
高科技產業	75.5	-13.4**	—	—	高科技產業	41.6	-13.1**	—	—
金融保險業	79.7	-17.6**	-4.2	—	金融保險業	50.9	-22.4**	-9.4	—
流通與服務業	70.0	-7.9	5.5	9.7**	流通與服務業	31.1	-2.6	10.5*	19.8**

顯著性 $^{*}p \le 0.05$ $^{**}p \le 0.01$

就***整體風險防護***而言，除了傳統製造業與流通服務業的資訊避險措施執行較無顯

著差異外，其餘各項產業兩兩間均有顯著差別。其中金融保險業的資訊避險措施執行最徹底，平均執行率達 70.00%，其次是高科技產業(61.04%)，再其次是流通服務業務(53.44%)及傳統製造業(52.60%)。

就***個別風險防護***而言，除了***軟體風險防護***較無顯著差異外，其餘各項風險防護在產業間均有差異。在***硬體與實體風險的防護***上，雖然各產業的防護程度均高(平均值>60%)，但金融保險業顯著性地高於其它三種產業。在***資料、人為、及管理相關風險防護***方面，則以金融保險與高科技兩者產業較重視。而***網路風險防護程度***在產業間差異較大，大致可分為三群，金融保險業執行率顯著高於高科技產業，而高科技產業又顯著高於流通服務業及傳統製造業。

此外，如由個別產業角度探討各項資訊風險防護，則可以發現四個產業防護程度較高的部份，主要皆集中在硬體、軟體、實體與資料四個風險防護，其次是人為風險防護、網路風險防護，執行比例最差的部份是管理相關風險防護。

前表 8 乃是產業間風險防護之整體執行率比較，表 9 則是各產業在各資訊安全防護措施細項上之個別執行比例。為增加易讀性，表 9 將實際獲得之執行比以符號表示；其中「□」表示執行率僅 10%以下、「◘」介於 10.1%~35%、「▣」介於 35.1%~65%、「◙」介於 65.1%~90%、「■」則在 90.1%以上。

如前論述，產業間較大的資訊風險防護差異在資料、網路、人為、及管理相關風險四方面。表 9 顯示在資料風險防護上，金融保險及高科技業者似乎比其它產業更重視下列措施—強迫路徑設定、存取權限設定、媒體報廢處理、資料庫修改程序及異動記錄(日誌)管理等。在網路風險防護上，金融保險業在密文方式傳送、網路身份確認、連線時間限制、數位簽章使用及入侵偵測等五項措施皆顯著高於其它產業；而高科技產業則以密文傳送及入侵偵測兩項控制較受重視。在人為風險防護上，主要差異項目包括員工保密契約、操作及應變程序、不定期系統稽核、及資訊操作訓練等，以金融保險業執行率較高。至於管理相關風險防護方面，不管是資訊安全政策、法律風險防範、或是資訊風險轉嫁等各方面控制措施，亦都是金融保險及高科技產業顯著較高。

表 9：不同產業型態對各項資訊風險控制措施執行異同 [a]

系統面風險	整體	產業型態 傳產	科技	金融	服務
1 軟體風險防護措施					
防毒軟體	■	■	■	■	■
系統修正驗證	◙	◙	■	■	◙
多人使用系統	◙	◙	■	◙	◙
系統回復	◙	◙	◙	◙	◙
系統修正認可	◙	◙	◙	■	◙
使用者進出日誌	◙	⊡	◙	◙	◙
避免木馬程式	⊡	⊡	⊡	◙	⊡
掃描或診斷軟體	⊡	⊡	⊡	⊡	■
除錯及自我測試	■	■	■	⊡	■
2 硬體風險防護措施					
不斷電系統	■	■	■	■	■
門禁刷卡管制	◙	◙	◙	■	◙
定期磁碟檢查	◙	◙	◙	◙	◙
監視裝置	⊡	⊡	⊡	◙	⊡
異地備援	⊡	⊡	■	⊡	⊡
3 資料風險防護措施					
定期備份資料	■	■	■	■	■
登入電腦密碼	■	■	■	■	■
強迫路徑設定	■	◙	■	■	■
存取權限設定	◙	⊡	◙	■	◙
資料庫修改程序	◙	⊡	◙	◙	⊡
異動記錄(日誌)	⊡	⊡	⊡	◙	⊡
媒體報廢處理	⊡	⊡	◙	⊡	⊡
儲存媒體控管	■	■	■	■	■
4 網路風險防護措施					
防火牆架設	■	■	■	■	■
線路備援	◙	⊡	◙	◙	◙
偵測入侵行為	⊡	⊡	⊡	◙	⊡
密文方式傳送	⊡	■	⊡	◙	■
網路身份確認	⊡	■	■	⊡	■
連線時間限制	■	■	■	⊡	■
數位簽章使用	■	□	■	■	■

管理面風險	整體	產業型態 傳產	科技	金融	服務
5 實體環境風險防護措施					
空調設備	■	■	■	■	■
防火措施或火險	◙	◙	◙	■	◙
避雷裝置	⊡	◙	⊡	⊡	⊡
防水措施或水險	⊡	⊡	⊡	◙	⊡
防震措施或震險	⊡	⊡	⊡	⊡	⊡
6 人為風險防護措施					
離職帳號撤銷	■	■	■	■	■
員工保密契約	◙	⊡	◙	◙	⊡
操作及應變程序	⊡	⊡	⊡	◙	⊡
不定期系統稽核	⊡	⊡	⊡	◙	⊡
資訊操作訓練	⊡	⊡	⊡	⊡	⊡
資訊安全課程	⊡	■	⊡	⊡	■
資訊安全顧問	■	■	■	■	■
7 管理相關風險防護措施					
7.1 資訊安全政策					
安全政策文件	◙	⊡	◙	◙	⊡
營運持續計劃	⊡	⊡	◙	◙	⊡
安全職責歸屬	⊡	⊡	⊡	◙	⊡
7.2 法律風險防護					
智慧財保護政策	⊡	⊡	◙	◙	⊡
隱私權保護政策	⊡	■	⊡	⊡	■
7.3 風險轉嫁措施					
專業保全系統	■	■	■	■	■
第一責任險	■	□	■	⊡	□
專業外包系統	■	□	■	□	■
第三責任險	□	□	□	■	□

[a]□表示僅執行 10%以下措施、■執行率 10.1%~35%、⊡執行率 35.1%~65%、◙執行率 65.1%~90%、■執行率 90.1%以上

(三)產業間對資訊風險之威脅認知

本節繼續探討各產業對其目前之資訊風險來源及未來風險趨勢認知。表 10 是樣本企業對自身過去、目前及未來各項風險來源威脅認知的平均值，其中，以灰底顯示者，為各產業目前之主要風險來源(平均值>4)。在風險趨勢之認知上，「△」及「▲」分別表示一產業對一風險之威脅性認知，在「目前比過去」以及「未來比目前」之比較上，達統計上之顯著水準(α=0.05)。

表 10：產業型態差異下，各項資訊風險對企業經營威脅認知 [ab]

	傳統製造業			高科技產業			金融保險業			流通與服務業		
風險認知	過去	現在	未來	過去	現在	未來	過去	現在	未來	過去	現在	未來
軟體風險認知	3.24	3.34	3.34	3.44	4.13△	4.28	3.91	4.50△	4.61	3.69	3.98△	4.12
硬體風險認知	3.40	3.38	3.26	3.52	3.80	3.72	4.11	4.20	4.02	3.77	3.85	3.77
資料風險認知	3.40	3.40	3.43	3.46	4.22△	4.33	4.30	4.76△	4.87	4.06	4.27	4.33
網路風險認知	3.16	3.83△	4.02	3.56	4.70△	4.76	3.37	5.04△	5.28▲	3.77	4.56△	5.00▲
實體風險認知	3.12	3.10	3.22	3.74	3.85	3.89	3.65	4.00	4.13	3.54	3.81	3.81
人為風險認知	3.24	3.41	3.26	3.74	4.33△	4.33	4.17	4.72△	4.91▲	3.98	4.33△	4.42
法律風險認知	2.71	2.84	2.79	3.41	3.69	3.78	2.76	3.50△	3.96▲	2.98	3.48△	3.52

[a]7 點量表，平均值愈高顯示風險認知威脅性愈大 [b]△該威脅目前比過去顯著增加 ▲該威脅未來比現在顯著增加

由表 10 中，可看出***傳統製造業***對各項資訊風險之威脅性看法偏低，目前各項資訊風險威脅平均值都未超過 4，顯示傳統製造企業對資訊風險敏感度不高；此外，其平均值在未來雖有增加，但皆沒有顯著性增加，可能表示其預期未來各項風險之威脅亦不高。

高科技產業認為目前主要資訊風險來源依序為網路風險、人為風險、資料風險、軟體風險等四項，這些風險相對於過去五年前均有顯著地上升，並且是未來主要威脅來源(平均值>4)，然而威脅性並無顯著增加。

金融保險業認為目前主要風險來源依序為網路風險、資料風險、人為風險、軟體風險、硬體風險及實體風險，其中前四項風險相較於過去五年均有顯著增加的趨勢。值得一提的是，雖然法律風險目前的威脅性並不高，但相較於過去也有顯著性增加。在未來風險趨勢之預期上，金融保險業者則認為網路、人為與法律風險的威脅性將顯著提高。

流通服務業目前主要風險威脅來源為網路、人為、資料風險三項。相較過去五年的威脅性，軟體、網路、人為、法律四項風險均有顯著增加趨勢；而在未來趨勢上，「網路風險」仍會持續增加其威脅性，其它風險則無顯著變化。

(四)資訊化程度之差異與資訊風險防護現況

前述多變量分析結果亦驗證資訊化程度對資訊安全防護的關聯性。本節繼續透過 Fisher 最小顯著差異法(LSD)進行事後分析，結果如表 11 所顯示。和表 8 一樣，表 11 的第一欄表示七項風險防護措施之平均執行率；而後三欄指不同資訊化程度下執行率差值(=行-列)。

表 11：資訊化程度差別在資訊風險防護程度上之差異分析

資訊化程度	平均執行率(%)	資訊化程度之差異百分比(%) 低	中	高	資訊化程度	平均執行率(%)	資訊化程度之差異百分比(%) 低	中	高
A.整體風險防護					4. 網路風險防護				
低 (階段二三)	48.7	—	—	—	低 (階段二三)	33.6	—	—	—
中 (階段四)	60.6	-11.9**	—	—	中 (階段四)	52.2	-14.7*	—	—
高 (階段五六)	66.3	-17.6**	-6.0	—	高 (階段五六)	58.9	-13.1*	1.6	—
1.軟體風險防護					5. 實體風險防護				
低 (階段二三)	60.1	—	—	—	低 (階段二三)	55.9	—	—	—
中 (階段四)	73.3	-13.1**	—	—	中 (階段四)	70.6	-18.6**	—	—
高 (階段五六)	75.8	-15.7**	-2.57	—	高 (階段五六)	69.0	-25.3**	-6.7	—
2.硬體風險防護					6.人為風險防護				
低 (階段二三)	58.8	—	—	—	低 (階段二三)	45.4	—	—	—
中 (階段四)	68.1	-9.3*	—	—	中 (階段四)	58.9	-13.6**	—	—
高 (階段五六)	78.0	-19.2**	-9.9*	—	高 (階段五六)	63.2	-17.8**	-4.3	—
3.資料風險防護					7.管理風險防護				
低 (階段二三)	62.9	—	—	—	低 (階段二三)	29.1	—	—	—
中 (階段四)	71.5	-8.6*	—	—	中 (階段四)	36.1	-7.0	—	—
高 (階段五六)	78.4	-15.6**	-7.0	—	高 (階段五六)	45.8	-16.8**	-9.7*	—

顯著性 *p ≤0.05 **p ≤0.01

就***整體資訊風險防護***而言，資訊化程度低、中、高企業之資訊安全防護措施執行率分別為 48.65%、60.56%、66.25%。表 11 結果亦顯示，中、高資訊化程度企業之資訊風險防護差別並不大，然而低資訊化程度企業(包含階段 1~3 企業)之資訊防護，卻與中高階段企業有明顯的差異。

就***個別資訊風險防護***而言，***硬體風險防護***是唯一低、中、高資訊化程度企業兩兩皆有差別者，這可能意謂企業會隨著資訊化程度提高而顯著增加硬體風險防護。而***軟體***、***資料***、***網路***、***實體及人為***等五項風險的防護，主要防護差異皆發生在資訊化程度[低、中]及[低、高]兩組企業，而資訊化程度[中、高]企業則無防護上差別，這顯示這些風險防護項目會隨著資訊化程度由第三階段邁向第四階段而提高。至於***管理相關風險防護***方面，資訊化程度高的企業顯著地高於資訊化中、低程度的企業，這結果也說明管理相關風險防護措施在資訊化程度達到第五、六階段以後才開始受到重視。

最後再依資訊化程度低、中、高三群分別比較七項風險防護之差異，發現三群的結果是相似的。以資料、軟體、硬體及實體四項風險防護較高；人為風險防護次之；

網路風險防護再次之；管理相關風險防護最差。

前述表 11 說明資訊化[低、中]的企業在軟體、硬體、實體、資料、網路及人為等六項風險的防護有顯著差異，表 12 再從資訊防護措施細項比較兩者企業在風險控制措施執行之不同處。如表 12 所示，在軟體風險控制措施上，差異是「使用者進出系統日誌」和「掃描或診斷軟體」兩項。硬體及實體風險防護主要不同點是「異地備援」及「避雷裝置」的實施。而資料風險防護措施執行比率差異較大有三項，分別是「存取權限設定」、「資訊庫修改程序」及「媒體報廢處理」。至於網路風險防護措施，差異點在「線路備援」、「偵測入侵行為」、「密文方式傳送」、以及伺服器「連線時間限制」等四項。人為風險防護方面，主要差別在於「員工保密契約」、「操作及應變程序」、及「不定期系統稽核」，可能顯示資訊化程度較中高企業對員工的不忠誠度比較在意，並且嚐試對「資訊系統操作程序」及「事件發生處理程序」文件化。

表 12 同時比較[中、高]資訊化程度企業在管理相關風險防護差異。其主要差異來自「法律風險防範」及「風險轉嫁」措施，而「資訊安全政策」措施並沒有很大差別。雖然資訊化程度高的企業相較其他企業重視管理相關風險，但執行率仍舊偏低，尤其是「風險轉嫁」的措施，如「專業保全系統」、「第一責任險」、「專業外包系統」及「第三責任險」等措施，執行率皆不到三成。

(五)資訊化程度之差異與資訊風險之威脅性認知

表 13 顯示不同資訊化程度之企業對其目前之資訊風險來源及未來風險趨勢認知。表 13 中之數據與符號意義和表 10 一樣。唯一差異之符號「▽」，表示該項風險之威脅性為顯著遞減。由表 13 可發現，***低資訊化程度者***目前與未來之主要風險來源為網路風險(平均值>4)；此外，與過去五年相較，其目前對軟體、法律風險之威脅性認知有顯著上升，而對實體風險之威脅性則為顯著下降。另其對未來硬體風險之威脅性認知亦顯著降低。

表 12：不同資訊化程度對各項資訊風險控制措施執行異同[a]

系統面風險	整體	資訊化程度 低	中	高
1 軟體風險防護措施				
防毒軟體	■	■	■	■
系統修正驗證	◙	◙	■	◙
多人使用系統	◙	◙	◙	■
系統回復	◙	◙	◙	◙
系統修正認可	◙	◙	◙	◙
使用者進出日誌	◙	⊡	◙	◙
避免木馬程式	⊡	⊡	⊡	⊡
掃描或診斷軟體	⊡	◘	⊡	⊡
除錯及自我測試	◘	◘	◘	⊡
2 硬體風險防護措施				
不斷電系統	■	■	■	■
門禁刷卡管制	◙	◙	◙	■
定期磁碟檢查	◙	◙	◙	◙
監視裝置	⊡	◘	⊡	⊡
異地備援	⊡	◘	⊡	⊡
3 資料風險防護措施				
定期備份資料	■	■	■	■
登入電腦密碼	■	■	■	■
強迫路徑設定	■	◙	■	■
存取權限設定	◙	◙	◙	◙
資料庫修改程序	◙	⊡	◙	◙
異動記錄(日誌)	⊡	⊡	⊡	◙
媒體報廢處理	⊡	⊡	⊡	◙
儲存媒體控管	◘	◘	◘	◘
4 網路風險防護措施				
防火牆架設	■	■	■	■
線路備援	◙	⊡	◙	◙
偵測入侵行為	⊡	◘	⊡	⊡
密文方式傳送	⊡	◘	⊡	⊡
網路身份確認	⊡	◘	◘	⊡
連線時間限制	◘	□	◘	◘
數位簽章使用	◘	□	◘	◘

管理面風險	整體	資訊化程度 低	中	高
5 實體環境風險防護措施				
空調設備	■	■	■	■
防火措施或火險	◙	◙	◙	◙
避雷裝置	⊡	⊡	◙	⊡
防水措施或水險	⊡	⊡	⊡	⊡
防震措施或震險	⊡	◘	⊡	⊡
6 人為風險防護措施				
離職帳號撤銷	■	■	■	■
員工保密契約	⊡	⊡	◙	◙
操作及應變程序	⊡	⊡	◙	◙
不定期系統稽核	⊡	⊡	⊡	◙
資訊操作訓練	⊡	⊡	⊡	⊡
資訊安全課程	⊡	◘	⊡	⊡
資訊安全顧問	◘	□	◘	◘
7 管理相關風險防護措施				
7.1 資訊安全政策				
安全政策文件	◙	⊡	◙	◙
營運持續計劃	⊡	⊡	⊡	◙
安全職責歸屬	⊡	⊡	⊡	⊡
7.2 法律風險防護				
智慧財保護政策	⊡	⊡	⊡	◙
隱私權保護政策	⊡	◘	◘	⊡
7.3 風險轉嫁措施				
專業保全系統	◘	□	◘	◘
第一責任險	◘	◘	□	◘
專業外包系統	◘	◘	□	◘
第三責任險	□	□	□	□

[a]□表示僅執行 10%以下措施、◘執行率 10.1%~35%、⊡執行率 35.1%~65%、◙執行率 65.1%~90%、■執行率 90.1%以上

表 13：不同資訊化程度下，各項資訊風險對企業經營威脅認知 [ab]

	低資訊化程度			中資訊化程度			高資訊化程度		
風險認知	過去	現在	未來	過去	現在	未來	過去	現在	未來
軟體風險認知	3.41	3.66△	3.67	3.38	3.91△	4.22▲	3.82	4.24△	4.25
硬體風險認知	3.44	3.41	3.13▽	3.67	3.92	4.0	3.88	3.95	3.85
資料風險認知	3.63	3.61	3.61	3.38	4.05△	4.22	4.25	4.63△	4.69
網路風險認知	3.47	4.21△	4.49△	3.14	4.38△	4.59	3.64	4.80△	5.01▲
實體風險認知	3.51	3.26▽	3.30	3.50	3.77	3.97▲	3.46	3.89△	3.88
人為風險認知	3.59	3.67	3.67	3.11	4.05△	4.20▲	4.38	4.63△	4.59
法律風險認知	2.50	2.80△	2.93	3.08	3.59△	3.67	3.22	3.63△	3.79▲

[a]7 點量表，平均值愈高顯示風險認知威脅性愈大

[b]△該威脅目前比過去顯著增加　▲該威脅未來比現在顯著增加　▽顯著遞減

中度資訊化者則認為目前主要風險威脅來源是網路、資料、人為風險三項。軟體、法律風險雖然不是目前主要風險，但相較過去五年，威脅性卻有顯著提高。未來主要資訊風險威脅仍來自網路、資料、軟體、人為等，其中軟體、人為風險呈顯著性增加。

高度資訊化者認為其目前之資訊風險主要來自網路、資料、人為、軟體四項。此外，實體及法律風險之威脅性也比過去顯著增加。而對未來之預期則以網路、資料、人為及軟體風險為主要威脅來源，其中網路風險的威脅性顯著增加。值得一提的是，法律風險也被認定為未來威脅性顯著增加的項目。

伍、研究發現與結論

一、研究結果彙整

由前述分析結果可以發現，產業間在資訊風險威脅、安全防護現況以及未來資訊風險趨勢之看法上，確實有顯著性的差異存在；此外，企業本身之資訊化程度亦是一顯著影響這些差異的因素。本節除將這些研究結果依產業型態及企業資訊化程度分別列表彙整說明外，並提出相對之資訊安全需求特色，彙整結果請見表 14 及表 15。

(一)資訊安全需求與產業別關係彙整

表 14 顯示本研究所發現四產業在目前資訊風險、安全防護現況優劣、與未來風險趨勢之認知，以及其所相對應之資訊與資訊安全需求特色。由表 14 可發現，傳統製造業及流通服務業之資訊需求主要是資訊可用性、高科技業主要在資訊機密性、而金融保險業則主要是資訊之完整性及機密性上。這些結論除源自文獻(如 Jung et al. 2001)及本文前述之分析結果外，亦來自本研究在資料分析過程中之觀察。比如***傳統製造業***資訊需求之所以較低，乃因其資訊系統主要在輔助作業性，非策略性之活動，且其主要商品，包括鋼鐵、塑膠、紙張…等，皆屬於實體製造商品，產品本身資訊化不易；

也因此表 14 建議其資訊安全策略應朝向「如何維持資訊之可用性」發展。而*高科技產業*之資訊應用常發生於產品及製程的技術創新，直接影響企業的經營，故表 14 建議其資訊應首重隱密性。*金融保險業*對資訊安全要求較嚴苛，任何可能威脅客戶帳戶資料的風險都必須避免，尤其應確保資訊不被篡改及機密資料不被揭露，故表 14 建議其資訊應首重資料之完整性與機密性。至於*流通服務業*，本研究結果顯示其屬於高資訊化之應用層次，但卻具相對較低之資訊安全需求認知。這可能是因為其資訊通常涉及較少敏感性資料之故，因此其資訊需求乃以維繫系統之正常運作為主。

表 14：產業型態與資訊安全需求之差異性分析結果彙整

		產業別			
		傳統製造業	高科技產業	金融保險業	流通與服務業
研究結果	1. 目前主要資訊風險[a]	—	網路、人為、資料、軟體風險	網路、資料、人為、軟體、硬體、實體風險	網路、人為、資料風險
	2. 安全防護現況之優劣[b]	—	良：資料及軟體風險防護 劣：網路及人為風險防護	優：硬體風險防護 良：資料、軟體、實體 普：網路、人為 劣：資訊風險轉嫁措施	良：資料風險防護 劣：網路及人為風險防護
	3. 未來風險趨勢	無顯著增加項目	無顯著增加項目	網路風險、人為風險、法律風險皆會顯著增加	網路風險顯著增加
需求特色	1. 資訊需求	資訊可用性	資訊隱密性	資訊完整性與隱密性	資訊可用性
	2. 資訊安全需求	維持資訊可用性	補強網路及人為風險防護不足	法律風險防護、資訊風險轉嫁	補強網路及人為風險防護不足，注意未來網路風險對企業影響

[a] 依風險威脅認知由高至低排序 [b] 目前防護措施之執行率屬優(80%以上)、良(70%~80%)、普(60%~70%)、及劣(60%以下)四級

表 14 同時亦顯示四產業之資訊安全需求特色(請見表 14 最後一列)，這些安全需求乃根據本研究所測出之各產業目前主要資訊風險中，安全防護現況做得較差(劣)的項目，以及未來對企業威脅比較可能增加之風險項目的認知所制定及建議。從這些建議可以發現，高科技產業應補強網路及人為風險防護；金融保險業應強調法律風險防護及資訊風險轉嫁措施；流通服務業也應注意網路及人為風險對企業之影響。值得一提的是，由於金融保險業必須接受政府定期及不定期金檢單位稽核，研究結果顯示金融業之資訊防護在四產業中做得最好。雖然如此，但其未來資訊安全需求仍是最高。尤其應著重在「法律風險防範」及「風險轉嫁」兩方面。主要原因有二：目前未被強調之「法律風險」，被金融業者認定為未來風險顯著增加的項目之一；其次，因為無百分百安全的系統，高度風險的安全策略應朝向「風險轉嫁」的方向思考(Siegel et al.2002)。

(二)資訊安全需求與企業資訊化之關係彙整

表 15 主要以企業之資訊化程度為分類主軸，彙整研究之結果。表 15 顯示，如不以產業為分群依據，而以資訊化程度高低來審視本研究結果，則可發現資訊化程度較低企業之資訊需求主要在協助企業內部例行性作業或管理活動，因此資訊系統誤用或

停擺對組織衝擊有限，故對資訊安全之需求亦較低；其資訊安全重點應在檢視各項網路風險防範措施之必要性。資訊化程度在中階段之企業，其資訊應用特色已逐漸由集中式系統趨向分散化，應用上亦漸提升至策略層次或決策支援，因此系統誤用及停擺的風險相對較大，資訊資產價值明顯提高；受到這些資訊需求特色之影響，企業之資訊風險亦產生變化，網路、資料及人為三風險益形重要。最後，資訊化程度在高階段之企業，其資訊系統除使用於例行管理活動外，亦逐漸應用於策略規劃、尋求市場之競爭優勢、客戶關係管理、與夥伴協同產銷上。由於資訊需求範圍已經延伸到企業外部，各項資訊風險重要性彼此有消長，資訊安全需求亦產生變化。比如未來法律風險的增加，可能是資訊系統範圍已擴大至企業外部的緣故。高資訊化企業雖然相較其它企業資訊防護措施執行徹底，然而網路及管理相關風險防護仍執行不足。表 15 顯示，高資訊化企業之資訊安全策略除應朝向如何防治網路漏洞外，更應朝向資訊安全政策制定、法律風險的防護、以及風險轉嫁措施的執行，以確保無絕對安全的資訊系統正常運作。

表 15：資訊化程度與資訊安全需求之差異性分析結果彙整

		資訊化程度		
		低（階段二三）	中（階段四）	高（階段五六）
研究結果	1. 目前主要資訊風險[a]	網路風險	網路、資料、人為風險	網路、人為、資料、軟體風險
	2. 安全防護現況之優劣[b]	劣：網路風險防護	良：資料風險防護 劣：網路及人為風險防護	良：軟體及資料風險防護 普：人為風險防護 劣：網路及管理相關風險防護
	3. 未來風險趨勢	網路風險顯著增加 硬體風險顯著降低	軟體風險、實體風險、網路風險、人為風險皆會顯著增加	法律風險顯著增加
需求特色	1. 資訊需求	1. 集中式系統架構或存在功能重覆的小系統 2. 支援企業內部作業及管理活動	1. 集中或非集中式系統架構 2. 支援內部決策活動	1. 分散式系統架構或整合上下游夥伴系統 2. 支援客戶關係管理或資訊導向之產品及服務
	2. 資訊安全需求	著重網路風險防範	補強網路及人為風險防護不足	網路安全措施、資訊安全政策制定、法律風險防護、資訊風險轉嫁

[a] 依風險威脅認知由高至低排序 [b] 目前防護措施之執行率屬優(80%以上)、良(70%~80%)、普(60%~70%)、及劣(60%以下)四級

二、資訊風險之趨避及安全防護策略

依據前述產業型態、資訊化程度與相對資訊安全需求間之關係，可以一 2×2 矩陣圖(如圖 2 左邊所示)。此圖分別以資訊化程度及資訊安全需求為橫、縱兩向度，並依個別向度再分別分為高、低水平；而依前述分析結果，可將四產業在此兩向度之中心點分別畫於此 2×2 方格內。此圖顯示金融保險及高科技產業屬高資訊化且高資訊安全需求之雙高產業；傳統製造業則屬低資訊化且低資訊安全需求之雙低產業；而流通服務業雖有高資訊化程度，但對資訊安全之需求並不高。

Birch & Mcevoy (1992)及 Pipkin (2000)曾提出四項資訊安全策略應考量重點—風險減緩、風險自承、風險規避及風險轉嫁。Birch 及 Pipkin 雖提出此四重點，但並未將此重點與企業所需之資訊安全需求作一適切聯結，圖 2 右邊之資訊安全策略乃依據 Birch 與 Pipkin 之策略及本研究所得出之資訊安全需求結論所提出一適切之資訊安全策略。由圖 2 右邊可發現，當資訊安全需求較低(或風險較小)時，安全策略須以「風險自承」及「風險減緩」為主，前者主要是風險為組織容許的範圍內自行承擔；後者為閃避主要的風險項目之威脅。倘若資訊安全需求較高(或風險較大)時，安全策略應以「風險規避」及「風險轉嫁」較適當，「風險規避」策略主要是執行保護措施，以降低可能之資訊風險至組織可接受之範圍；而「風險轉嫁」策略是當資訊風險或資訊資產重要性已經大到危及組織之主要活動或生存，適度將過高之風險移轉至其它組織。

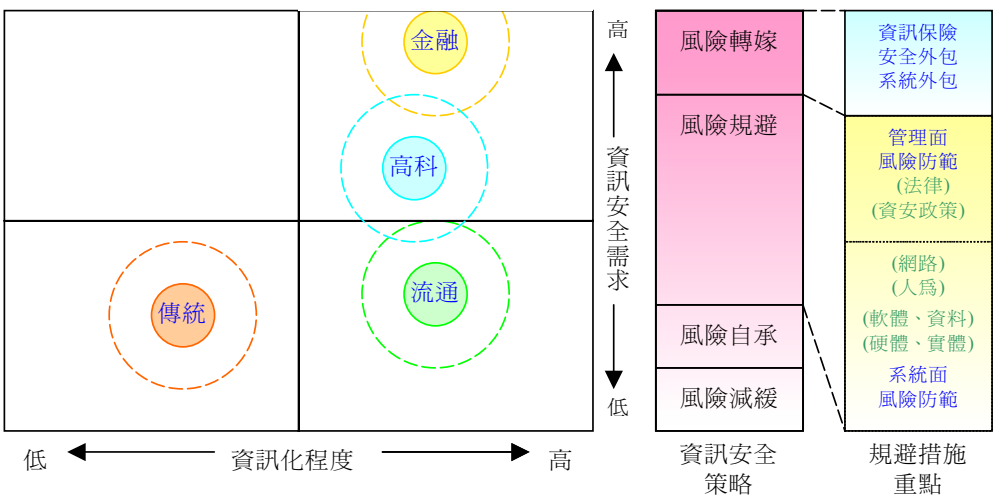

圖 2：企業之資訊安全策略圖

對於風險較大且無法閃避之資訊風險項目，多數企業採用「風險規避」措施以降低風險。再輔以前述研究結果—各產業及資訊化程度之資訊安全差異化需求，進行交叉分析，本研究亦歸納出規避措施重點方格(如圖 2 最右邊之規避措施重點所示)。主要意涵如下：當執行「風險規避」策略時，不同資訊安全需求之企業應著重不同「風險規避」策略，當資訊安全需求較低(或風險較低)時，資訊安全應著重在系統面之風險防範，如早期應以軟體、硬體、實體、資料風險防範措施為主，而後再延伸到網路及人為風險之防範措施。倘若資訊安全需求較高(或資訊風險較大)時，其系統面風險防範已達某個水準，其規避措施應朝向資訊安全政策之制訂、法律風險防範等較管理面之防範措施。

至於「風險轉嫁」策略，中小企業受限資訊資源稀少且資訊人力培養成本較高，應採整體「資訊系統外包」為宜；而較大型企業而言，因其保有資訊部門及相關技術人才，或敏感資料之處理，整體資訊系統外包較不適宜，風險轉嫁措施應採「安全外

包」或「資訊保險」，不但將資訊技術保留在企業內部且降低過高自承風險。

過去文獻顯示，多數企業在資訊資源分配都傾向「資訊系統功能」而忽略「資訊安全」議題，如何運用極稀少的資訊資源在資訊安全維護上，「資訊安全策略」之有效性將可以解決組織之困擾，這是本文提供「資訊安全策略」建議之主要目的。資訊主管在擬定資訊安全策略時，能藉由自身產業特性及透過本文前述所提供之「資訊化程度」指標式確認資訊化程度，擬定有效之資訊安全策略。

參考文獻

1. 李東峰、林子銘，2001，「企業資訊安全政策之探索性分析」，第七屆資訊管理研究暨實務研討會論文集，中華民國資訊管理學會。
2. Aivazian, C. “Information Security during Organizational Transitions,” *Information strategy: the executive's journal* (14:3) 1998, pp:21-27
3. Birch, D. G.W. and McEvoy, N. A. “Risk analysis for Information Systems,” *Journal of Information Technology* (7) 1992, pp:44-53
4. BSI (2002), BS7799-2:2002 British Standards for benchmarking Information Security Management Systems (ISMS)
5. Earl, M. J. *Management Strategies for Information Technology*, Prentice Hall, Hemel Hempstead, 1989
6. Eloff, M.M. and von Solms, S.H. “Information Security Management: A Hierachical Framework for Various Approaches,” *Computer & Security* (19) 2000, pp:243-256
7. Fitzgerald, K. J. “Information security baselines,” *information management & Computer Security* (3:2) 1995, pp:8-12
8. Galliers, R. D. The developing information systems organization: an evaluation of the ‘stages of growth’ hypothesis, paper presented at the London Business School, January 1989.
9. Galliers, R. D. and Sutherland, A.R. “Information systems management and strategy formulation: the ‘stages of growth’ model revisited,” *Journal of Information Systems* (1) 1991, pp:89-114
10. 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:13-22
11. Gibson, D. and Nolan, R.L., “Managing the four stages of EDP growth,” *Harvard Business Review*, (52:1) January-February 1974
12. Hoffer, J.A., and Straub, D.W. “The 9 to 5 underground: Are you policing computer crimes?” In P. Gray, W.R. King, E.R. Mclean, & H. Waston(Eds.), *Management of information systems* (pp:388-401) Fort Worth, TX: Harcourt Brace, 1994
13. Icove, D., Seger, K., and Vonstorch, W. *Computer Crime*, O’REILLY, 1999
14. Jarvenpaa, S.L., and Ives, B. Information technology and corporate strategy: A view from the top, *Information Systems Research* (1:4) 1990, pp:351-375
15. Jung, B., Han, I., and Lee, S. “Securtity threats to Internet: a Korean multi-industry investigation,” *Information & Management* (38:8) 2001, pp:487-498
16. Kankanhalli, A., Teo, H.-H., Tan, B. C.Y., and Wei, K.-K. “An integrative study of information systems security effectiveness,” *International Journal of Information Management* (23) 2003, pp:139-154
17. King, W. R. “Organizational characteristics and information systems planning: An

empirical study," *Information Systems Research* (5:2) 1994, pp:75-109
18. Kotulic, A.G. and Clark, J.G. "Why there aren't more information security research studies," *Information & Management* (41:5) 2004, pp:597-607
19. Kwok, L.-F. and Longley, D. "Information security management and modeling," *Information Management & Computer Security* (7:1) 1999, pp:30-39
20. Lichtenstein, S. "Factors in the selection of a risk assessment method," *Information Management & Computer Security*, (4:4) 1996, pp:20-25
21. Loch, K.D., Carr, H.H., and Warkentin, M.E. "Threats to information systems: Today's reality, yesterday's understanding," *MIS Quarterly* June 1992, pp:173-186
22. McFarlan, F. and McKenney, J. *Corporate Information Systems Management: The Issues Facing Senior Executives*, Dow Jones Irwin, New York, 1983
23. Nolan, R. "Managing the crises in data processing," *Harvard Business Review* (57:2) March-April 1979
24. Peltier, T.R. *Information security risk analysis*, Auerbach, New York, 2001
25. Pipkin, D.L. *Information security protecting the global enterprise*, Hewlett-Packard, New Jersey, 2000
26. Rainer Jr., R.K., Snyderr, C.A. and Carr, H.H. "Risk analysis for information technology," *Journal of Management Information Systems* Summer 1991, pp: 192-197
27. Richardson, R. "2003 CSI/FBI Computer crime and security survey," Computer Security Institute 2003. Accessed 20 Sept. 2003 http://www.gocsi.com/.
28. Ryan, S. D. and Bordoloi, B. "Evaluating security threats in mainframe and client/server environments," *Information & Management*, (32:3) 1997, pp:137-146
29. Ølnes, J. "Development of security policies," *Computers & Security* (13) 1994, pp:628-636
30. Sharma, S. *Applied Multivariate Techniques*, Wiley, New York, 1996.
31. Siegel, C.A., Sagalow, T.R., and Serritella, P., "Cyber-Risk Management: Technical and Insurance Controls for Enterprise-level Security," *Security management practices* Sept./Oct. 2002, pp:33-49
32. Siponen, M.T. "Towards maturity of information security maturity criteria: six lessons learned from software maturity criteria," *Information Management & Computer Security* (10:5) 2002, pp:210-224
33. Smits, M.T., van der Poel, V.G., and Ribbers, P.M.A. "Assessment of information strategies in insurance companies in the Netherlands," *Journal of Strategic Information Systems* (6:2) June 1997, pp:129-148
34. Straub, D.W. "Computer abuse and computer security: Update on an empirical study," *Security, Audit, and Control Review*, (4:2) 1986, pp:21-31
35. Straub, D.W., and Welke, R.J. "Coping with systems risk: security planning models for management decision making," *MIS Quarterly* December 1998, pp:441-469
36. Vermeulen, C. and von Solms, R. "The information security management toolbox-taking the pain out of security management," *Information management & computer security*, (10:3) 2002, pp:119-125
37. Von Solms, R. "Information Security Management: why standards are important," *Information Management & Computer Security* (7:1) 1999, pp:50-57
38. Von Solms, R.; H., Haar, van de; von Solms S.H.; and Caelli, W.J. "A framework for information security evaluation," *Information & Management* (26) 1994, pp:143-153
39. Von Solms, R. "Information Security Management: The Second Generation," *Computers & Security* (15:4) 1996, pp: 281-288

附錄 A：問卷

一、公司基本資料

1. 請問 貴公司成立至今幾年？□1~5 年 □6~10 年 □11~15 年 □16~20 年 □20 年以上
2. 請問 貴公司員工人數約：□50 人以下 □51-100 人 □101~200 人 □201~500 人 □501~1000 人
   □1001~2000 人 □2001~5000 人 □5001 人以上
3. 請問 貴公司屬於那一種產業？□資訊服務體業 □食品製造業 □塑膠紡織化學業 □金融保險業
   □電子業 □運輸倉儲通訊業 □營造建築業 □一般商業、服務業 □水電燃氣業 □非營利事業 □其它(請填寫) _____
4. 貴公司 90 年度之營業額約：□1000 萬以內 □1000 萬~2000 萬 □2000 萬~5000 萬 □5000 萬~1 億
   □1 億~10 億 □10 億~50 億 □50 億~100 億 □100 億以上

二、公司之資訊系統應用特色

1. 請由下列問題中，選出一項目前 貴公司最主要之資訊策略層次：(請單選)
   □僅幫助公司各部門取得必要之軟硬體
   □除上述軟硬體取得外，主要在依各部門使用者需求，開發各部門之特殊軟體
   □除上述兩項功能外，主要在考量公司之整體資訊需求，開發跨部門之資訊系統
   □除上述三項功能外，主要在控制協調各部門資訊資源分配，以整合公司整體資訊資源
   □除上述四項功能外，主要在檢視外部競爭環境，尋找資訊科技可能帶來的新機會
   □公司為業界之領導，除上述五項功能，主要利用現有資訊技術，維持企業之領導地位與優勢
   □其它_____
2. 請依您的看法，由下列敘述中選出一項最符合 貴公司目前資訊部門結構層次：(請單選)
   □目前無資訊部門，各功能部門自行控制資訊業務
   □目前無資訊部門，各功能部門資訊業務集中於 _____ 部門(請填寫)
   □有資訊(或資料處理)部門，各功能部門資訊業務皆集中於該資訊部門處理
   □有資訊部門外且成立資訊中心提供使用者開發系統諮詢服務、或程式撰寫之函數、記錄取得
   □資訊部門協助公司策略單位共同研擬公司策略。(資訊單位可影響公司策略單位之決策)
   □資訊單位主導公司未來之發展，是公司之策略單位
   □其它_____
3. 請依您的看法，由下列敘述中選出一項最符合 貴公司目前資訊系統結構之狀態：(請單選)
   □公司內部存在多個未整合的小型資訊系統，彼此獨立作業
   □公司嘗試整合內部各資訊系統，然而系統間仍存在相同、重複的功能
   □公司之資訊系統屬「集中化系統」，由總公司集中控制
   □公司之資訊系統屬「分散式系統」，總公司不易控制分散在外資源
   □公司之資訊系統屬「分散式系統」，但總公司能有效控制分散在外的資源
   □公司之資訊系統屬整合上下游廠商外部資料的資訊系統
   □其它_____
4. 請依您的看法，由下列敘述中選出一項最符合 貴公司目前資訊系統應用狀況：(請單選)
   □公司之資訊系統僅限於「財務」或「會計」方面的應用
   □公司之資訊系統主要用來解決人工作業流程的自動化，增加流程效率
   □公司之資訊系統幾乎支援公司所有內部各項管理、作業活動
   □公司之資訊系統除了上述支援公司內部活動外，也具備決策支援功能
   □公司之資訊系統除了上述支援內部活動及決策外，也支援行銷面客戶關係管理
   □公司之產品及服務以資訊為導向，須賴資訊系統才能完成所有生產或提供服務
   □其它_____

三、請依您對 貴公司資訊系統安全措施之認知，勾選 貴公司目前所採行之各項系統風險防護措施。若有其它未列之風險防護措施，請於其他欄填寫。

1. 公司目前採行之軟體風險防護措施：(可複選)
   □使用者進出資訊系統時，有詳細時間、作業流程之日誌記錄
   □公司有防毒軟體來保護系統
   □系統因不可抗拒因素而停止作業時，系統能夠回復原來狀態
   □系統運作可以同時多個人使用而不相衝突，造成軟體之損壞
   □系統可以透過掃描軟體，診斷目前安全程度
   □系統本身具有除錯、自我測試的功能
   □系統修正時，需經相關部門主管認可，方可作修改
   □系統修正時，需經測試與驗證，方可正式使用
   □軟體開發與取得時，會避免讓惡意程式附於軟體上(如隱密通道、特洛依木馬程式等)
   □其它軟體風險防護措施，請說明：_____
2. 公司目前採行之硬體風險防護措施：(可複選)
   □公司設有異地備用電腦以應付硬體突發狀況
   □公司設有監視裝置，保護系統硬體的安全
   □公司設有門禁刷卡系統或其它門禁管制措施
   □公司設有不斷電系統以因應停電
   □會定期磁碟檢查、掃瞄和恢復損毀的磁區，以及修正檔案系統的錯誤
   □其它硬體風險防護措施，請說明：_____
3. 公司目前採行之資料風險防護措施：(可複選)
   □定期備份資訊系統資料
   □登入電腦時，會首先檢查使用者名稱及使用者密碼
   □電腦中檔案皆設有每位使用者的新增、刪除、修改權限
   □使用者依其職位，僅能查詢其應知道的資料
   □系統對每項異動都有詳細記錄
   □電腦系統不安裝軟碟機
   □未透過使用者介面的資料庫修改，必須透過相關部門主管認可之程序，方可修改
   □資料儲存媒體的報廢須經特定程序處理
   □其它資料風險防護措施，請說明：_____
4. 公司目前採行之實體與環境風險防護措施：(可複選)
   □公司有避雷裝置，保護資訊系統
   □公司主要的資訊系統相關硬體設備皆位於空調室內
   □公司在系統設計時，有考慮防火措施(或保火險)
   □公司在系統設計時，有考慮防水措施(或保水險)
   □公司在系統設計時，有考慮防震措施(或地震險)
   □其它實體與環境風險防護措施，請說明：_____
5. 公司目前採行之網路風險防護措施：(可複選)
   □公司對外傳輸重要資料時，會以密文方式傳送
   □對外資料之傳輸或交流都會要求對方身份之確認
   □公司系統能偵測第三者入侵行為
   □公司對外資訊交流設有防火牆
   □公司對外資訊交流有多條線路以為備援
   □公司對外之資訊服務有要求客戶使用數位簽章或認證
   □公司主機有連線時間限制
   □其它通訊風險防護措施，請說明：_____
6. 公司目前採行之人為風險防護措施：(可複選)
   □員工須簽定保密契約，防止員工洩露機密
   □公司有處理離職員工電腦存取權的撤銷
   □公司有選聘資訊安全顧問來協助資訊安全事務
   □公司有不定期系統稽核，以避免員工憑藉其專業知識而搞鬼
   □公司定期辦理資訊安全課程，增加員工資訊安全防護能力
   □公司定期辦理資訊業務操作課程，避免員工操作錯誤產生損失
   □公司有完整系統操作程序檔案，或系統操作錯誤的應變處理程序

□其它人為風險防護措施，請說明：_____

7. 公司目前採行之管理相關風險防護措施：(可複選)

□公司聘有專業廠商保全資訊系統，以確保資訊系統使用時之可靠度
□公司委託專業廠商外包資訊系統安全
□公司有隱私權具體保護政策及措施
□公司有智慧財產權具體保護政策及措施
□公司有承保資訊系統財產保險，以降低系統無法正常運作之損失。(第一人險)
□公司有承保資訊系統內容之責任險，以降低資訊內容錯誤所引發之第三責任風險
□公司有明確的資訊安全政策文件及程序
□公司有明確的資訊安全職責歸屬文件及程序
□公司有營運持續計劃，以因應重大災難發生所造成之營運中斷
□其它管理相關風險防護措施，請說明：_____

四、請依您自己的看法 分別填寫下列各項風險對 貴公司經營之威脅程度，請依過去、目前、及未來之狀況圈選。1 表該項風險威脅性很低，7 表該項風險威脅性很高，以此類推。

	過去(約五年前) (公司未滿五年者不用填)	目 前	未 來
	低 ← → 高	低 ← → 高	低 ← → 高
實體與環境風險之威脅....	1 2 3 4 5 6 7	1 2 3 4 5 6 7	1 2 3 4 5 6 7
硬體風險之威脅.....	1 2 3 4 5 6 7	1 2 3 4 5 6 7	1 2 3 4 5 6 7
軟體風險之威脅.....	1 2 3 4 5 6 7	1 2 3 4 5 6 7	1 2 3 4 5 6 7
資料風險之威脅.....	1 2 3 4 5 6 7	1 2 3 4 5 6 7	1 2 3 4 5 6 7
網路風險之威脅.....	1 2 3 4 5 6 7	1 2 3 4 5 6 7	1 2 3 4 5 6 7
人為風險之威脅.....	1 2 3 4 5 6 7	1 2 3 4 5 6 7	1 2 3 4 5 6 7
法律風險之威脅*.....	1 2 3 4 5 6 7	1 2 3 4 5 6 7	1 2 3 4 5 6 7
其它(請說明)_____..	1 2 3 4 5 6 7	1 2 3 4 5 6 7	1 2 3 4 5 6 7

* 法律風險如智慧財產權誤用、隱私權之侵權、以及資訊內容所引發之第三責任。