國立臺灣大學管理學院資訊管理學研究所

碩士論文

Department of Information Management
College of Management
National Taiwan University

Master Thesis

董事會組成與資訊安全管理有效性之關聯性研究

-以管家理論為觀點

The Effective of Information Security Management and Board Composition: A Stewardship Perspective

江昱其

Yu-Chi Chiang

指導教授：許瑋元 博士

Advisor: Wei-Yuan Hsu, Ph.D.

中華民國 101 年 06 月

June 2012

國立臺灣大學碩士學位論文
口試委員會審定書

董事會組成與資訊安全管理有效性之關聯性研究
-以管家理論為觀點

The Effective of Information Security Management and Board Composition: A Stewardship Perspective

本論文係江昱其君(R99725031)在國立臺灣大學資訊管理學系、所完成之碩士學位論文，於民國 101 年 06 月 28 日承下列考試委員審查通過及口試及格，特此證明

口試委員：許瑋元

張欣綠　　戴基峯

所　　長：李瑞庭

誌謝

來到了提筆寫誌謝的這一刻，日子已經過了兩年。在這一路搖搖晃晃走過的生產論文日子裡，首先要感謝的是我的指導教授，許瑋元老師。如果說寫論文對我而言是一個不見天日的黑洞，那老師就是我走向洞口處的明燈，在矛盾與困惑的黑暗期，謝謝老師總以陽光般的笑容給予我一個充滿信心的方向，在邏輯打結萬念俱灰的撞牆期，謝謝老師不厭其煩的聽我告解，並提出精闢的見解，為我一一的拆開死結。在面對無數未知的未來，每次與您的談話都讓我有更多的勇氣，堅定的邁向人生下一個階段。其次，王大維老師在我論文草創時期，教導我許多跨領域的知識，提供我不同領域的思考邏輯與專業知識，讓我能更多元的思考，為產出論文的過程打下厚實的根基。老師，謝謝您。此外，感謝張欣綠老師與戴基峯老師於口試的過程中給予論文指教，謝謝您們用心的一字一句，讓我的論文能更加的完整。

Carol Lab 的大家，首先感謝的是學長姐們。育滋學姐，謝謝你教導我許多碩士生應該具備的技能以及思考邏輯，你的傳承讓我在往後一年的研究路上都非常的受用，謝謝你，真的很高興在人生的道路上能夠認識模姐;Shirley 學姐，就像我的心靈導師，在我為人生的路困惑的同時，給予我正面的信心與能量，我永遠都會記住您告訴我的:未來還有許許多多艱難的路要走，勇敢的面對自己的每一個決定;比爾哥，謝謝你在回國短短的幾天，願意花上一個下午為我排憂解惑，謝謝你在各方面給我的指教，不論是在論文上或是在未來工作上，你都給我許多非常受用的意見，謝謝你;小開與歐歐，剛好大一屆的你們是我最佳的模範，跟著你們的腳步，一步步的融入 Carol lab 的組織文化，歐歐謝謝你，即使畢業了，你仍對我持續的關心，謝謝你在工作之餘還忍受到我的諮詢，並且提供我在研究上的幫助與解惑，謝謝你。最後，呂昂、楊昕、林孜我這些單名的 LAB 胞們，一路上謝謝你們的陪伴，時而聽我抱怨，時而忍受我的無厘頭，謝謝你們，我們一起走過了，還有學弟妹們阿尖、小桃、彥伶和良丞，謝謝你們全程的協助口試的進行，幫忙採買、消化、提重物，辛苦你們了。

能夠在這邊提筆寫誌謝,都必須要感謝我身邊有一群不斷不斷的在幫助我、鼓勵我、

忍受我的笑點的同學與朋友，蔡歐盆、陳魔菇、林蠻弟、宜平、莊小璧，碩一時收留我的涵涵、周宣宣和美果以及九個月的室友小天才，還有我心中永遠的同儕也是我的好飯咖假掰妹珺，辛苦你們了，不論是聽我倒苦水或是忍受我的冷笑話，因為有你們的支持和大力相助，我才能夠科科難過科科過，我才能不露宿街頭，有好吃的晚餐等著我回家，有好聽的音樂等著我回宿舍。我的好友群們，蕭璇、米飛、菜渣、米米和愛瑪利還有發發們，元元、半半、張髒、韋香、仁、許芷瑋，每次聚餐聊天都給我一次又一次前進的動力，謝謝這些日子有你們在我身邊，為我帶來許許多多歡笑與回憶，因為有你們，我才能一步步的走到這，謝謝你們。

最後要感謝，也是最最重要的，就是我的家人。爸媽，謝謝你們在這求學的路上給我十足的信心，適時的給我安慰與鼓勵，讓我深深感受到家是最好的避風港，你們是我最信賴的靠山，真的很幸運能夠有你們這麼棒的爸媽，謝謝你們。再來是最疼我的姐姐，姐，謝謝你對我的照顧與關心，裡裡外外，上至論文研究，下至生活起居，許許多多生活大小事，都依賴你的幫忙，而在人生的經歷上你總是走在我的前端，不論是在論文研究、工作職場或是心靈成長方面，總是能以過來人的角度給我安心定神的良方。姐，謝謝你，對我無微不至的照顧，你總是默默的對我付出，卻時常要忍受我古怪的脾氣和思想，辛苦你也謝謝你。最後是我的哥哥，哥，謝謝你在學業的路上當我的學習範本，因為有你給我一路的跟隨與指導，我才能順利的走到這。謝謝你總是能夠給我不一樣的人生觀與國際觀，看著你走過的路，總讓我覺得人生還有無限的可能，有各式各樣的生活等著我去體驗。最後的最後，要告訴自己說，在學習的過程中有苦有淚，有樂有笑，但這就是人生，而畢業只是人生下一個階段的開始，在面對未來更多的苦樂，要具備勇氣與實力，追求自己的夢想，勇敢走自己的路。然後再大聲的告訴自己說:一路走來辛苦了!恭禧，畢業了!

摘要

本研究的主要目的在於探討台灣上市(櫃)公司董事會組成對於公司資訊安全管理有效性的關聯性。透過管家理論的觀點，以台灣經濟新報資料庫(TEJ)取得董事會組成資料，如:總經理的雙元性、內部董事比例、獨立董事比例，結合手動搜尋網站資料所取得的資訊安全事件樣本，探討董事會組成是否影響資訊安全事件發生的可能性以及資訊安全事件發生的次數。結果顯示，獨立董事占董事總席次的比例愈高，其資訊安全管理有效性愈差。此外，本研究將進一步的透過股權型態的分類來探討探討董事會組成對於公司資訊安全管理有效性的影響，其結果發現，股權型態為家族型態，其內部董事比例愈高、公司規模愈小、獨立董事比例愈低，資訊安全管理成效愈高。股權型態為非家族型態，其董事長與總經理由不同人兼任的企業，資訊安全管理成效愈高。

關鍵字:資訊安全管理、公司治理、董事會架構、管家理論

Abstract

This thesis focuses on the relationship between the effectiveness of information security management and the composition of the board. We build our hypotheses based on the stewardship theory. Using the data from Corporate Governance DB of Taiwan Economic Journal and the manually-searched information security breaches from Information Security and UDN website, we investigate that whether the composition of the board could affect the occurrence of information security breaches. Our results demonstrate that as the percentage of independent director increases, the effectiveness of information security management decreases. Furthermore，we also investigate the association between the effectiveness of information security management and the composition of the board after classifying by ownership structure- family firm or non-family firm. Our results demonstrate that for family firm, as the percentage of insider director increases, the size of company decreases, and the percentage of independent director has a negative impact on the effectiveness of information security management increase. For non-family firm, chairman and chief executive officer taken by different people has a good impact on the effectiveness of information security management.

Keywords: information security management, corporate governance, board composition, stewardship theory

目錄

表目錄

第一章　　導論

在現今高度依賴資訊科技且網際網路普及的社會下，資訊科技不僅協助企業提升決策品質與營運績效，更加便利組織間的溝通與合作。透過妥善的運用資訊科技，企業創造更多的競爭優勢與成功機會。隨著資訊科技在企業的策略優勢與營運作業中扮演愈來愈重要的角色，資訊科技所帶來的資訊安全議題也愈來愈受到重視。資訊是組織的重要資產之一，和其它重要的營運資產一樣具有價值，因此對任何組織而言，都必須要持續給予資訊妥善的保護 (BS 7799-2, 1999) 。

第一節　研究動機與目的

根據美國第二大通信廠商 Verizon 與美國特勤局(U.S. Secret Service)以及荷蘭國家警察局(Netherlands Policy Agency，KLPD)屬下的國家高科技罪案組(National High Tech Crime Unit)共同合作調查的「2011 資料外洩調查報告」中指出，2010 年網絡攻擊導致的資料外洩個案總數創下歷來新高。此外，美國聯邦政府問責事務處(U.S. Government Accountability Office)發現美國政府網站遭駭客攻擊次數由 2006 年的 5503 次，至 2010 年 41776 次，5 年內成長了 6.5 倍。近年來，由於資訊安全事件數量的攀升、網路攻擊事件頻傳，使得政府以及企業都持續關注資訊安全議題。資訊安全問題不僅影響國家安全問題，更為企業帶來嚴重的財務損失。隱私暨資訊管理研究機構 Ponemon Institute 接受惠普科技(HP)旗下子公司 ArcSight 委託，針對網路犯罪進行研究報告調查指出，網路犯罪導致企業利潤受極大損失，2011 年中報告損失金額$5,895,065 相較於 2010 年中的$3,788,468，大幅增加 56%的損失金額。資訊科技原被視為企業競爭優勢之利器，亦是現今企業邁向成功不可或缺之物，但是透過上述的調查報告中得知，其所衍伸的資訊安全問題卻著實為企業成功之路砸下一塊巨石。在過往，企業高階管理人只需關注企業財務表現，提高企業的獲利能力，追求利潤最大化，但是隨著資訊系統在企業作業與溝通流程扮演愈來愈重要的角色，其所造成的資訊安全問題足以嚴重影響企業之持續營運與經營績效(Harris, 2003)，因此迫使企業之高階管理人必須正視資訊安全議題。

近期的研究指出，針對資訊安全控制有效性而言，技術性因素(Technological factors)並非唯一的關鍵因素，了解組織和人的因素(Organizational and Human

factors)對於資訊安全控制產生影響也是相當重要的(Kraemer et al., 2009)。因此，企業對於解決資訊安全問題，除了著重於科技技術上的增進，組織內部管理層面的議題更是不容忽視。近年來，有許多資訊安全事件皆來自於企業內部控制不當而導致，例如:濫用授權、越權操作、洩露資訊、竄改財報數據、竄改薪資資料、盜用公款等。2011 年英國倫敦的瑞士銀行(UBS)爆發內部員工，涉嫌偽造交易所買賣基金交易記錄，進行未經授權的交易長達三年，而該事件讓 UBS 損失約 20 億美元。所謂的內部控制是指由管理階層所設計，並由董事會、管理階層和其他員工所執行之管理流程，其目的在於達到實現營運的效果和效率、財務報告的可靠性、遵守相關的法律法規三大目標。現今，企業高度整合資訊科技於營運流程中，內部控制成為企業在維護資訊系統安全時非常重要的環節。所謂的資訊安全內部控制是指「協助企業控制風險並保護企業資產的實作方法、程序、政策和責任架構(Dhillon, 2001)」，透過有效的內部控制能夠確保企業流程的完整性與連續性(Dhillon, 2001; Whitman, 2003)。不完善的內部控制不僅增加資訊安全事件發生風險，更因導致資訊安全問題而為企業所帶來威脅，例如:濫用授權、越權操作、洩露資訊、病毒、惡意程式攻擊、系統當機…等，都將會直接或間接的影響企業經營績效，造成企業的財務以及商譽的損失。

內部控制對於資訊安全與企業營運的重要性，使各國紛紛透過法令的制定來規範企業，例如:美國沙賓法案(Sarbanes-Oxley Act, SOX)、日本沙賓法案(J SOX)、聯邦健康保險法案(Health Insurance Portability and Accountability Act, HIPAA)等，透過法令的約束以提高管理階層對於內部控制的責任，迫使他們注重企業內部控制，進而提升內部控制之品質。以美國沙賓法案為例，該法案的誕生是由於美國於二十一世紀初接連爆發多起大型企業的財務醜聞與盜用公款等弊案，如恩隆(Enron)、世界通訊(Worldcom)等大型企業皆利用會計手法掩蓋企業虧損，揭露不實之財務報表，因而引發震盪美國與全球金融經濟的掏空舞弊案。接二連三的金融弊案，重新喚醒社會大眾對於公司治理的重視，因而促使美國國會通過保護投資者權益的沙賓法案。其內容針對企業內部控制與風險管理進行嚴格要求，並加強會計與證券市場監管、公司治理等方面，以嚴厲的刑責確保上市公司訊息揭露的準確性和可靠性。沙賓法案中 302 條款與 404 條款更是強調管理階層對於內部控制之責任，前者強調公司財務報告的責任，要求公司營運長及財務長必須對公司財務報告提

出書面擔保，並負責建立與維持足夠的內部控制以保證財務報告的正確性，後者則針對管理階層對於內部控制的評價報告，要求管理階層必須在年度報告中匯報公司在財務報告的內部控制完善程度，並且經過外部稽核認證此報告書。就上述法案條款可得知，法規主要針對公司治理層面進行規範，明確規定公司管理階層對於公司內部控制之責任,使其必須為公司整體的治理與內部控制品質擔負責任，以符合法規之要求。

根據之前所論述，企業內部控制允當與否是影響公司資訊安全管理成效的因素之一。再者，由於內部控制對於資訊安全與企業營運的重要性，因而出現許多法案透過公司治理層面來規範管理階層的責任,使其重視公司的內部控制。因此，管理階層為符合法規之規範，在強調內部控制重要的同時，由於目前財務數據的收集、資料的傳輸、公司核心的營運與作業流程皆與資訊系統相關，更間接的必須正視資訊安全的重要性。由此可知，由於法規針對公司治理層面進行規範，使資訊安全管理的成效不再只是資訊部門主管的責任,而是提升至管理階層的責任，因此，企業資訊安全管理議題已提升至公司治理層面。根據《Information Security Governance – a call to action》的報告內容指出「公司治理是由公司所領導並管理的一系列的政策與內部控制，資訊安全治理則是組織整體的公司治理的一部份」。由此可推論，就公司治理層面而言，管理階層為符合法規針對公司治理的規範，加強對內部控制的重視，會進而影響公司資訊安全管理績效。

第二節　研究問題

在現今企業中，資訊科技扮演儲存、處理與傳輸企業資訊的重要角色，網際網路則便利企業內部與外部資訊的傳遞，兩者皆已成為支持企業營運與作業的核心元素。然而，兩者的發展雖然提升企業資訊取得的便利性，卻也意味著企業必須更公開地分享其企業資訊，因而提高企業資訊安全的風險。企業資訊是企業最重要的資產之一，保護資訊安全已經是所有企業的共識。再者，保護消費者個人資料的認知與執行力不足，使得消費者個人資料外洩頻傳，政府因而更加重視資訊安全議題，並透過法律法規的頒佈，迫使企業高層正視資訊安全議題。法律法規的強制力，使得企業必須遵守法律規範，否則將導致嚴厲訟訴與高額的罰金。

資訊安全相關法規的推行，使得企業必須將資訊安全視為企業整體公司治理的一部份，以公司治理的角度滿足企業資訊安全需求。

針對公司治理而言，董事會是公司內部治理的核心機制。根據經濟合作暨發展組織(Organisation for Economic Co-operation and Development，OECD)於 2004 提出的公司治理六項原則中，將董事會之責任視為公司治理架構的六大原則之一，並定義“良好的公司治理架構必須確保董事會的策略性指導和有效監督公司管理階層，並且強調董事會對公司和股東善盡應負之責任”。此外，COSO 委員會在《Enterprise Risk Management—Integrated Framework》中對企業風險管理的定義裡提到，決定企業的風險管理實施成效因素之一就是董事會。因此，本研究將以管家理論(Stewardship Theory)為理論基礎，探討公司治理的核心機制-董事會之組成，對於公司資訊安全管理有效性的影響。董事會組成將以總經理雙元性和內部董事比例為變數，透過統計分析方法實證董事會組成與公司資訊安全管理有效性之關聯性。其後再進一步透過股權型態的分類，探討董事會組成對於公司資訊安全管理有效性的影響。

第三節　研究架構

本研究將分六章節，除第一章為導論外，第二章將從資訊安全管理與公司治理兩個領域進行文獻整理與探討；第三章論述本研究所採用的理論基礎－管家理論，並根據其理論發展研究假說；第四章將說明本研究所使用的研究資料、變數以及研究方法；第五章討論與分析實證結果；最後，於第六章進行本研究的結論與建議。

第二章　　文獻探討

本研究將由公司治理的角度切入，探討組織資訊安全管理之有效性是否受到公司治理的相關因素影響。因此，在文獻探討中，我們將分別從管理角度探討資訊安全議題以及針對公司治理領域進行相關研究的整理。

第一節　資訊安全管理相關議題探討

所謂的資訊安全就是可保護資訊不受各種威脅，確保持續營運，將營運損失降到最低，得到最豐厚的投資報酬率和商機(BS7799-2, 1999)。資訊安全最早始於電腦安全的概念。在尚未發展網際網路的世代，電腦安全主要在於防護電腦的實體位置、硬體和軟體，使它們免於外來的威脅(Harris, 2003)。隨著網際網路的發明並普及化，愈來愈多的電腦透過網際網路彼此相互連結、傳遞訊息，使得資訊的傳播變得更加便利。然而，由於在建構網際網路連結的初期對於資訊安全議題的忽視，使得資訊安全問題成為現今網際網路社會的一大問題。對企業而言，資訊被視為最重要的資產之一且已經成為影響企業營運的關鍵因素(von Solms B. and von Solms R., 2006a)，因此為維持企業永續之營運，資訊安全議題對也愈來愈受到企業的重視。

在 2000 年，Von Solms 整理資訊安全議題探討的趨勢，將資訊安全相關議題分成技術(Technical Wave)、管理(Management Wave)、組織(Institutionalization Wave)三種類別，其後隨著治理議題在資訊安全領域愈來愈受到重視，再於 2006 年提出第四種議題趨勢－資訊安全治理(Governance Wave)，以下將以此四種類型進行議題的探討。

技術議題

資訊安全發展的早期，由於資訊科技須要較多專業技術性觀點，因此將資訊安全議題視為技術性議題(Besnard and Arief, 2004)。技術性相關的議題探討的層面非常廣泛，Ransbotham 和 Mitra (2009)曾指出「過去有許多的研究投入於防護電腦安全的技術開發，特別是著重於電腦科學領域，例如:安全網路協定(DiPietro and Mancini, 2003)、入侵偵測技術(Ning et al., 2004)、資料庫安全防護方法(Sarathy and

Muralidhar, 2002)、存取控制技術(Sandhu and Samarati, 1996)」。其他的資訊安全技術還有生物辨識技術(Wildes, 1997)以及仿冒網站偵測技術(Abbasi et al., 2010)。

管理議題

現今的企業採取許多科技技術來增進企業資訊安全防護，使用科技技術來防護外部攻擊是企業保護資訊的首要措施。然而，單方面的仰賴科技技術無法完善的保護企業資訊安全。因此，除了透過科技的防護，更應建構完善的管理機制與組織文化，例如:資訊安全政策規劃、作業流程控管機制、企業資訊安全文化、資訊安全教育訓練計畫...等。

在管理上的議題，資訊安全政策的建立是防護企業資訊安全的首要工作，透過政策的制定能落實相關機制的執行，加強所有公司員工對於資訊安全的重視並減少威脅的產生。根據學者 Hone 和 Eloff (2002, p. 402)所強調「資訊安全政策是最重要資訊安全控管機制」。資訊安全政策的訂立目標在於使企業清楚掌握資訊安全管理的方向並且符合法律條規的規範(ISO/IEC, 2005)。在過去學者指出，企業建構良好的資訊安全政策能夠明確的聲明管理階層對於企業資訊安全的管理意圖與認同，讓所有使用者明瞭違反資訊安全規範可能產生後果及受到的懲處，是有效實施嚇阻的重要前提(Straub, 1990)。在資訊安全政策相關的研究中，Knapp et al.(2009)以質化研究的方式調查資訊安全專業人員，提出資訊安全政策的運作模型(ISP process model)，主張其模型中包含強調資訊安全訓練與認知、政策強制力的必需性、政策管理的週期性、公司治理的角色以及外部和內部的影響五個過去文獻研究所普遍探討的面向。洪國興等人(2003)則整理資訊安全政策相關研究，提出「安全政策理論」(Security Policy Theory)，並根據理論發展資訊安全政策模式(Information Security Policy Model)，探就組內政策相關因素對於資訊安全提升的影響，其研究結果發現政策的功能定位、內容、實施項目以及建立與維護皆會影響其組織資訊安全的提升。

管理議題除了著墨於資訊安全政策方面，學者亦對企業內部流程控制與資訊安全風險管理的議題加以探討。企業維護資訊安全的方法繁多，風險管理是傳統上被廣為使用的方法之一(Siponen, 2005)。所謂的風險意指企業營運過程中所產生的不確定性，此概念被廣泛的應用在資訊系統的運作上，資訊系統風險的產生來自於電腦資產例如:硬體、軟體、資料與服務的遺失與損害，其可能造成損害發生

的事件包含電腦濫用、災難、智慧財產遭盜取等(Straub and Welke, 1998)。文獻上，風險管理的議題包括風險分析、風險識別、風險監控等方面。所謂的風險識別是指判斷、歸類潛在風險的過程，以確定企業目前所面臨的風險，在其研究上，學者提出使用清單法(Checklist)來協助公司進行風險的分類與辨識，以提升其後進行風險評估、風險控制與降低風險的相關決策品質(Lihong et al., 2008)。風險分析指將已識別出的潛在風險根據其風險程度的高低加以分級，以利針對特定重要之風險採取合適及嚴謹的控制。主要的風險分析工具有質化分析與量化分析兩種方法，Bilbao(1992)利用故障樹分析(fault trees)以及模糊邏輯(fuzzy logic)所開發的分析工具 TUAR 即為量化分析方法，而 Kailey 和 Jarratt (1995)所提出的 RaMEX 則是質化分析工具的一種。

組織議題

在組織的議題，使用者與資訊安全文化相關的因素被學者認為是影響企業資訊安全的重要因素之一(Ruighaver et al., 2007, Werlinger et al., 2009; Woodhouse, 2007)。公司的資訊安全文化是一個多元層面的議題，其形成深受組織文化影響(Nosworthy, 2000)。目前，在資訊安全文化不同面向的探討議題有高階主管的支持程度(Knapp et al., 2006)、風險文化(Jahner and Krcmar, 2005)、使用者的資訊安全認知(Siponen, 2000)。其中，學者認為由於公司內部員工是公司所有鏈結中最脆弱的一環(Boss et al. 2009, Warkentin and Willison, 2009)，因此針對使用者電腦誤用與濫用行為、遵循資訊安全政策意圖以及使用者對於資訊安全議題的態度與認知三方面，進行心理因素對其行為的影響的研究。電腦誤用及濫用例如:非法下載及資料傳輸、濫用授權竄改資訊、銷毀及洩露內部資料、越權操作、假冒身份，皆被視為內部人員破壞公司資訊安全的行為，造成公司內部風險的增加。D'Arcy 等學者(2009)以犯罪學的一般威嚇理論為觀點，認為使用者對於懲罰嚴重性與確定性的認知程度會影響其電腦誤用行為，並透過實證研究發現，資訊安全政策、資訊安全認知教育訓練以及電腦的監控等公司資訊安全計畫與機制皆會影響使用者對於懲罰嚴重性與確定性的認知，進而影響其電腦濫用行為。不同於傳統上以一般威嚇理論的觀點，Sipone 和 Vance(2010)以中立化理論(Neutralization Theory)探討使用者違反資訊安全政策的行為，認為以下六個技巧:否認行為所應負的責任(Denial of responsibility)、否認行為所造成的傷害(Denial of injury)、以好的行為補償壞的行為

(The metaphor of the ledger)、強調行為的需求性(the defense of necessity)、責備造就其行為的人(Condemnation of the condemners)以及訴諸更高的情操與權威(Appeal to higher loyalties)是使用者用於中立化其行為動機並減輕罪惡感的方式，因此進而採取違反政策的行為。就遵循資訊安全政策意圖的研究，學者亦發現員工對於政策的態度、道德規範信仰(Normative beliefs)、習慣(Pahnila et al., 2007)、組織認同(Organizational Commitment)皆是影響其遵循資訊安全政策意圖的因素。Thomson and von Solms(1998)以心理學原理為基礎，藉由結合社會心理學領域中用以改變人的行為和態度的原理，使企業更有效執行資訊安全認知的教育計畫。除了探討行為與認知的因果關係，亦有學者提出資訊安全認知的檢索模型，以助於提升企業各個層級的資訊安全認知(Kritzinger and Smith, 2008)。

治理議題

現今的企業正面臨著法規條例對公司治理的規範，例如:美國沙賓法案、HIPAA (Health Insurance Portability and Accountability Act)、GLBA (Gramm-Leach-Bliley Act)，特別強調資訊安全與治理之間的鏈結(Volonino et al., 2004)。新興的法規條例和企業對於資訊科技高度的依賴，使得高階管理層以及董事會注重企業資訊安全，資訊安全議題提升至公司治理層面，企業資訊安全便為公司治理的直接責任(Von Solms, 2006)。“資訊安全是資訊科技治理中重要且完整的一部份” (ITGI 1, 2001)，資訊科技治理是公司治理中重要的一環，亦是董事會的責任之一(ITGI 2, 2003)。因此，企業內的高階管理層以及董事會必須完善整合資訊安全治理於資訊科技治理中，確保資訊安全妥善的受到治理(Damianides, 2005; ISACF ,2001)。資訊安全領域中，目前與治理相關的研究並不多，主要包含資訊安全治理與新興法規對於資訊安全影響的探討。學者針對資訊安全治理提出架構，以利於資訊安全治理完整的整合於公司治理之中(Posthumus and Von Solms, 2004)。Luthy and Forcht (2006)，從新律法規層面，探討新興法律法規(Sarbanes-Oxley Act of 2002、Basel Ⅱ Accord of 2004)對於企業資訊管理的影響。從過去資訊安全相關的文獻研究發現，治理層面的議題尚未針對公司治理的核心運作機制-董事會，進行相關的探討。然而，董事會負責制定、實施與監督企業策略，確保公司遵循法規並永續營運，是領導企業營運方向的最高指導單位，必須對企業營運績效與未來發展負完全的責任。法律內容則是要求高階主管對企業的內部控制擔保，強調董事會與高階經理人的治理

責任。資訊安全是公司治理的重要部份，而良好的公司治理是董事會責任之一。企業要達成資訊安全的目標，必須要透過完善的公司治理 (CGTF, 2004)，進而言之，企業資訊安全亦是董事會的責任之一，必須透過董事會的領導與運作，追求企業資訊安全的目標。本研究希望透過探討董事會組成，研究企業董事會對於資訊安全管理的影響。

第二節　公司治理議題

所謂的公司治理(Corporate Governance)至今仍尚未有一套公認的定義。近年來，學者認為公司治理議題的探討與理論的發展，兩極化於股東觀點(shareholder perspective)和利害關係人觀點(stakeholder perspective)兩個論點上(Letza et al., 2004)。傳統上，學者採股東觀點來探討公司治理議題，認為股東是企業的所有者，有權控制並主導公司，因此以追求股東利益的最大化為公司治理的目標。因此，將公司治理定義為是確保公司的資金提供者能夠回收合理的報酬，所設計的一套機制(Shleifer and Vishny, 1997)。然而，由於公司除了追求利潤更必須負擔社會責任，再者，公司的發展不僅需要股東投入資金，更包含各種利益相關者的參與。因此，僅以股東觀點定義公司治理略顯不足。近年來公司治理以利害關係人觀點出發，認為公司治理必須包含所有利害關係人的權益與義務，根據聯合國經濟合作與發展組織(OECD)於 1999 年為公司治理的定義:「公司治理是一套指導和控管公司的機制，其架構必須清楚地說明執行單位，例如:管理階層、董事(監)會、股東與其他利害關係人之間的權責分工，並且闡明公司事務決策的章程與程序。」我國學者李存修、葉銀華、柯承恩(2002)亦認為「公司治理機制是透過制度的設計與執行，目的在於提升策略管理效能與監督管理者行為，藉以確保外在投資者(小股東與債權人)應得的報酬，並兼顧其他利害關係人的利益。更具體而言，公司治理在於防範管理者傷害公司價值，並強化公司競爭力與管理效能，以保障資金提供與其他利害關係人的權益。」綜合國際組織與學者們的看法，公司治理是以所有利害關係人的利益為前提，以落實經營者責任和健全的公司營運為目標，所產生的一套管理與監控機制。

在公司治理機制的相關研究中，學者較多著墨於董事會與股權結構相關的研

究。根據世界銀行 1999 年所提出的公司治理架構，其公司治理機制可分為內部機制與外部機制。在公司治理內部機制中，董事會與股權結構是影響機制運作的重要元素(葉銀華、李存修及柯承恩, 2002)。董事會是治理機制的核心，必須負責公司重大之決策，確保公司以追求股東利益最大化為目標(Kosnik, 1987)並且監督公司管理階層的經營績效;股權結構是影響董事會組成的直接因素，是公司利益與權力配置的重要指標(葉銀華、李存修及柯承恩, 2002)。

公司治理的學術研究議題是由 Berle 和 Means 於 1932 年出版的《The Modern Corporation and Private Property》一書首開先例。兩位學者針對公司所有權與控制權的分離而產生代理問題提出研究觀點，認為在所有權與控制權分離的情況下，當實質掌有控制權的管理階層持股比例不高時，管理階層毋須承擔經營失敗的損失，若公司又因股權過於分散而使股東無法約束及制衡管理階層，則容易使管理階層根據個人利益運用公司資源，不以股東利潤最大化為目標，採取不利於股東的營運策略。經濟學家 Coase(1937)發表“The Nature of the Firm”一文中，首度將公司視為一連串契約的組合體。每位員工之間或員工與公司之間皆存在契約關係。透過契約的詮釋，每個成員各有其應享之權利與應盡之義務，各成員亦有不同的利益目標。因此，成員之間為滿足各自不同的利益目標，管理階層與公司所有人之間在利益目標上的產生落差，成為探討代理問題的起源。代理問題是公司治理議題發展的起源，在公司治理的研究領域中，有大部份的文獻是以解決代理問題為目標，提出因應的公司治理機制與理論發展。

在公司治理相關的理論中，受到學者廣為探討的理論包括代理理論(Agency Theory)、資源依賴理論(Resource Dependence Perspectives)以及管家理論(Stewardship Theory)，以下就其三種理論分別進行探討。代理理論由 Jensen 和 Meckling(1976)所提出，是日後探討公司治理相關議題的研究中普遍所採用的理論基礎。兩位學者於文中定義所謂的代理關係是指「一位或多位以上的委託人(Principal)授權給代理人(Agent)代為進行決策，代理方代表委託方執行任務時，彼此之間所存在的契約關係。」代理理論認為在公司所有權與控制權分離且股權極為分散的情況，代理關係內的契約成員以自利為前提，在利益立場上產生衝突，使握有資訊上優勢的管理階層追求自身利益最大化，因而在不用承擔剩餘風險的條件下，作出不利於股東的決策。因此，在契約約束力不足以保障公司利害關係

人的利益下，採用此理論的學者亦著墨於透過公司治理機制的設計，採取董事會監督或限制經理人持股比例下限、外部稽核等措施，以減少代理問題，降低代理成本(Agency Cost)。Eisenhardt(1989)提出代理理論主要是在處理代理關係中的兩大問題，其一是委託方與代理方利益衝突所產生的代理問題，其二則是委託方與代理方在風險方面態度上的衝突而產生的風險分散問題。

表 2-1 代理理論歸納表

理論核心	以有效率的契約規範委託人與代理人之間的代理關係
分析單位	委託人與代理人之間的契約
行為假設	自利(Self-interest) 有限理性(bounded rationality) 風險趨避(risk aversion)
組織假設	成員之間的目標衝突 效率(efficiency)是效能(effectiveness)的指標 委託人與代理人之間存有資訊不對稱
資訊假設	資訊是可購買的商品
契約問題	道德危險(moral hazard) 逆選擇(adverse selection) 風險分散(Risk Sharing)
問題範圍	探討委託人與代理人之間在目標和風險偏好上存在的差異

資料來源: Eisenhardt, Kathleen M.(1989)

以資源依賴理論觀點，公司為求生存必須取得外部環境的資源，因此公司與外部環境的連結是公司創造優勢與價值的關鍵。相較於代理理論主張董事會的監督功能，以資源依賴理論觀點探討公司治理議題的學者則認為，董事會有提供資源的責任，企業的生存依賴於董事會對於外部資源的連結與運用，董事會成員是提供公司決策所需資源的關鍵因素(Pfeffer, 1972; Pfeffer and Salancik, 1978)。就提供資源的觀點而言，Becker(1964)主張「人力資本」(Human Capital)是公司生產的重要資產，亦是影響企業績效的關鍵因素。將人力資本的觀點延伸至董事會而言，

董事會負責公司重大之決策，其董事會成員的資源提供能力則是影響公司決策的重要因素。因此，董事會成員的專業知識、能力、經驗與名聲皆可視為影響資源提供能力的因素，並進而影響公司決策品質與營運績效表現。學者根據實證研究結果發現董事會成員的知識與經驗會影響其決策方向，Zajac 和 Westphal(1996)主張董事在其他董事會執事的經驗會影響其對於後續任職董事會的選擇，並透過實證研究證實董事過去曾參與過提高董事會控制權的決策(例如:增加外部董事比例、主張董事長與總經理職位不由同一人兼任)，則其對於後續任職董事會的選擇會偏好選擇董事會控制權較高的董事會。Golden 和 Zajac(2001)其實證結果發現董事會中具有商業背景的董事比例與企業策略變革有正向關係。

管家理論則有別於代理理論假設管理階層以自利為前提的觀點，認為公司管理階層是以委託人利益為前提，公司應將授予管理階層更多的權力與資訊，以利為公司制定最佳策略(Davis et al., 1997)。本研究以管家理論為基礎，因此將於下一章節進行更詳細的探討。

在董事會相關研究中，學者探討董事會在公司治理中不同層面的影響。在公司經營績效層面的研究，Zahra 和 Pearce Ⅱ(1989)整理過去探討董事會與公司經營績效的文獻，歸納出四種觀點:法律觀點(The Legalistic Perspective)、資源依賴觀點(Resource Dependence Perspective)、階級領導權觀點(Class Hegemony Perspective)、代理理論觀點(Agency Theory Perspective)。四個觀點中，以資源依賴觀點最具實證研究的支持，而代理理論觀點受經濟與金融領域的重視。透過四種不同的觀點探析董事會在角色、功能、理論基礎以及影響公司經營績效的屬性上的差異，並提出一個整合性模型。模型架構中，將董事會屬性分成組成(Composition)、特性(Characteristics)、結構(Structure)、流程(Process)四類屬性。不同屬性構面對於公司經營績效的影響，過去的學者們各自表述。學者利用統合分析(Meta analysis)檢視過去有關董事會組成結構的實證研究，發現董事會規模、董事雙元性和內部董事比例在過去的實證研究中，對於公司經營績效並無顯著的影響(Dalton et al., 1998, 1999 ; Heracleous, 2001)。董事會必須具備領導以及制訂公司發展策略的功能，除了監督功能，更應具備專業性提供公司有價值的策略方向與建議(Heracleous, 2001)，是決定公司營運策略方向的核心單位。Zahra 和 Pearce Ⅱ(1989)在研究中提到董事會在公司扮演的角色包括服務角色、策略角色以及控制角色。在決策層面的研究，

Kosnik(1987)發現公司的外部董事比率較高時，其董事會在執行支付綠色郵件的決策時，拒絕支付綠色郵件的可能較高。此外，學者們透過實證研究，證實董事會特性多方面的影響公司決策，其影響層面包括總經理的選任(Zajac and Westphal, 1996)、設計與開發投資決策(Kor, 2006)。

公司股權結構是學者在公司治理機制探討的另一個要點。Shleifer 和 Vishny(1986)認為大股東具有較高的意願監督管理者，由於股權的集中，使他們具有較大的監督能力，可以更有效地限制管理階層偏離股東權益的行為，因而提升公司經營績效與股東價值。研究結果顯示，大股東的持股比例增加時，公司股票價值上升。

La Porta et al.(1999)於研究中發現，大股東利用金字塔結構、交叉持股等方式，提高決策控制權(投票權)，透過股權優勢控制董事會，影響董事會執行有利於大股東的決策，侵佔公司資源與小股東的權益。針對股權所有人的特性，學者亦各自表述提出不同的假說。Pound(1988)提出「效率監督假說」，認為法人股東相較於一般股東而言，擁有豐富的專業知識和能力，能以較低的監督成本監督管理經營團隊。Agrawal 和 Knoeber(1996)檢驗七種針對管理者與股東之間代理問題的公司治理機制，研究結果中發現內部人持股率與公司績效呈正相關。

由上述公司治理領域的文獻整理，可發現學者針對公司治理對於公司經營績效與策略領導的影響進行探討，並透過不同的理論基礎發展合適的公司治理機制。由第一節所述，資訊安全管理已提升至公司治理層面，資訊安全治理必須完整的整合於公司治理並透過公司上層的領導與完善的公司治理運作。目前在資訊安全領域中，與治理相關的研究並不多。因此，整合兩節的文獻論述，本研究將以公司治理的角度探討公司治理機制對於資訊安全管理有效性的影響。

第三章　　研究方法

本章根據研究問題，以管家理論(Stewardship Theory)為理論基礎，說明董事會在資訊安全策略領導上所扮演的角色。其後，根據理論基礎發展本研究的研究假說、研究方法與分析。

第一節　管家理論

不同於代理理論以經濟學的角度，並且假設人在理性情況下是採取自利主義和機會主義，管家理論從心理學與社會學的角度出發，認為公司管理階層是注重自我尊嚴與認同感，在工作上追求實質目標的達成以及成就感的滿足(Donaldson and Davis, 1989, 1991)。根據管家理論的觀點，管理階層追求的目標並非物質性的滿足，而更應該是達到具有挑戰性目標所獲得社會的認可、個人聲望的樹立、自我價值的認同等心理上的滿足。因此，管家理論認為管理階層是集產主義者(Collectivism)，以公司整體利益為優先，將公司的成功視為個人成功的指標，透過成功的公司經營來獲得自我價值的認同感與工作上的成就感(Davis et al., 1997)。在利益立場上，股東、管理階層以及所有利害關係人皆以追求公司價值最大化為目標。就公司治理層面而言，管家理論不同於代理理論強調以「監督」機制來規範所有人與管理階層之間的關係並減少代理問題，提升公司績效，而是認為公司在所有利害關係人利益立場一致的前提下，公司治理強調於建構一個有效率的組織架構，使其有助於管理階層制定並實施提升公司經營績效的計畫(Donaldson, 1985)。公司應給予管理階層充分的信任，授予更多的權力與資訊，以利管理階層面對瞬息萬變的競爭市場時，能夠為公司制定最佳策略，進而提升公司經營績效(Davis et al., 1997)。

以管家理論為基礎的研究中，Donaldson 和 Davis(1991)分別以代理理論與管家理論為基礎，發展總經理雙元性對於股東報酬率影響的假說，實證研究結果發現，以管家理論為基礎所提出總經理與董事長職位的合併能使股東報酬率提升。根據上述實證結果，我們亦可得知代理理論確實有其爭議之處，然而兩理論之間的關係是否為完全對立的立場，則學者試圖透過兩種理論在各方面的比較，來探討兩者之間的關係與差異(Davis et al., 1997)。Davis 等學者(1997)以心理因素

(Psychological Mechanisms)與組織情境(Situational Mechanisms)兩個層面進行理論特性的分析。其分析內容指出，代理理論與管家理論之間最根本的差異在於對人類行為的假設(Model of Man Behavior)，代理理論以經濟理性(economic rationality)為出發點，假設人類的行為皆以追求自我利益極大化為目標。管家理論則是以自我實現(Self-actualizing)作為人類行為的假設前提，認為追求集體利益的極大化不僅滿足所有利害關係人更是實現自我價值的途徑。在心理因素層面，代理理論著重於外在物質的激勵，例如:退休規畫、激勵獎金等能夠被量化的激勵方式，而管家理論則強調內在心靈層面的提升，例如: 成長與學習的機會、自我價值實現、達成目標的成就感等不易被量化的激勵方式，並且認為管理階層有較高的組織與自我認同感(Identification)。在組織情境層面，由於對於人性假設根本的差異，使其發展不同的管理哲學與公司治理機制。代理理論以控制取向(Control oriented)為公司管理的模式，管家理論則認為公司的管理哲學應是公司層級之間彼此建立信任與開放的溝通管道，充份將權力授權於實際作業的層級，使其能參與決策(Involvement oriented)。

表 3-1 代理理論與管家理論比較表

	Agency Theory	**Stewardship Theory**
Model of Man Behavior	Economic man Self-serving	Self-actualizing man Collective serving
Psychological Mechanisms		
Motivation	Lowerorder/economic needs (physiological, ecurity ,economic) Extrinsic	Higher order needs (growth, achievement, self-actualization) Intrinsic
Social Comparison	Other managers	Principal
Identification	Low value commitment	High value commitment
Power	Institutional(legitimate, coercive, reward)	Personal(expert, referent)
Situational Mechanisms		
Management Philosophy	Control oriented	Involvement oriented
Risk orientation	Control mechanisms	Trust
Time frame	Short term	Long term
Objective	Individualism	Performance Enhancement
Cultural Differences	High power distance	Low power distance

資料來源: Davis et al., 1997

第二節　研究假說

根據管家理論的觀點，管理階層在有效率的組織架構下並獲得充份授權，才能有效發揮其策略領導能力。在公司治理的機制中，董事會不僅扮演監督的角色，更是決定公司營運策略方向的核心單位，必須提供專業性建議並領導公司的策略發展。因此，本研究以管家理論為基礎，整理過去的文獻中探討董事會組成對於公司決策方向影響的變數，進而探究影響董事會決策方向的因子與資訊安全管理有效性的關係。

管家理論所假設的人類行為以自為實現為前提，管理階層是集產主義者(Collectivism)，以公司整體利益為優先，將公司的成功視為個人成功的指標，透過成功的公司經營來獲得自我價值的認同感與工作上的成就感(Davis et al., 1997)。由於資訊安全問題對於公司的影響是全面性的水平至公司各單位部門，垂直的上至管理階層，下至底層負責作業的前線人員，爆發資訊安全問題不僅降低公司財務績效表現，更嚴重毀損公司形象。因此，在管理階層將成功的公司經營與永續的企業持續營運視為個人成功指標的前提下，資訊安全問題的影響讓管理階層在面對資訊安全管理議題時，會將資訊安全議題視為影響公司永續營運以及整體發展的關鍵因素，並認為資訊安全問題應是公司管理階層的責任，是公司整體經營管理上應注重的，因而更加重視資訊安全管理整體性的發展。此外，資訊安全的投資就如同買保險般，透過風險管理的概念，辨視、分析風險，再進一步的落實控管步驟以降低風險，將風險程度降至可接受範圍。因此，若以買保險的概念來比擬資訊安全投資，企業無法得知危機何時會發生，只能盡其所能的控管風險，並完善的建置危機發生後的災後應變措施。由此可知，企業在資訊安全方面的投資並不像一般投資決策能夠清楚的量化其效益並計算其投資報酬率，也無法立即直接於經營績效表現上見其成效，因此，管理階層若以報酬的角度來衡量資訊安全投資的效益，則容易因無法明確看其成效而忽視資訊安全問題，甚至減少資金投入，因而提高企業發生資訊安全問題的風險。在管家理論的理論基礎下，管理階層追求心理層面的滿足，例如:社會的認可、成長與學習的機會、個人聲望的樹立、自我價值的認同…等較不易量化層面，而非物質上的追求。因此，管理階層在資訊安全投資決策的考量上，較不會以金錢、報酬這種較為物質層面的角度來衡量

投資決策，而是以公司未來整體性的發展來評估，追求公司能樹立良好形象並永續營運，以獲得社會的認可。因此，在管家理論基礎下，管理層面有較高的意願投入資訊安全防護的建置並更為注重資訊安全議題的發展，更加注重企業落實資訊安全相關規範。

總經理雙元性

所謂的總經理雙元性，意指公司董事長與總經理為同一人擔任(Finkelstein and D'Aveni, 1994)。過去有許多學者在研究董事會組成架構時，將董事長與總經理兼任議題視為探討因素之一(Rechner and Dalton, 1991;Donaldson and Davis, 1991; Boyd, 1994, 1995; Baliga et al., 1996)。根據管家理論認為管理階層在本質上是可信任並且以公司整體利益為已任，是盡忠職守管理公司資產的管家。總經理是公司經營管理的主要負責人，其擁有公司最高權限的執行力。董事長是董事會的領導人，更是領導公司整體策略發展的核心人物，其行為與態度亦能影響董事會的決策方向與文化(Huse, 2005)。因此，結合董事長與總經理的職務，能使熟悉公司內部經營狀況的總經理獲得足夠的授權，強化其領導能力。在控制權的提升下，能夠有效發揮執行力，加速各方立場的統一與政策的制定，並妥善執行資源配置(Heracleous, 2001)。

就公司資訊安全管理而言，資訊安全政策的實施必須仰賴公司高層的支持與積極推動。為完善資訊安全風險的控管，公司必須制定許多內部控制的機制，控管其作業流程能符合相關法規與準則的規定，其機制對於公司底層的作業人員而言，會降低作業時的效率與便利性，因而造成政策實施的反彈與失效。因此，透過結合公司高層的領導，控制權與執行權的結合，能提升公司決策效率，加速資訊安全政策的制定與執行，並領導人權力的強化，能使政策更加落實於公司的每個角落。本研究以管家理論為基礎，認為管理階層以公司利益為前提，結合個人目標與公司願景，以追求公司經營之卓越為個人成就的指標，為達其目標以滿足所有利害關係人的期待，必須獲得公司充份授權，同時具備執行力與決策權，才能有效發揮其策略領導能力，故發展假說一:

假說一:董事長雙元性與資訊安全管理有效性呈正相關

內部董事比例

Rechner and Dalton(1989)定義內部董事是指同時參與內部實際業務以及擔任行政職務的董事會成員，是直接受雇於公司並同時兼任公司董事會的成員。根據管家理論認為經理人員具備完善的能力且值得信賴的，因此應該由管理階層掌握公司經營的控制權，而非外部人員(Heracleous, 2001)。就董事會的決策品質而言，Baysinger 和 Hoskisson(1990)認為並非所有董事會成員都擁有相同的公司資訊量，內部董事同時兼任公司內部營運作業，應握有較豐富的公司即時相關資訊，不僅較熟悉企業內部經營狀況，更能提供切合公司實際需求的建議與策略方向。在公司治理機制中，管理階層與董事會之間存在著社會關係連結(social tie)，被視為缺乏獨立性的特性之一，亦會因此而降低董事會有效率的運作。然而，Westphal(1999)認為此種說法存有偏差，因此透過實證研究證實，董事會與管理階層之間存在有社會關係連結能夠幫助協調兩者的合作關係，減少不必要的監督成本，進而提升合作的決策品質。Patton 和 Baker (1987)指出，外部董事通常身兼數個公司的董事職位，因而分散專注，無法有效的針對公司實際的需求提出見解。反之，內部經理人以所屬公司的永續營運以及價值最大化為目標，專注於公司策略規畫與執行，更能善盡董事策略領導的功能。

就公司資訊安全管理而言，資訊安全風險的控管是公司內部控制的一環。因此，由熟悉企業內部運作流程的經理人參與內部控制機制的設計與資訊安全策略與規畫的發展，能夠更有效的制定出切合公司需求的機制與策略。再者，除了在策略規畫階段(Plan)的參與，內部經理人也同時參與資訊安全管理的執行(Do)與監督(Check)階段，因此在檢視策略執行的有效性時，不僅由於瞭解公司即時的相關資訊而能快速反應並改善策略之缺失，更能針對實際運作情形，提出策略優劣的看法，提升公司策略的切合度。本研究以管家理論為基礎，認為管理階層以追求公司經營之卓越為個人成就的指標，因此有更充足的意願投入公司營運策略的制定。再透過管理階層對於公司內部作業流程的熟悉與較多內部資訊的掌握，使其在董事會進行決策過程中，能提出更有利且切合公司的策略，提升董事會的決策品質。故發展假說二:

假說二:內部董事比例與資訊安全管理有效性呈正相關.

第四章　　研究設計

第一節　研究資料

本研究將以管家理論(Stewardship Theory)為理論基礎，探討公司治理的核心機制-董事會之組成，對於公司資訊安全管理有效性的影響。其中，公司資訊安全管理有效性的衡量方法，將根據 Hsu 和 Wan 於 2010 年的研究，以該年度公司是否發生資訊安全事件做為衡量的標準;而董事會組成的相關研究資料將取自台灣經濟新報資料庫(Taitwn Economic Journal, TEJ)。

資訊安全事件的資料收集方式，以台灣上市櫃公司為對象，手動搜尋資安人科技網與聯合新聞知識庫的網頁資料庫，資料年份自 1987 年到 2011 年 12 月底，共計發生 111 件資訊安全事件。由於台灣沒有資訊安全事件資料庫，因此參考 Compbell, Gordon, Loeb and Zhou(2003)以及陳美君(2004)的研究，利用關鍵字搜尋網頁資料庫，其中關鍵字包括: 駭客、阻絕服務攻擊、系統故障、系統當機、密碼外洩、資料外洩、置換網頁、資料竊取、行員盜領、人員操作疏失、程式設計錯誤、軟體缺陷網頁編寫疏失、硬體損毀(遭竊、遭破壞)。

董事會組成的相關研究資料取自台灣經濟新報資料庫底下的「TEJ 公司治理」。其中，總經理雙元性取自「待股東公平性、資訊透明、人事穩定度」資料頁面中的“董事長兼任總經理”欄位;內部董事比例則取自「控制持股與董事結構」頁面中的“董事兼任經理人比”欄位。研究對象包含台灣有價證券集中交易市場及證券商營業處所買賣之上市(櫃)公司。

在總樣本觀察筆數方面，雖然資訊安全事件的樣本區間是自 1987 年至 2011 年 12 月底，共計 25 年，但是在董事會組成方面的資料，其樣本區間僅包含 1996 年至 2011 年，共計 16 年。由於董事會組成的資料區間限制，使最初樣本數原為 846 筆，在剔除 1996 年以前的資料，最終總樣本觀察筆數為 604 筆。

就表 4-1 針對總樣本的分佈情形進行說明。從表中可得知，總樣本數為 604 筆，其中以 1996 年所佔的樣本數最少，為總樣本的 3.81%，其次是 1997 年與 1998 年，分別佔總樣本的 4.80%和 4.97%。就整體樣本分佈而言，1996 年至 2000 年的資料偏少，每年的樣本比率平均約佔總樣本數的 4.97%，自 2001 年起，樣本數增

加，每年的樣本比率平均約佔總樣本數的 6.83%。就資訊安全事件的分佈而言，2000 年以前資訊安全事件發生的次數明顯偏低，1996 年至 2000 年有資訊安全事件發生的樣本僅佔整年度樣本的 1.80%，自 2001 年開始，資訊安全事件發生愈來愈頻繁，在資訊安全事件逐年增加的情況下至 2004 年達到資訊安全事件發生的高峰，其資訊安全事件次數佔整年度樣本的 14.41%。爾後，資訊安全事件發生的次數皆維持於平均之上，每年平均約有 11 起的資訊安全事件發生。

表 4-1 各年度資訊安全事件發生次數分佈

年度	樣本比率	無資安事件		有資安事件	
	%	%	N	%	N
1996	3.81%	4.67%	23	0.0%	0
1997	4.80%	5.88%	29	0.0%	0
1998	4.97%	5.88%	29	0.90%	1
1999	5.46%	6.69%	33	0.0%	0
2000	5.79%	6.90%	34	0.90%	1
2001	6.62%	6.69%	33	6.31%	7
2002	7.12%	7.30%	36	6.31%	7
2003	7.28%	7.10%	35	8.11%	9
2004	7.12%	5.48%	27	14.41%	16
2005	7.12%	7.30%	36	6.31%	7
2006	7.12%	6.69%	33	9.01%	10
2007	6.95%	6.29%	31	9.91%	11
2008	6.46%	5.27%	26	11.71%	13
2009	6.46%	5.88%	29	9.01%	10
2010	6.46%	7.10%	35	3.60%	4
2011	6.46%	4.87%	24	13.51%	15
總計	100.00	81.62%	493	18.38%	111

本研究是針對台灣經濟新報資料庫內的上市(櫃)公司進行樣本的收集，然而由於在手動收集資訊安全事件發生資料後，僅採用歷年來有發生過資訊安全事件的公司資料，並未包含所有的上市(櫃)公司。因此，本研究以台灣經濟新報資料庫所訂定的產業別進行樣本的分類，其結果為表 4-2。從表中可以得知，樣本數最多為

金融保險業，佔總樣本的 39.24%，其次是電子工業，佔總樣本的 33.44%，剩餘的產業別僅佔總樣本的比例皆不超過 5%。

表 4-2 樣本之產業分佈情況

產業類別	樣本數	%
金融保險業	237	39.24%
電子工業	202	33.44%
食品工業	28	4.64%
航運	27	4.47%
其他	26	4.30%
證券	20	3.31%
紡織工業	16	2.65%
電器電纜	16	2.65%
造紙工業	16	2.65%
貿易百貨	16	2.65%

根據資訊安全事件類型的分佈整理，從表 4-3 可得知資料外洩佔事件類型的首位，佔 30.46%，其次是駭客與資料竊取，分別佔 23.84%與 10.60%。資料外洩與竊取佔居前三名的兩名，說明資料保護的當務之急。根據趨勢科技 2011 年度威脅報告指出「2011 年為全球資料外洩之年」，多家知名大企業發生嚴重客戶資料外洩事件而導致財務與商譽巨大的損失，如日本 SONY 於 2011 年的四月與五月接連發生客戶資料外洩事件，其總共的資料外洩筆數超過一億筆帳戶資料並花費至少一億七千一百萬來修補事件帶來的損害，亦造成 SONY 股價重挫，跌至兩年來新低。企業發生資料外洩不僅為來財務上的損失，更負面的影響企業品牌形象與永續營運。而近年來由於個資外洩情況嚴重，使政府大動作進行修法，擴大法規保護之客體，加重企業應負之刑責，如於民事責任上，同一事件之民事損害求償最高總額提升至新臺幣 2 億元，迫使企業正視個人資料保護議題。排名第二的駭客攻擊佔 23.84%，駭客攻擊的手法隨著科技技術的進步日新月異，根據 Microsoft 於 2011 年發佈的資訊安全報告(Microsoft Security Intelligence Report)顯示，將近一半的惡意攻擊來自於社交工程(Social Engineering)手法，而目前常見的駭客手法還包括有: 零時差攻擊(Zero Day Attack)、偷渡式下載(Drive-By Downloads)、分散式

阻斷服務攻擊(Distributed Denial of Service)、SQL 插入式攻擊(SQL Injection)等。

表 4-3 各類型事件資料之分佈

事件類型	%
資料外洩	30.46
駭客	23.84
資料竊取	10.60
系統故障	9.93
行員盜領	9.27
系統當機	7.95
置換網頁	1.99
硬體毀損(遭竊、遭破壞)	1.99
密碼外洩	1.32
程式設計錯誤	1.32
軟體缺陷網頁編寫疏失	0.66
人員操作疏失	0.66
阻絕服務	0.00

變數定義

應變數

本研究希望證實公司董事會組成對於資訊安全管理之有效性具有影響力。在資訊安全管理有效性的衡量上，由於資訊安全管理是否完善將會影響到公司資訊安全事件的發生，因此設一應變數(Breach_X)為是否發生資訊安全事件，若該公司於當年度有發生資訊安全事件，則 Breach_X 為 1。反之，則 Breach_X 為 0。此外，由於虛擬變數 Breach_X 未處理到該年度資訊安全事件生多次之情形，因此設另一應變數(Breach_Y)為是否發生多次資訊安全事件之情形，若該公司於當年度沒有發生資訊安全事件，則 Breach_Y 為 0;若該公司於當年度發生一次資訊安全事件，則 Breach_Y 為 1; 若發生二次以上資訊安全事件，則 Breach_Y 為 2。最後，為了探討董事會組成對於資訊安全事件發生次數之影響，再設一應變數(Breach_Z)為該年度資訊安全事件發生的次數。所有應變數的資料來源皆透過關鍵字搜尋資安人科技網與聯合新聞網資料庫。

自變數

1. 總經理雙元性

根據第三章的研究假說發展，管家理論以自我實現作為人類行為的假設

前提，認為管理階層透過成功的公司經營並追求集體利益的極大化以滿足所有利害關係人，來獲得自我價值的認同感與工作上的成就感(Davis et al., 1997)。因此，管理階層必須在有效率的組織架構下並獲得充份授權，才能有效發揮其策略領導能力。在結合總經理與董事長兩者的職務情況下，能使熟悉公司內部經營狀況的總經理獲得足夠的授權，在控制權與執行力的提升下，能夠有效落實公司資訊安全政策。因此本研究由台灣經濟資料庫之 TEJ 公司治理資料庫中的「待股東公平性、資訊透明、人事穩定度」資料頁面的"董事長兼任總經理"欄位取得總經理雙元性(DUALITY)變數，用其驗證假說一: 總經理雙元性與資訊安全管理有效性呈正相關。

2. 內部董事比例

管家理論認為公司經理人為善良管理人，具備完善且值得信賴的能力並以公司集體利益為目標，由於內部董事實際參與公司日常營運並且將公司的成功經營視為個人成就的理念，因而有較高的意願投入公司營運相關的策略制定。再者，亦有學者認為董事對於公司內部資訊量的掌握具有差異，內部董事由於同時參與公司內部營運作業，因此熟悉內部運作流程並掌握最即時的內部資訊(Baysinger&Hoskisson, 1990)。就資安角度而言，內部董事在熟悉內部作業流程與掌握較多內部資訊情況下，在積極參與決策的過程中，能夠有效的提出更切合公司整體策略的資訊安全管理策略，增進董事會在資訊安全相關的決策品質。因此本研究由台灣經濟資料庫的 TEJ 公司治理資料庫中的「控制持股與董事結構」頁面中的"董事兼任經理人比"欄位取得內部董事比例(INSIDER)變數，用其驗證假說二: 內部董事比例與資訊安全管理有效性呈正相關。

控制變數

除了前述透過管家理論提出關於董事會組成的相關變數外，尚有某些企業特性與董事會特徵可能影響公司資訊安全管理的有效性。因此，除採用總經理雙元性與內部董事比例作為主要的研究變數外，亦考量其他會對公司資訊安全管理有效性造成影響的因素。

1. 公司規模(SIZE)

在企業特性部份，公司規模是多數學者研究探討的變數(Ashbaugh-Skaife et al. , 2007; Evans, 1987)。在資訊安全方面，對大公司而言，由於公司的高知名度及其龐大的資產，使其較容易成為駭客攻擊的目標，再加上大公司營運活動複雜且對於資訊科技的高度依賴，資訊安全問題對於公司整體的營運影響層面相對較於嚴重，因此在擁有較充足的人力資源與資金的優勢條件下，願意投入資金積極建置資訊安全防護。由上述可推知公司的規模是影響公司投入資訊安全相關資源多寡的重要因素。關於公司規模研究中，常以總資產取對數作為衡量規模大小的標準。在 Gordon et al.(2009)研究企業風險的研究中，亦以總資產取對數作為衡量規模大小的標準。因此，本研究將以 1996 年至 2011 年年底的資產總額取對數後的數值，視之為公司規模變數(SIZE)，並不預期方向。

2. 公司年數(AGE)

企業特性的另一個變數即為公司年數。Douma et al. (2006)在研究中指出公司成立時間的長短應被視為影響公司表現的因素之一。公司隨著成立時間的增加，累積豐富的經驗，在富豐的經驗與學習曲線所帶來的有利優勢下，較能做出合適的危機反應與營運決策。然而，年齡過長的公司卻也容易在競爭激烈的環境中，由於守成而錯失快速反應的時機。本研究將以各筆觀察資料的收集年度與公司成立年度的減值，視為公司年數(AGE)，並不預期方向。

3. 獨立董事比例(INDEP)

由於本研究僅以管家理論為出發點，探討董事會組成的相關變數，在董事會中尚有其他因素亦會影響管理有效性，因此在此處提出討論。在過去的研究中，獨立董事比例雖然是被視為董事會監督品質的指標，Beasley (1996)於研究中指出獨立董事比例較高的公司，其財務報表作假的比率較低，然而亦有學者(Jensen, 1993)認為由於獨立董事對於公司實際專案運行的參與較少，因此擁有較少的內部相關資訊。獨立董事由於保有其獨立性的性質，因此不直接參與公司實際營運，在不瞭解公司實際運作的內部流程情況下，獨立董事較無法針對公司內部流程提出切合公司需要的解決方法。再者，由於獨立董事通常是站在外部監督者的立場，扮演嚴

格的監督者,因此執行長較不願透露內部關鍵資訊給獨立董事(Adams and Ferreira, 2007)。根據上述之論述，由於獨立董事對於公司內部資訊安全管理的不熟悉以及經驗的缺乏，使其無法達到良好的監督效果與決策品質。因此，本研究將預期獨立董事比例對於資訊安全管理有效性呈負相關，其變數資料來源取自 TEJ 公司治理 DB 的獨立董事比例欄位。

表 4-4 變數彙整表

變數名稱	變數說明	資料來源
應變數		
Breach_X	是否發生資安事件	關鍵字搜尋資安人科技網與聯合新聞網資料庫
Breach_Y	是否發生多次資安事件	
Breach_Z	發生資安事件的次數	
自變數		
DUALITY	是否為總經理雙元性	TEJ 公司治理 DB
INSIDER	內部董事比例	TEJ 公司治理 DB
控制變數		
SIZE	公司規模	TEJ Finance DB
AGE	公司成立年數	TEJ Finance DB
INDEP	獨立董事佔董事總人數比例	TEJ 公司治理 DB

敘述統計

首先，內部董事比例(INSIDER_P)平均數為 21.38%、標準差為 17.51，而第一四分位、第二四分位與第三四分位分別為 7.69%、14.29%、33.33%，平均數高於中位數，表示資料分佈偏右。在控制變數方面，取對數後的資產總額(SIZE)其平均數與四分位數相近，標準差亦小於 1，表示其值集中分佈於平均數附近。獨立董事佔董事會席次比的平均數、第一四分位、第二四分位與第三四分位分別為 7.49%、0.00%、0.00%、13.776%，表示樣本中獨立董事佔董事會席次比率集中於 0.00%，意即儘管法令規定必

須設置獨立董事，但實際情形仍屬於比例偏低的情況，多數的公司未設立獨立董事或僅設立人數極少的獨立董事。其次，表示當年度資訊安全事件發生次數的變數(Breach_Z)，第一四分位、第二四分位與第三四分位皆為 0，其平均數 0.22、標準差為 0.526，表示大多數的資訊安全事件發生次數仍集中於 0 的狀況。在虛擬變數方面，總經理雙元性(DUAL)平均數為 0.17、標準差為 0.372，但第一四分位、第二四分位與第三四分位皆為 0，表示在樣本中，多數公司屬於總經理與董事長非同一人。

表 4-5 變數敘述統計量

變數名稱	觀察值	平均數	標準差	四分位數		
				25	50	75
INSIDER_P(%)	604	21.38	17.51	7.69	14.29	33.33
SIZE	604	7.91	.98	7.16	8.069	8.62
AGE	604	24.25	22.77	8.00	16.00	35.00
INDEP	604	7.49	12.92	.00	.00	13.776
Breach_Z	604	0.22	0.526	.00	.00	.00
虛擬變數						
DUAL	604	.17	.372	.00	.00	.00

第二節　研究方法

本研究將探討董事會之組成對於公司資訊安全管理有效性的影響。以下為本研究之研究方法與模型建立。

模型一欲探討董事會組成與資訊安全事件發生是否有相關性，故以當年度是否發生資訊安全事件(Breach_X)為應變數，若當年度有發生資訊安全事件，其值為 1，反之為 0。董事會組成資料以總經理雙元性(DUALITY) 驗證假說一;內部董事比例(INSIDER)驗證假說二。由於應變數(Breach_X)為二元分類變數(binary variable)，因此將採二元邏輯斯迴歸模型來預測，以下為模型一:

$$Breach\_X_i = \beta_0 + \beta_1 DUALITY + \beta_2 INSIDER + \beta_3 SIZE + \beta_4 AGE + \beta_5 INDEP + \varepsilon_{1i}$$

模型二，使用是否發生多次資訊安全事件之情形(Breach_Y)為應變數，探討董事會組成與當年度多次發生資訊安全事件是否有相關性。縱使總樣本以當年度發生一次性的資訊安全事件為主，但仍有不少公司出現當年度多次發生資訊安全事件，故設應變數 Breach_Y 為發生多次資訊安全事件之情形，其值 0 代表當年度無資訊安全事件發生;1 為發生一次資訊安全事件;2 為發生多次資訊安全事件。由於 Breach_Y 代表畫分後的組本，數字本身不具順序意義，且不同於 Breach_X 僅有 0 與 1，因此透過多項式邏輯斯迴歸模型進行預測，以下為模型二:

$$Breach\_Y_i = \beta_0 + \beta_1 DUALITY + \beta_2 INSIDER + \beta_3 SIZE + \beta_4 AGE + \beta_5 INDEP + \varepsilon_{2i}$$

模型三，由於模型二僅將資訊安全事件分為無發生事件、發生一次事件以及發生多次事件三類，因而忽略發生多次事件情形的組內差異。發生多次事件情形可能包含發生 2 次或超過 2 次等情形，為探討其事件發生的次數是否與董事會組成相關，因而設應變數 Breach_Z 為當年度發生資訊安全事件的次數，並以多元迴歸(Multiple Regression)進行預測，以下為模型三:

$$Breach\_Z_i = \beta_0 + \beta_1 DUALITY + \beta_2 INSIDER + \beta_3 SIZE + \beta_4 AGE + \beta_5 INDEP + \varepsilon_{3i}$$

.

第五章　　實證結果與分析

本章節將透過統計分析軟體 SPSS 17.0 針對前章節所設計的三種模型進行驗證。其後，將依模型順序分別探討並進一步分析實證後之結果。於三種模型的討論過後，在額外測試中再針對股權型態的分類，分別探討家族企業與非家族企業公司，其董事會組成與資訊安全事件發生之相關性。

第一節　模型之實證結果

(一) 模型一: 探討董事會組成與資訊安全事件發生之相關性

首先，於模型一探討董事會組成與資訊安全事件發生是否有相關性，其實證結果列於表 5-1。由表 5-1 可得知，總經理雙元性(DUALITY)的係數方向為負但不達顯著水準(β=-0.306，P=0.992)，由於未達顯著水準且方向性不如預期，故實證結果無法支持假說一。內部董事比例(INSIDER)係數方向為負但不達顯著水準(β=-0.01，p=0.228)，由於未達顯著水準，故實證結果無法支持假說二。

在控制變數方面，公司規模(SIZE) 的係數方向為正但不達顯著水準(β=0.199，p=0.151)，故沒有足夠證據說公司規模影響資訊安全事件發生可能性。公司年數(AGE)的係數方向為負但不達顯著水準(β=-0.002，p=0.707) ，由於未達顯著水準，故沒有足夠證據說公司年數影響資訊安全事件發生可能性。獨立董事佔董事總人數比例(INDEP) 的係數方向為正且達 1%顯著水準(β=0.025，p=0.001)，此結果表示有足夠證據顯示獨立董事占董事總人數比例增加資訊安全事件發生的可能性，意即獨立董事所占董事總人數比例較高，其較可能發生資訊安全事件。此結果符合前述所推論，由於獨立董事對於公司內部資訊安全管理的不熟悉以及經驗的缺乏，使其無法達到良好的監督效果與決策品質，因而獨立董事比例較高，其公司資訊安全管理有效性較差。

表 5-1 董事會組成與資訊安全事件發生可能性之實證結果

變數	預期方向	係數	標準差	P 值
常數		-2.805	1.186	.018**
研究變數				
DUAL=0	+	-.306	.307	.992
INSIDER_P	-	-.010	.008	.228
控制變數				
SIZE		.199	.139	.151
AGE		-.002	.005	.707
INDEP	+	.025	.007	.001***
Model Chi-Square=17.742 Cox and Snell R2=0.029 -2Log Likelihood Ratio=558.558 P 值=0.003;N=604				
註 1:*、**、***分別代表 10%、5%、1%之顯著水準 註 2:各變數定義請參見表 4-4				

(二) 模型二: 探討董事會組成與發生多次資訊安全事件之相關性。

在第一步得知自變數與資訊安全事件發生可能性的相關性後，模型二，將探討發生多次資訊安全事件之情形。應變數部份分為當年度無發生資訊安全事件、發生一次、多次資訊安全事件三類，其實證結果列於表 5-2。採用多項式邏輯斯迴歸模型測試時，以當年度無事件組為基準，將其他的組別(發生一次事件組、發生多次事件組)與基準組比較而得出結果。在表 5-2 中， Panel A 為當年度發生一次資訊安全事件組的迴歸結果，其結果顯示，總經理雙元性(DUALITY)的係數方向為負但不達顯著水準(β=-.240，P=0.476)，故實證結果無法支持假說一。內部董事比例(INSIDER)係數方向為負但不達顯著水準(β=-.008，p=0.357)，故實證結果無法支持假說二。Panel B 為當年度發生多次資訊安全事件組的迴歸結果，其結果顯示，總經理雙元性(DUALITY)的係數方向為負但不達顯著水準(β

=-.560，P=0.367)，故實證結果無法支持假說一。內部董事比例(INSIDER)係數方向為負但不達顯著水準(β=-.021，p=0.230)，故實證結果無法支持假說二

表 5-2 董事會組成與發生多次資訊安全事件之相關性實證結果

	變數	預測方向	係數	標準差	P 值
A	常數		-3.176	1.303	.015
	DUAL=0	+	-.240	.337	.476
	INSIDER_P	-	-.008	.009	.357
	SIZE		.189	.152	.213
	AGE		.003	.005	.580
	INDEP	+	.029	.008	.000***
B	常數		-3.228	2.391	.177
	DUAL=0	+	-.560	.621	.367
	INSIDER_P	-	-.021	.018	.230
	SIZE		.172	.282	.542
	AGE		-.021	.013	.117
	INDEP	+	.003	.018	.861
Model Chi-Square=24.068 Cox and Snell R^2=0.039 -2Log Likelihood Ratio=666.175 P 值=0.007;N=604(492, 90 , 22)					
註 1:*、**、***分別代表 10%、5%、1%之顯著水準 註 2:各變數定義請參見表 4-4					

在控制變數方面，Panel A 的獨立董事比例(β=.029，p=.000) 係數方向為正且達 1%顯著水準(β=0.025，p=0.001)，此結果表示有足夠證據顯示獨立董事占董事總人數比例增加一次性資訊安全事件發生的成敗比，意即獨立董事所占董事總人數比例較高,其較可能一次性發生資訊安全事件。此結果符合前述所推論，由於獨立董事對於公司內部資訊安全管理的不熟悉以及經驗的缺乏，使其無法達到良好的監督效果與決策品質，因而

獨立董事比例較高，其公司資訊安全管理有效性較差。在 Panel A 的公司規模(β=.189，p=.580)、公司年數(β=.003，p=.58)以及 Panel B 的公司規模(β=.172，p=.542)、獨立董事比例(β=.003，p=.861)、公司年數(β=-.021，p=.117)皆不達顯著水準，故沒有足夠證據說變數影響一次性以及多次性資訊安全事件發生可能性。

(三) 模型三:董事會組成與資訊安全事件發生次數之相關性

為了解董事會組成與資訊安全風險事件發生次數是否有相關性，我們建立模型三並使用多元迴歸法，結果列於表 5-3。由表 5-3 可得知，總經理雙元性(DUALITY)的係數方向為正但不達顯著水準(β=0.051，p=0.413)，故無法支持假說一。內部董事比例(INSIDER)係數方向為負但未達顯著水準(β=-0.002，p=0.144)，故實證結果無法支持假說二。

表 5-3 董事會組成與資訊安全事件發生次數相關性之實證結果

變數	預期方向	係數	標準差	P 值
常數		.047	.242	.846
研究變數				
DUAL	-	.051	.063	.413
INSIDER_P	-	-.002	.002	.144
控制變數				
SIZE		.027	.028	.328
AGE		.000	.001	.391
INDEP	+	.003	.002	.054*
Model R^2=0.018 P 值=0.057;F 值=2.164				
註 1:*、**、***分別代表 10%、5%、1%之顯著水準 註 2:各變數定義請參見表 4-4				

在控制變數方面，公司規模(β=.027，p=.328)、公司年數(β=.000，p=.391)以及獨立董事比例(β=.003，p=.058) 係數方向皆為正，但僅獨立董事比例達顯著水準，意指結果沒有足夠證據說公司規模與公司年數正向影響資訊安全事件發生次數，但有足夠證據說獨立董事比例正向影響資訊安全事件發生次數，意即獨立董事所占董事總人數比例較高，其發生資訊安全事件次數較多，此結果亦符合前述之推論結果。

第二節　整體討論與分析

根據上述整體的實證結果，整理如表 5-4。在主要變數方面，總經理雙元性(DUALITY)方面，三個模型驗證中皆不達顯著水準且不符合預期之方向，故實證結果不支持假說一。在內部董事比例(INSIDER)方面，三個模型驗證中雖符合預期之方向但皆不達顯著水準，故實證結果不支持假說二。主要變數皆呈現不顯著之統計結果，可就理論基礎的層面來探究之。本研究採用管家理論作為理論基礎，其理論以“自我實現(Self-actualizing)”作為人類行為的假設前提，並且認為管理階層是集產主義者(Collectivism)，視集體利益極大化為目標，透過滿足所有利害關係人來實現自我價值。因此，在此前提下，管理階層會以公司整體利益為優先，將公司的成功視為個人成功的指標，透過成功的公司經營來獲得自我價值的認同感與工作上的成就感(Davis et al., 1997)。然而，在公司治理的理論中，亦有一派代理理論，其理論以“自利” 作為人類行為的假設前提，並且認為在現今所有權與經營權分離的企業經營環境中，提供資金的企業所有者與實際管理企業營運的經營者之間存有代理關係，此關係意指「一位或多位以上的委託人(Principal)授權給代理人(Agent)代為進行決策，代理方代表委託方執行任務時，彼此之間所存在的契約關係。」因此，在人類的行為皆以追求自我利益極大化為目標的假設前提下，由於負責經營的管理階層無須承擔所有的決策後果，極可能出現以自身利益為前提而非企業整體利益為前提的決策，所有者(委託人)與經營者(代理人)之間便因為利益立場衝突而導致代理問題。為減緩代理問題，可以透過建立監督機制和設計獎勵誘因等方式，一方面監督經營者行為與決策，另一方面結合經營者與所有者的目標，使兩者利益一致。就監督機制而言，董事會被視為監督經理人並保護股東的

重要機制, 其最重要的功能在於監督經理人是否遵照所有者(委託人)的目標來經營公司(Jensen and Meckling, 1976; Walsh and Seward, 1990)。

要就資訊安全事件的角度來看兩個理論，首先必須定義所謂的資訊安全意指必需能保護儲存於資訊系統中資料之機密性(Confidentiality)、完整性(Integrity)與可用性(Availability) (ISO/IEC 17799, 2000)，而資訊安全事件則是違反三者任一的事件發生。為確保資訊安全防護的完善，企業必須設立嚴謹的內部控制機制，以確立流程中的每一個環節皆符合資訊安全的三項特性。然而，就其作業的便利性而言，內部控制機制會降低作業上的效率，使其在完成工作的過程中需要較為繁雜的步驟以符合內部控制之規定。因此，若作業人員為求其自身之便利性，因而容易違反其應遵守之規定流程，故增加企業發生資訊安全事件的風險。此外，在現今企業高度整合資訊系統於企業流程中，許多企業出現經理人為了自身利益的考量，如:維持地位、隱瞞虧損、獲得不當利益，竄改財務報告並提供不實的財務資訊，或員工為追求自身之利益，盜用公款、竄改薪資資料等舞弊事件，如: 2008 年法國第二大銀行興業銀行爆發全球金融史上最大弊案，傳出交易員越權操作，超額交易歐洲股價指數期貨，使興業銀行虧損 49 億歐元，並且遭法國銀行監管當局處以 400 萬歐元罰鍰。2011 年台灣運動彩券爆發主管利用內部控管機制的漏洞，逾時下注，詐取約新台幣 230 萬元。這些事件都意味著企業資訊系統的內部控制不允當以及權限管理機制的失能。由上述所提及之資訊安全事件中可發現，資訊安全事件的發生易來自於追求自我利益的過程中，不論是追求金錢上的利益或是時間上的方便，皆容易造成資訊安全事件的發生。因此，結合資訊安全事件與上述兩個理論的比較，在人類行為假設上，代理理論的人類行為以“自利”為前提，或許較為符合實際導致資訊安全事件發生的人類行為假設。根據代理理論的論點而言，「監督」是規範代理關係並減少代理問題的重要機制，而董事會是內部控制最高階層的機制，是運行監督機制的核心單位，負責監督管理階層的行為 (Fama and Jensen, 1983)。在過去的研究中，持代理理論觀點的學者透過實證研究探討董事會特性與企業舞弊之間的相關性，台灣學者林嬋娟與張哲嘉(2009)於研究中發現，舞弊公司董監事席次異常變動的比例顯著較高; Farber(2005)以及 Beasley(1996)則是指出外部董事人數或席次比例較高的公司發生舞弊的機率較小; Beasley(1996)於同研究中也發現外部董事的任期與持股比例皆與舞弊發生的機率呈負相關。就上述

之探討結果可得知，董事會監督功能與公司發生舞弊機率之間存有相關性，監督是影響企業內部控制良窳的重要因素。因此，對於本研究之主要研究變數-總經理的雙元性與內部董事比例皆呈現不顯著而言，可能是由於在防護資訊的機密性、完整性與可用性方面，以及減少資訊安全事件發生的可能性的過程中，「監督」仍為不可或缺的機制。因此，在強調董事會資源的整合運用能力以及決策的效率與品質同時，仍應多加考量其最主要的監督能力，董事長與總經理之間應存有監督的關係，兩者職位分離能減少經理人控制董事會的機會，強化董事會在風險管理的監督功能，避免企業面臨危機。

表 5-4 所有模型的實證結果

變數	模型一	模型二		模型三
DUAL	-.306	A	-.240	.051
		B	-.560	
INSIDER_P	-.010	A	-.008	-.002
		B	-.021	
SIZE	.199	A	.189	.027
		B	.172	
AGE	-.002	A	.003	.000
		B	-.021	
INDEP	.025***	A	.029***	.003*
		B	.003	

第三節　額外測試

Zahra 和 Pearce Ⅱ (1989)在研究中提到由於董事會同時扮演服務、策略、控制角色，因此，公司會依據其股權控制型態形成不同型態的董事會，以掌控公司運作。延伸推論可得知，透過控制權的行使，持有控制權者能影響董事會之組成與運作，進而左右公司之重大決策。在台灣，上市櫃公司的股權型態普遍是由少數家族集中控股 (葉銀華, 1999)，約三分之二的公司為家族控制，且多數的公司董事會為家族完全掌控(林嬋娟與張哲嘉, 2009)。在過去，亦有學者針對存有控制股東影響公司決策的相關研究，James (1999)於研究中發現，家族企業其股東持股集中

且多為長期投資，因此在投資決策的選擇，會站在長期投資者的角度來評估公司投資方案，因此能減少短視近利的投資，提升投資效率。由於這種存有控制股東的所有權型態，使其董事會的決策受到控制股東的主導。因此，本研究將透過股權型態的分類，進一步探討在不同股權型態的環境下，董事會組成對資訊安全事件發生的影響。

在家族企業(存有最終控制股東)的分類標準上，本研究將參照林嬋娟與張哲嘉(2009)的作法定義家族與非家族企業。係年底最終控制者以個人名義、透過其所控制之(未)上市(櫃)公司、財團法人等出任之董事席次總和超過或等於年底董事會總席次 50%並且最終控制者的總持股數高於 10%者的樣本公司，為家族企業(存有最終控制股東)。延續模型一的研究方法，此部份亦以當年度是否發生資訊安全事件(Breach_X)為應變數，董事會組成為自變數，二元邏輯斯迴歸模型來探討，在不同的股權型態下，董事會組成對資訊安全事件發生的影響。實證結果列於表 5-5 與表 5-6。

首先就家族企業(存有最終控制股東)的實證結果(表 5-5) 可得知，原先不顯著的變數，在透過股權型態分類後，股權型態為存有最終控制股東的型態，其內部董事比例、公司規模、獨立董事比例皆達顯著水準且符合預期之方向。總經理雙元性(DUALITY)的係數方向為負但未達顯著水準(β=-0.099，p=0.819)，因此沒有足夠證據顯示，董事長與總經理由不同人兼任的企業，資訊安全事件發生的可能較低。內部董事比例(INSIDER)係數方向為負且達 10%顯著水準(β=-0.18，p=0.079)，因此有足夠證據顯示，內部董事比例愈高，資訊安全事件發生之可能性愈低。此結果同前述假說之推論，由於內部董事實際參與公司營運活動並熟悉的公司內部流程，故能提升董事會在資訊安全管理相關的決策品質，進而提升公司的資訊安全管理有效性。

在控制變數方面，公司規模(SIZE)係數方向為正且達 5%顯著水準(β=.407，p=0.016) ，因此有足夠證據顯示，公司規模愈大，資訊安全事件發生之可能性愈高。此結果可能是因為公司規模愈大，其風險管理流程愈複雜，因此公司無法完善的監控每一個環節，降低公司資訊安全風險管理的有效性。再者，公司規模較大，其高知名度與龐大誘人的利潤，都使其較容易成為駭客攻擊的目標，因而增加資訊安全事件發生的可能性。公司年數(AGE)係數方向為正但未達顯著水準(β

=.001，p=0.88) ，因此沒有足夠證據顯示，公司年數愈高，資訊安全事件發生的可能較高。獨立董事比例(INDEP)係數方向為正且達 5%顯著水準(β=0.022，p=0.015)，因此有足夠證據顯示，獨立董事比例愈高，資訊安全事件發生之可能性愈高。此結果可能是因為獨立董事是扮演監督的角色，因此公司傾向於不主動提供細部資料，使獨立董事對於公司作業流程的了解不深，因而難以提供切合公司需求的意見與資源，進而降低資訊安全管理的有效性。

表 5-5 股權型態為家族持股之實證結果

股權型態	變數	預期方向	係數	標準差	P 值
家族	常數		-4.661	1.501	.002***
	DUAL=0	+	-.099	.436	.819
	INSIDER_P	-	-.018	.010	.079*
	SIZE		.407	.170	.016**
	AGE		.001	.005	.880
	INDEP	+	.022	.009	.015**
Model Chi-Square=26.757 Cox and Snell R^2=0.053 -2Log Likelihood Ratio=433.88 P 值=0.000;N=496(82.1%)					
註 1:*、**、***分別代表 10%、5%、1%之顯著水準 註 2:各變數定義請參見表 4-4					

其次，就非家族持股的股權型態(沒有最終控制股東)的實證結果(表 5-6)可得知，原先不顯著的變數，在透過股權型態分類後，股權型態為不存在最終控制股東的型態，其總經理雙元性達顯著水準但不符合預期之方向。總經理雙元性(DUALITY)的係數方向為負且達 10%顯著水準(β=-0.938，p=0.074)，因此有足夠證據顯示，董事長與總經理由不同人兼任的企業，其資訊安全事件發生的可能較低。此結果可能是因為董事長與總經理職位分離的情況，能使董事會更完善的扮演監督的角色，監督公司風險管理的落實，減少高風險的營運決策發生，提升公司資訊安全管理的有效性。內部董事比例(INSIDER)係數方向為正但未達顯著水準

(β=0.024，p=0.194)。在控制變數方面，公司規模(SIZE)係數方向為負但未達顯著水準(β=-0.405，p=0.234)。公司年數(AGE)係數方向為正但未達顯著水準(β=.019，p=0.218)。獨立董事比例(INDEP)係數方向為正但未達顯著水準(β=0 .014，p=0.341)

表 5-6 股權型態為非家族持股之實證結果

股權型態	變數	預期方向	係數	標準差	P 值
非家族	常數		1.123	2.645	.671
	DUAL=0	+	-.938	.525	.074**
	INSIDER_P	-	.024	.019	.194
	SIZE		-.405	.340	.234
	AGE		.019	.015	.218
	INDEP	+	.014	.015	.341
Model Chi-Square=12.783 Cox and Snell R^2=0.112 -2Log Likelihood Ratio=101.634 P 值=0.026;N=108 (17.9%)					
註 1:*、**、***分別代表 10%、5%、1%之顯著水準 註 2:各變數定義請參見表 4-4					

第六章　　結果與建議

第一節　研究結果與貢獻

在現今競爭激烈的環境中，資訊科技的採用已被視為企業強化其競爭力時不可或缺的工具。資訊科技在企業中所扮演的角色，小至每日交易明細的處理，大至企業整體資源的規劃以及高階管理階層在重大營運決策上的輔助，資源科技對於企業營運流程的密切相關，使其在企業中佔有關鍵影響力。歷年來，資訊安全事件頻傳，不僅高度依賴資訊科技的企業遭受財務與商譽的損失，駭客入侵竊取國家機密亦使國家安全遭受威脅，因此資訊科技相關的資訊安全問題議題更為受到各界的重視。近年有許多資訊安全事件皆來自於企業內部流程控管不當而導致，更由於恩隆案的爆發，使各界開始重視企業內部控制與治理對於公司資訊安全管理的影響。各國透過法令的制定，迫使企業重視內部控制與治理，並且必須將資訊安全視為企業整體公司治理的一環，以公司治理的角度符合法規所強調的完善治理與資訊安全管理。在公司治理中，董事會為內部治理的核心機制，亦被視為決定企業風險管理成效的重要元素之一。因此可知，董事會是影響內部控制與治理的重要因素，其成員的組成將影響董事會監督效果與決策品質，進而影響企業資訊安全管理成效，故本研究目的將以管家理論(Stewardship Theory)為理論基礎探討董事會組成對於公司資訊安全管理有效性的影響。此外，由於在過去的研究中顯示，股權型態的差異會影響董事會的決策方向且台灣的股權型態普遍是由少數家族集中控股，因此，本研究將進一步的透過股權型態的分類來探討探討董事會組成對於公司資訊安全管理有效性的影響。

本研究以 1996 年至 2011 年台灣上市(櫃)公司為樣本，討論董事會組成對於公司資訊安全管理有效性的關聯性。結果顯示，公司獨立董事比例愈低，其資訊安全管理成效愈高。根據本研究的假說推論而言，並非董事會中的所有人員皆擁有相同的資訊量，獨立董事由於其獨立性，在沒有參與公司實際營運作業的情況下，使其相較於內部董事而言，較不了解公司內部作業流程。再者，由於獨立董事扮演監督的角色，因而公司傾向於不主動提供細部資料，也使獨立董事無法提供切合公司需求的關鍵意見與資源，進而降低資訊安全管理的有效性。此外，在透過股權型態分類後，股權型態為存有最終控制股東的型態，其內部董事比例愈高、

公司規模愈小、獨立董事比例愈低，資訊安全管理成效愈高。股權型態為沒有最終控制股東的型態，其董事長與總經理由不同人兼任的企業，資訊安全管理成效愈高。

在過去的研究中，不論是資訊安全領域或是公司治理領域，和公司董事會組成與資訊安全管理有效性相關的研究並不多。首先，本研究透過資訊安全管理方面與公司治理方面的文獻整理，結合管家理論的觀點詮釋，並進一步透過股權型態的分類來探討董事會組成對於資訊安全管理有效性的影響，可做提供為未來相關研究的參考。其次，希望透過本研究的實證結果，能夠給予企業在關於董事會組成的議題上一個參考與建議，讓企業在考量董事會的組成結構時，除了考量董事會的監督效益，更能進一步的思考董事成員在資源整合與提供的重要性以及企業股權型態的差異，使董事會在監督能力與關鍵資源提供能力上取得良好的權衡。

第二節　研究限制與建議

本研究之研究限制最主要在於樣本來源可靠性。應變數方面，由於台灣目前尚未建立統一收集資訊安全事件資料的單位和資料庫，因此本研究之資訊安全事件的樣本，是透過手動關鍵字搜尋各大相關網站來取得。藉由此方式取得樣本，則樣本品質受限於手動搜尋的時間與相關網站的可信度，故在資訊安全事件樣本方面，無法確保完全涵蓋每年度各公司發生的所有資訊安全事件，因而影響實證之結果。再者，就資訊安全事件樣本的分佈情況來看，樣本在產業分佈上呈現分佈不均的情形，並非涵蓋所有的產業，因此實證結果無法推論至所有上市櫃公司。自變數方面，董事會組成變數樣本資料皆來自於台灣經濟新報資料庫，故資料的正確性受該資料庫信度影響，亦可能影響實證之結果。再者，影響資訊安全管理有效性的董事會組成因素，仍有許多尚未被本研究納入考量，例如:董事背景、董事經驗、董事任期、董事涉入董事會程度等等，此部份仍待未來之實證研究證實。

基於前述所提的研究限制，本研究仍有許多地方需待未來學者進一步研究。首先，就前段所提的部份，未來研究可進一步探討會影響資訊安全管理有效性的董事會組成變數。其次，在額外測試中，本研究是以股權型態作為分類，然而，由於法規規範和企業所屬競爭環境的不同，使得不同產業對於資訊安全的注重程度

有所差異，亦會使其資訊安全管理成效有落差，因此在未來的研究中亦可針對產業類別進行分類，再進一步的探討董事會組成對於資訊安全管理有效性的影響。再者，股權型態除了家族型態，亦有其他學者提出法人、政府持股的比例的高低亦是影響企業營運績效的因素，因此，在未來的研究中，亦可以針對法人、政府持股比例進行分類，再進一步的探討董事會組成對於資訊安全管理有效性的影響。

文獻參考

[1] Abbasi, A., Zhang, Z., Zimbra, D., Chen, H., and Nunamaker, J. J. F. 2010. Detecting fake websites: the contribution of statistical learning theory. MIS Quarterly, 34:435-461.

[2] Adams, R. and D. Ferreira 2007. A theory of friendly boards. The Journal of Finance, 62(1):217-250

[3] Agrawal, A. and C. Knoeber. 1996. Firm performance and mechanisms to control agency problems between managers and shareholders. Journal of Financial and Quantitative Analysis, 31: 377-397.

[4] Ashbaugh-Skaife, H., D. W. Collins, and W. R. Kinney Jr. 2007. The Discovery and Reporting of Internal Control Deficiencies prior to SOX-Mandated Audits. Journal of Accounting and Economics, 44: 166-192.

[5] Baliga, B. R., N. C. Moyer, and R. S. Rao 1996. CEO duality and firm performance: What's the fuss. Strategic Management Journal, 17(1):41–53.

[6] Baysinger, B. D., and R. E. Hoskisson 1990. The Composition of Boards of Directors and Strategic Control: Effects on Corporate Strategy. Academy of Management Review, 15:72-87.

[7] Beasley, M. S. 1996. An empirical Analysis of the Relation between the Board of Director Composition and Financial Statement Fraud. The Accounting Review, 71: 443-465.

[8] Becker, G. 1964. Human Capital. New York: Columbia University Press.

[9] Berle, A. and Means. G. C. 1932. The Modern Corporation and Private Property, New York: Macmillan Publishing Co.

[10] Besnard, D and Arief, B. 2004. Computer security impaired by legitimate users. Computers and Security, 23:253–64.

[11] Bilbao A. TUAR 1992. A model of risk analysis in the security field. CH3119-5/92. IEEE.

[12] Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., and Boss, R. W. 2009. If Someone is Watching, I'll Do What I'm Asked: Mandatoriness, Control, and Information Security. European Journal of Information Systems, 18:151-164.

[13] Boyd, B. 1990. Corporate Linkages and Organizational Environment: A Test of the Resource Dependence Model. Strategic Management Journal, 11:419-430.

[14] Boyd, B. K. 1994. Board Control and CEO Compensation. Strategic Management

Journal, 15: 335-344.

[15] CGTF (Corporate Governance Task Force) Report, (2004) Information Security Governance, A Call to Action, National Cyber Security Summit Task Force, URL www.cyberpartnership.org/InfoSecGov4_04.pdf , Accessed 17 May 2004.

[16] Dalton, D. R., Daily, C. M., Ellstrand, A. E., and Johnson, J. L. 1998. Meta-analytic reviews of board composition, leadership structure, and financial performance. Strategic Management Journal, 19: 269-290.

[17] Dalton, D. R., Daily, C. M., Ellstrand, A. E., and Johnson, J. L. 1999. Number of directors and financial performance: A meta-analysis. Academy of Management Journal, 42: 674-686.

[18] Damianides M. 2005. Sarbanes-oxley and IT governance: new guidance on IT control and compliance. Information Systems Management, 22(1):77–85.

[19] D'Arcy, J., Hovav, A., and Galletta, D. F. 2009. User Awareness of Security Countermeasures and its Impact on Information Systems Misuse: A Deterrence Approach. Information Systems Research , 20(1): 79-98.

[20] Davis, J.H., Schoorman, F.D., and Donaldson, L. 1997. Toward a stewardship theory of management. Academy of Management Review, 22: 20-47.

[21] Dhillon, G. and Mishra, S. 2006. The Impact of Sarbanes-Oxley Act on Information Security Governance. In Enterprise Information Systems Assurance and Systems Security: Managerial and Technical Issues. Eds Warkentin, M. and Vaughn, R. Hershey PA, Idea Gr.

[22] Dhillon G. 2001. Violation of safeguards by trusted personnel and understanding related information security concerns. Computers and Security, 20:165e72.

[23] DiPietro, R. and L. V. Mancini. 2003. Security and privacy issues of handheld and wearable wireless devices. Communications ACM, 46(9):74–79.

[24] Donaldson, L., and Davis, J.H. 1989. CEO governance and shareholder returns: Agency theory or stewardship theory. Paper presented at the annual meeting of the Academy of Management, Washington, DC.

[25] Donaldson, L., and Davis, J. H. 1991. Stewardship theory or agency theory: CEO governance and shareholder returns. Australian Journal of Management, 16: 49-64.

[26] Donaldson, L., 1985, In Defence of Organization Theory. A Reply to the Critics (Cambridge, Cambridge University Press).

[27] Douma, S., R. George, and R. Kabir. 2006. Foreign and Domestic Ownership, Business Groups, and Firm Performance: Evidence from a Large Emerging Market. Strategic

Management Journal, 27: 637-657.

[28] Eisenhardt, K. M. 1989. Agency theory: An assessment and review. Academy of Management Review, 14: 57-74.

[29] Eloff, J. H. P., Labuschagne, L., and Badenhorst, K. P. 1993. A Comparative Framework for Risk Analysis Methods, Computers and Security, 12 (6) :597-603.

[30] Evans, D. S. 1987. The Relationship between Firm Growth, Size, and Age: Estimates for 100 Manufacturing Industries. Journal of Industrial Economics, 35(4):567-81.

[31] Farber, D. B. 2005. Restoring trust after fraud: Does corporate governance matter? The Accounting Review , 80: 539-561.

[32] Fama, E. F., and M. C. Jensen. 1983. Separation of ownership and control. Journal of Law and Economics, 26: 301-325.

[33] Finkelstein, S., and D'Aveni, R. A. 1994. CEO duality as a double-edged sword: How boards of directors balance entrenchment avoidance and unity of command. Academy of Management Journal, 37: 1079-1108.

[34] Golden, B. R. and E. J. Zajac. 2001. When will boards influence strategy? Inclination×Power=Strategic change. Strategic Management Journal, 22: 1087-1111.

[35] Gordon, L. A., M. P. Loeb, and C. Y. Tseng. 2009. Enterprise Risk Management and Firm Performance: A Contingency Perspective. Journal of Accounting and Public Policy, 28: 301-327.

[36] Harris S. 2003. All-in-one CISSP certification exam guide, second edition, McGraw-Hill/Osborne Media, pp20-21.

[37] Heracleous, L. 2001. What is the impact of corporate governance on organizational performance? Corporate Governance: An International Review, 9 (3):165-73

[38] Hone K, Eloff JHP. 2002. Information security policy – what do international standards say? Computers and Security, 21(5):402–9.

[39] Huse, M. 2005. Accountability and Creating Accountability: a Framework for Exploring Behavioural Perspectives of Corporate Governance. British Journal of Management, 16: S65-S79.

[40] ISACF (2001). Information Security Governance: Guidance for Boards of Directors and Executive Management. Information Systems Audit and Control Foundation. (online). (cited 05 May 2005). Available on Internet: URL http://www.isaca.org/Content/ContentGroups/ITGI3/Resources1/Information_Security_Governance_Guidance_for_Boards_of_Directors_and_Executive_Management/infosecurity.pdf.

[41] ISO/IEC. Information technology – code of practice for information security management, ISO/IEC 27002:2005. The International Organization for Standardization/The International Electrotechnical Commission; 2005.

[42] ITGI 1(IT Governance Institute), 2001. Information Security Governance: Guidance for Board of Directors and Executive Management, IT Governance Institute (ITGI), URL www.itgi.org, Accessed 17 May 2005.

[43] ITGI 2 (IT Governance Institute), 2003. IT Governance Executive Summary, URL www.itgi.org, Accessed 18 April 2004.

[44] Jahner, S., and Krcmar, H. 2005. Beyond Technical Aspects of Information Security: Risk Culture as a Success Factor for IT Risk Management. In Proceedings of the 11 th Americas Conference on Information Systems, Omaha, NE, August 11-14.

[45] James, H. S. 1999. Owner as manager, extended horizons and the family firm. International Journal of the Economics of Business, 6 (1): 41-56.

[46] Jensen, M.C and W.H. Mecking 1976. Theory of The Firm: Managerial Behavior, Agency Costs and Ownership Structure. Journal of Financial Economics ,3: 305-360.

[47] Kailey MP and Jarratt P. 1995. RAMeX: a prototype expert system for computer security risk analysis and management. Computers and Security, 14(5):449 e 63.

[48] Knapp, K. J., Franklin, M. R., Marshall, T. E., and Byrd, T. A. 2009. Information Security Policy: An Organizational-Level Process Model. Computers and Security, 28(7): 493-508.

[49] Knapp K, Marshall T. E., Rainer R. K., Ford F. N. 2006. Information security: management's effect on culture and policy. Information Management and Computer Security, 14(1):24–36.

[50] Kor, Y. Y. 2006. Direct and interaction effects of top management team and board compositions on R&D investment strategies. Strategic Management Journal, 27: 1081–99.

[51] Kosnik, R. D. 1987. Greenmail: A study of board performance in corporate governance. Administrative Science Quarterly, 32:163-185.

[52] Kraemer, S., Carayon, P. and Clem, J. 2009. Human and organizational factors in computer and information security: Pathways to vulnerabilities. Computers and Security, 28.

[53] Kritzinger and E. Smith 2008. Information security management: an information security retrieval and awareness model for industry. Computers and Security, 27:224–

231.

[54] La Porta, R., F. Lopez-de-Silanes, and A. Shleifer. 1999. Corporate ownership around the world. Journal of Finance, 54: 471-517.

[55] Letza, S., Sun, X. and Kirkbride, J. 2004. Shareholding versus Stakeholding: a critical review of corporate governance. Corporate Governance: An International Review, 12(3): 242–262.

[56] Lihong, Z., Casconcelos, A., and Nunes, M. 2008. Supporting decision making in risk management through an evidence-based information systems project risk checklist. Information Management and Computer Security, 16 (2):166–186.

[57] Luthy D. and Forcht K. 2006. Laws and regulations affecting information management and frameworks for assessing compliance. Information Management and Computer Security, 14(2):155-166.

[58] Ning, P., Y. Cui, D. S. Reeves, D. Xu. 2004. Techniques and tools for analyzing intrusion alerts. ACM Trans. Inform. System Security, 7(2): 274–318.

[59] Nosworthy J. 2000. Implementing information security in the 21stCentury – do you have the balancing factors? Computers and Security, 19(4):337–47.

[60] Pahnila, S., Siponen, M., and Mahomood, A. 2007. Employees' Behavior Towards IS Security Policy Compliance. Proceedings of the 40th Annual Hawaii International Conference on System Sciences, IEEE Computer Society, p.156b.

[61] Pfeffer, J. 1972. Size and composition of corporate boards of directors: The organization and its environment. Administrative Science Quarterly, 17: 218–28.

[62] Pfeffer, J. and Salancik, G. R. 1978. The External Control of Organizations: A Resource Dependency Perspective. Harper and Row, NewYork.

[63] Pound, J. 1988. Proxy Contests and the Efficiency of Shareholder Oversight. Journal of Financial Economics, 20:237－265

[64] Posthumus S and Von Solms R. 2004. A framework for the governance of information security. Computers and Security, 23(8):638–46.

[65] Rechner, P. L. and D. R. Dalton 1989. The Impact of CEO as Board Chairperson on Corporate Performance. Academy of Management Executive, 2:141－143

[66] Rechner, P. L. and D. R. Dalton 1991. CEO duality and organizational performance: A longitudinal analysis. Strategic Management Journal, 12(2):155–160.

[67] Richard P. W. 1997. Iris recognition: An emerging biometric technology, Proc. IEEE 85 (9):1348–1363.

[68] Ruighaver AB, Maynard SB, and Chang S. 2007. Organizational security culture: extending the end-user perspective. Computers and Security, 26(1):56–62.

[69] Sarathy, R. and K. Muralidhar. 2002. The security of confidential numerical data in databases. Information Systems Research, 13(4) :389–403.

[70] Sandhu, R. and P. Samarati. 1996. Authentication, access control, and audit. ACM Computing Surveys, 28(1): 241–243.

[71] Shleifer, Andrei, and Robert Vishny 1986. Large shareholders and corporate control. Journal of Political Economy, 94: 461-488.

[72] Shleifer, Andrei, and Robert W. Vishny, 1997, A survey of corporate governance, Journal of Finance, 52: 737-783.

[73] Siponen, M. T. 2005. An analysis of the traditional is security approaches: implications for research and practice. European Journal of Information Systems, 14 (3):303–315.

[74] Straub D. W. 1990. Effective IS security: an empirical study. Information Systems Research, 1(3):255–76.

[75] Straub, D. W. and Welke, R. J. 1998. Coping with systems risk: Security planning models for management decision making. MIS Quarterly, 23(4): 441–469.

[76] Siponen, M. T. and Vance, A. 2010. Neutralization: New Insight into the Problem of Employee Information Systems Security Policy Violations. MIS Quarterly, 34(3):487-502.

[77] Ransbotham, S. and S. Mitra 2009. Choice and chance: A conceptual model of paths to information security compromise. Information Systems Research , 20 (1): 121–139.

[78] Thomson, M.E. and von Solms, R. 1998. Information security awareness: educating our users effectively. Information Management and Computer Security, 6(4):167-73.

[79] Volonino L, Gessner GH, Kermis GF. 2004. Holistic compliance with sarbanes-oxley. Communications of the Association for Information Systems, 14:219–33.

[80] Von Solms, B. 2000. Information Security – The Third Wave? Computers and Security, 19:615–620.

[81] Von Solms, B. 2006. Information security – the fourth wave. Computers and Security, 25:165–168.

[82] Von Solms, B. and von Solms, R. 2006(a). Information security governance: Due care. Computers and Security, 25(7): 494-497.

[83] Walsh, J. P., and J. K. Seward. 1990. On the Efficiency of Internal and External Corporate Control Mechanisms. The Academy of Management Review, 15: 421-458.

[84] Warkentin, M., and Willison, R. 2009. Behavioral and Policy Issues in Information

Systems Security: The Insider Threat. European Journal of Information Systems, 18 (2) :101-105.

[85] Werlinger R, Hawkey K, Beznosov K. 2009. An integrated view of human, organizational, and technological challenges of IT security management. Information Management and Computer Security, 17(1):4–49.

[86] Westphal, J. D. and E. J. Zajac 1995. Who shall govern? CEO/board power, demographic similarity, and new director selection. Administrative Science Quarterly, 40:60–83.

[87] Westphal, J. D. 1999. Collaboration in the boardroom: Behavioral and performance consequences of CEO-board social ties. Academy of Management Journal, 42: 7-24.

[88] Whitman, M. 2003. Enemy at the Gate: Threats to Information Security. Communications of the ACM, 46 (8) : 91-95.

[89] Woodhouse, Steven, 2007 .Information Security: End User Behavior and Corporate Culture. 7th IEEE International Conference on Computer and Information Technology.

[90] Zahra, S. A. and J. A. PearceⅡ. 1989. Boards of directors and corporate financial performance: A review and integrative model. Journal of Management, 15: 291–334.

[91] Zajac, E. J. and J. D. Westphal. 1996. Director reputation, CEO-board power, and the dynamics of board interlocks. Administrative Science Quarterly, 41(3):507-529.

[92] 洪國興、季延平、趙榮耀 ，2003，<組織制定資訊安全政策對資訊安全影響之研究>，《資訊管理研究》，第 3 期,頁 65-96。

[93] 李存修、葉銀華、柯承恩，2002，公司治理與評等系統，商智文化