國立台灣大學管理學院資訊管理研究所

碩士論文

Department of Information Management

College of Management

National Taiwan University

Master Thesis

資訊安全委外與企業競爭優勢之探討

The Study of Information Security Outsourcing and Competitive Advantage of the Enterprises

陳禹帆

Yu-Fan, Chen

指導教授：許瑋元　博士

Advisor: Wei-Yuan Hsu, Ph.D.

中華民國九十九年六月

June, 2010

國立臺灣大學碩士學位論文
口試委員會審定書

資訊安全委外與企業競爭優勢之探討

本論文係 陳禹帆 君（學號 R97725028）在國立臺灣大學資訊管理學系、所完成之碩士學位論文，於民國九十九年七月二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：張欣綠

王大維

許漢文

所　　長：陳勁松

致謝

本論文得以順利完成,首先要感謝指導我的許瑋元老師,在整個研究過程中，老師的專業素養與研究精神深深的影響了學生，讓我獲益良多，也學習到作研究應有的態度與方法，而在平常與老師的相處之中，也讓學生更加的了解待人處世之道，如此的言教及身教，讓學生受益無窮。

另外，感謝張欣綠老師、王大維老師，撥冗審閱論文，並於口試期間給予許多寶貴意見,提供學生修正的方向,使得本論文更加的完善。對於師長們的提攜，學生萬分感激。

感謝林育滋、歐陽瑜學姐 學姊在研究中給出了許多寶貴的建議，幫助學生解決的許多的疑惑，而在日常生活中，學姐也給了很大的支持與鼓勵，讓我獲益非淺。感謝研究所同學及學弟妹們，振杰、偉銘、建宇、昱呈、似琪，在這兩年內大家一起努力、互相的砥礪，學習到了大家的長處，也讓我看見自己的不足，真的很高興這兩年的生活能跟你們共度。此外，感謝湛盧、PEG、BAFA、AMICI、星巴克水源門市，沒有這些地方的陪伴，我也無法順利的完成論文。

最後將此論文獻給我的家人，感謝父母多年來辛苦的照顧與栽培，以及舅舅及姑姑在研究過程中所給予的幫助，還有靜瑜，她的鼓勵與付出，讓我擁有前進的動力，謝謝你們。

摘要

現今的經營環境中，企業大量的運用資訊科技來輔助業務之運作，資訊已經變成企業的重要資產，伴隨而來的資訊安全風險也逐漸提高，但是想要建構完善的資訊安全環境需要龐大且複雜的資源，企業難以一己之力達成目標，因此組織試圖利用委外的方式，將資訊安全委由外部的服務供應商來完成，此舉促使企業能以較低的成本獲取較佳的資訊安全效益，包括基礎設備、科技能力、管理建議、事故回應能力等等，讓企業能夠更加專注於核心業務、降低資安風險，並透過與外部供應商合作創造出獨特的競爭優勢。

本研究以資源基礎理論之觀點，將資訊安全視為企業的資源，並且考慮企業在將資訊安全委外之後，所擁有或者觸及的資安資源與企業之競爭優勢之間的相互關係，期望能藉此深入了解資安委外是否能夠為企業帶來實質上的效益。透過實證研究後發現，委外後所獲得的資訊安全資產的確能夠為企業帶來競爭優勢，不論在降低成本或者差異化方面都有顯著的影響。但是在委外後企業所獲得的資訊安全能力方面，與降低成本或者差異化的關係，並非如預期般的呈現正向顯著相關。

本研究建議企業必須先確定對於資訊安全之定位，才能夠選擇適合自己的資安策略。而商業環境變化快速，維護資訊安全所需的要素及條件可能瞬間改變，單獨憑藉自身力量難以確保資訊安全，更多的是需要仰賴專業的服務供應商給予建議或協助，在互信互惠的情況下發展資訊安全，才能夠達成雙贏的局面，並且為企業帶來競爭優勢。

關鍵詞：資訊安全委外，資源基礎理論，競爭優勢

Abstract

In today's business environment, organizations applying various information technologies to facilitate business operational capability, as information itself become one of the important assets; it resulted in the increase awareness of organization's information security risks. Apparently, constructing a fine information security structure is complex; such work cannot be easily accomplished by the organization alone. For such reason, outsourcing information security service to external service provider is then considered to be an effective and efficient way to gain source of information security with lower cost.

Applying resource-based view as our theoretical foundation, we posited information security as a resource of business enterprise and its relationship with competitive advantages gained after outsourcing. Our empirical results reveal that the information security assets gained by outsourcing creates competitive advantages for organizations in both cost and market differentiation aspects. Surprisingly, the relationship between information security capabilities gained by outsourcing and the competitive advantages are not positive significant as expected.

Our finding suggested, organization shall precisely position their information security in favor of an adequate information security strategic planning. Business environment change rapidly continually, consequently, requirements and criteria to maintain information security subjected to diverse setting. We suggest by looking out for external resources from experts and maintaining good relationship with service providers, organizations can attain competitive advantages via cooperation and build on mutual trust.

Keywords: information security outsourcing, resource-based theory, competitive advantage

目錄

表目錄

圖目錄

第一章　緒論

第一節　研究背景與動機

1.1.1 資訊安全的定位與特性

隨著企業全球化的經營，企業所擁有的資訊已經變成重要的資產，隨之而來的資安風險也越來越高，企業為了保護所擁有的資產，開始尋找可能的解決方案(PWC, 2008)。而對大部分的企業而言，資訊安全並非其核心的業務，就如同 IT 一樣，雖然對於企業而言是不可或缺的一部分，但是應該更普及的使用，讓企業在執行核心業務時能夠得到 IT 適當地輔助，聚焦在競爭策略的思考及突破而非單純的想靠 IT 來獲取競爭優勢(Carr, 2003a)，在資訊安全上也是如此，企業當然需要完整的資訊安全解決方案，但是並不是單純靠執行良好的資安措施來獲取競爭優勢，而是將資安視為輔助，讓企業能夠放心的聚焦在核心業務，以及讓合作的廠商更加的放心，藉此來獲取競爭的優勢。

雖然資訊安全並非企業的主要業務，但是如果沒有做好資訊安全的管理卻可能給企業帶來極大的風險，尤其在近年經濟衰退的影響下，企業面臨的風險比以往都還要高，例如解僱的員工以及合作的公司倒閉都可能衍生出更多的資安問題，因此企業的經營者也比以往更重視整體的資訊安全(PWC, 2010)。然而對於企業而言，想要自行建置完整的資安措施相當不容易，像是資安人員的培訓不易、技術不足，資安需要 24/7 全天候、無間斷的監控管理，所需耗費的成本極高，大多數的企業缺乏足夠的經驗來處理資安事件，往往都是遭受攻擊或損失才開始重視資安問題，員工缺乏足夠的風險意識等等，都造成企業暴露在很高的資安風險之中，

然而若能考慮將資訊安全委外，由外在的服務供應商來提供資安服務，讓核心業務為資安服務的業者來提供服務，在技術上能夠得到很好的支援，全天候的監控對於服務商而言是基本的業務，能夠為企業減輕成本負擔，而且資安廠商擁有較為豐富的事故處理經驗，並且能夠掌握最新的資訊安全資訊，提供企業最即時的協助，總和上述幾點，資安委外將可以為企業帶來夠大的效益，解決不易處理的資安問題，獲取追求競爭優勢的機會(Bruder, 2006)。而在 E&Y(2009)的全球資安調查報告中也指出企業發展資訊安全主要的挑戰來自於缺乏適合的資源，其中有56%的受訪者認為自身企業所擁有的資源不足,所以 E&Y 建議企業應該在適合的情況下向外界尋求協助。

1.1.2 資訊安全委外的發展趨勢

現今企業將資訊安全管理委外的比例並不高，根據 CSI 2008 的調查報告指出，約有六成的受訪企業並沒有將資安委外的動作，而其他有將資安委外的企業裡面，又以低程度的外包比例(up to 20%)為多數，不過此調查中也提及在 IT 的預算裡面，資訊安全所佔用的比例逐年升高，而且在審計部門以及法務的部門也編列了用於資訊安全的預算，由此可以看出資訊安全已經逐漸受到企業的重視，在未來有很大的進步空間,此外如同上一段提到的企業自行建置資安措施並不容易，此調查認為資安委外仍然是一個相當具有吸引力的選項，而資安委外市場也具有相當不錯的發展潛力(Richardson, 2008)。

根據 IDC 估計從 2006 年至 2011 年全球資安服務市場將以 17.4%之複合成長率持續成長，在五年內市場規模將擴大兩倍，而資安服務佔整體資安市場的比例也逐年的增加，將於 2009 年突破五成，這表示企業投資在資安上面將有過半消費在服務上，而資安服務的需求大於資安產品的需求即說明了企業將資安委外的比

例越來越高(IDC, 2007)。Gartner 也於 2007 年提出預估，至 2012 年為止全球資安服務市場規模之年複合成長率將達到 30%(Gartner, 2007)。綜合上述的調查報告可以看出資訊安全委外這個領域雖然剛起步不久，不過未來的發展趨勢是相當看好的。

1.1.3 研究動機

在現今的商業環境之下，企業與外界的資訊流通極為頻繁並且伴隨著網路的普及變得難以掌控，保護這些資訊安全的重要性與日俱增，然而資訊安全並非大多數企業的核心業務，加上維護資訊安全的困難度很高，花費的成本是否達到成效也難以評估，因此企業開始思考是否能夠透過委外來降低成本、轉移風險、達到預期的效果，甚至是創造競爭的優勢。

資訊安全委外相較於一般的資訊系統委外有其特殊性，像是牽涉到了企業與服務供應商之間的信賴問題，以及資訊安全的投資較難看出成效等等，造成企業在面臨選擇資訊安全是否委外時，需要作更多更深入的考慮。加上之前也提到許多的調查報告都相當看好資訊安全委外這塊市場，這表示資訊安全委外被認為是一個可行的方向，因此現在這個時間點，對於該不該把資訊安全委外是企業急切需要了解的課題。

過去已經有許多的研究在探討資訊系統委外，但是在資訊安全委外這部份的研究仍然有很大的不足，因此本研究希望能夠透過理論以及實證來研究資訊安全委外這個領域，探討資安委外是否能夠幫助企業獲取競爭優勢。競爭優勢是指該公司目前及潛在的競爭對手，無法同步執行該公司現在所執行之價值造策略(value creating strategy)，而持久競爭優勢指的是對手除了無法同步執行該公司現在所執

行之價值造策略之外，也無法複製並取得該公司在此策略中所獲取的利益，可讓該公司的競爭優勢維持一段較長的時間(Barney, 1991)。利用理論作為基礎能夠更有力的支持研究的結果，除了繼續發展資訊安全委外的相關研究之外，對於企業而言也更具有參考的價值。

第二節　研究目的

本研究的主要目的是藉由學理及實務上的探討，透過理論所提供的架構來檢視企業組織在資訊安全委外的情況下，是否能夠獲得持久的競爭優勢，並且利用實證來檢視其成果。

本研究的主要目的是藉由資源理論的觀點作為基礎，並結合實務上的探討，以了解台灣地區的企業組織在其將資訊安全委外的活動之中，是否能夠實際的獲取利益，甚至取得持久的競爭優勢。

本研究的目的旨在探討下列各項議題：

一、探討企業在進行資訊安全委外的活動之後，是否能夠獲取實際的利益，創造競爭優勢。

二、了解企業在進行資訊安全委外活動之後，其資訊安全資源與成本之間的關聯性。

三、了解企業在進行資訊安全委外活動之後，其資訊安全資源與差異化之間的關聯性。

本研究的結果希望提供給台灣的企業，作為評估進行資訊安全委外活動時的參考,以協助企業接觸或者獲取資訊安全資源,並且轉化成為經營上的競爭優勢。而目前國內的學術界中，對於資訊安全委外的研究仍然不多，並且多數為理論的闡述，本研究希望能夠從實務的探討著手，提供學界對於資訊安全委外更深一層的認識。

第二章　文獻探討

第一節　資訊安全

2.1.1　資訊安全定義

Smith(1989)認為任何電腦安全政策之廣義目標，必須要能保護系統中資料之完整性(Integrity)、可用性(Availability)、與隱密性(Confidentiality)。而較為廣義的電腦安全則可以分成以下幾類(Icove, Seger, & VonStorch, 1995)：

一、實體安全(Physical Security)：實體安全保護電腦設備，包括了電腦主機、磁碟、相關文件、實體的建築設施等等。實體安全確保電腦設備不受天然災害、人為因素及其他環境因素所帶來的改變或破壞。

二、人員安全(Personnel Security)：人員安全確保電腦安全不受到來自人員的安全威脅，包括員工、廠商、犯罪者及其他可能的威脅來源。

三、通訊及資料安全(Communication and Data Security)：通訊安全旨在保障資料傳送的安全，包括了郵件、電訊、傳真、網路通訊的安全等等。

四、作業安全(Operations Security)：作業安全目的在於防止潛在的犯罪者進行電腦犯罪。

隨著資訊安全的問題在這幾年逐漸受到重視，Zafar 等學者認為資訊安全是個龐大且複雜的議題，不能夠單以一兩句話或者單一的面向就定義出其概念，應該要用較為完整的觀點來考量，他們認為資訊安全的定義需由下列的各項敘述所構成(Zafar & Clark, 2009)：

一、了解組織可能的潛在威脅，並且針對其威脅作適當地的風險評估。

二、在安全意識、處理的規則及資訊安全現存的最佳實務這幾個方面，給於人員完善的教育訓練。

三、建立資訊安全的政策及程序來保護資訊的資產，避免其受到有意或無意的傷害。

四、建立資訊安全的政策及程序來降低資訊安全事故發生時遭受的損失。

五、實行適合的科技並加以監控，來阻止或者減少未來資訊安全事故發生時造成的損失。

六、對於科技、政策、程序、人員各方面持續的評估，以確保對於資訊安全議題有適當地管理。

七、將資訊安全管理併入公司治理並視為重要的一部分。

然而隨著時代的演進，企業使用資訊的方式也產生了很大的變化，我們可以發現資訊安全的定義也不斷地跟著改變，所涵蓋的範圍持續的擴展，在下一個段落，我們將更詳細的敘述目前資訊安全的發展情形。

2.1.2 資訊安全發展現況

綜觀而言，資訊安全的發展過程與資訊系統的發展有著密不可分的關係，因為當使用的資訊技術出現了新的威脅或者發現了新的漏洞，才會有人注意到其安全問題所帶來的危險，這是難以避免的情況。在早期的大型主機時代，系統沒有網路對外連結，只有少數的技術人員能夠操作電腦，所以較注重實體上的安全，如一些對硬體的保護，避免其受到外來的人為或環境因素破壞。而隨著遠端存取機制的出現，與電腦接觸的人變多了，在人員安全上的發展日趨重要，為了因應越來越多的人存取電腦資訊的情況，許多辨識相關的技術開始發展，如早期的帳密系統、磁卡，發展至今的晶片卡、生物辨識等等，都是為了驗證使用者是否有

資格能夠存取資訊。在網路的出現及普及之後，已經成為企業與外界接觸的重要管道，無可避免地企業的資訊在網路中傳遞也產生了相對的資訊安全風險，也出現了許多利用網路特性的攻擊手法，於是相對應的防禦技術也隨之出現，像是一些用於資訊傳輸的加解密技術以及控管網路邊界的防火牆(Axelrod, 2004)。

雖然企業使用了資訊安全的技術來保護所擁有的資訊，但是資安事件仍然頻傳不窮，這揭露了資訊安全不只是單純的技術問題，而是包含了人員、管理及流程各方面的考量，現今的企業必須作整體的資訊安全規劃，將資訊安全融入企業經營管理的一部份(Zafar & Clark, 2009)。本研究借用 IBM 提出的資訊安全能力參考模型來體現目前的企業在規劃自己的資訊安全架構時需要考量到哪些面向(IBM, 2006)。

表 2–1 ：資訊安全能力參考模型 (修改自 IBM, 2006)

Security Theme	Assessment of Security Themes
Governance	Strategy and Information Security Policy Security Compliance Security Risk Management Governance Structure Information Security Advisory
Privacy	Policy, Practices and Controls Privacy and Information Management Strategy Data, Rules and Objects
Threat Mitigation	Network Segmentation and Boundary Protection Vulnerability Management Content Checking Incident Management
Transaction and Data Integrity	Business Process Transaction Security Database Security Security Storage Message protection System Integrity
Identity and Access	Identity Proofing

Management	Access and Identity life Cycle Management
Application Security	System Development Life Cycle Application Development Environment
Physical Security	Site Security Physical Asset Management
Perseonnel Security	Workforce Security

在公司治理方面，強調的是企業需要擁有健全的資訊安全管理架構，意即企業在資安政策、資安程序上必須有良好完善的規範，Lockman(1984)等學者對於大型的金融資訊系統引入了內部控管的觀念，強調系統在設計時必須納入驗證機制的考量，使得電腦產出的結果能夠符合規範，以確保審計程序的安全性，而Straub(1990)等學者也建議企業在針對電腦侵權濫用事件的偵測及處理上需要有一個良好的管理程序，Backhouse(1996)等學者認為透過分析企業結構中責任的範圍歸屬能夠幫助發展企業的資訊系統安全，von Solms(1994)等學者提及資訊安全管理涉及許多面向，包含了資安政策、風險分析及管理、災後復原等等，並提出了一個資訊安全管理的模型來協助企業評估本身資訊安全的架構。

在隱私的部份，考慮的是企業如何保護及管理內部或外部流通的資訊，避免遭受到惡意的取用，Cattela(1981)將資訊視為企業資產的一部份，認為企業內的資訊必須要妥善的保護以及控管其使用權限，以確保企業的隱私安全，而 Shim(2007)等學者在探討人們使用無線科技來傳輸資訊的同時，也提出了必須要考量資訊的隱私及安全的概念，這說明了隨著科技的進步，企業或人們使用資訊的方式改變，資訊流通的範圍也急劇的擴張，在思考如何保護資訊隱私及安全的時候，必須要有更完整周延的考量。

而在降低威脅這個領域，則包含了弱點偵測、事故管理、網路邊界管理等議

題，旨在預防資安事故發生及減輕事故所帶來之衝擊，Siponen(2006)等學者提出了一個發展安全的資訊系統的方法，並且定義了一些設計流程的準則及需求。關於確保交易及資料的完整性方面，主要的任務是保護交易過程的安全，從存放資料的資料庫、交易使用的系統、中間訊息傳遞的保護、到最後正確完善的儲存資料，中間的每一個環節都必須確保其安全完整，如 Bussolati(1981)等學者提出了一個多層次的邏輯安全架構，用來管理分散式的資料以及分散式系統，而 Lee(2003)也嘗試著識別出在發展安全的網路基礎資訊系統時，哪些議題需要被考量以及哪些問題需要解決，Yang(2004)等學者則是針對無線傳輸的應用探討其在科技、商業及社會各方面的議題，並且檢驗了無線傳輸的安全性。

身份及存取管理則是著重於身份的驗證，並且確保未經授權的人無法取得資料而經過授權的人可以安全的存取資料，Boukhonine(2005)等學者認為生物科技能夠應用於身份的辨識，與傳統科技相較之下能夠提供更佳的安全性，Zviran(2006)等學者則比較了多種的身份驗證機制，但是認為目前尚未有完美的單一解決方案，並期望未來能夠繼續研發更加精密、而在使用上及建置上更加便利的機制。在應用程式安全這部份，則包括了系統開發生命週期的管理、安全的程式撰寫實務管理、程式碼的安全性檢驗等等，如 Sumner(1986)驗證了不同的使用者是如何決定系統開發的方式，以及分辨其選擇的特徵。

實體安全講求保護組織實體的設備的安全，包括了廠房、資料儲存中心等等，避免遭受人為或者天災的危害，Duffy(1980)透過案例來陳述一個電腦中心該如何規劃來預防災害的發生，包括了災前的保險、軟硬體的備援、災後的復原等等。人員安全則包含了人力的安全以及員工的教育訓練，D'Arcy(2007)等學者試圖從電腦的使用者中調查資訊安全政策、教育訓練的成效，以及電腦監控對於阻止電腦侵權濫用的效果。

透過此資訊安全模型，我們可以充分的了解資訊安全包含了多元的面向，企業在規劃資訊安全業務之時必須作全盤的考量，不論是資安架構、作業程序、科技應用、管理政策、人員等等，都必須要納入考慮，並且缺一不可，因為資訊安全的強度是取決於其中最弱的一環。此外，我們也可以發現，想要充分的做好資訊安全防護，對於企業而言是很困難的，因為牽涉的層面太廣、複雜性太高，企業很難單獨依靠自身的力量來完成。

2.1.3 資訊安全未來發展方向

隨著資訊科技的迅速發展，透過電腦及網路與外界連結，已經成為了企業必備的能力，而資訊安全問題的重要性也日漸提昇，而資訊科技從 1970 年代發展至今，也歷經了許多不同階段的演變，在這期間也有許多相關的資訊安全研究被發表出來，但是從整體的資訊安全觀點看來，仍然有許多的不足需要被重視以及改進。

Siponen(2007)的研究指出，過往的資訊安全研究多集中於技術面的討論，而其中以存取資訊系統的安全問題及通訊安全這兩大類的主題受到最多的關注與探討，研究中也發現大多數的研究是使用數學或者邏輯的來作為研究的方法，這樣過度聚焦於科技的情況，並無法完全解決資訊安全的問題，因為大多數的資訊安全議題是相當複雜的，牽涉到了科技、人員、管理流程等等，研究者往往只發展了技術上的解決方法，但是在管理方面卻無法同步跟上，而且在探討人員相關的社會議題研究所佔的比例極低，關於人們在資訊安全中扮演如此重要的角色，但是探討的文章極少，實在是一種警戒。此外大多數的資訊安全研究缺乏理論的支持，而在少數有包含理論的研究中又以數學方面的理論為大宗，這更明顯的暴露

出在資訊安全的相關理論這塊領域，長期的發展並不完整。而研究也顯示某個特定領域的學者通常不太注意其他領域的發展，這造成了資訊安全的發展出現了分裂，並且與外界的連結性不足，很少有研究是利用其他學科的理論作為參考來解決問題，像是透過心理學、社會學、哲學等等(MT Siponen & Oinas-Kukkonen, 2007)。

由之前的文獻分析顯示資安研究主要集中於技術議題，並且多是使用數學、邏輯做為研究的方法，所以學者也建議之後的研究多往資訊系統的安全及資訊安全管理的議題作為發展方向，利用適當的理論作為參考，像是往心理學、社會學、哲學方向尋找是否有互通或者能夠連結的理論(Zviran & Erlich, 2006)，透過這種理論創造或是理論驗證等方法，將理論與實證作強而有力的連結，能夠使得資訊安全的研究發展更加的完整健全而且使人信服。

第二節　委外服務

委外是一種程序，透過公司或是一個商業實體分包契約給第三方供應商來完成某些服務，或是提供某些設備給公司內部人員使用(Gilbert, 1993)。若將委外的概念更為廣泛的來思考，任何一個公司價值鏈上的活動，包括其所需的人員等等，都可以視為一個可由外部購得的服務(Quinn, 1992)。

2.2.1 資訊系統委外

資訊系統的委外基本上可以視為組織將其部份或全部的資訊系統功能，交給外部專業的服務提供者來完成(Grover, Joong Cheon, & Teng, 1994)。然而自從柯達公司在 1989 年將其資訊系統委外之後，資訊系統的委外市場開始蓬勃興起並成為

一種可能的策略方向，在近數十年以來，資訊系統委外歷經了許多階段的演變，從早期 1960 年代開始，資訊系統委外主要是集中在硬體設施上面，因為當時的電腦體積龐大又昂貴，企業向外尋求專業電腦廠商的協助，以因應內部流程需求，而外部的供應商以提供專業服務及設備管理等服務為主，到了 1970 年代，企業在資訊科技應用上的需求增加但是人才卻不足以勝任，所以與外部服務供應商透過簽約的方式來發展企業內所需的軟體，這個時期資訊系統委外的業務是以提供標準的套裝應用軟體為主流，接著 1980 年代，大型電腦開始式微，取而代之的是小型的個人電腦，這時的資訊系統需求開始專注於一些客製化的軟體，能夠幫助企業整合其作業生產流程，所以委外服務的主流為幫助客戶建構能夠支援其業務流程的客製化資訊系統，而在 1990 年代，隨著網路的興起，企業開始有了要把遍佈各地的業務連結在一起的需求，所以資訊系統委外的趨勢也朝著提供整體解決方案的方向發展，包括了網路與通訊管理、分散式系統整合、系統操作的教育訓練等，往複雜較高之委外服務項目前進。而由這段歷史的進程可以發現由早期的委外服務供應商單純提供系統或軟體的服務，演變到後來的客製化軟體、網路建置、系統整合、教育訓練等等，服務商與企業主的關係越來越密切，現在的許多服務需要長期的合作並且保持良好的合作關係，或者是供應商需要派人到企業內部作顧問諮詢的工作等等，而隨著委外現象的出現，資訊科技的人才也出現由企業轉向供應商集中的趨勢，因為在委外的情況下企業無須擁有大量的人才來自行開發所需的資訊系統，反而是供應商必須具備大量專業資訊人才來因應各種不同企業的需求(J. Lee, Huynh, Kwok, & Pi, 2003)。

在資訊系統委外這方面的議題已經有許多的學者加以探討，學者(Richmond & Seidmann, 1993)提出讓組織以外的單位以簽約的方式接手，負責組織內部份或全部的資訊系統活動，而演變到了後來有學者(McFarlan & Nolan, 1995)開始將資訊系統委外視為策略聯盟之互助合作模式，而也有學者(Alpar & Saharia, 1995)也

提到委外通常會維持一段中長期的契約關係，在合約期限內服務供應商持續的提供客戶不同的資訊服務，可見得企業與委外廠商之間的關係變得越來越密切且重要。

而在委外的範圍方面，學者(Due, 1992)提出了將基本的資料處理、軟硬體、網路委外的作法，之後拓展到企業使用的資訊系統及通信功能(Minoli, 1995)，接著演變成將多樣的資訊系統功能，如應用系統開發及維護、網路通訊管理、資訊中心管理等等，轉由外部服務供應商來完成(Grover, Cheon, & Teng, 1996)，經過不斷地演變發展，委外的項目可概略分為資產委外及服務委外兩大類，資產委外指的是軟、硬體及人員的委外，服務委外指的是系統開發、系統整合、系統管理等服務(J. Lee & Kim, 1999)。

Lee(2003)等學者認為現今的委外合約已經越來越複雜，不論是委外的範圍或者是深度都已經比過往的合約大上許多，通常很難在合約上考慮到所有可能發生的情況，也就是說往往在合約簽訂之後還會有許多修改的動作，而在這樣的情況下想要達到預期的委外效果,企業與服務供應商之間的關係就扮演著重要的角色,也因此在未來資訊系統委外的合作方式，可能會以一種夥伴基礎的方式存在，企業與服務的供應商不在只是單純的考慮自身能夠獲得的經濟利益或者是策略優勢，而是從一個整合的觀點來考慮資訊系統委外，同時從經濟、社會、策略三個構面來考慮，在企業與服務供應商之間建立緊密的夥伴關係，服務供應商可能會開始分擔企業的風險及責任，甚至成為客戶的利害關係人，在這種彼此互信的情況下所建立起的合作夥伴關係可以帶來競爭上的優勢，達成雙贏的局面。

第三節 資訊安全委外

2.3.1 資訊安全委外概述

在這個電子商務的時代,幾乎所有的企業都透過網路與外部的供應商、客戶、遠端的使用者有所聯繫，然而伴隨而來的安全威脅也一一浮現，攻擊者可以透過多樣化的手法達到攻擊的目的，不過企業卻可能因為遭受單一的攻擊便使得營運中斷，而不論企業的規模大小，大多數的企業都沒有足夠的資源、專業技術、人力及時間來鞏固自己的資訊安全，而這樣的情況促使了資訊安全管理服務業的興起(Deshpande, 2005)。資訊安全的委外議題在近幾年來逐漸受到重視，如同先前提到的對於企業來說資安風險逐漸的升高，市場上也出現了越來越多的資安服務供應商，資安委外的情況也越來越頻繁。

本研究利用上述提及的資訊安全的定義及委外的概念，將資訊安全委外定義為：組織將部份或全部的資訊安全功能需求，分包契約給第三方服務供應商來完成。而主要的資訊安全服務可以大略的被分類為以下幾項(Deshpande, 2005; Hunt, 2001)：

一、資訊系統及網路的週邊管理：此服務考慮企業的資訊在與外界連通時所需具備的基本保護，如建置防火牆、入侵偵測系統、入侵防堵系統等等，並且由外部廠商負責軟硬體的管理與維護。

二、安全管理監控：這種監控通常需要長期不間斷的觀察，服務商透過監看客戶的網路流量或者網路的使用行為模式，找出異常的使用情況或者是辨認出來自外界的蓄意攻擊，如駭客入侵、阻斷服務(DoS)等行為，此外也可以針對客戶的使用情況做出未來趨勢的判斷，而這也是回應意外事件流程的第一步。

三、弱點評估與滲透測試：這個服務旨在模擬駭客的行為找出客戶的系統可

能存在的弱點，在遭受攻擊之前先設法改善系統或網路設置的缺失及漏洞，並且需要週期性的掃描測試，以確保客戶有能力因應新的攻擊手法或者是新上線的系統也受到良好的保護。

四、現場顧問諮詢：服務供應商需要幫助客戶評估企業的風險，在了解企業的需求之後協助發展資訊安全管理的政策及程序，建構良好的資訊安全架構，當然也包括技術上及操作時的協助，像是提供資訊安全產品，或者是在資安事件發生時給予回應，辨識原因及協助回復。

五、遵循管理的監控：這個服務監看公司內部人員是否有不符合資訊安全規範的行為，像是未經授權的變更系統內的資料、改變防火牆的設定等等，當有違規的紀錄產生便會發出通報警訊。

六、防毒與內容過濾：此服務包含了偵測所有的病毒、蠕蟲、惡意程式、垃圾郵件等等，並且進行有效的過濾防堵，避免危害企業內部的系統安全。

2.3.2 資安委外與競爭優勢

為了探究資安委外是否能夠為企業帶來實際的利益以及獲得競爭上的優勢，我們在此先借用資源基礎的概念，以便能夠更清楚的描述兩者之間的關係，而詳細的理論探討將會留到下一個章節來作介紹。

Grant 認為資源基礎的概念，不只關乎公司現有資源及能力的佈署，也與其未來的發展有關，為了利用公司現有的資源及能力，並且進一步發展競爭優勢，從外部獲取互補及不足的資源也是相當重要的(Grant, 1991)。而從外部獲取資源或能力，也就是透過委外的手段，是一個在策略管理領域常用的填補資源及能力與欲發展的策略其中落差(gap)的方法(Stevenson, 1976)。

如先前所言，資訊安全也可以視為公司所需要的一種資源及能力，但是如同 IT 一樣，雖然是公司必須具備的能力，但卻不是大多數公司的核心競爭力來源 (Carr, 2003a)，此外資安的建置比一般的 IT 更為困難，且需要耗費更大的成本 (Bruder, 2006)，因此，本研究考慮資安可以如同 IT 一樣，當公司現有的需求資源及能力與期望的程度有所落差(gap)，可以用委外策略來填補這個不足(Cheon, Grover, & Teng, 1995; Cronk & Sharp, 1995)。

Grant 也說明了委外的策略不但可以維持公司所需的資源及能力，同時也增強了公司的競爭優勢，並且有更佳的策略機會(Grant, 1991)。Kankanhalli 等學者也提到投資於資安管理能夠幫助企業獲得競爭優勢，而若將資安委外，將企業需要的資安服務交由專業的服務供應商來執行，則可能帶來更大的利益(Kankanhalli, Teo, Tan, & Wei, 2003)。

此外，Mishra 認為因為資訊的不對稱，賣家擁有比買家更多的資訊，而買家沒有足夠的判斷能力來辨別賣家的好壞，可能產生檸檬問題(lemons problem)，也就是說劣質的賣家提供了較差的產品或服務，也因此付出了較低的成本；而優質的賣家提供了較好的產品或服務，因此需要較高的成本，造成其要求的價格比劣質的賣家來的高，而買家在無法判斷的情況下，選擇了收費較低的劣質賣家，造成市場往劣質賣家傾斜的情況，而想要解決這類的問題，需要仰賴服務供應商提供訊號(signal)及認證(certification)，也就是賣家必須提供一些訊息或保證來證明自己產品或服務的品質，讓客戶能夠更容易的作出較好的選擇，而在資訊安全上也有類似的情況，如果企業在考慮資訊安全委外之時，能夠選擇較為著名的專業服務提供者，亦即提供了訊號(signal)讓客戶信任企業在資訊安全這方面能夠擁有較高的資訊安全能力，或者擁有較好的形象，則能夠增加客戶的信心，進一步提昇與企業合作的意願，也能夠為企業本身帶來更多的機會，以及創造出競爭優勢

(Mishra, 2006)。

儘管上述有許多的學者提出了相關的研究建議，但是我們的調查發現在學術界中關於資安委外的文章仍然極為稀少，我們搜尋了數個資管及資安領域的主要期刊，幾乎沒有資安委外的相關研究出現，另外我們也透過電子的資料庫來搜尋，在得出的結果當中，跟資安委外有關的幾乎都是短篇的雜誌文章，極少有完整的學術研究，大多數的文章仍然在探討委外的安全問題，這顯示出目前在資安委外這塊領域的學術研究有著嚴重的不足，對於正在成長的資安委外市場而言，是個必須要重視的警訊並且需要尋求解決之道。

因此，本研究主旨在於利用在探討競爭優勢時被廣泛使用的資源基礎理論為基礎，將資訊安全視為公司的一種資源及能力，探討公司在資安能力與預期達到的能力有所落差的情況下，透過委外的策略將資訊安全委託給外在的服務供應商，是否能夠為公司帶來更好的效益，並且取得競爭上的優勢。

第三章　理論架構與研究方法

第一節　資源基礎理論

3.1.1　資源基礎理論發展

資源基礎理論(Resource-Based Theory；RBT)將公司視為一些資源的組合，是一個由內部的觀點來分析，探討公司如何利用本身的資源條件來因應外部市場環境的需求變化，Penrose 最早提出將公司視為一些資源組合的概念，並將資源視為影響公司的重要因素，他認為公司必須擁有資源以及有效運用資源的能力才能夠為公司獲取利潤(Penrose, 1959)。Rubin 將資源定義為一個固定的輸入，讓公司能夠達成特定的工作(Rubin, 1973)。

Wernerfelt 根據 Penrose 的概念，透過資源基礎的觀點來看待公司的活動，他認為資源與產品兩者的關係是密不可分的就如同硬幣的兩面，在劃定公司的目標產品市場的大小的前提下，可以了解需要多少的資源來達成；而相對地，在確定公司擁有多少資源的情況下，可以找到對於目標市場最佳的活動規劃。Wernerfelt 也談到利用公司所擁有的資源能夠在多個產品市場形成資源位置的障礙，藉由先佔優勢的概念保護其擁有的資源並且較為有效的運用，使得其他後進的競爭者無法取得資源或者提供相同的產品，進而維持競爭上的長期優勢(Wernerfelt, 1984)。而 Rumelt 等學者也有類似的看法，認為資源在公司成長與發展競爭優勢上扮演了重要的角色，意即根據資源基礎的概念，公司的競爭地位取決於公司獲取資源的能力，以及保護獨特資源的能力(Barney, 1986; Conner, 1991; Rumelt, 1974)。

Dierickx & Cool 認為如果一個公司所擁有的資源不對稱的分佈在同個產業的不同公司中，並且這些資源都難以模仿及取代，那麼此公司能夠實行的競爭策略是其他公司無法構想及實行的，因為他們無法獲取相同的資源，當然此論點假設公司擁有足夠的資源並且能夠有效的利用他們來達成策略上的目標(Dierickx & Cool, 1989)。

Barney 認為一個公司的資源，包括了所有由公司所控制以及驅使公司能夠建構及實行策略來改善其工作效率的因素，例如公司的運作流程、資訊與知識、文化、信用等等(Barney, 1991)。而許多學者也提出了相似的概念，指出資源能夠幫公司實行許多的策略活動，並增進工作的效率及效果(Hitt & Ireland, 1986; Thompson & Strickland, 1983)。接著 Barney 更進一步的指出，資源要能夠提供長久的競爭優勢必須要有價值性(value)、稀少性(rareness)、不可模仿性(imperfect immutability)、及不可替代性(nonsubstitutability)等特性，價值性表示資源能夠在公司實行策略活動時,增進其效率與效果。稀少性則強調外在競爭者沒有的資源，或者當擁有有價值的資源的公司少於有此需求的公司。不可模仿性則體現在三個方面，當企業的競爭優勢是源自其時空背景的努力累積(獨特性)，或者資源與競爭優勢的創造過程無法釐清(模糊性)，抑或是其創造的過程無法模仿(複雜性)，都能夠成為創造競爭優勢的潛力。不可替代性是指無法以相似的資源執行同樣的策略來達到替代的效果，使得競爭者無法模仿。而在擁有這些特點之後，如果加以累積、培養，就有潛力能夠創造出持久的競爭優勢。

Peteraf 提出在利用資源基礎觀點在探討公司在獲取競爭優勢時,有四個條件必須同時被滿足,資源的異質性(resource heterogeneity)、不完整的移動性(imperfect resource mobility)、事前阻隔競爭(ex ante limits to competition)、以及事後阻隔競爭(ex post limits to competition)，異質性代表著公司能利用較好的資源在生產時降低

成本或者利用其獨特性提供其他公司無法給予的服務，不完整的移動性確保公司裡具有價值的資源無法被輕易的轉移或者被外界所獲取，事前阻隔競爭重視公司在利用資源實行策略之前必須先考量成本，以避免耗費過多成本卻得不到足夠的利潤，事後阻隔競爭強調的公司必須保護自己在競爭中所取得的利潤，避免被其他公司所侵蝕(Peteraf, 1993)。

而對於諸多學者在探討資源理論議題時，所共同面臨的挑戰就是對資源的定義，而究竟要如何來定義資源，有許多學者提出了不同的看法。Barney 將資源概分成三個類別，分別為實體資本資源，包含實際的廠房設備、實體技術、地理位置、原料取得方式等等；人力資本資源，像是員工的訓練、經驗、判斷、智慧、關係；組織資本資源，包括組織的架構、組織的規劃、控制及協調系統、還有組織內部的非正式團體等等。Sanchez 等學者將資源定義成那些對於公司有價值、能夠偵測及回應市場變化的機會及威脅的資產(asset)及能力(capability)，資產被視為可以幫助創造或生產產品的任何有形或無形的東西，而能力可以解釋為可重複執行的創造或生產產品的行為模式(Sanchez, Heene, & Thomas, 1996)。而針對了這部份的論述，有學者做了更完整的補充，資產可以是產品的輸入抑或是生產流程的輸出，而出現的型式可能為實體的硬體設備、網路基礎設施，或者非實體的軟體專利、與客戶的關係(Srivastava, Shervani, & Fahey, 1998)。而能力則將輸入轉換成更有價值的東西，包含了技術或者是管理的技巧及流程，系統的發展整合等等(Amit & Schoemaker, 1993; Sanchez, et al., 1996; Wade & Hulland, 2004)。

3.1.2 資源理論相關應用

利用資源基礎的觀點來探討公司的競爭策略已經日趨普遍，也有許多的學者透過此觀點發展資訊系統的研究，本研究將進一步探討資源理論與委外的議題。

關於資源基礎觀點與委外的議題，Duncan 提出了利用資源理論觀點來評估委外風險的論述，他認為因為現今科技變動快速，所以與資訊科技有關的資源的變動也非常的快速，可能現在盛行的資源或科技在新的技術出現之後，就忽然失去了原有的價值，所以這類資訊科技相關的資源相當難以掌握控制。而相同的資源帶給不同的公司的競爭價值也不同，Duncan 認為這點是利用資源基礎觀點在探討資訊科技委外時相當重要的認知，資源的價值會隨著與其他資源的不同組合對於不同的企業產生異質性的效果，而若想要了解哪些資源具有潛力，會對公司的未來產生有利的策略機會，則公司必須要具備對資源足夠的認知與知識、對資源能有效的控制、足夠的學習能力，才能夠辨認出此資源尚未被發掘的潛力，並且擁有能夠轉化成為策略機會的實力(Duncan, 1998)。

而 Roy 等學者也嘗試操作資源基礎理論的架構來應用在資訊系統委外的研究領域中，他考慮公司現有的合適資源與其策略價值，依其高低分為 Outsourcing、Conservation、Recuperate、Partnership 四個種類，並分別探討不同的資訊系統適合的來源取得模式，當中也提及當資訊系統的策略價值不高、現有的資源也不多的情況下，應該先考慮委外。此研究認為資源基礎理論提供了一個互補性的觀點來看待委外，讓我們能夠建構一個模型來研究資訊系統取得的方式，進而可以分析資源的取得及他們的策略價值，作為公司發展資訊系統的重要參考(Roy & Aubert, 2000)。

3.1.3 資源理論與競爭優勢

如之前所述，自從資源基礎觀點開始發展以來，許多研究者都試圖探討其與競爭優勢之間的關係，但是關於該如何準確的衡量到競爭優勢，實際上存在的許多難處。

Grant 提到資源是企業獲利能力的基礎，而影響公司獲取利潤的能力之因素主要有兩者，其一是企業所在的產業之吸引力，另一個是競爭優勢的建立，前者受到的是大環境的影響，在此不多加討論，而我們關注的是後者，也就是聚焦在同產業內的競爭，Grant 認為考量成本上的優勢以及差異化的優勢，能夠為企業在執行策略、尋求自己的資源定位時，提供選擇的依據，而透過這些企業在運用自己的資源及能力所創造出的成本優勢及差異化優勢，則可以為企業帶來競爭上的優勢(Grant, 1991)。

Roy 認為要衡量資源為公司帶來了何種價值，可以透過資源在公司活動中提供了哪些價值或者透過這些活動生產出了哪些產品來判斷，而要探討資源是否能夠為企業帶來競爭優勢則必須觀察這些資源在生產活動中的加值表現是否能夠為企業減輕威脅或者是能夠幫助企業探索新的機會，能夠增進作業的效率或者提供在生產活動間一些重要的輔助。而資源為企業帶來的競爭優勢有時不是能夠被明顯的察覺，而這時就需要有一些替代的衡量方式來幫助辨別，利用一些較為客觀的指標來作為判斷資源是否能夠帶來價值的依據(Roy & Aubert, 2000)。

第二節　研究架構

總和上述所言，經由委外的觀點來看，當公司現有的資源與期望的程度有所落差時，可以利用委外的策略來達成需求(Cheon, et al., 1995; Cronk & Sharp, 1995)，並透過這樣的委外策略能夠獲取競爭上的優勢(Kankanhalli, et al., 2003)。而經由資源基礎的觀點來探討，將資訊安全視為公司的一種資源，透過資源的有效利用可以為公司獲取利潤，並達成競爭上的優勢(Grant, 1991; Rumelt, 1974)。

本研究融合以上的觀點，利用資源基礎的觀點為基礎，將資訊安全視為公司的一種資源及能力，推論公司在資安能力與預期達到的能力有所落差的情況下，透過委外的策略將資訊安全委託給外在的服務供應商，將能夠為公司帶來更好的效益，並且取得競爭上的優勢。

關於將資訊安全視為公司資源的部份，本研究借用 Wade 等學者的架構，並將其延伸至資訊安全上，將資訊安全的資源分成資產以及能力兩部份，分別定義如下(Amit & Schoemaker, 1993; Sanchez, et al., 1996; Wade & Hulland, 2004)：

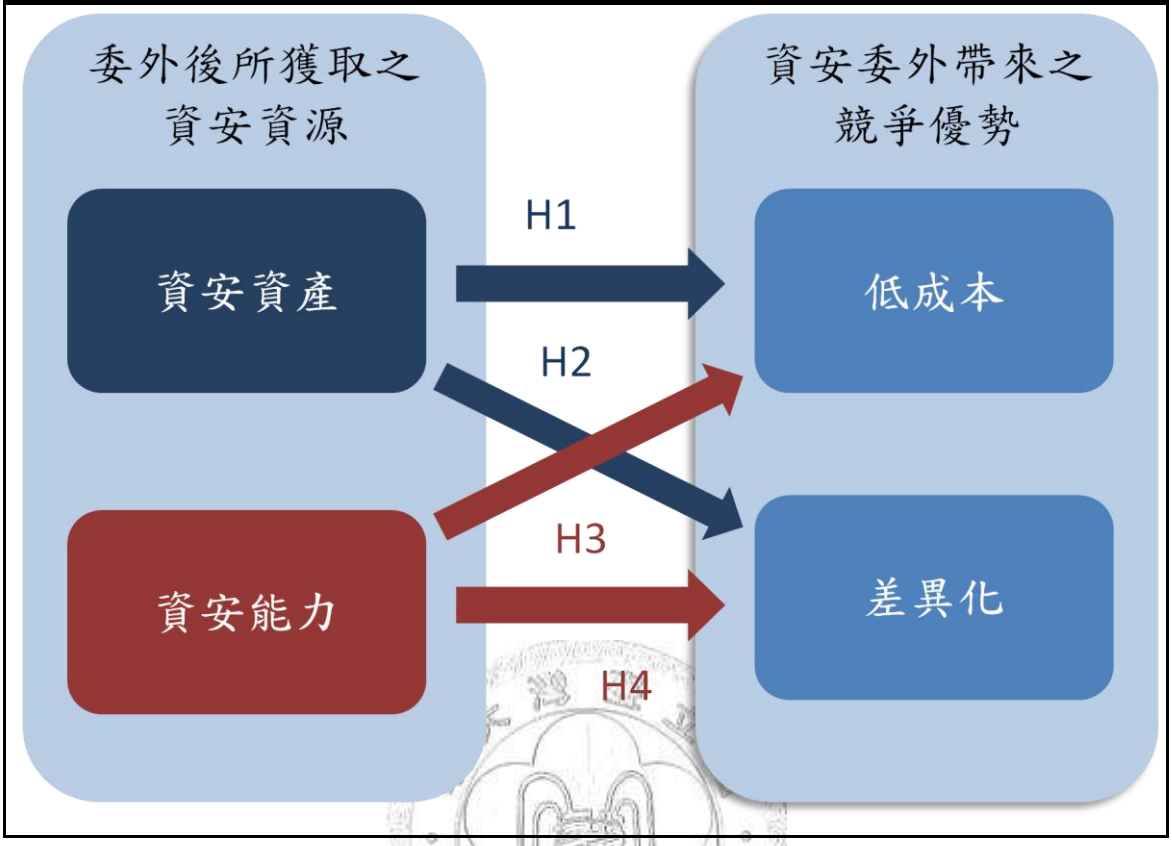
一、資訊安全資產：公司內能夠幫助公司擁有或者提升資訊安全任何有形或無形的東西，主要包括了資訊安全基礎建設、與合作夥伴的關係、與外部環境的關係。

二、資訊安全能力：公司內能夠重複執行來幫助公司擁有或者提升資訊安全任何行為模式，主要包括了資訊安全技術能力、資訊安全管理能力、回應外部變化的能力。

而在競爭優勢的衡量方面，本研究參考 Grant(1991)提出的概念，並且從資訊安全的觀點來考量，將成本優勢定義為企業能夠利用較低的成本來達成相同的資訊安全效果，或者是在花費相同成本的情況下，獲得比其他企業更加優越或者更有效率的資訊安全資源。而在差異化優勢的部份，則定義為企業與其他企業相比較擁有較佳的資訊安全資源，或者與外在環境有較好的關係，使得企業在執行競爭活動時能夠佔據較為優越的地位。

歸納上述推論，提出了本研究的架構，如圖 3-1：

圖 3－1 ：研究模型



第三節　研究假設

延續之前的討論，我們得知委外後所擁有的資訊安全資源，會對於公司的競爭優勢產生影響。利用上述所提，我們將資訊安全資源劃分為資產與能力兩部份(Amit & Schoemaker, 1993; Sanchez, et al., 1996; Wade & Hulland, 2004)，首先討論關於資訊安全的資產這部份，在企業將資訊安全委外之後，會從服務供應商接觸或者獲取資訊安全的資產，諸如有形的資訊安全的基礎建設，以及無形的與外部服務商的關係、與外部市場環境的關係等等(Grover, et al., 1996)，我們透過學者Grant(1991)的觀點將這些委外所獲得的資安資產視為企業的資源，而這些資產會對於企業在執行策略時產生成本上以及差異化的優勢，意即企業在將資訊安全委外之後能夠花費較少的成本來取得同樣的資產，並且能夠產生有別於其他企業的

差異化成果或行為，使得在雙方競爭時佔有優勢(Kankanhalli, et al., 2003)，據此我們給出下列兩個假設：

H1：企業將資訊安全委外後所獲得的資訊安全資產將正面影響企業的成本優勢。

H2：企業將資訊安全委外後所獲得的資訊安全資產將正面影響企業的差異化優勢。

而另一部份，在企業將資訊安全委外之後，企業會獲取資訊安全的能力，包含了資訊安全的技術能力、管理資訊安全的能力、回應外部變化的能力等等(Aral & Weill, 2007)，我們也將這些透過委外所獲取之資安能力視為企業所擁有的資源(Grant, 1991)，而有效的運用這些資安能力可以幫助企業在執行資訊安全活動時花費較少的成本來達成所需的效果，並且透過這些能力來與其他企業做出區別，在競爭時透過差異化的效果來產生競爭上的優勢(Grant, 1991; Kankanhalli, et al., 2003)，因此我們給出下列兩個假設：

H3：企業將資訊安全委外後所獲得的資訊安全能力將正面影響企業的成本優勢。

H4：企業將資訊安全委外後所獲得的資訊安全能力將正面影響企業的差異化優勢。

第四節 變項之衡量

本研究的研究變項包含了資訊安全資產、資訊安全能力、低成本的競爭優勢及差異化的競爭優勢，下面將詳述這些變項的衡量方式。

3.4.1 資訊安全資產

如上述所言，資訊安全資產為公司內能夠幫助公司擁有或者提升資訊安全任何有形或無形的東西，主要包括了資訊安全基礎建設、與合作夥伴的關係、與外部環境的關係(Sanchez, et al., 1996)。而我們進一步的參考了 Wade & Hulland(2004)的文章中所使用的資訊系統資源架構，來建構出資訊安全委外的資產構面，另外我們也引用了 Grover(1996)文章裡的問項，來衡量資訊安全委外廠商的服務品質以及夥伴關係。

表 3－1 ：資安資產構面之衡量變項

構面	衡量問項	編碼
資訊安全資產	1. 透過委外，本公司能使用或擁有新穎的資訊安全軟、硬體設備	ISA_1
	2. 透過委外，本公司能使用或擁有安全的傳輸及儲存設備	ISA_2
	3. 資訊安全委外廠商在本公司遇到問題時，有熱心的協助解決	ISA_3
	4. 資訊安全委外廠商所承諾過會完成的事項，有準時完成	ISA_4
	5. 資訊安全委外廠商所派遣的工作人員，看起來具有專業形象	ISA_5
	6. 委外廠商若遇到任何事先未預期的問題，會儘快告知，以共謀對策	ISA_6
	7. 根據過去及現在的經驗，本公司與委外廠商互信程度非常高	ISA_7
	8. 本公司與委外組織共事，是件很高興的事	ISA_8

3.4.2 資訊安全能力

而在資訊安全能力這部份，強調的是公司內能夠重複執行來幫助公司擁有或者提升資訊安全任何行為模式，主要包括了資訊安全技術能力、資訊安全管理能力、回應外部變化的能力。回顧過去的文獻，大部分都只討論關於資訊科技的能力，鮮少看到將其套用在資訊安全上面，故本部份的問項主要參考自 Aral & Weill(2007)、Wade & Hulland(2004)以及 Zafar & Clark(2009)的文章中的概念，並由經過修改而成。

表 3－2 ：資安能力構面之衡量變項

構面	衡量問項	編碼
資訊安全能力	1.透過委外，本公司擁有使用最新資訊安全科技的能力	ISC_1
	2.透過委外，本公司能夠使用或擁有因應新的攻擊手法之技術	ISC_2
	3. 透過委外，本公司能夠保護所使用的資訊系統的安全	ISC_3
	4. 本公司擁有良好的資訊安全架構	ISC_4
	5. 本公司擁有完整的資訊安全政策、程序及規範	ISC_5
	6. 本公司的員工擁有良好的資訊安全素養	ISC_6
	7. 透過委外，本公司能夠擁有安全監控的能力	ISC_7
	8. 當資安意外發生時，本公司能夠辨識出原因	ISC_8
	9. 當資安意外發生時，本公司能夠做出回應、排除事件	ISC_9

3.4.3 低成本競爭優勢

低成本是在論述競爭優勢時很常被提及的概念，在 Sethi(1994)等學者的文章裡面提及，低成本代表在生產的過程中能夠以較低的花費來完成產品，亦即在整個製造的流程中，比其他競爭對手更加的有效率，而這種效率越高，企業就越容易在成本上產生相對的優勢。而在 Krell(2009)等學者的文章中，也利用了降低成本的概念來衡量企業在受法規影響時，其資訊科技投資是否能夠帶來競爭優勢。雖然上述的文獻都有討論到關於低成本所帶來的競爭優勢，但是其主題都是圍繞在資訊科技的相關應用，與本研究所探討的資訊安全有些許的不同，故本研究參考了上述 Sethi(1994)及 Krell(2009)的文獻，並且做了一些修改使其更符合我們所欲測量的概念。

表 3－3 ：低成本競爭優勢構面之衡量變項

構面	衡量問項	編碼
低成本	1.用以維持公司資訊安全之人力成本	LC_1
	2.管理各項資訊安全活動之成本	LC_2
	3. 獲取各項資訊安全科技之成本	LC_3
	4. 公司內各部門與資訊安全部門之溝通協調成本	LC_4

3.4.4 差異化競爭優勢

根據 Grant(1991)的文章提及，差異化的優勢可能來自於品牌名聲、獨特的科技、廣大的服務網路，當企業擁有了與其他企業的區隔，並且可以因此吸引客戶的注意，便能夠在競爭之中佔據有利的地位。本研究參考了 Grover(1996)等學者對於委外成功的衡量變項，將其修改成為較符合資訊安全委外的情況，以及

Zhou(2009)等學者對於競爭優勢的衡量問項，並且加入與其他競爭者互相比較的情況，試圖用一個較為整體的角度來衡量，從內部的能力以及企業與外界的關係來判斷差異化的情況。

表 3－4 ：差異化競爭優勢構面之衡量變項

構面	衡量問項	編碼
差異化	1. 相較於其他競爭者，本公司更能夠接觸或獲取最新的資訊安全資源	DIF_1
	2. 相較於其他競爭者，本公司對於資訊安全資源的使用更有效率	DIF_2
	3. 相較於其他競爭者，本公司更能夠重新聚焦於核心業務	DIF_3
	4. 相較於其他競爭者，本公司與資安委外廠商的合作帶來了較好的聲譽	DIF_4
	5. 相較於其他競爭者，本公司提供給客戶更安全的服務感受	DIF_5
	6. 其他競爭者很難達成本公司將資訊安全委外所帶來的效益	DIF_6
	7. 其他競爭者很難複製本公司的資訊委外經驗	DIF_7
	8. 其他競爭者很難複製本公司的品牌聲譽	DIF_8

第五節　測量方法

3.5.1 問卷設計

本研究之問卷項目如附錄所示，主要包含資訊安全資產、資訊安全能力、低成本競爭優勢與差異化競爭優勢，共二十九個問項，問項皆以 Likert 七點尺度量表進行衡量，由非常不同意(1)到非常同意(7)，而委外的項目比例則是從完全不委外至完全委外區分成五個等分，來讓填答者勾選，此外還有填答者的基本資料部份，這部份包含了填答者的背景資料以及控制變項。

在問卷前測的部份，為了提昇問卷的品質，我們請了多位相關領域的專家，包含了資訊安全管理領域的教授，以及擔任企業資訊安全風險管理顧問的多位專家，企圖透過學界以及業界的多元觀點，協助我們從不同的角度來改善問卷，而在專家的協助下，我們大幅的改善了用字遣詞的精準性與易讀性，確保問卷的原意能夠精確的傳達，填答者也能夠很容易的理解問項。

3.5.2 控制變項

在進行本研究的同時，我們也必須考慮到競爭優勢也可能受到其他因素的影響，諸如公司的規模、資訊部門的預算、資訊部門的經驗等等，因此本研究將這三個項目放入控制變項中來作討論。

先前學者對於競爭優勢的相關研究顯示公司規模可能會影響競爭優勢的形成(Harris & Katz, 1991; Melville, Kraemer, & Gurbaxani, 2004)，規模較大的公司可能形成規模經濟，透過成本的降低來造就競爭上的優勢，而根據之前的學者所提出的概念(Dewar & Dutton, 1986)，本研究利用公司的員工數來作為公司規模大小的衡量指標。

企業對於資訊科技、資訊安全方面的投資額大小，也被認為會影響著競爭優勢創造(Melville, et al., 2004)，在資訊安全方面投入更多的資源可能為企業帶來更完善的資訊安全防護,因此投資額也很有可能會影響企業建置資訊安全的成果,所以本研究也試圖控制企業的資訊部門預算，以及資訊部門用在資訊安全方面的預算，以確保上述的情況不會干擾到本研究主要的假設情況。

此外競爭優勢也可能受到資訊部門的經驗影響(Chang, 2002)，也就是說當一

個資訊部門隨著時間的經過，裡面的人在資訊安全方面的經驗越豐富，使用某些資訊系統的時間較長可能使得員工更加熟練，在面對資訊安全問題時，可能更能夠快速的反應，相反地，如果資訊部門的經驗不足，可能導致企業需要耗費較多的資源在訓練上面，而資訊部門的員工可能也無法發揮資訊安全防護的最大效益，所以本研究利用資訊部門成立的時間來作為一個控制的變項。

第四章　分析與結果

本章首先對受訪者資料進行整理，並且簡述其基本分析之統計結果，接著針對蒐集到的資料分析其信度、效度與常態性，以確定資料可適用於接續之多變量分析過程，之後對於本研究所提出之模型和假設進行檢驗，最後針對研究之結果進行討論及分析。

第一節　基本資料分析

4.1.1 問卷回收

而本研究在蒐集的對象方面，也盡力的嘗試透過許多不同的管道來進行資料蒐集，包含了國際電腦稽核協會(ISACA)的台灣分會會員、資訊安全相關的研討會、學校機關、親友任職的企業、網路資安論壇以及網路相關討論看板，透過上述這些不同的國內企業、公私立機構、團體作為樣本來源，主要是希望能夠提昇樣本的數量、增加樣本的多樣性及代表性。

在紙本發放方式中，包含了電腦稽核協會會員以及資訊安全相關研討會的部份，我們透過會議現場發放之方式，總共發放 62 份問卷，回收有效問卷 11 份，回收率 17.74%(僅採計有效問卷)。而在電子郵件部份，主要包含學校機關以及親友任職之企業，一共寄發 38 份問卷，回收了 18 份有效問卷，回收率 47.36%。而在網路的發放部份，我們將問卷的線上版公佈在國內主要的資訊安全論壇以及相關網路討論看板，以方便回收，但是由於此部份無法確認實際發放之數量，故不計算其回收率。最後回收的問卷共 54 份，在經過資料整理及篩選後，將不合理或

有缺漏的無效問卷刪除，實際有效問卷為 43 份。

4.1.2 基本資料分析

本研究彙整後之有效樣本為 43 份，而針對受訪者背景所作之基本資料調查分述如下。

在受訪者的職稱分佈情形，以資訊部門人員最多，共 21 位佔樣本比例 48.9%，由於本研究主要針對資訊部門相關人員作為發放，故資訊及資安部門相關人員共計 37 位，佔樣本 86%，而在其他的填答者部份，包含了有總經理、副總經理、稽核人員等等，對於企業資訊安全這部份也有一定的了解，由此可知本研究之填答對象具有相當之代表性，而詳細分佈情形如表 4–1–a 所示。而在受訪者產業分佈，以科技製造業為主，共有 18 家佔樣本 41.9%，其次為服務業有 7 家，佔樣本 16.2%，再者為金融業，共有 6 家佔樣本 14.0%，詳細分佈情形如表 4–1–e 所示。

受訪者員工人數分佈，以 100 人以下最多，共計 15 家佔樣本 34.9%，其次為 100~500 人有 10 家，佔樣本 23.3%，而超過千人以上之大型企業共有 15 家，也佔了超過 1/3 之比例，詳細情況如表 4–1–c 所示。受訪者資訊部門人員數，以 10 人以下最多，共計 26 家佔樣本 60.5%，而其餘區間樣本數都非常接近，可得知此次調查之企業，資訊部門人數都以 10 人以下居多，而資訊人數達 100 人以上的公司共有八家，也佔樣本比例接近 1/5，如表 4–1–d 所示。

受訪者資訊部門成立年份，以 10 年以上最多，共計 22 家佔樣本 51.2%，其次為 4~6 年有 9 家，佔樣本 20.9%，由此可知此次調查的對象，有半數是成立時間超過十年的企業，詳細情況如表 4–1–b 所示。

在資訊安全委外項目比例這部份，我們針對主要的幾個委外項目請受訪者勾選其委外的比例，而在表 4–1–f 中所呈現的是計算平均之後的結果，而因為受訪者可能委外多個項目，故各項目樣本數的加總值並不等於所蒐集到的總樣本數，由表中我們可以看出，企業對於降低威脅及應用程式這部份，較多的採取委外的作法，其中降低威脅包括了弱點偵測、網路管理、內容過濾、資安事件管理等子項目，企業在此部份委外的比例將近五成，而在應用系統安全的部份，則是指系統建置的安全及維護，企業在此部份的委外比例也有 40%的表現，而其餘之項目雖然也有許多的企業願意採取委外，但是平均而言委外比例偏低，而整體看來，企業將資安委外的平均比例皆未超過 50%，可以看出國內企業考量資訊安全時依然偏重於自行建置。

而其餘的受訪者資料，例如年度資訊預算、年度資安預算、年度資安委外預算、資安預算佔資訊預算比例、資安委外預算佔資安預算比例等等，被本研究歸類為選填項目，而有部份填答者可能出於企業隱私考量並未填答，故無法計算其完整之分佈情形與比例，在此不多加贅述。

表 4－1 ：基本資料統計分析

(a)受訪者職稱			(b)資訊部門成立年份		
職稱	樣本數(人)	百分比(%)	年份分佈	樣本數(家)	百分比(%)
資訊部門主管	8	18.6	1 年以下	4	9.3
資安部門主管	3	6.9	1~3 年	4	9.3
資訊部門人員	21	48.9	4~6 年	9	20.9
資安部門人員	5	11.6	7~9 年	4	9.3
其他	6	14.0	10 年以上	22	51.2
(c)員工人數			(d)資訊部門員工人數		
人數分佈	樣本數(家)	百分比(%)	人數分佈	樣本數(家)	百分比(%)
100 人以下	15	34.9	10 人以下	26	60.5
101~500 人	10	23.3	11~50 人	4	9.3
501~1000 人	3	6.9	51~100 人	5	11.6
1001~5000 人	8	18.6	101~200 人	3	6.9
5001~10000 人	4	9.3	201~500 人	2	4.7
10001 人以上	3	6.9	500 人以上	3	6.9
(e)產業類別			(f)資安委外項目比例		
產業	樣本數(家)	百分比(%)	項目	樣本數(家)	委外比例(%)
科技製造業	18	41.9	實體安全	33	30.75
服務業	7	16.2	人員安全	34	31.40
金融業	6	14.0	交易完整性	32	27.90
政府機構	3	6.9	降低威脅	38	47.68
學校機構	5	11.6	應用系統安全	38	40.13
醫療機構	2	4.7	資料保護	26	23.83
財團法人	2	4.7	公司治理	31	27.33

第二節　信度與效度分析

本節將針對問項的資料進行信度與效度的分析，信度主要在評估結果的一致性(consistency)，即在不同次的測試中其測量概念的可靠度，效度則是在檢驗測量

的準確性(accuracy)及真實性(truthfulness)，判斷量表是否測量到所欲測量的概念，而在進行下一步的分析之前，我們必須先檢驗資料的信度與效度，故下面的段落我們將分別討論之。

4.2.1 信度分析

在分析資料的信度這部份，Nunnally(1978)建議使用 Cronbach's alpha 來作為檢定信度的係數，當值高於 0.8 時被認為信度是相當良好的、而大於 0.7 時表示信度是可以接受的程度，若值低於 0.35 則此部份之資料應該刪去不用(Hair, Anderson, Tatham, & Black, 1998; Nunnally, Bernstein, & Berge, 1994)，故本研究也利用此在學術界被普遍認可的 Cronbach's alpha 值來檢測問卷項目的信度，檢測結果如表 4－2 所示，可以看出所有測量的構面，其值都高於 0.8，所以本研究之信度相當良好。

表 4－2 ：研究構面之信度及效度檢測

研究變數	衡量問項	Cronbach's α	AVE
資訊安全資產(ISA)	ISA1~ISA8	0.968916	0.822267
資訊安全能力(ISC)	ISC1~ISC9	0.979339	0.858188
低成本(LC)	LC1~LC4	0.945249	0.858014
差異化(DIF)	DIF1~DIF8	0.968037	0.818385

4.2.2 效度分析

在效度的部份，我們利用建構效度(Construct Validity)來評估其好壞，建構效度主要透過檢驗收斂效度(Convergent Validity)以及區辨效度(Discriminant Validity)

來完成(Anderson & Gerbing, 1988)，收斂效度是以不同問項來測量相同的概念，若兩者分數相關性高則此兩問項，具有收斂效度(Nunnally, et al., 1994)，而區辨效度則是指測試不同概念的問項，其相關性必須較低，則問項間具有區辨效度(Anderson & Gerbing, 1988)，當收斂效度以及區辨效度同時成立時，我們便可以指稱此次測量具有建構效度。

欲檢測收斂效度，我們必須利用平均變異數抽取量(Average Variance Extracted;AVE)的概念，而平均變異數抽取量指的是在一構念中各因素負荷量(factor loading)平方和的平均值，學者建議平均變異數抽取量的值需大於 0.5，表示具有收斂效度(Fornell & Larcker, 1981)，而本研究之欲測量之構念，其 AVE 值均通過此標準，而且各個問項對於其構念之相關性均為顯著，故具有良好之收斂效度，詳細之結果如表 4－2 所示。

而為了判別區辨效度，每一個構念本身的變異抽取量需要大於此構念與其他構念的相關係數平方值(Fornell & Larcker, 1981)，如果存在某一構念之變異抽取量低於與其他構念的相關係數，即表示在該構念中，某一測量問項可能也是另一個構念之測量問項，因此我們需要證明，任一構念之 AVE 值在開平方根後大於與其他構念之相關係數，即代表有良好的區別效度，而表 4－3 呈現了每個構念之 AVE 開平方後之數據以及與其他構念之相關係數，可以看出本研究欲測量之構念具有良好的區辨效度。

透過上述兩種檢驗，我們可以得知本次研究蒐集之具有良好的效度，因此我們可以更進一步來檢驗資料的常態性以及整體是否符合多變量常態。而為了施作接下來的各項檢測，我們將些許在效度檢測中較差的個別問項、以及相關性太高

之問項予以刪除，基於之前所測得之信度相當高，而且各個構面之問項依然完整的保留並呈現，我們認為篩選過之資料能夠測度出更加貼近真實的結果呈現。

表 4－3 ：各研究構面之 AVE 平方根植與其相關係數比較

	資訊安全資產	資訊安全能力	低成本	差異化
資訊安全資產	**0.934124**			
資訊安全能力	0.859208	**0.932941**		
低成本	0.517460	0.436393	**0.951339**	
差異化	0.818900	0.715437	0.534989	**0.908231**

第三節　常態性檢定

常態性是多變量分析基本的假設，在進行下一步的假說檢定之前必須先檢測所蒐集之資料是否符合常態分配，而在確定資料確實為常態性的分配之後所實行的假設模型測試以及假說檢定才有意義，此外，多變量常態也是 SEM 分析中最重要的基本假設，因為 SEM 是利用資料的共變結構來進行分析，所以整體的情況也必須符合多變量常態的假設。

而本研究利用觀察資料的偏態(Skewness)及峰態(Kurtosis)來判別，學者建議單一問項的峰態值不能大於 7，否則不符合常態性(West, Finch, & Curran, 1995)，本研究之單一變量值均小於 7，可以看出個別問項均符合常態分配。而整體的多變量是否符合常態，則必須依靠臨界比(C.R.)值來判斷，當 C.R. 值大於 5 時，整體資料沒有呈常態性的分配，意即不符合多變量常態(Bentler, 2006)，而本研究之多變量 C.R.值為 3.555，因此整體而言符合多變量常態之假設，而由表 4－4 可以看出本研究各變項之資料的詳細分配情形，均符合常態性之分配。

表 4－4 ：各研究變項之常態性及多變量常態檢測				
衡量指標 變項名稱	Skew	C.R.	Kurtosis	C.R.
控制變項				
員工人數	.605	1.619	-1.173	-1.570
資訊部門經驗	-.769	-2.058	-.758	-1.014
資訊安全資產				
ISA_1	-.953	-2.553	-.297	-.397
ISA_2	-.587	-1.573	-.752	-1.006
ISA_3	-.996	-2.667	.327	.437
ISA_4	-.737	-1.974	-.338	-.453
ISA_5	-1.137	-3.045	.727	.973
ISA_6	-.697	-1.867	-.213	-.285
ISA_7	-1.112	-2.977	.737	.987
ISA_8	-1.167	-3.125	.768	1.027
資訊安全能力				
ISC_1	-1.110	-2.971	.287	.384
ISC_2	-1.287	-3.445	.910	1.219
ISC_4	-.981	-2.626	.440	.589
ISC_5	-.949	-2.540	.247	.330
ISC_6	-.559	-1.496	-.565	-.765
ISC_7	-1.061	-2.840	.220	.295
ISC_8	-.763	-2.042	-.575	-.769
ISC_9	-.806	-2.158	-.342	-.457
低成本				
LC_2	-.074	-.198	-1.066	-1.427
LC_3	-.153	-.410	-.792	-1.060
LC_4	-.198	-.531	-.760	-1.017
差異化				
DIF_2	-1.043	-2.793	.486	.651
DIF_3	-.816	-2.185	.156	.209
DIF_4	-.955	-2.555	.463	.620
DIF_5	-.957	-2.563	.501	.670
DIF_6	-.702	-1.880	.041	.055
DIF_7	-.787	-2.106	.120	.160
DIF_8	-.977	-2.615	1.071	1.433
多變量			41.371	3.555

第四節 模型適配度檢定

本節將介紹研究模型的適配度，由於本研究是透過理論發展出之研究模型，在經過考量之後決定使用結構方程模式(Structural Equation Modeling；SEM)作為驗證之方法並以 AMOS 18.0.0 作為分析之軟體工具，SEM 可以將難以直接觀察的構念以潛在變項的型式，透過觀察變項的模型化來加以分析估計，而除了能夠同時的對於許多變項進行相互的關係分析以及衡量潛在變數之外，也能夠針對測量誤差的部份進行探究(Hair Jr, Anderson, Tatham, & Black, 1995; Kline, 1998)。而由於利用 SEM 在進行檢測之前必須確認每個問項資料符合常態性的分配，因此我們在上一節也進行了驗證，以確保接下來檢測能夠成功的實行(Hoyle & Panter, 1995)。

適配度代表的是整體的資料與建構出模型謀合的程度，在 SEM 這種屬於驗證性的分析當中，被用來檢測所提出的模型是否擁有良好的配適，而大多數的研究者都會給出多個不同的適配指標，來驗證自己所提出的模型。而學者也將由不同概念發展出的各種指標加以分類，以下會將幾種不同的指標類型作簡單的介紹(James, Mulaik, & Brett, 1982; Tanaka, 1993)。

一、絕對適配指標：絕對適配指標不與其他型態之模型進行比較，而是單純的檢測蒐集到的資料與所提出之模型來進行適配，以衡量變項之共變關係並透過統計之方法來評估模型通過與否，常見的絕對適配指標有卡方值(χ^2)、非中心參數(NCP)、良性適配指標(GFI)、均方根殘差(RMR)、標準化均方根殘差(SRMR)、近似誤差均方根(RMSEA)。

二、相對適配指標：相對配適指標則是將所提出之模型與虛無模型(null model)作比較，而所謂的虛無模型則是指模式中所有觀察之變項皆獨立之情況，在比較

完全獨立之虛無模型以及依照理論所發展出之模型這兩者之間的統計卡方值，計算出其改善的比率，來作為判斷假說模型優劣之依據，常見的有比較適配指標(CFI)、規範適配指標(NFI)、增值適配指標(IFI)、相對適配指標(RFI)等等。

三、簡效適配指標：簡效(Parsimony)的概念是企圖對失去的自由度加以調整，對於較簡單的模型有所偏好，而對於較複雜之模型給予懲罰，通常是將相對適配指標乘上其簡效比率得到，較常見的有簡效規範適配指標(PNFI)、簡效良性適配指標(PGFI)、簡效比較適配指標(PCFI)等。

本研究採用了如表 4 - 5 所示之各項指標來檢驗模型的配適度，在絕對配適指標方面，我們採用了卡方值除以自由度之後之數值(χ^2/d.f.)來檢驗，此項指標也是被許多學者所建議採用，而所得出的測量值為 2.903，符合學者建議小於 5 的標準，接著在近似誤差均方根(RMSEA)的部份，我們所測量得到的數值 0.213 比學者所建議之小於 0.10 略高。而在相對適配指標方面，我們採用比較適配指標(CFI)以及規範適配指標(NFI)，所得到之值分別為 0.673 及 0.581，並未達到學者建議之 0.90 標準。最後在簡效適配指標這方面，簡效比較適配指標(PCFI)以及簡效規範適配指標(PNFI)，所得到之值分別為 0.611 及 0.527，高於學者所建議的大於 0.50 之標準。由整體情況來看，模型的適配度並沒有相當的完美，但是我們可以由數值中發現，RMSEA 數值與建議標準差異不算太大，而在簡效適配指標將失去的自由度進行調整之後，原本並未達標準之 CFI 與 NFI 值，轉換成 PCFI 與 PNFI 之後也落在了可以接受之範圍內，因此我們認為這次研究的模型適配度是可以被接受的。

表 4－5 ：模型適配度檢測			
配適指標	測量值	建議值	參考來源
χ^2/d.f.	2.903	<=5	(Bentler, 1995; Segars & Grover, 1993)
RMSEA	0.213	<=0.10	(Byrne, 2006)
CFI	0.673	>=0.90	(Bentler, 1995)
NFI	0.581	>=0.90	(Bentler & Bonett, 1980)
PCFI	0.611	>=0.50	(Hair, et al., 1998)
PNFI	0.527	>=0.50	(Hair, et al., 1998)

第五節 假說檢定

本節將針對假設模型進行驗證，並且針對結果進行討論，由表4－6可以看出，委外後所獲得之資訊安全資產對於競爭優勢有顯著的影響，不論是對於成本之降低以及差異化之表現都非常明顯，而在委外後所獲得的資訊安全能力與競爭優勢則出現了不同的情況，數據顯示委外後所獲得的資安能力與成本之降低並不存在顯著的關係，另外委外後所獲得的資安能力與差異化的競爭優勢則呈現負向的顯著關係。而除了原本的假設之外，我們也加入了兩個控制變項，員工人數及資訊部門經驗。兩者對於差異化競爭優勢之影響也是顯著的，下面我們將逐一檢驗假說模型。

表 4－6 ：路徑係數結果分析					
	Standardized Estimate	Estimate	S.E.	C.R.	P value[1]
LC ← ISA	.889	.609	.204	2.989	.003
DIF ← ISA	.909	1.369	.175	7.816	***
LC ← ISC	-.261	-.173	.156	-1.105	.269
DIF ← ISC	-.352	-.512	.126	-4.064	***
LC ← employee[2]	-3.00	-.153	.082	-1.867	.062
DIF ← employee	.174	.195	.061	3.190	.001
LC ← IT Year[3]	.225	.173	.118	1.464	.143
DIF ← IT Year	-.139	-.235	.089	-2.637	.008

4.5.1 資訊安全資產與低成本競爭優勢之分析

根據研究架構中，將資訊安全委外後所獲得之資安資產與低成本競爭優勢之間的關係，提出以下之假設：

H1：企業將資訊安全委外後所獲得的資訊安全資產將正面影響企業的成本優勢。

我們利用上述表 4－6 的結果得知，資訊安全資產與低成本競爭優勢有顯著正向相關，本研究假設成立。這也顯示在企業將資訊安全委外之後所獲得的資訊安全資產，諸如有形的資訊安全基礎設備、無形的與外部供應商之夥伴關係、供應商之服務品質等等，都能夠為企業帶來成本的降低，像是將基礎設備委外能夠讓

[1] ***表示 P value < 0.001
[2] Employee 表示員工人數
[3] IT Year 表示資訊部門經驗

企業以較低的價格負擔獲取先進的科技設備使用權，而當委外供應商的服務品質越好、與企業主的夥伴關係越好能夠使得企業花費在資訊安全這區域的人力、管理成本降低，致使企業能夠降低所需的成本，創造競爭的優勢。此外，在過往許多的相關研究當中都可以看出，降低成本是企業實行委外活動的主要考量因素之一，更能夠支持此項驗證之結果(Chan, 2005; Claver, Gonzalez, Gasco, & Llopis, 2002)。

而 Poppo(1998)等學者認為，企業若想要自行發展獨特的科技技術，不論是設備或系統，都可能對企業之表現沒有實質幫助，甚至造成成本的上升，因為現今的科技環境日新月異，當企業花費大量的資源所建立起的獨特工具，在短期內可能給予企業一些幫助，但是當科技之潮流改變，又有新的技術出現時，原本的投資可能瞬間失去價值,因此 Poppo 等學者更加傾向於透過市場來獲取新的設備，這樣的委外活動長期而言，不但能夠降低企業所需的成本，無須受限於自行建置的限制當中，還能夠使得企業變得更加靈活有彈性。而我們認為其研究結果也適用於企業發展資訊安全的情況，因為資訊安全所需的設備有都具有高度的技術性及特殊性，一般企業也很難自行發展出如此獨特的工具，另一方面，資安環境之變動也相當之迅速,新的攻擊手法層出不窮,當企業本身無法解決的困難出現時，就可能造成很高的資訊安全風險，甚至帶來很大的損失，因此企業應該透過市場來尋求解決的方案，除了降低成本之外也能夠提昇企業表現，因此這也呼應了我們的研究結果，當企業將資安資產委外時，的確能夠收穫實際的經濟效益並且提昇企業的競爭能力。

4.5.2 資訊安全資產與差異化競爭優勢之分析

根據研究架構中，將資訊安全委外後所獲得之資安資產與差異化競爭優勢之間的關係，提出以下之假設：

H2：企業將資訊安全委外後所獲得的資訊安全資產將正面影響企業的差異化優勢。

我們利用上述表 4－6 的結果得知，資訊安全資產與差異化競爭優勢有顯著的正向相關，故本研究假設成立。這表示在企業將資訊安全委外之後所獲得的資訊安全資產，諸如上述提及之資安基礎設備、夥伴關係、服務品質等等，都能夠為企業帶來差異化的競爭優勢，也就是說企業委外之後所有的這些資產，不但能讓企業重新聚焦於核心業務、提供給客戶更好的感受、還能夠提高企業本身的聲譽、並且讓其他競爭對手無法輕易的模仿，而這種競爭優勢也更加的持久並且難以複製，而先前也有相關的研究在這部份有類似的結論，在 Chan(2005)的研究中指出企業透過委外能夠有效的提昇運用資安系統的能力，如果能進一步與服務供應商雙方保持良好的夥伴關係，則雙方可以在各自的產業中獲取競爭之優勢。

而在資訊安全資產的構面中，我們將夥伴關係與服務品質列為考量的概念，在 Grover(1996)等學者的研究當中也使用了這兩個概念作為衡量資訊系統委外成功的評估指標，其研究發現服務品質與夥伴關係的確會對企業的資訊系統委外帶來很大的影響，維持良好的服務供應商與企業主關係，對於委外的成功很有幫助，而我們的研究也證實了當評估的委外活動由資訊系統轉移至資訊安全時，夥伴關係與服務品質這兩個概念仍然扮演著相當重要的角色，不只會對於委外的結果產生影響，當兩者的關係保持良好，能夠將雙方的合作提昇至更高的層次，使得其他企業難以複製同樣的成果，會給企業帶來獨特的競爭優勢。

4.5.3 資訊安全能力與低成本競爭優勢之分析

根據研究架構中，將資訊安全委外後所獲得之資訊安全能力與低成本競爭優勢之間的關係，提出以下之假設：

H3：企業將資訊安全委外後所獲得的資訊安全能力將正面影響企業的成本優勢。

由上述表 4－6 的結果得知，資訊安全能力與低成本競爭優勢並沒有顯著相關，本研究假設不成立。也就是說企業委外後所獲得的資訊安全科技能力、管理能力、反應能力等等，並無法對於企業所需付出之資訊安全成本有顯著的降低。而我們試圖從不同的角度來推論可能之原因，如同先前所提及維護企業資訊安全所需要的能力相當的複雜且專業(Deshpande, 2005)，企業難以單獨靠本身的力量來完成，而在台灣的資安環境中有能力來提供資安服務的廠商並不多，當考慮的是透過委外來獲得資安能力的時候，賣方提供的服務及價格可能有著極大的落差，並且難以有效的比較出其中之差異，造成買賣雙方資訊不對稱之情況發生，使得有資安委外需求的企業可能無法如本身預期的將成本降低至理想的程度。

先前的研究也指出，當在企業執行委外活動時，如果所委外的業務太複雜或者難度較高，導致企業無法正確的評估出執行的難度，造成企業委外無法如預期般地降低成本(Poppo & Zenger, 1998)。而本研究原本的假設，是透過委外來獲得資安能力，包含了發展資安所需的科技能力、管理企業資安整體架構、程序及流程的能力，還有當資安事故發生時處理應變的能力，這些能力不但涉及的層面極廣，所包含的內容也相當的複雜，因此造成委外供應商無法以客戶理想中的價格來提供相關的服務，以至於企業無法有效的透過委外來降低獲取這些資安能力的

成本，這也支持了本研究結果的陳述，企業將資訊安全委外後所獲得的資訊安全能力與降低企業成本的關係並不顯著。

而在先前的文獻探討中也提及 Peteraf(1993)認為公司在利用資源實行策略之前必須先考量成本，以避免耗費過多成本卻得不到足夠的利潤，便無法創造出足夠的競爭優勢，而我們認為資訊安全的委外投資可能面臨一樣的問題，因為資訊安全本身就屬於一個難以正確衡量其價值的投資，當企業將執行資安業務所需的科技能力、建構完整資安管理架構的業務及回應事故的反應程序委外交給服務供應商來執行時，可能需要較高的費用，但是得到的價值卻難以直接評斷，若非一些資安事故發生,也很難有機會驗收其成效,因此可能造成企業耗費過多的成本，使得企業難以從中獲得降低成本的優勢

在研究過程中，我們也發現目前台灣的企業在資訊安全部份，較少主動的去尋求自身資安能力的完備，大都是在外力的影響之下(如：資安事故、法規要求)才開始注重資訊安全，因此在企業尋求資安委外之時，可能被企業主視為是一種額外的成本支出，而不是從透過委外節省了多少成本的方向來思考。

4.5.4 資訊安全能力與差異化競爭優勢之分析

根據研究架構中，將資訊安全委外後所獲得之資安能力與差異化競爭優勢之間的關係，提出以下之假設：

H4：企業將資訊安全委外後所獲得的資訊安全能力將正面影響企業的差異化優勢。

我們利用上述表 4－6 的結果得知,資訊安全能力與差異化競爭優勢有著負向的顯著相關，本研究假設不成立。結果說明企業委外所獲得的資安能力越高，所獲得的差異化競爭優勢越低，這與我們原先假設的方向呈現相反的關係，而我們由研究過程中，重新檢視了當初假設的立意並且參照了研究過程中的發現，做出以下的推論，原先我們認為獲取資安能力相當的困難，一般企業難以獨立完成，在加上資訊安全並非企業核心業務,所以可以依靠委外的方式來獲得充分的能力，但是在研究的過程中發現，有許多的企業雖然並非以資訊安全為核心業務，但是在其執行核心業務的同時，伴隨著很高的資訊安全需求，如會計公司不願讓外部廠商接觸到企業內的客戶相關資訊、網購業者在將資安委外之後有了資料外洩的風險，這使得資訊安全不單只是操作上的考量，而開始與企業的競爭策略有了連結，造成企業在資訊安全能力委外這部份只有很低的風險容忍程度，因此當企業將資訊安全視為核心業務或者作為競爭策略來考量時，可能就需要利用不同於一般業務的思維以及處理方式，亦即不能將核心的能力委外給服務供應商。而在 Teng(1995)等學者的研究中也提及當企業在考慮資訊系統委外時，如果資訊系統過多的涉及組織的策略層面，則會使得組織委外意願較低，而這也能夠支持我們所作的推論，當企業將資訊安全列入競爭的策略來考量時，便會傾向於自身擁有資訊安全能力，以提昇企業之競爭力。

此外，我們也重新省視了資源基礎理論本身，當資源基礎觀點被提出之後，陸續有許多的學者提出了若企業想要利用所擁有的資源來創造競爭優勢時，這些資源必須具備若干的特性，Barney(1991)認為資源要能夠提供長久的競爭優勢必須要有價值性(value)、稀少性(rareness)、不可模仿性(imperfect immutability)、及不可替代性(nonsubstitutability)等特質，而在我們原本的考量中，因為這些資源必須是企業所獨有，因此可能較為不適合用於委外的討論，而此項假設中出現不成立的結果，也很有可能是因為本研究所考慮的資安能力在經過委外之後，喪失了

其稀少性、不可模仿性及不可替代性，因為將所需的資安能力委外即代表其他的企業也可能透過相同的方式來達成類似的成果，因此委外部份的越多對於企業的競爭優勢而言，可能帶來負面的影響。

而若從另一角度來看，Carr(2003b)的文章中認為，現在的經營環境之中資訊科技的運用已經變得非常普遍，從早期只有稀少的企業使用的情況演變至今，資訊科技已經從原本能夠帶給企業競爭優勢的地位變成了所有企業的必需品，所以學者認為資訊科技應該被視為一種企業的日常用品，其存在雖然必須但已經沒有過往那種能夠創造競爭優勢的能力，而若將場景置換到資訊安全的情境中，我們認為類似的情況也可能會發生，當企業將資訊安全的能力視為一種必須的同時，雖然因為自身資源不足而將其委外，但是目的已經不是為了創造企業的競爭優勢，而是為了保護企業執行業務的安全必須達成的目標，使得資安能力與競爭優勢的相關性變得不如預期的情況，而這些推論當然也需要更進一步的深入研究才能證實。

4.5.5 控制變項與競爭優勢分析

本研究中使用了員工人數來代表企業之規模以及資訊部門成立年份代表資訊部門經驗，來作為控制的變項，而從表 4－6 的數據結果中可以看出，這兩者與企業差異化的競爭優勢存在著顯著的關係，意即當企業的規模較大或者資訊部門的經驗較為豐富，能夠比其他的企業更容易獲取競爭上的差異化優勢，並且會讓其他企業難以輕易複製或模仿其業務之執行。因為當企業規模較大時，在資訊部門所獲得之資源可能較多，使得大企業在策略的規劃及執行時有更充足的力量，並且得到較佳的成果，而若資訊部門成立較久，擁有較多的經驗，不論是在業務執行規劃或者遇到事故的反應復原，可能都有較為完善的標準流程或者處理方式，

而這些經驗是透過時間的累積而成，其他企業難以在短時間內學習獲得，也因此形成其他企業無法達成的差異化優勢，而先前的研究也有類似的結果(Chang, 2002; Harris & Katz, 1991)，此部份雖然並非我們欲探討之重點，但仍然在此提出作為參考，此外原本的資訊及資安預算等控制變項，因為大多數的填答者不願作答，造成遺漏值太多無法進行統計分析。

4.5.6 補充分析

而我們在原本的假設模型之外，也嘗試了利用不同的概念來進行相關統計分析，如先前所言資產可視為產品的輸入抑或是生產流程的輸出，而能力則將輸入轉換成更有價值的東西(Amit & Schoemaker, 1993; Sanchez, et al., 1996; Wade & Hulland, 2004)，我們可以發現能力也擁有將資產轉換成產品的概念，因此我們考慮將資安能力作為資安資產與競爭優勢的中介變項，想要進一步的探究資安資產、資安能力與競爭優勢之間，是否存在著這樣的中介關係，也就是說企業在委外後所擁有的資安資產透過委外後所獲得的實行資安的能力來影響競爭的優勢，而根據這樣的假設所分析出來的結果，雖然在整體模型的適配度上沒有原本假設的模型這麼良好，但是其假設都成正向顯著相關(如表 4-7 所示)，藉此我們初步認為委外後所獲得的資安能力的確可以將資安資產轉變為企業實質上的競爭優勢，而且不論在降低成本以及差異化兩方面都有顯著的改善與提昇，當然這部份的推論還需要往後更加深入的探究，才能夠更清楚地界定其間的關係，我們在此提出此假設概念作為參考。

表 4－7 ：路徑係數結果分析(二)					
	Standardized Estimate	Estimate	S.E.	C.R.	P value[4]
ISC ← ISA	1.000	1.035	.105	9.852	***
LC ← ISC	.748	.419	.115	3.642	***
DIF ← ISC	.998	.792	.108	7.367	***

[4] ***表示 P value < 0.001

第五章　結論與建議

第一節　研究結果

本研究利用資源基礎的觀點為基礎，將資訊安全視為公司的一種資源，推論公司在資訊安全能力與預期達到的能力有所落差的情況下，透過委外的策略將資訊安全委託給外在的服務供應商，將能夠為公司帶來更好的效益，並且取得競爭上的優勢。而研究結果顯示，委外後所獲得的資訊安全資產的確能夠為企業帶來競爭優勢，不論在降低成本或者差異化方面都有顯著的影響。但是在企業委外後企業所獲得的資訊安全能力方面，對於降低成本或者差異化的關係，並非如預期般的呈現正向顯著相關，而我們認為這樣的結果可能是由許多不同的因素導致。

必須了解的重點是不同的企業對於資訊安全的定位也有所差異，當企業原先並不重視資訊安全的情況下，可能將委外視為額外的成本負擔，當企業將資訊安全視為核心業務發展策略的一部分時，可能將委外視為競爭優勢的流失。而在資訊安全資產與資訊安全能力所得出的結果不同也能夠說明台灣目前的資訊安全環境現況，根據之前資策會之調查顯示(王義智, 2009)，台灣目前的資訊安全委外服務市場稍微的落後全球趨勢，大多數的國內企業可能還是對於基本設備的委外較能接受,如防火牆或者入侵防禦系統的建置,但是對於一些流程式的委外服務，如整體的資安結構規劃、顧問諮詢、教育訓練等等並不如國外普及，這也是資訊安全資產與資訊安全能力兩者結果不同的原因之一。

整體而言，在資訊安全屬於一般支援業務的情況下，本研究的結果支持資訊安全委外能夠為企業帶來競爭優勢，然而值得注意的是企業必須先將本身對於資

訊安全之定位確定，才能夠確保能夠在資安委外之後獲得競爭優勢。在此我們必須重申，隨著環境改變，企業所面臨的資訊安全風險與日俱增，而在金融風暴的災害中以及雲端概念的浮現等等，許多不同的因素都會迅速地改變維護資訊安全所需要的要素及條件，而企業想要完善的保護其資訊安全的挑戰性也越來越高，不論是否考慮將資安委外，企業都不能夠只是閉門造車，單獨憑藉本身的力量難以保證企業的資訊安全,而更多的是需要仰賴專業的服務供應商給予建議或協助,在互信互惠的情況下發展企業的資訊安全，才能夠達成雙贏的局面，並且為企業帶來競爭的優勢。

第二節　研究貢獻

在資訊安全的領域裡，本研究也是首先嘗試引入資源基礎架構的研究之一，過往的相關研究，多是將資源基礎理論與資訊科技或資訊系統作結合，鮮少探討到資訊安全這部份,而且在資訊安全的領域裡與理論結合之研究依然相當的缺乏,此外我們關注的資訊安全委外議題，也在這幾年間逐漸受到研究者的重視，希望本研究能夠帶給往後的研究者一些發想，除了能夠更加的深入研究企業的資訊安全之外，還可以將更多的不同領域的理論應用至資訊安全的研究中，使得學界對於資訊安全的認識更加的豐富、多元且完整。

而在實務方面，本研究所提出之模型與研究成果亦能提供企業界的決策者一些幫助，作為實行資訊安全業務時的參考，對於正在評估資安委外的企業主能夠藉由我們的研究結果得知委外能夠帶給企業的實質幫助,藉此規劃其策略之行動,而已經委外的企業則可以了解企業內哪些方面的資源是影響委外成功的最重要因

素，藉此重新省視其委外的策略，是否有需要調整的地方，以提昇企業之競爭優勢。

第三節　研究限制

本研究根據理論之推演所提出研究架構，由於研究主題的特性、研究時間之限制、研究人力不足、及相關學術研究並不充足等因素，雖然在過程中也嘗試盡力改善,但整體研究仍有未及之處,此部份將針對這些研究上的限制來進行討論。

首先是關於研究主題的部份，由於主題涉及企業的資訊安全，使得一些企業填答的意願並不高，而探討委外議題，對於目前委外趨勢落後全球的台灣企業而言，有將資安委外的企業並不如預期中的普遍，兩者交互的影響對於資料蒐集產生一定的困難，在研究過程中我們也嘗試透過各種不同的管道來蒐集資料，包括了研討會現場發放、寄送電子郵件、網路發放給企業及學校、透過身邊的親友幫忙發放等等，雖然我們在蒐集的來源上作了很大的努力，最後蒐集的樣本仍然未達預期之數量，這也造成我們的研究仍有不足之處，在此也建議之後的研究者可以將研究的時間拉長或者嘗試更多的蒐集管道，來增加自己的資料數量。

本研究透過理論的基礎以及參考前人的文獻，設計了一些評估競爭優勢的問項，但是這些問項都是由各企業的填答者主觀的評估企業本身的情況，似乎缺乏較為客觀的比較，這部份也是在研究過程中所面臨的限制，但是若想從客觀的角度出發衡量企業間的差異，在執行上有著極大的難度，可能需要將研究對象範圍縮小到一定的程度或者透過質化研究的方式來完成，希望這也能夠給往後的研究者作為一個參考。

第四節　未來研究建議

在這次研究的過程中，我們盡可能的考慮各種情況的發生，並且為求嚴謹反覆地在研究過程進行修正，但有些部份仍然受限於先天上的研究限制，或者隨著研究進行發現了未來可以改善的部份，雖然無法即時且完善的修正呈現在研究結果中，但我們在此提出一些未來的研究建議，希望能夠提供對於資安委外議題有興趣的研究者一些幫助。

在本研究中我們利用了資訊安全委外後各方面成本的增減，來檢視委外對於降低作業成本的成效，但是由回覆的答案可以看出有些填答者將委外花費的成本視為作業成本的增加，這與我們原先研究設計的概念有些許的誤差，為了能夠更加準確的測度委外為企業所帶來的效益，我們也建議往後的研究可以將委外之成本與沒有委外所需花費之成本作一個比較，如此將能夠更加精確的衡量出資安委外之效益。

在未來的研究中，也可以更加完整的探討企業在資訊安全方面有委外與沒有委外之差異，透過兩者的比較可以更清楚的觀察出委外的實際功效，也可以更加深入的比較兩者的長處及缺失，當然這需要投入較多的研究成本。

隨著研究的過程中與業界的互動以及結果的呈現，我們觀察到在不同的產業類別中，企業對於資訊安全委外的看法及定位存在著很大的差異，而這也很大程度的影響到企業委外之意願，往後之研究也可以朝不同產業之間的比較來著手，探討不同產業間對於資安委外意願存在差異之成因，或者是探討哪些產業更適合進行資訊安全的委外活動。

而本研究所考慮的模型，主要是觀察委外後所獲得的資安資源以及企業競爭優勢之關係，但是在業界實際進行資安委外時，涉及許多風險層面的考量，也就是說委外風險的高低程度對於委外的意願以及競爭優勢的獲取之間的關係可能有其影響，因此我們也建議未來的研究者能夠將風險列入考量，發展出更完整的研究模型來探究資安委外的相關議題，相信能夠為實務上帶來更大的助益。

參考文獻

Alpar, P., & Saharia, A. (1995). Outsourcing information system functions: an organization economics perspective. *Journal of Organizational Computing, 5*(3), 197-217.

Amit, R., & Schoemaker, P. (1993). Strategic assets and organizational rent. *Strategic management journal, 14*(1), 33-46.

Anderson, J., & Gerbing, D. (1988). Structural equation modeling in practice: A review and recommended two-step approach. *Psychological bulletin, 103*(3), 411-423.

Aral, S., & Weill, P. (2007). IT assets, organizational capabilities and firm performance: How resource allocations and organizational differences explain performance variation. *Organization Science, 18*(5), 763-780.

Axelrod, C. (2004). *Outsourcing information security*: Artech House Publishers.

Backhouse, J., & Dhillon, G. (1996). Structures of responsibility and security of information systems. *European Journal of Information Systems, 5*(1), 2-9.

Barney, J. (1986). Strategic factor markets: expectations, luck, and business strategy. *Management science, 32*(10), 1231-1241.

Barney, J. (1991). Firm resources and sustainable competitive advantage. *Journal of management, 17*(1), 99-120.

Bentler, P. (1995). *EQS structural equations program manual*: Multivariate Software.

Bentler, P. (2006). EQS 6 structural equations modeling program manual. Encino, CA: Multivariate Software: Inc.

Bentler, P., & Bonett, D. (1980). Significance tests and goodness of fit in the analysis

of covariance structures. *Psychological bulletin, 88*(3), 588-606.

Boukhonine, S., Krotov, V., & Rupert, B. (2005). Future security approaches and biometrics. *Communications of the Association for Information Systems 16*, 937-966.

Bruder, C. (2006). Outsourcing information security. *Smart Business Detroit*.

Bussolati, U., & Martella, G. (1981). Treating data privacy in distributed systems. *Information & Management, 4*(6), 305-315.

Byrne, B. (2006). *Structural equation modeling with EQS: Basic concepts, applications, and programming*: Lawrence Erlbaum.

Carr, N. (2003a). It Doesn t Matter. *Harvard Business Review, 81*(5), 41-49.

Carr, N. (2003b). Why IT doesn't matter anymore. *Harvard Business Review, 81*(5).

Cattela, R. (1981). Information as a corporate asset. *Information & Management, 4*(1), 29-37.

Chan, Y.-C. (2005). *A Study of Factors Affecting Information Systems Security Outsourcing.* National Chung Cheng University.

Chang, H. (2002). A model of computerization of manufacturing systems: an international study. *Information & Management, 39*(7), 605-624.

Cheon, M., Grover, V., & Teng, J. (1995). Theoretical perspectives on the outsourcing of information systems. *Journal of Information Technology, 10*(4), 209-219.

Claver, E., Gonzalez, R., Gasco, J., & Llopis, J. (2002). Information systems outsourcing: reasons, reservations and success factors. *Logistics Information Management, 15*(4), 294-308.

Conner, K. (1991). A historical comparison of resource-based theory and five schools of thought within industrial organization economics: do we have a new theory of the firm? *Journal of management, 17*(1), 121.

Cronk, J., & Sharp, J. (1995). A framework for deciding what to outsource in information technology. *Journal of Information Technology*, *10*(4), 259-267.

D'Arcy, J., & Hovav, A. (2007). Deterring internal information systems misuse. *Communications of the ACM, 50*(10), 117.

Deshpande, D. (2005). *Managed security services: an emerging solution to security*.

Dewar, R., & Dutton, J. (1986). The adoption of radical and incremental innovations: an empirical analysis. *Management science, 32*(11), 1422-1433.

Dierickx, I., & Cool, K. (1989). Asset stock accumulation and sustainability of competitive advantage. *Management science*, 1504-1511.

Due, R. T. (1992). The Real Costs of Outsourcing. *Information Systems Management, 9*(1), 78-81.

Duffy, N. (1980). Countdown services: Fire and its aftermath in a computer bureau. *Information & Management, 3*(3), 103-111.

Duncan, N. (1998). *Beyond opportunism: a resource-based view of outsourcing risk*.

E&Y (2009). *The Global Information Security Survey*: Ernst & Young.

Fornell, C., & Larcker, D. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of marketing research*, 39-50.

Gartner (2007). *Defining the Security-as-a-Service Market*.

Gilbert, F. (1993). Issues to consider before outsourcing. *The National Law Journal, 16*(11), S7.

Grant, R. (1991). "The Resource-Based Theory of competitive advantage: Implications for strategy formulation.". *California Management Review, 33*(3), 114-135.

Grover, V., Cheon, M., & Teng, J. (1996). The effect of service quality and partnership on the outsourcing of information systems functions. *Journal of Management*

Information Systems, 12(4), 116.

Grover, V., Joong Cheon, M., & Teng, J. (1994). A descriptive study on the outsourcing of information systems functions. *Information & Management, 27*(1), 33-44.

Hair, J., Anderson, R., Tatham, R., & Black, W. (1998). *Multivariate data analysis*. New Jersey, NJ: Prentice-hall.

Hair Jr, J., Anderson, R., Tatham, R., & Black, W. (1995). *Multivariate data analysis: with readings*: Prentice-Hall, Inc. Upper Saddle River, NJ, USA.

Harris, S., & Katz, J. (1991). Firm size and the information technology investment intensity of life insurers. *MIS quarterly, 15*(3), 333-352.

Hitt, M., & Ireland, R. (1986). Relationships among corporate level distinctive competencies, diversification strategy, corporate structure and performance. *Journal of Managcmmt Studies, 23*(4), 0022-2380.

Hoyle, R., & Panter, A. (1995). Writing about structural equation models. *Structural equation modeling: Concepts, issues, and applications*, 158-176.

Hunt, S. (2001). Market overview: Managed security services, from http://bt.counterpane.com/giga3.pdf

IBM (2006). IBM Information Security Reference Model, from web.esaugumas.lt/.../IBM_ISF%20presentation.%2016-17%20Nov%202006%20(RRT).pps

Icove, D., Seger, K., & VonStorch, W. (1995). Computer Crime. A Crimefighter's Handbook. *No.: ISBN 1-56592-086-4*, 455.

IDC (2007). *Worldwide IT Security Software, Hardware, and Services 2007-2011 Forecast：The Big Picture*

James, L., Mulaik, S., & Brett, J. (1982). *Causal analysis: Assumptions, models, and data*: Sage Publications, Inc.

Kankanhalli, A., Teo, H., Tan, B., & Wei, K. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management, 23*(2), 139-154.

Kline, R. (1998). Principles and practice of structural equation modeling New York: Guilford Press.

Krell, K., & Matook, S. (2009). Competitive advantage from mandatory investments: An empirical study of Australian firms. *Journal of Strategic Information Systems, 18*(1), 31-45.

Lee, J., Huynh, M., Kwok, R., & Pi, S. (2003). IT outsourcing evolution---: past, present, and future.

Lee, J., & Kim, Y. (1999). Effect of partnership quality on IS outsourcing success: conceptual framework and empirical validation. *Journal of Management Information Systems, 15*(4), 61.

Lee, S. (2003). Business use of Internet-based information systems: the case of Korea. *European Journal of Information Systems, 12*(3), 168-181.

Lockman, A., & Minsky, N. (1984). Designing financial information systems for auditability. *Journal of Management Information Systems, 1*(1), 50-62.

McFarlan, F., & Nolan, R. (1995). How to manage an IT outsourcing alliance. *Sloan Management Review, 36*(2), 9.

Melville, N., Kraemer, K., & Gurbaxani, V. (2004). Review: Information technology and organizational performance: An integrative model of IT business value. *MIS quarterly*, 283-322.

Minoli, D. (1995). *Analyzing outsourcing: reengineering information and*

communication systems: McGraw-Hill, Inc. New York, NY, USA.

Mishra, D. (2006). The role of certification in service relationships: theory and empirical evidence. *Journal of Retailing and Consumer Services, 13*(1), 81-96.

Nunnally, J. (1978). *Psychometric theory* New York: McGrew-Hill

Nunnally, J., Bernstein, I., & Berge, J. (1994). *Psychometric theory*: McGraw-Hill New York.

Penrose, E. (1959). The Theory of the Growth of the Firm (1995): Oxford: Oxford University Press.

Peteraf, M. (1993). The cornerstones of competitive advantage: a resource-based view. *Strategic management journal, 14*(3), 179-191.

Poppo, L., & Zenger, T. (1998). Testing alternative theories of the firm: transaction cost, knowledge-based, and measurement explanations for make-or-buy decisions in information services. *Strategic management journal, 19*(9), 853-877.

PWC (2008). *The Global State of Information Security Survey*.

PWC (2010). *The Global State of Information Security Survey*.

Quinn, J. (1992). *Intelligent enterprise: A knowledge and service based paradigm for industry*: Free Pr.

Richardson, R. (2008). *CSI Computer Crime and Security Survey*: Computer Security Institute.

Richmond, W., & Seidmann, A. (1993). Software development outsourcing contract: Structure and business value. *Journal of Management Information Systems, 10*, 57-57.

Roy, V., & Aubert, B. (2000). *A resource based view of the information systems sourcing mode*.

Rubin, P. (1973). The expansion of firms. *The Journal of Political Economy, 81*(4), 936-949.

Rumelt, R. (1974). *Strategy, structure, and economic performance*: Not Avail.

Sanchez, R., Heene, A., & Thomas, H. (1996). Introduction: Towards the theory and practice of competence-based competition. *Dynamics of Competence-Based Competition. Oxford, UK: Pergamon*, 1–35.

Segars, A., & Grover, V. (1993). Re-examining perceived ease of use and usefulness: A confirmatory factor analysis. *MIS quarterly, 17*(4), 517-525.

Sethi, V., & King, W. (1994). Development of measures to assess the extent to which an information technology application provides competitive advantage. *Management science, 40*(12), 1601-1627.

Shim, J., Varshney, U., Dekleva, S., & Nickerson, R. (2007). Wireless Telecommunications Issues: Cell Phone TV, Wireless Networks in Disaster Management, Ubiquitous Computing, and Adoption of Future Wireless Applications. *Communications of the Association for Information Systems, 20*(1), 29.

Siponen, M., Baskerville, R., & Heikka, J. (2006). A Design Theory for Secure Information Systems Design Methods. *Journal of the Association for Information Systems, 7*(11), 31.

Siponen, M., & Oinas-Kukkonen, H. (2007). A review of information security issues and respective research contributions. *ACM SIGMIS Database, 38*(1), 80.

Smith, M. (1989). Computer security- threats, vulnerabilities and countermeasures. *INF. AGE., 11*(4), 205-210.

Srivastava, R., Shervani, T., & Fahey, L. (1998). Market-based assets and shareholder value: a framework for analysis. *The Journal of Marketing, 62*(1), 2-18.

Stevenson, H. (1976). Defining corporate strengths and weaknesses. *Sloan Management Review, 17*(3), 51-68.

Straub Jr, D., & Nance, W. (1990). Discovering and disciplining computer abuse in organizations: a field study. *MIS quarterly, 14*(1), 45-60.

Sumner, M. (1986). An assessment of alternative application development approaches. *Information & Management, 10*(4), 197-206.

Tanaka, J. (1993). Multifaceted conceptions of fit in structural equation models. *Testing structural equation models, 10*, 39.

Teng, J., Cheon, M., & Grover, V. (1995). Decisions to outsource information systems functions: testing a strategy-theoretic discrepancy model. *Decision Sciences, 26*(1), 75-103.

Thompson, A., & Strickland, A. (1983). *Strategy formulation and implementation: tasks of the general manager*: Business Publications.

Von Solms, R., & van der Haar, S. (1994). A framework for information security evaluation. *Information & Management, 26*(3), 143-153.

Wade, M., & Hulland, J. (2004). Review: T HE Resource-Based View AND Information Systems Research: Review, Extension, AND Suggestions FOR Future Research. *MIS quarterly, 28*(1), 107-142.

Wernerfelt, B. (1984). A resource-based view of the firm. *Strategic management journal*, 171-180.

West, S., Finch, J., & Curran, P. (1995). Structural equation models with nonnormal variables: Problems and remedies. *Structural equation modeling: Concepts, issues, and applications*, 56–75.

Yang, S., Chatterjee, S., & Chan, C. (2004). Wireless communications: myths and reality. *Communications of the Association for Information Systems, 13*(1), 39.

Zafar, H., & Clark, J. G. (2009). Current State of Information Security Research In IS. *Communications of the Association for Information Systems, 24*.

Zhou, K., Brown, J., & Dev, C. (2009). Market orientation, competitive advantage, and performance: A demand-based perspective. *Journal of business research, 62*(11), 1063-1070.

Zviran, M., & Erlich, Z. (2006). Identification and authentication: technology and implementation issues. *Communications of the Association for Information Systems, 17*(1), 4.

王義智 (2009). *剖析台灣中小企業資安投資現況*: Market Intelligence & Consulting Institute, MIC.

附錄

附錄一　問卷調查表[5]

資訊安全委外風險及成效調查

各位先生、女士，您好：

本研究主要在探討資訊安全委外，希望藉由此問卷，調查企業採用資訊安全委外時的風險因子,以及探索採用資訊安全委外的成效。研究結果將可提供企業與政府機關，作為進行資訊安全服務委外決策參考依據。

本問卷內容僅供作學術整體分析之用，絕對不會對外公開個別組織之資料。懇請您花費約十五分鐘的時間填寫此一問卷，並期待能早日收到您的寶貴回應。您的每項意見將對本研究有莫大的幫助。為感謝您的協助，我們很樂意將研究成果與您分享。

敬祝

健康順心

台灣大學資訊管理研究所
指導教授　許瑋元 博士
研究生　詹偉銘
研究生　陳禹帆

[5] 由於此問卷前兩部份為另一位研究者的部份，故在此不特別列出。

第三部分：資訊安全委外成果

此部分旨在了解貴公司在將資訊安全委外之後，在資訊安全方面有何種程度的改變以及影響，請您依貴公司實　際委外後的情況填答，若貴公司曾經無委外經驗者，第三部分免填答，請從 74. 開始繼續作答。

I.　資訊安全資源

資訊安全資產 請描述貴公司將資訊安全委外(部份或全部)之後，你同意或者不同意組織具有下列的情況	非常不同意	不同意	有點不同意	普通	有點同意	同意	非常同意
8.　透過委外，本公司能使用或擁有新穎的資訊安全軟、硬體設備							
9.　透過委外，本公司能使用或擁有安全的傳輸及儲存設備							
10. 資訊安全委外廠商在顧客遇到任何問題時，能夠熱心的協助解決							
11. 資訊安全委外廠商所承諾過會完成的事項，能夠準時完成							
12. 資訊安全廠商所派遣的工作人員，看起來具有專業形象							
13. 委外廠商若遇到任何未預期的問題，會儘快告知，以共謀對策							
14. 根據過去及現在的經驗，本組織與委外廠商互信程度非常高							
15. 本組織與委外廠商共事，是件很高興的事							

資訊安全能力 請描述貴公司將資訊安全委外(部份或全部)之後，你同意或者不同意組織具備有下列的資訊安全能力	非常不同意	不同意	有點不同意	普通	有點同意	同意	非常同意
16. 透過委外，本公司擁有使用最新資訊安全科技的能力							
17. 透過委外，本公司能夠使用或擁有因應新的攻擊手法之技術							
18. 透過委外，本公司能夠保護所使用的資訊系統的安全							
19. 透過委外，本公司擁有良好的資訊安全架構							
20. 透過委外，本公司擁有完整的資訊安全政策、程序及規範							
21. 透過委外，本公司的員工擁有良好的資訊安全素養							
22. 透過委外，本公司能夠擁有安全監控的能力							
23. 當資安意外發生時，本公司能夠辨識出原因							
24. 當資安意外發生後，本公司能夠做出適當回應，排除事件							

II. 競爭優勢

低成本 請描述貴公司將資訊安全委外(部份或全部)之後，對於公司的各項成本產生了何種程度之影響	大幅增加	適度增加	略為增加	沒有改變	略為減少	適度減少	大幅減少
25. 用以維持公司資訊安全之人力成本							
26. 管理各項資訊安全活動之成本							
27. 獲取各項資訊安全科技之成本							
28. 公司內各部門與資訊(安全)部門之溝通協調成本							

差異化 請描述貴公司將資訊安全委外(部份或全部)之後，對於公司與外界的關係產生了何種程度的影響	非常不同意	不同意	有點不同意	普通	有點同意	同意	非常同意
29. 相較於其他競爭者，本公司更能夠接觸或獲取最新的資訊安全資源							
30. 相較於其他競爭者，本公司對於資安資源的使用更有效率							
31. 相較於其他競爭者，本公司更能夠重新聚焦於核心業務							
32. 相較於其他競爭者，我們與資訊安全委外廠商的合作帶來了較佳的聲譽							
33. 相較於其他競爭者，我們提供給客戶更安全的服務感受							
34. 其他競爭者很難達成我們將資訊安全委外所帶來的效益							
35. 其他競爭者很難複製我們的資訊安全委外經驗							
36. 其他競爭者很難複製我們的品牌聲譽							

III. 資訊安全委外的程度比例

下列各個項目，請根據貴公司將其委外給外界廠商的程度，給出一個適當地百分比：	完全不委外	極少委外	部份委外	大部份委外	完全委外
37. 實體安全(包含公司的機房、資料儲存中心等等，防止遭受天災或人為的襲擊)					
38. 人員安全(如人力安全、員工資安教育訓練)					
39. 應用系統安全(如系統建置之安全與維護)					
40. 身份認證、存取管理(如存取權限控制、身份管理)					
41. 交易及資料完整性(如企業交易流程安全、資料庫安全、訊息保護)					
42. 降低威脅(如弱點偵測、網路管理、內容過濾檢查、資安事件管理)					
43. 資料保護(如隱私管理策略及規範)					

44. 公司治理(如資訊安全架構、資安政策等方向制定、資安風險管理)					
45. 其他 _____					

第四部分:組織概況

46. 貴公司(機關)的員工總數約為

□100 人以下 □100 人~500 人 □500~1000 人 □1000~ 5000 人 □5000~1 萬人 □1 萬人以上

75. 貴公司(機關)的 98 年度營業淨額約為(新台幣)

□10 億以下 □10 億~50 億 □50 億~100 億 □100 億~500 億 □500 億~1000 億 □1000 億以上

76. 貴公司(機關)所屬的產業類別

□政府機關 □金融保險 □電子資訊 □傳統製造
□營建土木 □批發零售 □法律會計 □醫療保健
□物流倉儲 □文教服務 □大眾傳播 □其他(請說明)_____

77. 貴公司(機關)資訊部門已成立幾年？

□1 年以內 □1~3 年 □4~5 年 □6~9 年 □10 年以上

78. 貴公司(機關)資訊部門(或資訊專業人員)的人數大約：

□10 人以下 □10~50 人 □50 人~100 人 □100~200 人 □200 人~500 人 □500 人以上

79. 貴公司(機關)每年的**資訊總預算**大約為: (新台幣)

□10 萬以下 □10~100 萬 □100~1000 萬 □1000 萬~1 億 □1000 萬~1 億 □1 億~10 億 □10 億以上

，大約佔**公司總預算** _____% □不清楚

80. 貴公司(機關)每年的**資訊安全總預算**大約為: (新台幣)

□1 萬以下 □1 萬~10 萬 □10~50 萬 □50 萬~100 萬 □100 萬~1000 萬 □1000 萬以上

，大約占**資訊總預算**_____% □不清楚

81. 貴公司(機關)每年的**資訊安全委外預算**大約為 (無委外者免填答):

□1 萬以下　□1~5 萬　□5~10 萬　□10 萬~20 萬　□20 萬~50 萬　□50 萬~100 萬　□100 萬以上

，大約佔**資訊安全總預算** _____% □不清楚

若您有意了解研究結果，請於填寫完畢後留下連絡的 E-mail Address，我們將為您寄出研究的結果。

Email：_____

問卷到此結束， 謝謝您的熱心填答！