企業導入 BS7799 資訊安全管理系統之關鍵成功因素－以石化產業為例

黃士銘
中正大學會計與資訊科技學系

張碩毅
中正大學會計與資訊科技學系

蘇耿弘
中國石油股份有限公司煉製研究所

摘要

隨著電子交易的發展，資訊安全逐漸受到企業重視。「BS 7799」是由英國國家標準協會(BSI)於 1995 年所制定；企業只要做到 BS 7799 的要求，並通過獨立稽核機構評鑑，便可獲頒 BS7799 資訊安全認證。因此，可向其客戶與合作夥伴宣告，該企業網路內與他們相關的資料都受到適當的保護，而且該企業整體的安全度也值得信任。國外許多石化公司紛紛建立供應鏈體系及電子市集，以期降低交易成本、掌握市場趨勢及交換市場訊息。而國內由經濟部工業局推動「石化產業電子化標準推動計劃」，積極輔導業者成立電子化產銷體系，以因應國際化之電子交易趨勢。另外石化業者為即時掌握生產狀況及監控工廠運作情形，利用網路、控制介面及數據擷取等技術將程控資訊與管理資訊系統整合，為管理上帶來極大的便利。但相對地因資訊安全問題所造成的風險會更加嚴重，由於石化原料及產品多屬易燃物，其所造成的影響不僅是資訊及經濟的損失，嚴重時可能造成公共安全問題，使得石化產業的資訊安全更應受到重視。本研究以 BS 7799 為基礎，針對國內石化產業的資訊安全議題及現況進行調查，以瞭解該產業資訊安全狀況及其差異。並利用區別分析找出影響石化產業導入資訊安全管理機制的關鍵成功因素。研究發現其關鍵成功因素分別為安全防護、資訊安全技能、供應商、法令規章、競爭壓力、商業夥伴影響、安全事件處理、員工參與、電腦化程度、高階主管支持、組織規模及安全風險程度等因素。

關鍵字：BS7799、ISO17799、資訊安全管理、關鍵因素、石化產業

Critical Success Factors for Implementing BS7799 Information Security Management System - Based on Petrochemical Industry

Shi-Ming Huang
Department of Accounting and Information Technology, National Chung Cheng University

She-I Chang
Department of Accounting and Information Technology, National Chung Cheng University

Keng-Hung Su
Chinese Petroleum Corp. Refining & Manufacturing Research Institute

ABSTRACT

Due to the rapid development of electronic commerce, maintaining information security in order to protect information assets is a key concern for every enterprise today. The BS7799 administrated by the British Standards Institute (BSI) since 1995, is a comprehensive system for implementing effective Internet security, by far, it is the most appropriate approach to best practices for information security management. By gaining the BS7799 certification, companies may assure customers and partners that their data, which being kept on the enterprise networks, will be secure and that the overall security of the enterprise is trustworthy. In the case of Petrochemical manufacturing industry, in Taiwan, many companies try to minimize the cost and achieve their gross profit margin by implementing e-commerce and applying vendors' supply chain management technology. The purpose of this study is to explore the critical success factors for the implementation of information security management system in the Petrochemical Industry. The results reveal that factors such as information security protection, information security skill, supplier, industrial regulations, competitive pressure, the interdependence among business partners, occupational health and safety practice, degree of computerization, top management support, scale of organization and tolerant of risk are crucial to the success for implementing the business electronically.

Keyword: BS7799, ISO17799, Information Security Management, Critical Success Factors, Petrochemical Industry

壹、緒論

安全是網路交易最重要的議題之一，電子商務的交易安全必須考慮資料來源、身份識別、資料完整性、資料保密性及存取控制等安全考量。為了防範交易資料遭人偽造、篡改、洩密、冒送假資料或非法取得資料等威脅，解決之道有資料辨別碼、數位簽章、採用加解密系統(如 DES、RSA 等)、防火牆及稽核追蹤等機制，以確保資料在傳輸中有高度的可靠性。

這種從技術層面來考量的資訊安全策略，目前已有許多產品評估機制。最被普遍接受的有：80 年代美國國防部基於軍事電腦系統的保密需要所訂定 TCSEC（Trusted Computer System Evaluation Criteria）；另 90 年代初，英、法、德、荷四國針對 TCSEC 準則只考慮保密性的局限，聯合提出了包括私密性、完整性、可利用性概念的“資訊技術安全評價準則”簡稱 ITSEC（Information Technology Security Evaluation Criteria）；接著美國又聯合六國七方（美國國家安全局和國家技術標準研究所、加、英、法、德、荷）共同提出了資訊技術安全評價通用準則 CC（Common Criteria），CC 綜合了國際上已有的評審準則和技術標準的精華，訂出了框架和原則要求，作為取代 TCSEC 用於系統安全的評測的國際標準。而國際標準組織（ISO）於 1999 年 6 月接受了 CC 的安全準則標準，重新命名為 ISO/IEC 15408，並於同年 12 月發行實施。

然而資訊安全除了重視產品的安全機制及標準外，管理層面的機制亦不能忽略，因此英國標準協會 (British Standards Institute，簡稱 BSI)制定了資訊安全的標準 BS7799。它是一種資訊安全架構，讓組織以標準方法來管理資訊安全(Chao 2005)。BS7799 於 1995 年開始實施，企業只要作到 BS7799 的要求，並通過獨立稽核機構評鑑，便可獲頒 BS7799 資訊安全認證。因此，可向其客戶與合作夥伴宣告，該企業網路內與他們相關的資料都受到適當的保護，而且該企業整體的安全度也值得信任。許多機構有感於面臨的安全威脅有增無減，也開始依照 BS7799 的規定施行，當作最佳指導原則。其中「BS 7799」第一部份已在 2000 年 12 月 1 日成為 ISO/IEC17799 國際標準。ISO17799 制定完成後將會影響我國產業的發展，如同企業必須實施 ISO 9000 及 ISO 14000 一樣，例如在供應鏈體系中，在進行電子交易或資料交換時，會要求上下游廠商須獲得 ISO 17799 認證，以確保整個供應鏈體系中的資訊安全達到一定水準(Symantec 2000)。未獲得 ISO 17799 認證之企業，在 B2B 電子商務建置或者加入電子市集的競爭中將遭受壓力或排擠。因此資訊安全議題已不再是企業本身的問題，而會受到供應鏈上下游廠商及商業夥伴的影響。

企業要建構並制定完整的安全政策畢竟不是件容易的事，BS7799 資訊安全標準其所提供的資訊安全架構雖說適用於各行各業，但各個產業間均具不同的特性，其導入之關鍵成功因素及安全架構亦不相同，針對不同產業的特性提出導入資訊安全的架構及關鍵成功因素將會是未來研究的重要課題，這也是本研究要以 BS7799 為基礎探討石化產業導入資訊安全機制關鍵成功因素主要動機。

石化產業是工業的基礎，日常生活中許多的產品均由石化原料衍製而成。然而石化產業的景氣近年來一直在谷底徘徊，台灣業界亦免受到相當衝擊，2001 年台灣石化工業之艱困，充分表現在獲利率之下降，大約有一半的廠家之瀕臨損益平衡點邊緣，獲利的業者其盈餘亦不理想(台灣區石化公會 2001)。由於電子商務的興起國外許多石化公司紛紛建立供應鏈體系及電子市集，以期降低交易成本、掌握市場趨勢及交換市

場訊息。例如：BASF 公司除加入 Elemica 電子市集外，另建立了石化原料的入口網站。拜耳公司建立 Bayerone 網站提供石化產品電子交易平臺，亦加入 Elemica 電子市場進行大宗交易(沈倩如 2001)。國內方面為因應國外石化產業這種電子化交易及供應鏈體系的建置，由經濟部工業局積極推動「石化產業電子化標準推動計劃」，由資策會、台灣石化公會及工研院化工所合力執行，建立我國石化產業之電子化標準(XML)，計劃中未來國內石化產業電子交易將首先以 Hub 或市集型態出現(經濟部技術處 2002)。

由於我國石化產業電子化推動，加上為與國際石化產業接軌，跨企業或跨國之電子交易勢在必行，而企業之資訊安全是否符合國際資訊安全標準，關係著產業未來的生存。而近年來由於科技進步及管理上的需求，石化業者為即時掌握生產狀況及監控工廠運作情形，利用網路、控制介面及數據擷取等技術將程控資訊與管理資訊系統整合，為管理上帶來極大的方便(葉瑞萍 2001)。但相對地因資訊安全問題所造成風險會更加嚴重，由於石化原料及產品多屬易燃物，其所造成的影響不僅是資訊的損失，嚴重時可能造成公共安全問題(游輝祥 2001)。

基於以上原因，本研究以我國石化產業及其供應鏈體系做為研究對象，期對石化產業之資訊安全議題有所貢獻。本研究以 BS 7799 為基礎對石化產業及其供應鏈體系的資訊安全現況進行研究，並希望達到下列目的：(1)針對我國石化產業對於資訊安全的現況進行調查，以瞭解該產業資訊安全狀況及其差異。提供政府、資訊業者及學界輔導石化產業取得資訊安全認證之參考；(2)確立影響石化產業導入資訊安全管理機制之關鍵因素，以做為石化產業資訊安全實施之參考。

貳、文獻探討

一、石化產業與資訊科技

石油化學工業，一般簡稱「石化工業」；乃以石油及天然氣為出發原料之基礎（原料）工業，舉凡日常所見之塑膠類製品、清潔劑、農藥、化學肥料、橡膠、染料、塗料…等生活用品皆其衍生而來，十分符合聯產品之特性，故亦為化學工業中極具份量之一環。一般石化工業產業架構概分為：上游石化基本原料製造業、中游之中間石化原料製造業及下游之石化製品製造業。石化工業具備技術層次高及設備複雜的產業特性，因此在生產、管理及銷售的過程當中均大量依賴資訊科技的使用，以提昇生產產能、管理效率及降低操作成本，茲將石化產業利用資訊科技的目的及效能說明如下：

（一）生產及監控系統

由於石化廠的操作設備眾多，管線複雜，加上其原料及產品均具可燃性，跟其他產業相比其操作較困難且危險性高，因此在操作上大都仰賴分散式程控系統(DCS)的協助。近年來由於管理上的需求，管理階層為即時掌握生產狀況及監控工廠運作情形，利用網路、控制介面及數據擷取等技術將程控資訊與管理資訊系統整合，亦即利用內部網路即可監看及控制工廠的運作狀況，為管理上帶來極大的方便。但相對地因資訊安全問題所造成風險會更加嚴重，其所造成的影響不僅是資訊的損失，嚴重時可能造成公共安全問題(游輝祥 2001)。

（二）企業資源管理

石油化學工業主要產品都是聯產品，產品線複雜，加上原料、半成品及成品種類多樣，因此早期均採用 MRP 以解決企業長久以來的物料管理問題，但為了因應世界市場的變化，提高生產力且降低生產成本，於是就發展出了 MRP II，涵蓋了製造、設計、採購、配銷、生產、庫存、資金流動等各個層面。但隨著電腦硬體的快速發展，再加上產業的激烈競爭，MRP II 更已發展到成為 ERP 企業資源規劃系統，利用資訊系統將整個組織的作業流程貫穿起來，讓企業內部的各種資訊透明化、即時化，使得企業資源能更有效的運用。

（三）產銷管理

電子商務的興起,使得石化業產銷管理產生了變化，許多國外石化公司紛紛建立 B2B 供應鏈體系及電子市集，以期降低交易成本、掌握市場趨勢及交換市場訊息。由於線上供應鏈和網際網路市集使用增加,預計在 2006 年美國在電子商務市場中石油化學產業交易金額將達 3,010 億美元以上(沈倩如 2001)。國內業者亦在經濟部工業局的輔導下結合資策會、台灣石化公會及工研院化工所合力執行，期望早日建立電子化產銷體系。

二、資訊安全標準

關於資訊安全的標準，Eloff & Solms (2000)將之分為兩大類別，一種是以產品技術為安全規範的驗證標準，最常見的產品評估機制有 TCSEC、ITSEC 及 CC 等標準。另一種是以組織安全之管理流程為安全規範的認証標準，較著名的安全認証標準有 COBIT、COSO 及 BS7799 等標準。茲將主要資訊安全標準說明如下：

(一)產品技術驗證標準

1. TCSEC (Trusted Computer System Evaluation Criteria)

80 年代，美國國防部基於軍事電腦系統的保密需要，在 70 年代的基礎理論研究成果電腦保密模型（Bell & La padula 模型）的基礎上，制訂了"可信電腦系統安全評價準則"（TCSEC），其後又制訂了關於網路系統、資料庫等方面和系列安全解釋，形成了安全資訊系統體系結構的最早原則。

2. ITSEC (Information Technology Security Evaluation Criteria)

90 年代初，英、法、德、荷四國針對 TCSEC 準則只考慮保密性的局限，聯合提出了包括保密性、完整性、可用性概念的"資訊技術安全評價準則"（TISFC）。但是該準則中並沒有訂出綜合解決以上問題的理論模型和方案(Eloff & Solms 2000; 張振接 2001)。

3.CC (Common Criteria)

由美國發起提出了「資訊技術安全評價通用準則 CC（Common Criteria）」新評估準則的辦法。綜合了國際上已有的評審準則和技術標準的精華，訂出了框架和原則要求，作為取代 TCSEC 用於系統安全的評測的國際標準。1999 年 6 月 ISO 國際組織將 CC 納為 ISO/IEC 15408 標準，成為資訊技術安全評估的國際規範。

(二)組織安全之管理流程

1. COBIT (Control Objectives for Information and Related Technology)

COBIT 是國際電腦稽核學會（Information Systems Audit and Control Association, ISACA）發展並廣為應用之一套實用的資訊技術安全稽核與控制標準，用以提供使用者、資訊系統稽核人員執行任務時之參考架構，將於2005年11月更新至第四版。COBIT 4.0 在控制目標、管理之指導方針等部份已作適當之更新，如第四版的高層控管目標雖仍為34項，但實質內容已不同於第3版的34項高層控管目標，新版之更新集中於資訊科技管理、企業需求、修訂術語與原則使其與其它資訊安全規範一致....等方向。

2. COSO (The Committee of Sponsoring Organizations)

COSO 是一國際「內部控制稽核規範」，其目標原本是藉由專注在組織的管理（corporate governance）、道德的實踐（ethical practices）、及內部控制（internal control）來改善財務報表的品質，但以財務控制為重點的傳統的理論已經實質上逐漸擴大其範圍，COSO 的架構不再只是評估如責任劃分等的 hard controls，也包含了如員工的能力和專業性等的 soft controls。特別是在美國，這些概念已被許多的組織所接受，尤其是政府的部門。針對近年來受到高度重視的風險管理，COSO 於 2001 年研究發展出企業風險管理(Enterprise Risk Management, ERM)架構，讓管理者可以快速地運用該架構，來衡量及改善組織的風險管理流程。

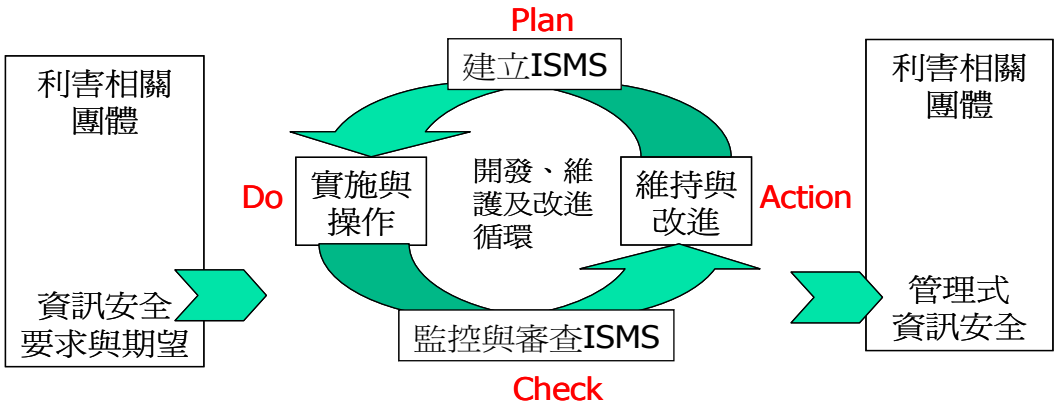
3. BS7799

BS7799 於 1995 年 2 月由英國標準協會(British Standards Institution)提出並經多次改版，為目前國際上最知名的安全規範。BS7799 可以適用於各種產業與所有的組織與機構，是一個非常詳盡甚至有些複雜的資訊安全標準。它廣泛地涵蓋了所有的安全議題，包含了所有面向的最先進企業安全政策，從安全政策的擬定、安全責任的歸屬、風險的評估、到定義與強化安全參數及存取控制，甚至防毒的策略(Trcek 2003; Kankanhalli et. al. 2003)。

BS7799 大致上可分成兩個部分，Part 1 為資訊安全管理作業要點(Code of practice for information security systems，以下簡稱 BS7799-1)，它設立了產業最佳的管理資訊安全準則，此準則僅供指導之用，提供廣泛性的安全控制措施，但不作為評鑑與認證的依據。BS7799-1 包括 10 個控管要點，36 個控制目標及 127 個控制措施，分別為安全政策(含 2 個項目)、安全組織(含 10 個項目)、資產分類與管制(含 3 個項目) 、人員安全(含 10 個項目) 、實體與環境安全(含 13 個項目)、通訊與操作管理(含 24 個項目) 、存取控制(含 31 個項目) 、系統開發與維護(含 18 個項目) 、企業永續運作管理(含 5 個項目)及遵行(含 11 個項目)等。BS7799-1 於 2000 年通 ISO 國際標準組織的審議，頒佈為國際標準 ISO/IEC 17799，而我國中央標準局亦於 2003 年參考 BS7799-1 規範通過 CNS17799 及 CNS17800，作為國內資訊安全實施及認證之規範。

Part 2 則是資訊安全管理系統要求(Specification for Information Security Management Systems - ISMS，以下簡稱 BS7799-2)，即資訊安全管理系統詳細說明書，提供資訊安全管理系統(ISMS)建立實施與書面化的具體要求，可做為正式驗證的標準。BS7799-2 於 2002 年 9 月 5 日正式改版，引進循環不斷的 PDCA 的機制，如圖一所示，藉由不斷的稽核、檢討、規劃及強化讓企業的資訊安全等級不斷提升與改進(BSI 2002 - Part2)。 BS7799-2 原希望在 2001 年底以前通過 ISO 國際標準組織審核頒布(ISO/IEC 17799-2)，但截至目前為止尚未通過。BS7799 不是技術標準，而是管理標準，

它處理的是 IT 系統中非技術內容的管控。這些內容與人員、流程、實體安全及一般意義上的安全管理有關，強調的是均衡管理。企業組織可藉由 BS7799 管理標準評鑑其本身的安全，亦可藉由 BS7799 的驗證證明企業確實依照 BS7799 所敘述的相關控制措施建立 ISMS。



圖一 BS7799 PDCA 模式

四、我國資通安全相關法令

受到國內外資訊安全事件頻傳以及 ISO 17799 制定通過的影響，而行政院及相關主管機關為防範因資訊安全事件而危及國家安全、人民損失及產業發展，因此以 ISO 17799 及 BS7799-2 為基礎制定了一系列的資通安全的相關法令，將嚴格要求國內政府機關與產業界配合執行。我國資通安全相關法令及措施如下：

（1）「行政院及所屬各機關資訊安全管理規範」－行政院為推動各機關強化資訊安全管理，建立安全及可信賴之電子化政府，確保資料、系統、設備及網路安全，保障民眾權益，以 BS7799 為基礎於 88 年特訂定「行政院及所屬各機關資訊安全管理規範」，要求行政院所屬各部會及事業單位確實遵守，並成立「行政院資通安全稽核服務團」對行政機關及事業單位進行資訊安全稽核工作(行政院研考會, 2000)。

（2）「CNS 17799」資訊安全國家標準之制定－為因應產業需求及加速我國資訊安全相關國家標準之制定，中央標準局已於 91 年參考 BS 7799 規範通過 CNS17799 及 CNS17800，作為國內資訊安全實施及認證之規範(經濟部標準檢驗局 2002)。

（3）財政部於 91 年底公佈「公開發行公司建立內部控制制度處理準則」，其中新增資通安全檢查之控制規定，將使得上櫃上市公司考量依據 ISO17799/ BS7799/ CNS17799 執行資通安全檢查控制(財政部 2002)。

五、影響企業資訊安全的因素

許多文獻探討影響企業資訊安全的因素，其中 Huang et. al. (2000) 從資訊科技、人為因數、外在環境及組織內部等構面探討不同類型之金融機構之安全考量因素，發現不同類型之金融機構在採用軟體系統、保障硬體安全、以特殊作業系統控制、高階

主管支持、人事政策、定義組織網路安全、組織政策以及組織特性等因素時，有顯著的差異。

曾淑惠(2002)以BS7799-2為量表調查本國銀行及外商銀行在資訊安全運用上最重視的三個控管要點依序為「存取控制」、「實體與環境安全」與「系統開發與維護」，而最需要加強是「安全組織」、「遵行」、「安全政策」方面的運用。

BSI (BSI 2000 - Part1)從以往的經驗來說明，在組織中成功地實施資訊安全保護，以下因素非常關鍵：(1)反映組織目標的安全政策、目標以及活動；(2)與組織文化一致的實施安全保護的方法；(3)來自管理層的實際支援和承諾；(4)對安全要求、風險評估以及風險管理的深入理解；(5)向全體管理人員和雇員有效地推銷安全的理念；(6)向所有雇員和承包商宣傳資訊安全政策的指導原則和標準；(7)提供適當的訓練和教育；(8)一個全面的平衡的測量系統，用於評估資訊安全管理的執行情況和反饋意見和建議，以便進一步改進。

Caminada (1998) 等學者進行荷蘭企業網路安全調查，提出企業網路安全的關鍵為：(1)定期修補安全漏洞；(2)安全防護設備的規劃、測試及維護；(3)明確的安全政策及執行程序；(4)安全偵測機制；(5)人為因素包括安全相關知識及系統管理者的工作負荷。

吳俊德(2002)以質性研究方式，針對幾種不同類型的資訊安全管理專家以ISO17799為議題進行深度訪談，同時匯集整理相關的研究報告及文獻，發展出8項關鍵重點，分別為：(1)高階主管支持；(2)以風險管理為基礎；(3)風險評估採定量與定性並存；(4)安全政策應以整體制度的設計及容易落實為主；(5)管理重於技術；(6)備援作業不可輕忽；(7)遵循相關法令規定；(8)BS7799 的 127 控制項，是資訊安全管理的精華，適用於各種產業。

參、研究方法

依據研究之目的，本研究以兩階段來進行。第一階段先經由文獻探討提出研究架構雛型及問卷初步內容，其次再與石化業界及學者專家進行訪談，以了解石化公司其建置資訊安全機制時，實際考慮之因素為何? 及其以 BS7799 為基礎的資訊安全架構為何?經由深入訪談了解建構資訊安全之關鍵因素，以作為修改研究架構雛型及問卷內容的依據。研究架構及問卷內容確立後，即進行第二階段之問卷調查，並且利用統計分析方式將問卷所得之結果進行研究模式與假說驗證，並提出影響石化產業導入資訊安全機制的關鍵因素。以下即詳述研究架構雛型建立、研究構面及變數、研究假說、問卷調查。

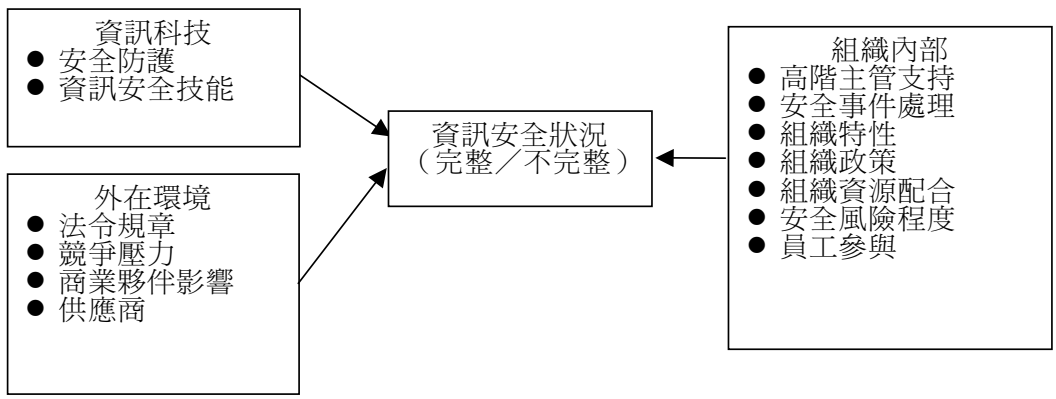
一、研究架構

根據研究目的及國內外相關文獻之探討(e.g. Caminada 1998; Huang et al. 2000; BSI 2002)及透過專家訪談結果，整理出企業在資訊安全實施上所考量的各相關因素，並依據其特性歸納出資訊科技、外在環境及組織內部等三個構面。本研究的三個構面主要是參考 Huang et al.（2000）之歸類而來。

Huang et al.（2000）依據文獻及專家訪談將影響資訊安全的構面分為「資訊科技」、「組織內部」、「外在環境」及「人為因素」，而本研究依據專家訪談後僅採用「資訊科技」、「組織內部」及「外在環境」等三個構面，主要考量係依據文獻中影響企業資

訊安全的「人為因素構面」的因素有安全相關知識、系統管理者的工作負荷(Caminada 1998)、第三方存取(BSI 2002)及 駭客入侵(Solms 2001)等, 這些因素均可歸類至「資訊科技」、「組織內部」及「外在環境」等三個構面中, 如本論文中「資訊科技構面」中產品安全及資訊安全技能等因素即是探討安全相關知識及駭客入侵等因素;「組織內部構面」中組織資源配合因素即是探討系統管理者的工作負荷因素; 而「外在環境構面」中供應商及商業夥伴影響等因素即探討第三方存取因素。

因此本研究仍採用「資訊科技」、「組織內部」、「外在環境」及「人為因素」等做為研究構面，故本研究之研究架構雛型如圖二，研究架構中資訊科技構面包括安全防護、資訊安全技能等二項因素；外在環境構面包括法令規章、競爭壓力、商業夥伴影響、供應商等四項因素；而組織內部構面包括高階主管支持、安全事件處理、組織特性、組織政策、組織資源配合、安全風險程度及員工參與等七項因素。



圖二　研究架構雛型

二、研究構面及變數

因研究進行階段, 並未找到與石化產業相關連的資訊安全研究論文, 因此主要參考 Huang et. al.（2000）、Caminada（1998）及 BSI 之因素為基礎, 並透過三位專家訪談結果所整理出來, 專家中二位為石化公司之資訊主管, 另一位為學校教授, 用以支持本研究所提出之導入 BS7799 關鍵成功因素。其中區間尺度採用 Likert 五點量尺來衡量，而安全風險程度變數採用國家資通安全應變中心之分類分成四級。因變數部分則採用行政院依據 BS7799 所編製的資通安全自我檢測調查 B 類問卷(行政院研考會 2000)共 31 個問項進行衡量，每個問項以「完全達成」、「部份完成」、「建置中」、「規劃中」、「尚未考慮」(分數由 5 分到 1 分)方式來調查資訊安全狀況，平均分數在 4 分(含)以上則歸類為「完整」，其他則歸類為「不完整」。

雖然 BS7799 共有 127 控制項，行政院以此設計為自行檢查表，針對政府機關及國營企業進行資安調查。但調查結果顯示，對於民間企業而言，127 個題項太多，致填答意願不高，於是行政院召集 BSI(英國標準協會)及國內數位資安專家學者將 127 個題項濃縮成 31 個題項，以提昇填答意願，此問卷係 BSI 及國內資安專家所設計，應具備相當程度之內容效度。且研究當時並未從文獻上找到有關衡量資訊安全狀況的工具或方法，因此本研究才採用資通安全自我檢測調查 B 類問卷做為衡量工具。此外不同的公司對於每個題項的權重可能有不同看法，為使衡量的標準一致，故假設 31 個題項中每個題項權重均相同來進行衡量。另採用平均值 4 分以上做為資安狀況完不

完整，係平均值 4 分以上代表企業平均達到「部份完成」的以上階段，具備基本的資安防護能力，因此以歸類為「完整」，反之則歸類為「不完整」。問卷各問項、變數來源及衡量尺度的關係，如表一及附錄所示。

表一 研究變數

	構面	變數	變數型態	文獻出處
自變數	資訊科技	安全防護	區間尺度	Huang et al.(2000), Caminada (1998), Eloff & Solms (2000)
		資訊安全技能	區間尺度	Huang et al.(2000), Caminada (2000)
	外在環境	法令規章	區間尺度	Huang et al.(2000), 行政院研考會(1999)
		競爭壓力	區間尺度	Cohen (1998), Premkumar (1994)
		商業夥伴影響	區間尺度	Symantec (2000), Premkumar (1994)
		供應商	區間尺度	Powell (1993), Huang et al.(2000)
	組織內部	高階主管支持	區間尺度	Huang et al.(2000)、Eloff & Solms (2000)
		安全事件處理	區間尺度	Solms (2001)、行政院研考會(1999)
		組織特性	區間尺度	Caminada (1998), Huang et. al.(2000)
		組織政策	區間尺度	Caminada (1998)
		組織資源配合	區間尺度	Huang et al.(2000)、Symantec (2000)
		安全風險程度	名目尺度	行政院研考會(2000)
		員工參與	區間尺度	Huang et al.(2000), BSI (2000 Part1)
因變數	資訊安全	資訊安全程度	名目尺度	行政院研考會(2000), BSI (2002 Part2)

二、研究假說

根據以上之文獻探討，及本研究之理論架構與目的提出研究假說，整理成表二 ，以便進行資料分析後之驗證。

表二 研究假說

研究假說一：資訊科技的構面考量對於組織資訊安全程度的完整性與否有顯著差異。	
H1a	安全防護的因素對於組織資訊安全程度的完整性與否有顯著差異。
H1b	資訊安全技能的因素對於組織資訊安全程度的完整性與否有顯著差異。
研究假說二：外在環境的構面考量對於組織資訊安全程度的完整性與否有顯著差異。	
H2a	法令規章的因素對於組織資訊安全程度的完整性與否有顯著差異。
H2b	競爭壓力的因素對於組織資訊安全程度的完整性與否有顯著差異。
H2c	商業夥伴影響的因素對於組織資訊安全程度的完整性與否有顯著差異。
H2d	供應商的因素對於組織資訊安全程度的完整性與否有顯著差異。
研究假說三：組織內部的構面考量對於組織資訊安全程度的完整性與否有顯著差異。	
H3a	高階主管支持的因素對於組織資訊安全程度的完整性與否有顯著差異。
H3b	安全事件處理的因素對於組織資訊安全程度的完整性與否有顯著差異。
H3c	組織特性的因素考量對於組織資訊安全程度的完整性與否有顯著差異。
H3d	組織政策的因素考量對於組織資訊安全程度的完整性與否有顯著差異。
H3e	組織資源配合的因素考量對於組織資訊安全程度的完整性與否有顯著差異。
H3f	安全風險程度的因素對於組織資訊安全程度的完整性與否有顯著差異。
H3g	員工參與的因素對於組織資訊安全程度的完整性與否有顯著差異。

肆、資料分析

一、樣本基本資料分析

本研究係整理台灣區石化公會之會員名冊及上櫃上市石化公司為問卷對象(共212家)，每家公司僅發一份問卷，問卷對象在問卷上註明為資訊主管、資訊安全主管或稽核主管，總共寄發問卷 212 份，回收 66 份問卷，回收率達 31.13%，而扣除 2 份無效問卷，總計有效回收 64 份問卷，因此實際回收率為 30.18%。

受訪者基本資料分析如下：(1)受訪者職稱部份： 64%(41 家)受訪者的職稱是屬於管理階層。其他不是管理階層者大部份均具備資訊或稽核背景，因此和本研究設定之問卷對象大致相符。(2)定期檢討修改資訊安全政策：在是否定期修改資訊安全政策部份：25%(16 家)廠商有定期修改資訊安全政策，60.94%(39 家)廠商會不定期修改資訊安全政策。(3)成立資訊安全部門：在是否成立資訊安全部門的部份僅 25%(16 家)廠商有另外成立資訊安全部門，另外有 75%(48 家)未成立資訊安全部門。(4)負責資訊安全員工：在是否有負責資訊安全員工部份 67.2%(43 家)廠家有設立負責資訊安全的員工。其中 37.2%(16 家)廠家負責資訊安全的員工為專職人員；55.8%(24 家)廠家負責資訊安全的員工為兼職人員。(5)成立電腦稽核的部門：在是否成立電腦稽核部門的部份有 32.8%(21 家)廠家有另外成立電腦稽核部門，另外有 67.2%(43 家)未成立電腦稽核部門。(6)負責電腦稽核員工:56.3%(36 家)廠家有設立負責電腦稽核的員工。其中 25%(9家) 廠家負責電腦稽核的員工為專職人員；52.8%(19 家)廠家負責電腦稽核的員工為兼職人員。

表三係針對資訊安全組織及人力配置方面和曾淑惠(2002)調查國內銀行業現況作一比較，結果發現石化產業無論在資訊安全政策、資訊安全組織的建立以及資訊安全人力的配置，均遠低於銀行業，例如銀行業有 61%成立資訊安全管理部門及 71%有定期修改資訊安全政策，而石化業均僅 25%成立資訊安全管理部門及定期修改資訊安全政策，顯示目前石化產業對資訊安全狀況的重視程度並不高。

表三　資訊安全組織及人力配置比較

資訊安全組織及人力配置		石化產業(本研究)	銀行業(曾淑惠，91 年)
定期修改資訊安全政策	是	25%	71%
	不定期	61%	10%
	否	14%	19%
成立資訊安全管理部門	是	25%	61%
	否	75%	39%
成立電腦稽核部門	是	33%	80%
	否	67%	20%
負責資訊安全的員工	是	67%	92%
	否	33%	8%
負責電腦稽核的員工	是	56%	90%
	否	44%	10%

二、資料穩定度分析

本研究依據資本額、年平均營業額以及員工人數等三項企業基本特性變數，經由獨立樣本 t 檢定來比較填答內容在前後期回收問卷之差異，藉以衡量未回收問卷之偏誤，以確保回收問卷具有充分、有效之母體代表性。在 0.05 顯著水準下，檢定結果如表四所示，p 值均大於 0.05，顯示前後期回收樣本在公司基本特性變數上並無顯著之差異，故推論未回收之問卷並不會對研究結果造成太大的偏誤，換言之，本研究之回收樣本具有相當程度的母體代表性。

表四 前後期回收問卷差異之 t 檢定

企業特性	檢定方法	檢定值	顯著性
資本額	獨立樣本 t 檢定	-1.070	p=0.289
年平均營業額	獨立樣本 t 檢定	-0.263	p=0.794
員工人數	獨立樣本 t 檢定	-0.154	p=0.878

三、因素分析及信度分析

本研究藉著因素分析來測量問卷的建構效度，檢視被分類的因素是否與研究架構相同。依據各變數測量項目的平均值，進行主成份分析法(Principal Components)，將變數群集依據因素負荷量(Factor Loading)分類在幾個主要的因素群中，並將每群根據其特性重新為因素命名，因素截取的基準是取特徵值(Eigenvalue)大於 1 的因素。而因素轉軸方法是採一般常用正交轉軸法之一的最大變異法(即 Varimax Rotation)，以求轉軸後因素與其他因素的因素負荷量相差達到最大，而因素內的每個變項差異達到最小，以利共同因素的辨認和命名。而每個因素變項之截取，根據 Hair et al. (1998)的研究，α=0.05 的顯著水準下，樣本大小在 60 時，因素負荷量應達到 0.7 以上，因此本研究將因素負荷量大於 0.7 的變項酌量納入各群因素中。

因素分析結果如表五所示, 其中組織內部構面中原有 7 項因數，但經因素分析後萃取出 6 項因數, 其中「高階主管支持」、「安全事件處理」、「安全風險程度」及「員工參與」等 4 項符合原研究架構所提之變項，而「組織特性」、「組織政策」及「組織資源配合」則並未趨集成為因素，因此剩餘 2 項因數則依據問卷題項內容與專家討論後重新命名為「組織規模」及「電腦化程度」，並依重新命名之因素名稱進行假設檢定。

對於信度的檢測，採 Cronbach's α 係數來衡量同一概念變數下各個衡量指標之間的一致性。一般而言 α 值介於 0.7 至 0.98 之間，均屬於高信度值，而介於 0.7 與 0.35 之間則為可接受之信度值，而若低於 0.35 者，則應捨棄使用。回收問卷檢測之結果，如表四，除了高階主管支持為 0.66 稍小於 0.7 外，其餘變數之信度均大於 0.7，顯示本研究之信度均高於可接受程度。

本研究之各變數是依據文獻探討而來, 目前有關影響企業資訊安全因素的研究並不多, 樣本數並不足以進行統計分析以檢驗信效度, 因此本研究才透過三位專家進行面對面深入訪談, 經由專家的討論與檢視，應具有相當程度的內容效度。

表五 因素分析及信度分析結果彙整表

資訊科技構面				
因素	命名	特徵值	Cronbach's α	指標個數
1	安全防護	2.923	0.763	2
2	資訊安全技能	1.175	0.829	2
外在環境構面				
因素	命名	特徵值	Cronbach's α	指標個數
1	供應商	5.801	0.923	4
2	法令規章	1.929	0.909	3
3	競爭壓力	1.322	0.800	3
4	商業夥伴影響	1.002	0.882	2
組織內部構面				
因素	命名	特徵值	Cronbach's α	指標個數
1	安全事件處理	9.183	0.928	4
2	員工參與	2.493	0.824	3
3	電腦化程度	1.909	單一問項	1
4	高階主管支持	1.230	0.665	2
5	組織規模	1.111	0.860	2
6	安全風險程度	NonMetrix 單一問項		

四、區別分析及假說驗証

進行區別分析之前因變數資訊安全狀況部分，共有 23 個樣本平均分數在 4 分(含)以上則歸類為「完整」，而有 41 個樣本則歸類為「不完整」。而自變數部份，安全風險程度變數為名目尺度因此先將之轉換為虛擬變數再進行分析。區別分析檢定結果，如表六所示。由於 Wilks' Lambda 值為 0.482(Chi-square=40.136，df=14，Sig.=0.000)顯示本研究具顯著區別之效力，換言之資訊安全狀況完整與不完整兩群體間有顯著差異存在。而各個預測變數對於資訊安全狀況是否有顯著差異，可由表六中 F 檢定值及顯著性得知，研究假說驗証結果如表七所示。

表六 區別分析結果

Wilks' Lambda：0.482				Chi-square：40.136		
Df：14				Sig.：0.000		
檢定值 / 預測變數	標準化區別係數	區別負荷量	F 檢定值	顯著性	資訊安全完整平均值/標準差	資訊安全不完整平均值/標準差
安全防護	0.371	0.530	18.7270	0.000	4.00/0.46	4.55/0.51
資訊安全技能	0.493	0.508	17.166	0.000	3.69/0.55	4.28/0.51
供應商	0.261	0.431	6.200	0.015	16.2/5.05	19.5/4.94
法令規章	0.054	0.414	11.403	0.001	3.81/0.64	4.36/0.50
競爭壓力	-0.071	0.327	7.134	0.010	3.63/0.71	4.10/0.61
商業夥伴影響	0.197	0.431	12.367	0.001	3.04/0.81	3.84/0.96
安全事件處理	-0.274	0.37	9.109	0.004	3.99/0.56	4.43/0.56
員工參與	0.411	0.627	26.189	0.000	3.45/0.57	4.21/0.57
電腦化程度	-0.004	0.332	7.346	0.009	3.82/0.83	4.39/0.72
高階主管支持	0.040	0.331	7.287	0.009	3.47/0.67	3.94/0.66
組織規模	0.024	0.297	5.891	0.018	3.92/0.72	4.36/0.66
風險程度 (虛擬變數 1)	-0.191	0.142	1.350	0.250	0.04/0.21	0.13/0.34
風險程度 (虛擬變數 2)	-0.031	0.165	1.815	0.183	0.39/0.49	0.56/0.50
風險程度 (虛擬變數 3)	-0.652	-0.378	9.497	0.003	0.43/0.50	0.08/0.28

表七 研究假說驗証結果

假說		成立與否
研究假說一：資訊科技的構面考量對於組織資訊安全程度的完整性與否有顯著差異。		是
H1a	安全防護的因素對於組織資訊安全程度的完整性與否有顯著差異。	是
H1b	資訊安全技能的因素對於組織資訊安全程度的完整性與否有顯著差異。	是
研究假說二：外在環境的構面考量對於組織資訊安全程度的完整性與否有顯著差異。		是
H2a	法令規章的因素對於組織資訊安全程度的完整性與否有顯著差異。	是
H2b	競爭壓力的因素對於組織資訊安全程度的完整性與否有顯著差異。	是
H2c	商業夥伴影響的因素對於組織資訊安全程度的完整性與否有顯著差異。	是
H2d	供應商的因素對於組織資訊安全程度的完整性與否有顯著差異。	是
研究假說三：組織內部的構面考量對於組織資訊安全程度的完整性與否有顯著差異。		是
H3a	高階主管支持的因素對於組織資訊安全程度的完整性與否有顯著差異。	是
H3b	安全事件處理的因素對於組織資訊安全程度的完整性與否有顯著差異。	是
H3c	組織規模的因素考量對於組織資訊安全程度的完整性與否有顯著差異。	是
H3d	電腦化程度的因素考量對於組織資訊安全程度的完整性與否有顯著差異。	是
H3e	安全風險程度的因素對於組織資訊安全程度的完整性與否有顯著差異。	是
H3f	員工參與的因素對於組織資訊安全程度的完整性與否有顯著差異。	是

伍、結論

一、研究結論

從表七研究假說驗証結果，清楚發現本研究根據文獻探討及理論架構所提出之研究假說，無論從資訊科技構面、外在環境構面及組織內部構面而言，對於兩群資訊安全狀況(完整/不完整)均有顯著差異。顯見石化業界如要達到 BS7799 的資訊安全要求，須全面性考量各項因素之影響，茲將本研究之結論及建議說明如下，以提供業界導入資訊安全認證時之參考，期有助於業界能更快速、經濟有效的達到資訊安全的國際認證標準：

- 資訊技術層面：資訊安全防護是建立資訊安全機制的第一道防線，除了基本的防毒系統及防火牆外，為防範層出不窮的惡意入侵，入侵偵測產品的建置已逐漸為企業所接受。然而有了完善的防禦設備尚須培育相關人才加以配合，例如資訊安全人員是否具備資訊安全相關知識及技術？是否有處理資訊安全問題的經驗？這些因素均會影響企業資訊安全程度的現況。
- 管理層面：資訊安全不僅是安全技術上問題，在管理層面上尚有許多因素要加以配合，在本研究所驗證的結果發現「高階主管支持」、「安全事件處理」、「員工參與」及「供應商」等因素對於企業資訊安全程度現況會有顯著影響，結果及建議說明如下：(1)高階主管支持：資訊安全管理的實行，首先必須獲得高階主管的支持，因為資訊安全管理主要是在於風險控管以避免損失，無法獲得財務上的利益及績效，再加上實行時有許多的困難，因而如未能獲得高階主管的支持，容易流於半途而廢，因此資訊安全管理的實行，首重高層主管的支持。而「行政院及所屬各機關資訊安全管理規範」也明文規定，應指定副首長或高層主管人員，負責推動、協調及督導各項資訊安全管理事項，可見高階主管支持對於資訊安全管理之重要性。(2)安全事件處理：危機處理能力關係到企業能否永續發展的重要因素，因此企業面對層出不窮各項資訊安全的挑戰時，須建立因應資訊安全事件處理的管理機制，包括安全偵測機制、安全稽核機制、資訊安全通報機制及資訊安全危機處理流程。(3)員工參與：許多研究指出員工參與程度是資訊系統導入成功與否的關鍵因素之一，在資訊安全管理機制的建立上亦是如此，其中員工對於組織資訊安全政策能充分配合以及接受適當的資訊安全訓練和教育，都可正面提昇企業資訊安全的程度。(4)供應商：資訊安全系統的建置需整合不同專業領域的人員，若由企業內自行培育人才在成本上可能負擔較重，況且資訊安全系統發展的經驗亦較為缺乏，因此供應商將扮演關鍵性的角色。供應商的選擇除了應具備良好的資訊安全技術、提供充分的市場情報以及要有與其他顧客合作的成功案例外，更應重視供應商的信譽，在與供應商的交往的過程中須做好商業秘密的保護以及合約的管理。
- 組織的某些特性及外在環境的因素會促進石化業者更加重視資訊安全狀況，而進一步導入資訊安全管理機制，這些因素包括「組織規模」、「電腦化程度」、「安全風險程度」、「法令規章」、「競爭壓力」及「商業夥伴影響」等因素對於企業資訊安全程度現況會有顯著影響，說明如下：(1)組織規模：由分析結果發現，組織特性中營業規模大、市場佔有率高以及產業成熟度高的石化企業比較重視資訊安全現況，探究其原因主要是國內石化大廠彼此間競爭激烈，為保持現有的優勢，因

此會比較重視資訊安全的狀況，以防止資訊安全事件影響企業營運。(2)電腦化程度：電腦化程度愈高的企業其仰賴電腦處理的業務的需求愈大，因此會比較重視資訊安全的狀況，以防止資訊安全事件影響業務運轉。(3)安全風險程度：行政院將資訊安全的風險程度分為四個等級，風險程度高低分別為「影響公共安全、社會秩序、人民生命財產」、「系統停頓，業務無法運作」、「業務中斷，影響系統效率」、「業務短暫停頓，可立即修復」。研究發現風險程度愈高的石化企業比較重視資訊安全的建置。(4)法令規章：政府的法令規章愈嚴格，會迫使企業更重視資訊安全的問題，例如證期會規定申請上櫃上市公司須依據 ISO17799 執行資通安全檢查循環，企業必須認真改善資訊安全現況，以順利申請上櫃上市。(5)競爭壓力：面對高度競爭壓力的石化企業，因擔心資訊安全事件而喪失競爭優勢，會比競爭壓力低的企業較重視資訊安全的現況。(6)商業夥伴影響：商業夥伴的要求或因同業普遍導入資訊安全管理機制，將會促使企業重視資訊安全的現況。

- 石化產業業者會因組織內部因素(如營業規模、市場佔有率、電腦化程度及安全風險程度)及外在環境因素(如政府法令規章、競爭壓力及商業夥伴影響)的影響而開始導入資訊安全管理機制，在導入的過程當中要有兩個層面的關鍵因素要配合執行，一是資訊技術層面，另一是管理層面。在資訊技術上首先要建立資訊安全防護系統，並培養相關資訊安全技能，有了良好的防禦設施後，再配合適當的管理活動，在管理層面上首先要獲得高階主管支持，建立安全事件的相關處理程序，並鼓勵員工積極參與，及選擇信譽良好的供應商，提供相關的技術諮詢及輔導。以上是本研究針對石化產業所實証之關鍵因素，期有助於石化業界建立資訊安全管理機制或導入資訊安全認證時之參考。
- 石化產業對於資訊安全的重視程度及資訊人才均普遍不足，由本研究調查結果和以往銀行業的調查比較，發現石化產業對於資訊安全政策的修正，資訊安全及稽核部門的成立，以及資訊安全及稽核人力的配置，均遠低於銀行業。因應未來法令的嚴格要求，ISO 通過後商業夥伴的影響或是為確保公司的資訊資產及永續經營，石化業界應儘早在於人力和資源上做準備，以因應資訊安全議題所帶來的挑戰。

二、研究貢獻與限制

本研究針對國內石化產業的資訊安全議題及現況進行調查，並找出影響石化產業導入資訊安全管理機制的關鍵因素，實際瞭解石化產業的資訊安全狀況，並找出影響石化產業導入資訊管理安全機制的關鍵因素，此成果可提供業界導入資訊安全認證時之參考，將有助於業界能更快速、經濟有效的達到資訊安全的國際認證標準。

對學術界而言，本研究藉由文獻及專家檢視找出影響企業資訊安全的因素，並以 BS7799 相關量表衡量石化產業之資訊安全狀況，並依據樣本資料來檢測假說找出關鍵因素，有別於以往之研究架構，因此研究的成果相信可提供相關研究者日後之參考。

本研究首先根據文獻及資訊安全專家進行訪談以確定本研究之研究模式，接著採用問卷調查的方式，以石化產業為研究對象，驗證本研究之研究假說，在研究過程中力求嚴謹，但依然有研究上的限制，說明如下：(1)樣本大小的限制：本研究在經過問卷寄發、問卷催收及第二次寄發後，有效回收樣本數僅有 64 家，雖已達到區別分析所需要求，然而本研究樣本數小於 100，無法將資料區分為分析樣本與驗證樣本，以進一步確認區別效果，而僅能利用分析樣本來做資料之驗證，這或許對分析結果會產生些許偏差。(2)資訊安全狀況分群：資訊安全狀況的分群(完整/不完整)最理想的做法是

將通過 BS7799 認証的企業分為一群，未通過認証的企業歸為另外一群，來進行關鍵因素的驗證分析，所得結果應最具代表性。然而 BS7799 尚在推廣階段，國內通過認証的機構僅 4 家(包括 1 家銀行，3 家資訊服務業)，且石化產業中尚未有廠家通過 BS7799 認証，因此本研究僅能以 BS7799 的相關量表來衡量石化產業的資訊安全狀況。將來如果更多國內企業得到 BS7799 認証，再進行相同研究，所得的結果應更具參考價值。(3)外部稽核工作的缺乏：企業資訊安全的狀況除以自我檢查衡量外，當然藉由外部單位的稽核找出缺失提出改善建議，才能使企業對資安狀況的衡量不致偏頗誤差。但本研究限於人力及財力無法執行外部稽核工作，另外企業基於安全理由除非公權力要求，否則不會接受外人進入稽核。故未來研究學者可以考慮加入外部稽核因素，所得結果應更有參考價值。

參考文獻

1. 台灣區石化公會，2001『台灣區石化公會九十年石化工業概況』，台北市 ： 台灣區石化公會。
2. 行政院研考會，2000 『行政院及所屬各機關資訊安全管理規範』。
3. 吳俊德，2002，ISO 17799 資訊安全管理關鍵重點之探討，國立中正大學企業管理研究所碩士論文。
4. 沈倩如，2001『美國電子商務簡易市調』，經濟部國貿局九十年度第一季簡易市調。
5. 財政部，2002『公開發行公司建立內部控制制度處理準則』。
6. 張振接，2001『打造堅不可摧的國產 Linux OS－為 Power by Taiwan 的「資訊安全產業」催生』，軟體產業通訊，第四十三卷：13～21 頁。
7. 曾淑惠，2002，以 BS 7799 為基礎評估銀行業的資訊安全環境，淡江大學資訊管理學系碩士論文。
8. 游輝祥，2001『工廠資訊管理系統』，e-safety 工安簡訊電子報，第八期。
9. 經濟部技術處，2002『產業電子化白皮書』，台北市 ： 經濟部技術處。
10. 經濟部標準檢驗局，2002『資訊安全管理系統(ISMS)---CNS 17800 標準』。
11. 葉瑞萍，2001『製程資訊整合實廠建置經驗談』，e-safety 工安簡訊電子報，第五期。
12. 蒲樹盛，2004『台灣金融業應用 BS7799 資訊安全管理系統(ISMS)分析』，電腦稽核，第十期：17～25 頁。
13. BSI. “Information security management- Part 1: Code of practice for information security management,” *BS 7799-1:2000*, BSI (British Standards Institution), 2000
14. BSI. “Information security management- Part 2: Specification for information security management systems,” *BS 7799-2:2002*, BSI (British Standards Institution), 2002
15. Caminada, M. “Internet security incidents, a survey within Dutch organizations,” *Computers & Security* (17:1) 1998, pp:417-433
16. Chau, Jacqui. “Skimming the technical and legal aspects of BS7799 can give a false sense of security,” *Computer Fraud & Security* (2005:9) September 2005, pp8-10
17. Cohen, F. “A cause and effect model of attacks on information systems,” *Computers & Security* (17:1) 1998, pp:221-226
18. Eloff, M.M. and Solms S.H. von . “Information Security Management: An Approach to Combine Process Certification And Product Evaluation,” *Computers & Security* (19:1) 2000, pp:698-709

19. Hair, J.F. , Anderson, R.E., Tatham, R.L. and Black, W.C. *Multivariate Data Analysis*, 5th Ed., Prentice-Hall, Inc. 1998
20. http://www.coso.org/, October 12, 2005
21. http://www.isaca.org/Template.cfm?Section=COBIT6&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=55&ContentID=7981, October 12, 2005
22. Huang, H.Y. and Hwang, H.G., and Yen, D.C. "A Study on Internet Security Factors of Different Financial Institutions in Taiwan," *Proceedings of the International Conference of Pacific Rim Management*, New York, USA, August 2000
23. Kankanhalli, A., H. H. Teo, B.C.Y. Bernard, and K.K. Wei. "An Integrative Study of Information Systems Security Effectiveness," *International Journal of Information Management* (13) 2003, pp:139-154
24. Powell, D. "To Outsourcing or not to Outsourcing?," *Networking Management* 1993, pp:56-61
25. Premkumar, G.., Ramamurthy, K. and Nilakanta, S. "Implementation of electronic data interchange: An innovation," *Journal of Management Information Systems* (11:1) 1994, pp:157-186
26. Root, Steven J. *Beyond COSO: internal control to enhance corporate governance*, John Wiley, New York, 1998
27. Solms, Basie von. "Information Security Multidimensional Discipline," *Computers & Security* (20:1) 2001, pp:504-508
28. Solms, Basie von and Solms, Rossouw von. "Incremental Information Security Certification," *Computers & Security* (20:1) 2001, pp:308-310
29. Symantec. "Symantec Enterprise Solutions," http://enterprisesecurity.symantec.com/article.cfm?articleid=356&PID=6526177#two , 2000.10
30. Trcek, D. "An Integral Framework for Information Security Management," *Computers & Security* (22:4) 2003, pp: 337-360

附錄 本研究問卷

敬啟者：

隨著電子交易的發展，資訊安全逐漸受到企業重視，「BS 7799」是由英國國家標準協會(BSI)於 1995 年所制定，企業只要做到 BS 7799 的要求，並通過獨立稽核機構評鑑，便可獲頒 BS7799 資訊安全認證，向其客戶與合作夥伴宣告，該企業網路內與他們相關的資料都受到適當的保護，而且該企業整體的安全度也值得信任。另外「BS 7799」第一部份已在 2000 年 12 月 1 日成為 ISO 17799 國際標準，預計未來二年第二部份通過後資訊安全管理認證將正式成為國際標準，而我國中央標準局亦於 91 年通過 CNS17799 及 CNS18000，作為業界資訊安全實施及認證之規範。

ISO 17799 如果通過後，資訊安全的政策實施，將如同 ISO 9000 及 ISO 14000 影響我國產業的發展，例如在供應鏈體系中，在進行電子資料交換時，會要求上下游廠商須獲得 ISO 17799 認証，以確保整個供應鏈體系中的資訊安全達到一定水準。因此未獲得 ISO 17799 認証之企業，在 B2B 電子商務建置或者加入電子市集的競爭中將遭受壓力或排擠，而失去競爭優勢。

有鑑於此，本研究是以 BS 7799 為基礎對國內石化產業的資訊安全現況進行了解，並探討影響企業資訊安全的因素，並將調查結果進行統計分析，找出顯著的影響因素，以做為業界資訊安全實施之參考。

此次問卷調查的對象為貴公司資訊主管或負責資訊安全的主管為主，若您不是本問卷的調查對象，煩請轉交適合的人員填寫。所有提供的任何資料都僅供本研究彙總分析使用，絕不具名及個別對外公佈，敬請放心，問卷內容因涵蓋範圍較廣而稍多，但您的協助將使本研究更具參考價值，敬請撥冗耐心填完，並請於四月十日前將問卷直接裝訂擲回。在此先對您的熱心支持與幫忙致上十二萬分的謝意。

謹祝

鴻圖大展　事事如意

國立中正大學資訊管理系碩士班
指導教授：黃 士 銘　博士
研 究 生：蘇 耿 弘
E-Mail:sukh@mis.ccu.edu.tw

中華民國九十二年三月二十日

第一部份：公司及受訪者基本資料—這部份在請教您及貴公司的基本資料，所有資料僅供整體統計分析，敬請安心作答

1.您的職稱是：

☐資訊部門主管 ☐資訊安全主管 ☐資訊部門兼資訊安全主管

☐資訊部門人員 ☐資訊安全部門人員 ☐其他：_____

2.您的性別是： ☐ 男 ☐ 女

3.貴公司目前的資本額為：

☐ 1 千萬元(含)以下 ☐ 1~5 千萬元(含) ☐ 5 千萬~1 億元(含) ☐ 1 億元-10 億元(含)

☐ 10 億~20 億元(含) ☐ 20 億~50 億元(含) ☐ 50 億~100 億元(含) ☐ 100 億元以上

4.貴公司去年的營業額為：

☐ 1 千萬元(含)以下 ☐ 1~5 千萬元(含) ☐ 5 千萬~1 億元(含) ☐ 1 億元-10 億元(含)

☐ 10 億~20 億元(含) ☐ 20 億~50 億元(含) ☐ 50 億~100 億元(含) ☐ 100 億元以上

5.貴公司員工人數為：

☐ 100 人以下 ☐ 101-250 人 ☐ 251-500 人 ☐ 501-1000 人

☐ 1001-2000 人 ☐ 2001-5000 人 ☐ 5001-10000 人 ☐ 10000 人以上

6.貴資訊部門的員工人數為：

☐ 10 人以下 ☐ 11-25 人 ☐ 26-35 人 ☐ 36-50 人

☐ 51-100 人 ☐ 101-150 人 ☐ 151-200 人 ☐ 201 人以上

7.貴公司是否有定期檢討修改資訊安全政策:

☐ 是，多久一次：_____次/年 ☐ 不定期 ☐ 否

8.貴公司是否有專職資訊安全的部門：

☐ 是 ☐ 否

9.貴公司是否有負責資訊安全的員工：

☐ 有，其中專職____人，兼職____人 ☐ 無

10.貴公司是否有專職電腦稽核的部門：

☐ 是 ☐ 否

11.貴公司是否有負責電腦稽核的員工：

☐ 有，其中專職____人，兼職____人 ☐ 無

第二部份：資訊科技因素—這部份在請教貴公司在資訊安全方面有關資訊科技建置及實施狀況

	非常同意	同意	普通	不同意	非常不同意
1. 使用通過資訊安全認證(如 ITSEC)的資訊產品對貴公司資訊安全有相當大的貢獻	☐	☐	☐	☐	☐
2. 使用防火牆對貴公司資訊安全有相當大的貢獻	☐	☐	☐	☐	☐
3. 使用網路防毒產品對貴公司資訊安全有相當大的貢獻	☐	☐	☐	☐	☐
4. 使用網路入侵偵測產品對貴公司資訊安全有相當大的貢獻	☐	☐	☐	☐	☐
5. 貴公司負責資訊安全人員具備資訊安全相關知識及技術	☐	☐	☐	☐	☐
6. 貴公司負責資訊安全人員有處理資訊安全問題的經驗	☐	☐	☐	☐	☐

第三部份：外在環境因素－這部份在請教貴公司在資訊安全方面有關外在環境的影響現況

	非常同意	同意	普通	不同意	非常不同意
1. 政府明定安全條例，公布資訊安全獎懲辦法，對貴公司資訊安全推動會有幫助	□	□	□	□	□
2. 政府政策對資訊安全的推動與支持，對貴公司資訊安全推動會有幫助	□	□	□	□	□
3. 政府明定相關資訊安全犯罪條文，對貴公司資訊安全推動會有幫助	□	□	□	□	□
4. 同業競爭者的操守對貴公司的資訊安全是一大威脅	□	□	□	□	□
5. 商業間諜對貴公司的資訊安全是一大威脅	□	□	□	□	□
6. 貴公司將因資訊安全事件發生而喪失競爭優勢	□	□	□	□	□
7. 貴公司因配合商業夥伴的要求而必須導入資訊安全管理機制	□	□	□	□	□
8. 貴公司因業界均已普遍採用而必須導入資訊安全管理機制	□	□	□	□	□
9. 建置資訊安全設備時貴公司會要求供應商必須有與其他顧客合作的成功案例	□	□	□	□	□
10. 建置資訊安全設備時貴公司會要求供應商必須有規劃完整的技術及方案	□	□	□	□	□
11. 建置資訊安全設備時貴公司會要求供應商必須提供充分的市場情報	□	□	□	□	□
12. 建置資訊安全設備時設備供應商的誠信對貴公司資訊安全有很大影響	□	□	□	□	□

第四部份：組織內部因素－這部份在請教貴公司在資訊安全方面有關組織內部的配合現況

	非常同意	同意	普通	不同意	非常不同意
1. 高階主管對資訊安全措施的建置及導入相當支持	□	□	□	□	□
2. 高階主管願意參加資訊安全實施相關會議及決策	□	□	□	□	□
3. 高階主管關心資訊安全措施建置後，使用者的滿意度	□	□	□	□	□
4. 高階主管關心資訊安全措施建置後，員工是否產生抗拒	□	□	□	□	□
5. 建立安全偵測機制對貴公司的資訊安全防護相當重要	□	□	□	□	□
6. 建立安全稽核機制對貴公司的資訊安全防護相當重要	□	□	□	□	□
7. 訂定資訊安全通報機制對貴公司的資訊安全防護相當重要	□	□	□	□	□
8. 訂定資訊安全危機處理流程對貴公司的資訊安全防護相當重要	□	□	□	□	□
9. 貴公司各項業務的電腦化程度相當高	□	□	□	□	□
10. 貴公司的營業規模及市場佔有率相當高	□	□	□	□	□
11. 貴公司的產業成熟度(公司年齡)相當高	□	□	□	□	□
12. 資訊安全政策的訂定對貴公司資訊安全有相當大的貢獻	□	□	□	□	□
13. 安全需求及風險評估的訂定對貴公司資訊安全有相當大的貢獻	□	□	□	□	□
14. 安全責任的明確劃分對貴公司資訊安全有相當大的貢獻	□	□	□	□	□
15. 貴公司對於資訊安全所需預算相當支持	□	□	□	□	□
16. 貴公司對於導入資訊安全機制的時間相當充足	□	□	□	□	□
17. 貴公司對於導入資訊安全機制所需人力充分支援	□	□	□	□	□
18. 員工的操守對貴公司資訊安全推動相當重要	□	□	□	□	□
19. 員工對於組織資訊安全的理念充分了解	□	□	□	□	□
20. 員工對於組織資訊安全政策充分配合	□	□	□	□	□
21. 員工接受適當的資訊安全訓練和教育	□	□	□	□	□
22. 因資訊安全事件而造成貴公司最嚴重的風險程度為：	□	□	□	□	□

□影響公共安全、社會秩序、人民生命財產
□系統停頓，業務無法運作
□業務中斷，影響系統效率
□業務短暫停頓，可立即修復

第五部份（續）：資訊安全現況—這部份在請教貴公司在資訊安全的實施現況

	非常同意	同意	普通	不同意	非常不同意
21. 貴公司有無一套以風險評估為基礎的策略規劃，以利全面達到企業之永續運作？	□	□	□	□	□
22. 貴公司有無建立「災害回復計畫」？	□	□	□	□	□
23. 貴公司企業永續運作之計畫，是否有考量各計畫之演練與其先後之順序性？	□	□	□	□	□
24. 企業永續運作之計畫是否有定期測試與檢討維護，以確保計畫內容之最新及有效？	□	□	□	□	□
25. 所有有關法令、法規和契約的要求，貴公司是否有考量應予以明確定義每一個資訊系統的適用性？	□	□	□	□	□
26. 智慧財產權貴公司是否有加以維護？	□	□	□	□	□
27. 對重要記錄，貴公司是否有加以保護，避免損失、破壞和偽造？	□	□	□	□	□
28. 資料保護之控管制度，貴公司是否有確實執行？	□	□	□	□	□
29. 是否有避免使用者誤用資訊處理設備之管制措施？	□	□	□	□	□
30. 對加密工具之使用，貴公司是否有控管程序來確保？	□	□	□	□	□
31. 所有程序所記載之內容，貴公司是否有遵循日後若需訴諸法律所能接受之證據型式？	□	□	□	□	□

問卷到此全部結束，請再檢查是否有漏答的項目。然後將問卷放入回郵信封寄回即可，衷心感謝您的協助！！

若您需要本研究結果，請留下電子郵件信箱，報告完成後將以電子檔傳送給您。

E-Mail：_____