企業對行動式員工的資訊安全防護之規劃

作者[1]許麗玲　　作者[2]陳澔輝　　作者[3]邱銘乾

[1]國立高雄第一科技大學資訊管理系　karenhsu@ccms.nkfust.edu.tw
[2]國立高雄第一科技大學企業電子化所　u9524038@gmail.com
[3]家登精密工業股份有限公司　Bill@gudeng.com

摘要

隨著科技快速發展，人們及企業對於資訊系統應用需求不斷增加。在提升工作效率的目標下，愈來愈多企業仰賴行動裝置。根據市場研究機構 IDC 預測，今年全球行動工作者的人口將突破 10 億大關，可望達到 12 億，到 2013 年行動工作者將佔全球人口的三分之一以上。企業行動性雖為商業世界帶來更多的機會，但同時所伴隨的資訊安全風險與威脅亦不容忽視。企業所面臨的挑戰包括佈建這些裝置、確保其安全性，以及對其進行日常管理。

本研究利用國際間遵行之資訊安全管理規範(BS7799)之標準規範之評估模式，對個案公司的行動式資訊安全活動進行探討，檢視個案公司對行動式資訊安全管理系統之整體認知、實施程度；同時在機密性、可用性及整體性的三項指標下，進行資訊安全風險評估，瞭解執行上的障礙並試圖有效降低風險。經文獻探討與實務觀察，歸納本研究之結論，期能以漸進方式，建構符合企業個別需求之安全管理系統，以達到企業永續經營之目的。

關鍵詞: 行動工作者、資訊安全

1. 緒論

1.1 研究背景

21 世紀的新經濟時代，傳統企業正逐步朝 Mobilization (以下簡稱 M 化)發展，在 M 化的環境中，行動裝置不但改變了企業固有的經營方向，也提供企業多元化服務的管道。近年來全球產業環境面臨了榮景與大衰退的重大變化，企業面臨了變遷快速的產業環境與強大的競爭壓力，為了有效掌握營運資訊流向與快速決策反應，企業導入 e 化衍然成為經營上非做不可的義務性投資。然而在產業競爭者爭相投入 e 化的狀況之下，企業間彼此差異化越來越小，隨著資訊科技進步與商業經營腳步的互相牽動之下，很多企業開始轉換思維，從營運服務模式的創新發展並結合資訊科技技術，來創造出獨特的競爭優勢，也展現出企業價值。在作業環節中，由於訂單交易頻繁、作業繁瑣、企業內部或上下游企業資訊溝通不易等問題，使得資訊化的腳步更顯重要，也是企業的競爭力的主要基礎。而企業如何提升顧客滿意度、時間、速度、服務、品質等?在現今講求時間就是金錢與速度就是快速回應的競爭環境下，『速度的提升與保證』必是服務戰場的重要關鍵。因此，服務機制與內部流程趨勢將勢必與 M 化整合。

隨著行動通訊技術的成熟、各式行動設備的普及，全面 e 化已無法滿足企業的需求，取而代之的是具備即時性及無地域性限制的工作及服務型態，目標為達到 Any Time、Any Where、Any Device 的服務提供。M 化不只提升企業的效率，也大幅提升客戶對企業的觀感及信任，因為企業將可以即時幫客戶解答及服務。根據各種資料顯示，企業 M 化目前有逐漸加溫的趨勢，且未來會以更高的比例上升，並將運用在各種不同產業及業務的應用上，例如物流倉儲業者可透過行動物流/倉儲系統即時查詢貨物的最新狀況、業務人員可利用 PDA 即時查詢客戶資料來作好客戶關係管理、甚至改善原本的作業流程及管理機制等。據產業專家表示，當企業導入 M 化，將可有效的降低人力、設備、通訊、時間管理等成本，並提升企業效率及顧客滿意度，因此企業 M 化已經成為不可抑制的潮流，藉由 M 化將可帶來比現行運作模式效益大上數十倍的經濟產值。

但越來越多使用者以遠端的方式連接網路，企業需要讓員工於任何時刻、任何地點都能透過行動裝置來存取企業資料，為了保護公司資料與資源，企業同時也在行動運算技術上面臨到更大的資安挑戰，行動企業所講求的是機密性、可用性與完整性。所以開始關心 M 化後所帶來的「資訊安全」議題，因為安全性是企業導入行動解決方案的重要基石，也是無法妥協的必須要務。

1.2 研究動機與目的

許多企業為了因應外部競爭與提升營運績效，有愈來愈多企業選擇為員工配置智慧型手機或是筆記型電腦，以便即時接收或提供訊息。儘管 M 化成為企業提升競爭力的工具之一，然而，凡事皆有一體兩面，企業在享受 M 化效益的同時，也必須面對伴隨而來的資安挑戰，稍有不慎，就會嚐到機密資料外流的苦果。

根據市場研究機構 IDC 預測，今年全球行動工作者的人口將突破 10 億大關，可望達到 12 億，到 2013 年行動工作者將佔全球人口的三分之一以上。有鑑於行動辦公室需求日益旺盛，而企業也開始意識完善的資安防護方案。另外安永會計事務所於 2010 年的 6 月至 8 月，針對全球 1,600 家企業進行全球資訊安全調查。美國商業資訊報導指出，根據該會計事務所第 13 期年度資訊安全調查的結果顯示，行動裝置的逐漸流行，使的行動工作者的人數逐漸增加，這也是使得未可知的資訊安全風險層級明顯提高。有將近一半的受訪者都認為行動安全是未來很大的挑戰，不僅是在解決方案和資訊流上都需要更新，終端使用者，也就是這些企業的員工，其安全意識的水準才是一大挑戰。

該調查亦指出，只有十分之一的企業會在考量資安活動時，也將新科技趨勢造成的影響考慮進去。儘管有 23%的企業受訪者正打算採用雲端運算服務，但仍只有不到一半的受訪者表示會加碼資訊安全方面的年度投資。

2. 文獻探討

2.1 資訊安全管理制度(ISMS)

21 世紀企業隨著企業經營環境的變化，對於資訊依賴之重要度提高。資訊(Information)，已成為現今企業重要的資產，也是企業成功的基礎與命脈。如何確保企業資訊的機密性、完整性及可用性是當今最重要的課題之一，在今日許多組織均處於高度連網(內部網路與網際網路)的環境下，更顯示出其重要性。資訊安全管理系統(Information Security Management Systems，簡稱 ISMS)因此孕育而生，由英國工業貿易部倡導，正在全球普遍推行當中；2005 年國際標準組織(ISO)已正式頒布 ISO 27000：2005 資訊安全管理系統標準，且我中華民國也依此制定國家資訊安全標準，編號為 CNS 27001。

根據行政院資通安全會報規定，資訊安全等級列 A、B 級之政府單位必須於 96、97 年建置完成資訊安全管理系統(ISMS)，並取得第三方認證通過。在政府帶動及民間企業也體認 ISMS 的重要，許多大型電信業者或金融、資訊服務業，為取信於客戶，紛紛推動 ISMS 的建置。因此，在法規要求以及客戶期望下，這波 ISMS 建置熱潮帶動下，推行 ISO 27001 管理系統已成為企業永續經營之必要工作。

2.1.1 ISO 27001 沿革與歷史

國內國際標準組織(International Organization for Standardization, ISO)於2005年10月15日公佈ISO 27001資訊安全標準(全名是ISO/IEC 27001：2005 - Information Security Management Systems Certification)，為資訊安全管理系統(ISMS)之認證標準，是一種國際認可的資訊安全管理體系(Information Security Management Systems)驗證標準；ISO 27001資訊安全標準是從英國標準協會(British Standards Institute)提出之BS7799-2 標準(全名是BS7799 Information technology-Security techniques-Information security management systems-Requirements)，延伸整合而成的國際資訊安全標準，其演進過程如下：

1995年：英國公佈BS7799 Part I

1998年：英國公佈BS7799 Part II

1999年：英國公佈新版BS7799 Part I、II

2000年：ISO通過成為ISO/IEC 17799 Part I

2005年：ISO/IEC 17799：2005

2005年：BS7799：2-2005，2005年10月15日成為國際標準 ISO27001

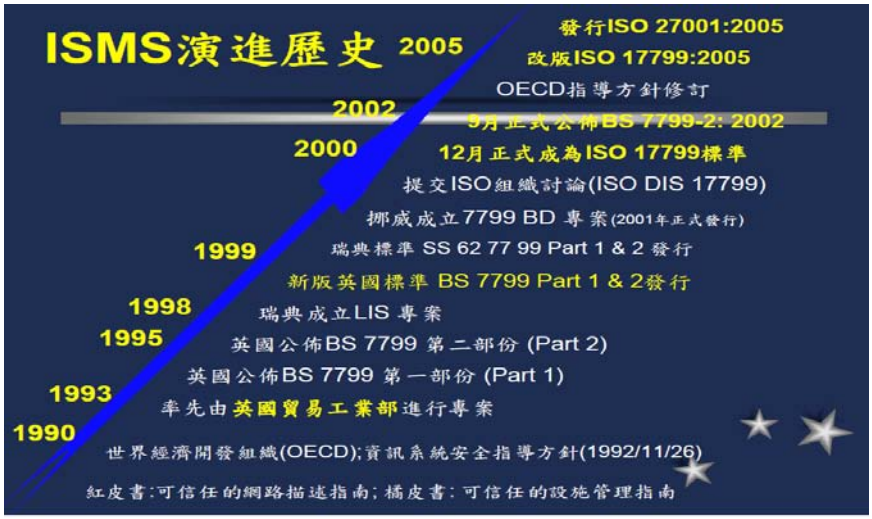

圖1:ISO 27001 演進歷史

(資料來源:經濟部標準檢驗局整理)

2.1.2 ISO 核心精神

ISO 27001 總計有 133 個控制要項，可歸納為安全政策、資產管理、風險管理、事故管理等十二系統框架(見圖 2)。

圖 2: ISMS12 大系統框架

(資料來源:本研究整理)

ISO 27001資訊安全標準的規範要求，是一般性且可廣泛應用的，適用於任何型式的組織，並不限制組織規模大小和營業性質；因此，只要組織在經營策略上有必須取得ISO27001資訊安全標準認證，皆可參考及依照ISO 27001資訊安全標準的規範，訂定欲取得認證的範圍，制定符合且適當的資訊安全制度文件及控制措施，運用「計劃、執行、檢查、行動」(Plan-Do-Check-Act, PDCA)持續改進模式運作(如圖3)，在整體資訊安全管理制度落實後，即可請驗證單位(例如：BSI、SGS、DNV)進行ISO 27001資訊安全標準驗證作業。

圖3: ISMS運作流程

(資料來源:經濟部標準檢驗局整理)

ISO 27001雖有百餘條項目，但事實上條文不會告訴說要做到什麼程度，才會獲得單項的滿分；而是要拿出證據(例如:政策文件、表單紀錄)，證明可以確保這個項目有做好安全管控。評量方式如此設計是因為每個機構的規模、人力、財力等狀況不同，很難用齊一的標準規範大家，ISO只要確認最主要的執行精神:Plan(計畫)、Do(執行)、Check(查核)、Act(行動)已落實在組織中，當組織運用這套循環模式的流程管理，即可自行調校做不好的地方、自我療癒與進化(如圖4)。

也因此導入過ISMS資訊安全管理系統的組織就知道，在這個管理系統裡沒有如聖旨般不可修改的文件、也沒有不會填寫的表單，當然不保證零事故發生，因為只要不足、不適當、有失誤，就將PDCA從頭來一遍，這樣組織就有能力自行調校出最切實的實用的資安政策與做法。

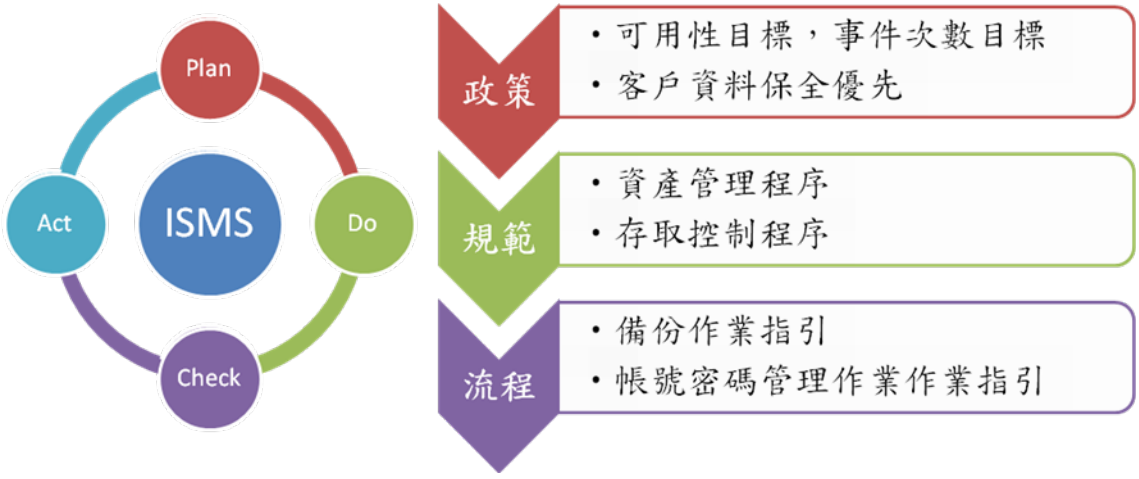

圖4 :ISO核心精神-PDCA

(資料來源:江敏霞2010整理)

2.2 資訊安全政策

Hong et al. (2006) 彙集過去有關安全政策的文獻，歸納出安全政策的共同概念而形成了「安全政策理論」 (Security Policy Theory) 。所謂資訊「安全政策理論」是透過資訊安全政策(Information Security Policy)制定、實施與維護程序並以資訊安全政策為核心所形成的資訊安全管理循環(Information Security Management Cycle)，經由政策的執行以實現資訊安全目標。該理論所闡述的要旨為資訊政策及在規劃資訊安全需求並在組織內形成安全共識，政策之制定與實施，之後定期對實施效果加以檢討修正以滿足組織的最新安全需求之資訊安全的管理程序，如圖5所示。

Wood (1995)認為資訊安全政策是組織高層次的安全目標與策略之一般性宣示。其描繪組織總體性的資訊安全之最高管理方針，並指出組織在整體安全上所要的依循的方向，其不涉及如何達成目標之具體實施手段、方法與步驟。資訊安全政策只需對於特殊問題，陳述其概念而不需做太過詳細或冗長的描述(Rees et al， 2003)。資訊安全政策可定義為組織如何管理與保護資訊資源以達到安全目的之規則，定將予以書面化且發布廣為使用者所知Allen (1968)。綜合上述定義，本研究認為資訊安全政策除了是依據組織目標、策略或需求，所形成的資訊安全管理方針外，它也是安全目標與方法的一般性陳述之書面化文件。故凡事可促進資訊安全政策順利推行並使其發揮成效的相關管理活動或實務，例如安全政策宣導、安全教育訓練等，這些為維護資訊安全所採取的控管對策皆為「資訊安全政策」。

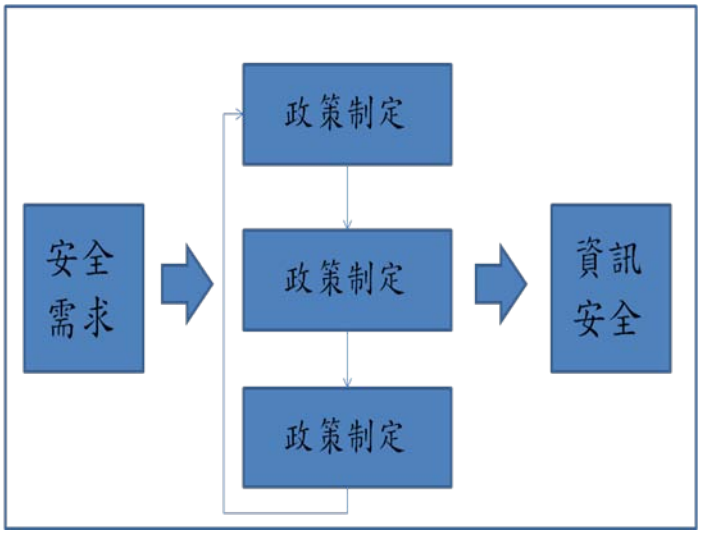

圖5:「安全政策理論」示意圖

資料來源:Hong et al. (2006)

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

2.2.1 制定資訊安全政策相關文件

資訊安全政策是有關組織資訊安全管理的方針與實作方法之大略性描述。因此組織

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

2.2.2 實施資訊安全教育與宣傳

Siponen (2000)提出資訊安全政策的成功實施，主要繫於組織是否提供的足夠及適當資訊安全教育訓練，讓成員了解安全政策對組織資訊安全的重要性也強化成員的安全認知，而主動將資訊安全政策規範及規則落實於工作中。Karyda et al. (2005) 及 Gaunt (1998) 的研究中亦指出資訊安全教育訓練與宣導的重要性影響，其結果發現有配合資訊安全政策宣導及訓練的組織，其整體成員具備有較高的資訊安全認知，而能遵循相關之安全政策規範，展現正向的安全態度、行為；反之在缺乏相關資訊安全教育訓練的組織，由於組織全體缺乏正確的安全認知，造成政策日後被採用與執行成效有限，也阻礙資訊安全文化的發展。此外 Horrocks (2001) 和Siponen (2000)指出資訊安全政策推行通常比政策的制定還困難，由於資訊安全政策的導入對組織而言是一項新項的規則，為了降低可能的衝擊與抗拒，充沛的資訊安全訓練可提供員工對安全政策規範細部的認識與對安全上的認知，有助日後員工便是潛在安全問題，進一步運用安全法則且降低安全問題所帶來的風險，並形成安全行為與態度並將其融入工作中。

2.2.3 實行違反資訊安全規範的懲處

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

2.2.4 資訊安全政策維護

根據ISO 27001所公布的資訊安全管理規範，說明資訊安全政策實行後，應定期檢視與評估現行的安全政策，特別是在組織或資訊系統運作改變，更需注意安全政策是否

符合現況而須進行跟新。Gupta(1991)和Flynn(2001)指出資訊安全政策及在規劃資訊安全需求，於組織內形成共識並制定與實施政策，之後定期對實施效果加以檢討修正以滿足組織最新安全需求，促進資訊安全的管理程序。資訊安全政策的維護與評估是一個回饋的機制，透過相關的評估維護，來驗證現有安全政策內容是否反映政府法令、外部環境及技術之最新狀況且符合組織目前需求，以確保資訊安全政策與組織實際作業之吻合且合乎時宜。同時，瞭解現有安全政策的使用狀況，發覺安全政策的缺失，作為安全政策修改與改善的依據，並重新形成適合的組織使用的資訊安全政策，讓資訊安全政策更可行而能有效推行(Karyda et al. 2005；Hong et al. 2006) 。

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

3. 分析架構與方法

3.1 研究模型

本研究旨在探討適用於行動式員工對於公司資訊安全上所帶來的影響。本研究變項分為：實體與環境安全、資訊安全風險評鑑與管理、安全組織、存取控制、制定行動工作者資訊安全政策文件、行動工作者資訊安全政策維護共六部份。本研究模型如圖 6 所示。

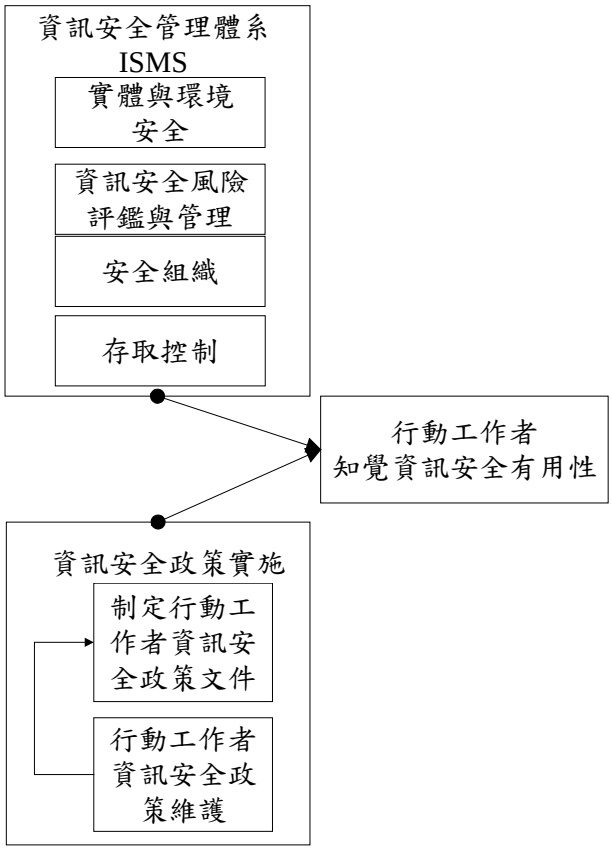

圖 6:本研究模型

(資料來源:本研究自行整理)

3.2 研究流程

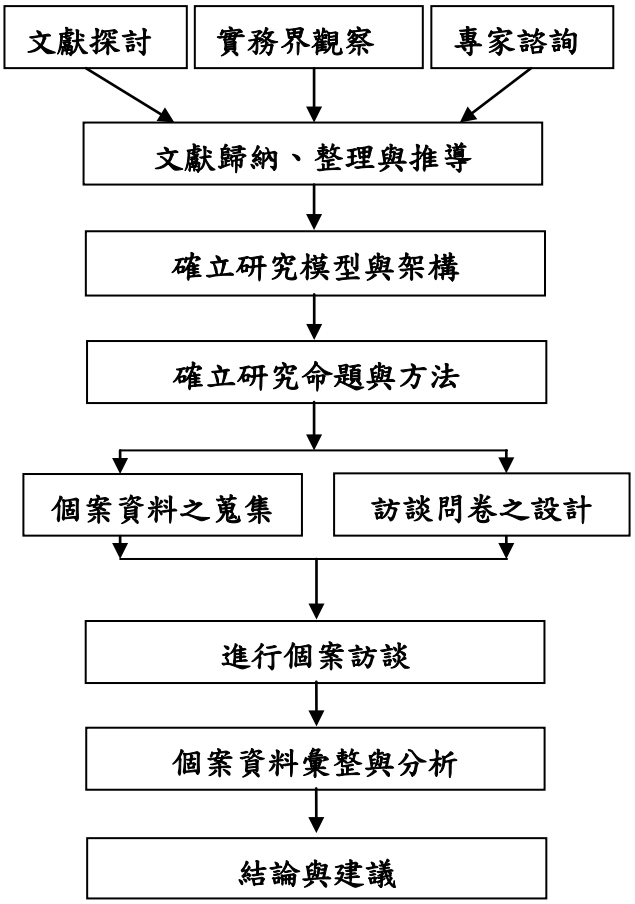

圖 7：本研究之研究流程圖

(資料來源:本研究自行整理)

3.3 研究設計

本研究採用個案研究法，個案研究可採用的資料收集方法有下列幾種：訪談(開放式或封閉式問卷)、親身參與、觀察法、組織內部資料、書面文件(正式報告、公文、剪報資料等)、檔案分析。在正式實地收集資料前，需設計好所欲收集的資料項目、訪談問題等。所收集的資料紀錄亦馬上處理。甚至用三角驗證法來驗證資料的真實性，包括：(1)資料收集的相互驗證。(2)研究人員的相互驗證。(3)理論的相互驗證。(4)方法的相互驗證等幾種的複驗。

個案訪談進行的方式如下所示：

(一)本研究以凌群電腦股份有限公司、庫柏資訊軟體股份有限公司、達友科技股份有限公司與阿碼科技股份有限公司做為個案研究對象。採用專家訪談的方式進行訪談，以軟體公司為訪談對象。故，將分別訪問上述四間公司之專業人員。先透過中華民國資訊軟體協會代為與凌群電腦股份有限公司、庫柏資訊軟體股份有限公司、達友科技股份有限公司與阿碼科技股份有限公司聯絡；再與公司受訪人聯絡，約定訪談時間。

(二)至受訪個案公司與受訪者進行實際面對面深入訪談。為避免訪談重要資料遺漏，故進行訪談時向受訪者徵詢及說明使用錄音裝置的必要性。經取得受訪者同意後，本研究

全部訪談過程皆以錄音之方式記錄與保存，以確保訪談過程中相關資料之完整性。

(三)本研究之問卷分為二部分：第一部份為結構化問項，第二部分則為非結構式之開放式問卷。進行實地訪談時先由受訪者填寫結構化問項部分，若對問項有所疑問時，研究人員應立即與受訪者作溝通與解釋；而非結構化問項部分則由研究人員與受訪者作深入訪談，訪談過程全程以錄音裝置進行錄音。

(四)於個案公司訪談結束後，研究人員即將個案訪談所得之記錄資料予以匯整，並將訪談相關資料以電腦建檔，依每家個案進行分類歸檔，以利本研究後續歸納與分析之用。

4. 個案研究與分析

4.1 訪談對象背景

本節陳述訪談對象的背景資料。茲列出訪談對象的成立背景、發展現況等資訊如下：

表 1:個案公司資料

	A 公司	**B 公司**	**C 公司**	**D 公司**
名稱	凌群電腦	庫柏資訊	達友科技	阿碼科技
成立年度	1975 年	2002 年	2003 年	2005 年
員工總人數	1000 人	60 人	23 人	60 人
資本總額	11 億元	1550 萬元	2150 萬元	1 億 3000 萬元

資料來源:本研究自行整理

4.2 個案分析

4.2.1 A 公司非結構化訪談彙整結果

(1) 公司參考國際資訊安全規範 ISO 27001 標準，並由公司資訊安全中心評估公司風險，考量風險發生情況來規畫解決之道，並依照規劃內部 SOP 相關配套措施來解決相關風險。

(2) 由公司客戶服務部事業群的資訊安全技術處所負責，屬於一級單位，並由此單位規劃與推動公司資訊安全政策。

(3) 公司進出皆透過刷卡進出，所以進出機房會有刷卡機制與監控設備來管控。

(4) 對於公司資訊安全政策上，面對機密資料連結會透過加密方式來保護資料，並定期每三個月備份資料。

(5) 公司採用 CISCO 設備，透過外部網路存取時，採用 CISCO 專用的 VPN 加密連線方式，並採取身分鑑別方式來確認使使用者，避免資料被截取。

4.2.2 B 公司非結構化訪談結果彙整結果

(1) 公司規模較小，所以在人員工作分配及負責項目都同時身兼多職，因人力不足在加上 ISO 27001 並非每項規範均符合公司所需，所以只參考部分 ISO 27001

重點，來提升公司資訊安全的防護。

(2) 公司產品主要為資料庫方面，也非常了解資料庫內的資料十分重要，因資料庫內是存放所有的資料，所以一但資料被竊取，對於公司商譽的影響是非常大的。

(3) 行動式員工在外，透過外部網路存取公司內部資料都使用 SSL VPN 加密方式來存取資料，以確保連線上的安全。

(4) 而公司認為行動裝置所帶給公司最大的效益，是能給即時處理顧客問題，並提高工作效率與速度。

4.2.3 C 公司非結構化訪談結果彙整結果

(1) 公司資安參考 ISO 27001 規範，並遵循 ISMS 中 PDCA 流程，並透過風險轉移、規避風險等方式讓損失降到最低。

(2) 公司員工的行動裝置大多屬於個人財產，雖無強制規定要安裝加密工具等軟體，但在存取控制上的管控以及 SSL VPN 的方式，只能拿到數筆，確保連線安全以及員工無法存取公司內部全部資料，避免資料外洩。

(3) 對於新版個資法的看法以及內部建議，若資料不慎外洩時，一定要主動告知受害者，並提供協助。二來要佐證公司相關資安資料，證明公司已做到最妥善的安全防護規劃，讓公司的損失降到最低。

4.2.4 D 公司非結構化訪談結果彙整結果

(1) 公司內部系統已逐漸使用 GOOGLE 企業版相關服務，將資料存放在雲端，透過雲端的方式來使用，不僅可以讓資訊安全的疑惑降到最低，更可精簡在資訊安全上的人力。

(2) 對於公司部分服務還未轉向 GOOGLE，透過外部連線是使用 SSL VPN 方式連線，來存取公司內部資料。

(3) 對於新版個資法，若屆時公司個資外洩，第一:須了解哪些資料被竊取。第二:聯絡個資被竊的客戶。第三:協助個資被竊的客戶。第四:提供公司對於資安上的相關證明。以降低對公司的傷害。

5. 結論與建議

5.1 研究結論彙整

5.1.1 風險評鑑與管理：

四家公司均參考 ISO 27001 規範，主要是 ISO 27001 為資安領域中的標竿，並依照 ISMS 中 PDCA 流程執行。比較值得注意的一點，個案 B 公司與 C 公司均提到公司對於 ISO 27001 的規範，並無足夠的人員來規劃與執行，所以操作上會與 ISO 27001 規範內容有所落差。而個案 A 與 D 公司因公司規模較大所以有較足夠的人員來參與規劃和執行。所以 ISO 27001 雖是各家公司對於資安認證所追求的方向，但須考量公司大小規模及人力上的安排。

5.1.2 安全組織：

個案四家公司的資安工作均由資訊部門所統籌負責已執行。根據 MIC 在 2007 年針對台灣大型企業資安現況的報告指出，有七成大型企業的資安人力配置低於 2 人，其中 5.6%根本沒有設置任何資安人力，而僅配置 1 人的大型企業也佔有 30.4%。可看出多數大型企業的資安人力配置明顯不足。因此對網管人員來說，除了確保網路連線順暢的既有任務之外，防制可能的網路攻擊也成為必要的責任。但是該如何去防治千變萬化的網路攻擊手法，若缺少適當的學習方式與管道，資安工作就會變成是個沈重的負擔，尤其是資安涵蓋的層面太廣，如果沒有適當的認知與學習方法，恐怕也會迷失在茫茫的資安大海之中。

5.1.3 實體與環境安全：

個案四家公司對於資安實體的管理，對於機房均透過門禁管理與監控方式來管理。而 D 公司已逐漸將資料雲端化。其他三家公司還是普遍將資料存放公司機房，但已漸漸朝向部分資料雲端化、部分機密資料，並思考如何有效節省成本是未來的方向。

5.1.4 行動式資訊安全政策：

A 公司與 D 公司會強制控管員工的行動裝置，透過適當的管理可以有效的控管資訊安全。而 B 與 C 公司，因大部分的行動裝置屬於員工個人設備，不能強制控管只能口頭上的建議，所以對於資安的風險存在較高。

5.1.5 存取控制：

四家公司行動裝置均透過 SSL VPN 方式來連線，此方式可避免外部不安全的網路，但需思考公司資安環境是否完善，否則即使確保透過 VPN 連線是安全的，但內部網路已出現漏洞豈不是沒有防禦的效果存在，所以內、外網路均需妥善規劃資訊安全。

5.2 實務建議

5.2.1 資料雲端化

在雲端運算環境下，遠端用戶及行動工作者有可能會藉由網咖、家中／飯店內的電腦、委外廠商／合作夥伴的設備，以及外地出差人員本身攜帶的行動裝置等多樣方式，連線回公司進行資料存取作業。為確保其存取的安全性，有部分雲端運算業者開始提供 SSL VPN 加值服務技術，利用 SSL 進行加密的遠端登入及權限控管，以建立安全的虛擬私有網路，供遠端用戶使用。李立國指出，由於使用者能任意使用一般網頁瀏覽器，建立 SSL VPN 通道，因此可同時兼顧方便與安全性，而系統管理人員亦可針對各項應用程式及使用者，制定存取控管政策。一般認為，促使企業採取各種雲端代管服務的最大動能即是節省成本，不過雲端安全聯盟(Cloud Security Alliance)創辦人之一的 Tim Mather 提醒，各企業在採用之前，應先自我檢視，倘若企業計劃將內部資料移往公有雲，首先要做好資料屬性分類、有效的管理與移轉機制，也要有相關配套的資安程序與技術，甚至整體企業營運模式也必須跟著調整。

5.2.2 接納資訊安全產品服務化的市場轉變

據本研究非結構化資料分析顯示，多數個案公司的資安防護措施，仍以購置軟硬體防護設備為主。然而，資安產品與一般實體 IT 產品不同，隨著資訊科技不斷創新、企業 IT 及 IS 結構變動，資安設備也需定期更新或是政策調整，因此，資安廠商所提供的

售後服務也就相形重要，然而，據資訊安全專業管理雜誌「資安人」(2010)指出，有太多企業無法接受買了軟硬體設備還要買服務的商業模式，企業普遍只願花錢買設備而不願採購資安服務，資安市場買賣雙方的認知差異，致使資安廠商的營運模式漸漸地轉變，除了實體軟硬體產品銷售外，也演繹為純粹服務化的資訊安全商業模式。資安產品服務化概念成型後，有越來越多的 IT 廠商從銷售軟硬體轉型為資安服務提供業者，資安廠商轉型為「服務提供商」的趨勢在資訊安全領域裡格外地顯見，箇中原因很多，其一就是企業無法認同買軟硬體又要買服務的商業模式，因此資安廠商乾脆改變商業模式，改以資安服務提供商自居。

再者，受到雲端運算(Cloud Computing)與軟體服務化(Software As A Service)盛行的影響，公司資訊結構轉變，IT 軟硬體設施不見得都在公司的管理環境或者機房內，部分已經授權由資訊業者管理，故在選擇資安解決方案時，就必須考量服務形式的資安方案。例如：當企業 Mail Server 交由資訊業者代管時，資安業者便成了唯一有能力提供資安相關服務的角色。

在高度競爭的資訊市場，商業模式瞬息萬變，只要有機會發展新商務，縱使不是軟硬體研發廠商，但只要有資訊配置及管理的專業人員，仍然有機會掌握商機，且資安領域涉及許多專業知識以及經驗累積，這種產業特性讓廠商的代管服務有了很大的發展空間，需求端可以客製化地選擇要如何安排人力及其它資源，服務供應商則能專注於特定領域，提供更有經驗更專業的服務，進而藉由規模經濟(Economy of Scale)來降低服務成本。

另外，近幾年企業的資安架構逐步從防火牆內(公司內部網路)移動到防火牆之外(資訊服務廠商)，是最顯著的變化之一。例如：以前的郵件安全解決方案，通常是將軟體安裝於郵件伺服器，或是直接在郵件伺服器前端架設郵件安全硬體設備，以達到郵件安全的防護目的，然而，現在有越來越多的廠商會直接把郵件防護機制挪到自家機房中，形成了企業將郵件傳送配置(MX record)導向廠商的服務點，而本地端郵件就只與廠商進行服務交談。例如：當初入侵防禦/入侵偵測系統(IPS/IDS)的商業模式就是直接採購 IPS/IDS 硬體或軟體，然後安裝使用。不過，現今有越來越多的第三方資訊業者直接代企業管理或監控系統，業者會與資訊部門討論入侵偵測的架構以及執行方式，並配置設備，最後，由 MIS 微調設定後，交付廠商監控，如果遇到特殊情況就通知 MIS 進行下一步的處理，平常則委由資安業者進行一般監控，讓企業可以專注於核心競爭力上。而資安服務化的產品，除了郵件安全代管與入侵偵測系統(IPS)代管外，還有認證服務、程式碼開發安全稽核、安全設備代管(防火牆、VPN)、滲透測試(Penetration Test)、程式補強管理(Patch Management) 、防毒管理等等，幾乎舉得出來的資安課題，都有資安業者可以提供相對應的代管服務。

資安服務化的優點，資安人(2010)指出，包括：1.因應資訊環境其他環節服務化，資安服務化才能讓這樣的資訊環境與安全需求緊密結合，提供更適合的安全功能；2.集中企業資源專注發展核心價值，資訊安全雖然屬於高度機密的作業，但並不代表企業不能將部分資訊安全的功能外包予廠商；3.符合企業的財務政策，以往購買軟硬體的作法，在會計科目上必須列為資產(assets)且要計算折舊(depreciation)，但採購服務卻是屬於費

用(expense)的一環，部分企業的財務策略傾向於後者，此點效益雖然跟資訊安全課題沒有直接關係，但站在經營者的觀點來看，卻是必須納入考量的一環。而資訊服務化的缺點，包括：1.增加資料外洩的風險，這部份與資訊安全功能的特性有關，如果該項資訊安全服務有可能要檢視公司的機密資料，企業就得考量機密資料外洩的風險；2.購買資安服務與傳統購置軟硬體觀念不同，需要時間來增加接受度；3.某些計畫需要兩個(或以上)廠商共同合作的時候， 就增加了整合的困難度，例如：公司需要將虛擬私有網路(VPN)結合雙重認證(two factor authentication) 來增加安全性，分別交由不同的資安服務商來管理，如何整合雙方資源完成設定，透過廠商管理以及專案管理來降低整合的困難度便相形重要，便成為計畫的難度之一。

綜言之，無論企業是否喜歡這樣的市場轉變，現在的趨勢的確是往資安服務化的方向來走，然而，根據資安人(2010)，以下是幾點可供業界於資安服務化趨勢下的因應之道：1.維護以及更新資訊環境的架構圖。無論資訊環境的哪些架構發生改變，例如：引進新的解決方案、資訊流改變等，MIS 或 IT 人員都要隨時更新，唯有確保最新最正確的資訊架構，才能在評估資安服務的時候做出正確決策。2.服務等級協定(Service Level Agreement)。購買資安服務，甚至任何服務時，與廠商簽訂雙方同意服務品質是一個重要關鍵，除了廠商對客戶口頭承諾應有的服務品質，企業仍然必須與之簽訂協議，以防範當服務等級達不到的時候，廠商應有的相對應合理賠償。3.在選擇資安服務的時候，須謹慎且有計畫地規劃選擇合適的服務方案，從上述第一點的資訊架構圖進行分析，思考如何分割或規劃資訊環境、哪些資安工作可以放到遠端由廠商來做、哪些因為機密或者其他考量而必須放在公司內部處理，接著再評估合適的服務方案，如果擔心服務所帶來的反效果，則應思考透過何種方式將壞處降到最低 ，例如：將機密資料環境切割隔離、簽訂保密條約等。4.資安產品服務化，並不代表企業 MIS 人員可以輕輕鬆鬆地放手給服務廠商去作所有的事情；雖然有些資安作業不在公司內部進行，MIS 人員仍然要瞭解服務運作的模式、特性及細節，一旦發生緊急情況，或是有新的需求出現，MIS 人員才能做出正確判斷，找到對的廠商，進行對的任務，並把資訊安全服務所帶來的正面效益發揮到最大。

5.2.3 全球行動工作風潮盛行 提升員工資安意識

行動設備普及化與商業模式轉變，使得行動工作者的人數激增，然而這也使得未知的資訊安全風險層級明顯地提升。根據安永會計師事務所於 2010 年的 6 至 8 月間，針對全球 1,600 家企業進行全球資訊安全調查顯示，有將近一半的受訪者都認為行動安全是未來很大的挑戰，不僅是在解決方案和資訊流上都需要更新，終端使用者，也就是這些企業的員工，其安全意識的水準才是一大挑戰。該調查亦指出，只有 10%的企業會在考量資安活動時，會將新科技趨勢造成的影響考慮進去。儘管有 23%的企業受訪者正打算採用雲端運算服務，但仍只有不到一半的受訪者企業表示會加碼資訊安全方面的年度投資。儘管如此，相較於 2010 年度，安永會計師事務所針對 2011 年度的資安預期調查顯示，比起去年將有 50%的企業受訪者將會增加防制資料外洩的支出約 7%左右，過去市場反應比較冷淡的加密技術市場也有將近 30%的企業正在實施，並且針對身份和使用權限控制也有 28%的企業更加嚴格的進行管理，而有將近 4 成的受訪者也在進行資安策

略的調整。綜言之，提升行動工作者的資安意識才是企業面對全球化行動商務浪潮下的第一道資安防護根本。

5.2.4 改變行動工作者的商務習慣

本研究之受訪個案無不擔憂個資法通過後的罰則問題，以及因應之道是否足夠。然而，許多資安廠商領著個資法口號大肆宣傳，似乎只要導入資安工具就能避開個資外洩風險，但是，SGS 全球產品經理呂敏誠認為，員工作業流程比 IT 工具更重要，企業不一定要導入 IT 工具，甚至有時只要改變作業習慣，也許就能避開個資外洩的風險。行動工作者面對變動的商務辦公環境亦是如此。KPMG 資訊科技諮詢服務公司也認同指出，新版個資法通過後，企業必須改變以往的商務習慣。例如：電子商務業者經常將送貨單及訂購者的手機號碼貼在商品外箱上，雖說是方便送貨員聯絡訂購者，但也容易外洩了消費者的消費資訊及個人資料；或者，例如：銀行可能為了達到行銷目的，允許理專大量下載客戶資料並存放在 USB 中，這就是一個資料管控的商務習慣缺失。另外，像東森購物在經歷個資外洩事件後，也提高了客服人員對資料存取的管控，例如：電腦禁止連到外部網站、員工不能攜帶手機或紙筆等，雖然沒有工具，卻同樣以改變員工商務習慣達到資安管控目的。企業面對日益增長的行動工作者，其根本措施亦是如此。綜言之，企業要防範行動工作者或所屬員工外洩個資的方法有很多，而購買資安工具亦非首要王道，最重要的還是回歸根本，從員工的作業流程或商務習慣著手。

5.2.5 收回離職員工資料存取權限

據受訪個案對於資料存取控制的機制表示，為了保障公司的資訊安全，降低 MIS 部門的管控負荷，企業需要的是一套有效的極簡權限(Least Privilege)管理機制，從根本上來解決 Windows Admin 權限管理窘境。透過極簡權限管理原則，協助企業讓所有 Windows O/S(Windows XP、Vista、Win7、Server 2003、Server 2008)的電腦僅能以標準使用者(Stand- ard User)身份運作，有效減少電腦中毒機率以及蓄意或無意的系統設定修改；或者由於所屬員工任意安裝非法軟體、個人軟體而導致工作效率低落、濫用公司資源；更能為 MIS 部門省下重覆性的電腦重灌、環境設定與程式安裝等不具生產力的繁瑣工作，進而將有限的人力、資源投入到對企業貢獻度更高的商業任務。以確保企業不會因為離職員工或管理員存取權限收回問題，影響企業日常營運流程或資訊安全。良好的權限管理機制不但減輕了 MIS 部門的工作負擔，也大幅提昇企業 IT 環境的整體性與安全性，降低企業 IT 資產的生命週期成本(TCO/Total Cost of Ownership)。

綜合本研究受訪個案表述及資安人(2010)，企業面對行動工作者資安權限問題實質作法例如：1.提昇 Windows 7 UAC 使用便利性，避免干擾行動工作者業務，杜絕管理員帳號洩漏問題，企業可使用警示小視窗或是不干擾使用者的靜默模式，要求使用者輸入理由、申請開放安裝軟體、或是執行使用者身分認證。2.選擇性開放部分系統管理工具(例如:網卡、印表機、磁碟重整、系統小時鐘)給使用者，杜絕使用者自行修改系統設定的機會，減輕 MIS 的管控負擔，收回本機管理員(Admin/Power User)權限，達到極簡權限的企業最高管理原則；3.符合資安法規的管理員權限回收要求，例如: PCI DSS、沙賓法(SOX)、HIPPA、以及政府的資通安全檢測評鑑需求；4.可依 AD 使用者/群組定義權限開放政策；5.降低病毒、木馬、惡意程式、間諜程式入侵的破壞力；6.彈性化允許/ 限制

使用者安裝與執行程式，防止行動工作者或員工未經公司同意安裝盜版或個人軟體，提昇公司系統與網路的可用性與穩定性；7.選擇性允許/限制 ActiveX 控制元件的安裝。

5.3 研究限制與未來研究方向

5.3.1 個案研究之概化能力不足

個案研究法主要是追求研究的內部效度而非量化統計的外部效度(Yin 1994)，但為了提升本研究之外部效度，本研究採用多重個案的訪談方式進行。但礙於訪談資料來源受限，只能對四家個案公司作分析與整理，因此研究結果概化程度仍有其限制，且樣本數過少，導致沒有足夠公司高層樣本數來進行統計驗證分析。所以，未來有足夠使用者時，仍需更進一步以定量研究之法來增加本研究之外部效度。

5.3.2 受訪者主觀意識限制

本研究係探討產業別網際網路資料庫網站整體行銷，其涵概之範疇甚廣，受訪者對此研究議題之熟悉度與主觀認知之程度皆對本研究之結果有所影響，且因本研究探討之問題牽涉層面甚廣，受訪者礙於本身職務與專業知識等限制，很難對每一問題都能瞭解與熟悉，因此，只能依本身主觀認知之想法來解釋與回答，且每位受訪者對本研究議題之熟悉度很難一致，難免有所偏誤。鑑此；後續相關研究可以多重線民之訪談方式，以降低受訪者主觀認知所造成之偏誤。

5.3.3 橫斷面之研究

本研究係為橫斷面之研究，優點在於容易掌握研究當下某一時間點的現象、情境、問題、態度或議題等，但在人力、時間的限制下，本研究無法針對各家公司決策考量進行長時間的觀察與比較，且因每個公司所屬之性質不一，因此，採用長期縱斷面之研究方法將使本研究更具信度與效度，但受限於本研究之人力與時間上之限制，僅能對現今四家個案公司高層主管思維作比較對照，而無法對此四家個案公司作長時間之觀察與分析。

5.3.4 未考慮企業對資訊安全文化的研究

在文獻探討中討論到資訊安全成為組織安全上重要的一環，故近年來國外學者開始逐漸探討「資訊安全文化」一詞。(Chau 2005)、(Kuusisto et al. 2004)和(Martins與 Eloff 2002)皆認為資訊安全文化文組織文化的一環，它指引個人、工作與組織特徵對組織的安全影響，故資訊安全文化的發展可以視為如同組織文化產生的過程。

在未來的研究建議上可探討組織與安全文化定義之共同要素：『組織成員所共享的資訊安全態度、價值、規範及實務，使資訊安全成為員工日常活動中自然的一面，以此所支援所有的活動，建立外部參與者間之信任』。並藉由安全政策規範與程序的落實並建立具體的安全管理，方能讓相關作業的資訊井然有序且能有效的稽核，並讓員工更能融入安全態度與習慣，進而形成一個對組織與個人有價值的資訊安全文化。另亦可針對大公司的CIO進行對資安防護措施之個案訪談，如此，可深入了解企業應用面與資訊軟體公司對行動資安防護上認知。

6. 參考文獻

[1] 吳依恂 ，2010，「全球行動風潮盛行 50%企業主擔憂員工安全意識不足」，資安人雜誌，第 72 期，11 月。

[2] 李東峰，2003，「企業資訊安全控管決策之研究-從組織決策理論觀點探討」，博士論文, 國立中央大學資訊管理研究所。

[3] 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》，第三期。

[4] 資策會產業情報研究所 ，2010，「2010-2011 台灣大型企業資訊科技投資與應用趨勢」，資策會產業情報研究所，臺北市。

[5] 資安人雜誌，2008，台灣人，你為什麼不買服務!?」，第 53 期，6 月。

[6] 資安人雜誌，2010，「Admin 權限未能收回，資訊安全等於白做！」，第 71 期，9 月。

[7] 資安人雜誌，2010，「中小企業 IT 人力委外，創造三贏：節省成本、提升效益、兼顧安全」，第 69 期，5 月，6 月。

[8] 資安人雜誌，2010，「內容感知的 DLP 技術探討」，第 69 期，5 月，6 月。

[9] 資安人雜誌，2010，「後個資法時代之 Log 安全稽核記錄管理」，第 69 期，5 月，6 月。

[10] 資安人雜誌，2010，「輕忽委外管理工作 小心埋下資安地雷」，第 72 期，11 月。

[11] 廖邦彥，2010，「資安買服務 聽聽資安人員怎麼說」，資安人雜誌，第 71 期，9 月，10 月。

[12] 廖珮君，2010，「改變作業習慣 避免個資外洩不必花大錢」，資安人雜誌，第 71 期，9 月。

[13] 蘇建源、江琬瑠、阮金聲，2010「資訊安全政策實施對資訊安全文化與資訊安全有效性影響之研究」，中華民國資訊管理學報，第十七卷，第四期：61-87 頁。

[14] Adams, J.S., Tashchian, A., and Shore, T.H. "Codes of ethics as signals for ethical behavior," Journal of Business Ethics (29), 2001, pp:199–211.

[15] Allen, B. "Danger ahead! Safeguard your computer", Harvard Business Review, 1968, pp97-101.

[16] Anderson, J. M. "Why we need a new definition of information security", Computers & Security, Vol. 22, 2003, pp:308-313.

[17] Baggett, W. O. "Creating a Culture of Security," Internal Auditor, 60(3), 2003, pp:37-39.

[18] Barney, J. B. "Organizational Culture: Can It Be a Source of Sustainable Competitive Advantage? ," Academy of Management Review, 11(3), 1986, pp:656-665.

[19] Fang, D.P., Chen, Y., and Louisa, W. "Safety Climate in Construction Industry: A Case Study in Hong Kong," Journal of Construction Engineering and Management (132: 6), 2006, pp:573-584.

[20] Ford, R. C., and Richardson, W. D. "Ethical Decision Making: A Review of the Empirical Literature," Journal of business ethics (13:3), 1994, pp:205-221.

[21] Flynn, N.L. The Epolicy Handbook: Designing and Implementing Effective E-mail, Internet and Software Policies, American Management Association,2001, New York, NY.

[22] Gaunt, N. "Installing an Appropriate Information Security Policy," International Journal of Medical Informatics (49:1), 1998, pp:131-134.

[23] Gupta, Y. P. "The Chief Executive Officer and the Chief Information Officer: The Strategic Partnership," Journal of Information Technology (6:3-4), 1991, pp:128-139.

[24] Hone, K., and Eloff, J. H. P. "Information Security Policy－What Do International Information Security Standards Say? ," Computers & Security (21:5), 2002, pp:402-409.

[25] Horrocks, I. "Security Training: Education for an Emerging Profession? ," Computers & Security (20:3), 2001, pp. 219-226.

[26] Karyda, M., Kiountouzis, E., and Kokolakis, S. "Information Systems Security Policies: A Contextual Perspective," Computers & Security (24:3), 2005, pp:246-260.

[27] Loe, T. W., Ferrell, L., and Mansfield, P. "A Review of Empirical Studies Assessing Ethical Decision Making in Business," Journal of business ethics (25:3), 2000, pp:185-204.

[28] Siponen, M. T. "A Conceptual Foundation for Organizational Information Security Awareness," Information Management & Computer Security (8:1), 2000, pp:31-41.

[29] Straub, D. W. "Effective IS Security: An Empirical Study," Information Systems Research (1:3), 1990, pp:255-276.

[30] Thomson, K. L., and Von Solms, R. "Information Security Obedience: A Definition,"

Computer & Security (24:1), 2005, pp:69-75.

[31] Tudor, J. K. Information Security Architecture: An Integrated Approach to Security in the Organization, CRC Press, Boca Raton, 2001.

[32] Rees, J., Bandyopadhyay, S., and Spafford, E. H. "PFIRES: A Policy Framework for Information Security," Communications of the ACM (46:7), 2003,pp:101-106.

A business plan of information security for mobile workers

Author[1]: Li-Ling Hsu Author[2]: Hau - Chau Chen Author[3]: Bill Chiu

[1] NKFUST karenhsu@ccms.nkfust.edu.tw
[2] NKFUST u9524038@gmail.com
[3] Gudeng Precision Industrial CO., LTD. Bill@gudeng.com

Abstract

Along with the rapid development of technology, people and businesses more and more rely on information systems, also, more and more businesses use mobile device to increase work efficiency. According to a prediction of IDC, mobile workers will exceed 1 billion, even reach 1.2 billion and become one third of whole world people until 2013. As soon as business mobility brought lots of opportunities for the market, it also brought information security problem and threat that we can ignore. Businesses have to set these mobile device, ensure security and do daily management.

We uses evaluation mode of BS7799 to discuss a case company's mobile information secure activity to survey its cognition and development of mobile information secure activity of this company. Moreover, we use indicators of confidentiality, usability and integrity to evaluate information secure risk to realize the difficulty of implementation and reduce risk efficiently. We discuss from literature and practice observation to draw a conclusion to collect demand of information systems of every single company to achieve sustainable operation.

Key Word : Mobile Workers、Information Security