第壹章　緒論

第一節 研究背景與動機

隨著資訊科技的發展，網際網路爲我們的生活帶來了更多的便利性。不論政府、企業甚至是個人都講求 e 化生活與服務，各方面的電子化，如政府電子化、企業電子化、生活電子化…等，使得網際網路更融入於我們的日常生活中。在這個資訊系統與網路連結快速成長的時代中，各個機關、企業組織以及個人使用者也越來越仰賴資訊系統間所帶來的便利性，習慣透過資訊系統來做資訊間的交流。不過，只要有網路的地方，網路威脅便無所不在。隨著網際網路與資訊科技的蓬勃發展，網路威脅的種類與管道也愈來愈多變。

客戶滿意度一直以來都是企業組織非常重視的問題之一，也是令企業組織難以去擔保的，即使這些企業組織處於最佳的環境之中也是如此，尤其是企業組織正面臨網路威脅的攻擊之下[24]。當企業組織無法做到將客戶資料保密不會外洩時，很多交易與合作機會皆會因此而錯失掉，直影響也將直接或間接地反應在企業組織的收益上。根據報導，病毒的攻擊已經造成無數金額的損失，而且還會繼續加速增長它所影響的範圍以及嚴重性[8]。而且這些攻擊對於有使用電子商務（E-Commerce）的企業組織比沒有使用電子商務的企業組織影響要來得嚴重[23]。根據 Radicati Group 的估計，影響資訊工作環境（Information Workplace）的網路威脅在 2006 年將會使得企業組織損失超過 540 億美金的金額。對於企業組織而言，必需去保護資訊工作環境以避免來自透過電子郵件、即時通訊軟體與文件分享的管理等管道所帶滲入的網路威脅的攻擊，因爲這個環境是企業組織將資訊與員工、生意夥伴、客戶與其他股東等人員做交流的平台。讀取的安全性、認證的管理、確認的程序、入侵的偵測等，每一個環節對於企業組織的安全系統都是非常重要的，馬虎不得。只要一個環節出了錯，就會直接或是間接影響該企業組織的形象與顧客對該產品服務的滿意度上。

賽門鐵克（Symantec）2002 年全球性網路安全威脅研究報告（Symantec Internet Security Threat Report）顯示，網路安全漏洞數量正急速地上升。當網路使用的人

數增加時，其遭受到的網路攻擊與威脅的潛在風險也會相對地提高。該報告中也指出在 2002 年上半年，平均每星期每一家公司所遭受到的有計劃性之網路攻擊有 32 次之多。駭客會利用新的安全漏洞，輕易地入侵各企業組織的資訊系統的現象仍然沒有改變。由於某些資訊系統安全漏洞並不需要使用攻擊程式（exploit code），或是這些攻擊程式非常容易被取得，使得約有 60%的新安全漏洞仍然非常容易被當作駭客入侵攻擊的管道。據該份統計，在 2002 年有 23.7%的安全漏洞攻擊程式確實能夠輕易地被取得。

另外，在賽門鐵克 2005 年所公佈的網路安全威脅研究報告顯示，發現「網路釣魚」（Phishing）[13]於半年內大幅度地成長 366%，根據該份報告統計，2004 年 7 月平均每週有 900 萬次的「網路釣魚」攻擊，到 2005 年底時，已經高達每週 3300 萬次。而且機密遭竊、網路應用程式漏洞，以針對 Microsoft 平台的電腦病毒等威脅，都持續困擾著使用者。在近幾年來不斷廣被使用的即時通訊軟體（Instant Messenger）也會被超過 20 種蠕蟲所利用來散佈以攻擊全球各使用者的電腦[22]。即時通訊軟體將是遭惡意攻擊的新的平台。除此之外，病毒與網路威脅對企業組織所造成的影響，也使得企業組織所需要回復的時間（Recovery Time）比之前增加了。從 ICSA Lab Virus Prevalence Survey 2004[28]所做的調查，300 位受訪者中有 112 位受訪者的組織，2004 年所受到的病毒爆發數比 2003 年成長了 12%；而 2004 年，企業組織的回復時間也增加爲 7 個工作天，約增加了 25%。

一連串的全球病毒疫情爆發事件更讓網路安全動盪不安，也讓企業組織非常地憂心。根據 IDC 在 2004 年所做的企業安全調查（Enterprise Security Survey）顯示病毒的攻擊是永不停止的，所攻擊的企業組織規模也不分大小[11]。快速增加的 Bot program[26]、垃圾郵件、網路釣魚、以及越來越猖獗的間諜軟體（Spyware）與廣告軟體（ADware），都在顯示現在的網路攻擊目標是全面性的－網路上的每個環節的每個弱點、每台有漏洞的電腦、每個可能警覺性不夠的電腦使用者，都可能成爲駭客覬覦的攻擊對象，或其藉此賺取每一分不義之財的機會。駭客的攻擊技術日新月異，惡意程式傳播的速度與廣度今非昔比了，潛在的巨大不法獲利也是網路攻擊事件頻傳的原因之一。當我們對於電腦網路的依賴感愈重，組織內部所面臨的威脅也就愈大。對於企業而言，不論是天災還是人爲的疏忽，所造成的資料毀損的災難，都會對整個組織帶來莫大的衝擊與影響。使用者如果疏於防

範，將導致嚴重的財務損失、機密外洩及資料遺失；而企業在現有資源上，也將承受更大的壓力。

根據美國的電腦危機處理小組（CERT/CC；Computer Emergency Response Team / Coordination Center）所公佈的資料，資訊系統弱點從 1995 年的 171 個，增加到 2005 年第三季的 4268 個（表 1）。而資訊安全事故發生件數從 1990 年的 252 件，增加到 2003 年的 137529 件（表 2）。

表1 資訊系統弱點統計(1995-2005)

年份	弱點數
1995	171
1996	435
1997	311
1998	262
1999	417
2000	1090
2001	2437
2002	4129
2003	3784
2004	3780
2005(1Q-3Q)	4268
	23868

[資料來源：CERT/CC] **[40]**

表2 資訊安全事故發生統計(1990-2003)

年份	資訊安全事件數
1990	252
1991	406
1992	773
1993	1334
1994	2340
1995	2412
1996	2573
1997	2134
1998	3734
1999	9859

2000	21756
2001	52658
2002	82094
2003	137529
	819854

[資料來源：CERT/CC] **[40]**

在這個資訊系統弱點與網路威脅不斷增加的年代，組織會不會受到網路威脅已經不再是個令企業會擔憂的問題了，企業要擔憂的是網路威脅何時會出現。爲了防止網路威脅造成企業重大的損失，企業愈來愈重視資訊安全的維護，因此也著手架設防護機制。擁有一套完善的計劃將會更鞏固企業的安全機制並且使得企業能夠掌控資訊安全的潛在問題。前幾年有一些保險公司開始嘗試設計精算的表格來估計企業組織受到駭客攻擊或是電腦中斷作業所造成的損失。但是在學術研究上卻少有評估資訊安全所帶來財務上的威脅與財政上的漏洞的研發[15][20]就要有這些研發往往缺乏一些歷史性的資料，所以這些估計通常是不可靠的[36]。

如果以功能而言，目前各廠家的防毒軟體（Anti-Virus Software）或是威脅管理系統（Threat Management System）所能提供企業組織使用的基本功能其實是大同小異，其效能也在伯仲之間；但是不同的企業組織使用後的成效卻大不相同。因此顯示影響企業網路安全的因子並非全是資訊安全產品本身的功能，應該還有其他因子互動所導致。所以，如何掌握左右企業組織資訊安全風險的主要影響因子，並根據該影響因子提供企業組織一套較實用的資訊安全策略以解決其所面臨的風險與使其金錢上的損失降到最低，將是改善企業組織資訊安全風險的關鍵成功因素。

在爲企業組織做資訊安全規劃前，必須先瞭解影響企業組織資訊安全的主要影響因子以做風險評估，才能使得資訊安全規劃更有說服力[39]。因此本研究希望透過對造成資訊安全威脅的可能因素做深入的瞭解，探討這些因素如何左右資訊安全威脅的發生，並且分析與評估哪些特質的企業組織是可能面臨高風險資訊安全威脅的潛在企業組織，以整理出可供企業遵循的資訊安全策略方向。

第二節 研究目的

隨著資訊系統弱點與網路安全威脅突飛猛進地成長，資訊安全這個領域已經愈來愈被企業所重視，不過大部分的企業往往都會有同樣的迷思『爲什麼我們裝了防毒軟體，還是會中毒呢？』事實上，就資訊安全的掌控部分，應該要從四個構面共同來分析與討論，分別是組織(Organization)、技術(Technology)、人員(People)與程序(Process)。組織主要是包括組織產業別、組織特質與組織規模等；技術主要探討資訊安全架構和資訊系統整合；人員主要探討資訊安全人員、終端使用者與組織高層主管的特質與表現；程序主要探討事件的分類、威脅損失評估與收集相關資訊歸檔。因此，本研究的目的在於，以系統的研究方法，探討及評估導致企業組織在資訊安全受到威脅的主要因素，並提供企業資訊安全策略的具體建議。

第三節 研究方法

研究設計通常分爲三種，探索性研究（Exploratory Research）、敘述性研究（Descriptive Research）與實證性研究（Hypothesis Research）。探索性研究的目的在對新主題或現象進行初步摸索，以建立初步的概念，利於後續研究的進行。敘述性研究用以描述研究對象的特性，頻次分配、平均數的計算結果呈現或者研究對象的變數間的關係。實證性研究著重於實驗或是問卷調查，利用統計方法證明某理論。

以往文獻中用在了解資訊安全弱點（Vulnerability）或威脅（Threat）的方法多用內容分析法（Content Analysis），內容分析法是去分析一個目前存在於資訊系統中的威脅（如 Viruses），控制（如 Anti-Virus Software）及資訊安全的標準，以試圖找出這個威脅的組成份子。調查法通常是用來了解目前企業對資訊系統安全的投資及重視程度等整體環境資訊（如 2004 CSI/FBI Computer Crime and Security Survey[29]），例如因爲網路使用的普及，企業在資訊安全上的投入資金都較前先年增加之類。

統計方法或資料探勘技術也許是可以用來加強分析企業資訊安全關鍵因素的方法。由於本研究的主要目的在於探討可能影響企業資訊安全威脅的主要影響

因素與這些影響因素之間的相互影響關係。因此本研究將採取敘述性研究並輔佐以部分實證性研究（問卷調查）。本研究爲了不要遺漏可能的影響因素，因此與國外某知名防毒軟體公司技術人員進行訪談瞭解所有可能影響資訊安全的重要因素，並且將其都列示在調查問卷內，利用統計分法的變異數分析及卡方檢定找出關鍵影響因素，再試圖以集群分析找出安全高與低不同的樣本類型。

第四節 論文架構

本論文的研究架構，首先在於確定研究的方向與範圍，由於本研究以企業資訊安全與主要方向，因此在本章說明研究背景與動機並確定研究範圍。且由於本研究的目的在於找出資訊安全事件發生的可能影響因素，因此收集國內外與資訊安全影響素相關的文獻進行探討研究，根據文獻探討研究的結果，建立本研究的架構以及問卷內容的設計，再根據問卷調查以及訪談的結果，作資料的整理與分析，並整理分析結果，最後對研究作相關的結論與建議。

本論文共分爲五章，各章摘要如下：

第一章　緒論

說明本研究的背景、動機、目的、研究方法與架構等。

第二章　文獻探討

定義「資訊安全」並說明資訊安全事件發生的可能影響因素。

第三章　研究設計

資料問卷的設計、資料收集與分析的方法與工具。

第四章　研究分析

分析各企業組織、技術、人員與程序對於資訊安全事件多寡的影響程度。

第五章　結論與建議

總結企業在於資訊安全運作上有待加強與改善的部分，並作後續建議。

本論文的研究流程，如下所示：

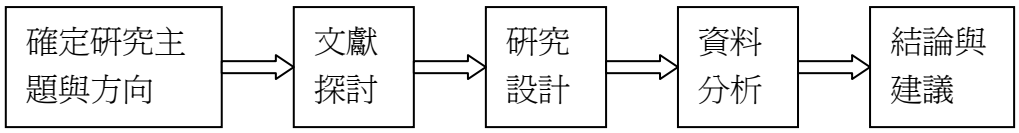

圖1　本論文的研究流程