第貳章　文獻探討

文獻探討共分爲資訊安全定義與範圍、資訊安全現況、影響資訊安全因素、有效掌控資訊事故之基礎以及資訊安全產品的種類，敘述如下：

第一節 資訊安全定義及範圍

「資訊安全」在一般人的觀念中，一直以來都會輕易地將它和使用加密、解密技術的密碼學、防火牆與網路駭客攻擊畫上等號，都是屬於技術層面上的觀念。這個觀念以過去對於資訊安全的解讀而言，並沒有錯。不過隨著資訊科技愈來愈發達與電腦網路的來臨，若單是以加密、解密技術的密碼學或是防火牆等技術層面來談資訊安全的議題就會略顯不足了。也是因爲如此，這個刻板印象可能是導致現今各企業組織內部不斷產生資訊安全問題的主要原因之一。資訊安全隨著時代的演進與網路化時代的來臨，資訊安全的重點不再只是單一著重在於技術層面，而是著重在由上而下的整體架構，重視的是「管理」，而非「技術」。資訊安全的定義也已漸漸由技術的角度轉向爲由管理主導的角度。在大部分的資訊系統的資訊安全並無法單靠過去的經驗就可以處理的，技術性的解決方法始終是有限的，而需要仰賴管理來協助[7]。可以從表 3 得知，國內外對資訊安全的定義，從 1984 年的「對資訊資產的有意或意外情下，未經授權的公開、修改、破壞或使之失效等等的行爲的保護」到 2002 年的「資訊安全，是一種管理而非技術」。

表3　國內外對資訊安全的定義

年代	定義
1984 年	對資訊資產的有意或意外情形下，未經授權的公開、修改、破壞或使之失效等等行爲的保護。
1992 年	就是把管理程序和安全防護技術應用於電腦的硬體、軟體和數據（或資料上），以確保儲存中或傳遞中的數據（或資料）免於他人有意或無意的讀取、刪除或修改。

表 3 國內外對資訊安全的定義 (續)

年代	定義
1995 年	電腦安全的保護範圍包括：機房、電腦主機、終端機、電腦網路線、軟體與資料等有形及無形的電腦相關事務，良好的安全措施維護了這些資料的機密性、完整性與可用性。
1997 年	資訊安全的全貌就是對於有關個人或組織在使用所有關於說的、印行的及自動化紀錄等事情的保護；及保護資訊的產生、處理過程、傳遞、儲存使用、展示及控制等來源。
2000 年	爲降低資訊的風險所進行的各種測量方式。
2002 年	資訊安全，是一種管理而非技術。

[資料來源：李順仁，資訊安全] **[1]**

由表 3 瞭解看來，資訊安全的種類主要分成三類：

- 硬體安全：包含硬體環境控制及人爲管理控制等。
- 軟體安全：包含資料安全、程式安全及通訊安全等。
- 個人安全防護：包含人身安全、個人隱私權安全以及通訊（網路）安全等。

資訊安全的四大防護重點包括：防毒、防駭、防災、防竊**[5]**。其發生情況敘述如下：

- 防毒：電腦病毒（Virus）是一種會將本身複製到其他電腦的惡性程式，以惡意地方式散播出去，任意地或是不定期性的破壞與攻擊使用者的電腦資料**[32]**。電腦中毒是讓每個使用電腦的使用者都非常頭痛的一件事，也是讓所有電腦使用者幾乎都無法避免掉的夢魘。早期是使用資料備份的消極方法來自保，現在雖然有防毒軟體來協助電腦使用者積極地防禦。不過在病毒不斷的產生與病毒碼持續的更新情境下，彷彿是病毒與防毒軟體及病毒碼在進行一場無止盡的追逐賽，而資訊系統便成爲他

們的競技場。

- 防駭：隨著資訊科技的發展，網路的普及與使用，使得駭客也因此產生了。早期的駭客只是「登門拜訪」留留記錄告知使用者電腦有漏洞等等，屬於良性的電腦高手。而演變至今，駭客（或稱黑客，Hacker）已經成爲入侵使用者電腦進行惡意性的系統破壞，甚至是資料竊取的系統殺手。於是系統安全規劃，如密碼、身份認證到防火牆的建置已是現今被普遍使用的技術了。
- 防災：自然性的天災是企業組織無可避免的，不過一次意外即可以使得企業組織有著莫大的財務或是資源損失。自從台灣 921 地震以及美國 911 事件後，使用者更嚴肅地面對要建立更完整的防災計劃。從針對環境（如空氣、溫度、溼度、電力等）與系統容錯（如磁碟陣列、容錯元件，主機叢集等高可用性規劃）到資料、系統的異地備援，都已經廣泛被企業組織所使用。
- 防竊：資訊系統的普及，已經到了幾乎是每個使用者皆配有一台個人電腦的地步了。但是也因爲資訊系統的普及使得資訊的氾濫與不當使用，又成爲企業組織所頭痛的事。所謂「外賊易防，家賊難防」，資料的內部安全，自然成爲資訊安全的新課題。

第二節 資訊安全現況

機密性（Confidentiality）、完整性（Integrity）與可用性（Availability）爲資訊安全的基礎[21]。機密性指資訊安全必須要確定唯有通過安全認證的使用者才可以存取資料；完整性即爲在資訊保護及傳送過程中，不會被非認證的使用者修改過，必須從頭到尾確保資訊的正確性與完整性；可用性是通過安全認證的使用者隨時都可以取得所需要的資訊。機密性、完整性與可用性如果單獨以產品技術層面來談的話，這三者都不難達成，不過困難之處在於如何管理，以同時可以滿足這三種基本要素。

表4 93 年資訊安全防護裝置建置概況

建置類別	家數	百分比
無建置	2961	8.81
防毒軟體	29972	89.14

表 4 93 年資訊安全防護裝置建置概況(續)

建置類別	家數	百分比
防火牆	21033	62.56
入侵偵測系統	6290	18.71
漏洞偵測系統	4345	12.92
其他	340	1.01

[資料來源：行政院主計處電子處理資料中心] **[3]**

表5 93 年度遭遇到資訊安全事件概況

事故別	家數	百分比
電腦病毒攻擊	16253	48.34
駭客攻擊	2421	7.20
被植入後門程式	1654	4.92
資料遭竊或被破壞	186	0.55
網頁被置換	386	1.15
其他	126	0.37

[資料來源：行政院主計處電子處理資料中心] **[3]**

網路安全的議題以及其威脅對於大型企業組織或是中小企業而言，都是同等危險的**[9]**。而企業組織也會謹慎留意競爭對手是否有利用這些網路威脅來增加自身的比較利益**[38]**。資訊安全涵蓋的範圍很廣，並非只侷限於網際網路，也絕非只需要靠著防毒軟體（Anti-Virus）、防火牆(FireWall)、威脅管理系統(Threat Management System)、入侵偵測系統(IDS；Intrusion Detection System)與入侵防護系統（IPS；Intrusion Protection System）等資訊安全產品，就可以確保資訊系統萬無一失，絕對安全了。從表 4 與表 5（表 4 與表 5 同母體，爲複選題的問項）可以得知，到 2004 年底止，由行政院主計處電子處理資料中心所做的統計顯示，有 89.14%的企業組織有安裝防毒軟體，有 62.56%的企業組織有建置防火牆，不過受到電腦病毒攻擊的比例還是達到 48.34%。另外，根據 2003 年 CSI/FBI 電腦犯罪與安全調查（CSI/FBI Computer Crime and Security Survey），近四年來，網路連線是主要的攻擊來源，有 78%是透過網路連線來進行攻擊**[33]**。雖然資訊安全這個領域已經愈來愈被企業所重視，不過大部分的企業組織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？』。

表6 近年重大病毒事故災害統計

年份	病毒名稱	特徵	損失金額	感染電腦台數
2001	紅色警戒（Code Red）	透過 port 80 傳播並且自行複製攻擊 Microsoft IIS Server 漏洞，發動 DDoS 攻擊。可遠端控制中毒電腦。	超過 26 億美金	超過 100 萬台
2001	娜靼病毒（Nimda）	透過電子郵件、資源分享、Microsoft IIS Server 及網頁瀏覽等方式來傳播	6 億美金	800 萬台
2002	求職信病毒（Klez）	透過電子郵件傳輸，會反安裝防毒軟體。	超過 90 億美金	600 萬台
2003	疾風病毒（Blaster）	攻擊 Microsoft 作業系統 RPC Buffer Overrun 的漏洞發動攻擊，透過 TCP135 感染其他電腦並且對 Microsoft Windows Update Server 進行 DDoS 攻擊	超過 30 億美金	超過 140 萬台
2004	殺手病毒（SASSER）	利用 Microsoft 作業系統弱點 LSASS 透過 TCP445 對全球網路發動攻擊。	超過 30 億美金	超過 1800 萬台

[資料來源：某公司] **[4]**

由表 4 看來，有 89%的企業組織會安裝防毒軟體、63%的企業組織會架構防火牆，不過從表 6 看來，這些防毒軟體與防火牆並沒有因此幫助企業組織免於病毒的威脅，例如 2003 年的 8 月，Slammer 蠕蟲感染了網路上近 90%有此弱點的電腦主機**[12]**。全球每年都會陷入病毒的威脅，有如掉入某種無窮迴圈之中，悲劇每一年都會重新上演，日復一復、年復一年的。

第三節 影響資訊安全因素

資訊安全的問題混合了企業組織仰賴著由上百台甚至上千台電腦主機以及各種網路設備所連結合成的網路之複雜度，而每個網路上的節點都有可能是發生漏洞的問題點**[30]**。美國知名的資訊大師 Bruce Shneier 說過：「資訊安全是一種過

程（程序），而絕非是一種產品！」（Security is a Process, not a Product!）[10]， 這些資訊安全系統產品並非「萬靈丹」，不是服了就可以“百毒不侵、強身健體”。資訊安全系統產品絕非可以提供企業組織 100%的安全保護，而是處於一種輔助性的角色從旁來協助企業組織的資訊安全人員來控管資訊系統。這些技術的背後，還是需要有人員的參與以及管理，才能夠發揮這些資訊安全系統產品的特色與功能。根據計算機技術協會（CompTI；Computer Technique Institute）所做的安全事故調查中，63%的事故是因爲人爲錯誤所導致的；只有 8%的事故是因爲技術原因所引起的。以行政院主計處電子處理資料中心 90 年度的調查統計報告顯示，當年度所發生的資訊安全事故中，技術性較高的駭客入侵的比例佔不到 4%，其餘都是例行性日常維護工作不良所導致的。例如天然災害的預防、人爲疏忽的避免與電力中斷的備源問題，幾乎都不具備技術層面的資訊安全領域專業知識就有能力可以輕易避免掉了。由於造成資訊安全事故的原因大部分都不是專業技術的層面，而是在人性管理層面上出現的明顯漏洞所導致的（表 7）。因此資訊安全系統產品固然重要，不過是以協助資訊安全管理政策爲目的，而非處於主導的角色，可以用來取代資訊安全管理政策。因此要進行資訊安全的計劃便要瞭解整個大環境以及會影響資訊安全的因素[16]。

表7　九十年資訊安全事故統計表

事故別	家數	百分比
天然災害	28976	13.70
人爲疏忽	87115	41.20
電力中斷	62533	29.57
駭客入侵	7379	3.49
病毒危害	115425	54.59
內部人爲因素	2029	0.96
其他	13729	6.49

[資料來源：行政院主計處電子處理資料中心] **[2]**

資訊安全威脅一般可以分成爲人爲威脅以及自然環境的威脅兩大類。人員的威脅又可以分成爲內部人員以及外部人員所造成的威脅。內部人員的威脅最常見的就是內部人員本身是沒有養成良好的電腦使用習慣的終端使用者，有一些易遭受安全攻擊的行爲，如不當開啓電子郵件的附件、任意點擊網頁以及下載來路不明的檔案等，或者是意圖不良的員工盜賣組織機密等等。外部人員所造成的威脅

往往爲熟知各種病毒的特性、系統漏洞型的網路黑客，企圖透過病毒與系統漏來攻擊企業組織資訊系統或竊取組織內部機密資料等等。自然環境的威脅，包括了天災與人禍，以台灣爲例，常見的有颱風、火災、停電與地震等等。

黑客（Cracker）、騙子與天災是資訊安全的三大威脅，由於網際網路四通八達的特性，資訊系統的弱點容易暴露在全球所有黑客的眼裡，以便黑客進行入侵破壞的不當行爲。另外，騙子利用人爲疏忽破壞資訊安全，以所謂的「社會工程」（Social Engineering）騙取帳號密碼或是重要的機密文件等等。至於天災部分，1999 年的 921 大地震造成全台大規模的停電，與 2001 年納莉颱風淹水的災情，造成未建制異地備援的企業組織，無法持續正常運作。

第四節 有效掌控資訊事故之基礎

資訊系統的風險非常受到企業組織的重視，因爲資訊安全將直接或間接地影響企業組織的營運與資金表現[35]。因此，資訊安全策略便必需在這些安全威脅的舉動與將金錢的損失降到最低的需要間找到一個平衡點（tradeoff）[17]。一個受到威脅攻擊的電腦將會導致企業組織經營上的生產力的損失、停工期的延長、非認證的資料讀取、非認證的登入以及軟硬體的損害等等[30]。企業組織必需確保不會受到壓倒性數量的網路威脅的攻擊。不幸的是，保護企業免於這些網路威脅已經愈來愈難以做到了[37]。安全漏洞發佈到病毒爆發的時間愈來愈短、愈來愈複雜的網路架構以及缺乏部分資訊安全的資源和管理知識，都是造成企業組織資訊安全遭受到安全攻擊案例增加的原因。企業組織若是忽視資訊安全議題的話，將會導致企業組織損失掉時間、金錢與生產力，也可能因此而面臨重大的挫敗[18]。

就資訊安全事故掌控的部分，主要可以從三個構面來分析與討論，分別是技術(Technology)、人員(People)以及程序(Process)[43]。技術主要探討資訊安全的架構和資訊系統的整合；人員主要探討資訊安全人員、終端使用者與企業組織高層主管的特質與表現；程序主要探討事件的分類、威脅損失的評估與收集相關資訊歸檔。

技術在資訊安全防護中爲第一項要件。在資訊安全架構中，應該提供主從式（Client-Sever）架構的防毒安全，而在企業組織所使用的各項資訊安全系統產品的功能所得到的防護功能基本上都是大同小異的。就這方面而言，比較沒有什麼太大的問題。偶而可能會有產品問題的情況發生，這部分比較小，也比較容易解決。除非是因爲產品的功能故障導致無法偵測到病毒或是網路威脅，這部分的問題才會顯得比較嚴重。但這種情況發生的機率並不高。資訊安全在技術上有困難的原因是許多企業的各項應用程式（Application Program）通常是透過招標的方式，外包給外面的廠商，因此長期下來，許多的應用程式都可能分別由不同家廠商所開發的，而導致會有“歷史的包袱”的情況發生。也就是說，因爲每個應用程式間的資料結構大不相同，使得在整合資訊安全技術及策略方面上，產生問題，不容易制訂一個統一的規格。因此在推動資訊安全防護政策時，無法快速的推動。

人員在整個資訊安全防護中是最重要的要件。人員包括資訊安全人員以及終端使用者兩類，在資訊安全人員的方面，雖然技術與程序可以提供許多有用的資訊給資訊安全人員，不過資訊安全人員必需透過這些大量的資訊，找出一個適當的應變之道。因此除了靠培訓使得資訊安全人員擁有資訊安全這個領域的專業知識之外，經驗的累積對於資訊安全人員也是非常重要的。再多的訓練、再多的理論知識也無法取代長期累積下來的實戰經驗。一個經驗豐富的資訊安全人員，在遇到事件發生時，應該具備有能夠輕易地識別可疑的威脅的能力，並且能夠在短時間內快速地做出應變措施，盡量將企業組織所受到的損失降到最低。許多資訊安全事件常常因爲組織內部人員的警覺性不夠，或者是說人員對資訊安全方面的認知並不夠所導致的。

終端使用者是直接使用到終端電腦的使用者，因此終端使用者的使用習慣也是企業組織會不會因此受到網路威脅的主要原因之一。在很多的情況之下，終端使用者的行爲是無法強制限制的。有些部分當然可以直接透過資訊安全防護系統去控制與監管，不過有些部分是終端使用者的行爲的問題，無法輕易地或有效地控制與監管。這些部分就必需透過資訊安全教育訓練來改善終端使用者的使用電腦的行爲與習慣，如告訴終端使用者需要對於電子郵件的附件與網址以抱著懷疑謹慎的態度小心開啓、使用組織所配送的電腦不要使用網路電子郵件（Web Mail）

以及鼓勵終端使用者在家裡的環境中應該安裝防毒軟體、個人防火牆（Personal Firewall）並且定期更新病毒碼與修補檔等等[14]，且在正常工作中切實遵守企業組織的安全政策。控制與監管嚴謹固然對企業組織的資訊安全有很大的幫忙，不過資訊安全人員也必需考量終端使用者的需求，若是這個程式能夠提升終端使用者的生作生產力，資訊安全人員可以適度地放行，並且監控其使用狀況。資訊安全人員必需在嚴謹控管與滿足終端使用者需求間，找到一個平衡點，才能爲企業組織帶來雙贏的局面。

組織高層對資訊安全重視的程度對於整個資訊安全影響很大。在部分組織中，資訊安全人員的地位並不高，所做的資訊安全政策不被終端使用者所接受與配合。資訊安全人員藉著多年累積的 Domain Know-how 與經驗以制訂適合整個組織架構的資訊安全政策，不過若是無法透過高層對此的支持並且推動，終端使用者往往會因爲覺得綁手綁腳的而不願意配合，使得該組織的資訊安全政策只是白紙一堆，無法發揮實質的功用。部分組織因高層高度支持，並且由高層發公文與電子郵件要求終端使用者配合資訊安全策略的推動，使得網路威脅有明顯的減少。因此主要還是得看組織高層是否有意識到資訊安全的重要性與資訊安全策略執行的必要性，才能使得資訊安全政策推動地更快速、更有效率。

威脅事件等級的分類是資訊安全防護的第一步程序。事件分類將會確認事件發生的嚴重性，並且根據其輕重緩急，來訂定其處理的優先權。這方面可以透過平時不定期舉辦病毒爆發以及網路威脅演習的方式來培養員工們對於威脅事件發生的反應，也可製訂處理威脅事件的流程圖，加快危機處理的時間，以求降低威脅事件發生時所造成的損失。威脅損失評估與收集相關資訊歸檔是在事件發生之後的後續處理程序。事件發生往往有許多的途徑，不易防治也不易反查。因此威脅損失評估可以確保最具有威脅性的事件將來若不幸再發生，可以根據其等級在第一時間做出回應措施。透過監控系統可以收集到可能威脅的相關資料，再透過資料探勘（Data Mining）的方式，分析以及歸納找出網路威脅的種類、攻擊來源與入侵途徑等相關資訊，以供定期掃描，降低未來再發生類似網路威脅的可能性。

一個有效的事故掌控機制對一個需要長時間在線的企業組織是很重要的一

件事。在弱點與攻擊不斷增加的年代，會不會有網路威脅已經不再是個令企業組織所困擾的問題了，而真正困擾的應該是威脅何時會出現。隨著這些安全威脅特性的不斷改變，企業組織必需持續地對內部的資訊系統所受到威脅進行評估[19][25]。因此，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問題。

第五節 現有的資訊安全產品種類

目前現有的資訊安全技術能夠針對特定的設備以及特定的網路位置，給予特定的安全防護，以滿足特定的需求，而衍生出不同種類的資訊安全產品。主要可以分成桌上型與客戶端（Desktop & Client）、病毒爆發管理（Outbreak Management）、網路防護（Network Protection）、電子郵件與群組軟體（Email & Groupware）、網際網路閘道器（Internet Gateway）、檔案伺服器與儲存裝置（File Server & Storage）、行動安全（Mobile Security）等種類。

桌上型與客戶端防毒軟體（Desktop & Client）是一般最常見使用的「防護措施」。可以協助保護使用者的電腦，使其免於受到病毒、電腦蟲、木馬程式與其他不懷好意入侵者的攻擊。有效的病毒爆發管理（Outbreak Management）對於企業組織而言，是一大挑戰。

而病毒爆發管理（Outbreak Management）系統的目的可以協助企業組織提早發現病毒爆發的預兆、快速的開始進入控管監控以及隔離弱點與受感染的電腦，以降低病毒爆發的可能性與減弱病毒爆發的規模大小。一般採用集中式管理的方式來控管整個環境的病毒爆發情況以及提供各種網路威脅的提醒、查詢以及統計等等[41]。

一般常見的安全方案無法有效阻擋來自複雜網路環境下的網路蠕蟲、防制因爲企業安全政策的網路存取所引進的攻擊與因網路蠕蟲所引發的疫情所耗費的大量善後成本。網路防護（Network Protection）採用主動式網路蠕蟲疫情防制裝置來保護企業組織的區域網路、分支機構、不同的網路區段以及重要的應用系統。

群組軟體是一種電腦應用工具，結合電子郵件、文件分享、電子表單、群組排程等多功能軟體，可以讓一群使用者利用不同的電腦系統來一同工作，以交換與分享彼此資訊的系統[27][42]。由於群組軟體的主要目的是提供一群使用者可以同時利用電腦工作，所以在於資訊安全的層面也是非常要求的。電子郵件與群組軟體防毒（Email & Groupware）可以提供企業組織有效地偵測、監控、過濾以及管理病毒與網路威脅，減少不適當的內容與檔案透過群組軟體流入網路中以破壞使用者的電腦。

網際網路閘道器（Internet Gateway）是外部連線是各企業組織連線的第一道防線，因此各企業組織對於網際網路閘道器的資訊安全也非常重視。網際網路閘道器的資訊安全產品，可以協助企業組織在病毒、間諜軟體（Spyware）、垃圾郵件、網路釣魚與傀儡程式攻擊內部網路前予以封鎖以及封鎖惡意間諜軟體網站的存取，並且偵測內部終端使用者電腦上的間諜軟體活動情形以進行刪除，來提供企業組織有彈性的資訊安全防護。

企業組織常常會架設檔案伺服器（File Server）來保存進行 CRM（客戶關係管理，Customer Relation Management）與 ERP（企業資源規劃，Enterprise Resource Planning）的相關資料。因此需要能夠即時地保護網路共享資料，避免病毒以及其他惡性程式等網路威脅的侵入與破壞，以確保企業組織資料的高度安全。隨著即時通訊軟體在工作環境中使用率的增加，也增加企業組織必需去考量即時通訊軟體所衍生的資訊安全方面的問題[31]。這類的主機在病毒與網路威脅的管理也是不可馬虎的。檔案伺服器與儲存裝置防毒（File Server & Storage）的產品是專為這類裝置所特別設計的。能夠有效管理內部網路防毒，保護檔案伺服器與網域內的資訊安全，免受電腦病毒的攻擊。並且能夠集中控管病毒偵測以及掃瞄的情況，以隨時掌控伺服器防毒的狀況。在病毒與惡性程式有機會在分享文件中擴散以及感染其他電腦前，都能夠存檔案伺服器端，進行有效的過濾以減低病毒爆發的機率。

由於無線行動裝置（Wireless Mobile Device）數量成長快速，因此越來越多的病毒利用這個平台當作新的散播溫床。行動安全（Mobile Security）考量是現成企業在廣泛採用無線技術以及遠端運算（Remote Computing）時，所面臨的最大

障礙。根據統計，目前有 55%的西歐企業已經部署行動安全軟體以確保行動資料的安全性，亞太區則爲 44%，而北美地區則有 36%[6]。行動裝置將是下一個駭客與病毒攻擊的重要目標，而行動安全系統能夠有效地提供使用者一個安全的保護，如攔截垃圾簡訊、病毒掃瞄以及集中式的管理，免受駭客與病毒的攻擊，以降低受到網路威脅的可能性。