行政院及所屬各機關出國報告
（出國類別：研究）

研究網路銀行交易安全規範與管理

服務機關：臺灣銀行
出國人　職　　稱：辦事員　辦事員
　　姓　　名：吳玉慶　陳建平

出國地區：美國
出國期間：89.11.28～90.01.26
報告日期：90年6月

目　　錄

壹、前言 1

貳、網路安全事故 3
安全事故來源 4
安全事故類型 4
安全事故與網際之成長 6
安全事故之趨勢 7

參、資訊安全政策 8
資訊安全政策之制定 9
資訊安全政策之評估 10
資訊安全政策及規定之宣達 10
資訊安全組織及權責 11

肆、密碼學 13

伍、軟硬體建置安全規範 18
網路 18
電子商務 19
目標與範圍 20
網路安全政策制定 20
BS7799：十大項目 21
網路設備安全說明 22
網路通訊設備之基本安全規範 22
網路路由器安全控管規範 23
區域網路交換器安全控管規範 26
網路資源管理者之認證及授權機制 26
安全管理機制 26
企業網路安全架構建置範例 29
第一期目標規劃 30
第二期目標規劃 32
第三期目標規劃 33
第四期目標規劃 35
企業資訊系統安全 36

陸、網路銀行交易安全規範 38
網路交易安全課題 38
SSL 38
SET 39

柒、網路安全管理 42
控制風險 42
動態策略調整設定 43
存取權限隱私權控制 43
可信賴的系統回復與完整詳盡的記錄 43
組織圖 44
職位說明 44
計劃 45
控制 46

捌、建議 48

玖、結論 52

參考文獻 54

壹、前言

隨著網際網路的風起雲湧，由於其跨平台的特性，使得全世界的電腦可以輕易地連接起來。除了資源的分享，也創造了無限的商機、掀起強勁的競爭與帶來嚴峻的挑戰。對連上網際網路的機構，無論是政府機構、營利企業、非營利組織、甚或個人，共同面對的重要課題均是網路的安全性。對金融機構而言，網路安全已成為其經營中具舉足輕重的重要地位。首先，銀行是以信用收受存款，再將其貸放、投資等，發生任何網路安全的事故，銀行的信用均會招致不同程度的損傷。其次，由於電子商務的興起，透過網際網路進行線上交易已是不可逆轉的趨勢，不安全的網站將失去客戶，必在未來的競爭中喪失優勢。再者，網路交易的安全不只是IT部門人員的職責，所有組織內的員工均需有高度的安全意識，只要一位員工有所疏失，就可能造成網安事故，因此網路的安全性亦成為評估銀行經營管理良窳重要參考指標，在美國其甚至會影響金融機構的評等。

企業之資訊安全不僅是靠技術就可達成，完整的資訊安全尚包含企業安全政策(程序)、組織、人員訓練、管理和應變計劃等。技術包含三大部份，密碼學、資訊科技和通訊科技。前者在建構一套有效的加解密機制，讓有心人(如hacker)無法或必須以很高的代價才得以解開密文，從而保護資料之安全。資訊科技在發展更好的軟硬體技術，除被動的保護組織不被入侵，更要主動的偵測潛在的危險，化解可能的危機。通訊科技在以更快速又安全的方式傳遞訊息，確保通訊的品質及資料的安全。就技術而言，此三者必須並肩作戰，合作無間，才不致讓人有可乘之機，維護機構和個人的隱私、財產及信譽。

從交易的層面分析，最重要的是如何辨認交易當事人的身份(辨識性(identification & authentication))、如何確保交易資料不遭篡改(完整性(integrity))、如何保護交易內容不被無關者知曉(隱密性(confidential))、如何確知交易訊息是何人發出(不可否認性(non-reputation))。除辨識性需藉助其他科技如語音、生物外，其他三項均需仰賴密碼學。舊有的私密金鑰系統(如 DES)，只有一把私密金鑰，加解密速度快，但需經常更換金鑰，適用於交易對象較少(如金融機構與財金公司)、並能處理大量的資料。先進的公開金鑰系統(如 RSA)，具有公開金鑰及私密金鑰，不易被破解、不需經常更換金鑰，但因運算複雜，加解密速度慢，適用於交易對象較多(如金融機構與一般客戶)、小量資料的處

理。而雜湊函數(hash function)，則可將不同長度的內容轉換成固定長度(稱之為 digest)，和公開金鑰系統結合構成數位簽章，達成交易不可否認的目的。

電子銀行業務已成為各銀行必爭之地，規劃一個安全、便利又能滿足客戶需要的網路銀行實有必要。本文將先談論有關網際網路上的一些威脅，以作為企業在訂定其安全政策之參考。接著說明企業整體安全的基石-企業安全政策。其次，我們將就和網路銀行安全有關的技術性課題作一論述，包括 DES、RSA、Hash Function、SSL、SET 等。然後是各種軟、硬體可能有的弱點作一探討，以增強系統的防衛能力。我們也將介紹美國存款保險公司對電子銀行安全檢查的一些規範，試著提出安全的網路銀行架構，以及管理之道。最後我們將參考紐約區美國聯邦銀行對資訊安全的實務指引，提出對本行網路銀行安全的一些建議。網路化已是現在企業經營的最重要的工作，希望本文也能喚起大家對網路資訊安全的重視，避免發生資訊危機的可能，奠定永續發展的基礎。

貳、網路安全事故

根據美國國家電腦安全局(National Computer Security Agency)所宣佈的一項數據顯示，由美國國防資訊系統局(Defense Information System Agency)對該國國防部 9,000 台電腦所作的測試攻擊中，成功的比率為 88%，且有高達 95%以上的電腦不知道遭受攻擊。而在 5%知道遭受攻擊的目標中，僅有 5%的比率採取行動，也就是只有 22 台。另根據美國 CERT/CC(Coordination Center)對安全事故(incidents)及系統弱點(vulnerabilities)所作的一項統計報告顯示，自 1988 年至 2000 年間發生安全事故數由 6 件增至 21,756 件，總計 47,711 件；自 1995 年至 2000 間已知的弱點數由 71 件增至 774 件 (請參見下表)。

安全事故及弱點數統計表

Year	Incidents	Vulnerabilities
1988	6	-
1989	132	-
1990	252	-
1991	406	-
1992	773	-
1993	1334	-
1994	2,340	-
1995	2,412	171
1996	2,573	345
1997	2,134	311
1998	3,734	262
1999	9,859	417
2000	21,756	774
合計	47,711	2,280

資料來源 CERT/CC，製表：陳建平

1. A *network security incident* is any network-related activity with negative security implications. This usually means that the activity violates an explicit or implicit security policy.(CERT/CC 對安全事故之說明)
2. A *vulnerability* is a weakness that a person can exploit to accomplish something that is not authorized or intended as legitimate use of a network or system.

由上表觀之，隨著網際網路快速發展，網路安全事故發生的次數也成倍數成長。網路攻擊可能來自網際網路的任何角落，不論其來自特定系統或網路、或欲求對特別的帳號具有存取權。典型的攻擊型態包含獲取使用者之存取權限、取得專有的權限、並且使用無辜的系統作為攻擊平台，以攻擊其他網站。

安全事故來源

一般要對製造網路事故的人作分類是很困難的。入侵的人可能只是對在網路上能作些什麼事充滿好奇的青年人，亦可能是剛創作一新軟體的學子，也許是為尋求自身利益的個人、或是為某家公司或他國之經濟利益而蒐集資訊的間諜。當然也可能是不滿的離職員工或正在為公司工作而取得存取權限的顧問人員。這些人的目的可能是一時興起、挑戰智力、為權力感、也許是為引起政治的注意、或者是為金錢利益，不一而足。而電子社群、最新出版的入侵技術、和入侵技術有關的會議對發生安全事故均有推波助瀾的效果。如此，藉由知識分享及易於使用之軟體工具，成功的入侵者能增加入侵者的數目和他們的影響力。

安全事故類型

去年一月間，美國著名的網站如 Yahoo、Amazon 等在數秒內遭受入侵，以致伺服主機無法提供任何服務，網路安全的課題又再度引起世人的注意。這種名為 DDoS(Distributed Denial of Service-分散式阻絕服務)的攻擊，是同時從世界各地成千上萬不同伺服器和桌上型電腦對特定的網站發動攻勢，致使服務主機不堪負荷或資源耗盡而中止服務。各種入侵方式說明如后。

一、Probe 及 Scan

Probe 是用一種企圖獲得系統存取權或發現有關系統的資訊。例如：試圖簽入一個未使用過的帳戶。Probe 如同一種電子式的門把，以發現未上鎖而可輕易進入的門戶。雖然有時 Probe 會造成一個很嚴重的安全事故，不過通常是起因於好奇或誤入。不同於 Probe 是以人工的方式進行，Scan 則是以自動化的工具完成大量的 Probe 之企圖。入侵者常先發現系統可能的弱點，而 Probe 或 Scan 是遂行其攻擊的前奏曲。

二、Account 及 Root Compromise

Account Compromise 是以他人之名義未經授權使用第三人之電腦帳戶。Root Compromise 類似於 Account Compromise，但遭破壞帳戶所有人擁有較高之權限或專屬的權限。雖然未有管理者階級存取權表示危害較有限，然一般使用者權限的帳戶卻是取得更大系統權限的進入點，故對 Account Compromise 亦是輕忽不得。

三、Packet Sniffer

是以程式抓取傳輸於網路間封包之資訊，以取得具價值之資料。這些資料可能是以明碼方式傳送的使用者名稱、密碼和財物資訊。由於有成千上萬的資訊以 sniffer 的方式取得，入侵者即可對系統發動全面性的攻擊。安裝 packet sniffer 無須取得專有權限，然就多使用者系統而言，packet sniffer 的存在表示有 root compromise 之情事存在。

四、Denial of Service

Denial of service 的目的並非截取機器或資料的未授權存取權，而在使合法使用者無法享有服務。有多種 Denial of service 之型式，攻擊者或在很短的時間內對系統送出大量資料、任意的消耗稀少或有限的伺服器之資源、破壞實體的網路元件或傳送中含有加密資料的訊息。

五、Exploitation of Trust

網路中的電腦，通常存在有一種信任的關係，以方便資源的共享。利用電腦網路系統之信任關係，攻擊者可偽造(forge)身份，使他們看起來像是可以使用受信任的電腦。如此，他們就可取得未經授權的權限，以便

存取其他的電腦。

六、Malicious Code

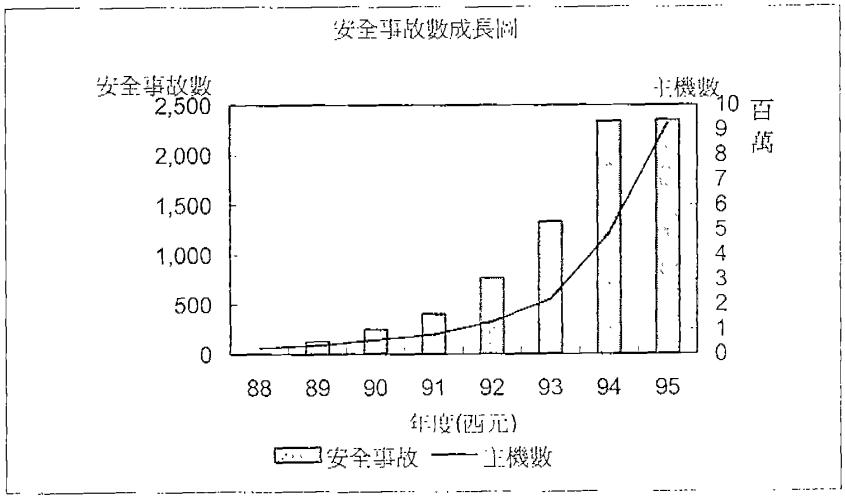
是一種具破壞性的程式碼，會造成系統意想不到的後果。通常要等到使用者發現危險時，才會意識到這種程式碼的存在。常見的三種 malicious code 為 Trojan horses、viruses、worms。前兩者隱藏在合法使用者之程式或檔案中，攻擊者藉由更改檔案或程式而作出更多不可預期的事。Worms 是會自我複製的程式，當他們被啟動後就不需人力的介入而擴散。這些程式均會造成嚴重的資料流失、系統當機、阻絕服務和其他型式的安全事故。

七、Internet Infrastructure Attacks

會攻擊網路的基礎設施的主要元件，而非網際網路上特定的系統。例如其攻擊目標常為網路名稱伺服器、網路存取提供者、許多使用者依賴的大型網站。此種攻擊影響相當廣泛，並且會阻礙許多網站每日正常的營運。

安全事故與網際之成長

根據一項 CERT/CC 所作的統計顯示，網路安全事故在 1988 年至 1995 年間有將近 25 倍的成長。到 1995 年，網路安全事故的報告數成長比率差不多和網際網路主機成長的幅度相同。如下圖所示。



資料來源：CERT/CC

安全事故之趨勢

由於網際網路的開放性，資訊唾手可得，攻擊者也有了更多學習的管道。根據 CERT/CC 八年的統計，發現入侵者的技術知識已越來越進步。他們不僅可以利用已知的漏洞，甚至可以測知原始程式碼(如 E-mail)及 World Wide Web 之弱點，更容易入侵 End-user 之電腦和伺服主機。由於這些居心不良之人技術愈來愈純熟，其攻擊的手法也越來越複雜。譬如他們能夠偵測出剛上線的用戶，趁安全設定尚未完成前的最脆弱時刻進行攻擊，讓人防不勝防。同時他們也開發出很多有效的、易於使用的、不需高深知識即可應用的軟體套件作為攻擊的工具，愈來愈具威脅性。另外，有許多運作在運算領域之工具，也被攻擊者利用而使攻擊更自動化，可以不費吹灰之力的獲取成千上萬台主機的資訊。所得之資訊可能是用來分享、或是交換之用、或預備攻擊之用、甚或即刻下達攻擊指令。以下列出幾種侵略者常用的工具，以作為我們防範的參考。

- network scanner
- password cracking tool and large dictionaries
- packet sniffer
- variety of Trojan horse programs and libraries
- tools for selectively modifying system log files
- tools to conceal current activity
- tools for automatically modifying system configuration files
- tools for reporting bogus checksums

參、資訊安全政策

基本上，電腦安全是為非技術性的問題尋求技術性的解決方案。因為其並非花了大筆的金錢、時間、人力、物力，就可以百分之百的防範資料意外地流失或他人蓄意的攻擊。有時也有可能因為軟體的瑕疵、意外事件、人為操作錯誤、運氣不佳、惡劣的天氣或是意圖不良等。甚至裝備精良的入侵者，都可能造成電腦系統的停擺。亦即系統的安全與否並沒有一個絕對的標準。所以，對於資訊安全我們所要作的是儘量提高系統的「受信任程度」，希望它能在我們需要服務的時候發揮其應有的功能

擬定有效的策略與安全規劃時，需要特別注意以下兩點：

一、系統安全與策略，需要組織內部由上而下的推行及認知。

雖然使用者在系統安全中扮演重要的角色，但沒有組織內部的風行草偃，系統安全還是很難有效建立。尤其重要的是，組織內部的高階主管，更需要切實遵守有關系統安全的一切規定。

二、有效的系統安全就是對資訊的確實保護。

系統安全的策略和指導方針，都應專注於保護資訊，不管它們以什麼樣的形式存在。資料的重要性是不因其為報表、傳真、不存於磁片中就降低。

換句話說，無論資訊傳送或儲存的方式為何，都需要受到不同程度的保護。因此，對建立一個能正常、有效運作的系統，並確實依照需求運轉是最重要的。唯有如此，才能建構一個安全的系統。一般而言，考慮資訊系統安全時，應注意的幾個方向：

一、機密性(Confidential)

所謂機密性是所有的資料，不論其敏感性高低，未經所有人的允許，任何人不得存取資料。

二、資料完整性(Data Integrity)

資料的完整性是指非經資料擁有人之同意，任何人不得對資料(包括程式)的內容進行變更或刪除。諸如公司營業的會計紀錄、日常營運活動的備份磁帶、檔案使用狀況，以及其他必要的參考文件。

三、可用性(Availability)

在以各種方式和手段，不讓系統的服務品質降低；或是即使發生未預期的

狀況，系統亦不會當機。

四、一致性(Consistency)

一致性在確保依照合法使用者所習慣、預期的方式運作。亦即系統管理者應要提高警覺，如果系統的軟體或硬體突然出現和以往不同的運作結果，尤其是在升級或修正錯誤之後。當然，所使用的資料和軟體亦應納入考量，確保其是安全的。

五、控制(Control)

簡單言之就是使系統的運作是在正常的狀態。當系統出現沒有經過授權的使用者或軟體，系統就有出現大問題的可能。其所隱含的意義是，系統可能遭受入侵，亦即可能失去了對系統的控制。此時我們可能要擔心他們是怎麼進來的？意圖為何？是否還有我所不知道的東西也一起進到系統內了？

六、稽核(Audit)

不只是未經授權的使用者會出錯，一般的使用者也可能會出錯，甚至做出不軌之事。因此系統必須要能知道誰在什麼時候做了那些事？造成什麼結果？保留一份完整的日誌檔才可達成這樣的目的。在選擇系統時，稽核的功能中甚至應包括 undo(取消執行)之功能。

資訊安全政策之制定

不論就國內或國外，在制定資訊安全政策時，均應參考現行的法令規定。在美國有所謂的消費者保護法案(Consumer Protection Act)、電腦安全法(Computer Security Act)、電子資金移轉法(Electronic Fund Transfer Act)和聯邦儲備規範 C 等。國內則應依據電腦處理個人資料保護法、電子銀行安全作業控管基準、國家機密保護辦法與行政院及所屬各機關資訊安全管理要點等有關法令。由於各銀行間的經營條件不同，故尚應衡酌機關業務需求訂定資訊安全政策，研訂資訊作業之安全水準，並以書面、電子或其他方式通知員工及與機關連線作業之有關機關（構）、廠商。

一般而言，制訂資訊安全政策，應至少包括下列事項：

一、資訊安全之定義、資訊安全之目標及資訊安全之範圍等。

二、資訊安全政策之解釋及說明，資訊安全之原則、標準，以及員工應遵守之規定。

三、推行資訊安全工作之組織、權責及分工。

四、員工應負的一般性及特定的資訊安全責任。

五、發生資訊安全事件之緊急通報程序、處理流程、相關規定及說明。

資訊安全政策之評估

制訂之資訊安全政策，應定期進行獨立及客觀的評估，以反映資訊安全管理政策、法令、技術及機關業務之最新狀況，確保資訊安全之實務作業，確實遵守資訊安全政策，以及確保資訊安全實務作業之可行性及有效性。

資訊安全政策評估作業，可責由具有專業技術及知識之內部稽核單位、獨立客觀的資深主管人員，或是委請公正超然的民間專業組織或團體，進行資訊安全政策執行成果之評估。

應定期對所屬單位及人員進行資訊系統及技術應用之安全評估，以確保其遵守資訊安全政策及規定。

一、應列入資訊安全評估的對象：包括使用者、管理者、系統維護者等

二、資訊系統擁有者應配合定期的資訊安全評估，檢討相關人員是否遵守機關資訊安全政策、規範及有關安全規定。

三、應定期檢討及評估各項軟、硬設備的安全性，以確保其符合機關訂定的安全標準；評估對象應包括作業系統之評估，以確保系統軟體及硬體的安全措施，正確及有效地執行。

四、如專業人力及經驗不足，得委請民間專業組織團體或學者專家之協助。

五、系統安全評估應由具有專業知識及豐富經驗的系統工程人員，在權責主管人員的監督下，以人工的方式執行，或是以自動化的軟體工具執行安全檢查，產生技術評估報告，以利日後解讀分析。

資訊安全政策及規定之宣達

一、資訊安全政策及人員在資訊安全應扮演之角色及責任等有關規定，應在工作說明書或有關作業手冊中載明。

二、工作說明書或作業手冊規定之資訊安全政策、說明及規定，應包括執行及維護資訊安全政策的一般性責任規定、保護特定資訊資產的特別責任規定，以及執行特別安全程序及作為的特別責任規定。

三、員工如違反資訊安全相關規定，應依紀律程序處理。

資訊安全組織及權責

一、資訊安全組織

應指定副首長或高層主管人員，負責推動、協調及督導下列資訊安全管理事項：

(一)、資訊安全政策之核定、核轉及督導。

(二)、資訊安全責任之分配及協調。

(三)、資訊資產保護事項之監督。

(四)、資訊安全事件之檢討及監督。

(五)、其他資訊安全事項之核定。

得視需要成立跨部門資訊安全推行小組，推動下列事項：

(一)、跨部門資訊安全事項權責分工之協調。

(二)、應採用之資訊安全技術、方法及程序之協調研議。

(三)、整體資訊安全措施之協調研議。

(四)、資訊安全計畫之協調研議。

(五)、其他重要資訊安全事項之協調研議。

二、資訊安全組織權責

(一)、資訊安全責任分配

1、應訂定保護個人資訊資產及執行特定資訊安全作業，有關人員應負之責任。

2、應訂定有關人員在資訊安全作業應扮演之角色，責任分配之一般性指導原則，以作為各單位之權責分工依據。

3、每一系統應指定系統擁有者，並課予必要的安全責任。

4、應明定每一管理者應負的資訊安全責任。

5、應訂定每一系統的資訊資產項目，並訂定必要的安全程序及措施。

6、應指定每一項資訊資產及資訊安全程序的管理人員，並以書面、電子或其他方式告知其責任。

7、應訂定資訊安全之授權規定、授權等級及授權程序等，並以書面、電子或其他方式記錄之。

(二)、資訊安全分工原則

1、資訊安全管理之分工原則如下：資訊安全相關政策、計畫、措施及技

術規範之研議，以及安全技術之研究、建置及評估相關事項，由資訊單位負責辦理。

(1)資料及資訊系統之安全需求研議、使用管理及保護等事項，由業務單位負責辦理。

(2)資訊機密維護及稽核使用管理事項，由政風單位會同相關單位負責辦理。

2、設有稽核單位者，稽核使用管理事項由稽核單位會同政風單位辦理。

3、未設置資訊及政風單位者，由機關首長指定適當的單位及人員負責辦理資訊安全管理事項。

4、業務性質特殊者，得視實際需要由首長調整上述資訊安全分工原則。

(三)、資訊設施之使用授權

1、引進及啟用新資訊科技（如軟體、硬體、通信及管理措施等），應於事前進行安全評估，瞭解新資訊科技之安全保護措施及水準，並依行政程序經權責主管人員核准，始得引用，以免影響既有的資訊安全措施。

2、引進新資訊科技設施之行政程序辦理：

(1)業務上的核准程序

A.每一項系統及設備的裝置及使用，應經權責主管人員的核准始得使用。

B.系統及設備如有遠地連線作業需求，亦應獲得負責維護當地資訊安全之權責主管人員之同意。

(2)技術上的核准程序：所有連上網路的設施，或是由資訊服務提供者維護的設施，須經技術上的安全評估程序及權責主管人員之核准，始得上線使用。

(四)、資訊安全顧問及諮詢

1、資訊安全人力、能力及經驗，如有不足之處，得委請外界的學者專家或民間專業組織及團體，提供資訊安全顧問諮詢服務。

2、對委請資訊安全顧問，或負責資訊安全之人員，各單位及人員應予必要的協助及支援。

肆、密碼學

密碼學作為一門應用的學問，其基本功效即是保密－將資訊加密，以令第三者無從識別，這在公眾通訊環境上(例如 Internet)進行秘密通訊時最為需要。

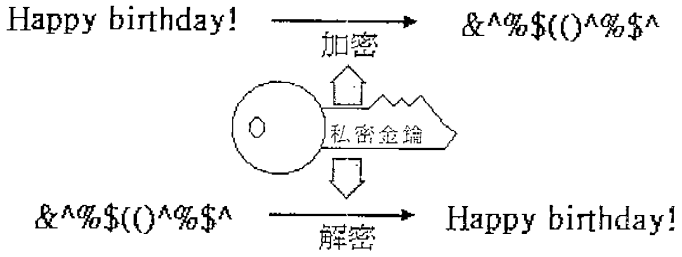
私密金鑰(secret key，也稱 private key)及公開金鑰(public key)的技術皆可滿足保密的需要。在前者，雙方皆須持有相同的鍵值(金鑰)對所傳送的資料加密、解密，如此雖然連線暴露在外，也無需畏懼任何可能的網路竊聽。但由於至少有兩人知道該金鑰，故任一方皆不能完全確定另一方是否已有意、無意將金鑰透露予第三者，這是利用私密金鑰通訊的缺點。

公開金鑰加密之作法為，通訊雙方除保有自身之私密金鑰，並擁有對方之公開金鑰。欲通訊時，一方使用對方的公開金鑰加密，在收訊時則使用自己的私有金鑰解密。公開金鑰雖無金鑰共享金鑰的問題，但它的缺點是，須要有較高的運算能量，故為達到經濟有效的目的，一般應用時皆採私密金鑰及公開金鑰的組合方式運作。

私密金鑰(Secret key，也稱 Private key)加密法

私密金鑰加密又名對稱式加密或傳統加密法，其特色是利用它加密或解密時皆使用同一個鍵值(金鑰)，明文(plaintext)經此種演算法與一組鍵值加密之後產生密文(ciphertext)，其長度約略與明文的相近，且須使用同一組鍵值方可將密文解回原本的明文。

私密金鑰(Secret key，也稱 private key)加密及解密



私密金鑰加密一般是用在機密資料的儲存及公眾網路的秘密通訊上，其它應用諸如資料完整性的驗證、連線時身份的識別等。

公開金鑰 (Public Key) 加密法

公開金鑰加密亦可稱為非對稱式(asymmetric)加密法，是近代密碼學新興的一門領域。根據文獻記載，此概念約起源於 1976 年，當時的技術人員一直為大型網路的

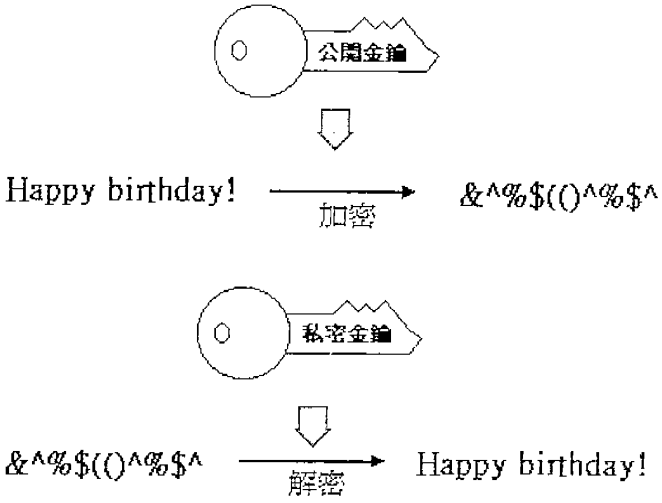
認證及保密問題所困，自從由 Whitfield Diffie 及 Martin Hellman 發表了不須交換私密金鑰的公開金鑰概念後，這些問題始獲得解決的契機。

公開金鑰加密的特色是利用它加密及解密時須使用兩組不同的鍵值，這兩組鍵值是成對的，若稱它們為 A、B 兩鍵值，則明文(plaintext)經此 A 鍵值的加密之後產生密文(ciphertext)，其長度約略與明文的相近，須使用 B 鍵值方可將此密文解回原本的明文。反之，由 B 鍵值加密的密文須使用 A 鍵值解碼。

在應用上，人們習慣將其中的一組鍵值稱作私密金鑰(private key)，由個人妥善保管，不對外洩漏，而另一組稱作公開金鑰，於大眾網路中廣為流佈。此種作法的好處是，當大眾中，某甲欲傳送資料給某乙時，甲可先將資料以乙的公開金鑰加密之後再傳至乙，乙收到之後再以其私有金鑰解密。因為乙的公開金鑰眾所週知，故眾人皆可用它加密之後傳送予乙，而僅乙持有其私有金鑰，故任何第三者皆不可能解讀寄予乙的資料。

公開金鑰的技巧因不須將自己的私有金鑰與他人共享，免除因雙方共同享有一把私密金鑰之可能缺點。

公開金鑰(Public Key)加密及解密



公開金鑰加密除了用在公眾網路的秘密通訊外，也可應用在包括連線時的身份識別及數位簽章等。

雜湊(Hash)函數

雜湊(hash)函數又稱作訊息摘要(message digest)，這是種單向的映射函數，它將一

任意長度的訊息映射成一較短的固定長度的數值，其特性是:

雜湊函數產生的值與輸入的訊息息息相關，原訊息的任何規律的或些微的變動皆會導致極為不同的輸出結果。

雜湊函數是多對一的(失真的)映射，故不應該由其輸出值計算出原本的輸入訊息，且由於是多對一的，故存在許多訊息其映射值是相同的。

雜湊函數的運算效率須極快，以滿足實際的各種應用，例如產生驗證值、進行即時的資料完整性驗證的。

換言之，雜湊函數即是在萃取給定訊息的精要。它將訊息快速濃縮成一組固定長度的值，並以此值作為該訊息的"代表"，此又稱該訊息的指印(message fingerprint)。並且，雜湊函數的演算法"保證"要再發現具有相同映射值、但訊息內容不同的機率極低，此機率一般是決定於映射值的長度，其位元數越多，可映射的範圍越大、重複的機率越低。

理論上，一個好的雜湊演算法對於原資料的任何變動須有極高的靈敏度，意即，無論原資料有著怎樣規律或無規律的變動，好的雜湊演算法皆應產生極無序的核對值。這類技巧有許多，例如 CRC，它將原資料視為一巨大的整數值，將之除以某精選的常數值之後，所得餘數即為雜湊值。

任何人皆可發明新的雜湊技巧，例如，將原資料視為一巨大的整數值，並取其平方根的某幾位作為雜湊值，只要他的新發明滿足雜湊函式的基本原則即可。

雜湊函式一般是用於產生資料的驗證值，它也被用於用戶密碼的儲存，為避免密碼被盜用，許多作業系統(如 Unix、Windows NT)皆只儲存用戶密碼的雜湊值，當用戶登入時，則計算他輸入的密碼的雜湊值，並與系統原有的儲存值相比對，若相同，方允許該用戶登入系統。

雜湊函數也用於加密通訊的認證程序，它可秘密(如密碼、認證過程的亂數)映射成非原來的樣子，以茲保護。雜湊函數另一較著名的應用是與公開金鑰加密法合併使用、以產生訊息的數位簽章，它提供一有效的方式以證明數位資料的來源、完整性、及無可否認。

DES 演算法

目前國際上較普遍的私密金鑰加密演算法是 DES 及 IDEA，前者為美國國家標準局(NBS,NIST 前身)於 1976 年公佈的加密標準，DES 主要用於業界及美國政府當局的非機密(unclassified)應用。DES 的金鑰長 64 位元，但因其中每個位元組皆取

1 位元作為同位(parity)核對，故有效鍵長 56 位元，DES 的基本運算是以連續 16 次的位元代換(substitution)及移位(commutation)及與鍵值相運算、將一 64 位元明碼區塊編碼成 64 位元暗碼區塊，對於大塊資料則將之切成每 64 位元為單位的區塊，並施以鍊接、回饋等多種技巧編碼。

RSA 演算法

公開金鑰加密在 1977 年之前仍屬理論，直到 MIT 的三位教授發表了 RSA 公開金鑰演算法，才正式將想法化為現實，RSA 此名稱源於它的三位發明人 Rivest、Shamir、及 Adleman，他們後來也參與籌組了 RSA 資料安全有限公司。

RSA 是目前最普遍的公開金鑰加密法，它的金鑰長度不定，普通是 512 位元。若考慮效率，可選擇較短的金鑰；若考慮安全，可使用較長的金鑰。其基本運算區塊長度也是可變的，但明碼區塊須小於金鑰長度，暗碼區塊則等於金鑰長度，由於 RSA 速率較一般的私密金鑰演算法(如 DES、IDEA)還慢，故較常用於加密較短的訊息，或對私密金鑰加密保護、再以私密金鑰加密訊息，或用於數位簽章。

RSA 演算法的基本概念是，任意選擇兩個極大的質數 p 及 q，並令:

n = pq q

Φ(n) = (p - 1) (q - 1)

再選擇一個與 Φ(n)互質的值 e，並尋找一值 d，且滿足:

ed d = 1 mod Φ(n)

如此，公開金鑰即是 n、c 的配對，標記為(n, c)，私有金鑰為 n、d 的配對(n, d)，在產生了金鑰對之後，p、q 兩值已無用處，應予以拋棄。

加密時，假設 m 為明碼訊息，可將它視為一極大數，則暗碼訊息 c 的求法是:

c = m^e mod n

解密時 :

m = c^d mod n

RSA 演算法要義如下：

若知道某人的公開金鑰，即表示知道了 n 與 e，若能反推得 p、q，即可獲得 d，解出私有金鑰，換言之，破解 RSA 的關鍵在尋找一極大數 n 的因數，但 n 可能長達數百位元，根據目前已知的最佳演算法，若欲分解一長 512 位元的數字的所有因數，可能得耗掉 50 萬 MIPS 年(1MIPS 年 = 一秒執行 1 百萬道指令、連續執行一年)這麼多道指令。

到目前無止，可以說，RSA 很安全，套用密碼學的基本公設，若已有許多聰明人無法解出某問題，此很可能表示該問題無解。

MD2、MD4、MD5、及 SHA 演算法

常見的雜湊函式有 RSA 公司的 MD2、MD4、MD5 及 NIST 在 1993 年 5 月公佈的 SHA，這些演算法的功能皆同，都在萃取給定訊息的精要、將之快速映射成一組固定長度的值，其間差異則在運算、效率、安全性、與雜湊值的長度等方面。

雜湊函式比較表

函式	運算	效率	安全性	雜湊值長度
MD2	最少	低	低	128 bits
MD4	較少	高	高	128 bits
MD5	少	中	較高	128 bits
SHA	最多	較低	最高	160 bits

伍、軟硬體建置安全規範

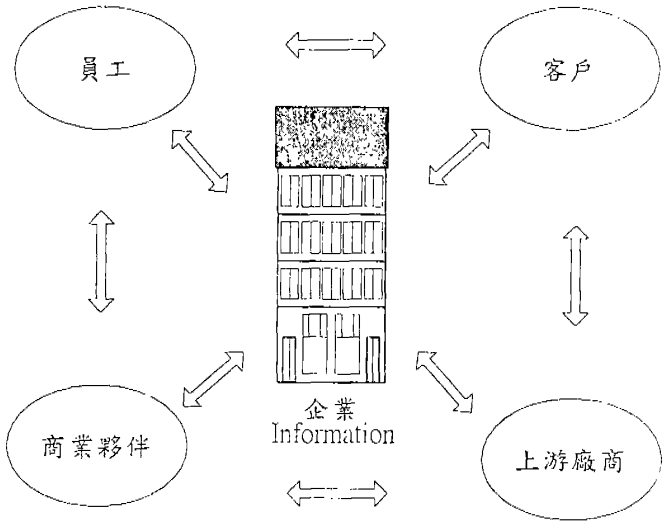
大約在十年前，網際網路的應用尚處於發展階段的時期時，大多數的公司企業所面對的電腦系統以及網路設備多屬於專屬性的系統，因為先天上架構的封閉便構築了天然的防護，使得企業內部的電腦資訊安全課題就顯得沒有那麼重要。但是隨著網際網路發展進程的迅速演化，越來越開放的網路環境和系統，現今整個企業運算的環境因為網際網路的蓬勃發展而起了重大的變化，企業安全管理人員所面對的是各種安全的挑戰，愈來愈龐大的系統及複雜的管理問題，使得電腦系統安全管理比以往更為複雜，所造成的影響也更令人無法預測。

本行的電腦系統由早期的 IBM 經 PhillipBouroughs 到現今的 Unisys 都是屬於專屬性大型主機系統，因為環境的單純以及封閉式網路的特殊性質、因此對於安全的課題只要著眼於主機電腦所提供的安全機制以及一些作業程序上的安全要求即可，但是到了近幾年，「開放式系統」逐漸成長茁壯，並以其日新月異發展之軟硬體架構及極具競爭力的市場價格和網際網路規模漸具成熟的推波助瀾之下，在短短數年之間不但橫掃桌面電腦市場，即使在傳統高階伺服器的領域也已搶下了半壁江山，金融產業面臨 IT 產業的巨變自然不免受到影響，傳統的業務已不敷社會一般民眾消費者的需求，以網際網路為架構發展出來的多元化全新通路將重新改變金融事業的面貌，諸如網路銀行、電子商務等新型態的業務將是繼信用卡塑膠貨幣之後改變民眾消費習慣的明日之星。

網路

現今的企業網路應用與幾年前的企業網路應用已不可同日而語，在網際網路蓬勃發展的帶動之下，許多企業的網路應用也走向了高普及性以及多元化的境界，許許多多的服務開始在企業間以及網際網路上蔓延，所以網路的重要性已經成為許多企業的生存關鍵，如同以前由人手作業進入電腦化作業一般，在今日企業的網路化與 e 化已成為企業面臨永續經營及競爭課題時最有效之工具，網路基礎建設是所有電腦化架構的基本，世界各國無不將網路建設視為國家競爭力提昇的一個重要的指標而全力發展。因此，一個穩定、有效率而且安全的網路環境對於企業的運作而言是不可或缺的。尤其是如金融、保險等產業，在網路上傳遞的資料都是攸關金錢交易的重要訊息，而且因其即時性的特性要求，對於企業網路

品質的要求更是嚴格，是故在今日，IT 人員，尤其是網路管理及網路安全人員所面臨的挑戰更甚於以往，要如何為企業打造一個可以信賴的電腦作業環境是我們必須努力以赴的目標。



網路化的商業環境圖

電子商務

近年來，由於網際網路的蓬勃發展，整個網路的環境已由早期學術性質進入具備商業運作條件，因此逐漸有愈來愈多的企業將商業運轉於網際網路上，電子商務的導入對全球產業產生了莫大的衝擊，無論是 B2B、B2C、C2C 等商業模式皆可強化各個公司間、協力廠商、客戶、員工的關係，此外透過網路高效率的連線方式，更可提供快速回應及效率化並發展企業間的資訊整合。本行自架構全行 MIS 系統開始陸續開發商業 EDI 等應用，隨後在網際網路上架設台銀網站提供外界各種金融服務，整合企業銀行、電子銀行朝向網路銀行功能發展。未來藉由網路無遠弗屆的特性更可提供許多過去無法想像的便利快速的金融服務。

電子商務、網路銀行的願景固然是美好的，但是要能夠成功必須要有主觀和客觀環境許多因素相互配合才能達到，而其中最為重要的部分應該還是在網路安全的考量上，因為經濟活動若是化為數位資料傳遞交易之模式，在虛擬化的環境下安全能夠確保才能讓使用者放心的使用商家提供的服務，因此如何提供一個網路安全的整體解決方案是所有打算投入網路商務的企業組織所必須面對的最大課

題。

目標與範圍

Internet Security 規劃時，應考慮到以下幾個層面：

一、實體設備 (Physical Equipment)

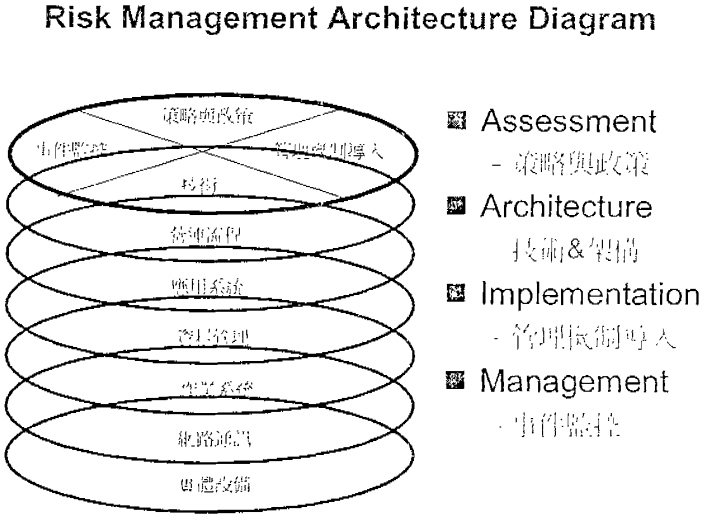
二、網路通訊 (Network Communication)

三、作業系統 (Operating System)

四、資料管理 (Database)

五、應用程式 (Application)

六、營運流程 (Business Process)



所有層面中相關的資訊安全內容，都需要對現有安全技術有所認知，進而規劃出完善的安全政策及計劃。針對以上各層面，也有相對應的資訊安全解決方案。本段之重點，將著重在 Internet Security 相關實體設備、網路通訊及作業系統的安全上。其他層面的安全，也將提及，藉以達成全方位資訊安全服務。

網路安全政策制定

網路安全政策的制定是建制網路安全的第一步。 清楚縝密的資訊政策評估、制定才能架構出完整可行的企業安全政策據以實行。目前業界最適宜的資訊

安全政策制定規範標準為 BS7799(British Standard Institute Code of Practice for Information Security Management). BS7799 是一專門為資訊安全管理所設計的標準。目的是為增加管理效能，並提供確保企業資訊資產的完整性、可用性及保密性。BS7799 對企業安全管理政策提供最完整的考量及建議(Guideline)，並為日後成為 ISO17799 認證奠定基礎。

BS7799：十大項目

一、資訊安全政策 (Security Policy):

提供管理的原則與方向及資訊安全的支援（Providing management direction and support for information security.）。

二、資訊安全部門 (Security Organization):

企業組織中以提供專職完整的資訊安全管理(Managing information security within the organization.)。

三、資產分級與控制 (Assets Classification and Control):

對企業資產做適切的保護及維護(Maintaining appropriate protection of organization assets.)。

四、人事安全 (Personnel Security):

以降低人事錯誤，竊賊，與設施的誤用(Reducing the risks of human error, theft, fraud or misuse of facilities.)。

五、實體與環境安全 (Physical and Environmental Security):

以避免未經認證的存取，破壞及對資訊系統服務的干擾(Preventing unauthorized access, damage and interference to Information Technology services.)。

六、電腦及網路安全 (Computer and Network Security):

確保電腦及網路設施運作的正確性與安全性(Ensuring the correct and secure operation of computer and network facilities.)。

七、系統存取控制 (System Access Control):

控制對商業資訊的存取權限(Controlling access to business information.)。

八、系統開發與維護 (Systems Development and Maintenance):

確保資訊系統內建置完整的安全功能(Ensuring that security is built into Information Technology systems.)。

九、企業持續經營計劃書 (Business Continuity Planning):

規劃當企業活動被意外中斷時所必須採取的計劃緊急應變措施(Having plans available to counteract interruptions of business activities.)。

十、合法性 (Compliance):

避免與任何刑事及民事法律衝突(Avoiding breaches of any statutory, criminal or civil obligations and of any security requirements.)。

網路設備安全說明

依據企業電子資產安全管理(Digital Assets Management)原則，可以粗淺定義'凡是屬於電子處理相關之硬軟體設備及系統均應列入管理稽核'。因此，電子資產安全討論規範範圍應該包含電腦系統硬軟體、網路通訊系統。

電腦系統硬軟體安控原則，按不同之專業認知有不同之分類方式，並依此而規範安全法則，但是不管從硬體或軟體觀點來看都會有不夠嚴謹之處，因此，或許可以從應用系統觀點來涵蓋作業系統、資料庫系統及相關之電腦硬體設施。但是以下只針對'網路通訊設備'安全討論。

網路通訊處理元件可分為主動及被動元件，按安控管理原則均需說明安全管理機制。然而，目前台灣電訊通訊法規規定，所有之數據服務被動元件均由第二類電信業者提供，所以舉凡數據線路(Leased Line)、數位服務數據機(Channel Service Unit ;CSU/Digital Service Unit ;DSU)等設備之安全管理及稽核將不在討論範疇之內。

網路通訊設備之基本安全規範 (Networks Infrastructure)

網路安全規範架構，第一個步驟必須先定義控管標的物，然後針對控管標的物訂定安全規範。一般企業網路甚至大至廣泛之 Internet Service Provider (ISP)之 Internet 服務網路架構內基本之網路設備不外乎廣域網路交換器(WAN Switch for ATM or Frame Relay)、路由器(L3 Router)、區域網路交換器(L2&L3 LAN Switch)

及 Web 交換器(L4~7 Web Content Switch)等。下文中將針對常見之網路設備如路由器(L3 Router)、區域網路交換器(L2&L3 LAN Switch)之基本安全管理規範討論。安全控管規劃概念主要針對設備所提供之管理軟體或方式所延伸之管控漏洞，而加以補強並可形成稽核點。並分別以下篇幅敘述。

網路路由器安全控管規範 (Router Secure Managed)

- 管制 Router Telnet 進出機制 — 如果需開放此功能可以 Reverse Telnet 方式或加入 ACL(Access Control List)或導入 AAA 機制，可以使用類如 AAA(TACACS+ or RADIUS)機制。
- 管制 SNMP 進出機制 — SNMP version 1 只能以"community string"及"Read or Write only"方式控管，SNMP version 2 支援" MD5-based digest"方式加強控管功能。可以使用類如" MD5-based digest"機制。若 SNMP version 1 因其他因素短期內不可能更換，可建議加強：

  關閉對Internet之所有Service或加入ACL(Access Control List)

  設定管理機制如Log(Trap)Received/Read/Write之絕對IP
- 管制使用 HTTP 管理 — 如果需開放此功能可以加入 ACL(Access Control List ；**ip http access-class & ip http authentication**) 或導入 AAA 機制。
- 關閉不需要之網路協定服務(大部分為 Router 預設值)如(Cisco IOS 為例)：

Use	To
no service tcp-small-servers **no service udp-small-servers**	Prevent abuse of the "small services" for denial of service or other attacks.
no service finger	Avoid releasing user information to possible attackers.
no cdp running **no cdp enable**	Avoid releasing information about the router to directly-connected devices.
no ntp enable	Prevent attacks against the NTP service.
no ip directed-broadcast	Prevent attackers from using the router as a "smurf" amplifier.
no ip source-route	Prevent IP source routing options from

	being used to spoof traffic.
no ip bootp server **no ip domain-lookup** **no ip http server**	Prevent non-authorizes required

- System Log-Messages – 路由器軟體系統之 Log-Messages 包括 AAA logging(TACACS+ or RADIUS)、SNMP trap logging、System logging 記錄系統重要訊息必須依照安全控管機制予與管理。以 Cisco 路由器為例 Logging 輸出方式包括以下方式均應注意控管：
  1. 系統 In-band 控管埠 Console Port 及 Out-band 控管埠 Aux. (系統指令: **logging console**).
  2. 使用 UNIX 系統主機之"syslog" 協定收訊息(系統指令：**logging** *ip-address*, **logging trap**).
  3. 遠端與近端 VTYs sessions 協定收訊息(系統指令：**logging monitor**, **terminal monitor**).
  4. 將訊息接收並存放在路由器動態記憶體內的緩衝區(系統指令：**logging buffered**).
- 管制路由協定交換 – 靜態路由協定(Static Routing)不會主動與相鄰路由器交換路由表，必須經由指令設定才知道下一個路徑、所以是最安全之路由控管方式，然而在中大型企業網路中繁複之靜態路由表設定反而會造成管理死角。因此，動態路由協定配合靜態路由管制和路由交換安全規範，即可保證路由表不被竊聽及複製而造成網路災難。IP 路由表交換基本原理為 Neighbor 關係，IP Routing Security 又稱為 Neighbor Authentication 以 Cisco 路由器 IOS 為例:

  IP BPG : "Configure Neighbor Options"

  IP EIRP: "Configure Enhanced IGRP Route Authentication"

  IP OSPF: "Configure OSPF Interface Parameters" and "Configure OSPF Area Parameters" and "Create Virtual Links"

  IP RIP : "Enable RIP Authentication"

- Routing Policy – 制訂路由協定策略可統籌控管企業內路由協定交換機制，並可依路由協定特色調整出最佳狀態。例如：一般企業網路會因網路規模大小，而將網路細分為核心路由器(Core Router)、集線路由器

(Distribution Router)、端末路由器(Access Router)三種各司路由機制。

(一)、核心路由器(Core Router)負責企業內所有路由表交換，所以必須使用具備容錯之動態路由協定如 OSPF 或 EIGRP，需注意以下設置要點：

1.所有路由表交換均需加入加密機制如 MD5 authentication 避免被仿製。

2.將設定交換條件為"絕對性"而非 "相對性"例如：OSPF 協定設定時一般會採用 IP Network Range 廣義性定義所有符合條件介面均可收發 OSPF Routing Broadcasting，一不小心就被有心人竊聽、仿製造成安全控管漏洞。

3.設定路由交換條件為控管依據，如路由器內支援四個通訊介面，就可依安全管制條件設定任意兩介面之間路徑交換機制。可成為企業網路安全控管中樞。

4.如果核心路由器兼具企業內部 Intranet 安全控管機制，則需關閉所有之動態路由協定，而以靜態路由為主。

(二)、集線路由器(Distribution Router)負責企業內不同路由協定之路由表交換，可以設定 IP Networks 交換過濾條件，但是很多情形會以處理效率為主而省略路由控管機制，因此會較著重於網路架構及整體設計彌補，基本之 Neighbor Authentication 仍須加入。

(三)、端末路由器(Access Router)負責端末網路處理通訊，存在許多遠地環境及人為控管問題，必須以較嚴謹之方式控管。在路由協定控管方式中分別可以不同技巧達到目的。

1.最佳方式是端末路由器不與鄰近路由器交換任何路由表，即所謂設定 Default Route 而上層路由器則相對設定靜態路由設定回送之 IP Network。因為沒有交換任何路由表，所以不會有仿冒及竊聽行為發生。

2.若因其他原因為了加速路由處理，也可能加上動態路由協定設定，除了基本之 Neighbor Authentication 須加入外，需注意 IP 路由交換介面之設定外，路由過濾機制必須設定。

3.另外可設定 VPN 方式保證兩端點間資料通訊安全，可以使用的技術有 IP Tunnel 及 IBGP。

區域網路交換器安全控管規範 (LAN Switch Secure Managed)

- 許多區域網路交換器將 Port Trunk 預設值為 auto，安全控管原則下必須設定為 Off，因為有心人可以藉此漏洞接收網路內各 VLAN 資訊。
- 設定區域交換器內部使用的通訊埠不能屬於任何 Layer3 路由交換區段，可以避免路由資訊被竊聽或仿冒。
- 區域網路 VLAN to VLAN 交換會經由 Layer3 Switch/Routing CPU 處理，預設值為廣義性全通，而以安控角度考量，應該有條件控管。
- MAC Address 具有絕對性，可以被使用在控管端末 PC 或處理單元之連線控管機制。
- 管理方式同樣必須由中心統一控管，加入 AAA 機制並謹防成為侵入企業網路之跳板。

網路資源管理者之認證及授權機制 （AAA）

Authentication, Authorization, and Accounting 通稱AAA，基本功能包括使用者名稱及密碼認證、資源使用權限授權、記錄資源使用時間等。所有被控管之網路通訊設備需設定通用之AAA協定，一般使用RADIUS & TACAS+協定，並需配合AAA應用軟體系統(如RSA公司設計的ACE Server)，應用設定使用範圍如下：

- Configuring local login authentication
- Controlling login using security server authentication
- Defining method lists for authentication

所有進入路由器或區域網路交換器之近端(Console or AUX ports)或遠端(Virtual Telnet)入口均需導入AAA控管機制。

安全管理機制

安全控管機制原則，屬於例行安控作業之規範及未來任何網路設備增加或變更任何設計所應該遵行之作業方針。

控管系統可分為：

- SNMP 管理主機 – 提供藉由 SNMP 協定管理所有具備 SNAMP Agent 的設備
- Syslog 管理主機 – 集中收集網路設備 log 資訊以為稽核基礎資訊

- 進出網路設備管理伺服器(AAA Server) – 提供網路設備 one-time 及兩階段使用者認證服務機制
- 系統管理主機 – 遠端管理如果只能使用 Telnet 必須加入"絕對語法" ACL 設定。近端管理可使用 Reverse Telnet 設定，並 Disable Telnet 服務，而最佳管理方式係使用制度及機房作業管理機制，主要提供網路設備管理設定、軟體及聯絡人更改等功能

安全控管機制涵蓋範圍：

- 進出管理網路設備之使用者認證及管理權限
- 管理網路設備之管理系統主機控管
- 使用路由器軟體功能設定，阻絕不屬於正面表列之 IP address、Sub-Networks、VLAN Trunk Protocols、Routing Protocols、Protocol Broadcast、 Multicasting

增加上述控管機制，將可以減低以下侵略性威脅

- 未被授權而欲進入網路設備控制系統
- 藉由網路欲進入網路路由器而進行破壞或癱瘓網路行為
- 系統管理當時的資訊被竊聽或仿製
- Broadcasting or Multication 造成之管理問題
- IP 資訊被仿冒利用危機

基本安全架構需求設計表

Location	Key Devices	減低或直接消除以下威脅
Core Module	Layer 3 Switching -路由器或交換器設備	Packet Sniffer -- 資訊竊聽、仿製、破壞
Building Distribution Module	Layer 3 switches – 使用 Layer2/3 交換器提供伺服器或重要資訊使用者	Unauthorized Access – 可在 Layer3 VLAN 內設定 Subnet 過濾 IP Spofing – 依 RFC2827 規範設定 Packet Sniffers
Building Module	Layer 2 switch User workstation—提供端末機使用網路資源認證 IP phone – 防止類比交換系統安控漏洞	Packet sniffers 電腦病毒及特諾伊馬威脅(Virus and Trojan horse applications)
Server Module	Layer 3 Switch Corporate/Department Servers E-Mail Server IDS	Unauthorized Access AP層攻擊 – 保障OS 、設備、應用軟體安全 Packet Sniffers IP Spoofing Trust Exploitation –提供 VLAN 控管基本原則 Port Redirection – Host Base IDS
Edge Distribution Module	Layer 3 switches	Unauthorized Access IP Spoofing Network Reconnaissance Packet Sniffer

企業網路安全架構建置範例

有鑑於企業資訊的保存以及企業對外服務的持續提供之不易，下文將以一個常見的企業網路安全架構建置範例，分為四個階段來討論企業主機系統的安全防禦政策以及安全政策對於企業網路以及系統的衝擊：

一、企業第一期安全規劃建議

(一)、防火牆的導入

(二)、DMZ 區域的建立

(三)、網路拓樸的變更

(四)、病毒防禦計劃

(五)、VPN 的導入

(六)、PKI 的建立

(七)、安全政策的訂定

二、企業第二期安全規劃建議

防火牆的備援及加強強固性

三、企業第三期安全規劃建議

IDS 工具的應用

四、企業進階安全規劃建議

(一)、PGP 加密技術的導入

(二)、Certificate Server 的角色

(三)、PKI 的進階應用

(四)、補強已知的漏洞

本文所討論之防護措施之所以會分成四個階段來實施是因為企業系統安全的軟硬體基礎建設有可能在短時間內設定完成，但是企業內部員工以及資訊管理人員的安全觀念以及操作習慣卻是需要一段時間來適應的！因此企業可以經由以上四階段的步驟來逐步完成企業的安全防禦措施以面對內部使用者的適應性以及網際網路上的各種挑戰。下一章節將介紹一個標準的企業網路以及初期的建置規劃。

第一期目標規劃

初期的企業安全規劃是以防火牆為主，因為此時的企業使用者多半對系統安全的認識不深而且對其做教育訓練較不易吸收；而防火牆的特性之一就是能夠儘量不引起內部使用者對外使用資訊的操作行為改變，因此在企業初期的系統網路安全是以防火牆為主軸並且配合企業特有的安全政策來對企業內部員工做適度的使用習慣改變！

Demilitarize Zone (DMZ)是在建置企業防火牆時的重要觀念，許多企業即使在建立防火牆後仍希望能持續提供企業的網站或是郵件以及檔案傳輸等等服務給外界來使用，但是把這一些企業應用伺服器放在防火牆的內部就等於是讓網際網路的使用者封包進入到防火牆內部，這樣在安全的考量下會為內部的其他系統主機造成傷害！因此將這一些主機移至 DMZ 中將可以降低風險。DMZ 是指連接在防火牆上的一個特殊的區域，一般來說在 DMZ 中只會有伺服器存在，而防火牆再視 DMZ 中有那些服務來決定要讓那一類型的封包進入，舉例來說，假設企業提供網站以進行電子商務時，管理者可將網站建置在 DMZ 中以強制使防火牆將由網際網路上的主機所送出的 http 的封包只送至 DMZ 中而不直接送至防火牆的內部網路中以求內部網路的安全。

企業網路的拓樸是否需要做更動是視管理者的設計理念而定，但是一旦將防火牆裝置上線後，企業網路的拓樸就得要有所改變！變更的幅度可大可小，主要的目的就是卻使企業內沒有任何一台主機可以不透過防火牆而被外界的主機所存取！這其中也包含了數據機的使用，假使企業內部的主機可以透過數據機來與外接取得聯繫的話，那外部的使用者就有可能可以存取內部網路上的其他主機了！因此企業網路拓樸在安全的課題上也是重要的一環。

在企業系統安全的領域裡，防毒一直是一個被忽略的課題，當網際網路的應用越來越成熟及快速時，病毒以及網路上不良的程式的傳播速度以及破壞力也是隨著網際網路的成長而成長！因此訂定一個良好的病毒防禦措施是相當重要的一個步驟。防毒政策倚賴一個好的防毒軟體來達成，而好的防毒軟體不但要有能力處理病毒的入侵以及不良的程式的下載，而且還要有能力在不同的作業系統以及應用程式平台上執行的能力，但是最重要的就是在防毒管理上必須要能做到單一且集

中的管理主機、企業內防毒軟體版本一致、病毒碼一次更新以及定期的作全域排程掃描以及病毒感染報告等等要求！

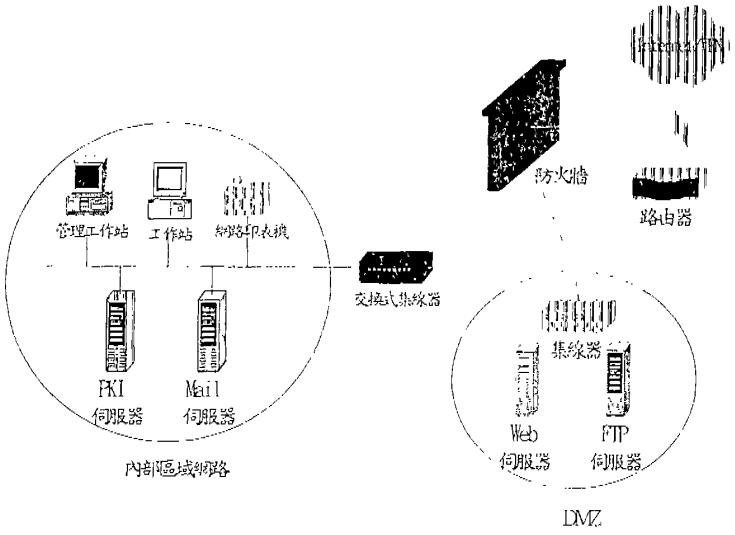
VPN(Virtual Private Network)在企業對外資料傳輸的領域裡已經是相當成熟的一個解決方案！許多的企業在版圖擴大時都遭遇到類似的問題，就是如何的在各個分公司之間安全的傳輸資料以及如何將操作過程簡化，接下來的問題就是企業資訊完全電子化以後需要在企業以外的地方工作的行動使用者如何安全的與企業內部主機做溝通。VPN 能夠滿足企業對於此類問題的需求，它使用了包含多種演算法的加密技術來讓資料在企業外的各個節點之間作安全傳輸，如此便足以確保資料在總公司、分公司、商業夥伴以及行動使用者之間作安全的傳輸，並且還可以配合企業安全策略的運用以讓遠端的節點不會察覺到防火牆的存在！

PKI(Public Key Infrastructure)的在此階段建立是為了因應 VPN 的導入，雖然 PKI 所能做的事情還有很多，但是在此階段並不建議企業對於 PKI 做太深入的運用。承繼上一段介紹 VPN 的功能，當 VPN 要與其他 VPN 節點通訊時有兩種認證方式可以選擇，Pre share secret 讓兩個節點預先溝通好一組密語，將來兩個節點互相使用 VPN 溝通時就是使用這一組密語來互相認證，這樣有一個好處就是設定簡單方便，但是卻有一些壞處就是管理上的安全性不高以及雙方都必須是使用固定的 IP 位址。Certificate Based 是使用 PKI 所發出的 certificate 來為雙方做認證，因此雙方的使用者都沒有機會輸入任何資料來試圖闖過 VPN Server 的認證機制，這樣的好處是在管理上的安全性很高，因為 PKI 所發出的 certificate 具有唯一性的電子憑證，而且適合於動態 IP 位址的使用者來使用，但是它也有一些壞處，那就是電子憑證一但遺失或是被竊取後必須立刻通知 certificate 的管理單位，否則身分容易被盜用！而且另外一個缺點就是 PKI 的觀念還很新，因此管理人員需要再培養。

企業安全策略的訂定必須要有完善的規劃以及全員的參與才能夠有良好的效果，在企業初期制訂安全政策時應由主導單位彙集企業內部各部門使用者的需求以及分公司之間的需求後經過詳細的評估後再來制定安全政策。制定企業安全政策時必須先簡化使用者的需求以避免因使用者需求過多而造成企業制定系統安全政策時容易造成政策互相衝突的現象，接著必須考慮企業網路拓樸是否有改變的需要，然後再將所有的需求轉化為一項一項的安全規範以便讓防火牆管理員以及企業其他管理人員易於參考以及實施！接著就是實驗性的實施一至二週後再對企業

內部使用者做教育訓練以及商業夥伴做資訊系統使用效率調查以及，再依調查的結果做系統修正以及改進，如此反覆執行直到使用者完全熟悉為止。

初期目標適用產品例如：IBM Tivoli SecureWay、NAI E-ppliance WebShield Firewall、Check-Point Firewall-1、Cisco Secure PIX Firewall、WatchGuard LiveSecurity System 等



第一期網路示意圖

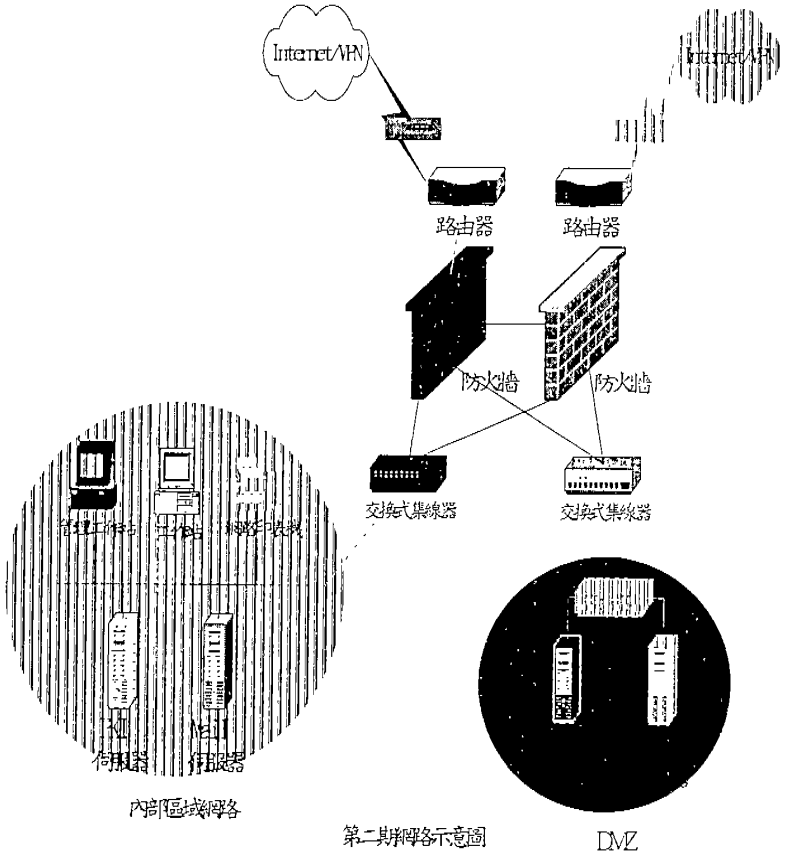
第二期目標規劃

前期的規劃已經將防火牆以及其附屬的功能部署到企業內部，因此接下來的工作就是讓這一個系統安全的主控角色-防火牆具有備援的特性以讓企業內外部通訊的斷線率達到最低。此外也考慮使用硬體防火牆及軟體防火牆同時兼備達到最大的安全效果。一般來說防火牆損毀時就幾乎跟專線斷線是畫上了等號，企業在與網際網路的溝通時如遇到斷線時所有對外提供的服務都會停擺！因此這一期

的目標就是要使防火牆具有備援效果。

第二期目標適用產品

StoneBeat Firewall FullCluster、NAI E-ppliance WebShield Firewall Backup



第二期網路示意圖

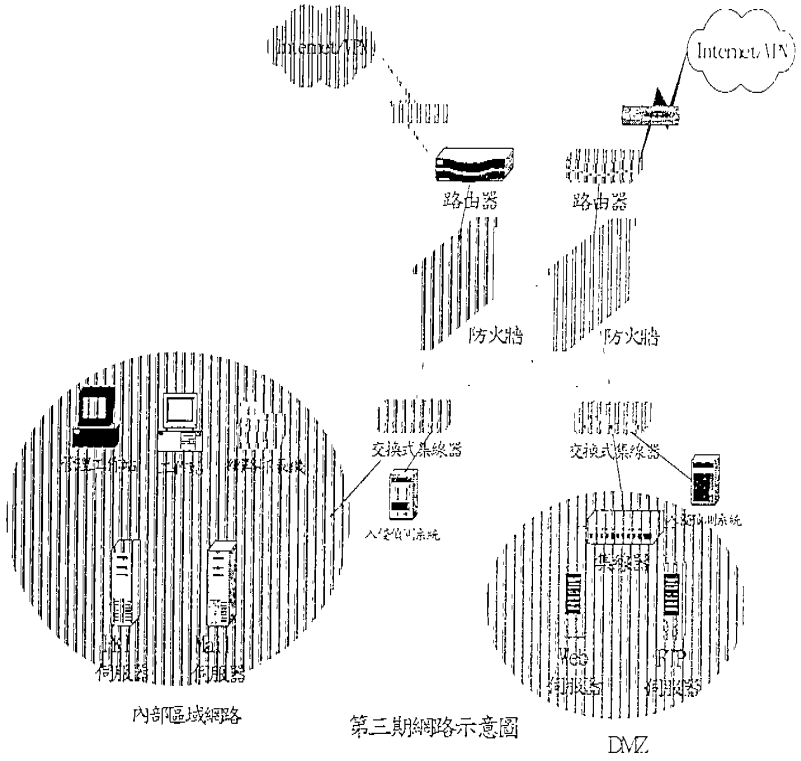
第三期目標規劃

在前兩期的規劃中我們將防火牆等相關的設施的功能大部分都已設定完畢，而目前所有進出企業的一切服務以及網路封包資料也已經由防火牆上的安全政策來處理，傳輸給企業外部人員的資料也使用了 VPN 保護起來，照理來說企業系統以及資料的安全方面的顧慮已經可以說是考慮周密且萬無一失了！但是這是真的嗎！在系統安全的考量裡可以說是沒有萬無一失的這一回事，因為駭客永遠會想盡辦

法去研究一些新的攻擊方法去攻擊作業系統、通訊協定或是應用程式的漏洞，同時企業也無法保證每一個內部的員工都是對企業內部機密資料守口如瓶的，更可怕的是企業碰上的是屬於破壞型的駭客或是不良的員工，這一種人對你的機密資料並不感興趣，他純粹只是想要破壞你的系統以及資料而已！因此企業系統安全的工作並不是做一會兒功夫就可以一勞永逸的工作，而是企業管理人員與惡意攻擊者的一場永無休止的戰爭。因此第三期的重點將放在 IDS(Intrusion Detection System)工具上。

許多的企業在安全規範以及設備建立完成後都會用 IDS 等等的工具來對系統以及防火牆來做安全漏洞的掃描，而 IDS 工具的廠商也不斷的蒐集許多新型的駭客攻擊方式來充實 IDS 的資料庫以讓 IDS 能使用更多的方法來刺探企業的安全防禦主機。

第三期目標適用產品 ISS RealSecure IDS、Cisco Switch-based IDS module、Cisco Secure IDS、NAI CyberCop Scanner IDS



第三期網路示意圖

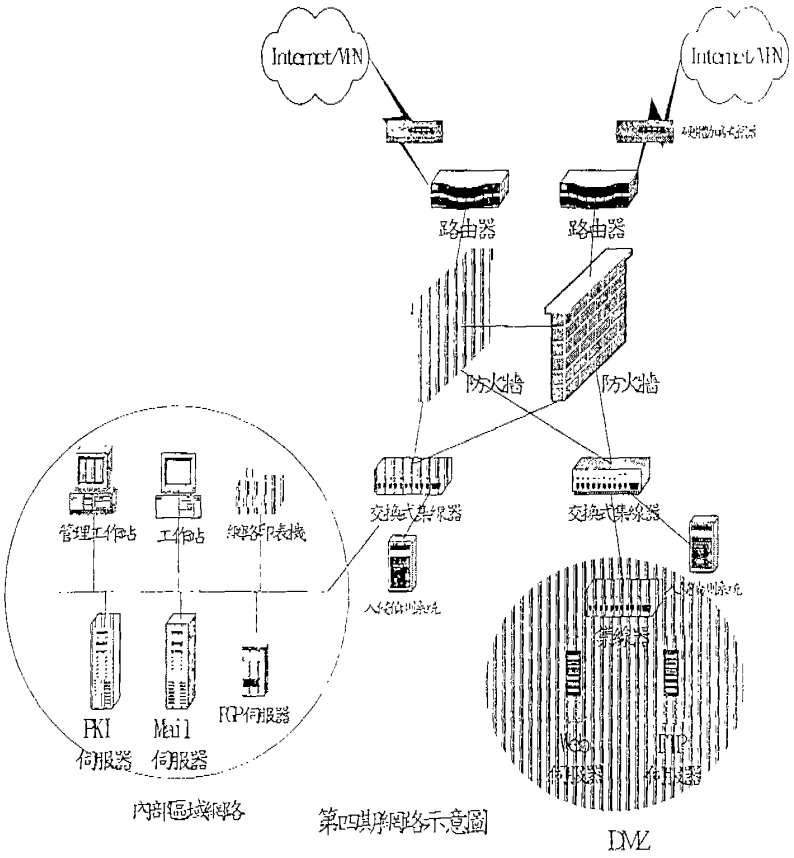
第四期目標規劃

在前幾期規劃的過程中已經將企業與網際網路間的通道用防火牆隔絕了起來，因此第四期的規劃建議就將安全重點放在防火牆內部的資料安全問題上！在一般的企業網路安全規劃中比較不常提及企業防火牆建置完成後的內部資料加密安全的動作，似乎防火牆就代表了一切！所以往往有許多企業的防火牆被突破後，資料就讓人予取予求了。因此企業必須更進一步的將內部敏感的資料用比較特殊的方式來儲存與管理。

PGP 是從 Unix 盛行的時代就存在的一個軟體，它可以快速的將使用者的資料如檔案、磁碟機、電子郵件等等以數位加密的方式來儲存以及傳送，除了加密的功能以外，PGP 還提供了數位簽認的功能使得企業所使用的資料如檔案以及電子郵件等等都能夠做數位簽認以達到不可否認的有力證據。當企業內部使用者在儲存他們的重要檔案時可以選擇是否要將此檔案單獨加密或是存到一個經過加密處理的磁碟機中，而電子郵件也可以做安全的加密傳輸。加密驗算法包括對稱式加密的 DES、Triple DES、CAST、IDEA 以及非對稱式加密的 DH/DSS、RSA 等等提供使用者更安全的加密機制，PGP 並且為美國政府正式允許出口的 128 bits 加密解決方案。

PGP Certificate Server 提供企業使用者一個集中的場所來儲存企業內使用者所產生出來的公開鑰匙。因為企業內部的使用者在使用 PGP 前必須先產生出一對專屬於自己的鑰匙以後才可以使用 PGP，而要傳送加密文件給企業內的某位收件者時必須先與此一位收件者交換公開鑰匙後才可使用對方的公開鑰匙來為欲傳送的物件加密。正因為交換過程是如此的繁雜以及不便，所以 PGP Certificate Server 正好可以提供使用者將其公開鑰匙上傳至此以供其他使用者搜尋下載使用。

第四期目標可用產品如 PGP Data Security Suite、PGP Certificate Server 等



第四期網路示意圖

企業資訊系統安全

上文的規劃舉例主要是針對想要在網際網路上執行電子商務以及資料交換的企業所做的系統性以及整體性的規劃！在產品的使用方面則目前資訊業界專業相關廠商均有完整配套的產品可資選擇使用，使用同一家公司的產品的好處是在產品橫向的整合方便且技術支援較不會發生廠商相互推諉的問題，否則就得慎選合作廠商業者必須有足夠的技術能力整合各種軟硬體設備及提供後續之支援服務，並且企業主在選擇工具來執行系統資料安全的規劃使用時必須注意產品的成熟度以及完整的整合性。

如企業因本身的需求或是其他的考量因素等等無法實作以上的四個步驟時，管理規劃者可依企業需求自行增加或是省略，但是對於企業應用環境的安全考量來說每一個步驟都是相當重要且不宜省略的！資料系統的安全的觀念是無論是老闆與員工、無論是大系統或是小主機都該一視同仁！完善的系統資料安全規

劃除了精確的事前規劃工作、快速的架設實作效率以外還有賴企業安全稽核人員的定期檢查以及調整產品的功能才能使得企業網路服務足夠因應網際網路上各種嚴苛的挑戰。

陸、網路銀行交易安全規範

由於網際網路的規模、和其上服務的內容持續不斷地擴增，銀行從過往只提供資訊服務轉變成必須提供全交易金融服務。因此，如何參酌國內外法令、技術的規範以提供安全交易的環境，實極重要。本章節主要是針對技術層面上作一論述，以作為銀行在選擇有關網路銀行交易安全技術的參考，對於法令的規範，我們將簡述美國政府規範網路銀行(Internet banking)交易的相關法規。

網路交易安全課題

在網路交易過程中最應重視的是商家如何知道消費者有合法的帳戶？消費者如何信任素未謀面的商家？當商家無法確知交易要求的真假時，信任和安全議題不僅限制零售商銷售額也產生很大的調查和退款成本。從技術層面觀之，網路銀行交易安全規範中最重要的兩項標準 SET(Secure Electronic Transaction)和 SSL(Secure Sockets Layer)，可用以解決上述信任和安全的議題。SSL(Secure Sockets Layer)最早是由 Netscape 所發展出來，其目的是在使網際網路通訊雙方能有一安全的方式進行資料的傳輸。其間經過幾次的更版，現行最常用的是 3.0 版。SET 則是由 IBM 和信用卡組織為確保網上交易的安全，所訂出的一個安全交易架構，以確保消費者、商家和收單銀行之權益。

SSL

SSL 允許主從端的應用程式以一種避免遺漏、遭竊取或資料損毀的方式溝通，因此可以提供通訊雙方應用程式的私密性和可靠性。SSL 包含兩層-SSL Record Protocol 和 SSL Handshake Protocol。前者位於 TCP 之上，其作用是在對各種較高的通訊協定作封裝(encapsulation)的動作。後者可允許伺服器和 Client 間彼此認證，同時在應用程式協定傳送或接收第一個位元組資料前協調出一個加密的演繹法和加密金鑰。SSL 的另一個好處是他獨立於應用程式(application protocol independent)，即使較高階的通訊協定亦可透通地架構於 SSL 通訊協定之上。以下列出 SSL 三種基本的特性：

一、聯結是私密的。在起始商談以定義好加密金鑰後，雙方才開始進行加密，通常是以對稱式加密(如 DES[DES])的方法作資料加密。

二、雙方之間以非對稱式或公開金鑰加密方式作認證(如

RSA[RSA],DSS[DSS])

三、聯結具可靠性。使用上鎖的 MAC(keyed Message Authentication Code)作為訊息完整性檢查之用，在傳送訊息將其包含在內，並採用安全的雜湊函數計算 MAC 值。

SET

SET 可以說是一個共同的技術標準，他設計用來保護在網際網路上以卡片付款購物之行為。現階段而言，SET 是網際網路上可最為安全掌握付款的方法，同時提供消費者、商家和金融機構需要在網際網路上全方位承諾利益的工具和信心。網際網路的成長帶給消費者購物的便利、為商家帶來全球的客戶、也為金融機構帶來以付款卡付款客戶的基礎。他經由認證的方式，加強兩者間一系列的檢查和反檢查工作，以使資料可以被正確地和安全地處理。在這樣的方式，SET 建立一個電子商務交易處理的新架構，並確保機密性、資料的完整性和每一個體的認證。

要完成上述的安全性和認證性，SET 需要一些元件：

一、數位憑證

是在 SET 安全交易中一個重要元素。而藉由數位簽章驗證參與者的身份，數位憑證可被確認。在國外金融機構可充當憑證簽發機構(Certificate Authority)，核發存戶和商家憑證。對商家而言有了數位憑證，其合法性可被確認，提供了品牌的保證。(有點類似實體商家門口貼的信用卡組織標識)消費者在網路交易過程中提示數位簽章，就如同在面對面交易中出示塑膠卡片。

二、憑證機構

有兩種憑證機構，一種可以簽發憑證予發卡行和收單行，另一種可以簽發憑證予個別的付款閘道。發卡行簽發憑證予個別的消費者，收單行簽發憑證予他們的商家。如此構成一個階層式的信任結構，可和實體世界繼存的付款關係相對應。

三、電子錢包和加密

為要求和取得數位簽章，消費者需要連上網際網路、瀏覽器，再配合可

用於 SET 的電子錢包。所謂電子錢包是一個軟體程式，可以存在消費者的電腦內，亦可存在於發卡行的安全伺服器上。電子錢包內存有一些重要的資訊，如付款帳號和到期日及 SET 憑證。資訊在網際網路上傳送前電子錢包須先將資料加密，所以電子錢包可確使付款資訊在網路上繞送時保持機密。

四、商家 SET 軟體要件

要成為 SET 的一員，商家只需要整合 SET 軟體元件進其虛擬前置系統即可。其可用作付款過程之實體認證和清算程序。

五、付款閘道

付款閘道位於符合 SET 標準商家和商家銀行(收單銀行)間之介面，他對許多形式的卡片執行付款認證服務，如果有必要付款閘道執行清算服務和資料抓取。他有三個主要的功能：

(一)、解密

(二)、認證交易中所有的參與者

(三)、將 SET 訊息重新組成符合商家 POS 系統的格式 0 字元 SET 交易程序

當消費者從商家的網站選擇欲購置項目並送出訂購單，SET 交易程序即開始：

- 持卡人選擇以 SET 方式付款選項，然後選付款的卡片：如 Visa 或 Master Card。
- 商家起動持卡人的 SET 電子錢包，電子錢包送出一個訊息給商家，指定消費者付款的卡片。
- 商家與持卡人彼此交換訊息，驗證每一個身份、並對付款資訊加密。加密訊息送往商家，商家將加密的資訊送往收單行解密並認證。
- 收單銀行對交易的所有單位進行認證，並在正常授權程序處理交易。
- 如果獲得授權，商家就會運送要求的貨物或提供必要的服務。在請款後，收到金融機構的款項。

在美國，網路銀行交易安全應該受限於和傳統銀行交易相同的法令和規範。這些應用到網路銀行交易的法令引起一些懷疑，如 compliance with advertising requirements and the provision of timely disclosures in an appropriate form. 金融機構亦可能因未符合強制的法令或國家法令而有經營的風險。依交易所發生種類的

不同(譬如：extension of credit or deposit or withdrawal of funds from an account at a financial institution)，以下是應遵守的美國聯邦法令及規範：

- 平等信貸機會法及聯邦規範 B(Equal Credit Opportunity Act and Federal Reserve Regulation B)

  以禁止的基礎，禁止放款交易過程中，借款人行任何型式的歧視。同時要求借款人應在有關的放款條文中提供告知的義務。

- 公平購屋法(Fair Housing Act)

  在禁止的基礎上，禁止對相關購屋借款進行任何型式的的歧視。

- 家庭借貸揭露法及聯邦規範 C(Home Mortgage Disclosure Act and Federal Reserve Regulation C)

  要求存款機構和放貸機構報告放款條件、起源和購買之資料。

- 電子資金移轉法及聯邦規範 E(Electronic Fund Transfer Act and Federal Reserve Regulation E)

  在與客戶帳戶有關的電子資金移轉，金融機構應被要求揭露和客戶保護(如錯誤解決程序和對未授權移轉債務限制)。

- 誠實借貸法及聯邦規範 Z(Truth in Lending Act and Federal Reserve Regulation Z)

  在消費者信用交易，要求 creditors 提供揭露(包括廣告)及消費者保護(如錯誤受理及解決程序)。

為確保一致性的規範政策可應用於網路銀行，應該加強以下的課題：

- 對繼存的廣告要求，可能需要在線上介面中建立適當的 triggers
- 當使用線上揭露、定期報表和通知而非寄送影本之方式較適當時，其標準應先被建立。
- 類似的，以 e-mail 方式取代傳統與客戶溝通方式較佳之評估狀況，應先被指出。
- 對在何種時間框架所提供揭露、財務報表和通知的規則，應該以線上傳輸的方式採用或評估。

柒、網路安全管理

網路安全不是「全有或全無」(whole or none)，安全性是程度上的問題，安全程度愈高面臨的風險愈低。網路安全管理即在現行環境下降低風險，並採用額外的措施，確保當安全意外發生時，可以很快地使系統恢復正常運作。

網路安全管理的四大範疇如下：

一、控制風險

二、動態策略調整設定

三、存取權限隱私權控制

四、可信賴的系統回復與完整詳盡的紀錄

控制風險

藉由風險評估，了解整體網路環境的缺失，其可分為潛在性威脅及顯而易見之危險，顯而易見之危險較易採取修正措施。潛在性威脅則需依賴平日之維護改善。在控制風險中首重整合式防衛功能，不同功能產品，依需求部署，各司其職，共同維護網路系統整體安全。

其主要風險在於下列數個部份：

- 作業系統安全與應用程式安全
  作業系統安全針對系統程式漏洞作修正，應隨時注意是否有新的漏洞產生。新漏洞的產生代表新的攻擊手法開始流行，若未及時防範將嚴重影響系統安全。
  應用程式漏洞也需及時更新，避免因程式漏洞，影響整個系統之安全。如 Win Nt 之漏洞和 Internet Information Server 漏洞，都應盡力尋求解決方案，若更新程式未能即時提供，應考慮是否有其他備援方案。
- 網路安全程式更新與負面表列更新
  包括 Firewall 與 IDS 和 AAA Server 需在有更新修正程式發行時即作更新，其中若需要使用負面表列資料進行比對，應定期更新負面表列資料庫。

動態策略調整設定

將 Firewall & IDS 高度整合，使其對於整個網路安全決策能提供動態性策略調整，及時的回應，迅速有效的阻擋攻勢，協助網路安全決策的執行。

防禦策略的擬定，應視整體網路環境安全變化而調整，並非一成不變，能確實改弦更張即時迅速反應環境之威脅，才是最佳策略，這有賴于詳盡的風險評估以產生明確的決策。

存取權限隱私權控制

網路安全漏洞常來自管理者的不察，而非系統程式或服務程式之臭蟲，因管理者的疏忽使得權限未被詳加規範，致使外落，危及系統資源安全。或因不慎對於程式之使用權限未詳加定義，導致因程式的執行而取得超級使用者權限。這不僅嚴重影響系統安全和侵犯隱私權。

可信賴的系統回復與完整詳盡的紀錄

在詳盡的風險評估，產生明確的決策，完善策略規劃，確實部署網路安全工具後，最需要的是系統回復機制，不論網路設備裝置，系統主機，作業系統本身和資料，都應有對應的備援和回復機制，資料備份絕對是不可缺少之先前條件。完整詳盡的紀錄是最好的蒐證資料，利用記錄檔的判讀可以提供決策者策略之擬定及做為日後司法上的證據。

為達成上述的目標，組織應時常問自己：資訊系統的管理是否取決於組織當前所要面對的且應加強的與科技有關的主要挑戰、課題和問題；是否已適當的組織起來、有合格的人力資源、和適當的控制；是否正確而有效的監理及內部控制已被建立和維護，以確保財務報表和管理資訊系統的完整；是否管理資訊系統已能符合組織決策和報告的需要；是否資訊系統人員已受過持續、恰當和充分的教育訓

練。以下分就管理的三大重要功能組織、計劃、控制等作一說明。

組織圖

組織圖是衡量一個組織是否已有效分工的基準，從圖中我們可對組織各部門的功能作探討，並作為管理之依據。所以當我們規劃好組織後，第一件要問的就是權力範圍和責任歸屬。同時我們也應該要問，監督是否適當和權責的劃分是否明顯。同時更應避免重複的責任，如程式人員又負予電腦操作的責任；使用者部門主管兼管資料中心作業。再者，像臺灣銀行這樣大的組織，必須要有類似指導委員會的組織(steering committee)，定期就有關資訊安全管理有關的議題進行溝通，以增強安全監理的功能。各部門所擁有的獨立系統，亦應納入考量，避免成為網路安全事件可能的死角。對網路銀行交易而言，最核心的部分或是最容易接觸到帳務資料的就是資訊部門。資訊部門內部是否有一安全又能快速應變的組織，也必須在組織圖中展現，以維護網路銀行運作的安全，支應銀行業務的需要。

職位說明(position description)

經由組織內所有相關職位的描述，每個人的應從事的工作內容、職責及從屬關係。當員工想瞭解管理的期望時，職位說明提供一客觀衡量工作績效的工具。對網路安全而言，清楚的職務說明是未來組織執行獎懲的重要依據。譬如：

電腦操作員—根據操作手冊之指令操作電腦之硬體。無論其工作職責範圍為何，操作員的功能均應限制在其所操作設備之手冊內。他們不能設計任何程式或函式庫，且應只有對文件載明所必須執行的程式具有存取權。

通訊支援經理—負責督導區域網路和廣域網路通訊系統的計劃、安裝和測試；負責指揮支援組織通訊資源的專業員工。

安全長—對資訊系統資源及資產之實體及邏輯安全負有責任；進行風險分析以決定電腦資源的暴露值及威脅。

技術支援組員—扮演與電腦製造商、軟體支援人員、應用程式設計員和系統分析師之聯絡員；監督介於程式設計和資訊系統作業間之系統發展；應由具有高階技術知識的系統程式設計人員擔任。

就第一項而言，若系統內發生有操作員存取規定外之程式，則可判定其違反存取規定。同理若未發現硬體安全弱點而發生系統被破壞，則安全長應負有最大的責任。故組織內所有職位均應有一職位說明書，且每一成員均應知曉其所在職位所應負起之責任，以確保組織內所有人員擔負其應有的責任。

計劃

組織管理的第二項重要功能為計劃。計劃隱含有為達成所定目標和策略而為未來預作準備的活動，故資訊系統安全亦必須被整合進管理活動或企業計劃的程序中。為達成組織短期及長期對安全的要求，經常檢視組織所擬定的計劃並作修正是非常重要的事。譬如：由於防火牆技術的精進及網路安全威脅的手法不斷翻新，組織預計一年後更換防火牆系統，除審視短期計劃外，尚應檢視長程的計劃，以符合本行對交易安全的要求。一項好的計劃必定是董事會、高階主管和一般使用者均應涉入。組織制定一項有效的安全計劃時，其程序通常應包括下列數項：

一、發展一項任務

二、評估組織資訊系統和技術

三、評定目前和未來資訊系統所面臨的環境

四、制定目標

五、分配資源

六、分析結果

七、更新計劃

同時組織制定資訊安全計劃時亦考慮應用程式、作業系統程式、硬體、人員和預算。由於組織所面對的競爭、市場的力量和改變中的規範，均會造成組織改變其用來提供予客戶使用的軟體，當在更新這些應用程式時，組織的計劃應將這些改變計入未來安全需求中。同理，由於資訊科技的快速發展，許多現行所使用的作業系統或硬體通常會有很多潛在的漏洞，因此安全計劃亦應將兩者含括進來。組織是由人所組成，再完善的技術，仍不能保障系統完全的安全。因此安全計劃中亦考量人員異動(如新進、調職、離職等)對安全可能的影響，且計劃中亦應納入安全教育訓練。在有限的預算中，計劃亦應評估輕重緩急，以最經濟的方式達成組織對安全的最大期望。

控制

網路安全系統中，控制的發展和建置是在確保所有的工作能精確、及時且完整的處理，同時控制也是組織管理活動中第三項重要的活動。組織為達成其策略常會訂定一些標準和程序，而這些程序通常應包括：允許權責的劃分；限制有價資產的存取；確保所有授權的事項均在資料處理的範圍內；提供有效率及有用的資源配置。程序將使組織的活動被記錄下來成為稽核的足跡，確保使用者部門的獨立控制可被實現。

控制當中一項最重要的方式是內部控制。控制包括帳務資料中心、系統軟體的取得和維護、存取安全性和應用系統的發展和維護。控制也不應限制在任何系統，大至大型主機、小至個人用電腦亦應含括在內。同時控制也應包括電腦程式、作業系統軟體、保留在電腦系統上的程式和資料的存取權。以下是幾個有關控制的內容：

一、管理性控制

(一)、短期和長期計劃

(二)、策略、目標和程序

(三)、組織架構

(四)、權責劃分

(五)、人員訓練

(六)、內部稽核

二、系統發展和設計控制

(一)、系統發展生命週期方法論的運用

(二)、程式變更程序

(三)、系統測試

(四)、存取控制和安全性

三、帳務中心作業控制

(一)、實體安全

(二)、操作程序

(三)、備份和回復程序

(四)、災難應變計劃

(五)、預算、硬體取得計劃和備載容量計劃

為達成控制的目的，組織中從事控制功能的人員常依賴管理報表系統。該系統可衡量組織系統的安全執行績效，同時也是整體控制系統中重要的一步。為方便區分，可將此系統區分為作業、系統發展和程式設計、一般及人員。透過此報表系統可知道譬如由操作者所造成系統當機的意外事故數。透過此報表管理人員方有可能立刻對異常事故或突發事故採取行動，以避免或降低網路安全事故發生所造成的損失。

捌、建議

建議主要放在兩項上：增強本行區域網路及廣域網路(行內全球資訊網)之安全性、並加強本行資訊安全之強度。以下是我們所提出的建議：

一、增強本行區域網路及廣域網路(行內全球資訊網)之安全性

一般而言，內部員工具有較外人為佳的業務知識，同時又最瞭解組織運作和程序，故由內部人員所產生的網路安全事件可說是最危險的。據統計有 80%的安全事故是由內部員工所為，可見增強本行私有區域網路和行內網路之安全性應具有優先性的。況且目前本行網路銀行的許多交易均在內部網路上傳送，更印證其為本行首應重視之事情。各項作法如下：

(一)、機密性

作好資料之分類

這是所有工作中看似最簡單、最容易、但也最會被忽視的一項。資料可區分為高敏感性資料、敏感性資料及開放性資料。至於如何分類，則需依本行業務之需要事先定義。

高敏感性資料加密

如網路安全事故章節所述，攻擊者可用多種方式取得網路交易時所需之資訊。若能事先對內部網路上要儲存和傳送的資料加密，使其取得後亦很難知曉資料之內容。同時對金鑰亦應加密保管，並明定更換的期限。

會在公眾網路上傳送之高敏感性及敏感性資料亦應加密

攻擊者在一般網路上能作的攻擊行為，在專線網路亦可進行。故即使是在專線上傳送之高敏感性及敏感性資料亦應加密。

(二)、存取控制

- 區隔網路以防止資料遭遮攔
- 將支援 LAN 及行內全球資訊網之重要的設備集中於透明的房間以增強實體設備之存取控制
- 限制對伺服主機之操作只能在透明房間內進行
- 組織內網路之連結點應集中於安全的區域
- 建立並維持所有使用者之安全權限是最新狀態
- 不允許控制高風險資料之重要營運邏輯存在桌上型電腦
- 所有重大的營運邏輯應建置在透明房間內之伺服主機內
- 以集中撥入/撥出之數據機進行遠端存取

- 定期"war-dial"所有交換機之電話號碼以偵測未授權之數據機
- 提供桌上型電腦具有自動中止服務的功能
- 報廢電腦之前應從硬碟中移除所有高敏感性和敏感性之資料
- 以密碼保護筆記型電腦並將高敏感性和敏感性之資料加密
- 使用如'one-time password'之強認證(strong authentication)方式存取網路

(三)、密碼政策

- 建立有效的密碼政策

  密碼應有一個最小的長度，並且要包含數字、字母和符號

  系統可定期自動提醒使用者更改密碼

  不可和他人共用密碼、也不可將密碼寫在紙張或筆記中

  不可使用明顯或易猜之密碼
- 傳送和儲存之可再用密碼應加密
- 應記錄密碼歷史，以避免最近使用的密碼又被使用
- 使用商業性的軟體工具測試使用者密碼的合法性
- 一段時間未用之帳戶應暫停使用；長時間未用之帳戶應刪除
- 對多次登入不成功而遭暫停使用之使用者通知系統管理者
- 顯示上次登入成功的日期及時間

(四)、設定控制

- 支援內部網路的伺服器應集中置放於透明房間
- 定期測試伺服器之設定
- 正確設定控制

(五)、安全政策

- 建置一個易於瞭解的資訊安全政策
- 考慮要求所有供應商提供軟體的預設值設成全部拒絕
- 應用程式、作業系統和公用程式應維持最新和最正確的備份
- 要求與服務提供者所簽定的合約應包括安全課題
- 建置一個交換控制機制，以維持對軟體和安全變更機制的控制
- 建立一個災難管理的機制

(五)、網路安全的管理

- 選擇位於咽喉點(critical points)的系統元件(如防火牆)，以記錄使用者、網路和應用程式活動
- 在咽喉點處提供病毒碼掃瞄軟體，且每台網路上的工作站也應安裝
- 要求所有的磁片和光碟片均應檢查病毒
- 利用可信任的第三者評估網路安全
- 安排定期收到安全弱點的通知
- 利用可用在作業系統的安全子系統，以將系統轉成可信賴的系統

(六)、人事

- 限制員工對敏感性資訊之存取權
- 限制顧問人員和員工應有相同的安全檢查和監督程序
- 確保重要技術人員能得到適當訓練，成為一永具專業水準之人員
- 採用可對付'社會工程'(social engineering)的工具
- 鼓勵使用者將網路異常行為帶給系統管理者

(七)、企業永續計劃

- 確使災難備份主機和主要主機有相同的安全水準
- 定期進行演練

二、加強本行網際網路安全之強度

(一)、使用適當的防火牆架構

- 使用防火牆監督位置、隔離網路、監控網路和檢驗訊息流
- 使用多層且不同系統平台之防火牆以防止駭客之入侵
- 在可充分支持業務需求的條件下，將防火牆功能簡單化
- 在可充分支持業務需求的條件下，將伺服主機功能單純化
- 移除防火牆和伺服主機不需要的通信埠

(二)、適當規劃檔案和目錄的存取權限

(三)、使用已作商業應用的應用程式定期探測網路及防火牆的弱點

(四)、對每一種應用，考慮使用不同的伺服代理機(proxy server)

(五)、不允許任何外部使用者用遠程登入服務(Telnet)進入任何重要的網路元件

(六)、只允許對特定地點進行外部遠端登入服務

(七)、與使用者間的溝通，考慮使用公、私鑰加密技術

(八)、對全交易處理(fully transaction processing)服務要求對客戶作強認證(strong authentication)

玖、結論

有效的資訊管理是所有金融服務機構成功和生存的要件，而安全是一種有效資訊管理的整合元素，特別是在今日網路更公開的溝通環境中。因此每一個機構必須評估它所面對的風險，並且也願意接受這些風險，也就是要管理資訊安全之風險。而要管理風險，必須體認到非所有的網路具有相同的弱點、也非所有的系統是相同的重要程度、亦非所有的資料具有相同的敏感性。因此，能參照上述觀點並因應本行業務需要對風險作出區分，是我們維護網路安全的第一步。而訂定有效的資訊管理的基礎必須要有易於瞭解的資訊安全政策，且必須受到董事會及高階管理者的強力支持。網路銀行安全是本行整體資訊安全的一部分，故優先建立一易於瞭解的資訊安全政策是極為重要的事。

不同於美國政府對電子銀行之規範，政府對網路銀行發展的規範也將技術面涵括在內。如銀行公會訂定之（電子銀行業務安控作業基準）明訂因所使用的機制不同，決定其金鑰長度。例如交易類若採 RSA 機制，則金鑰長度訂為至少 512bits。然就資訊技術快速發展之角度而言，訂定金鑰長度是否反而會造成發展電子銀行安全的危機，甚或阻礙電子銀行的發展。因政府實際上很難決定什麼樣的技術才是安全的、適當的；什麼樣的技術才是未來的趨勢。故應放手由各銀行自行決定採用的技術、學習管理風險才是重要的。再者，未來一定會有更多、更好、更方便、更易於應用的技術產生，為金融業務訂定技術規範不但無此需要，反而可能造成銀行發展的障礙。同時，在自由化、國際化的浪潮下，政府對網路銀行安全的技術規範是否有助於台灣金融的國際化，亦有待商榷。

任何規範要能有效的執行，仍要依賴組織中的每一成員確實執行，亦即要能落實在日常的作業中。譬如，駭客可利用自動撥號測試軟體，對組織電話交換機所屬之電話機進行撥號測試，未關機的電腦就會被駭客利用，成為駭客犯罪的跳板。又譬如公司規定所有的磁碟在使用前均應掃毒，疏忽的員工可能未作此項工作，致使病毒透過網路散佈、重要的資料因而損毀，甚或造成公司財務損失及營運停頓。又例如網路管理者設定密碼不當，例如長度太短、只有英文字母或數字，給予有心人可趁之機，掌控設定的權限，未來可輕易的進出，造成不可計數的損害。因此，喚起所有員工的危機意識，並不斷地教育員工提高警覺，是奠定未來成功管理網路安全的基礎。

不論是對內或對外的網路化已是現代企業競爭不可或缺的要項，未網路化的公司肯定無法繼續生存。然而網路化亦為組織帶來一些風險，如何明訂資訊安全的風險、妥適的規劃、施以良好的管理、追蹤改善，是現代企業極大的挑戰。尤其網路環境是錯綜複雜的、網路技術是日新月異的、網路應用是推陳出新的、網路犯罪是變化多端的，為企業經營添加更多的

變數。有鑑於此，如何在組織之最高決策機制中納入可綜觀全局的科技人員，以輔助企業的永續發展，是一刻不容緩、亟待解決的課題。網路安全是企業經營永不能輕忽的重大議題，期待本文能有拋磚引玉之效，使銀行在承擔風險時，亦能維持其良好的信用，給予客戶便利的交易管道，滿足客戶即時理財的需要，並為銀行賺取利潤。

本文於業務之餘從事研究之工作，若有任何疏漏或不足之處，尚祈各界先進、前輩不吝賜教，給予指導。

參考文獻

1. Unix 與 Internet 安全防護-系統篇，原著者 Simson Garfinkel and Gene Spafford，陳志昌、林逸文、蔣大偉譯，O'Reilly 公司出版。
2. 電腦犯罪，原著者 David Icove，Karl Seger & William Vonstorcb，陳永旺編譯，O'Reilly 公司出版。
3. 我愛 WINDOWS NT 網路安全與管理，作者 戴建耘，松崗公司出版。
4. 網路安全：在多重環境下－2000 年版，Dan Blacharski 編著，李正源，簡崑鎰 譯，文魁資訊出版。
5. 精通網路安全技術，作者 孫銘新 邱柏豪，儒林公司出版。
6. 網路安全實用秘笈，編著 宇群數位研究室，文魁資訊出版。
7. 網路安全按步操兵廿，原著 Lincoln D. Stein，和碩公司出版。
8. 密碼學及其應用，作者 賴溪洲。
9. Internet 網路安全手冊，作者 沈文智，碁峰出版社。
10. 駭客現形第二版：網路安全之秘辛與解決方案，Joel Scambray，Stuart McClure，George Kurtz/著、美商麥格羅・希爾（McGraw-Hill）國際出版公司。
11. 電子商務與網路安全，Simson Garfinkel with Gene Spafford，歐萊禮出版。
12. Sound Practices Guidance on Information Security，Federal Reserve Bank of New York，September 1997。
13. Electronic Banking-Safety and Soundness Examination Procedures，Federal Deposit Insurance Corporation Division of Supervision。
14. Mastering Network Security by Chris Brenton ，Sybex Inc.。
15. The Process of Network Security，Thomas A. Wadlow，Addison-Wesley Pub Co.。

Reference Sites

- http://www.w3.org/Security/Faq/www-security-faq.html
- http://www.cs.berkeley.edu/idsg/security/
- http://socrates.berkeley.edu:2001/security/itatf_swg_report.html

Computer Security Advisories

- CERT Advisories(http://www.cert.org)
- Microsoft Patches (http://www.microsoft.com/downloads)
- Sun public patches (http://access1.sun.com)
- Digitial UNIX Patches (http://ftp.digital.com/pub/Digital)
- Linux Redhat Patches (http://redhat.cs.berkley.edu/redhat/local)

Alerts and Announcements

- Solaris snmpXdmid Buffer Overflow Vulnerability (3/21/2001)
- Red Hat Linux rpc.statd vulnerabilty (8/11/2000)
- Virus scanning of departmental e-mail (7/25/2000)
- EECS Computing Security Incidents Report (7/21/2000) (internal access only)
- HP-UX 10.20 Software Distributor vulnerability (7/10/2000)
- Microsoft "scriplet.typelib" vulnerability (5/10/00)
- Loveletter Virus/Worm Security Alert (5/5/00) (updated 5/10/00 with a link to a Eudora advisory)
- Linux Systems Security Alert
- Solaris Systems Attack in Soda (07/06/99)