R94725021 陳俊維, R94725041 林岦毅, R94725054 陳怡孜

Introduction to Network Security

摘要：介紹有關網路攻擊手法、各式防禦技術與實際的案例。

所謂的入侵(incident)是企圖去擾亂安全的政策，像是攻擊一台電腦或是企圖去獲得一些未被授權的權限。由 Figure 1 我們可以發現，從 1988 年的第一隻病毒 – Morris Worm 開始，到 1999 年的 Melissa 病毒，使 E-mail 成為主要的病毒傳播途徑，也讓入侵事件在這一年開始大幅的成長，到 2003 年為止共有 **319,992** 的入侵報告，如 Figure 1 所示，其成長的幅度相當大。(自 2004 年起，CERT/CC 不再發布入侵數量的報告，取而代之的是將攻擊的數目分類到不同的類別中。)

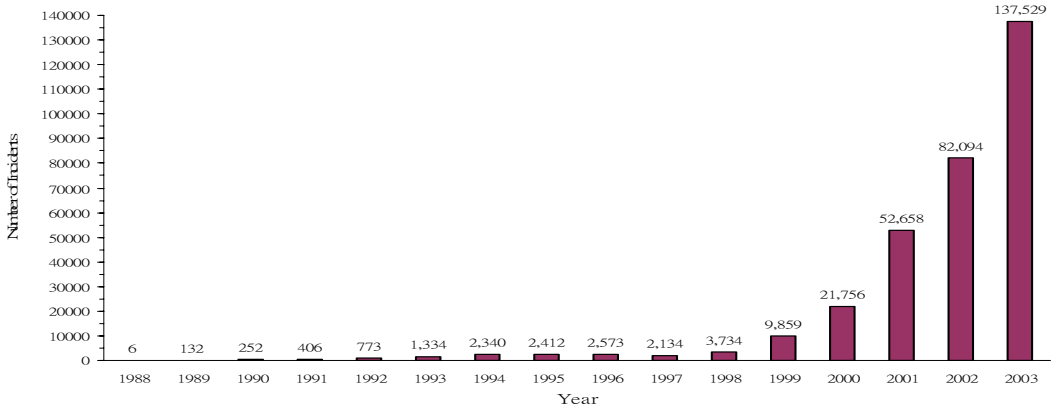

Figure 1. Number of Incidents
Source: http://www.cert.org/stats/cert_stats.html

雖然網路攻擊越來越複雜，但駭客與使用者的技術能力卻持續下降，最主要是因為一些有經驗的駭客，寫了一些攻擊的 Scripts 或 Toolkits，讓一些初學者可以輕易地發動攻擊，並能將攻擊的軌跡隱藏起來，這種刪除或隱藏相關證據的技術也變成是這些 Toolkits 的一部分了。其關係可由 Figure 2 表示之。

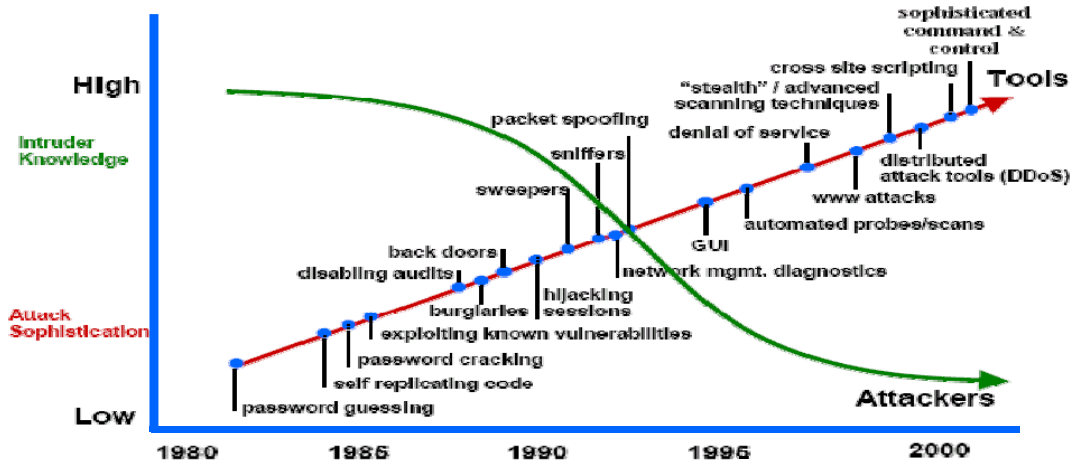

Figure 2. Attack sophistication vs. intruder technical knowledge [10]

1 攻擊手法

1.1 竊聽(Eavesdropping)

- 網路竊聽：
  - 被動式：在傳送方與接收方之間，偷偷的監控與竊聽。
  - 主動式：竄改溝通的頻道，讓兩者無法溝通或是取代其中一方，或是收集網路的架構。
- 隱藏的頻道：偷偷開啟一個未被授權的網路連線，去存取一些未被授權的資料。
- War Walking：利用無線網路移動的特性，攻擊者可以拿著筆記型電腦開著車，或邊走邊收集附近無線網路的資訊。

1.2 阻斷服務攻擊(Denial of Service, DoS)

- TCP DoS 攻擊，主要是由於攻擊主機發送大量的或不正常的 TCP 網路封包，造成被攻擊的目標主機當機、重新啟動，或是目標網段的交通壅塞，以致於該主機無法繼續進行某項服務。主要有三種攻擊途徑：
  - Land 攻擊：利用特殊的 TCP 封包傳送至目標主機，使其因無法判別而當機或被迫重新啟動。當封包的來源和目的主機的 IP 位址和埠號都相同的時候（經過偽造 spoofed 的封包），則會造成主機的損毀，或是當機。Land 攻擊是利用 TCP 通訊協定中，定義規則與作業系統之間漏洞所造成的攻擊手法，而由於與作業系統相關，許多新版本的作業系統（或經過修補 patch 後）都已經免疫於此種攻擊手法。
  - Teardrop 攻擊：在 IP 層中定義的封包分割和重組的規則為：「分割後的封包的大小必須小於傳輸介面的 MTU（maximum transfer unit，最大傳送單位），並且符合以 8 byte 為單位的倍數。」Teardrop 攻擊就是利用這種分割重組間的漏洞而產生的攻擊方式。
  - TCP SYN 攻擊：此種攻擊主要是利用 TCP 連結時的三向交握訊息來造成的。當攻擊者惡意地送出許多 TCP SYN 封包給被攻擊端，而沒有後續連結的封包傳出時，被攻擊端的 SYN queue 會因為儲存太多正在等待連結的資訊而超過其容許量，因而導致暫停服務。
- UDP Flood Dos 攻擊又稱為 Fraggle 攻擊，它是透過 UDP protocol 送出假造來源的 UDP broadcast 封包至目標網路，以產生放大的資料流，目標埠號（port）通常為 7（echo，回應服務）；當目的網域中的眾多主機回應之後，便可以造成網路的壅塞。即使某些 IP 位址沒有回應，但產生的 ICMP 封包仍然可以達到 DoS 攻擊的效果。

- DDoS 就是 2000 年年初時全球知名網站攻擊事件的主角。它是利用許多分散在世界各處的 DoS agent（攻擊代理人，或稱執行者），在某一時刻點對特定目標主機以前述各種攻擊手法的混和方式，將大量封包傳入目標網域，以阻絕被攻擊者的服務功能。其手法特別之處是必須先選定一定數目的主機，入侵並植入其 DDoS agent 程式，並在攻擊發起時遠端操控它們的行為。
- ICMP（Internet Control Message Protocol）是 TCP/IP 通訊協定中定義封包的一種，主要功能是用來在網路上傳遞一些簡單的控制訊號。在大部分的作業系統中都會提供"Ping"這個常見的系統指令；其功能為測試自身主機與某特定目標間連線是否暢通，這是典型的 ICMP 應用。它的工作原理是利用發出 ICMP 的 Echo Request 給對方主機，當對方收到這個 request 封包後，IP 層會發出一個中斷訊號給作業系統，請系統回送一個 Echo Reply。當原系統接收了這個回應之後，同樣的 IP 層會中斷作業系統，並由作業系統將此回應訊息傳達給每一個曾經在系統中發出 ICMP Echo Request 的行程。ICMP DoS 攻擊主要有以下兩種手法：

- **Ping of Death**：ICMP Echo Request/Reply 的封包格式包括 Option Data 這一部分，雖然其內容可有可無，但是當 Echo Request 包含此部分資料時，接收端必須將這些資料原封不動的包含在 Echo Reply 中回送給發送端。由於 Option Data 的大小並非固定，因此形成了有心人士用來破壞系統的安全漏洞。當超過大小限制的封包送入被攻擊的主機時，由於作業系統本身無法處理這種變形封包，因此會造成當機的狀況。由於這是作業系統中對於 ICMP 處理的漏洞，因此部分的新版作業系統都已經針對這個問題作了修復。
- **Smurf 攻擊**：這是目前為止最為可怕的一種的 DoS 攻擊，因為它可以在極短的時間內造成非常龐大的資料流，不但造成攻擊目標的暫停服務，並且會使目標所在的網段壅塞，造成網路交通癱瘓。在 TCP/IP 對網路定址的定義中，攻擊者可透過所謂的廣播位址，並假冒目標主機(受害者)將封包傳送到網路上，而所有連接此網路的網路卡都會將此封包接收進主機中，對此封包進行回應或處理。如此一來，所有的 ICMP 封包在極短的時間內湧入目標主機內，不但造成網路壅塞，更會使目標主機因為無法反應如此多的系統 interrupt 而導致當機、暫停服務。除此之外，如果一連串的 ICMP broadcast 封包流被送進目標網域內的話，將會造成網路交通長時間的極度壅塞，使該網域上的電腦（包括中介者 router）都成為攻擊的受害者。

1.3 擷取連線攻擊(Session Hijacking Attacks)

- IP Spoofing Attacks: IP Spoofing 可以利用去改變 IP packet 的 source address，來讓接收到這個封包的人根本不知道是誰傳送過來的，也可讓系統以為它正在跟自己知道的人做溝通。

- LANMAN (LAN Manager)的缺點：密碼只能有 14 個字元、不足 14 個字元會以空白補完、小寫字母會被轉成大寫字母，以及 14 個字元會被切割成兩組 7 字元的片段，因此更容易遭到破解。
- TCP Sequence Number Attacks: 攻擊者可以將惡意的程式碼利用猜測 TCP Sequence number，塞在一大群封包之中。
- DNS 下毒(DNS Poisoning): 攻擊者可以利用 DNS 散佈不正確的攻擊目標 IP Address，讓封包沒辦法傳到要傳的目的地。

1.4 片段攻擊(Fragmentation Attacks)

將封包用各種 IP 的資料碎片來掩飾惡意的內容，繞過攻擊目標的過濾封包設備。其主要有兩種方式如下：

- Tiny fragment attack：將惡意的訊息拆成幾個沒有意義的 IP fragments，當 IP fragments 穿過攻擊目標的過濾器後，就再次組合成為具有攻擊意圖的訊息。
- Overlapping fragment attack：讓第二個 IP fragment 在穿過過濾設備後，去覆蓋掉第一個 IP fragment 的 Destination address，將它改成要攻擊的目標。

1.5 撥號攻擊(Dial-Up Attacks)

- War dialing：測試大量的電話號碼，檢查是否有連結數據機，接著利用這些數據機所具有已知的漏洞來做攻擊。
- Demon dialing：針對一台數據機，用暴力法來猜這台數據機的密碼，以獲得存取使用的能力。

1.6 惡意程式(Malicious Code)

- 病毒(Viruses):
  - 病毒以下面兩種方式感染作業系統：
    - 完全取代一個或多個系統程式。
    - 將自己附加在系統程式上，並修改系統程式的一些功能。
  - 病毒生命週期
    - 複製期：躲藏起來，並且不妨礙系統的運作。
    - 活躍期：逐漸的或是突然的將系統毀掉。
- 巨集病毒(Macro Viruses):巨集病毒會將自己附加在應用程式起始執行的位置，因此當應用程式執行時，病毒的指令會在應用程式取得電腦控制權前先被執行。
- 多構式病毒/自我變種病毒(Polymorphic Viruses):每次感染後，病毒的外觀就會改變，因此也較難被偵測出來。

- 隱形病毒(Stealth Viruses):將自己隱藏起來，不讓他人 (作業系統或防毒軟體)發現，並能隱藏對檔案內容與時間的改變、隱藏感染檔案所改變的檔案大小或利用加密來躲過防毒機制的偵測，跟多構式病毒一樣很難被偵測出來。
- 特洛伊木馬(Trojan Horses):

• 特洛伊木馬是在看似有用的程式之內，暗藏入惡意程式碼，特洛伊木馬就是那個包在外面，看似有用的軟體或圖片檔；而特洛伊木馬不會自我複製，因此不算是病毒。
• 病毒、蠕蟲、或是其他的惡意程式都可以被特洛伊木馬包在裡面。當你執行特洛伊木馬時，他可能會將你的電腦開一個後門，或是開啟一個較大數字的連接埠(port)來允許對這個電腦存取，可以進行資料的竊取或破壞。

- 邏輯炸彈(Logic Bombs):存在應用程式中的惡意程式碼，但它並不會立即對程式或系統有影響，而是當某些事件發生時，才會驅動這個程式。
- 蠕蟲(Worms):蠕蟲並不像其他的病毒一樣，它並不會將自己依附在一個主程式中。蠕蟲攻擊一個網路時，就是在這個網路中亂竄，具有自我複製的能力，透過網路從一個電腦傳到下一個電腦。當這台電腦被蠕蟲滲透，它會將改變資料，甚至是把資料毀掉。

2 防禦科技

上一個章節提及各式各樣的攻擊手法與各種惡意程式，而身為一個系統管理者或防禦者又要如何去因應這種不斷進步、複雜並帶有極大破壞的攻擊呢？以下概略介紹各類防禦技術，說明如何防禦攻擊者的攻擊。

2.1 基礎防禦技術

為了網路安全的需求，因此發展出許多資訊安全相關技術，像是防毒軟體、防火牆、入侵偵測系統等等，以下分別概略說明各個科技的作用。

- 防毒軟體 (Anti-Virus Software)：它主要針對「檔案」的掃描，可協助保護電腦，使其免於受到會讓電腦出現問題的多數病毒、蠕蟲、木馬程式和其他有害入侵者的傷害。病毒、蠕蟲之類的入侵者通常會執行惡意的動作，如刪除檔案、存取個人資料，或使用您的電腦攻擊其他電腦等 [1]。
- 防火牆 (Firewall)：防火牆是一套軟體或硬體，主要監控「程式與服務」對網路存取的控制，可協助阻擋試圖透過網際網路進入駭客、病毒和蠕蟲。部分防火牆也能有助於防範他人在我們不知情的情況下，使用我們的電腦攻擊其他人。因此，無論使用撥接數據機、纜線數據機或數位用戶迴路 (DSL 或 ADSL) 連接上網際網路，使用防火牆都是非常重要 [2] [5]。
- 入侵偵測/預防系統 (Intrusion Detection/Prevention System, IDS/IPS)：入侵偵測系統針對經過的網路「封包」分析偵測或攔截，可以快速的偵測到入侵，

除了可以確認入侵者，更可以在入侵者危及系統之前將入侵者逐出系統。而就算無法在第一時間偵測到入侵者，越快偵測到非法入侵，就越能降低系統所招受的損失，並且也能越快的復原系統。此外，有效的入侵偵測也是嚇阻入侵的力量，經常也能收到阻止入侵的效果 [3] [5]。

2.2 實作方式

上一小節所提及的防禦技術，在實現方式上大致分為兩種，一種是利用知識庫比對的 Knowledge-Based (又稱 Signature-Based)，另一種是依據異常行為判斷的 Behavior-Based [4]。

- Knowledge-Based：Knowledge-Based 的防禦技術，主要是將之前遇過的攻擊與系統的弱點利用資料庫存起來，形成一個龐大的知識庫。當發生一些可能是攻擊的動作時，就去知識庫中比對，看是否有符合的特徵值，其優缺點如下。

  優點：

  - 誤報率低，不會把正常的封包檔掉。
  - 因為所有攻擊警報都以知識庫的資料為依據，因此可以對這些攻擊的資料做更完整清楚有規則的描述。

  缺點：

  - 資訊密集，因為這種防禦技術取決於知識庫的資料量多寡，攻擊的資料越多，相對而言就能發現並抵擋更多的攻擊發生。
  - 只有知識庫存有的攻擊資料，防禦設備才能發現，因此對一些新的，或是專門針對某人的攻擊，就不能發現。

- Behavior-Based：Behavior-Based 的防禦技術，管理者必須先對這套系統設定一些規則，告訴他什麼是正常的行為，然後該設備再對電腦執行的活動做判斷，發現跟平常的行為不同時就發出警訊給管理者，其優缺點如下。

  優點：

  - 可以偵測出一些新的、獨特的攻擊方式。
  - 權限遭到濫用也可以偵測出來，例如平常明明就不會將資料傳遞出去，現今卻有向外的資料流，就可發出警示。

  缺點：

  - 誤判率較高，會把正常的封包判斷為不正常檔掉，就是所謂的 False Positive。
  - 使用者的行為並不是那麼的固定，有時候可能必須傳遞一些較龐大的檔案，像是實驗模擬結果，此時 Behavior-Based 的防禦設備就很可能將他擋下來。
  - 因為此類型的防禦設備需要時間去分析判斷，因此當該設備發覺一個攻擊的時候，該攻擊行為可能已經完成。

2.3 入侵偵測系統(Intrusion Detection System, IDS)與入侵預防系統(Intrusion Prevention System, IPS)之比較

IDS 與 IPS 都是作為檢查封包的網路安全設備，在資訊安全領域各有兩大陣營各自為入侵偵測系統與入侵預防系統熟優熟劣爭執不下，究竟兩者有何不同，各有什麼優缺點呢？

- 入侵偵測系統：IDS 就像是大樓的保全攝影機一樣，保全攝影機雖然可拍下不法活動，但之後還是要靠人力才有辦法阻止入侵者。IDS 裝置的功能相當類似如此，他們從旁監視封包的活動，若有可疑行徑，他們就會發出警訊，接下來就看安全管理者出面檢視這些警訊，決定下一步的行動 [5]。
- 入侵預防系統：IPS 就像是安全檢查哨，封包必需經過 IPS 嚴格的審訊才能通過到達目的地，但只要有任何違反協定或內含惡意程式的封包都會被擋掉。為了執行這樣的任務，IPS 裝置在安全基礎設施中扮演了相當活躍的角色，跟路由器(Router)與交換器(Switch)一樣平起平坐地決定封包的動向。

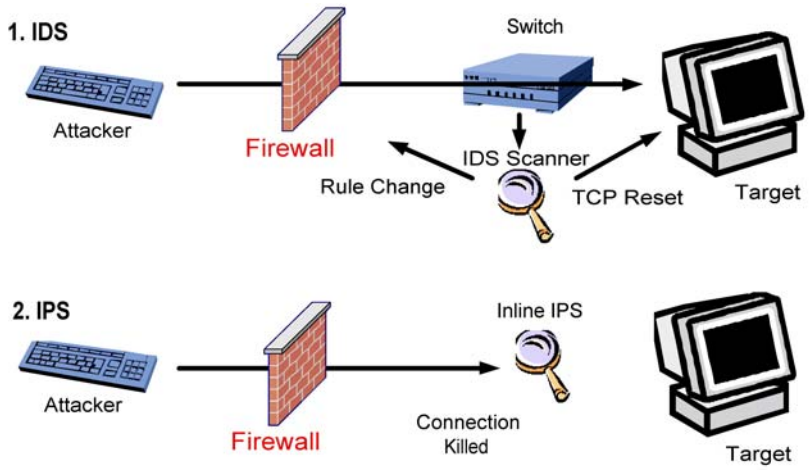

Figure 3. IDS vs. IPS

如上圖 Figure 3，IDS 會從交換器掃描埠(Span port)連出來，稱為 Off-line Mode，而 IPS 是直接從防火牆連出來，也就是所謂的 In-line Mode。IPS 支持者認為現今的威脅必需立刻處理，而 IDS 太過被動，來不及檔下攻擊事件。他們也認為 IDS 動輒送出上千個誤判的警示，使得 IT 安全人員疲於奔命。而 IDS 擁護者認為 IPS 裝置會拖慢網路速度，成為最容易故障的地方，或把合法的流量都攔了下來。當封包數目過量時，IDS 會因此而失去作用，但封包仍然可以正常流過，而 IPS 因為在同一條線上，因此當他失去作用時，封包也會被直接丟棄。

其實現今的 IPS 系統都建立在高速元件上，足堪趕得上任何網路的速度，同時，系統也必需調校過才能確保不法程式會被擋下，而合法流量可安全通過。IDS 與 IPS 裝置一同聯手的效果最好，IPS 裝置負責攔阻已知惡意程式碼，IDS 則專門監看即時與歷史安全事件，同時部署 IDS 與 IPS 裝置才能提供最高層級的安全保護。

2.4 威脅與弱點的管理

防禦技術不停的演進，各種安全設備不停的開發，但是該如何在有限的預算中取決，且如何衡量投資在資訊安全設備所得到的成效呢？

- 木桶理論 – 最短的木板

一個由許多塊長短不同的木板箍成的木桶，決定其容水量大小的並非是其中最長的那塊木板或全部木板長度的平均值，而是取決於其中最短的那塊木板。在資訊安全中，認為資訊安全的防護強度取決於其中最為薄弱的一環，因此出現的一個狀況是發現哪個安全問題嚴重就買什麼樣的產品，這其實只是治標不治本的方法。

- 新木桶理論 – 木桶底板 與 縫隙

實際上，我們可以看到一個木桶能不能容水，容多少水，除了看最短木板之外，還要看一些關鍵資訊：這個木桶是否有堅實的底板，木板之間是否有縫隙。大家不太重視的底板，卻決定這只木桶能不能裝水，能裝多大重量的水。這只底板正是資訊安全的基礎，即企業的資訊安全架構（Information Security Architecture）、制度建設和流程管理。木桶能否有效地容水，除了需要堅實的底板外，還取決於木板之間的縫隙。對於一個安全防護體系而言，其不同產品之間的協作和連動有如木板之間的縫隙，安全產品之間的不協同工作，將致使木桶不能容納一滴水。因此將各式安全設備做整合管理，才能有效防護資訊的安全 [8]。

- 風險管理 – 風險評鑑(Risk Assessment)與風險處理(Risk Treatment)

由上面兩個理論我們知道資訊安全中重要的環節與弱點在何處，但究竟該不該投資預算在上面，或是該投資多少，或是如何衡量投資在資訊安全設備所得到的成效？利用風險管理的技巧能讓我們有效的衡量成效。

何謂風險？風險是「威脅」運用「弱點」針對「資產」造成「影響」的「可能性」，因此我們先利用風險評鑑來分析與評估資產的價值與各式威脅和弱點，再透過風險處理來決定針對該資產的防護機制。另用這種評估的方式，可以有效衡量是否投資預算在該資產，且可分析達成的成效如何。

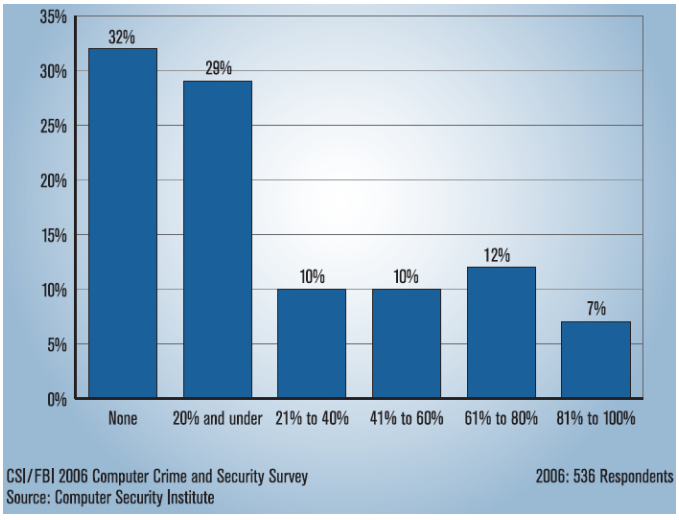

Figure 4. Insider Threat [6]

除了以上的資訊科技之外，其實「人」才是資訊外洩的主因，不論是電腦失竊導致的資料外洩，或是病毒、蠕蟲產生的資訊缺口，幾乎都與人為脫不了關係。根據 CSI/FBI 針對 2006 年的調查 Computer Crime and Security Survey [6] 在左圖 Figure 4 中顯示，32%回應的企業認為內部威脅跟企業損失無關，29%認為因為

內部人員的關係所造成的損失佔公司總損失的 20%之內，剩下的 39%認為內部人員所造成的損失最少有 20%，其中有 7% 甚至認為公司損失的 80%都是內部人員所造成的。雖然大部分的企業並沒有真正計算內部人員對公司造成的資安損失，但回應企業中的有一大部分認為內部人員仍然須對公司的損失負一部分的責任。因此對於人員的資訊安全意識的訓練、網路使用習慣的教導、內部與外部的安全稽核、滲透測試等等，都是改善內部威脅有效的做法 [6] [7] [9]。

3 資安實務

早期，所有的資安管理流程都是仰賴人力的處理，必須由值班人員主動監控所有的訊息（如：網路、營運主機設備、資安設備等），在由人工紀錄下來。當事件發生的時候，透過電話或是電子郵件來通知負責人員，負責人員處理完流程之後在電話告知監控人員，但是這樣的流程往往有 時效上的問題，並且難以追蹤處理後續的問題。

Figure 5. 資訊安全示意圖

於是現在的資安管理，更希望能夠利用現有的人才、科技與制度，達到安全有品質的服務，讓整個系統更具機密性及完整性，如 Figure 5 所示。因此，目前資安管理逐漸轉向了有統一整合的系統，由中央來負責監控處理所有的事件，達到即時反應的優點，以下將以三個案例作分享：

3.1 日月光半導體股份有限公司

在台灣部分企業 E 化才剛起步的同時，四月光已經體認出資訊 E 化潛藏的風險，面對環境的變化，高階主管們開始有這樣的警覺，因此開始打造屬於一套日月光專有的 ISMS(Information Security Management System 資訊安全管理系統)。

- **資訊風險和弱點評估**：利用 ISMS 整理出重建系統或是檔案損毀的經驗，逐步整理出穩定的經驗流程及 SOP(Standard of Process)，利用系統的設備，如：Firewall 或是 IDS/IPS 等，利用其統計資料建構圖表等分析，瞭解系統風險所在，並且定期作風險評估，瞭解隱藏的異常行為，達到「預防勝於治療」的效果。

- **備份及恢復機制：**儘管系統穩定，但是能有小疏失造成系統停機或是遺失的問題，所以確認這系統的重要性，分別對各系統定期作備份，謹慎的選擇適合的規劃，並且訂及作演練。
- **控管機制：**針對所有的人員分別有不同的權限，不僅對人原有所管控，帳號密碼也定期更新，不同機房、機櫃達到獨立，並且設立門禁制度。

3.2 關貿網路股份有限公司

關貿網路資訊安全監控中心(SOC)提供 365X24 全年無休的「資訊安全監控服務」。防護的範圍涵蓋了對入侵攻擊事件的即時監控、線上緊急應變處理及長期網路威脅分析與防範建議。協助企業面對日益嚴重的網路安全威脅，即時監控網路入侵、攻擊、電腦病毒、蠕蟲、網路釣魚和間諜軟體等威脅事件，適時的進行事件應變處理，並提供安全事件處置狀況及統計報表，讓企業處於高度安全的網路防護環境，免除資訊安全威脅的後顧之憂，安心致力於本身業務的開拓與發展，提昇企業整體的競爭力，如圖 Figure 6。

Figure 6. 關貿病毒防護之業務

Source: http://www.tradevan.com.tw/web/guest/IndexIndex

例行業務:

- **365 x 24 全天候資安事件監控：**主動監控是否有違反安全政策的非法存取行為、網路濫用或誤用的狀況並即時掌握網路型病毒(蠕蟲)及高風險攻擊事件。
- **資安事件通報：**發現並確認為可疑的網路活動(事件)時，於時效內通知客戶的安全事件聯絡人員，並提供全中文的事件說明及建議解決方案。
- **主動式防護政策調整：**經偵測並判別為重大資安事件，且需要進行緊急處理時，可於客戶同意後隨即協助調整客戶端防護設備，將威脅阻擋在外。
- **中文預警資訊服務：**即時掌握來自全球網路之風險狀態與最新安全資訊，透過電子郵件主動傳送中文預警資訊。
- **中文化資安事件管理系統：**提供全中文的 Web 介面，可查詢客戶個別資訊資產相關事件及弱點資料庫，並產生圖形化報表。
- **中文月/季定期事件報表：**依攻擊來源、攻擊目標、攻擊事件等進行長期性資安事件的統計分析，並每月統計資安事件，產生通報及處理記錄報表。

3.3 台北縣政府

一般傳統的印象，公家政府管理單位，總是以不變應萬變，但是在資訊安全方面，台北縣政府利用有限的人力和經費，卻也有效的達成了既定目標，台北縣政府採取集中式的資訊管理策略，由於資源整合，所以近幾年來台北縣政府行政電腦化作業，如何因應各項資訊安全威脅與挑戰，在龐大的資訊設備與管理，成為各機換資訊能量的縣政府資訊中心。以下分別探討台北市政府在各面向的成果。

例行業務

- **集中式網路管理：**台北縣行政資訊網路以 GSN VPN 為基礎（政府網際服務網）連結線屬各雞歡為內部網路，以縣府的資訊中心作為連接網路的單一窗口，無論是機關同仁上網，或是民眾要連接各機關網路都要透過縣府資訊中心，因此各項網路安全設施，不需各機關個別設置，只需著重於資訊安全中心，相對節省大量設備及管理成本。
- **主機監控設備：**由於縣府資訊中心納管的主機數量已超過 340 台，要是要逐台檢查機器設備，勢必耗時耗力，因此必須借重自動化 IP 管理工具，風能達到有效管裡的目的。
- **實體機房防護：**因為台北縣政府有新的大樓興建，所以可以在沒有包袱情形下，打造專業的電**腦機房，透過電力系統、門禁系統、消防系統等集中管理所有設備。**
- **使用者權限管理：**統一規劃電腦帳號命名原則，並且定期更改密碼，以及管理帳號，避免幽靈帳號或是重複帳號的出現。
- **資料備份異地備援工作交付委外：**由於集中管裡的方式，所以要是資訊中心遭遇重大事變，很有可能造成縣政中斷，所以委外以專業的廠商提供資料備份異地備援工作。
- **防毒反駭併入委外：**由委外的場昌提供必要的軟硬體設施，以及維運人力完成全縣之電腦病毒防禦及監控。

參考資料

[1] “防毒軟體常見問題集,” http://www.microsoft.atat.at/taiwan/security/protect/antivirus.asp

[2] “網際網路防火牆常見問題集,” http://www.microsoft.com/taiwan/security/protect/firewall.asp

[3] 賴榮樞, “入侵偵測,” 企業資安防護的重要觀念, Oct. 2005

[4] Ronald L. Krutz and Russell Dean Vines, “Telecommunication and Network Security,” The CISSP Prep Guide 2E. - Mastering the CISSP and ISSEP Exams, pp.80 – 150 and pp.166 – 192, 2nd Edit, 31 Dec.2004, John Wiley & Sons, Inc.

[5] 賴溪松, “防火牆技術與實驗操作,” and “入侵偵測系統之觀念與實驗操作,” 資通安全專輯十四 -網路攻防實驗教材, pp.57 – 145, Jun. 2005, 財團法人國家實驗研究院科技政策研究與資訊中心

[6] Lawrence A. Gordon, Martin P. Loeb, William Lucyshyn, and Robert Richardson, “CSI/FBI Computer Crime and Security Survey,” 2006

[7] 林信良, “員工上網行為管理必修四堂課,” 網管人 NetAdmin, No.5, pp.26 – 43, Jun. 2006

[8] 林信良, “整合資安閘道設備必修四堂課,” 網管人 NetAdmin, No.6, pp.24 – 42, Jul. 2006

[9] 編輯部, “2006 資安事件回顧系列 – 資安認知教育與用戶防禦已是當務之急,” 資安人 Information Security, No.37, pp.20 – 25, Dec. 2006

[10] Simon Hansman and Ray Hunt, “A taxonomy of network and computer attacks,” Computers & Security, pp. 31 – 43, (24), 2005

[11] 吳家名 and 林矗宏,“日月光資安+稽核+人事三位一體具體落實,” 資安兵法・部署二 OO 六, pp. 18 – 23, 紐奧良文化

[12] 高永煌, “台北縣資訊集中・效率、資安兩相得,” 資安兵法・部署二 OO 六, pp. 38 – 45, 紐奧良文化

[13] 王婉伶, “關貿網路導入 SOC 平台・簡化資安管理,” 資安兵法・部署二 OO 六, pp. 46 – 50, 紐奧良文化