# 資訊安全你和我

資訊室/翁孝悌

資訊設備日益普及，價格越來越便宜及親和，企業或個人可以買到價優質精的產品來提高企業或個人的需求與效率。然在享受各項設備便捷、快速之下，另一項重要的課題”資訊安全“已悄悄的來到。資料愈重要，資訊安全就越重要，因為如網頁竄改、植入木馬程式、Dos 及 DDos、隱碼程式攻擊等問題都可能導致企業生存危機或個人財產損失。

本院於 95 年 10 月開始導入資訊安全，從資安政策制定、公告，資訊安全政策宣導、到分體系依序推動，總院長兼任資訊安全長，再再都顯示醫院對資訊安全導入的重視。然資訊安全的導入無可避免的必需要添購一些硬體配備，但絕非花錢買安全，因為「資訊安全」導入的成功與否，除了基本的硬體設備來防止駭客的入侵擷取資料外，最重要的一點還是醫院全體同仁「資安觀念」的落實。

在這次資安硬體的購置方面，本院即針對本身的環境及重要性共列出六大項硬體購置：

第一：防火牆(Internal Firewall)：類似本院的大門警衛一樣，所有出入的人都必須透過此門，可以阻擋一些企圖不明人士入侵。

設備特色：

1. 採用在線式(In-Line)即時分析模式,能主動防護流量異常和通訊協定異常之狀況，並能偵測後門、IP 偽裝、DoS/DDos 等安全威脅，並加以阻絕。
2. 能阻擋 P2P 軟體、網址或關鍵字過濾、即時訊息(MSN)軟體。
3. 圖形化報表系統，能彙整進出閘道之網路流量、入侵攻擊警訊及排行榜等,以便制訂網路管理策略並修正本院資訊安全政策。

第二：病毒暨垃圾郵件過濾設備(Virus/Spam Filter)：病毒及 SPAM 為本次資安設備購置的重點項目，在目前本院最普遍的資訊安

全問題，以病毒攻擊最為嚴重，然大多數的病毒可能來自於人為的收信動作，並在不知不覺中開啟信件導致病毒入侵。

設備特色：

1. 垃圾郵件過濾技術：具備黑/白名單、RBL/DNS 反查、行為特徵過濾、自動學習過濾、貝氏演算法過濾、關鍵字過濾、Sender ID、Domain Key、浮動 IP/寄件人/收件人身分辨識、主旨/副檔名/檔案大小限制攔截等。
2. 具備統計報表功能，彙整病毒偵測警訊與垃圾郵件統計，以便調整系統敏感度。

第三：網站入侵偵測與防禦設備(DMZ IDP)：本院網頁主機、院內網站主機因作業需要，必須要開放讓外部能夠連接到此台電腦，但也因此容易被駭客入侵或植入木馬程式。

設備特色：

1. 能夠針對使用者上網收信不透過 Outlook 收信，當信件中有病毒時能夠及時攔阻，並防止網路釣魚攻擊，適當調整其防禦敏感度。

第四：網路流量監控伺服器(NetFlow Server)：網路監控最主要的目的是監控對外網路流量，是否有某台電腦持續不斷佔用頻寬，影響本院正常運作。

設備特色：

1. 能監控大里院區(Cisco 6509、6506)核心交換器 NetFlow 模組之網路流量，蒐集網路封包活動情況，並能針對網路型病毒等攻擊行為之異常流量有效進行管制。
2. 能即時顯示目前或指定網段之網路使用情況。

第五：Windows 系統修補伺服器(Windows Server Update Service)：因本院電腦之作業系統以 Window 為主，必須定期更新作業系統 Patch，但因每台電腦業務性質不同，並非所有電腦均能夠上

網；此一伺服器即是讓大家不需要上網就能透過內部連接至此伺服器將自己的作業系統漏洞修補起來。

設備特色：

1. 用戶端更新統一由本伺服器派送部署，不經由 Internet，故不影響 Internet 頻寬。
2. 提供用戶端更新及未更新狀態清單，以便掌握系統漏洞修補狀況。

第六：防毒軟體：分為 Client 端、Server 端，將本院所有電腦防毒軟體版本統一，並且透過統一更新機制上網同步更新病毒碼及掃毒引擎。

設備特色：

1. 採中央集中管理，病毒碼、控制設定及特徵資料庫等均由中央主控伺服器統一派送更新，用戶端不經由 Internet，故不影響 Internet 頻寬。
2. 中央主控伺服器能監視所有用戶端病毒碼更新狀況、中毒警示與統計圖表。

前段有提到，資訊安全並非花錢買安全，最重要的是資安政策面的落實。各企業組織的資安政策不盡然相同，因為每個組織的大環境一定不同，把資訊安全想像是一個恆溫器，沒有一個恆溫器是一樣的；但也沒有一個恆溫器是一成不變的，因為大環境會改變。本院資安政策中就提到必須定期來檢視目前資安政策是否符合本身需求，且須定期開會做修正，並經總院長公告後實施。

人為觀念的改變，就是資訊安全推動成功一半以上，以最簡單的個人系統帳號及密碼來說，「定期變更密碼、加強密碼長度以及加強密碼複雜性的觀念是沒有那麼容易被接受的」，若這點行為觀念能被大家所接受，我相信資訊安全觀念的落實應該沒有什麼困難的。