

學校資訊科技保安管理 分區研討會

- 簡介管理學校資訊科技保安的理念
- 管理學校資訊科技保安的經驗分享

教育統籌局，2003年

「管理學校資訊科技保安」 參考文件

- 資訊科技保安政策及準則
- 制訂校本資訊科技保安政策
- 保護學校電腦系統免受一些自然或人為造成的損害。

其他有關的參考文件

- Windows 2000 Technical Guidelines for School Network Implementation 學校區域網絡實施技術指引-視窗2000版 (只有英文版)
- Technical Guidelines for School Network Implementation 學校區域網絡實施技術指引
- IT Security in Schools 學校資訊科技保安指引 (只有英文版)
- Understanding Internet Gateway 認識互聯網網間連接器 (只有英文版)
- Server Hacking 伺服器的剽竊 (只有英文版)
- Remote Access - Virtual Private Network 遠程存取 - 虛擬專用網絡 (只有英文版)

甚麼是資訊科技保安？

- 『資訊保安』指保護資訊的各個範疇
- 可分為三類
 - 保密性(Confidentiality)
 - 對資訊確保免受未獲授權人士讀取
 - 完整性(Integrity)
 - 對資訊確保免遭未獲授權人士擅自更改
 - 可用性(Availability)
 - 獲授權人士提出要求時，資訊可供使用的情況。

- 『資訊科技保安』一詞並沒有正式的定義，但一般指對任何資訊科技(IT)資訊及資源的保密性、完整性和可用性所作出的保護。

- 資訊科技**保安**就是一種防止與偵測未經授權而使用你的電腦的程序
- 事前的檢測動作幫助你發現及停止未經授權使用者（入侵者）對電腦系統的使用：幫助你瞭解是否有人企圖入侵你的電腦，及他們對你做了什麼。

家用電腦的情況

- 家用電腦內的資料，包括
 - 私人資料，如信件、銀行、投資、購物或透過E-mail與人聯絡的記錄
 - 工作有關的資料，如教學筆記、考試卷、學生成績
 - 其他

家用者電腦安全風險

- 不會讓陌生人任意的去閱讀你的文件
- 將你在電腦上的工作保持隱密
- 確認你的投資、發email給你的親人及朋友時，保證你所輸入電腦的資訊在下次需要它時完整無誤。

誰想要入侵我的家用電腦？

- 病毒或其他一些惡意性的程式碼
- 入侵者（hackers、attackers、crackers）
 - 通常是把對方當作跳板，目的是獲得你電腦的控制權，並用之以攻擊入侵其他人的系統
- 意外事故與其他風險
 - 磁碟錯誤、電源故障、實體偷竊（physical theft）

入侵家用電腦

- 電腦軟件中的新漏洞
 - － 系統管理員若時時更新、安裝修補程式，並正確的設定電腦軟體，入侵事件將得以被預防
- 對你電腦惡意的濫用
 - － 特洛伊木馬程式、後門程式與遠端管理者程式、拒絕服務（Denial of Service）、成爲另一個入侵的跳板媒介
- 寬頻服務與撥號上網服務

撥號上網服務

- 撥號上網：當有需要用網絡時才連接上網，通常連接到互聯網服務供應商（ISP）的數據機，去獲得一個被分配的動態IP地址。每一次撥接的IP地址並不會重複，所以入侵者較難（並非不可能，只是較困難）利用系統網絡服務中的漏洞去取得你電腦的控制權。

寬頻服務

- 寬頻服務：一直保持連接的。當有資料需要傳遞，服務並不需經過撥接設定，家用電腦透過網絡卡一直保持連線，等待傳輸資料或接收資料，所以IP地址就很少改變，容易成爲有心人的攻擊目標。

寬頻與撥號上網的比較

	寬頻	撥號
連線型態	永遠連線	撥號上網
IP 位址	靜態或極少改變	每次撥接皆改變
連線速度的比較	快	慢
遠端控制的功能	電腦總是開啓，所以在任何時間都能控制	電腦必須連上網才有機會
ISP提供的安全機制	極少甚至沒有？	極少甚至沒有

家用者採取的安全措施

- 使用防毒軟件
- 不要任意開啓未知的E-mail附件
- 不要執行未知來源的程式
- 保持軟體更新修正檔
- 對重要的資料進行備份
- 不用電腦或不連上網時關閉電腦
- 使用密碼/防火牆

學校內的情況

- 個人
- 學校整體

學校內個人的情況

- 使用密碼
- 使用防毒軟件
- 不要任意開啓未知的E-mail附件
- 不要執行未知來源的程式
- 保持軟體更新修正檔
- 不用電腦或不連上網時關閉電腦
- 對重要的資料進行備份

學校整體上的資訊科技保安

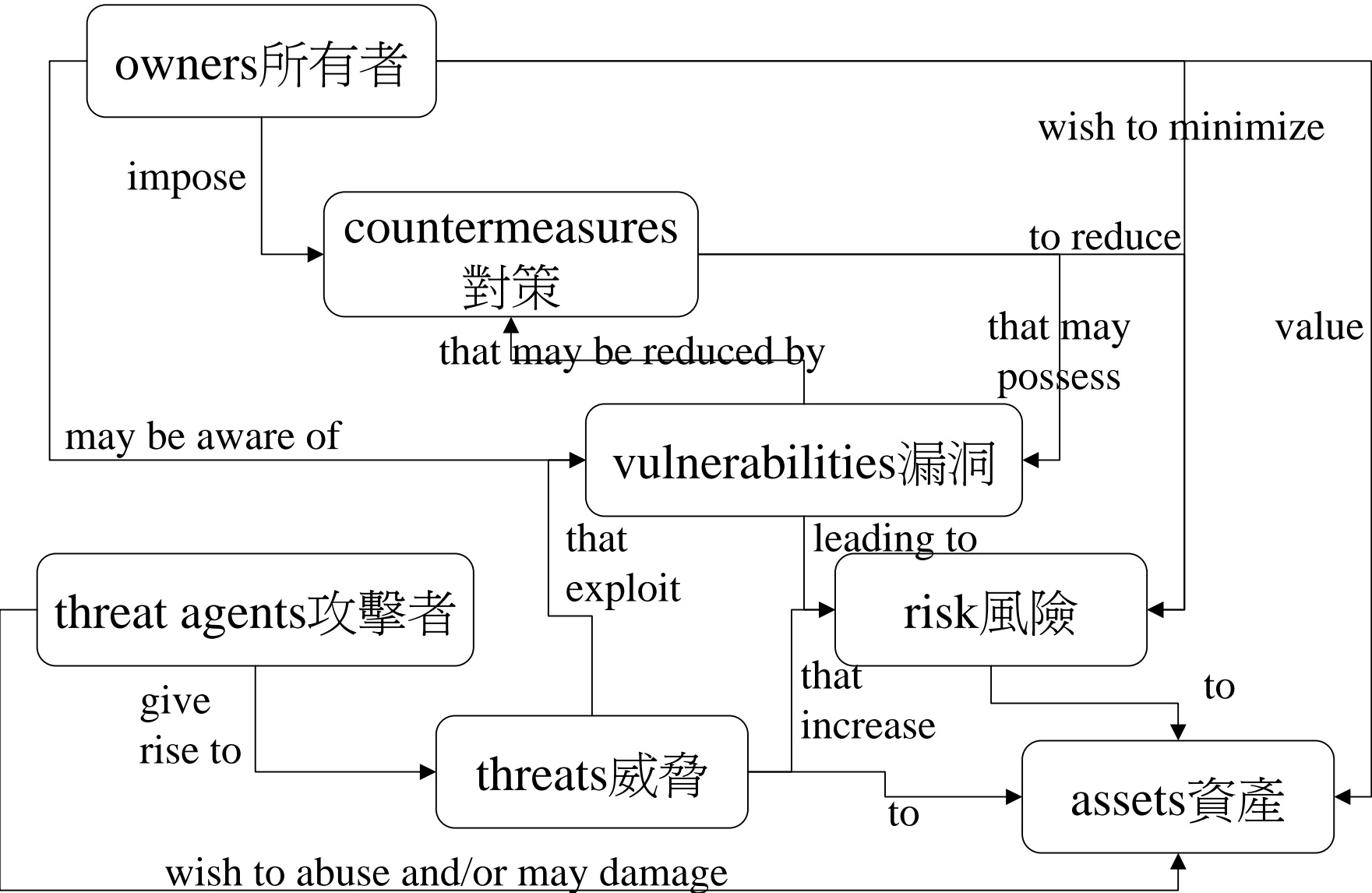
- 國際上每20秒就有一件黑客事件發生
 - 早期的消遣或展示自己在電腦方面的運用能力
 - 近年入侵網絡以達到政治、經濟目的

學校資訊科技保安關注地方

- 資訊科技保安是動態發展的問題
 - 服務提供
 - 保安需求
 - 保安政策
 - 管理實施
 - 管方支持

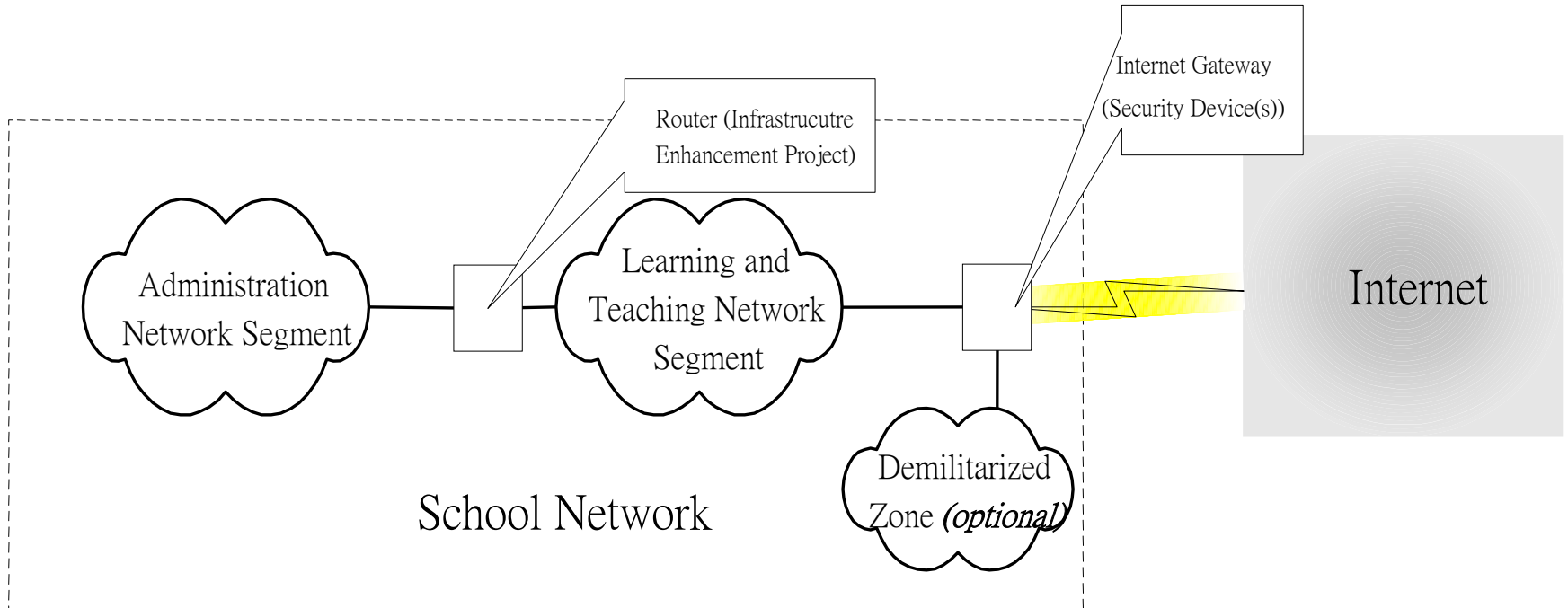
服務與「風險分析」

- 甚麼是須予以保護的資產
- 該類資產的相對重要性
- 處理緊急事件時的先後次序
- 所需的保護程度



Source: **Common criteria for IT security evaluation**

學校網絡



保安政策

- 根據機構的保安需求、業務目的和目標而制定
- 載列有關資訊保安的基本強制性規則和原則
- 整個機構須予以遵守
- 保安規則、指引和程序是推行和執行保安政策的工具
- 與保安政策相比，規則、指引和程序須要有頻密的檢討

保安政策的內容

- 政策的目的是和範圍、將予以保護的資產、受影響人士的職責和責任、有關須予遵守和禁止進行事宜的規則，以及呈報和處理保安事件的措施。
 - 實體保安 physical security
 - 存取控制 access control
 - 數據保安 data security
 - 網絡和通訊保安 network and communication security
 - 保安審計和如何處理保安事件 security audit and incident handling

學校資訊科技保安**10**個小技巧

- 鼓勵或者要求老師/學生選擇比較複雜的密碼
- 要求老師/學生每隔90天更改一次密碼
- 確認防毒軟件的病毒庫是最新的
- 定期升級Web伺服器軟體
- 在員工離開學校以後，儘快取消他（她）的使用存取權

- 不要運行任何不必要的網絡服務
- 如果允許老師在家辦公，就務必要為遠端流量提供一個安全的、集中管理的伺服器
- 使每人都明白電子郵件附件的危險性
- 定期評估保安政策
- 實施一個完整的、全面的資訊科技保安解決方案

人爲因素

對資訊科技保安的影響

- 在構建資訊科技保安時，人爲因素對資訊科技保安的影響非常重要
- 即使是學校已經制定了相應完善的安全制度，如果校內的使用者不認真履行規範性操作規程或違法執行某些越權的行爲，都將對系統安全造成威脅，也會給不法入侵者打開方便之門
- 安全制度最容易由內部攻破，因此加強內部防範和堵塞漏洞是最好的防範機制

- 爲了保證所有的安全工具和安全措施得以發揮最大的效果，教育是最重要的
- 必要對相關人員進行有關的產品售後培訓、安全意識培訓、安全習慣和機制培訓等

如何處理保安事件

保安事件包括

- 電腦病毒感染（通過電郵感染）
- 用戶管理（職員的更替）
- 資產的破壞/損失（盜竊）
- 系統/網絡的不適當的使用（伺服器的不當配置）
- 網絡的入侵（黑客）

保安事件的處理

- 事件的處理計劃應事先予以界定
- 事件一旦出現，負責職員須遵照保安事件處理計劃內列明的程序處理
- 計劃需列出所有活動，包括：
 - 須獲通知的人
 - 為保護證據和記錄冊而須採取的行動
 - 把事件的影響程度加以限制的方法
 - 及採取對用戶產生最少影響為原則的運作復原程序
- 不應忽略對事件作出評估，將有助檢討現行的保安措施，及確保該等措施是完備的措施

Handling network intrusion

網絡入侵的處理

Step 1: remain calm

Step 2: take good notes

Step 3: notify the right people and get help

Step 4: enforce a 'need-to-know' policy

Step 5: use 'out-of-band' communication

Step 9: get back to business and review

Step 8: get rid of the problem

Step 7: make backup

Step 6: contain the problem

