訓練課程名稱：GSN 資訊安全基礎班
訓練日期：2006 年 6 月 21 日
地點：板橋市中華電信訓練所
第一單元：安全漏洞修補

1-1：弱點(漏洞)成因：權限程式、基本程式撰寫實務、信賴不可信任之資訊、Timing windows、演算法的不當使用、其他。

1-2：MBSA 弱點掃瞄：利用微軟所提供的 MBSA 程式，自動掃瞄弱點及手動的方式清除弱點的存在。

1-3：安全性修正(security patch)：將電腦設定爲自動更新的方式，爲最好的解決方法，但是作業系統必需爲正版，因爲本中心有設置 WSUS 伺服器系統，因此只要執行完成便可以做所有的自動更新，包含 Office 辦公室軟體的更新。

1-4：Zero-day exploit：零時差攻擊：在漏洞被公佈的同一天(或之前)就發生利用該漏洞執行被攻擊的事件，主要原因是 CC/CERT 的報告中發現，漏洞數量相同，但是漏洞發現到被攻擊的時間卻明顯縮短。

第二單元：資料備份與復原簡介

2-1：資料備份：將資料複製至其它場所，若原始資料遺失或毀損時，可從備份還原資料，因此資料備份是保護資料的最後一道防線，若沒有資料備份，「業數持續營運」或「災後復原」無法實現。

2-2：資料遺失的可能威脅：分爲天然災害、人爲錯誤、軟體錯誤、硬體故障、病毒。

2-3：備份的三個基本原則：避開尖峰時間、不備份非必要檔案、以排程備份

2-4：備援：備援是保護資料最佳策略與原則：三項優點-容錯能力、防止單點失效、高度可用性。

2-5：備份問題：備份時間過長、還原時間過長、無法確認備份作業是否成功，儲存媒體管理困難(以上爲本校所可能遭遇的問題)

2-6：解決備份問題：可以採用最新的備份技術(SAN、iSCSI、採用快照或鏡像的備份技術)、減少備份的資料量、合宜的備份策略、導入資安管理系統，確保備份媒體與備份資料之管理安全。

第三單元：電腦病毒原理說明及防治方式

3-1：電腦病毒原理說明：此部份經查略講義文件之相關的說明，發現電腦病毒的原理及說明太過於複雜及難以瞭解，因此我們學校只需要求全面安裝掃毒軟體便可以，不需要瞭解其他與電腦病毒有關係的知識，將解毒的相關專業知識交由協力廠商處理便可以。

3-2：中毒原因分析：共享目錄設定不當、帳號密碼設定不當、系統漏洞未修補、防毒軟體、其他

3-3：共享目錄設定不當：windows XP 資料夾共用問題：不能設定爲完整分享，

要設爲唯讀。不能分享開機磁碟、文件與設定資料夾等。
3-4：作業系統內建的還原功能：如果要清除病毒的時候，要先關閉作業系統的還原功能，清除完病毒之後，再開啓還原功能，不然電腦病毒也會因爲還原的關係，還原成有病毒的作業環境。
3-5：自己解毒的方法：拔除網路線->關閉所有共享資料->將中毒電腦重開機至安全模式->執行掃毒程式(工具程式。
3-6：防毒四原則：即時修補安全漏洞、正確設定資源共享、設定複雜的帳號密碼+即時防毒軟體更新。