

## 訓練講習心得報告

日期：96/01/25

訓練講習課程：政府資通安全防護巡迴研討會－資安管理及技術經驗分享

講習者：許曉萍

今天的課程，共分為三個階段，第一階段有 60 分鐘，「營運持續管理(BCM)簡介」，原本以為這個題目似乎與資安沒有什麼關係，後來經過主講者的敘述，才知道它的重要性，因為主講者他都會舉例來說明而且都是用比較工作上或管理上會遇到的一些例子，因此把整個管理的說明更加清楚。

BCM 營運持續管理－整合流程：應包括：危機管理、風險管理與復原技術...等，而且不應受限於資訊資術方面之災難復原。

1. Risk management
2. Disaster Recovery
3. Facilities Management
4. Supply Chain Management
5. Quality Management
6. Health & Safety Management
7. Knowledge Management
8. Emergency Management
9. Security Management
10. Crisis communications & PR

例如：機房的安全設置：儲存媒體是否應安置於機房？因為 CD-ROM 於高溫 80°C 以上會釋放出有毒氣體。

BCM 未來發展：

1. 已成為管理活動不可或缺的工作
2. 已形成國際新標準 BS 25999
3. 整合組織所有營運功能，不再侷限於 IT 領域
4. 亦將發展為可稽核系統

第二階段的課程是「社交工程手法展示」(40 分鐘)，原因是美國加州大學的砲台被入侵，利用網路安全關係，砲台被搬移到另外一個美國大學，舉這個例子來表示社交工程與駭客入侵展示：駭客可以截取觀看對方的畫面，也可以用 FTP 方式將對方的資料下載回來。

結論：

1. 偽冒身份之電子郵件誘使使用者開啓惡意電子郵件之安例層出不窮。
2. 結合社交工程與零時差弱點的精準攻擊，更增加入侵防護之困難度
3. 定期修補軟體漏洞，防範已知軟體弱點所造成的攻擊
4. 使用者認知教育與管理稽核之落實仍為根本解決之道
5. 目前研考會正在政府機關推動職務憑證與資安防護認知訓練，以降低社

交工程電子郵件攻擊之風險。

第三階段的課程是「軟體弱點修補管理機制」：

一、管理機制：可從政策面、程序面、執行面、改善矯正面 4 個方向做起；  
軟體修補重要性必須讓主管以及使用者明瞭清楚它的必要性。

二、軟體修補工具介紹：WSUS—是個微軟免費更新修補程式的工具，網站：  
<http://www.microsoft.com taiwan/windowserversystem/updateservices/downloads/WSUS.aspx>

三、稽核工具介紹—MBSA：(Microsoft Baseline Security Analyzer) 可讓系統管理員掃描一部或多部windows系統電腦，檢查是否有一般的安全性組織錯誤。網站：

<http://www.microsoft.com/technet/security/tools/mbsa2/default.aspx>

以下是上課和區網相關資料網址：

<Http://lisa.tyc.edu.tw/>