第參章　研究設計

第一節　　研究架構

本研究根據文獻探討與訪談結果，訂出可能影響資訊安全結果的三類自變數：技術（Technology）、人員（People）與程序（Process）。因爲不同的組織中，其技術、人員與程序之間的關係可能不同，因此加入組織爲一中介變數。本研究之研究架構如圖 2。

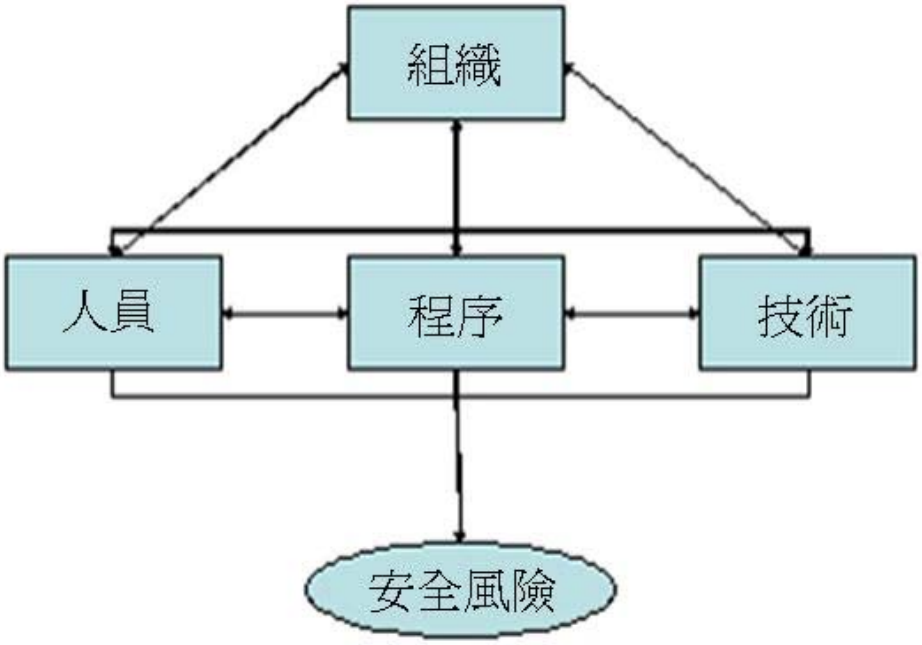

圖2　　研究架構圖

第二節　　資料蒐集

本研究共用訪談及問卷調查兩種方式蒐集資料，訪談對象爲國內某知名防毒軟體公司的技術人員，目的是透過這些技術人員對於資訊安全領域豐富的經驗分享，並且瞭解該公司的客戶群所遭受資訊安全問題的可能主要影響因子。本研究根據訪談後結果製成問卷，問卷調查對象爲國內某知名防毒軟體公司的客戶之資

訊主管或負責資訊安全的人員。問卷資料蒐集分兩種途徑，一個是使用網路問卷調查；由本研究合作廠商提供其客戶電子郵件名單，本研究人員寄電子郵件邀請其進入網路連結填寫問卷。另一個方式是透過郵寄的方式回收書面的問卷；對於沒有提供電子郵件之合作廠商客戶用此方式。本研究之電子郵件網路問卷放置 http://www.my3q.com/home2/73/esite2005/A.phtml (密碼爲 mis@nccu)，邀請信之內容將置於附錄Ⅱ中。

第三節　研究假設

根據前述的文獻探討以及研究架構，本研究提出以下假設，說明如下：

- 資訊安全管理方式對於資訊安全的影響

根據第二章文獻探討指出，資訊安全是一種過程，而並非只有一種產品，因此雖然市面上有許許多多不同的資訊安全系統產品，提供各式各樣的服務來滿足企業組織對於資訊安全的需求。但是對於企業組織而言，他們所採取的資訊安全管理方式不同，即使使用相同的資訊安全產品，成效仍會天壤之別，因此建立假設如下：

H1：不同的「資訊安全管理程序」，其「資訊安全風險」不同。

- 組織特質策對於資訊安全的影響

環境對於個人或是整個組織影響很大，不同的組織會造就不同的環境。一個政策的推動是否能夠成功，除了靠企業組織人員的配合外，組織高層是否支持也是主要的影響來源，尤其是資訊安全政策的推動。在許多企業組織中，資訊部門往往是處於弱勢的一方，權力比一般終端使用者來得小，所以相對上資訊安全政策並不容易推動，即使有完善的資訊安全政策，也是無用武之地。因此建立假設如下：

H2：不同的「組織特質」，其「資訊安全風險」不同。

- 終端使用者使用習慣對於資訊安全的影響

在很多的情況之下，人的行爲是無法強制限制的。有些部分是可以直接透過

資訊安全防護系統去控制與監管，不過有些部分是人的使用行爲所導致的問題，無法輕易地或有效地控制與監管。因此建立假設如下：

H3：不同「終端使用者使用習慣」，其「資訊安全風險」不同。

- 技術對於資訊安全的影響

資訊安全在技術上有困難的原因是許多企業的各項應用程式通常是透過招標的方式，外包給外面的廠商，因爲每個應用程式間的資料結構大不相同，使得在整合資訊安全技術及策略方面上，產生問題，不容易制訂一個統一的規格。因此在推動資訊安全防護政策時，無法快速的推動，因此建立假設如下：

H4：不同「資訊系統整合」，其「資訊安全風險」不同。

第四節　研究變數定義與問卷設計

本研究採用訪談與問卷調查方式，問卷設計是與國內某知名防毒軟體公司的四位 TAM（Technique Account Manager）進行訪談，藉由他們在資訊安全領域的豐富的知識與長年的工作經驗，並參考相關文獻所提出的三類別：技術（Technology）、人員（People）與程序（Process）作一些影響關鍵因子整理。另外把組織背景當作間接變數藉由影響技術、人員與程序而影響資訊安全的結果。這四大類共包含 122 個可能影響的資訊安全風險的變數，及實際發生的可能狀況爲內容，據以設計而成（見附錄Ⅰ）。各研究變數說明如下：

一、組織背景，包括：

- 產業別
- 員工數
- 年收入（營利與非營利單位）
- 分支數（不在同一個地方辦公）

二、技術，包括：

2.1 資訊架構

- 電腦數

- 仰賴網路程度

2.2 防毒設備

2.2.1 裝哪些

以國內知名防毒廠商的產品爲代表

- Desktop&Client
- Outbreak Management
- Network Protection
- Email & Groupware
- Internet Gateway
- File Server & Storage
- Mobile Security

2.2.2 裝在哪

- 防毒軟體安裝的網路位置

2.2.3 類別

- 防毒軟體工具

三、程序，包括：

3.1 統一資訊安全政策（集中管理）

- 是否統一訂定

3.2 一般電腦與軟體管理政策（帳號、密碼與軟體安裝）

- 帳號核對程序
- 密碼控管政策
- 軟體安裝政策
- 定期系統備份方案

3.3 網路使用規範

3.3.1 內/外部使用者規範

- 內部使用者使用網路
- 外部使用者使用網路
- 遠端登入
- 機構間資訊交流

3.3.2 網路劃分

- 不同網路區段
- 中斷不同網路區段

3.3.3 筆記型電腦使用

3.3.4 其他網路控管規範

- Email 附件的過濾
- 惡意網路的過濾
- 即時檔案傳輸的過濾
- 串流式媒體的過濾
- P2P 軟體的過濾
- 無法管理的網路連線
- 分享資訊夾
- 即時通訊軟體的過濾

3.4 防毒管理

3.4.1 安裝

- 防毒軟體安裝率

3.4.2 維護

- 安裝與移除防毒軟體方式
- 部署防毒元件
- 病毒爆發反應程序
- 防毒管理績效評估

3.4.3 追蹤

- 客戶端病毒碼過期比例
- 伺服器端病毒碼過期比例
- 防毒硬體裝置病毒碼過期比例
- 防毒監控與偵測能力
- 資訊收集的格式
- 追蹤電腦實體位置

3.5 弱點管理

3.5.1 安裝

- 弱點掃描
- 入侵偵測系統
- 入侵保護系統
- 修補程式自動部署工具

3.5.2 維護

- 瞭解弱點程度
- 部署安全修補檔

3.5.3 追蹤

- 客戶端修補檔未更新比例
- 伺服器端修補檔未更新比例
- 發佈最新型態威脅的警報

四、人員，包括：

4.1 資訊安全人員

- 專職資訊安全人員數
- 電腦安全部門

4.2 其他部門配合

- 遵守資訊安全政策的使用者比例
- 資訊安全政策強制執行程度

4.3 終端使用者教育訓練

- 教育訓練頻次
- 教育訓練型態
- 教育訓練主題

五、安全風險結果，包括：

- 病毒爆發事件數
- 病毒感染嚴重程度
- 偵測病毒數
- 偵測可能感染事件數

第五節　　分析方法

本研究採用訪談分析法與調查分析法。

- 訪談分析法：
  是利用內容分析法（Content Analysis）找出令企業組織資訊安全系統「健康」與「不健康」的關鍵影響因子。

- 調查分析法：
  1. 利用頻次分析法（Frequency Analyses）瞭解回收樣本的特質。
  2. 利用變異數分析法（ANOVA）找出「健康」或「不健康」的關鍵差異問項。
  3. 利用卡方分配檢定找出「健康」或「不健康」組織的關鍵差異問項。
  4. 分類：利用上述 2 與 3 所找出的關鍵差異問項，進行 Cluster 分析，分成 3 或 4 個群組，驗證以上述的問題來分群的正確性。

本研究使用的分析工具：以 SPSS for Windows13.0 與 Microsoft Excel 2003 爲主。