第伍章　結論與建議

第一節　　結論與建議

本研究採用文獻探討、人員訪談、與問卷調查三管齊下方式。結果發現：資訊安全必須靠擬定合適資訊安全策略（Plan）、能夠執行公司資訊安全政策（Implement）、及能夠有資訊評估公司資訊安全情形（Audit）三者來共同完成。最佳的狀況一定是

- 採用集中控管
- 能更自動化收集訊息（如每台電腦偵測到的感染數目、中毒數目等等）
- 有專人負責資訊安全政策制定〈至少在組織最高層要有〉
- 下層使用者能配合執行及按規定使用電腦設備
- 有 audit 會評估執行結果

這種最佳狀況其實是無法達到的，因爲投入資訊安全的效益其實很難具體量化，以至於無法做成本效益分析。所以我們試圖由本次收集到資料按照文獻中所提的三類別：技術（Technology）、人員（People）與程序（Process）作一些影響關鍵因素整理。另外把組織背景當作一控制外變數（Uncontrolable Variable）或間接變數會藉由影響技術、人員或程序而影響資訊安全的結果。

（一）　組織背景

組織特質在本研究中共包含四項組織背景變數（產業別、員工人數、營利事業收入、分支機構個數），這些變數是用來當作間接變數，也就是用來了解組織背景對其技術、人員或程序的安排是否有影響。根據相關分析結果顯示員工人數是一個和技術〈員工數多則電腦多、對網路仰賴程度也高〉、人員〈員工數多則資訊安全人員多且教育訓練也多〉或程序〈員工數多的公司在資訊安全政策上會比較謹慎〉的安排有顯著相關的組織因素，因此員工人數可能是一個重要的影響人員、技術、及程序的變數。

在與技術人員訪談中得到有比較嚴重中毒問題的組織幾乎常是公家機關，他

們的資訊安全管理相對較缺乏彈性。但是在問卷調查結果並沒有發現公家機關中毒頻次比較高或者中毒比較嚴重，那可能是因爲就業務形式而言，並不是所有的公家機關都會有較多頻次或較緊密的與外部資料接觸。

（二） 技術

調查問卷中資訊架構相關問題包括組織電腦數目、及對網路的仰賴程度兩題。根據調查資料卡方檢定分析結果顯示

- 電腦少的公司比較容易管理，因爲電腦數少的機構比電腦數多的機構所偵測到的病毒數較少
- 仰賴網路程度較多的機構會比較重視資訊安全，因此其病毒爆發數會比較少

本次研究結果上，技術相對人員及程序顯得不重要。無論是訪談或問卷調查結果均大多無法證明使用趨勢產品能對防毒有顯著效果，因爲裝與不裝的兩類公司大多無法證明有太多顯著差異；在技術人員訪談中無人提到技術的影響。至於在問卷調查卡方檢定中有顯著差異的項目不是太多；除了

- 若有使用防毒管理工具的機構在病毒爆發的數量上，會比沒有使用防毒管理工具的機構少
- 使用某公司產品的「Email & Groupware」產品的機構在病毒爆發數量上，有顯著的幫助
- 使用「File Server & Storage」的機構在於偵測感染事件上，會偵測比較少的可能感染事件數

之外也沒有任何其他的某公司產品在安裝與沒有安裝兩群顯示有顯著差異。這個結果多少證明安裝防毒軟體，特別是「Email & Groupware」產品是有用的；可能是與目前藉由 Email 傳送的病毒很流行之故。至於其他類防毒軟體體爲何沒有顯著差異，猜想可能有幾個原因會造成這樣結果：第一個原因當然是因爲購買防毒軟體其實如同買保險一樣，即使大多的病毒被偵錯到，使用者或維護人員也不會感受到，第二個可能原因是單一技術不能顯示出差異，例如 A 產品必須與 B 產品搭配才可能有防毒效果，這點要在和技術人員確認。第三個原因也可能是樣本代表性有誤差。

（三） 程序

程序成爲第二項也是最可行的增加資訊安全的工具，因爲人員相對於程序更不容易改變；而技術又不是太重要會影響資訊安全效果的因素。因此本調查中試圖利用統計方法找出一些在程序中比較需要被重視的因素。另外後續也可以做長期的問卷分析，比較一下程序中各關鍵因素對組織中毒嚴重性影響的變化。本次調查結果顯示：不論是訪談或調查結果顯示統一集中管理的資訊安全政策對病毒感染預防有顯著效果。在變異數分析結果顯示有集中管理的資訊安全政策其組織病毒爆發事件只有沒有集中管理的資訊安全政策組織的五分之一；在卡方檢定中顯示推動資訊安全政策與教育訓練並且強制性的機構，其病毒爆發影響嚴重性會比較容易掌控。

如果一個組織能設定以下之一般電腦與軟體管理政策，則會對中毒結果有顯著好的影響，這些有效管理政策包括有

- 新增刪除帳號核對確認程序
- 密碼控管政策
- 軟體安裝政策
- 惡意網站過濾
- 禁止分享資料夾

上述五種管制均對病毒爆發數量或病毒爆發影響嚴重性有正面的影響。因爲越來越多的病毒是借由網路傳送的，因此對網路使用的規劃會對中毒情形有較嚴重的影響；例如調查結果顯示

- 若禁止外部使用者使用機構內部網路，會降低偵測到可能感染的事件數
- 不能區隔辦公系統與關鍵任務系統間並隨時中斷兩者連線的組織有比較高的偵測到可能感染事件值

不過訪談中也可得知如果以上兩者做不到的話，其實可能是因爲有組織特質上的原因。例如業務上必須提供這樣的便利性。卡方檢定顯示如果能監控使用者的網路使用狀況，對於病毒爆發數量、病毒爆發影響嚴重性、偵測病毒數與偵測感染事件數上，都會有顯著的幫助。

在防毒管理上不論防毒軟體的事先安裝規劃或維護都是很重要的。變異數分析結果顯示會事先規劃部署防毒元件更新程序的組織其病毒爆發影響嚴重性較低；變異數分析結果顯示覺得更新不理想時會有後續補救措施的組織其病毒爆發影響嚴重性較低。卡方檢定結果顯示客戶端病毒碼、伺服器端病毒碼與防毒硬體裝置病毒碼過期比例較低的機構在於偵測到可能感染事件數上，會比過期比例高的機構來得少；卡方檢定顯示有監控資訊安全相關資訊〈不論是監控防毒軟體安裝率、監控防毒硬體裝置病毒碼過期比例〉的組織其病毒爆發數量或病毒爆發影響嚴重性都較未進行監控資訊安全相關資訊的組織低。並且如果由監控機制所搜集到的資訊會透過監控系統自動分析並且轉換成一些報表的機構，取得的資訊是比較詳細的，因此在病毒爆發數量上也會比較少。

資訊安全會有漏洞其實有很多根本是無法克服的先天障礙，例如 Windows 修補檔那麼多，修補工作其實很花人力，所以勤於研究哪些修補檔應該做，勤於做修補的組織其中毒比例比較低；或是修補檔更新比例過低會有後續修補動作的組織其病毒爆發影響嚴重性較低。所以勤於做這些漏洞管理是有效的。但是一個組織不做修補的原因並不一定是懶惰或是人手不足，也可能是害怕與舊的 AP 可能會相衝；在可能中毒與 AP 可能會相衝而不能用兩害相權之下，企業寧願選擇冒可能有漏洞的風險，大公司或是老公司於此種情形會比較嚴重。不論文獻或本次調查的卡方檢定結果均顯示一個組織如果能持續收集一些可能產生漏洞的監控資訊是對資訊安全很有幫助。例如有監控資訊安全相關資訊〈不論是監控伺服器離線率、或監控 AP 伺服器修補檔未更新比例〉的組織，其病毒爆發數量或病毒爆發影響嚴重性都較未進行監控資訊安全相關資訊的組織低。

（四） 人員

在與技術人員訪談中得到重要的影響資訊安全的關鍵因素是人員，由技術人員所提出的案例看來，專業的資訊安全人員且持續的從事資訊安全工作是很重要的，如部分公家機關的個案中，其中的資訊安全人員不被視爲專業人員，而需要與一般行人員一樣必須二年輪調職務是主要原因。在資訊安全人員安排上比較重要會影響中毒頻率及中毒結果嚴重性的有兩點

- 由專人擬定資訊安全策略並由專人去執行是很重要的，不論在訪談或由問卷

調查中均有相同結論。組織應該要把資訊安全人員當作專業人員

- 專職且持續負責資訊安全人員：要在中毒事件未爆發前就能完全防範其實做不到，比較合理的方式是在事後能有檢討改進，因此資訊安全計畫需要長期持續的去改進。在錯誤中求進步

如同其他的妨礙組織進步的管理因素一般，如果有高階主管在人事上無法調整的瓶頸，那麼相對而言，技術就顯得不是重要因素了。所以公家機關會較私人企業在對資訊安全的重視程度上感覺差很多，主要倒不在於技術，而是人事安排及組織缺乏彈性之故。除了前述所提到的資訊安全人員的人事安排，其他部門之配合度亦是重要因素，如訪談資料顯示終端使用者的強勢，使得資訊安全人員根本無權要求。

在與其他部門的配合上比較重要會影響中毒頻率及中毒結果嚴重性的有兩點：

- 高階主管支持：既然資訊安全的成本效益無法估計，而且資訊安全人員永遠像是救火隊在滅火，事後又要去檢討防範未來，因此資訊安全人員的績效認定恐怕多只能靠高階主管的信任了
- 資訊安全與使用者的關係：這是指資訊安全人員是否有足夠權利（Power or Authority）去執行他所擬定的資訊安全計畫，這當然和高階主管的支持及其所服務的使用單位在公司的地位有關

資訊安全教育訓練可能是資訊安全人員比較算來可行的策略了。如果無法做到集中控管，也很難改變組織的人事制度及文化，那使用者個別的資訊安全素養可以藉由教育訓練來修正，期待使用者能自行認知中毒的痛苦及哪些使用習慣會帶來比較大的危險能性。調查結果顯示資訊安全教育較多的組織其相對病毒爆發影響嚴重性顯著低。

第二節　　研究限制

要討論如何讓企業資訊安全的增強〈以降低中毒問題爲主的話〉，應先考慮其控管方式的真相，然後加以評估其可能之漏洞在哪裡。如果是集中式的控管，那我們只需要問一個負責控管的人員就可以了解整個組織的控管情形，但是如果

是分散式的控管方式，一份問卷或訪談一個人通常就無法得到真相，需要同一企業中問多個員工才比較能描繪出真相。本問卷因爲無法事先知道受測組織的資訊安全結構，爲方便起見，在所有組織中都只有選擇一位聯絡人作爲問卷填答者，因此問卷結論需謹慎使用。

另外，其實許多學者對調查研究結果本身都會存疑，因爲調查研究比較適合驗證性，也就是對我們假設的結論加以驗證，如果用此方法去發現一些事實恐怕會令人質疑。本研究爲了不要遺漏可能的影響因素，因此選擇將所有可能影響資安的因素都列示在調查問卷內，然後以統計上能顯著的因素列爲關鍵因素；因此對研究結果使用上必須要謹慎，因爲「統計結果顯著並不絕對代表理論顯著，而統計結果不顯著並不絕對代表理論不顯著」。

本研究也試圖透過統計方法 K-Means Cluster 方法去驗證我們所找出來的關鍵因素能否將本研究之樣本加以適當分類，結果不理想，這代表其實所得的關鍵問題還不夠穩定。因此在做結論時我們沒有用題目本身而是希望用比較大的分類來說明。