附錄I 本研究問卷

一、組織背景

1 貴機構是屬於以下哪種產業？

- ☐ 金融業
- ☐ 製造業
- ☐ 電子資訊業-硬體
- ☐ 電子資訊業-軟體
- ☐ 通訊與傳媒
- ☐ 政府機關
- ☐ 教育學術單位(學校等)
- ☐ 貿易, 百貨及零售商
- ☐ 醫療相關行業(醫院等)
- ☐ 建築營造業
- ☐ 運輸及航運業
- ☐ 其他，請說明_____

2 在您的機構中，目前有多少位員工？

- ☐ 1-500 位
- ☐ 501-1000 位
- ☐ 1001-3000 位
- ☐ 3001-5000 位
- ☐ 5001-10000 位
- ☐ 10000 位以上

3 請問貴機構去年的年收入爲何(單位：千元)？**(非必填)**

- ☐ 非營利機構
- ☐ 營利機構年收入(單位：千元)：_____

4 貴機構有多少個分支單位(不在同一個地方辦公)？

- ☐ 0-5
- ☐ 6-10
- ☐ 11+

二、技術

2.1 資訊架構

5 貴機構中有多少台電腦？

- ☐ 1-500 台
- ☐ 501-1000 台
- ☐ 1001-3000 台
- ☐ 3001-5000 台

☐ 5001-10000 台

☐ 10000 台以上

6 貴機構的業務仰賴網路的程度爲何？

☐ 沒有

☐ 一點點

☐ 有點

☐ 非常多

2.2 防毒設備

2.2.1 裝哪些

7 貴機構安裝了哪些某公司的產品？請勾選**(多選)**

Desktop & Client

☐ 沒有

☐ OfficeScan.

☐ Anti-Spyware.

☐ PC-cillin Internet Security.

☐ Home Network Security.

Outbreak Management

☐ 沒有

☐ Control Management.

Network Protection

☐ 沒有

☐ Network VirusWall.

Email & Groupware

☐ 沒有

☐ ScanMail for Microsoft Exchange.

☐ ScanMail eManager.

☐ ScanMail for Lotus Domino.

☐ IM Security for Microsoft Office Live Communications Server.

Internet Gateway

☐ 沒有

☐ Spam Prevention Solution.

☐ InterScan Messaging Security Suite.

☐ InterScan Web Security Suite.

☐ URL Filtering.

☐ Java Applet.

☐ InterScan VirusWall.
☐ InterScan eManager.
☐ InterScan AppletTrap.
☐ InterScan WebProtect for ISA.

File Server & Storage

☐ 沒有
☐ ServerProtect for Microsoft Windows/Novell NetWare.
☐ ServerProtect for Network Appliance filers.
☐ ServerProtect for EMC Celerra.
☐ ServerProtect for Linux.
☐ PortalProtect for SharePoint.

Mobile Security

☐ 沒有
☐ TM Mobile Security.

2.2.2 裝在哪

8 問貴機構使用幾台 OfficeScan 伺服器？_____

9 請問貴機構有多少台 OfficeScan 客戶端？_____

10 請問貴機構的 OfficeScan 伺服器平均每台管理多少台 OfficeScan 客戶端？

_____

11 機構將該防毒軟體安裝在網路上的哪個位置？**(複選)**

☐ Internet Gateway
☐ Email/Groupware Server
☐ LAN Server
☐ Client PCs

2.2.3 類別

12 問貴機構使用下列哪些防毒管理工具？**(複選)**

☐ 沒有
☐ FTP 閘道防毒..
☐ HTTP 閘道防毒.
☐ Email 閘道防毒.
☐ 其他. 請說明: _____.

三、程序

3.1 統一資訊安全政策(集中管理)

13 貴機構的資訊安全政策是否統一訂定(集中管理)？

☐ 集中管理 (總部高層制定所有的資訊安全政策，分支單位必須遵守)
☐ 沒有集中管理 (分支單位可以自行制訂自己的資訊安全政策)

3.2 一般電腦與軟體管理政策(帳號、密碼、軟體安裝)

14 貴機構在新增或刪除帳號時，是否有核對確認(verification)的程序？

☐ 沒有，我們只根據紙上作業，並沒有核對確認的程序。

☐ 有，我們在新增帳號時會與人事部門核對，但是我們沒有管道可以得知該帳號將來是否會成爲“幽靈帳號”。

☐ 有，我們在新增帳號時會與人事部門核對，並且定期清除不再使用的帳號，以避免“幽靈帳號”的存在。

15 貴機構是否有密碼控管政策（如密碼格式、更新頻率以及加密之要求）？

☐ 否，我們沒有正式的密碼控管政策

☐ 是，我們有正式的密碼控管政策，但是沒有強制執行

☐ 是，我們有正式的密碼控管政策，並且有效地執行（每位使用者採用事先定義好的密碼格式，並且定時更換密碼）

16 貴機構是否有軟體安裝政策（例如：禁止安裝未授權軟體與即時通軟體）？

☐ 我們沒有正式的軟體安裝政策（使用者自行安裝自己需要用的程式）

☐ 我們有正式的軟體安裝政策，但是我們無法預防使用者自行安裝軟體。

☐ 我們有正式的軟體安裝政策，且我們會定時清查使用者的電腦，以確保他們確實遵守此政策。

17 貴機構是否有定期的系統備份方案？

☐ 否，我們並沒有定期的系統備份方案

☐ 有，我們有定期的系統備份方案。但是，那個方案只有適用於最重要的伺服器，並不適用於防毒伺服器。

☐ 有，我們有定期的系統備份方案，且適用於所有應用程式與防毒伺服器。

3.3 網路使用規範

3.3.1 內/外部使用者規範

18 貴機構是否允許內部使用者(比如員工)使用 Internet？

☐ 是

☐ 否

19 機構是否允許外部使用者(比如外來的廠商)在貴機構中使用 Internet？

☐ 是

☐ 否

20 貴機構是否允許機構外的電腦進入您的企業網路？

☐ 是

☐ 否

21 機構是否允許外界的機構與貴機構間作資訊的交流？

☐ 是

☐ 否

3.3.2 網路劃分

22 貴機構是否將辦公系統(office automation)與關鍵任務系統(mission critical

systems)分隔於不同的網路區段(network segments)？

☐ 否，我們並沒有將網路分成辦公使用與關鍵任務系統使用兩個部分。

☐ 是，我們將網路分成辦公使用與關鍵任務系統使用兩個部分，二者之間只允許少數連線。

☐ 是，我們將網路分成辦公使用與關鍵任務系統使用兩個部分，二者之間不允許任何連線。

23 您是否可以隨時中斷辦公系統與關鍵任務系統間的網路連線？

☐ 否，我們無法中斷辦公系統與關鍵任務系統間的網路連線。

☐ 是，不過我們很少中斷辦公系統與關鍵任務系統間的網路連線。

☐ 是，我們可以很容易中斷辦公系統與關鍵任務系統間的網路連線。

3.3.3 筆記型電腦使用

24 貴機構是否禁止以下各類型的電腦使用網路？**(複選)**

☐ 沒有限制

☐ 內部人員個人的筆記型電腦

☐ 安全修補程式(patch files)過期或未更新的筆記型電腦

☐ 病毒碼(或病毒定義檔)過期的筆記型電腦

☐ 其他，請說明：_____

3.3.4 其他網路控管規範

25 貴機構是否制定並執行以下各種規範，以控管使用者的網路使用狀況？**(複選)**

☐ 沒有

☐ Email 附件的過濾（不允許.exe, .com, …等格式, 或過大的附件等）

☐ 惡意網站的過濾

☐ 即時通訊軟體(Instant Messenger)的過濾（包括即時檔案傳輸）

☐ 串流式媒體(streaming media)的過濾（包括 real-audio 等）

☐ P2P 軟體的過濾（Skype, Kazaa, …等）

☐ 禁止無法管理的網路連接（例如 ADSL, 撥接…等）

☐ 禁止分享資料夾

☐ 禁止使用即時通訊軟體

3.4 防毒

3.4.1 安裝

26 貴機構的總體(包含客戶端 client 與伺服器端 server)防毒軟體安裝率爲何？

☐ 我們並沒有追蹤這方面的資訊

☐ 95% - 100%

☐ 90% - 95%

☐ 小於 90%，請提供大約的比例: _____

3.4.2 維護

27 以下哪個敘述最能正確說明貴機構安裝或移除客戶端防毒軟體的方式？

☐ 終端使用者(end users)自行安裝防毒軟體

☐ IT 人員替所有終端使用者安裝防毒軟體，而終端使用者擁有移除防毒軟體的權力

☐ IT 人員替所有終端使用者安裝防毒軟體，且終端使用者沒有移除防毒軟體的權力

28 貴機構如何部署防毒的元件(Scan engine, Pattern, Program, Clean Tool)？

☐ 終端使用者(end users)自行更新防毒元件。我們並不追蹤結果。

☐ IT 人員更新防毒元件並且持續監控，以達到滿意的程度.

☐ 透過系統，視需要定期自動更新防毒元件。

29 (如果您並未追蹤病毒碼更新比例，請略過此題。) 當您覺得病毒碼更新比例過低而不滿意時，您會有後續動作來改進病毒碼的更新嗎？

☐ 我們沒有足夠的資源或權力來採取後續動作。

☐ 有時候。當有重大事件發生時，我們會採取後續動作。

☐ 是的。我們會分析資料，並且在必要時，採取後續動作。

30 貴機構是否有病毒爆發反應程序(virus outbreak response process)？

☐ 沒有，我們並沒有病毒爆發反應程序。我們都是當作個案處理。

☐ 有，我們有病毒爆發反應程序，但是沒有完全遵循。

☐ 有，我們有病毒爆發反應程序，且每次病毒爆發時都會遵循。

31 貴機構是否有防毒管理的績效評估？

☐ 沒有。我們並沒有防毒管理的績效評估。

☐ 有一部分。我們評估我們整體安全績效，但是，我們並沒有評估防毒績效。

☐ 有。除了整體的安全績效之外，我們也同時利用量化指標(quantitative indicators)來評估防毒績效。

3.4.3 追蹤

32 平均來說, 貴機構客戶端(client)電腦的病毒碼(病毒定義檔)過期的比例爲何？

☐ 我們並沒有追蹤這方面的資訊

☐ 0% - 5%

☐ 5% - 10%

☐ 大於 10%，請提供大約的比例: _____

33 平均來說, 貴機構伺服器端電腦(例如 application servers, web server, file server, email server, ftp server, and network components)的病毒碼過期的比例爲何？

☐ 我們並沒有追蹤這方面的資訊

☐ 0% - 2%

☐ 2% - 5%

☐ 大於 5%，請提供大約的比例: _____

34 平均來說, 貴機構防毒硬體裝置的病毒碼過期的比例爲何？

☐ 我們並沒有追蹤這方面的資訊

☐ 0% - 2%

☐ 2% - 5%

☐ 大於 5%，請提供大約的比例: _____

35 以下哪個情況比較適合說明貴機構防毒監控與偵測能力（例如: 監控病毒感染狀況或防護程度）

☐ 我們並未進行防毒監控與偵測

☐ 我們有使用一些防毒監控，但並不完全能夠偵測到安全威脅及病毒入侵

☐ 我們有使用防毒監控，而且能夠偵測到大部分的情況

36 請問您如何使用由監控機制所搜集到的資訊？

☐ 搜集到的資訊是未經分析或僅有簡單分析的原始資料記錄格式(log)

☐ 搜集到的資訊會透過大量的人力來分析, 並且轉換成一些簡單的報表.

☐ 搜集到的資訊會透過監控系統自動分分析並且轉換成一些報表.

37 貴機構可以透過電腦名稱來追蹤電腦的實體位置嗎？

☐ 否。我們沒辦法透過電腦名稱來追蹤電腦的實體位置。

☐ 一部分。我們可以透過電腦的登錄值(registry)或是一些手動的方式來追蹤電腦的實體位置。

☐ 可以，我們很容易便可以透過電腦名稱來追蹤電腦的實體位置。

3.5 弱點管理

3.5.1 安裝

38 請問貴機構使用哪些弱點管理工具(vulnerability management tools)？ **(複選)**

☐ 沒有

☐ 弱點掃描 (vulnerability scanners).

☐ 入侵偵測系統 (intrusion detection systems).

☐ 入侵保護系統 (intrusion protection systems).

☐ 修補程式自動部署工具 (automatic patches distribution (pull/push) tools).

☐ 其他. 請說明: _____.

3.5.2 維護

39 貴機構是否知道目前有無任何弱點(vulnerabilities)存在於貴機構的電腦中？

☐ 否，我們無法確定是否有任何弱點存在於我們的系統中。

☐ 有時候，我們偶爾掃描檢查，但因爲一些電腦在掃描時離線，導致掃描不完全。

☐ 是，我們會留意弱點，而且隨時更新最新的修補檔(patch files)。

40 貴機構如何部署安全修補檔(deploy security patch files)？

☐ 修補檔由終端使用者(end users)自行手動更新，我們並沒有進一步追蹤。

☐ 修補檔由資訊人員更新並監控, 以達到滿意的程度。

☐ 透過系統，視需要定期自動更新修補檔。

41 (如果您並未追蹤修補檔更新比例，請略過此題。)當您覺得修補檔更新比例過低而不滿意時，您會有後續動作來改進修補檔的部署嗎？

☐ 我們沒有足夠的資源或權力來採取後續動作。

☐ 有時候。當有重大事件發生時，我們會採取後續動作。

☐ 是的。我們會分析資料，並且在必要時，採取後續動作。

3.5.3 追蹤

42 平均來說, 貴機構的 Windows 客戶端的修補檔(patch files)未更新的比例爲何？

☐ 我們並沒有追蹤這方面的資訊

☐ 0% - 10%

☐ 10% - 20%

☐ 大於 20%，請提供大約的比例: _____

43 平均來說, 貴機構的 Windows 伺服器端的修補檔未更新的比例爲何？

☐ 我們並沒有追蹤這方面的資訊

☐ 0% - 5%

☐ 5% - 10%

☐ 大於 10%，請提供大約的比例: _____

44 平均來說, 貴機構伺服器端（比如 Web Servers, Email Servers, Database servers, and Application servers）的修補檔未更新的比例爲何？

☐ 我們並沒有追蹤這方面的資訊

☐ 0% - 5%

☐ 5% - 10%

☐ 大於 10%，請提供大約的比例: _____

45 貴機構是否有正式的管道，來向使用者發布最新型態威脅的警報？

☐ 沒有，我們沒有正式的管道來通知使用者有關最新型態的威脅。我們只有在威脅發生事後才會通知使用者。

☐ 有，我們有正式的管道來通知使用者有關最新型態的威脅，但是只有在嚴重類型的威脅才會使用。

☐ 有，我們有正式的管道（例如 newsletter 或 email）通知使用者有關最新型態的威脅。

四、人員

4.1 資訊安全人員

46 貴機構有幾位處理防毒工作的專職員工？

☐ 0

☐ 1-5

☐ 6-15

☐ 16-50

☐ 51+

47 貴機構是否有專門負責電腦安全問題的部門？

☐ 沒有。我們沒有專門負責電腦安全問題的部門。

☐ 部分有。我們沒有特定的組織負責電腦安全問題，但是有專門的人員來負責。任務與責任有清楚地訂出，但是沒有正式的通報處理(escalation)流程及政策來管理這部分。

☐ 有。我們有專門負責電腦安全問題部門。該部門有明確的任務與責任並且有正式的通報處理流程及政策。

4.2 其他部門配合

48 有多少比例的使用者會確實遵從貴機構發佈的資訊安全政策（如郵件附件的限制或不准瀏覽某些網站等）？

☐ 低於 50%

☐ 50% - 80%

☐ 超過 80%

49 貴機構資訊安全政策強制執行的程度如何？

☐ 資訊安全政策僅限於書面，並沒有強制執行。

☐ 當情況嚴重時，可以強制執行資訊安全政策。

☐ 平時就會強制執行資訊安全政策，並且將重大違紀的事件送交人事部門懲處。

4.3 End User 教育訓練

50 貴機構對員工做資訊安全教育訓練的頻次爲何？

☐ 一季一次

☐ 一年一次

☐ 很少

☐ 從未舉行

51 貴機構採用以下哪些類型的資訊安全教育訓練？**(複選)**

☐ 線上教育訓練課程

☐ 標準的課堂教育訓練

☐ 客制化教育訓練 (customized training)

☐ 病毒爆發模擬演習

52 貴機構實施以下哪些主題的資訊安全教育訓練？**(複選)**

☐ 病毒介紹與防護方法

☐ 其他安全威脅（Phishing, Zombie, MSN）

☐ 社會工程(Social Engineering)

☐ 其他，請說明: _____

五、安全風險結果

5.1 病毒爆發事件數

53 在過去的三年間，就貴機構所發現的病毒爆發(大量散播)事件，平均一年幾件？_____

5.2 病毒感染嚴重程度

54　在過去的三年間，就貴機構所發現的病毒爆發事件，平均一次有多少比例的電腦受到感染，並且使其無法提供每日例行的運作(單位：%)？_____

5.3 偵測病毒數

55　最近的三個月中，貴機構每個月所偵測到的病毒數爲何？(若您使用某公司的 TMCM, 其紀錄檔中可取得此一資訊）_____

5.4 偵測可能感染事件數

56　最近的三個月中，貴機構每個月所偵測到可能感染的事件數爲何？（若您使用某公司的 TMCM, 其紀錄檔中可取得此一資訊）_____