摘要

隨著網際網路的快速成長，資訊安全已成爲企業最重視的議題之一。企業必須保護自己免於網路威脅(Cyber-Threat)，不過防止企業免受網際威脅已非易事，這也爲企業資訊安全風險埋下了一顆不定時炸彈。換句話說，資訊安全風險是現今企業所面臨的主要挑戰之一，企業資訊安全防護的好壞將直接反應在企業的盈虧上，甚至可能影響到顧客對該企業產品或服務的滿意度等，對企業的殺傷力是不容忽視的。目前的防毒軟體(Anti-Virus)與威脅管理系統(Threat Management System)所能提供的基本功能都是大同小異，其效能也在伯仲之間，但是企業使用的成效則大不相同。因此如何掌握左右企業資訊安全風險的主要影響因子，並根據該影響因子提供企業一套資訊安全策略以解決其所面臨的風險與使得金錢上的損失降到最低，將是改善企業資訊安全風險的關鍵成功因素。

本研究首先透過與五位企業安全維護有實務經驗的專家訪談，了解資訊安全之重要影響因素並不在於投入防毒軟體的預算金額，反而是企業的資訊安全策略類型，如使用者與資訊安全人員關係型態、資訊安全人員的素質、高階主管對資訊安全政策的支持之類因素更重要。

接著藉由問卷調查，以國內某著名防毒軟體客戶爲樣本，發出 1910 份郵寄問卷與網路問卷邀請 email 信，共回收 102 份有效問卷，回收率 5.3%。問卷共分爲兩大部份：組織特徵（包括公司背景、過去三年病毒感染情形、防毒系統、資訊安全管理現況）及防毒能力評估（防毒軟體的使用、監控與過濾、追蹤裝置、區隔網路等四類防毒技術的使用，與弱點管理、病毒碼部署、帳號管理、應用程式與網路使用的權限、回應與恢復程序等五類安全程序政策，組織的責任與能力、組織的順從、對教育訓練的重視等三項組織因素）。以「病毒爆發數量」、「病毒爆發影響嚴重性」、「偵測病毒數」與「偵測感染事件事」爲應變數，以公司概況及防毒能力評估各變項爲自變數進行單因子與多因子變異數分析，分析結果顯示組織大小及防毒軟體的使用、弱點管理、帳號管理等安全程序政策是影響「病毒爆發數量」的重要因素；組織大小、網路管理等組織特徵，防毒軟體的使用、弱點管理、病毒碼部署等安全程序政策及教育訓練等是影響「病毒爆發影響嚴重性」的重要因素；組織大小與防毒軟體的使用、監控與過濾等防毒技術的使用，

弱點管理影響「偵測病毒數」的重要因素；組織大小、弱點管理、與教育訓練等是影響「偵測感染事件數」的重要因素。

本研究藉由分析企業在資訊安全所面臨到的風險，得以建立並發展相關評量的模型，研究結果除了可以提供廠商與設計人員在開發企業資訊安全風險評量時參考的依據，也爲後續的相關實證研究提供一些建議的方向。

關鍵字：資訊安全、病毒、網路威脅、弱點管理

Abstract

Following the growth of the www internet in the latest years, information security has become the most important topic among all enterprise companies. Enterprise companies have to protect themselves from Cyber-Threat, but this is not an easy job at all. That means a hidden bomb has already been planted inside their information systems. In another words, the information security threat is the main challenge that all enterprise companies are facing right now. The performance of the defensive system that an enterprise company is using directly impacts whether this company can have a profit gain or loss; furthermore, this affects the customers' satisfaction about the company's products and services. This threat can harm the company and should not be ignored. Right now the basic service that Anti Virus software and Threat Management System can provide and their performance are functionally the same, but the effective factor of how each different companies use them may yield a big difference. Hence, knowing how to control the main factor of the information security threat of the company and knowing how to provide the best and the most secured strategy according to the threat to solve any possible future threat such that the loss of profit can be minimized, will be the most important aspect for an enterprise company to be succeeded.

This research was conducted by interviewing with five experienced enterprise security maintenance experts at first. From the conservation, we have learned that the main factor of the information security is not depending on the amount of budget that the company has spent on anti-virus software. In fact the strategy type that the company uses for information security is the main reason. This includes the relational model between the users and the information security members, the quality of the information security members, the support of information security strategy from the top manager, and etc. These are more important factors.

We have then conducted a survey among the customers from one of the famous anti virus software in Taiwan. We have sent out 1910 questionnaire mails and online survey invitation emails, we have collected back 102 copies of valid questionnaires (5.3% of the

total). The questionnaire contains two parts: the characteristic of the company (including the background of company, the virus infection situation in the past three years, the anti virus system, the present situation of information security management), and the performance evaluation of the anti-virus system (which one(s) out of the four anti-virus techniques that the current company is applying: using anti-virus software, monitoring and filtering, using some tools for tracing, and the separation of local area network. Which one(s) out of five security process strategies that the company is using: weakness management, virus pattern deployment, account management, permission of using application and network, and response and restore process. And the factor of company: the responsibility and ability, the obedient, and the weight that was put for educational training.) Using the infection number of virus, the impact severity of virus spread, the quantity of detectable virus, and the number of detectable infection events as dependent variables, along with using the situation of company and each items in anti-virus ability evaluation as single factor or multiple factor variant analysis, the analyzed result shows that the size of companies and the security process strategies such as the use of anti-virus software, weakness management, and account management, are the main factors of the infection number of virus. The characteristic of the company such as the size of companies and its network management, the security process strategies such as the use of anti-virus, weakness management, and virus pattern deployment, and the educational training are the main reasons of affecting the severity of virus spread. The size of company, the use of anti virus technique such as the use of anti-virus software and the monitoring and filtering, and weakness management are the main factors of the number of detected virus. The size of company, weakness management, and the educational training are the main factor of the number of events of detected infection.

According to the analysis of the threat of information security that an enterprise company would face, this research has built and developed a related evaluation model. The result from this research not only can provide a reference for companies and software designers when they evaluate their enterprise information security, but also suggest a new direction for future research.

Keywords: Information Security, Virus, Cyber-Threat, Vulnerability Management