航空技術學院學報　第十四卷　第一期　第 35－44 頁（民國一〇四年）
Journal of Air Force Institute of Technology, Vol. 14, No. 1, pp. 35-44, 2015

因應網路惡意程式威脅資訊安全風險評估理論分析研究

Modern Information Security and Computer Risk Management Technologies Against Network Cyber Malicious Treats

吳嘉龍

Chia-Long Wu

和春技術學院資訊工程學系專任教授兼系主任

Professor and Director of Computer Science and Information Engineering Department, Fortune University

摘要

隨著科技的發展，藉由網際網路世界各地的電腦主機透過網際網路連結成為一個巨大的資訊網，但在其中所衍生出來的網際網路系統安全漏洞之問題卻使得資訊的安全傳遞承受了相當大的威脅。網際網路已經變成生活的一部份，各個公司及政府部門更是依賴網路的運作，此時如果攻擊者惡意程式攻擊對於組織或是政府單位使其癱瘓的話，其所造成的損失將不亞於傳統戰爭，因此我們不得不小心謹慎。隨著資訊科技日新月異，資訊化愈發深入公司組織與民間，資訊安全與風險管理儼然成為不容忽視的重要議題。在享受資訊化便利性的同時，必須注意相關資訊資產是否受到妥善保護，並深思背後可能引發的風險問題。如何善用有限資源與有效落實資訊安全管理，是現代科技的重大挑戰。資訊安全機制必須妥善保護資訊相關處理設備、系統與網路的機密性、完整性與可用性，不受各種威脅的影響，並將可能的衝擊與損害降至最低，以確保單位組織的正常營運與發展。

關鍵字：風險評估、資訊安全、網路管理、惡意程式攻擊、電腦緊急應變。

Abstract

With the development of technology, the rapid transfer of information has become a key issue for today's world. With the host server, computer can be connected to Internet all over the world to become a huge information network, but the problem of Internet security vulnerabilities in the system which are derived from the transfer of information is making a secure bear a considerable threat. Internet has become a part of life, companies and government departments is dependent on the operation of the network at this time if the attacker or malware attack government units for the organization to make it paralyzed, then they have caused the loss will exceed traditional war. As information technology advances, the more in-depth information technology companies and civil organizations, information security and risk management have already become an important issue can’t be ignored. Security mechanisms must be properly protected information and related processing equipment, systems and network confidentiality, integrity and availability, is not affected by a variety of threats. Enjoy the convenience of information technology at the same time, we must pay attention to the relevant information is properly protected assets, and ponder the risks that may arise behind.

Keywords: Risk assessment、information security、network management、malicious code attack、computer emergency response.

1. 前言

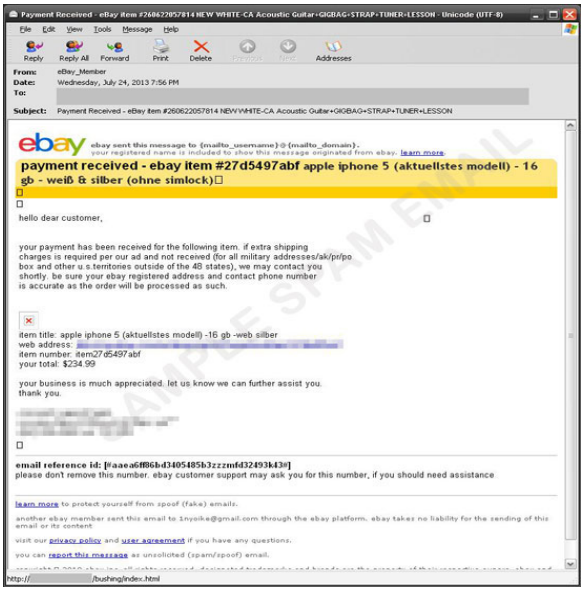
根據 FBI 調查統計 2001 年的受訪者，有 70%的比例為內部安全意識缺乏與不當使用所致。英國官方統計報告「2002 年資訊安全入侵調查」指出，在規模較小的公司裡，最重大的系統入侵案件有 32%是內賊所為；在大企業，因內部員工所造成重大系統入侵案件更達到 48%。2002 年 9 月偽卡集團涉嫌勾結財政部所屬的財金資訊公司工程師，盜取客戶信用卡內外碼資料高達一百萬筆以上及金融卡資料，顯見人員資安意識不足產生的資安威脅。而美國因應資訊安全與惡意程式攻擊威脅發展，小布希總統於 2002 年已簽屬總統另要求各部門制定網路攻擊策略。2011 年美國國防部公布新戰略，把美國可能遭受的嚴重網路攻擊定位成戰爭行為，並進行包括網路與傳統等攻擊武器反制作為[1-2]。

2010 年 1 月 12 日，Google 報導了公司遭到網路攻擊，該文報導更指出，極光行動（Operation Aurora）是 2009 年 12 月中旬可能源自中國的一場網路攻擊，遭受攻擊的除了 Google 外，還有 20 多家公司；其中包括 Adobe Systems、Rackspace、Juniper Networks、雅虎、賽門鐵克、諾斯洛普·格魯門、英特爾、摩根史坦利和陶氏化工（而部分來源顯示超過 34 家），調查人員追查到最根源發現，網路駭客們最初是利用廣為應用的 IE6.0 瀏覽器中一個未被發現的漏洞，對受害者進行攻擊的。事實上，中共所進行的網絡攻擊可以說是「組織嚴密、操作專業、技術尖端、具有高級軟體開發資源、深諳掌握攻擊目標情報，並具有在攻擊目標內部進行持久活動的能力，有時可長達數月之久。這場攻擊過後，Google 提出了它的新計劃，表示將在必要的法律範圍內，於中國運營一個完全不受過濾的搜尋引擎；同時 Google 也承認，如果該計劃不可實現，它將可能離開中國並關閉它在中國的辦事處[3-4]。

2010 年 2013 年 5 月，聯合國表示全球已有 46 個國家設立了網路部隊，新形態戰爭指的是網路駭客有組織性目標明確的惡意攻擊，攻擊行動透過長時間規劃、情蒐、佈署與分析針對於攻擊目標找出安全漏洞與弱點，因應於此，美國於 2012 年將資訊戰爭納入第五作戰空間。2013 年 5 月臺灣國家檔案局政府公文系統遭植入惡意木馬程式以及因海南事件而遭菲律賓駭客發動鍵盤戰爭。而依據大紀元中央社於 2014 年 12 月 14 日報導指出網路犯罪對飛航安全更構成嚴重威脅，歐洲航管組織（Eurocontrol），12 月初英國倫敦空域因電腦當機而關閉，航空業表示要在釀成災難性事件前對抗此威脅。值得注意的是，駭客、網路罪犯與其他恐怖分子正竊取資訊，甚至亂搞飛航系統而危害到生命安全。報導更指出，包括國際航空運輸協會（IATA）在內等 5 個機構聯手採取行動對抗駭客，並簽署新的網路安全協議，正式向網路犯罪宣戰，足以顯示資通網路安全已被視為國家甚至是國際安全問題[1-6]。

2. 網際網路惡意程式發展分析研究

Trend Labs 趨勢科技全球技術支援與研發中心 2013 年 8 月發表 Blackhole 漏洞攻擊會駭入金融帳戶破解系統安全機制 。這一波垃圾郵件所偵測到的變種名稱為 TSPY_FAREIT.AFM，它不僅會在感染的系統上竊取 FTP 用戶端程式帳號資訊，還會竊取電子郵件帳號密碼、瀏覽器儲存的登入資訊，「而且」還會利用一份預先準備的密碼清單，試圖以暴力方式破解 Windows 登入密碼。值得注意的是，這波垃圾郵件(SPAM)行動的垃圾訊息數量高達同時期所有垃圾郵件數量 0.8% 左右，相較於其他行動，此比例偏高，基本上，它會盜取感染電腦上的個人資訊，然後駭入使用者的金融帳戶，竊取個人資料，甚至破解系統的安全機制[7]。

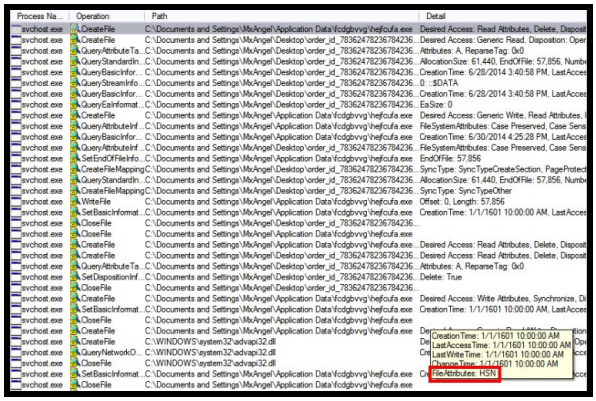


圖一、Blackhole 漏洞攻擊示意圖[7]

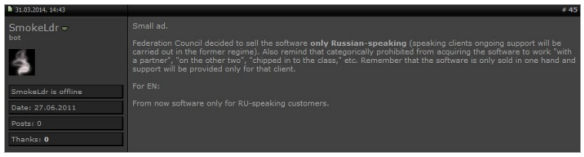
另一項值得注意的是，該行動所散布的惡意程式當中包含了 TSPY_FAREIT 資料竊取程式。TSPY_FAREIT 變種通常都是用於一些使用 Blackhole 漏洞攻擊套件 (BHEK) 的攻擊行動。這一波垃圾郵件所偵測到的確切變種名稱為 TSPY_FAREIT.AFM，它不僅會在感染的系統上竊取 FTP 用戶端程式帳號資訊，還會竊取電子郵件帳號密碼、瀏覽器儲存的登入資訊，「而且」還會利用一份預先準備的密碼清單，試圖以暴力方式破解 Windows 登入密碼。基本上，它會盜取感染電腦上的個人資訊，然後駭入使用者的金融帳戶，竊取個人資料，甚至破解系統的安全機制，圖一為 Blackhole 漏洞攻擊示意圖[7]。

W32.Ramnit 是賽門鐵克安全回應中心 2010 年偵測到的一種新蠕蟲。它能夠感染使用者電腦系統中的.exe、.dll 和.html 文件。W32.Ramnit 將自身加密之後附加到目的檔案中。當被感染的檔運行時，該蠕蟲會被釋放到目前的目錄並被命名為[InfectedFilename]Srv.exe，然後執行。同時在%\ProgramFiles%\目錄下增加一個 MNetwork 目錄。感染該病毒的電腦會試圖連接到網站 rmnz[removed]ed.com，從該網站下載.dll 檔註冊到系統中。該病毒主要通過行動儲存裝置進行傳播。傳播時，它會把自己複製到移動存放裝置根目錄下面的 Recycle Bin 目錄中，同時新增 autorun 檔以達到自動啟動的目的[8]。

根據 Smoke Loader 木馬惡意程式可以對感染主機做遠端遙控執行一系列包括下載到受駭主機地緣關係電腦惡意軟體安裝 (malware installing) 、偷取其他遠端存取主機（包括瀏覽器、即時通與電子郵件使用者）密碼等攻擊活動，圖二、圖三與圖四為 Smoke Loader 木馬惡意程式攻擊示意圖，最新攻擊 PROCMON 模組可下載及執行檔案可將電腦執行程序自動刪除並將電腦重新開機，相關其他模組可在 Tracking Cybercrime Blog 找到更詳細資訊[9]。



圖二、Smoke Loader 木馬攻擊示意圖[9]



圖三、Smoke Loader 木馬攻擊示意圖[9]

圖四、Smoke Loader 木馬攻擊示意圖[9]

APT-進階持續性滲透攻擊 (Advanced Persistent Threat，簡稱 APT) 針對特定組織作複雜多方位的網路攻擊且集中於間諜與竊取機敏資料，其影響程度雖大但攻擊範圍甚小，使得難以蒐集有用證據。攻擊者除了使用現成的惡意程式外亦使用客制化的惡意元件外，並建立一個類似殭屍網路的遠端控制架構而隱身其後。網路犯罪和網絡間諜之間的界限越來越模糊，藉由使用一般的惡意程式、漏洞與架構使得要區分與調查這類案件越來越困難[10]。

3. 資訊安全理論與風險管理技術探討

英國國家標準協會的 ISO/IEC 27001 資訊安全管理系統國際標準已成為業界最具公信力的資訊安全標準之一，其核心理念亦是風險管理。企業訂定資訊安全政策與目標時，應該與組織營運目標連結，建立一套認同理解的指標，並定期進行衡量與檢討。資訊對組織而言就是一種資產，和其它重要的營運資產一樣有價值，因此需要持續給予妥善保護。資訊安全可保護資訊不受各種威脅，確保持續營運，將營運損失降到最低，得到最豐厚的投資報酬率和商機。造成資訊安全事件的原因僅約25%是技術方案的解決，重要的是人性管理面上出現漏洞，資訊安全三要素分析如表一，表二為資訊安全風險相關名詞定義表。組織依據資訊安全政策、目標與實際經驗，以評鑑及測量過程績效，並將結果回報給管理階層加以審查。風險評估應基於固有風險及剩餘風險，採用定性與定量的評估方法，分析風險發生的可能性及衝擊程度，再據以決定如何管理。組織依據風險回應成本效益、可能性與衝擊降低幅度等因素，評估選用適當風險回應方案。控制項目為降低安全風險所需之程序規則或機制，表三為資訊安全風險評估分析表，表四為組織作業風險評估分析表，表五則為資訊安全控制措施分析表[11-13]。

表一、資訊安全三要素分析表

資訊安全要素	資訊安全要素內容
Confidentiality 機密性	保護資訊不被非法存取或揭露
Integrity 完整性	確保資訊在任何階段沒有不適當的修改或損毀
Availability 可用性	經授權的使用者能適時的存取所需資訊

表二、資訊安全風險相關名詞定義表

資安名詞	資安風險相關名詞定義
Threat 威脅	是指可能對資產或組織造成損害事故的潛在原因
Vulnerability 薄弱點	指資產或資產組中能被威脅利用的弱點
Risk 風險	特定威脅事件發生的可能性與後果的結合
Risk Assessment 風險評估	對資訊和資訊處理設施的威脅、影響和薄弱點及三者發生可能性的評估
Risk Management 風險管理	可以接受的費用識別、控制、降低或消除可能影響資訊系統安全風險的過程
Security Control 安全	安全風險是指威脅事件對資產造成潛在傷害或損失

控制	程度，安全控制為降低安全風險慣例、程序或機制
Residual Risk 剩餘風險	剩餘風險或稱為殘餘風險，指實施安全控制後，剩下的安全風險
Applicability Statement 適用性聲明	適用於組織需要的目標和控制的評述
Risk Response 風險回應	評估選用適當的資安風險回應方案包括風險規避、風險抑減、風險分擔或風險承受

表三、資訊安全風險評估分析表

資安風險評估	資訊安全風險評估分析
漠視風險	漠視資訊危機的存在，遭受的風險損失將無法估計
降低風險	找出風險，使用適當的解決方法，降低可能的損失
接受風險	在可接受的範圍內，承擔風險所帶來的損失
轉移風險	將風險所帶來的損失轉移給第三者

表四、組織作業風險評估分析表

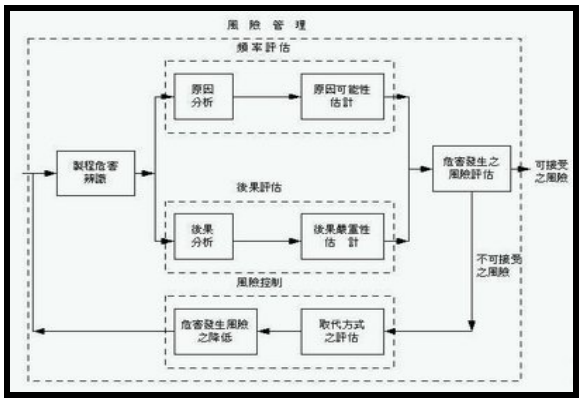
作業風險目標分類	組織作業風險評估分析
Strategic 策略性	追隨組織使命或願景，並支援其達成的高層次目標
Operations 營運	資源使用的效果與效率
Reporting 報導	財務報導的可靠度
Compliance 遵循	相關法令的遵循度

表五、資訊安全控制措施分析表

資訊安全控制措施	資訊安全控制措施分析
Policies & Procedures 政策程序	政策揭示目標、職責、權限及從屬關係，程序則詳細列明內部運作流程、人員、文件及資訊流向等
Review 審視	由上司、同儕或其他相關部門人員等審視並提出意見
Authorization 授權	作業須獲得上級同意後才可以進行
Physical Controls 實體控制	實體管控，例如現金鎖在保險櫃、電腦資訊裝備固定資產貼上標籤並造冊列管等
Exceptional Reporting 異常報告	發現異常情形（例如：系統被入侵、交易金額異常等）時，向相關單位或人員報告
Segregation of Duties 職責分離	同一作業的準備、審核、執行與記錄分別由不同人員負責

資訊系統之定義為負責蒐集、處理、傳送、儲存及流通資訊的一組資產，其內容包括硬體、軟體、網路、員工、實體環境及組織架構，特別強調資產間之關連，並加以群組，以獲得一致的防護水準，用以協助政府機關決策、協調、控制、分析及執行。每個資訊系統可能存在其脆弱性，但若是無威脅可以利用該脆弱性，將不構成風險；但是如果威脅利用該資訊系統所存在之脆弱性，則可能對政府機關造成衝擊。因此政府機關必須採取適當的「控制保護措施」，藉以消弭脆弱性或者阻止威脅之利用，以降低風險；惟風險很難完全消除，務必講求成本效益，使「剩餘風險(殘餘風險)」

降低至機關可接受之水準。作業風險管理必須配合組織目標的達成，管理階層首先必須確立組織使命（Mission）或願景（Vision），據以設定策略性目標（Strategic objectives），進而選擇策略訂定目標，而目標訂定則是一種由上而下的歷程，我國於 88 年 9 月 15 日訂頒行政院及所屬各機關資訊安全管理要點，圖五為作業風險管理流程圖[10-13]。



圖五、作業風險管理流程圖

4.資訊安全標準與安全管理應用發展

行政院研考會於 99 年訂頒資訊系統風險評鑑參考指引，並於 100 年修訂，旨在說明「行政院及所屬各機關資訊安全管理要點」之「各機關應依有關法令，考量施政目標，進行資訊安全風險評估，確定各項資訊作業安全需求水準，採行適當及充足之資訊安全措施，確保各機關資訊蒐集、處理、傳送、儲存及流通之安全」的內容。ISO/IEC 27001 是國際標準局 ISO 組織驗證規格，ISO27003 是新的 ISMS(Information Security Management System) 標準由英國標準局 BSI (British Standard Institute)的資安標準 BS 7799-2 發展而來，ISMS 是一套有系統地分析和管理資訊安全風險的方法，其重要性為表達提供安全營運環境的決心與承諾。此方法讓組織具備安全管理能力、建立「安全等級」資訊管理制度與為資訊架設一套安全防護機制。對外防範病毒及駭客入侵遭受攻擊時，系統仍可維持正常運作能力。經濟部標準檢驗局配合行政院資通安全會報資通安全管理政策，於 102 年 10 月 31 日公告 CNS 27005「資訊技術－安全技術－資訊安全風險管理」，該標準係參考 2011 年 ISO 27005 修訂版，為資訊安全管理系統(Information security management system，ISMS)系列標準之一，該標準提供資訊安全風險管理重要指導綱要，新增風險管理高階觀點，調整資訊安全風險評鑑內容結構，以增加使用者參考使用之方便性。值得注意的是，CNS 27005 內容包含資訊安全風險管理過程概觀、全景建立、資安風險評鑑、資安風險處理、資安風險接受、資安風險溝通及諮詢、資安風險監視及審查，適用於管理可能危及組織資訊安全之風險的所有型式組織；有關資通安全相關國家標準詳細資料內容，請查詢經濟部標準檢驗局網站，表六為 CNS 27000 資訊安全技術系列標準說明表 [14-16]。

表六、CNS 27000 資安系列標準說明表

資安技術系列標準	CNS 27000 資安系列標準安全技術說明
CNS 27000	資訊安全管理系統－概觀及詞彙
CNS 27001	資訊安全管理系統－要求事項
CNS 27002	資訊安全管理之作業規範
CNS 27003	資訊安全管理系統實作與指引
CNS 27004	資訊安全管理－量測
CNS 27005	資訊安全風險管理
CNS 27006	提供資訊安全管理系統稽核與驗證機構之要求

資料防護從實體文書時代環境直到當前行動化、虛擬化與雲端化時代一直存在且不斷

演繹更新的重大議題。風險評估的方式可應用在整個組織或部份，不但單獨的資訊系統，特定的系統的一部份均可以應用。進而施以有效益之控制措施在有限的資源下施以控制措施之成本，優先針對具重要性及時效性之衝擊施以控制措施，其餘者接受或轉移風險。風險評估包括評量分析每一弱點可能有多個威脅項目（例如存取控制不當可導致資料遭竊取及遭置後門程式當跳板之威脅），且同一威脅項目可能針對不同的弱點（例如病毒威脅針對系統漏洞及防毒軟體失效弱點起作用）。在此，資安威脅特別強調利用資訊資產既有存在的脆弱性，以便成功地造成資訊資產的傷害或者損失，例如：未經授權的入侵、揭露、修改、毀壞造成資訊無法使用或損失。威脅可能是環境(天然)或人為因素，而人為因素中可分為意外或故意兩種狀況。一般而言，控制措施的性質可分為三種：預防性措施（Preventive Control）、偵測性措施（Detective Control）及矯正性措施（Corrective Control）；預防性措施是預防問題發生，偵測性措施是發現問題就通知，矯正性措施則是發現問題就改正。值得注意的是，隨著大環境的改變，加上各種推陳出新技術的推波助瀾，使得資訊安全不論攻與防都出現了極大的變動。如果存在於資訊系統中之脆弱性遭曝露後將會導致風險的增加，同時如果威脅可以利用已遭曝露的脆弱性，也會增加機關之風險。其中個資法的全面實施刺激了全新資安意識、資安策略、資安投資與資安產業發展。由於現代科技發展快速，網路基本頻寬的增加，及隨身碟、Web Mail與網路硬碟儲存空間的愈來愈大，隨即敏感性與個資機密資料也可方便迅速地被有心員工外洩而出，若缺乏完善的日誌追蹤與稽核機制，將無法追查出洩密人員與相關資訊，也將造成單位組織莫大損失。因為外洩管道如此多元，所以完備的資料外洩防護機制須分別部署在網路閘道端、郵件端、Web 端、端點設備與資料庫端等各個面向。隨著雲端運算興起與手持裝置大行其道，讓資安管理更加艱困，因為許多雲端應用與行動 App 可將資料儲存在雲端上。許多單位組織及政府部門為了節省成本，採用雲端運算及 Google Drive、Dropbox 等雲端儲存服務，這類服務強調可以同時在 PC、筆電、智慧型手機或平板電腦之間進行文件資料的同步與分享，雖然極其方便且效率十足，但也成為讓資料外洩問題愈益嚴重的溫床[7-13]。當前有愈來愈多內部及外部的網路罪犯，會透過 SSL 連線加密來規避偵測並散布惡意程式。例如當前駭客會在「命令與控制」(Command & Control)伺服器及被植入惡意程式的受害電腦之間，建立 SSL 加密通道，進而將下達的指令，乃至資料竊取或其他攻擊的意圖及行為隱藏起來。除此須另行搭配 SSL Proxy 來加強既有資料外洩方案檢測 SSL 加密內容的能力外，或許搭配不同資料外洩的組合性方案才是降低敏感資料洩漏風險的最佳解決之道。從外部防禦而漸趨內部安控的趨勢，隨著組織及政府逐漸重視資料外洩防護後，整個防護重點與方案取向，也從一開始只以加解密機制來因應外部威脅的做法，逐步藉由權限控管機制來防止內部有心員工非法竊取機密的行為；表七為資料外洩防護(Data Leakage Protection)建議分析[17-18]。

表七、資料外洩防護建議分析表

資料外洩防護分類	資料外洩防護建議分析
內部安控與稽核	就需求來評估各類型手持與行動裝置的風險程度，給予不同層級的安全控管及防護
依需求優先順序訂	須就需求優先順序考量將有限資源先放在最急迫的

定規則	安全防護點上，然後再循序漸近地進行其他防護面向的加強工作，進而逐步完善整體資料外洩防護的能力
資安政策宣導稽核	除了導入良好的資料外洩防護方案外，須加強對於敏感資料保護政策的擬定、宣導，培訓與稽核
兼顧組織面、流程面及技術面	從組織面、流程面及技術面做好全面性的資料外洩風險管控；組織面包括人員、設備與裝置，以及本地端、公開場所等不同環境，流程面則涵蓋所有內部工作流程及之間作業流程的管控
整合性資料外洩防護(DLP)機制	單純只靠 DLP 並無法有效解決資料外洩問題，必須從源頭著手然後配合監測、阻絕及還原機制，如此才能在不斷循環性地調整資安政策與管控措施下，達到完整有效的資訊安全防護機制
強化 SSL 封包檢視能力	隨著 Google、Yahoo 各項服務均採用 HTTPS 後，當前 HTTPS 流量已佔網路流量的 40-50%，唯有透過 SSL Proxy 的部署，才能控管 100%的 Web 流量
因應巨量資料精準資料外洩防護機制	隨著巨量資料時代來臨，著當前在組織內部資料越來越多的情況下，資料安全管理也會隨之更加嚴峻，換言之，需要建立一套更「精準」的數位資料防護機制
行動化以及雲端架構因應	如今雲端與行動化所帶來的工作行為改變，正劇烈改變企業今後發展的模式與方向。如何讓使用者可以享受行動化帶來的便利，同時仍可確保資料的安全性，會是下一階段的重大課題

5.結語與未來因應作為

現代戰爭形態已步入高科技和電子化戰爭，但保密的落實與否攸關戰爭的勝負。當前國家安全所面臨最大的威脅來自中共，近幾年來政府機關不斷遭到中共駭客、網軍攻擊，其蒐情管道更以高司幕僚、科研及機敏單位為首要目標，其中國軍機密資訊向來是中共網軍竊密的重點，對各項機密資訊的竊取也積極進行。國際電腦安全協會（ICSA）報告曾指出，60%的洩密事件，是來自組織內部，只有 15%是來自外部入侵，在科技設備不斷精進的現代，資訊不斷地更新與網路蓬勃的發展，導致訊息的傳遞速度與容量遠遠超越我們的想像，雖然帶給我們便利與生活品質提升，也因而衍生許多新的社會與國家安全問題。資訊時代所帶來的「虛擬攻擊」已成為中共各種滲透、分化及竊密的蒐情伎倆之一。民國 103 年 5 月 19 日美國司法部以「網路間諜」罪名起訴五名共軍軍官，指控他們透過網際網路竊取美國核能、金屬及太陽能等高科技產業機密，聯邦調查局追查這五名共軍軍官，都是來自先前曝光的共軍總參三部第二局一個代號為「61398」的網軍部隊。而美國麥迪安（Madiant）網路安全公司曾於去年發表報告指出，這支中共網軍部隊六年來涉及 114 起入侵竊密案件，其中在臺灣就有 2 起，並持續透過外圍的駭客集團對全球發動進階持續性滲透攻擊，積極蒐集各國政府機密資訊與智慧財產[19-20]。

研究指出，造成資訊安全事件的原因僅約 25%是技術方案的解決，重要的是人性管理面

上出現漏洞。惡意程式攻擊事件層出不窮，中央社華盛頓 2014 年 11 月 6 日綜合外電報導美國資訊安全業者發現新惡意程式 WireLurker，能透過蘋果公司（Apple）的電腦感染 iPhone 智慧手機等行動裝置，引起使用者關切。蘋果發表聲明表示，已採取行動防堵。針對於網路威脅，歐洲聯盟電腦網路安全機構在雅典舉行歐洲歷來最大規模的演習，以防範針對歐洲公用事業設施及通信網絡攻擊。美聯社報導，歐洲網路暨資訊安全局（European Network and Information Security Agency）局長指出，2014 年 10 月舉行演習，有 29 個國家、200 個機構參加，演練並針對「重要基礎建設」攻擊情況因應。針對資安威脅日增，除了實體隨身碟及外接式硬碟外，從傳統電子郵件、即時通訊、網站，到 Line、行動 App、雲端儲存與各類型手持與行動裝置全都是資料外洩的可能管道。 資訊安全管理目的在於確保資訊資源之合法存取，在所有可能遭受資訊攻擊的階段，提供完整、未中斷之資訊系統運作。有鑒於此，必須加強隨身碟、網路及郵件等常見外洩管道的安全控管機制，在駭客與內賊的因應上，應具備郵件與 Web 雙向進出管道內容的檢測機制，才能杜絕任何內外資料竊賊的不軌之舉[21-22]。

參考文獻

[1] 財團法人國家實驗研究院，科技政策研究與資訊中心，國家資通安全會報資通安全資訊網，第201412010期資通安全電子報，2014年12月16日存取。

[2] 維基百科，極光行動，http://en.wikipedia.org/wiki/Operation_Aurora，2014年12月16日存取。

[3] 人民電子報，恐怖的中共「極光行動」，http://www.renminbao.info/，第 223 期，2014 年 12 月 16 日存取。

[4] 資訊管理中心，國家中山科學研究院，新形態戰爭集資安防護策略探討，新新季刊第 42 卷第 1 期，第 226-232 頁。

[5] 資訊通信研究所，國家中山科學研究院，網路攻擊與防禦訓練系統之建模與模擬技術探討，新新季刊第42卷第2期，第210-213頁。

[6] 財團法人國家實驗研究院科技政策研究與資訊中心，國家資通安全會報，資通安全資訊網，第201412011期資通安全電子報，2014年12月16日存取。

[7] Trend Labs 趨勢科技全球技術支援與研發中心，新的 Blackhole漏洞攻擊會駭入金融帳戶,破解系統安全機制，2013 年 08 月 14 日。

[8] ITHome，諾頓病毒週報：小心可執行檔被蠕蟲W32.Ramnit附身，2010年2月2日，http://www.ithome.com.tw/。

[9] Kimberly，Posted at Rootkits，stop Malvertising，Analysis of Smoke Loader，http:// stopmalvertising.com/rootkits/analysis-of-smoke-loader.htmll，2014年7月1日。

[10] Trend Labs 趨勢科技全球技術支援與研發中心，認識APT-進階持續性滲透攻擊(Advanced Persistent Threat, APT)，2012年3月7日。

[11] 廖君美，企業風險管理與資訊安全機制設計，財金資訊季刊，No.75，23-31頁，2013年7月。

[12] 行政院，行政院及所屬各機關資訊安全管理要點，1999年9月15日台88經字第34735號函訂頒。

[13] 賴溪松，資訊安全稽核，國立成功大學計算機與網路中心，http://www.icsc.ncku.edu.tw，2014年12月16日存取。

[14] 財政部財政資訊中心，財政部暨所屬機關（構）資訊安全管理準則，2002年6月訂頒，http://www.fia.gov.tw/，2014年12月16日存取。

[15] 行政院研考會，資訊系統風險評鑑參考指引(修訂)v2.0，2000年。

[16] 行政院國家資通安全會報，資訊安全風險管理國家標準規範(更新版)，2013年10月31日。

[17] 資安人科技網，Information Security，14位資安專家-分享資料外洩防護導入分析與建議，http://www.informationsecurity.com.tw，2014年10月30日。

[18] 資安人科技網，Information Security，資料外洩防護 2大面向、9大建議：14位資安專家分享，http://www.informationsecurity.com.tw，2014年10月31日。

[19] 王弘，保持高度警覺 確保資訊安全，青年日報論壇，2014年12月12日。

[20] 青年日報，防堵新惡意程式蘋果稱有行動，青年日報國際即時報導–中央社新聞，2014年11月7日。

[21] 青年日報，防網攻歐盟舉行網路安全演習，青年日報國際即時報導–中央社雅典新聞，2014年10月31日。

[22] 政戰局保防安全處，確遵資安保密 杜絕機密外洩，青年日報報導–莒光園地，2014年7月21日。