樹德科技大學資訊工程研究所

碩士論文

以 CNS27002 資安規範探討基層公務機關之教育訓練

Analysis Education and Training Procedures for Primary Public Organizations Based on CNS27002 Information Security Standard

研究生：閻一平

指導教授：林峻立教授

中華民國九十九年六月

以 CNS27002 資安規範探討基層公務機關之教育訓練

Analysis Education and Training Procedures for Primary Public Organizations Based on CNS27002 Information Security Standard

研究生：閻一平
指導教授：林峻立博士

樹德科技大學
資訊工程系碩士班
碩士論文

A Thesis
Submitted to Department of Computer Science and Information Engineering
College of Informatics
Shu-Te University
In Partial Fulfillment of the Requirements
For the Degree of
Master
in
Computer Science and Information Engineering

June 2010
Kaohsiung Taiwan, Republic of China

中華民國九十九年六月

樹德科技大學博碩士論文授權書

本授權書所授權之論文為授權人 閻一平 在樹德科技大學 資訊 學院 資訊工程 系所 ___ 組 98 學年度第 二 學期取得 □博士 ■碩士 學位之論文。

論文名稱：以CNS27002資安規範探討基層公務機關之教育訓練

指導教授：林峻立教授

授權事項：

壹、授權人（研究生）及共同授權人（指導教授），以下簡稱授權人等。

貳、電子全文公開存取之時間及授權方式

一、校內：授權人等同意無償授權樹德科技大學（請勾選下列一個選項，若未勾選任何選項，則視為立即公開）：

■ 立即公開　□ 一年後公開　□ 二年後公開

二、校外：

1. 請勾選下列一個選項（若未勾選任何選項，則視為立即公開）

■ 立即公開　□ 一年後公開　□ 二年後公開　□ 不公開

2. 若勾選以上任意一個公開選項，請勾選下列授權方式（若未勾選任何選項，則視為無償授權）：

□ 有償授權　■ 無償授權

（若勾選有償授權，則權利金捐贈學校。）

參、若授權人等同意論文電子全文公開，亦即同意樹德科技大學將上列論文全文資料以微縮、數位化或其他方式進行重製收錄於資料庫，並以電子形式透過單機、網際網路、無線網路或其他傳輸方式進行檢索、瀏覽、下載、傳輸、列印等。樹德科技大學在上述範圍內得再授權第三人進行重製。

肆、以上之所有授權均為非專屬授權，授權人仍擁有上述授權著作之著作權。授權人擔保本著作為授權人所創作之著作，有權依本授權書內容進行各項授權，且未侵害任何第三人之智慧財產權。如有侵害他人權益及觸犯法律之情事，授權人願自行負責一切法律責任，被授權人一概無涉。

伍、若發生本授權書與論文系統授權項目不符時，授權人等同意樹德科技大學依本授權書修改論文系統之授權資料，以符合本授權書之初衷。

授權人簽名：閻一平（研究生）　共同授權人簽名：林峻立（指導教授）

中華民國 99 年 8 月 16 日

樹德科技大學
研究所碩士班
論文口試委員審定書

本校 資訊工程系 碩士班 閻一平 君

所提論文 以 CNS27002 資安規範探討基層公務機關之教育訓練

合於碩士水準，業經本委員會評審認可。

口試委員：溫翔安　楊政道

指導教授：

系所主任：

中華民國　九十九　年　六　月

樹德科技大學資訊工程研究所

學生：閻一平　　指導教授：林峻立

以 CNS27002 資安規範探討基層公務機關之教育訓練

摘 要

自資訊科技快速的發展，造就網際網路的興起，各類的資訊設備也日新月異，使得人類的生活方式與空間距離也日趨方便近在咫尺。但個人隱私與資訊安全保護能力亦趨受到重視，特別是防止網路上洩露、盜取、入侵及犯罪所引發的資訊安全維護能力也受到疑慮。縱使投入大量的資金更新及強化資訊設備(環境)，未必可化解危機。因此，資訊安全最重要的課題之一即為教育及認知，要如何確保資安教育能有效的建立資安概念，以防範資訊安全類案再生，即是本研究的方向。

本研究係依我國資訊安全管理之作業規範(CNS27002)為問卷藍本，並以基層人員為對象，研究其對資安概念瞭解程度及教育規劃之探討。本研究以 200 份問卷調查為基礎，經初步分項統計顯示，未受過資安教育訓練相關課程，已達到資安概念標準僅佔 17%，未達標準者高達 83%；而受過現行資安教育訓練相關課程之基層人員，達到資安概念標準僅佔 36%，未達標準者仍高達 64%。顯見目前的資安教育課程，已無法使基層人員的資安概念隨著教育訓練課程增加應有的效益。本篇最後針對現行資安教育課程提出相關建議方案。

關鍵字：資訊安全、
資訊安全教育、
資訊安全事件、
資訊安全管理、
資訊安全管理之作業規範(CNS27002)

Analysis Education and Training Procedures for Primary Public Organizations Based on CNS27002 Information Security Standard

Student：Yang Yi Ping Advisors：Dr. Chun-Li Lin

A B S T R A C T

Since the development of information technology is rapid, the several types of information devices are change with each passing day. It let human life become more convenience and distance between each others becomes closer. The issues regarding to protect personal privacy and information security have been got increasingly attention. In particular, the abilities which is used to prevent the network leakage, theft, hack and crime are doubted. It may be useless to resolve the above problems even much money involves to update and strengthen the information equipment (or environment). Because the education and awareness are important issues in information security field, This study researches on estimating the current education for information security is effective enough to establish the users' concepts or not, and given some advises to avoid similar security risks arise again.

The questionnaire in this study is based on Code of practice for information security management (CNS27002) and the target of questionnaire is focus on junior officers. Their degree of understanding on the concept of information security can be detected by the questionnaire, as well as the planning of current education principle can be analyzed. In the study, the total of available feetbacks amounted to 193. The result which is analyzed is given as follows: the junior offices who have not received the related training course, only 17% understand of information security enough. On the other words, their are 83% offices (have notreceived the related training course yet) lack the concept of information security. It is surprising, even the officers have received the related courses, only 36% officers understand information security enough, there are 64% offers still not enough. Base on above result, the current information security education programs seems not effective enough for junior officers. The study proposes some recommend for improving current information security course.

Keywords:Information Security,
Information Security Education,
Information Security Events,
Information Security Management,
Information Security Management Operating Standards (CNS27002)

誌 謝

自高中畢業後即投入軍旅工作迄今；當工作遇到瓶頸後，總覺專業識能不足，常想利用公餘時間自我進修，確因自己主動性不夠，錯失多次進修的機會。因此，進修計畫往往只是空想而已。自 97 年初，工作單位長官多次鼓勵本人應運用公餘時間自我進修，除加強專業知能外，亦可運用校方學術領域及研究方式，結合工作經驗精進工作效能。

于 97 年初夏考取樹德科技大學資訊工程研究所後，便重拾學生的生活，不同的是要南北兩地奔波，往往需要在工作、學業及家庭上找尋平衡點。這兩年來研究所的學業過程中，最感謝就是我的指導教授林峻立老師，讓我學會如何蒐集資料、分析、研討等工作。在撰寫論文階段期間，更是不厭其煩的指導與修正，使我在論文撰寫、資料的彙整及研析方面，有更長足的進步與成長。其次，是工作單位的長官與同事，在課業期(中)末考期間，協助本人處理公務，讓我有充裕的時間研習課業。還有要感謝同事致軒從旁協助與指導問卷調查的蒐整及研析。當然還有這二年來，同班同學-俞揮與銘鍠，在我面對工作與課業壓力時，有他們的鼓勵及不厭其煩的指導，才讓我在課業及工作上能如此順利。

最後感謝的是我父母及妻兒，父母親深怕因工作與課業無法兼顧，除常常叮嚀生活要規律多注意身體健康外，也幫我照顧兒子，父母恩難回報啊。此外，妻子綿芳與二位可愛的兒子-天立、天正，在我這二年就學期間，也常常犧牲她們假日休閒的時間，陪著我一起研習課業，也是辛苦妳們；您們的鼓勵、關懷及恩情會永記銘心。

閻一平 2010.6.27

目 錄

表 目 錄

圖 目 錄

一、緒論

電腦及網路的快速發展，為我們生活上帶來許多的便利，隨著對資訊科技的依賴與日俱增，且能夠享受「多用網路、少走馬路」的好處；不過當我們享受這種種的方便之餘，卻有一些不法份子(駭客)為了自己的利益，趁機利用各種管道來竊取機密資訊或破壞設備。這種破壞對人們的工作與生活便產生更大的衝擊，不但會造成個人資料的遺失，甚至導致系統癱瘓，影響企業或組織的正常營運。因此，資訊安全問題隨著資訊科技的不斷創新而越趨複雜(潘天佑，2008)。要如何保護資訊的安全性已成為企業或組織非常重視的一項工作。然而要確保資訊的安全性，除了由管理面著手外，也要依單位的工作特性來全面性規劃資訊安全教育訓練課程，並以科技協助建立資訊安全管理制度及規律性的教育課成，惟有如此才能確實防範資訊安全事件再度發生(左豪官，2009)。

在2002年7月25日經濟合作及發展組織(OECD)理事會通過「資訊系統與網路安全準則」，提出認知(Awareness)、責任(Responsibility)、反應(Response)、倫理道德(Ethics)、民主(Democracy)、風險評估(Risk Assessment)、安全設計與執行(Security design and implementation）、安全管理(Security management)、安全再評估(Reassessment)等九項資訊安全政策高階指導原則，作為其會員國推動資訊安全相關政策、法令的參考準則(OECD,2002)。此外，美國於911事件後已突顯出資訊科技作為國家「關鍵基礎設施」的重要性。因此，美國特別將國家網路安全列為國土保安的重點，於 2002年12月提出「國家網路安全策略」(The National Strategy to Secure Cyberspace)，並以「防止對美國重要基礎設施的網路攻擊」、「減少足以造成網路攻擊的安全弱點」及「減少真正發生網路攻擊事件的傷害及復原時間」為目標。此外，美國國會於2002年12月通過「電子化政府法」，明定各機關應採取各種保護政府資訊安全之作為(吳倩萍，2006)。

網路世界今非昔比，再多的資安設備都仍難以抵禦有計畫的內部竊賊，人的問題若擺不平，資安問題也難太平(資安人，2010)。近幾年來，國內外政府、軍事單位、學校及企業的資訊安全疏漏，除個資外洩外，也造成金錢的損失及軍事機

密遭竊取，這些損失往往無法估計。尤其以軍方的資料，大多牽涉到限閱或機敏性的問題，所損及的不只是資料遭竊或金錢的損失，更嚴重的是危及整個國家的安全。網路犯罪案件層出不窮且逐年增加，顯現資訊安全防護工作的重要性(林翠娥、程毓明、鄭進興，2006)。

1.1 研究背景與動機

近年來，資訊事件的犯罪案例，由傳統的資料破壞到網(路)站的入侵、個資的盜取及資料庫的破壞，都顯示犯罪手法不斷的翻新。另依據台灣網路資訊中心(TWNIC)截至 2010 年 2 月 12 日，公布最新「2010 年台灣寬頻網路使用調查報告」指出，台灣地區上網人口約有 1,622 萬，共計有 16,217,009 人曾上網(整體人口 0-100 歲)，比 98 年(2009)1,582 萬人，增加約 40 萬人；12 歲以上之曾經上網人口有 14,669,915 人，曾經上網比例為 72.56%，比 98 年(2009)增加了 1.61 個百分點，其中曾經使用寬頻網路人數為 13,590,123 人，寬頻使用普及率為 67.21%，比 98 年(2009)增加 0.74 個百分點，以上數據顯示出台灣網路的使用情形已經非常普及，因此，資訊安全更是一項必須重視的重要議題(徐桂尼，2010)。

舉例來說，在 2003 年 3 月 28 日，總統府的網頁被一位高二的學生入侵，並加以更改假消息：四月一日愚人節為國定假日，造成民眾普遍困擾(石文南、林晨柏，2003)。連國家等級的系統，都可能會被駭客日以繼夜地測試漏洞而入侵，一般企業與各公家單位情況更可想而知。

不僅如此，現在電腦雖然普遍，但是民眾的資訊素養並沒有顯著提升。尤其網路使用的普及，造成很多人使用上並不會注意到自己的資料可能因為駭客的盜取而被有心人獲得。像有線上遊戲虛擬寶物被偷竊的消息，就是因為這些玩家不小心執行木馬程式，讓駭客可以偷取被害人的虛擬錢幣與寶物，雖然最後駭客被依違反妨害電腦使用罪而移送法辦，但也由此可以看出現在人對資訊安全素養之不足(教育部，2010)。

而網路上的系統，不僅是總統府這種國家等級的系統可能被入侵而讓一般民

眾誤解，連大型的網路入口網站也可能受到駭客持續測試密碼而有私人資料流出。以無名為例，幾件最有名的案例就是前黑澀會美眉容瑄的裸照，因為設置的密碼被駭客測試出來而被盜走，並且已經被散佈在各大論壇上，個人相信未來這些照片都會在網路上持續被公布，而且無法用公權力讓他消除(王昭濱，2007)。

而且無名系統因為過於龐大，當系統需要新增或更改功能時，很可能有資訊安全的空窗期。在 2007 年 4 月 14 日，無名小站新增功能，但因為功能發生異常，因此在 14 日凌晨的 5 點到 7 點，所有上鎖的相簿此時都可以讓人隨意瀏覽。因此很多人在這段時間也下載很多他人的私密照片，造成使用者的困擾。雖然事後無名小站已經修正程式，協理林弘全也表示因為是離峰時間，所以受影響的人數僅有數百人。但是由此也可以看出，資訊安全的重要，已經不是網站管理者所能控管，個人應該也要有基本的認知，並且不該將會造成困擾的照片、個資、文件等放在網路上，以免遭人破解下載，造成資安事件，並徒增自己與他人困擾。

1.2 研究目的

依據行政院主計處 97 年度遭遇資通安全事件概況調查統發現，國內電腦用戶於 97 年度(53.20%)發生過資安事件，其中仍以電腦病毒攻擊 53.20％為最，次為被植入後門程式 10.68％，再次為遭阻斷式攻擊(DDoS)2.96％。由此不難發現從外部入侵資訊系統的駭客所佔比例也只不是 13.64%，而因人員疏失所造成的資安事件仍是佔較高的比例(行政院主計處，2008)。

雖然資訊安全首重於資訊設備建置前的規劃，若人員對資訊安全的認知偏差或資安教育訓練及宣導不足時，縱使再嚴謹、高技術的資訊安全規劃，仍會不斷發生資安事件。因此，資訊安全教育訓練的工作，便是防範資訊安全的基本要件，更是杜絕事件發生的守門員。

近年來發生的資安事件均可看出，大多數人員對資訊安全認知往往是以直覺反應、自我作業方便為優先，對於是否違反資訊安全法規，就變得不是如此的重要。很多資安事件的肇生，往往是一念之間，如果說是觀念偏差也不至於如此，

若以人為疏失來說，又似乎輕藐了資訊安全教育的工作成效與方向。

1.3 研究範圍

….本研究係以基層公務機關人員為對象，透過問卷方式來先行瞭解基層人員對資安概念熟悉度後，再行分析教育規劃的方向，以做為資安教育訓練工作的基本依據及參考。

本研究對象共 200 人，均為單位從事資訊安全管理相關工作，概分執行階層、管理階層及領導階層等 3 個部分，以個人從事資訊安全實務工作經驗填寫問卷，可讓本研究清楚瞭解研究各階層人員對資訊安全的認知，並依問卷所得到的結果，提供給需求單位作為資訊安全教育規畫參考、應用與分析。

1.4 資安相關人員

公務機關概分為業務單位及幕僚單位，幕僚單位係以中央政府組織為主，本研究係以基層公務機關人員為對象，故幕僚單位不在此研究範圍內。一般基層公務機關均以業務單位為主，主要以提供資訊協助機關首長(領導階層)作為決策之依據。因此，將基層公務機關內部人員依實務工作為區分，概分為以下三類：

1. 領導階層(機關主官)：為機關之正副首長，其中副首長為機關資訊安全長。對於資訊安全的政策有 100%的決策權及執行權。
2. 管理階層：分為業務(非資訊主管職務)及資訊主管等 2 類。其中，資訊主管針對資訊業務及工作有較為正式的權威、責任及協商能力。
3. 執行階層：分為資訊人員、一般資訊業務人員及一般行政管理人員等 3 類，區分如后：

   (1)資訊人員：為機關內負責資訊軟硬系統應用及維護人員。如面對資安事件時，大多數人員均抱持「報喜不報憂」的心態，也因如此，常常造成不可彌補的資安事件及漏洞。另大多數資訊人員離職後，常將機關資訊資料攜出後，再以駭客身分侵入機關資訊系統，造成資料大量外洩。

(2)一般資訊業務使用人員：需透過辦公室之網路與電腦，經常使用資訊應用作業之人員。

(3)經常使用資訊應用作業之人員：係指機關內職務較為低階之人員，工作方面較不接觸資訊系統，如駕駛、工友等(吳倩萍，2006)。

另經常使用資訊應用作業之人員，因工作方面較不接觸資訊系統，因此不列為研究對象，於實施問卷前已先行排除；另本研究所謂執行階層，係以資訊人員為主，一般資訊業務使用人員僅透過資訊系統執行作業，與資訊人員不同，亦不列為研究對象，於實施問卷前亦已先行排除。

二、資訊安全規範及相關文獻探討

2.1 資訊安全的演進

從 1960 年代電腦才開始市場化，至 1980 年代初期，電腦在比較封閉的環境中由少數人操作，安全風險不高。大型電腦主機(Mainframe)的時代，資訊安全事件大多是『人為操作』錯誤造成的資料遺失，或是單位內部人員操守問題所造成的洩密(潘天佑，2008)。

個人電腦自 1980 年代逐漸普及化，影響個人私密的資訊安全問題也開始浮現。早期個人電腦並無存取控制(Access Control)的設計考量，因此無法保護資訊的完整性。另軟碟(Floppy Disks)也讓電腦病毒(Computer Viruses)開始出現，在 1982 年由一位 15 歲的美國學生 Rich Skrenta 寫在 Apple II 電腦上，在電腦開關機 50 次後，便受到病毒感染，而受到感染的電腦會在螢幕上出現一首打油詩。

網際網路(Internet)在 1990 年代迅速成長，因網路將個人電腦串接在一起，使電腦病毒的散播與駭客的攻擊更加快速及方便。Melissa 是 1999 年由電子郵件傳播的 Word 巨集(Macro)電腦病毒，是利用已受感染電腦的電子郵件通訊錄，發出 50 封病毒郵件。因此，在數小時內就可傳遍全球。如 Code Red 蠕蟲(Worm)就是利用電腦作業系統的瑕疵，在 2001 年 7 月 19 日以一天的時間感染全球 359,000 台腦，其攻擊速度與範圍皆駭人聽聞(潘天佑，2008)。

較早的電腦或網路破壞者，大多以炫耀技術或惡作劇為主。在 21 世紀蓬勃發展的電子商務卻以逐漸成為獲取非法利益的跳板。如 1999 年俄國駭客侵入 CD Universe 公司的網路，盜取 30 萬筆信用卡資料。再勒索 10 萬元美金未遂後，就以報復手段將數千筆資料公布在網際網路上。另 2000 年 9 月 Western Union 金融服務機構關閉網站 5 天，因為被駭客入侵盜走 1500 萬筆信用卡資料；後追查原因發現，駭客利用該公司系統維修時，防火牆關閉的 15 分鐘內入侵。

近年來資安事件頻傳且日趨嚴重，每次資安事件的發生，除了公務機關機密文件被外洩、盜取、竄改外，最嚴重的是莫過於個人資料(如信用卡、帳戶密碼等)外洩，造成個人不少的困擾(潘天佑，2008)。

美國有線電視新聞網頁(CNN.com)報導，引述國際電子商務顧問局(International Council ofElectronic Commerce Consultants，EC-Council)共同創始人兼總裁巴維希(Jay Bavisi)的話說:「要打敗駭客，需要有駭客一樣的想法。」EC-Council發言人巴特包赫(Eric Butterbaugh)說：「國防部人員不是學習如何侵入電腦，而是學習如何保護電腦網路免於駭客侵入。」這項訓練計劃名為「道德駭客資格認證(Certified Ethical Hacker Certification)」。據美國政府報告，2009 年上半年，國防部電腦遭駭客侵入將近 4 萬 5000 次。報告估計，2009 年駭客侵入次數較前一年(2008 年)增加 60%。為攔堵這些攻擊，五角大廈已花費約 1 億美元。巴維希表示，訓練著重教育學員侵入電腦的技術，學習使用與傳統駭客侵入電腦網路使用的相同工具和技巧。他說，基本概念是國防部人員將利用這項訓練，侵入國防部的電腦。當道德駭客發現有非道德駭客可能攻擊的弱點，就升高安全防護以消除潛在的威脅(資安資眼網站，2010)。

2008 年 9 月 28 日自由時報報載，某縣市警察局於個人電腦安裝了 P2P 分享軟體，導致警局公文、筆錄及個人資料外洩。經查發現為中北部某警局有 70 餘筆公文資料外洩到網路上。經分析研討後，肇生資料外洩除了個人電腦感染病毒、木馬程式以外，最有可能的原因就是該警局員警將公文攜回家中，利用私人電腦「公務家辦」，不慎由私人電腦內安裝的 P2P、BT、FOXY 等網路分享軟體，將公務資料外洩到網路上。究其原因，該員警對 P2P、BT、FOXY 等網路分享軟體的功能不瞭解，又將公務資料攜回家中「公務家辦」，因此肇生公務資料及個資外洩到網路上。且違反「電腦處理個人資料保護法」第 17 條規定，應對於受損之民眾應賠償其損失(行政院，2009)。

在回顧 2009 年資安事件年度大事(如圖 1)，國內以台灣大哥大電信公司，於 2009 跨年系統當機 5 小時，癱軟通信系統造成 2 萬名客戶求償及商譽損失。經檢調於 2009 年 10 月介入調查發現，是由台灣摃大哥大系統委外廠商諾基亞西門子通信公司(NSN)的離職員工所為。起因為該離職員工於 2008 年 3 月遭諾基亞西門子通信公司(NSN)解職，因此心生報復。該名員工先前被派駐台灣大哥大負責管理

維修「門號可攜認證服務網路系統」，在他離職前違約設定一組帳號密碼，並選擇在 2009 跨年時利用 3.5G 行動上網連上「門號可攜認證服務網路系統」，破壞主程式設定，並刪除資料庫中可攜號碼資料與連線登入紀錄，使得兩套系統無法同時作業。因此，造成 2009 年跨年當機 5 小時(資安人雜誌，2010)。

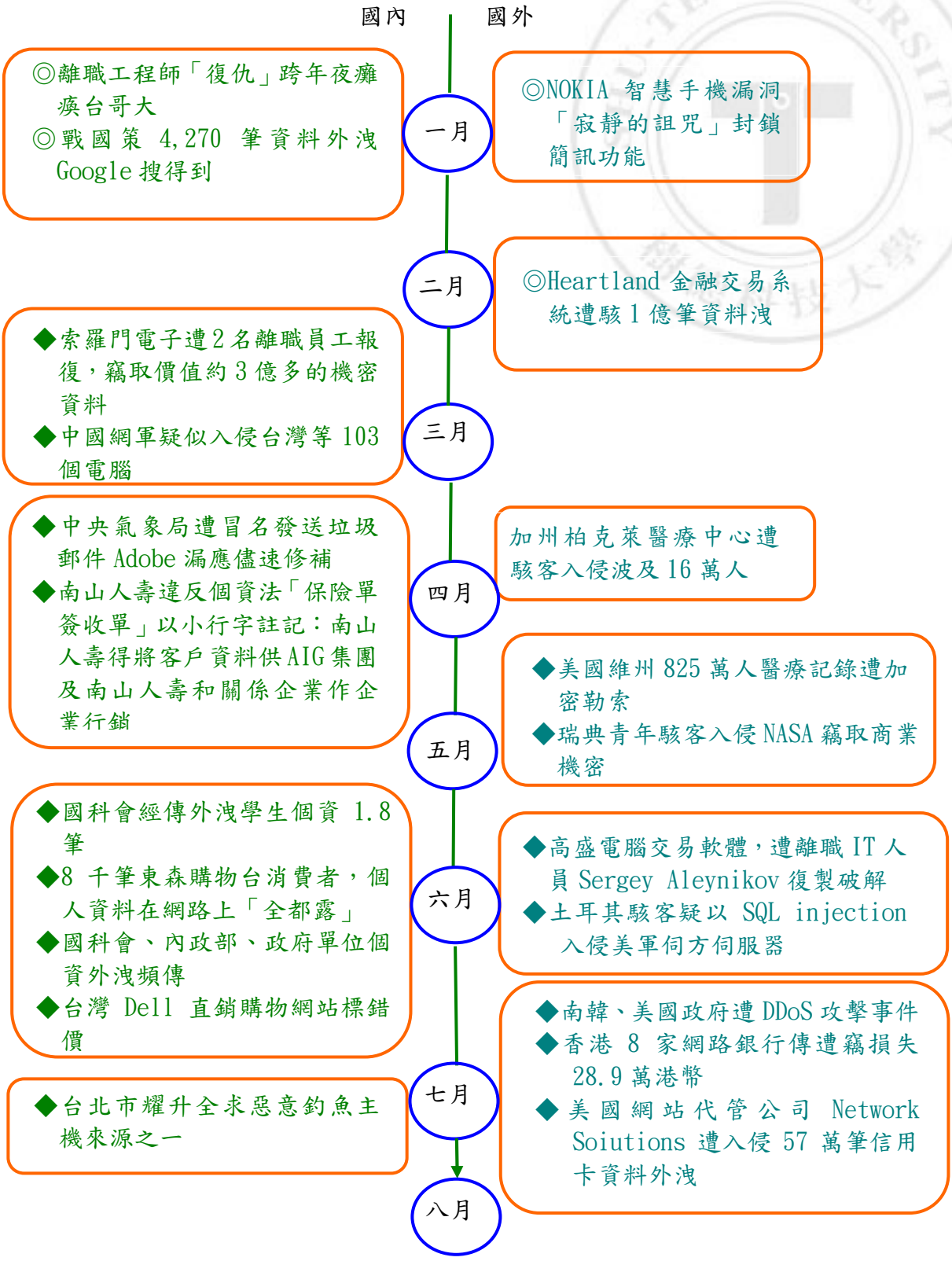

圖 1. 2009 年資安事件年度大事

資料來源：資安人雜誌，NO.67(2010.JAN/FEB)，頁 73-頁 74

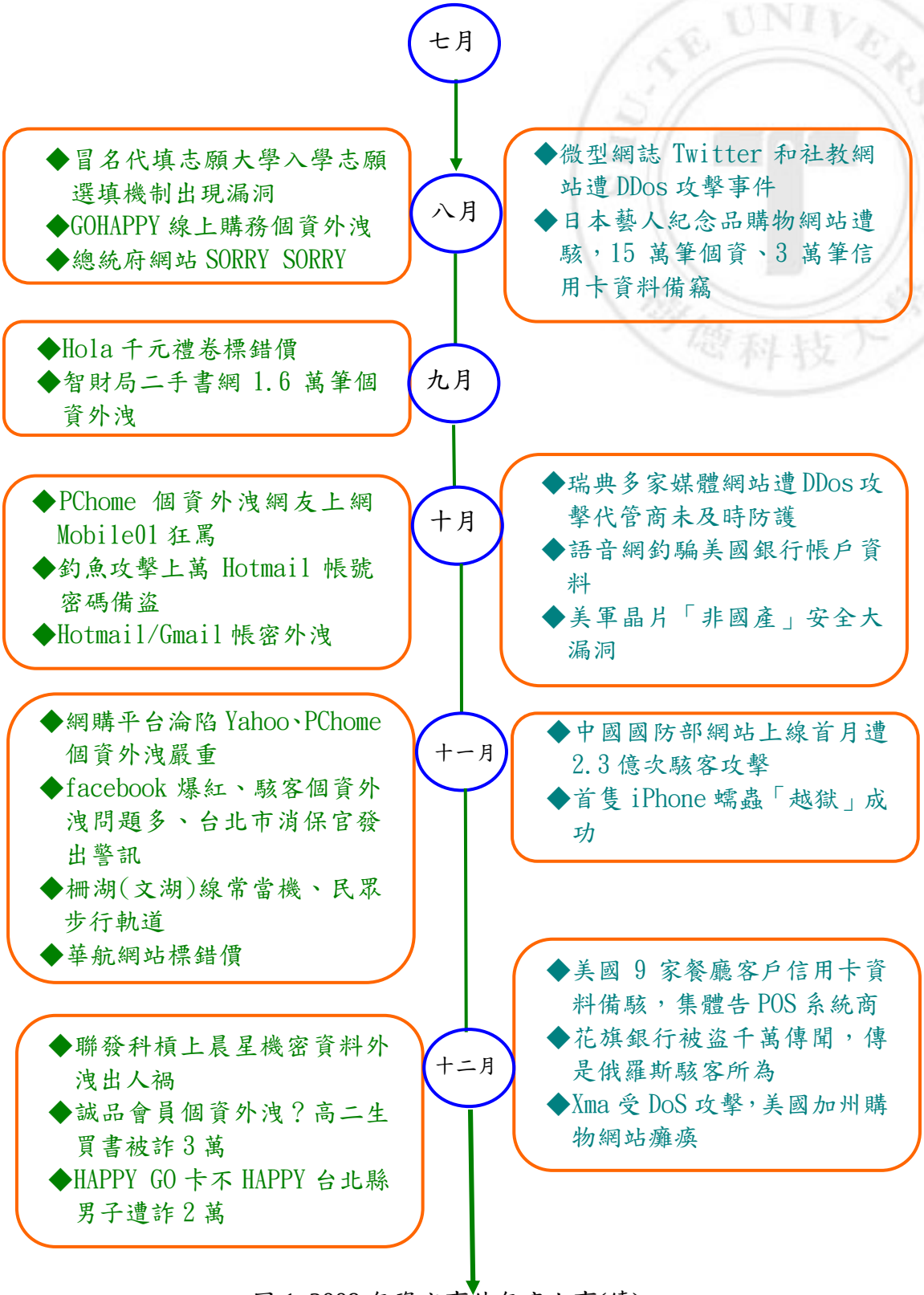

圖 1. 2009 年資安事件年度大事(續)

資料來源：資安人雜誌，NO.67(2010.JAN/FEB)，頁 73-頁 74

2.2 資訊安全應有的概念

在推動資訊安全宣導工作時，常常聽到的一句話：「推動資訊安全工作就是工作負單的增加，並影響單位原有的工作型態及模式」。因此，公務機關基層人員常抱著僥倖的心態-自認不會這麼倒楣，資安事件會發生在自己身上，或認為資訊安全工作已做得很完善。故當資安事件發生時，才驚覺事態嚴重，多筆機密資料已被盜取或破壞殆盡，甚至影響公務機關機密工作。也有人常常認為資訊安全問題可以「一次解決、永不外洩」的錯誤觀念，只要花大筆經費建置嚴謹安全無虞的防(毒)禦系統後，就可「一勞永逸，高枕無憂」。另外也常聽到錯誤的認知，只要購置資訊安全產品，靠強大的防毒軟體(Anti-virus)及防火牆(Firewall)，就足以防只駭客入侵及達到資訊安全的目的。其實，這些觀念都是錯誤的，除了建置完備的資訊防(毒)禦系統外，還必須將單位人員依工作性質不同，規劃相關的資訊安全教育課程及訓練，以強化基層人員資訊安全概念，以降低公務機關資訊危安事件。

美國五角大廈訓練工作人員侵入自己的國防電腦網路，甚至在訓練課程結束後發給證書，目的在協助工作人員從真正的駭客經驗中學習如何保護自己的電腦系統(資安資眼網站，2010)。

資料本身是威脅最終影響的目標，Verizon Business 的 2009 年資料外洩報告指出 15 種最常見的資訊相關攻擊，導致重要的個資與隱私外洩(如附表 1)。另 Verizon Business 的報告也指出，整體資安威脅的類型並沒有太大的變畫化，若由威脅導致的案件來看，駭客入侵佔 64%(其中 94%與資料外洩有關)，遠超過惡意程式(38%)所導致的 90%資料外洩相關的威脅(如圖 2)。因此，也很明顯可看出資料安全威脅與衝擊和外在的駭客攻擊密切相關。再加上公務機關內部威脅的問題，研究報告亦指出 59%離職員工會將工作上相關資料帶離公司，88%資料外洩事件與員工和合作夥伴相關，亦不可輕略忽視(資安人雜誌，2010)。

表 1.2009 DBIR 前 15 大威脅行動

威脅類別	威脅種類	說明	資料外洩案件比例	資料外洩筆數比例
惡意軟體	鑑盤側錄與間諜軟體	KEYLOG	19%	82%
惡意軟體	後門程式	BACKDR	18%	79%
駭客	SQL Injection	SQLINJ	18%	79%
盜用	系統權限誤用	ABUSE	17%	1%
駭客	透過預設憑證的未授權存取	DFCRED	16%	53%
盜用	違反政策規定	POLICY	12%	<19%
駭客	存取清單設定錯誤的未授權存取	WKACL	10%	66%
惡意軟體	封包側錄	SNIFFER	9%	89%
惡意軟體	偷來的身分鑑別	STLCRED	8%	<1%
詐騙	社交工程	SOCIAL	8%	2%
駭客	破解身分鑑別	BYPASS	6%	<1%
實體	實體資產遭竊	THEFE	6%	2%
駭客	暴力破解	BRUTE	4%	7%
惡意軟體	記憶體內容竊取	RANMSCR	4%	<1%
詐騙	網路釣漁	PHISH	4%	4%

資料來源：Verizon Business 2009 年資料外洩報告

資安人雜誌，NO.67(2010.JAN/FEB)，頁 82-頁 86

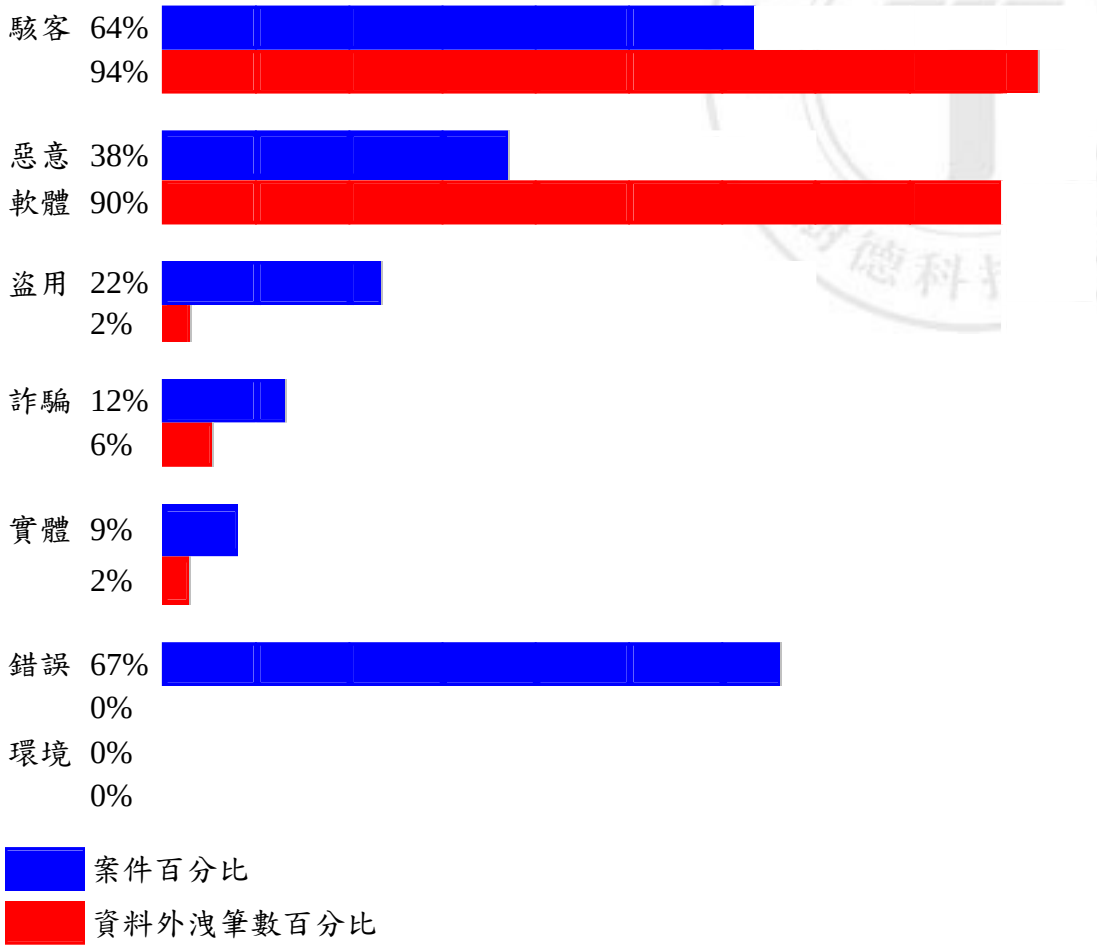

圖 2. 資料外洩案件與筆數威脅類別百分比

資料來源：Verizon Business 2009 年資料外洩報告

資安人雜誌，NO.67(2010.JAN/FEB)，頁 82-頁 86

2.3 資訊「安全」與「便利」的取捨

資訊安全工作的推動，是個相當耗費人力、物力及長時間的持續性工作，往往因單位建立標準的資訊安全作業模式(SOP)後，便犧牲基層人員工作的方便性、自由性及降低工作效率。因此，公務機關領導階層人員都採取比較務實性的法規來化解基層人員的抱怨與阻力。

資訊安全中沒有絕對成功的防禦。所以，資訊安全是一種取捨(Tradeoff)，在有限的條件下，將資源投資在最容易受到攻擊或對單位衝擊最大的安全弱點上。因此，資訊安全防禦措施需在「安全」與「便利」之間做取捨。因為過度的防禦會造成使用者的不便，反而違背資訊科技帶給人類便利的目的。舉例來說，某機關為了要嚴密防範及落實資訊安全的工作，便編列相關預算設置安全性極高的門禁及監視系統，造成職員進出辦公大樓時必需耗費 2-5 分鐘時間，執行相關的安全檢查，另職員的識別證磁卡必需每月 25 日前完成更新設定作業。如此造成職員的不方便，所以辦公大樓大門職員就不關門。如此，反而造成更嚴重的安全漏洞。

2.4 資訊安全管理之作業規範(CNS 27002)

BS 7799 為英國標準協會(British Standards Institution, BSI)所製訂的資訊安全管理標準，被國際標準組織(International Organization for Standardization, ISO)認定為國際之資訊安全管理標準。而原 BS 7799 標準分為兩個部份，一為 BS 7799 Part1，一為 BS 7799 Part2。BS 7799 Part1 被歸納為國際標準「ISO 17799：Information technology-Security techniques-Code of practice for information security management」；而 BS 7799 Part2 被編納為國際標準「ISO 27001：Information technology-Security techniques-Information security management systems-Requirements」。而 ISO 17799 於 2007 年 7 月，正式更名為 ISO 27002(經濟部標準檢驗局)。

我國經濟部標準檢驗局參考 ISO 27002 制定「CNS 27002：資訊技術－安全技術－資訊安全管理之作業規範標準」；參考 ISO 27001 制定「CNS 27001：資訊技術－安全技術－資訊安全管理系統－要求事項標準」。CNS 27002 是資訊安全管理之參考規範，內容包含 11 大管控項目(包括：安全政策、安全組織、資產分類與控制、人力資源安全、實體與環境安全、通訊與作業管理、存取控制、資訊系統之獲得發展與維護、資安事故管理、營運持續管理、遵循與稽核)、39 個管控目標、133 個管控措施。因 ISO 17799 於 2007 年 7 月，正式更名為 ISO 27002。所以，我

國國家標準 CNS 27002「資訊技術-安全技術--資訊安全管理之作業規範」，也於 2007 年 10 月 24 日依據國際標準 ISO 17799：2005 內容完成修訂，並由經濟部公告(經濟部標準檢驗局)。

本研究係以我國資訊安全管理之作業規範(CNS 27002)為藍本，作為研究導向。因為可提供建立、實作、運作、監視、審查、維持及改進資訊安全管理系統(Imformation Security Management System)之模型。因本研究對象以基層公務機關人員為主，故採用我國資訊安全管理之作業規範(CNS 27002)較能函蓋實際工作層面及提高問卷數據的有效性。

三、資訊安全認知與教育

在探討資訊安全認知與教育的關聯性，首先要瞭解資訊安全定義、資訊安全的重要性、影響資訊安全的因素及資訊安全威脅等面向之後，再進一步談談資訊安全認知與教育。

3.1 資訊安全定義

「資訊安全」乃是用以保護資訊系統各項資源(包括：硬體、軟體、資料庫)，防止遭受變更、破壞及未經授權(Unauthorized)使用資訊系統資源之一切控制措施，資訊安全需兼顧人員、程序、資料、硬體、軟體、實體環境等安全管理議題。所以，其涵蓋的範圍不僅包含技術層面，還包括組織管理層面缺一不可。另資訊安全管理標準 ISO 27001 文件，也提到由管理層面的角度來看，資訊是一種資產，是不可或缺而需要妥善保護的。

在美國國防部的「軍事及相關術語國防辭典」中對資訊安全有更明確的定義：「保護資訊及資訊系統，以避免在儲存、處理或傳輸中的資訊遭受未經授權的存取或更改，而且也可避免經授權存取的使用者遭到服務拒絕而無法順利存取」。

根據 RFC2828 的定義，所謂資訊安全服務是一種為了保護特定系統資源所提供的處理機制或通訊服務。一個廣泛被採用的安全服務模式為 CIA 大三元(CIA Triad；Big Three)，即將機密性、完整性與可用性(Confidentiality、Integrity、Availability；CIA)視為最重要的資訊安全基本原則與目標。

1. 機密性(Confidentiality)：就是系統內的資訊不會洩漏給不相關的人士，以保護資訊不被非法存取或揭露。
2. 完整性(Integrity)：就是保護系統內的資訊不會被外人(未授權者)所故意篡改或毀壞，通常資訊系統的內部有層層的安全機制保護，外人(未授權者)想要竄改相當困難，以確保資訊在任何階段沒有不適當的修改損毀。
3. 可用性(Availability)：就是當我們想要使用系統內的資訊(Data)或服務(Services)時，可以順利取得相關的資訊和服務。一般所採用的技術不外

乎是提供重複性的資源(Redundant Hardware and Software)，採用相互備援(Backup)的辦法，並採用負載平衡(Load-Balancing)的技術。

另資訊安全的相反詞分別為揭露(Disclosure)、篡改(Alteration)與破壞(Destruction)(羅英嘉，2007)。

美國國家標準技術局(National Institute Standard and Technology，NIST)在「電腦安全訓練指引」文件中指出，認知(Awareness)意指能使個人對威脅與弱點感到敏感，並可識別出所需保護的資料、資訊與處理的過程。另外，NIST在「建置資訊安全認知與訓練計畫」(Special Publication 800-50)文件中也對認知更有具體的定義為：給予個人明白了解資訊安全的重要為何，並能相對的作出回應，其目的是要將注意力著重於安全上。

此外，NIST亦在「資訊技術安全訓練需求」(Special Publication 800-16)文件中定義，認知不是訓練，認知的目的是在於呈現資訊安全上簡單的重點，及未來允許個人去識別資訊科技安全之利害關係與相對應的反應，讓使用者對一個簡單知識或是主題有認知的概念，應用在資訊安全領域上以減少資訊安全風險的發生。而在SP 800-50也提到學習是持續性的，學習起始於認知，擴大到訓練，並發展成教育。認知是一個改變人或組織態度和觀念的學習過程，以了解安全的重要和當他失誤時的反面結果；訓練是建立知識和技術以增加和提昇工作效率，使得工作能更有效的執行；教育是更進階的訓練型式，提昇某一項研究領域的經驗、發展、知識、技術和能力(蕭瑞祥，2006)。

資訊安全學習歷程中，「認知」階段讓所有的基層人員都必須具備資訊安全基礎知識；「訓練」階段開始於「資訊安全基礎與素養」(Security Basics and Literacy)，「資訊安全基礎與素養」是與資訊系統有關的員工都需要了解，包括委外廠商、供應商等。在現今的環境中，代表著所有在公務機關內服務的人員，對於重要的資訊安全詞彙與概念需要有全面性的了解，並作為訓練的基礎。「訓練」則是依照個人在公務機關內特定的工作與責任，來建立人員所需的安全相關知識與技能；「教育」階段是學習歷程的頂端，並實施複雜的多重訓練活動與技術，

使人員可應付未來資訊科技的威脅與改變，培育具有專門知識的資訊安全專家。

另美國國家標準技術局(National Institute Standard and Technology，NIST)也提出任何與資訊系統有關的人員都需要了解資訊安全基礎與素養(Security Basics and Literacy)。這是指個人必須熟悉的資訊安全基礎知識，且要有能夠運用來保護電子資訊與系統，是適用於所有未來資訊安全的學習基礎，不限於公務機關的特定系統上。

對於如何保護資訊之安全，不同的學者均有不同的定義與解釋，針對資訊安全定義，最早提出是在1984年IBM Data Security Support Programs中所提出的，由表2中摘錄了近年來不同學者對資訊安全之定義。

表2. 資訊安全定義一覽表

年代	資訊安全定義
1984年	在惡意或非惡意之情況下，對資訊資產於未經授權公開、修改、破壞或失效行為之保護(IBM,1984)。
1992年	把管理程序和安全防護技術應用於電腦的硬體、軟體和數據(或資料)，以確保他人有意或無意的讀取、刪除或修改(Donn B. Parker,1997)。
1997年	1.資訊安全的重點不僅是工具(經由技術的控制)，更重要的是實施(經由程序的控制)(Rossouw von Solm,1997)。 2.資訊安全之全貌就是對於有關個人或組織在使用所有關於說的、印行的及自動化紀錄的保護，以及保護資訊的產生、處理過程、傳遞、儲存使用、展示及控制等來源(Donn B. Parker,1997)。 3.資訊安全為保護資訊及資訊系統，使之免於遭受未經授權的存取、使用、揭露、瓦解、變更或毀壞，以提供其完整性、機密性及可用性(The United States Code)。
1999年	BS 7799是資訊安全管理的標準，其主要的設計理念是用來保護資訊和資訊資產，並降低危安事件所造成的影響，它包含三項基本概念： 1.機密性：確保只有獲得授權的人才能存取資訊。 2.完整性：保護資訊和處理方法的準確性和完整性。 3.可用性：確保獲得授權的用戶在需要時可以存取資訊，並使用相關資訊資產(Tom Lillywhite,1999)。
2000年	在網路分散環境中，運用一些控制機制對資源存取提供保護能力，以防止未經合法授權的使用者，入侵網路使用資源與破壞系統運作。其中控制機制包含技術、管理及組織文化層面(人事安全、實體安全、網路通訊安全、系統軟體安全、應用軟體與資料安全及電腦作業安全)(吳琮璠、謝清佳，2003)。

年代	資訊安全定義
2003年	1.資訊安全是指用來防止非法存取、竄改、偷竊和對資訊系統造成傷害的一些政策、程序和方法；藉由一些技術和工具來保護硬體、軟體、通訊網路和資料，以提升資料的安全性(周宣光，2007)。 2.資訊安全是企業之母，在數位時代沒有資訊安全就等於整個企業建築在脆弱的基礎上，是經不起考驗的(朱延智，2007)。
2005年	保護資訊之機密性、完整性與可用性，得增加諸如鑑別性、可歸責性、不可否認性與可靠性。 1.鑑別性：確保一主體或資源之識別就是其所聲明者的特性；適用於如使用者、程序、系統與資訊等實體。 2.可歸責性：確保實體之行為可惟一追溯到該實體的特性。 3.不可否認性：對一已發生之行動或事件的證明，使該行動或事件往後不能被否認的能力。 4.可靠性：始終如一預期之行為與結果的特性(ISO，2005)。
2007年	資訊安全重在人員管理，而非技術控制(李順仁，2007)。
2008年	資訊安全是一種需要技術輔助之管理議題(陳麗珠、柏松齡，2003)。

資料來源：左豪官(2009)資訊安全事件分析及管理作為

3.2 資訊安全的重要性

隨著電腦運用的普及與網際網路的蓬勃發展，已帶給人類有急速且巨大的衝擊，並在生活模式上也有重大的改變。然而隨著資訊便利而來的則是令人擔憂的資訊安全問題。因此，我們必須做好資訊安全防護措施，唯有在確保資訊安全之前提下享受資訊便利，才是面對資訊世紀來臨的正確態度，進而迎接未來更大的挑戰與衝擊。

完整的資訊安全是同時要建立人員(People)、程序(Process)及產品(Product)等三方面的平衡關係，也就是俗稱的「資訊安全三個 P」(如圖 3)。也就是說人員都應

遵守資訊安全的作業程序，產品才能發揮最大的效能(潘天佑，2008)。

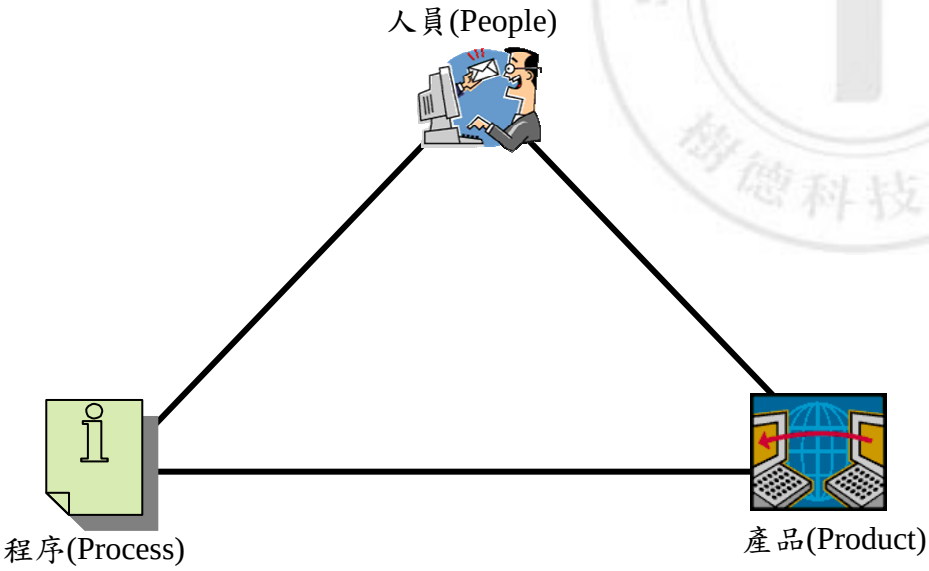

圖 3. 資訊安全三個 P

資料來源：本研究整理

3.3 影響資訊安全的因素

自從網際網路的應用興起以後，網際網路已成為犯罪工具的主要媒介，資訊安全威脅也不斷升高，使資訊安全面臨更嚴峻的挑戰。任何造成資訊系統異常的事物都稱為「威脅」，而資訊系統所面臨的威脅可分為二大部分：「人為因素」、「自然因素」，但又以「人為因素」佔絕大多數。資訊安全問題，則有科技因素外，「人的因素」仍是遠大於自然因素；屬於「自然因素」僅佔資安事件 15%，但「人的因素」高達 85%，其中 80%來自於基層人員的「人為疏失」及「蓄意破壞」等二項(如表 3)。

表 3 資訊安全威脅分類

資訊安全威脅			影響安全的事件	舉例說明
人為因素	人為疏失		系統操作、維護管理失當	密碼外洩、系統使用後未登出
	蓄意破壞	資料破壞	資訊系統破壞	病毒破壞
			硬體設施破壞	
			軟體程式破壞	
		資料濫用	未經授權使用資訊系統	未經受權下載資料 駭客入侵
			不當使用資料或通訊服務	
			不當管道取得重要資料	
		違反隱私權	不當使用及蒐集資料	竊取網路帳號密碼

自然因素	天然災害	颱風、水患、地震等	颱風
	系統故障	軟體程式、硬體設施、網路通訊故障	軟體設計錯誤 硬體設施故障

資料來源：李永山、張勇翔(2004)，結合 BS7799 與資訊安全藍圖建構資訊安全評估機制之研究，94 年 6 月

美國電腦安全局及聯邦調查局(CSI/FBI)對於電腦犯罪及安全所做的一項研究調查也顯示，大多數之危安事件均是由於人員的疏失或是蓄意破壞所造成的，其中企業或組織內部的員工所造成的危安事件更占了80%，由此可知即使企業或組織使用再好的資訊技術，也無法防範人員所造成的威脅或意外事件。因此如何強化組織的內部管理已成為現階段非常重要之議題(左豪官，2009)。

3.4 資訊安全威脅

根據 2009 年各項網路犯罪與安全攻擊統計資料顯示，有 64%的受訪者表示曾處理過惡意程式感染(Malware Infection)事件(2008 年為 50%)，而 23%曾處理過殭屍電腦(Bots/Zombies)事件(2008 年為 20%)，這些統計數據的上升反映 Conficker 與 Bookface 等惡意程式於 2009 年的盛行。25%受訪者認為，因資安事件所造成的損失中，有超過 60%導因於內部人為疏失(行政院國家資通安全會報技術服務中心，2009)。

另根據 Datapro Research Corporation 的資安調查，約有 5 成的資安事件是由人為失誤所造成，加上離(退)職人員或內部犯罪所佔僅 1 成，人為因素造成資安事件所佔的比例高達 6 成。在 2008 年全球最大液晶面板玻璃製造商康寧公司的一名前員工，遭美國聯邦調查局逮捕，被指控竊取該公司的重要業務機密，出售給競爭對手台灣的碧悠公司。任職 AOL(American Online)的一位工程師，盜用另一位同事的帳號，竊取 3,000 多萬筆的客戶資料販售給垃圾郵件業者，這些資安事件案例，

都是來自於內部人員或離(退)職人員的電腦犯罪(邱瑩青，2009)。

以提供虛擬主機及網頁服務為主的科技公司「戰國策」，在 2009 年因公司內部後台管理頁面的控制權限管理失當，約有 4,270 筆客戶客戶訂單資料被 Google 快取抓走變成公開網頁資料。

就國家安全方面而言，目前資訊網路攻擊已成為另類「無聲」的軍事武器，世界各軍事強國已陸續發展出許多網路攻防戰的手段，甚至仍有國家大量網羅國內外駭客高手進行軍事網路演習。因此，資訊網路攻擊是屬於資訊戰的一環。近年來，國軍也透過年度「漢光演習」，將電腦病毒、釣魚郵件、網頁置換等惡意程式加入演習階段，進行國軍各級單位(部隊)資訊攻防戰。因此，未來戰爭中使用的資訊武器也扮演重要角色。而資訊戰中，電腦則是資訊戰的重要核心，一旦遭到駭客攻擊(如植入木馬、蠕蟲、邏輯炸彈等電腦病毒)時，就有可能造成國軍整個作戰及指管系統全數癱瘓。另外，敵軍也可在戰爭發動前，就先行癱瘓我政府的通訊、運輸、交通、民生設施及軍事指管系統。這就如同孫子兵法說的「不戰而屈人之兵」是相同的意思。

就上述例子均顯示，維有持續不斷的依照不同階層人員的工作性質，實施不同的資訊安全意識和相關技能的教育就顯得非常重要且必要。

3.5 資安政策與訓練

人員經常是資訊安全管理實務中最弱、最難掌控及最易出問題的一環。因此，基層人員的教育訓練是與資訊使用的安全性有著密不可分的關係。其政策包括：

1. 背景與安全性調查(Background Checks and Security Clearance)。
2. 工作描述(Jobs Description)。
3. 工作活動(Jobs Activities)。
4. 資訊安全認知與教育訓練(Security Awareness and Education Training)。

其中雇用終止(Termination)部份，因屬於企業雇主與員工之關係，在此不列討論。資訊安全的認知教育又特別與資安政策是否可以正確而順利的推動和落實有

直接的相關性。

美國國家標準與技術局(National Institute of Standards and Technology，NIST)在「電腦安全訓練指引」(Special Publication 500-172)文件中指出，各組織機構應對於所有與管理、使用電腦系統作業的人員，必需強制實施且定期的電腦安全認知訓練(NIST 1989)。

OECD(Organization for Economic Co-operation and Development)於 2002 所提出之 9 項資訊系統與網路安全指引中，將資訊安全認知(Awareness)列為第一條規則，說明認知是資訊系統與網路防護第一線，加強組織成員對於資訊安全認知是有其重要性的。

另國、內外組織與政府單位所發佈的資訊也顯示，人是資訊安全中最可能發生問題的元素，而人員不當的認知是資訊安全推動最大瓶頸。因此，要如何有效地推動基層人員的資訊安全認知是非常重要的。但是，基層人員資訊安全認知應如何提昇？資訊安全認知訓練的課程內容需要哪些？都需要進一步規劃與設計的(蕭瑞祥，2006)。

由於人員常因資訊安全認知不足、系統(設備)操作錯誤及以個人工作經驗值來處理資訊安全問題，也因如此造成許多無法彌補及損失慘重的重大資安事件。近年來，最被常用的釣魚(Phishing)等社會工程的詐騙手段，就是終端系統(設備)人員對此類型攻擊的認知不足，輕忽了使用電子郵件或搜尋引擎內超連結的潛在風險性而造成資料外洩。若能提供此種攻擊的教育認知，則可大幅降低此類詐騙手法的攻擊。而安全性的認知、教育與訓練實施的有效性，也直接關係到單位資訊安全政策被理解的程度和實踐的效果(羅英嘉，2007)。

3.6 教育、訓練與認知大三元

安全性認知(Awareness)、訓練(Training)及教育(Education)被視為加強基層人員了解安全性知識技能的大三元(如圖 4)。安全性認知著重在人員對安全性有持續性的警覺與關注，安全性訓練則讓人員擁有必要的安全性技術與能力，這通常是屬

於短期且針對特定的個別技術，至於安全性教育通常會整合安全技能與其它必要的觀念與原則，而教育通常會應用在較廣泛且長期的目標(羅英嘉，2007)。

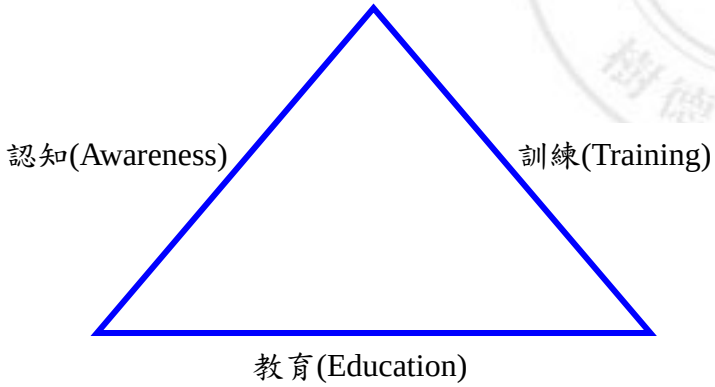

圖 4. 教育、訓練與認知大三元

資料來源：本研究整理

因此，為了保護資訊安全的成功和有效性，人員必須先瞭解並嚴格遵從單位的資訊安全政策。另再針對高階管理人員、技術人員、終端使用者等不同層級，進行不同的資訊安全培訓，使教育工作能具體的由上而下(Top-Down)實施訓練：

1. 主管資訊安全工作的高級負責人或管理人員：重點是瞭解及掌握組織資訊安全的整體政策及目標、資訊安全體系的構成、安全管理部門的建立與管理制度的制定。
2. 負責資訊安全管理及維護的技術人員：重點在充分瞭解安全管理政策，以掌握安全評估的基本方法，並對安全操作和維護技術的運用。
3. 終端使用者：重點在於學習各類安全操作程序，瞭解和掌握相關的安全政策，包括自身應該承擔的安全職責及各項安全程序與正確使用資訊系統(設備)。

四、研究方法與設計

4.1 研究架構

本研究係以我國資訊安全管理作業規範(CNS27002)為藍本，結合基層公務機關執行階層、管理階層及領導階層等 3 部分的人員工作性質，設定研究方向、研究相關文獻、擬定研究核心主題、設計研究驗證方式、問卷設計及修改、進行問卷調查、建立問卷樣本數、數據分析統計，以建立資訊安全概念與教育規劃之探討，研究架構流程程圖(如圖 5)。

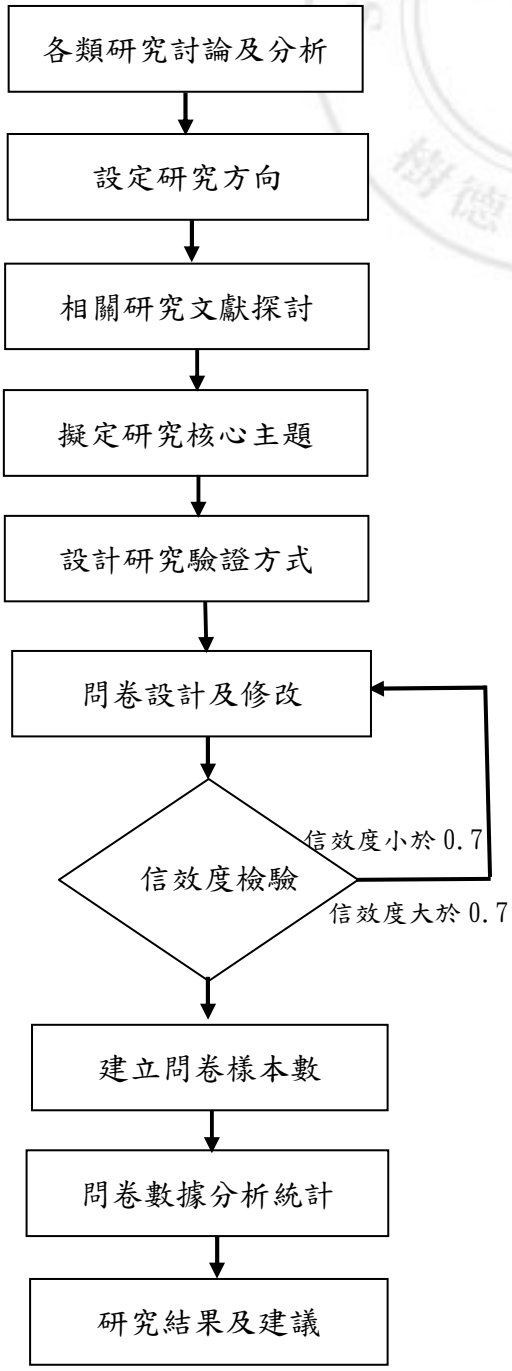

圖 5. 本研究流架構程圖

資料來源：本研究整理

4.2 問卷內容設計

問卷之初稿係以我國資訊安全管理之作業規範(CNS 27002)為基礎，另以國、外內相關理論及研究為依據，並經由公務機關實務工作者先行實施問卷前測後，根據受測人員的建議修正，即正式定稿，隨將問卷分發至公務機關單位實施問卷調查工作，問卷設計作業過程如下：

1. 相關理論及研究資料蒐集：

   以我國資訊安全管理之作業規範(CNS 27002)為基礎，蒐集國、內外相關研究資料及整理後作為為問卷依據。

2. 進行問卷設計：

   將我國資訊安全管理作業規範(CNS27002)內容加以整理、分類及說明後，再以基層公務機關執行階層、管理階層及領導階層等 3 部分階層人員實務工作，提出相關資料後初擬問卷內容。

3. 設定問卷對象：

   以基層公務機關執行階層、管理階層及領導階層等 3 部分不同階層人員為對象，以不記名方式實施問卷調查工作。

4. 問卷第一次修訂：

   以基層公務機關依執行階層、管理階層及領導階層等 3 部分不同階層人員接受第一次問卷調查後，針對問卷內容設計提出缺失、陳述用語修訂後，即進行問卷內容修訂及難易度調整。

5. 問卷前測：

   於問卷初稿修訂後，再依執行階層、管理階層及領導階層等 3 部分人員，挑選非第一次接受問卷調查人員進行第二次問卷測試，再依建議事項針對問卷內各項問題進行第二次修訂，再將不合適宜之處進行調整。

6. 正式定稿：

   經過二次問卷修訂後，即完成問卷定稿作業，並在問卷前加上說明，即

正式成案，分發至基層公務機關進行問卷調查工作。

4.3 問卷設計及編審

問卷項目計 12 部份，除第 12 部份為受訪人員基本資料，僅作為參考數據外，其餘項目均與我國資訊安全管理作業規範(CNS27002)11 項主控項目內容相同，分述說明如下：

第 1 部份：安全政策：

主要在於基層公務機關之執行、管理及領導階層人員對資訊安全之指示與政策是否瞭解其一致性。

第 2 部份：資訊安全的組織(單位內部、單位外部)：

1. 單位內部：

   在於基層公務機關之管理及領導階層人員，對於資訊安全管理是否明確瞭解指派及資訊系統(設備)的授權過程。

2. 單位外部：

   在於基層公務機關之管理及領導階層人員，對於機關所屬資訊系統(設備)工程之承包商是否瞭解依法令簽定協議書、提供資訊安全品質服務等事項。

第 3 部份：資產管理(資產責任、資訊分類)：

1. 資產責任：

   在於瞭解基層公務機關之基層、管理及領導人員是否瞭解資訊資產管理與資訊安全工作之間的關係；使實務工作者能瞭解資產管理，應由專人專責負責，以達成及維持單位資產的適切保護。

2. 資訊分類：

   在於瞭解基層公務機關之管理階層是否瞭解資訊設施需依系統(設備)、種類、品項等逐一建立帳籍以便管理，避免發生資訊設備遺失造成機敏資料外洩。

第 4 部份：人力資源員安全：

在於瞭解基層公務機關之領導階層是否瞭解單位職員、承包商業者及第三方使用者等三方面之責任，及勝任所被認定的角色，以降低竊盜、詐欺或設施誤用的風險。

第 5 部份：資訊安全區域：

在於瞭解基層公務機關之管理階層是否瞭解安全區域可防止單位各辦公室與資訊遭未授權的實體存取、損害及干擾；另是否瞭解機敏性較高的資訊設備宜妥善安置於安全區域內，由界定的安全周界、適當的安全屏障及人員進出管制，可以讓高機敏性之資訊設備受到保護，其資訊資料遭未授權的實體存取、損害及干擾。

第 6 部分：通訊與作業管理：

重點置於基層公務機關之執行、管理及領導階層人員是否瞭解其資訊安全標準作業程序(SOP)的製作，以確保資料的安全及資訊設施正確的操作，以降低人為忽略或蓄意的系統誤用風險。

第 7 部分：存取控制：

在於基層公務機關之執行與管理階層否瞭解資訊系統存取的安全要求，並建立文件化及審查存取控制政策，以確保經授權使用者對資訊系統的存取與防止未經授權的存取限制。

第 8 部分：資訊系統獲取、開發、維護：

重點置於基層公務機關之執行階層對資訊系統的維護是否瞭解依規定執行及安全檢測工作；管理階層是否瞭解作業系統、基礎建設及資安事件正確的處置作為；領導階層是否瞭解資訊系統環控、軟體應用、安全措施、管理工作及安全查核等工作項目的安全性及運用。

第 9 部分：資訊安全事故的管理：

重點在於基層公務機關之執行、管理者及領導階層是否瞭解資安

事件通報與提報程序；一旦接獲事件通報後，是否能有效迅速的處置資安事件及弱點；處置過程中，是否將回報、監視、評估及資安事件的資料做整體審查管理，以確保法律訴訟時提出證據說明。

第 10 部分：系統運作管理：

重點在於單位系統運作期間突發生系統中斷、功能失效或災害的影響時，執行及管理階層是否能隨即依標準作業程序(SOP)維持系統資料完整，或以最小化降低系統災損且能迅速復原資訊資產。

第 11 部分：遵循性：

在於基層公務機關執行、管理及領導階層是否瞭解資訊系統的設計、運作、使用及管理工作都受法律、法令、法規或契約均為安全要求的規範。

4.4 研究對象

本研究對象主要是基層公務機關(執行階層、管理階層及領導階層)等不同階層人員為主，再結合我國資訊安全管理之作業規範(CNS27002)為問卷藍本，採一人一卷方式，計蒐集 200 份問卷樣本。

為求問卷數據有效性，本研究對象基層公務機關工作業務性質均為資訊安全相關工作，受訪人員均為實際從事資訊安全維護工作者，以採全面受訪，以提高數據可信度。問卷共發送 200 份，回收 200 份，回收率達 100%。經彙審整理後，有效問卷仍為 200 份，無無效問卷。因此，有效回收率為 100%，問卷發放及回收統計表如表 4。

表4. 問卷發放及回收統計表

受訪單位	問卷發放數	受訪人員數	有效回收數	有效回收率
P	200	200	200	100%

資料來源：本研究整理

4.5 問卷信度檢驗

為能瞭解本研究問卷信度檢驗，除依據受訪人員提供問卷設計缺失及建議，以期問卷內容陳述用語清晰明瞭；另採用電腦套裝軟體 SPSS 15 for windows 中文版，針對 200 份問卷進行信度檢驗分析，一般性認為 Cronbach's α 信度係數大於 0.7 者為佳，若小於 0.35 者不具有信度，應予調整。但 Ually(1978)及 Wortzel(1979)認為 Cronbach's α 信度係數介於 0.70 至 0.98 間，都可算是高信度值。

本研究問卷信度檢驗量表，經檢驗後有效個數達 100%，均為有效問卷；另整份問卷之可靠性統計量，其係數為 0.924，大於 Cronbach's α 信度係數大於 0.7，表示問卷整體性信度良好，如附表 5、6。

表 5. 整份問卷之個數分析表

		N	%
個數	有效個數	200	100.0
	排除個數	0	0
	總數	200	100.0

資料來源：本研究整理

表6. 整份問卷之可靠性統計量

Cronbach's Alpha	項目個數
.924	73

資料來源：本研究整理

另在本問卷中，每一題的Cronbach's α信度範圍值為0.922~09.25，均大於0.7值。顯示本問卷各項目均為可信度高如附表7。

表 7. 問卷項目整數統計量

	項目刪除時的尺度平均數	項目刪除時的尺度變異數	修正的項目總相關	項目刪除時的Cronbach’s Alpha值
q1	167.53	1146.502	.399	.923
q2	167.28	1146.411	.413	.923
q3	166.65	1141.736	.342	.923
q4	167.67	1154.817	.318	.923
q5	167.53	1152.723	.377	.923
q6	167.73	1152.962	.294	.924
q7	167.62	1153.513	.287	.924
q8	167.15	1144.490	.310	.924
q9	167.51	1155.015	.323	.923
q10	167.74	1145.613	.432	.923
q11	167.60	1161.779	.193	.924
q12	167.65	1151.999	.340	.923
q13	168.09	1162.571	.195	.924
q14	168.10	1163.725	.180	.924
q15	167.15	1144.771	.323	.923
q16	167.55	1152.139	.250	.924
q17	167.61	1148.863	.301	.924
q18	167.35	1151.234	.353	.923
q19	167.28	1149.258	.345	.923
q20	166.66	1139.291	.368	.923
q21	166.39	1128.902	.413	.923
q22	166.47	1131.818	.456	.923

	項目刪除時的尺度平均數	項目刪除時的尺度變異數	修正的項目總相關	項目刪除時的Cronbach's Alpha值
q23	167.61	1148.259	.378	.923
q24	167.80	1159.822	.199	.924
q25	166.38	1133.131	.380	.923
q26	166.78	1133.971	.381	.923
q27	167.04	1141.602	.586	.922
q28	167.23	1143.485	.459	.923
q29	167.06	1147.007	.322	.923
q30	167.47	1143.346	.417	.923
q31	167.01	1134.472	.407	.923
q32	166.12	1127.992	.415	.923
q33	165.94	1135.323	.355	.923
q34	167.01	1143.718	.444	.923
q35	167.01	1141.909	.464	.923
q36	166.35	1132.500	.430	.923
q37	166.31	1131.369	.417	.923
q38	167.18	1139.756	.335	.923
q39	167.17	1142.078	.466	.923
q40	167.23	1151.904	.410	.923
q41	167.16	1143.120	.500	.923
q42	166.37	1139.802	.486	.922
q43	167.38	1149.262	.389	.923
q44	167.70	1149.309	.330	.923
q45	167.59	1147.891	.319	.923
q46	167.63	1147.963	.310	.924
q47	167.40	1146.834	.285	.924
q48	166.74	1130.133	.383	.923
q49	166.99	1133.829	.467	.922

	項目刪除時的尺度平均數	項目刪除時的尺度變異數	修正的項目總相關	項目刪除時的Cronbach's Alpha值
q50	167.12	1145.563	.436	.923
q51	167.10	1142.247	.485	.923
q52	167.68	1147.937	.363	.923
q53	167.71	1152.549	.347	.923
q54	167.02	1139.216	.459	.923
q55	167.66	1150.378	.309	.923
q56	167.61	1144.711	.388	.923
q57	166.95	1140.791	.414	.923
q58	167.45	1155.384	.147	.925
q59	167.49	1150.492	.422	.923
q60	167.31	1151.258	.337	.923
q61	167.57	1144.940	.387	.923
q62	167.16	1142.202	.488	.923
q63	167.65	1141.193	.424	.923
q64	167.65	1145.887	.370	.923
q65	167.00	1144.658	.416	.923
q66	167.30	1147.224	.361	.923
q67	167.54	1145.526	.347	.923
q68	167.16	1141.301	.428	.923
q69	167.04	1138.275	.419	.923
q70	167.69	1149.051	.342	.923
q71	167.55	1141.123	.362	.923
q72	166.62	1138.419	.334	.924
q73	167.10	1143.212	.463	.923

資料來源：自行整理

表8及表9為「安全政策」因素信度分析，為問卷第1部分共3題，其信度為0.745。在表9中發現，若將第3題題目刪除後，其信度雖能提高到0.783。但第3題題目主要重點在於基層公務機關人員對於資訊安全政策法令規章的責任屬性是否瞭解，屬重要問題。因此，第3題題目不予以刪除。

表8. 「安全政策」因素之可靠性統計量

Cronbach's Alpha	項目個數
.745	3

資料來源：本研究整理

表9. 「安全政策」因素之項目統計整理量

	項目刪除時的尺度平均數	項目刪除時的尺度變異數	修正的項目總相關	項目刪除時的Cronbach’s Alpha值
q1	5.19	4.443	.567	.671
q2	4.93	4.146	.692	.545
q3	4.31	3.479	.506	.783

資料來源：本研究整理

表10及表11為「資訊安全的組織」因素信度分析，為問卷第2部分，概分單位內部共11題，單位外部共3題，總計14題。其信度為0.738。在表11中發現，各題題目均未超過信度0.738，表示問卷第2部分信度良好，各題目均不需要刪除。

表10.「資訊安全的組織」因素之可靠性統計量

Cronbach's Alpha	項目個數
.738	14

資料來源：本研究整理

表11.「資訊安全的組織」因素之項目統計整理量

	項目刪除時的尺度平均數	項目刪除時的尺度變異數	修正的項目總相關	項目刪除時的Cronbach's Alpha值
q4	25.22	45.670	.443	.715
q5	25.09	45.224	.521	.709
q6	25.29	45.672	.359	.723
q7	25.18	46.175	.323	.726
q8	24.71	46.556	.358）	.724
q9	25.06	45.514	.470	.713
q10	25.29	44.247	.517	.707
q11	25.16	46.142	.370	.722
q12	25.20	45.156	.448	.714
q13	25.64	44.955	.503	.710
q14	25.65	45.917	.432	.717
q15	24.71	46.254	.504	.709
q16	25.10	45.729	.269	.735
q17	25.16	46.226	.255	.736

資料來源：本研究整理

表12及表13為「資產管理」因素信度分析，為問卷第3部分，概分資產責任共2題，資產分類共2題，總計4題。其信度為0.671。在表13中發現，各題題目均未超過信度0.671，表示問卷第3部分信度良好，各題目均不需要刪除。

表12. 「資產管理」因素之可靠性統計量

Cronbach's Alpha	項目個數
.671	4

資料來源：本研究整理

表13. 「資產管理」項目統計整理量

	項目刪除時的尺度平均數	項目刪除時的尺度變異數	修正的項目總相關	項目刪除時的Cronbach’s Alpha值
q18	8.34	9.963	.389	.648
q19	8.27	9.392	.418	.629
q20	7.65	7.094	.583	.508
q21	7.38	6.869	.469	.610

資料來源：本研究整理

表14及表15為「人力資源安全」因素信度分析，為問卷第4部分共計7題。其信度為0.624。在表15中發現，若將第23、24題題目刪除後，其信度將提高到0.693。但第23題題目置重點於基層公務機關人員是否瞭解資訊安全角色與責任應包括那些要求；第24題題目係探討基層公務機關人員是否瞭解應由那些人員簽署資訊安全保密協議書 (切結書)，均屬重要問題。因此，第23、24題題目不予以刪除。

表14.「人力資源安全」因素之可靠性統計量

Cronbach's Alpha	項目個數
.624	7

資料來源：本研究整理

表15.「人力資源安全」項目統計整理量

	項目刪除時的尺度平均數	項目刪除時的尺度變異數	修正的項目總相關	項目刪除時的Cronbach's Alpha值
q22	14.50	15.106	.564	.500
q23	15.64	21.337	.061	.659
q24	15.83	22.477	-.066	.693
q25	14.41	14.927	.461	.539
q26	14.81	15.049	.467	.536
q27	15.07	17.880	.615	.530
q28	15.26	18.857	.356	.584

資料來源：本研究整理

表16及表17為「資訊安全區域」因素信度分析，為問卷第5部分共計7題。其信度為0.676。在表17中發現，若將第29、30題題目刪除後，其信度將提高到0.689。但第29題題目探討基層公務機關人員是否瞭解資訊設備周邊安全為資訊安全的一環；第30題題目主要是分析公務機關人員對資訊設備周邊環境的設置是否瞭解，均屬重要問題。因此，第29、30題題目不予以刪除。

表16.「資訊安全區域」因素之可靠性統計量

Cronbach's Alpha	項目個數
.676	5

資料來源：本研究整理

表17.「資訊安全區域」項目統計整理量

	項目刪除時的尺度平均數	項目刪除時的尺度變異數	修正的項目總相關	項目刪除時的Cronbach’s Alpha值
q29	11.69	17.393	.265	.689
q30	12.10	17.930	.273	.683
q31	11.64	14.302	.495	.595
q32	10.75	11.910	.643	.511
q33	10.57	13.563	.481	.601

資料來源：本研究整理

表18及表19為「通訊與作業管理」因素信度分析，為問卷第6部分共計17題。其信度為0.788。在表19中發現，各題題目均未超過信度0.788，表示問卷第6部分信度良好，各題目均不需要刪除。

表18.「通訊與作業管理」因素之可靠性統計量

Cronbach's Alpha	項目個數
.788	17

資料來源：本研究整理

表19.「通訊與作業管理」項目統計整理量

	項目刪除時的尺度平均數	項目刪除時的尺度變異數	修正的項目總相關	項目刪除時的Cronbach's Alpha值
q34	39.57	88.266	.389	.777
q35	39.57	86.829	.459	.772
q36	38.91	86.514	.314	.783
q37	38.87	84.841	.353	.780
q38	39.74	85.118	.345	.781
q39	39.73	85.638	.530	.768
q40	39.79	88.270	.505	.772
q41	39.72	87.097	.507	.771
q42	38.93	86.819	.452	.773
q43	39.94	88.338	.417	.775
q44	40.26	87.528	.384	.777
q45	40.15	88.299	.309	.782
q46	40.19	87.089	.353	.779
q47	39.96	87.044	.302	.784
q48	39.30	85.236	.289	.788
q49	39.55	86.812	.352	.779
q50	39.68	88.460	.399	.776

資料來源：本研究整理

表20及表21為「存取控制」因素信度分析，為問卷第7部分共計5題。其信度為0.562。在表21中發現，若將第54題題目刪除後，其信度將提高到0.623。但第54題題目主要探討基層公務機關人員是否瞭解對單位的公用程式使用應嚴密監控及限制，屬重要問題。因此，第54題題目不予以刪除。

表20.「存取控制」因素之可靠性統計量

Cronbach's Alpha	項目個數
.562	5

資料來源：本研究整理

表21.「存取控制」項目統計整理量

	項目刪除時的尺度平均數	項目刪除時的尺度變異數	修正的項目總相關	項目刪除時的Cronbach's Alpha值
q51	8.16	7.730	.288	.526
q52	8.74	6.465	.482	.407
q53	8.77	7.545	.357	.490
q54	8.08	8.205	.122	.623
q55	8.72	6.617	.401	.457

資料來源：本研究整理

表22及表23為「資訊系統獲取、開發及維護」因素信度分析，為問卷第8部分共計4題。其信度為0.387。在表23中發現，若將第57、58題刪除後，其信度將提高到0.449。但第57題題目主要瞭解基層公務機關人員是否明瞭應妥善管理單位金鑰；第58題題目，系瞭解基層公務機關人員是否單位系統檔案、測試資料應備妥各項各項程序、保護及管理，以確保公務機關系統檔案的安全，均屬重要問題。因此，第57、58題題目不予以刪除。

表22.「資訊系統獲取、開發及維護」因素之可靠性統計量

Cronbach's Alpha	項目個數
.387	5

資料來源：本研究整理

表23.「資訊系統獲取、開發及維護」項目統計整理量

	項目刪除時的尺度平均數	項目刪除時的尺度變異數	修正的項目總相關	項目刪除時的Cronbach’s Alpha值
q56	9.03	7.401	.358	.209
q57	8.37	8.615	.121	.390
q58	8.87	6.801	.120	.449
q59	8.91	8.840	.261	.308
q60	8.72	8.585	.211	.327

資料來源：本研究整理

表24及表25為「資訊安全事故管理」因素信度分析，為問卷第9部分共計4題。其信度為0.765。在表23中發現，各題目均未超過信度0.765，表示問卷第9部分信度良好，各題題目均不需要刪除。

表24. 「資訊安全事故管理」因素之可靠性統計量

Cronbach's Alpha	項目個數
.765	4

資料來源：本研究整理

表25.「資訊安全事故管理」項目統計整理量

	項目刪除時的尺度平均數	項目刪除時的尺度變異數	修正的項目總相關	項目刪除時的Cronbach’s Alpha值
q61	6.21	7.081	.522	.733
q62	5.80	7.521	.552	.719
q63	6.29	6.317	.657	.657
q64	6.29	6.941	.539	.724

資料來源：本研究整理

表26及表27為「資訊安全事故管理」因素信度分析，為問卷第10部分共計4題。其信度為0.393。在表25中發現，若將第66、67題題目刪除後，其信度將提高到0.478。但第66題題目係探討基層公務機關人員對於單位系統運作的發展與維持是否瞭解應納入資訊安全作為；第67題題目亦探討基層公務機關人員是否瞭解系統運作管理與維護需有優先順序，均屬重要問題。因此，第57、58題題目不予以刪除。

表26.「系統運作管理」因素之可靠性統計量

Cronbach's Alpha	項目個數
.393	4

資料來源：本研究整理

表27.「系統運作管理」項目統計整理量

	項目刪除時的尺度平均數	項目刪除時的尺度變異數	修正的項目總相關	項目刪除時的Cronbach’s Alpha值
q65	6.68	4.612	.355	.179
q66	6.98	5.572	.103	.438
q67	7.22	5.426	.078	.478
q68	6.84	4.316	.364	.152

資料來源：本研究整理

表28及表29為「遵循性」因素信度分析，為問卷第11部分共計5題。其信度為0.625。在表27中發現，若將第71題題目刪除後，其信度將提高到0.675。但第71題題目係探討基層公務機關管理階層是否應瞭解其工作責任範圍所有安全程序皆正確執行，屬重要問題。因此，第71題題目不予以刪除。

表28.「遵循性」因素之可靠性統計量

Cronbach's Alpha	項目個數
.625	5

資料來源：本研究整理

表29.「遵循性」項目統計整理量

	項目刪除時的尺度平均數	項目刪除時的尺度變異數	修正的項目總相關	項目刪除時的Cronbach's Alpha值
q69	9.28	10.432	.493	.511
q70	9.93	12.592	.291	.610
q71	9.79	12.639	.171	.675
q72	8.86	9.592	.424	.550
q73	9.34	11.008	.607	.482

資料來源：本研究整理

4.6 資料分析

針對基層公務機關人員進行資訊安全認知問卷調查工作，問卷調查計 200 份。於問卷資料回收後，經彙整、分類、分析、統計後，發現目前基層公務機關人員未受過資訊安全教育訓練相關課程，但已達到資訊安全概念標準人員僅佔總人數 17%，未達標準者佔總人數高達 83%；而受過公務機關現行資訊安全教育訓練相關課程人員，已達到資訊安全概念標準也僅佔總人數 36%，未達標準者佔總人數仍高達 64%(如圖 6、7)。

顯見目前公務機關規劃的資訊安全教育課程訓練，已無法使公務基層人員的資訊安全概念隨著教育訓練課程提升應有的效益；同時也說明了資訊安全教育課程的規劃也須要有所改變。

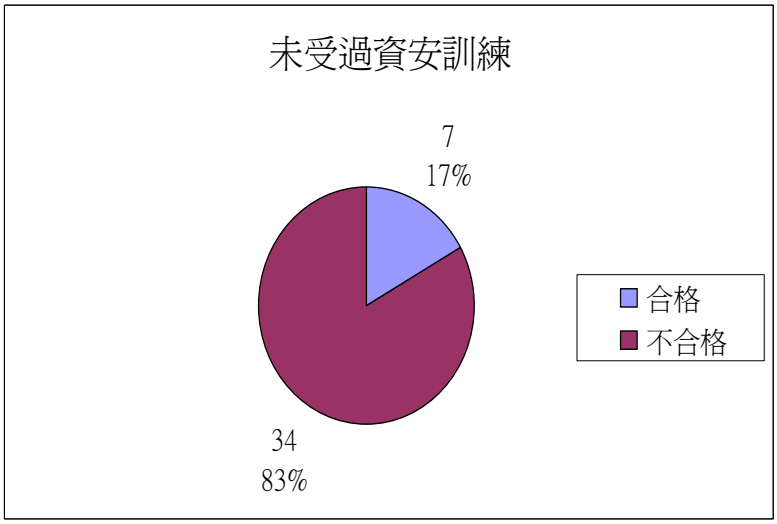

圖 6.未受過資安訓練合格比例圖

資料來源：本研究問卷調查結果

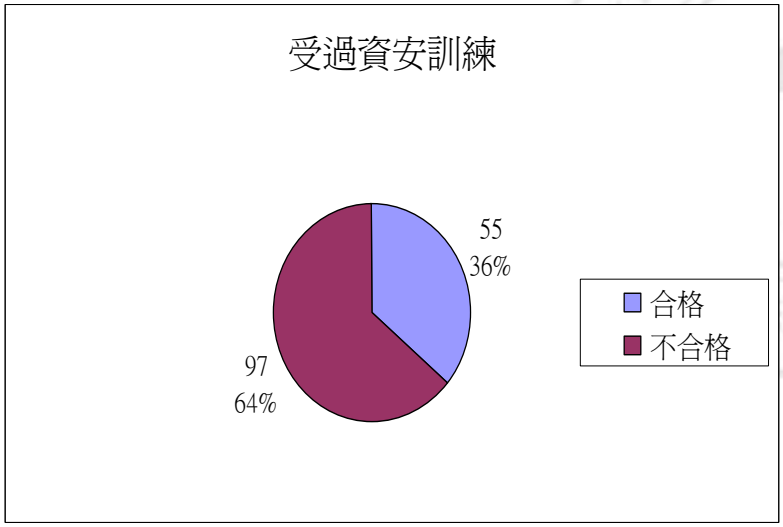

圖 7.受過資安訓練合格比例圖

資料來源：本研究問卷調查結果

另由基層公務機關對 CNS 27002 問卷調查各項平均百分比資料顯示，總平均百分比僅 41.1%且未達 60%以上的標準。同時也發現問卷內容第 2 部分，資訊安全的組織-單位外部項目的百分比僅佔 16.1%。顯示基層公務機關針對資訊安全與承包商簽署協議書應包含的項目、是否應導入承包商的資訊產品及共同工作時需由承包商先行提供風險管理等範疇均不甚瞭解。也說明公務機關肇生資安事件原因之一，在於與單位外部(以承包商為主)所簽訂的資訊安全協議書內容未詳加審查及瞭解程度不足。

而在問卷內容第 9 部分，資訊安全事故管理部分百分比雖達 50.4%，但仍不及 60%以上。究其原因，公務機關針對資安事件處置作為較為嚴謹且有時限限制。若單位發生資安事件時，大多採取先懲後查的態度，避免資安事件擴大。除違規單位失職人員依法懲處(法辦)外，單位業務承辦人、業務主管及資安長等人員，需於期限內至指定單位參加資訊安全再教育課程訓練；同時也列為案例宣導。且其上一級督導單位資安業務主管及資安長亦受連帶檢討失職責任；並與違規單位人員(肇事者、資安長)共同參加資訊安全再教育課程。因此，在問卷調查平均百分比也就相對性的提高(如表 30)。

表 30. 基層公務機關對 CNS27002 問卷調查各項平均百分比

第一部分	第二部分		第三部分		第四部分
安全政策	資訊安全的組織-單位內部	資訊安全的組織-單位外部	資產管理-資產責任	資產管理-資訊分類	人力資源安全
44.4%	46.9%	**16.1%**	22.3%	29.0%	43.0%
第五部分	第六部分	第七部分	第八部分	第九部分	第十部分
資訊安全區域	通訊與作業管理	存取與控制	資訊系統獲取、開發及維護	資訊安全事故管理	系統運作管理
35.9%	45.2%	39.7%	36.2%	50.4%	44.0%
第十一部分 遵循性	總平均				
39.3%	41.1%				

此外，問卷調查工作亦針對基層公務機關之執行、管理及領導階層等 3 部分進行各項數據分析，結果發現資訊安全合格率總平均百分比僅達 41.1%且亦未達 60%以上合格標準。顯示各階層人員的資訊安全認知，也未因受過資訊安全教育訓練相關課程後有所提升。並針對執行、管理及領導階層等 3 部分問卷調查數據較低部分進行分析，分述如下：

1. 執行階層部分：

(1) 在 CNS 27002 問卷調查各項平均百分比中，以問卷內容第 2 部分資

訊安全的組織(單位外部 13.4%)、第 3 部分資產管理(資產責任部份 21.3%、資訊分類 23.6%)等 3 項百分比較低，其中以訊安全的組織(單位外部 13.4%)最低。

(2) 經分析結果：就基層公務機關執行階層而言，對於單位與承包商簽訂協議書應注意事項部分及資產管理的工作均不屬於其工作範疇。因此，就上述 3 項部分瞭解程度就相對性的不足。

(3) 原因探討：在基層公務機關執行階層，係屬於工作(業務)執行面(者)，對於上述 3 部分而言，均非屬基層公務機關執行階層工作範疇。因此，在問卷統計數據資料上也就顯得較為低落(如表 31)。

表 31. 執行階層對 CNS27002 問卷調查各項平均百分比

第一部分	第二部分		第三部分		第四部分
安全政策	資訊安全的組織-單位內部	資訊安全的組織-單位外部	資產管理-資產責任	資產管理-資訊分類	人力資源安全
47.3%	44.9%	**13.4%**	**21.3%**	**23.6%**	37.8%
第五部分	第六部分	第七部分	第八部分	第九部分	第十部分
資訊安全區域	通訊與作業管理	存取與控制	資訊系統獲取、開發及維護	資訊安全事故管理	系統運作管理
34.3%	39.2%	33.3%	34.5%	49.7%	42.8%

第十一部分 遵循性	總平均				
41.8%	38.2%				

資料來源：本研究問卷調查結果

2. 管理階層部分：

(1) 在 CNS 27002 問卷調查各項平均百分比中，以問卷內容第 2 部分資訊安全的組織(單位外部 18.1%)、第 3 部分資產管理(資產責任 23.4%、資訊分類 33.2%)等 3 項百分比較低，其中以訊安全的組織(單位外部 18.1%)最低。

(2) 經分析結果：就基層公務機關而言，管理階層係依據上一級機關所頒布之法令、法規，督導執行階層依法執行各項資訊安全工作。對於上述 3 項部分，均不屬於其管理階層工作範籌。因此，對於資訊安全的組織及資產管理的項目，瞭解程度就略顯不足。

(3) 原因探討：在基層公務機關管理階層，係屬於督導工作性質，對於上述 3 部分而言，均非屬基層公務機關管理階層工作範疇。因此，在問卷統計數據資料上也就顯得低落(如表 32)。

表 32. 管理階層對 CNS27002 問卷調查各項平均百分比

第一部分	第二部分		第三部分		第四部分
安全政策	資訊安全的組織-單位內部	資訊安全的組織-單位外部	資產管理-資產責任	資產管理-資訊分類	人力資源安全

42.4%	49.0%	**18.1%**	**23.4%**	**33.2%**	47.0%
第五部分	第六部分	第七部分	第八部分	第九部分	第十部分
資訊安全區域	通訊與作業管理	存取與控制	資訊系統獲取、開發及維護	資訊安全事故管理	系統運作管理
38.5%	49.9%	43.5%	35.9%	49.7%	45.7%
第十部分 遵循性	總平均				
39.1%	43.5%				

資料來源：本研究問卷調查結果

3. 領導階層部分：

(1) 在 CNS27002 問卷調查各項平均百分比中，以問卷第 2 部分資訊安全的組織(單位內部 19.0%)、第 3 部分資產管理(資產責任 21.4%)及第 11 部分遵循性 24.3%較低，其中以訊安全的組織(單位外部 19.0%)最低。

(2) 經分析結果：就基層公務機關而言，領導階層仍被視為被受權者，對於重大資安事件及決策，仍屬於上一級機關權責。因此，對於資訊安全的組織(單位內部)、資產管理(資產責任)及遵循性等 3 項目，均非屬於基層公務機關領導階層可決策的部分，故對上述 3 項目的重要性仍瞭解不足。

(3) 原因探討：在基層公務機關領導階層，仍被視為被受權者，須接受

上一級機關的政策指導及命令行事。針對上述 3 項目均無決策權；因此，在問卷統計數據資料上也就顯得低落(如表 33)。

表 33. 領導階層對 CNS27002 問卷調查各項平均百分比

安全政策	資訊安全的組織-單位內部	資訊安全的組織-單位外部	資產管理-資產責任	資產管理-資訊分類	人力資源安全
40.5%	45.7%	**19.0%**	**21.4%**	35.7%	49.0%
資訊安全區域	通訊與作業管理	存取與控制	資訊系統獲取、開發及維護	資訊安全事故管理	系統運作管理
28.6%	51.7%	54.3%	48.6%	58.9%	41.1%
遵循性	總平均				
24.3%	43.8%				

資料來源：本研究問卷調查結果

五、結論與建議

5.1 結論

本研究目的係以 CNS 27002 資安規範探討基層公務機關之教育訓練，並針對基層公務機關人員以不計名方式採問卷調查，經彙整、分類、分析後，本研究得歸納以下事項：

1. 執行階層：

   大多數人員均抱持「我只是執行者」或「工作者」的態度，對於資訊安全事務，均為被動。因此，在問卷調查中第 2 部分資訊安全的組織(單位外部)所顯示的數據百分比也就僅 13.4%(最低)。這也說明執行階層的資訊安全教育課程應加強資訊安全法令(法規)的課程內容及違反資安事件的案例宣教，使執行階層亦能瞭解單位與承包商所簽定的協議書內容，於承包商至單位實施資訊系統(設備)維護、保養等工作時，可隨時監督承包商是否違反資訊安全法令(法規)，以避免因承包商疏失造成單位嚴重的資安事件。

2. 管理階層方面：

   就基層機關而言，管理階層的工作態度以「是依上級命令做事」或「這是上級單位的命令」的消極態度為多。因此，在問卷調查中第 2 部分資訊安全的組織(單位外部)所顯示的數據百分比也就僅 18.1%(最低)。但因管理階層負有督導及管理之責，在工作態度上也較執行階層略為主動，因此較執行階層 13.4%略高 4.7%。另管理階層雖負有督導及管理之責，但消極的工作態度也失去瞭解資訊安全相關法令(法規)的主動性。所以，除對管理階層應加強工作的主動性及責任心外；另仍需賡續強化資訊安全相關法令(法規)課程教育，藉以管理階層落實資訊安全的工作。

3. 領導階層方面：

   在問卷調查中第 2 部分資訊安全的組織(單位外部)所顯示的數據百分

比僅 19.0%(最低)。其原因是基層公務機關的領導階層，仍視為被授權者，對於單位發生資安事件時，常因無法即時獲得授權妥處事件，往往造成更嚴重的資安事件。因多數領導階層人員也缺乏主動瞭解承包商所簽署協議書內容的法令(法規)是否適宜；自然就對承包商所簽署協議書內容的法令(法規)的適宜性略顯不足。所以在資訊安全的組織(單位外部)所顯示的數據百分比也就相對的低落。

5.2 現行狀況

1. 現階段基層公務機關所規劃的資訊安全教育訓練課程，多數仍未依據機關各階層工作性質實施資訊安全教育訓練規劃，另也常因年度預算不足或短缺，無法依規劃期程及教育課程執行訓練工作。因此，資訊安全訓練課程也往往受年度預算不足之苦，而選擇較為便宜或無連貫性的課程實施訓練工作。如此也無法達到機關所要求的訓練成效。
2. 其次，也發現訓練課程的排定，亦常受限於「人為因素」而有所改變或簡化了課程內容。許多公務機關委託業界依機關工作性質需求，設計多套的教育課程，但因「人為因素」而取消或修正為分段式課程。同時，更發現多數機關單位在派訓時，除受訓人員非業務(工作)相關人員外，也發現受訓人員常以「出差」、「受訓即休假」、「為何是我」等諸多的心態參加教育課程，造成學習成效不彰的窘境。
3. 參與進修課程因為屬不同階層的人員，確因公務繁忙而逃避進修課程的參與。除了預算公帑浪費外，也無法更進一步改善機關單位的資安危安事件及教育訓練的精進。

5.3 未來規劃

針對目前的資安教育課程設計，歸納出以下 6 點未來規劃之建議：

1. 「課程綱要」制定：

依據機關年度工作計畫期程表，制訂下年度資訊安全「課程綱要」，主要說明訓練方針、課程目標其涵蓋面及各階層人員必需達到的課程成效。

2. 「課程發展」計畫制訂：

依據課程綱要內容及機關各階層業務所需之課程，制訂課程發，其內容應包括：課程目標、訓練對象、要求時程、教學設計、評量方式、師資規劃等。

3. 「因才施教」:

除在課程教材上，應針對資訊安全認知程度不同的人員，設計其適妥內容。例如，針對管理及領導階層所設計的課程，應規劃全面性的資訊安全課程，注重於法令、規章等法律條文；而執行階層則依機關業務需求設計與業務相關的資安教材。

4. 「活化教材」:

除依據機關不同階層設計相關教材外，教材亦以「生活化」、「平易化」、「遊戲化」等方式來呈現教材的內容及重點，以提升各階層人員的學習興趣，也可達到資訊安全教育訓練的成效。

5. 「稽核追蹤」：

各階層人員完成資訊安全教育訓練課程後即輔以測驗外，另機關亦定期實施各項資安訓練成效檢驗，初次未達稽核標準，應加強在職教育訓練，仍未達標準者，即檢討調整工作，以減低因「人」而造成資安事件。

6. 「資安宣導」工作：

除了制訂各項資訊安全教育訓練課程外，仍需不定期針對機關各階層實施資訊安全工宣導，以循序漸進的方式改進個人使用資訊設備的習慣，以降低資安及公務機密外洩事件危機。

參 考 文 獻

中文部分

1. 潘天佑，2008，資訊安全概念與實務，2008 年 12 月初版，頁 1-2。
2. 徐桂尼，2010，「2010 年台灣寬頻網路使用調查報告」，1 月 18 日至 2 月 12 日，頁 1-3。
3. 資安人雜誌，資安人雜誌第第 67 期，「威脅又新又快又厲害」，頁 82-86，2010 年 1 月/2 月。
4. 資安之眼網站(2010 年 3 月 11 日)發表。
5. 羅英嘉，2007，財團法人資訊工業策進會，「CISSP 與資訊安全基礎技術」，97 年 3 月，頁 1-3。
6. 左豪官，2009，資訊安全事件分析及管理作為。
7. 黃亮宇，1992，資訊安全規畫與管理，松崗圖書。
8. 吳琮璠、謝清佳，2003，資訊管理：理論與實務，智勝，92 年 06 月 17 日。
9. 周宣光，管理資訊系統--- 管理數位化公司（Management Information Systems:Managing the Digital Firm, 7th Ed.)，東華，2007 年 9 月 12 日。
10. 李順仁，2007，資訊安全，文魁圖書，96 年 10 月 31 日。
11. 蕭瑞祥，2006，資訊安全認知訓練之規劃與設計，95 年 4 月 15 日。
12. 李永山、張勇翔(2004)，結合 BS7799 與資訊安全藍圖建構資訊安全評估機制之研究，94 年 6 月。
13. 邱瑩青(2009)，資安人雜誌第 34 期，「資訊安全最大的威脅-人員安全」，2009 年 8 月 31 日
14. 林翠娥、程毓明、鄭進興，2006，國軍人員資訊安全素養之評量與分析。
15. 吳倩萍，2006，政府機關個人資訊安全認知與行為之探討。
16. 范錚強、范懿文、侯永昌、李世才，2007，資訊管理導論，旗標出版股份有限公司。
17. 許雪蓮，2006，以 BS 7799 為基礎評估軍事單位資訊安全環境之研究。

18. 行政院國家資通安全會報技術服務中心，2009， CSI 2009 年電腦犯罪與安全調查報告，http：//www.icst.org.tw/icst_page.aspx，2009 年 12 月 24 日。
19. 行政院國家資通安全會報技術服務中心，2010，資料外洩案例，http：//www.icst.org.tw，2010 年 1 月 29 日。
20. 紀佳妮，行政院國家資通安全會報技術服務中心，2010，公務人員資安職能課程開發與施行，http：//www.icst.org.tw，2010 年 6 月 4 日。
21. 財團法人台灣網路資訊中心(TWINC) ，2010，「2010 年台灣寬頻網路使用況狀調查摘要分析」，2009 年 12 月 17 日-2010 年 3 月 10 日，pp.1-59(台北,台灣)。
22. 教育部，2010，中小學網路素養與認知：網路法律，http://eteacher.edu.tw/8_law.asp。
23. 王昭濱，2007，黑澀會美眉裸照被駭走，http://tw.nextmedia.com/applenews/article/art_id/3395511/IssueID/20070414。
24. 魏紜鈴(2010)，資安人雜誌第第 67 期，「人若擺不平，資安難太平」，頁 71-75，2010 年 1 月/2 月。
25. 經濟部標準檢驗局，http://www.bsmi.gov.tw。
26. 行政院主計處，2007，97 年電腦應用概況報告，http://www.dgbas.gov.tw/public/Attachment/992811305871.pdf
27. 自由時報，2008，2008 年 9 月 28 日報導「分享軟體出包？防外洩，警局要刪除家中資料」
28. 吳琮璠、謝清佳，2003，資訊管理：理論與實務，智勝，2003 年 06 月 17 日。
29. 朱延智，2007，企業危機管理，五南，2007 年 10 月 01 日。
30. 李順仁，2007，資訊安全，文魁圖書，2007 年 10 月 31 日。
31. 陳麗珠、柏松齡，2003，客戶資料外洩花旗暫停網路申請業務，自由時報，大紀元，2003 年 11 月 12 日，取自：http://www.epochtimes.com/b5/3/11/12/n409636.htm。

英文部分

1. IBM, 1984, IBM Data Security Support Programs。
2. Rossouw von Solms, Driving Safely on the Information Superhighway,Information Management & Computer Security, 5(1), 1997, pp. 20-22.
3. NITS Special Publication 500-172 Computer Security Training Guide ,November 1989
4. ISO, Information Technology --- Security Techniques --- Code of Practice for Information Security Management, ISO, ISO/IEC 17799:2005, 2005.

附 錄 ： 問 卷 樣 本

敬啟者您好：

BS 7799 是 1995 年由英國標準協會所提出，為世界所公認的資訊安全規範及認證標準，是一套完整的計畫，依我國資訊安全制定一套資訊安全管理之作業規範(CNS 27002)，本問卷是以國家標準(CNS 27002)為基礎，目的藉由 CNS 27002 瞭解對資訊安全認知。

希望能借重您的寶貴經驗與思維，懇請您撥出一點時間回答此問卷，您的回答對此研究有很重要的價值與貢獻，希您不吝指導。

本研究所得資料內容僅供學術研究參考，不做任何發表與存證，感謝您的熱心協助及參與。

敬祝

事事順利，身體健康！

樹德科技大學資訊工程研究所

指導教授：林峻立教授

研 究 生：閻一平

敬上

第一部份：安全政策

請就您的看法在適當的□內打『Ｖ』

1、您認為資訊安全政策是否需要公告？

□1、非常需要□2、需要□3、普通□4、不需要□5、重大政策才公告

2、您認為安全政策是否需要召集人員說明其重要性？

□1、非常需要□2、需要□3、普通□4、不需要□5、網頁公告即可

3、您認為資訊安全政策的法令規章，應該由誰負責公告？

□1、使用者□2、資安主管□3、員工□4、單位主官□5、都可以

第二部份：資訊安全的組織

請就您的看法在適當的□內打『Ｖ』

一、單位內部

4、您認為管理階層是否需要了解組織內部的管理資訊安全？

□1、非常需要□2、需要□3、普通□4、不需要□5、無所謂

5、您認為管理階層是否需要明確的支持組織內部的資訊安全措施？

□1、非常需要□2、需要□3、普通□4、不需要□5、無所謂

6、您認為資訊安全的協調工作是否僅資訊安全部門人員可以擔任？

□1、視協調工作而定□2、是□3、否□4、只有主管可以執行資訊安全協調工作□5、只有高階長官可以擔任

7、您認為資訊安全責任的配置應該為何？

□1、全體人員□2、資訊部門人員□3、資訊部門主管□4、管理階層人員□5、不需特別配置

8、您認為資訊處理設施的授權過程是否要上級單位全權負責，還是下授分級負責？

□1、上級單位全權負責□2、下授分級負責□3、視設備機敏等級而定□4、不需特別歸類□5、視單位性質而定

9、您對資訊安全工作內容屬於機密性的規定與要求是否瞭解？

□1、非常瞭解□2、瞭解□3、普通□4、不瞭解□5、完全不瞭解

10、您認為資訊安全工作是否要不定期與主管機關聯繫或由主管機關提供相關資訊給您？

□1、要□2、需定期與主管機關聯繫□3、只需不定期與主管機關聯繫□4、只需由主管機關提供相關資訊□5、都不需要

11、您認為資訊安全的相關資訊是要如何建立？

□1、由上級單位不定期發布□2、由單位資安部門定期發布□3、由個人自行蒐集資料運用□4、都可以□5、無所謂

12、您認為資訊安全審查的工作應該由誰(部門)負責？

□1、管理階層□2、部門主管□3、業務承辦人□4、使用者提出申請□5、任何人都可以

13、在工作中發現違返資訊安全法規或產生疑慮時，您的態度為何？

□1、立即通知資安部門□2、下班後再通知□3、工作結束後再通知□4、事不關己□5、完全不通知

14、當收到不明E-mail信件時，您的作法為何？

□1、立刻刪除並通知資安部門□2、開啟看看□3、開啟後再轉寄同事□4、開啟後並通知資安部門□5、立即轉寄給大家

二、單位外部

15、單位與承包商簽訂協議書中，是否應該包含資訊安全政策、軟硬體資產、資料完整性、不受惡意軟體攻擊控制措施等項目？

□1、由單位決策者決定□2、都可以□3、視協議項目而定□4、應該要且要更完善□5、由資安部門主管決定

16、您認為單位資訊與處理設備的安全，是否不宜因導入承包商的資訊產品而降低服務品質？

□1、應該維持服務品質□2、都可以□3、若產品價錢可以更低廉，服務品質稍降可以接受□4、應該要且要更完善□5、由資安部門主管決定

17、因單位任務需求需與承包商(以外單位)共同工作，要求存取單位資訊與處理設備時，或由承包商(以外單位)提供相對性之產品(設備)，您認為是否應該要先行完成風險評鑑後再行決定？

□1、視承包商所提供的設備有無涉及機敏性決定□2、相信承包商(以外單位)□3、承包商所提供的設備因風險性一律不允許使用□4、一定要□5、都可以

第三部份：資產管理

請就您的看法在適當的□內打『Ｖ』

一、資產責任

18、您認為單位的資產清冊應由誰來負責管理？

□1、上級單位□2、管理階層□3、資安部門□4、業務承辦人□5、使用者

19、您認為單位的資訊資產的擁有權應該由誰負責？

□1、上級單位□2、管理階層□3、資安部門□4、業務承辦人□5、使用者

二、資訊分類

20、您認為資訊分類是否應依資訊的價值、法律要求、敏感性及重要性加以分類嗎？

□1、不一定□2、由單位決策者決定□3、由資安部門主管決定□4、由業務承辦人決定□5、一定要

21、您認為資訊標示與處置是否應該依照單位所採用的分類法，訂定一套適當的資訊標示與處置程序？

□1、若承辦人已經非常熟悉流程則不需要訂定程序□2、都可以□3、由資安部門主管決定□4、由業務承辦人決定□5、一定要

第四部份：人力資源安全

請就您的看法在適當的□內打『Ｖ』

22、您認為單位、承包商及使用者的安全角色與責任，是否應依照單位的資訊安全政策加以界定與文件化？

□1、無所謂□2、都可以□3、由資安部門主管決定□4、由單位決策者決定□5、需要

23、您認為安全角色與責任是否應包括下列要求：依單位的資訊安全政策實作與行動；保護資產不受未經授權的存取、揭露、修改、消毀或干擾；特定的安全過程與活動；指派專責人員管理；通告資安事件或潛存的風險因子？

□1、一定要□2、由資安部門主管決定□3、都可以□4、由單位決策者決定□5、單位內任何一位人員階可

24、您認為應該由那些人簽署資訊安全保密協議書(切結書)？

□1、單位全體人員□2、資安部門主管□3、資安管控中心值勤人員□4、單位各部門主管□5、不一定要簽署

25、您認為應該由誰參加資訊安全認知、教育及訓練課程？

□1、自由參加□2、資安部門主管□3、資安管控中心值勤人員□4、單位各部門主管□5、單位全體人員

26、您認為資訊安全認知、教育及訓練課程是否應適切有關單位人員的職務、責任與技術加以分類實施？

□1、皆可□2、不分職務、責任與技術□3、尊重個人意願□4、由單位長官決定□5、應該適切分類實施

27、發生資訊安全違例事件，但尚未詳實查證前，您認為是否宜先行懲處以示負責？
□1、立即懲處□2、先調查事件嚴重性□3、證據蒐集、調查確認、再行懲處□4、視資安部門主管決定□5、由單位決策者決定

28、您認為懲處過程最主要的意義為何？
□1、重懲重罰□2、嚇阻及預防□3、調(離)職□4、依法究辦□5、賠嘗損失

第五部份：資訊安全區域

請就您的看法在適當的□內打『Ｖ』

29、您認為資訊設備的周邊安全是否為資訊安全的一環？
□1、若周邊安全無虞則不需歸到資訊安全內□2、視資訊設備的性質決定□3、是□4、不是□5、兩者之間沒有關聯

30、您認為資訊設備周邊環境應該如何設置？
□1、單獨環境及門禁管制□2、設置在資訊部門辦公室由該部門人員管制□3、設置在單位保全室由該室人員管制□4、設置在單位決策者辦公室由單位決策者管制□5、只要辦公室都可以

31、您認為資訊設備周邊環境應如何管理？
□1、設置24小時監視器嚴密門禁管制□2、除資管人員外其餘均管制□3、單位內外人員全數管制□4、以上均是□5、隨機驗證管制

32、您認為資訊設備的安全保護應該有那些？
□1、資訊線佈的規劃□2、人員進出暨資訊設備攜出入管制□3、電力設備□4、環控設備□5、以上均是

33、您認為設備安全的管理應該有那些？
□1、設備定期的維護□2、資訊設備攜出入管制□3、緊急支援的設施建置□4、設備軟體版本更新□5、以上均是

第六部份：通訊與作業管理

請就您的看法在適當的□內打『Ｖ』

34、您認為資訊作業之程序與責任的目標為何？(1)確保資訊設備操作及(2)確保資料庫安全？

□1、確保資訊設備操作□2、確保資料庫安全□3、以上皆是□4、不一定□5、視程序的性質為何

35、您是否認為資訊設備的操作程序應該視為單位正式文件？
□1、不是□2、是□3、若操作程序簡易就不需視為正式文件□4、由資安部門主管認定□5、視資訊設備的重要程度而定

36、您認為資訊安全控制措施是否應分隔為開發、測試及運作之設施，以降低運作系統未經授權存取或變更的風險？
□1、都可以□2、不應分隔□3、由資安部門主管認定□4、視單位工作需求□5、應該分隔

37、您認為承包商將資訊系統交付前，是否應依約定協議書內容逐一驗證及實作無誤後，始由單位予以使用及維持？
□1、不一定□2、由雙方約定□、3隨機驗證□4、視單位工作需求□5、應依約定執行

38、單位接收資訊系統後，您認為承包商是否應該定期提供咨詢、報告及稽核等服務？
□1、是□2、不一定□3、不定期□4、視承包商公作期程□5、依約定執行

39、您是否認為對抗惡意碼的控制措施應實作防範惡意碼的偵測、預防及復原控制措施以及適切的讓使用者瞭解程序？
□1、不一定□2、是□3、不是□4、視工作需要□5、由使用者決定

40、您是否認為資料備份的目標在於維持資訊資料及資訊設施的完整性與可用性？
□1、不是□2、是□3、只能維持資料的完整性與可用性□4、只能維持設備的完整性與可用性□5、不需要備份

41、您是否認為網路安全管理的目標在於確保網路內資訊與支援性基礎建設的保護？
□1、不是□2、是□3、只能確保網路內資訊□4、只能確保支援性基礎建設□5、由資安部門主管認定

42、網路控制措施除應適切的加以管理與控制，使其不受威脅外，您認為還應包括下列那些？(1)網路系統安全(2)應用程式安全(3)傳輸中的資訊安全
□1、(1)□2、(2)□3、(3)□4、以上皆是□5、皆不需要

43、您是否認為網路服務安全應識別所有網路服務的安全特徵，其中服務水準及管理要求，也應備納入網路服務協議中？
□1、都可以□2、都應該□3、只需納入管理要求□4、只需納入服務水準□5、皆不需要

44、您是否認為媒體的處置目標在於防止資產被未經授權的揭露、修改、移除獲破壞，以及運作的中斷？
□1、是□2、不是□3、不一定□4、無法防止資產被未經授權的移除□5、無法避免運作中斷

45、您認為資訊媒體的汰(換)除是否應以正式作業程序執行並且安全無害的方法汰(換)除？
□1、是□2、不是□3、不一定□4、非正式的簡便程序即可□5、依媒體的形態決定

46、您認為是否應制定適當的正式交換政策、程序及控制措施，以保護經通訊設施的資訊交換？
□1、是□2、不是□3、不一定□4、由資安部門主管決定□5、視單位工作需要決定

47、您認為是否應建立營運資訊系統，以保護與營運資訊系統互連有關的資訊？
□1、是□2、不是□3、不一定□4、由資安部門主管決定□5、視單位工作需要決定

48、您認為電子商務控制措施是否應保護在公眾網路上傳輸有關電子商務的資訊時，使之不受詐欺行為、契約爭議及未經授權的存取？
□1、不能使之避免契約爭議□2、不能使之避免不受詐欺行為□3、電子商務監控措施才能，而非電子商務控制措施□4、不能使之避免未經授權的揭露與修改□5、是

49、稽核日誌係使用者活動、異常及資訊安全事件的記錄，您認為稽核日誌是否有其必要性且宜保留一段議定的期間，以協助未來調查與存取控制監視？
□1、若一切正常即可刪除避免浪費儲存空間□2、由資安部門主管認定□3、是□4、一般使用者無需產生稽核日誌□5、不是

50、您是否認為日誌資訊的保護控制措施應為下列何者，才能確保不受竄改與未經授權的存取？

□1、保護存錄設施□2、保護日誌資訊□3、以上皆是□4、以上皆不是□5、視日誌性質決定保護控制措施

第七部份：存取控制

請就您的看法在適當的□內打『Ｖ』

51、您認為控制資訊的存取是否應基於存取的營運與安全要求，以建立文件化及審查存取控制政策？

□1、不一定□2、視單位需求□3、一定要□4、控制資訊的存取與存取的營運無關□5、視資訊的機敏程度而定

52、您認為使用者是否有防止未經授權之使用者存取資訊與使用設施的責任，以避免資訊資料及設施遭受竊盜或破壞？

□1、是□2、應為資安人員的責任□3、不一定□4、視使用者而論□5、視資料性質而定

53、您是否認為應該將資訊服務、使用者及資訊系統各群組使用的網路加以區隔分類？

□1、是□2、視單位使用需求□3、由資安部門主管認定□4、不需要□5、都可以

54、您認為單位公用程式的使用是否應加以限制與嚴密監控不當程式之使用？

□1、不該限制□2、由資安部門管制□3、不一定□4、需要限制□5、只需監控即可

55、您認為敏感系統的隔離是否應該有專屬的(隔離的)電腦作業環境？

□1、需要□2、有安裝監視系統就無需隔離□3、由資安部門主管認定□4、無需隔離只需加強使用人員管控□5、不需要

第八部份：資訊系統獲取、開發及維護

請就您的看法在適當的□內打『Ｖ』

56、您認為系統使用方式是否應併入查核，以偵測經由錯誤操作或故意行為所造成之資訊損毀？

□1、是□2、不是□3、由資安部門主管認定□4、無須併入□5、視單位需求

57、您認為單位是否應妥善管理金鑰，以支援單位使用密碼技術？

□1、不一定□2、由上級單位備妥管理□3、由資安部門主管備妥管理□4、一定要□5、視單位需求

58、您認為系統檔案的作業軟體、測試資料的保護等安全管理是否應備妥各項程序、保護及管制，以確保系統檔案的安全？
□1、一定要□2、視單位需求□3、由資安部門主管決定□4、依使用者需求決定□5、不需要

59、您認為作業系統變更時，是否應審查與測試重大的應用系統，以確保對單位作業或資訊安全無不利的衝擊？
□1、視單位需求□2、一定要□3、由資安部門主管決定□4、依使用者需求決定□5、不需要

60、您認為承包商進行單位作業系統軟體開發、維護、修改及測試時，單位是否應檢派相關資訊人員隨同監督，以避免機密資料外洩？
□1、單位人員陪同即可□2、由資安部門主管陪同□3、由資安部門人員隨同□4、視業務軟體機敏性決定□5、不需要派員

第九部份：資訊安全事故管理

請就您的看法在適當的□內打『Ｖ』

61、您認為通報資訊安全事件與弱點的目標為能夠採取即時矯正措施以確保資訊系統資料庫的安全？
□1、是□2、有通報獎金可以拿□3、可以列為績優人員□4、以上皆是□5、不是

62、您認為是否應要求單位全體人員及承包商通報任何觀察到資訊系統可疑的安全弱點？
□1、不是□2、是□3、可疑的安全弱點可立即改善就不需通報□4、由資安部門專職負責□5、只需通報嚴重安全弱點

63、從資訊安全事故中，您是否認為資訊安全事故的型式、數量及成本應量化與監視？
□1、是□2、以嚴重事件為主□3、不一定□4、由資安部門主管決定□5、由事故型式決定

64、資訊安全事故發生後，對當時單位及人員蒐集的證據，若涉及法律行動(民事或刑事)，您是否認為應適當保存，以利審判時提出證據的說明。

□1、是□2、隨機蒐證□3、不一定□4、由資安部門負責□5、都可以

第十部份：系統運作管理：

請就您的看法在適當的□內打『Ｖ』

65、您認為管理系統運作資訊的目標為何？(1)單位系統突然停止運作時，能保護系統不受損壞及重要資料的安全，並(2)確保系統能即時再運作？

□1、僅能保護資料的安全□2、僅能維持系統部份的運作□3、以上皆是□4、以上皆非□5、視系統特性而定

66、單位系統運作管理的發展與維持，您是否認為應該納入資訊安全作為，以維持系統運作管理正常？

□1、由資訊安全部門主管認定□2、不需要□3、應該□4、由系統管理員自行認定□5、由單位主官認定

67、您是否認為資訊安全需持續要求，且系統運作管理與維護需有優先順序？

□1、是□2、不需要□3、資訊安全僅需不定期要求即可□4、由系統管理員認定□5、系統運作管理與維護無優先順序都很重要

68、您認為系統是否應定期測試與更新，以確保系統資料維持在最新及有效的狀況？

□1、由業務承辦人自行認定□2、要定期更新與測試□3、不一定□4、由資訊安全部門主管認定□5、不需要定期測試與更新

第十一部份：遵循性

請就您的看法在適當的□內打『Ｖ』

69、您認為遵循適法性要求的目標是為何？避免違反(1)任何法律、法令、法規(2)契約義務(3)任何安全要求？

□1、避免違反(1)□2、避免違反(2)□3、避免違反(3)□4、以上皆是□5、不需遵循適法性要求

70、您認為個人資訊的資料保護與隱私是否應符合相關法令、法規及適用的契約條文所要求，以確保資料保護與隱私？

□1、一定要□2、視個人需求公開□3、可以公開□4、不需要□5、若上級要求可適度公開

71、您認為資訊安全管理人員是否應確保其工作責任範圍內所有安全程序皆正確執行，以配合各項安全政策與標準？
□1、要□2、為了效率有些程序可以省略□3、只需確保重要工作的安全程序即可□4、不需要□5、視資安部門主管決定

72、您是否認為資訊系統稽核考量的目標在於最大化稽核過程的有效性，並使結果所受之干擾降至最低？
□1、不是□2、無法降低干擾□3、視資訊系統的性質決定目的□4、無須最大化□5、是

73、您是否認為智慧財產權應訂定適當法規，以確保當使用的資料可能涉及智慧財產權或所使用的專屬軟體產品時，可遵循法律、法規及契約的要求？
□1、不是□2、視所使用的資料性質決定□3、是□4、視單位需求□5、以口頭方式取得所有權人的同意即可

第十二部份：基本資料

請就您的看法在適當的□內打『Ｖ』

一、請問您的性別：□男□女

二、請問您的年齡為：
□20歲以下□20歲~24歲□25歲~29歲□30歲~34歲□35歲~34歲□35歲~39歲□40歲~49歲□50歲~59歲□60歲以上

三、請問您的學歷為：□國小□國中□高中(職)□專科□大學□碩士(含)以上

四、請問您的級職為：□士兵□士官□士官長□尉官□校官

五、請問您的職務為：
□人事□情報□作戰□後勤□補給□工程□通資電□資訊□文書□行政□通資電□電子

六、請問您是否參加過相關資訊安全教育課程訓練？□是□否

七、請問您實際從事相關資訊安全工作多久？
□3個月以下□6個月□1年□3年□5年以上