警察資通安全認知之研究_以台北縣政府警察局為例

林宜隆 [1]　邱士娟 [2]　呂明達 [3]
警察大學資訊管理系教授 [1]
台北縣政府警察局資訊室 [2]
銘傳大學資訊管理系研究生 [3]
paul@mail.cpu.edu.tw[1]
cathy@tcpsung.gov.tw[2]
s4750303@ms24.mcu.edu.tw[3]

摘要

在資訊科技與網際網路盛行的現代，資訊已成為我們日常生活的一部份，不論它以什麼樣的形式出現，舉凡食、衣、住、行、育、樂等都日漸受其的影響。而近年來資通安全(Cyber Security)事件不斷發生，相關資訊犯罪案件及手法不斷的翻新，為保護資訊相關資產，確保營運的持續，各國無不加強各種資通安全作為。本研究係以蒐集國際資通安全規範、我國資通安全規範、我國資通安全管理政策及警政署資通安全管理規定等相關資料研析後，並參考美國國家標準與技術研究院(NIST)資通安全認知教育及訓練等資料歸納分析，並以台北縣政府警察局員警進行問卷調查，據此提出我國警察資通安全認知訓練建議事項。

關鍵詞：資通安全認知、美國國家標準與技術研究院、警察資通安全。

Abstract

In this new century of information technology and the Internet, information plays a very important part in our daily life. Our life – in the aspect of eating, clothing, housing, transportation, education and entertainment – is being changed in gradual but profound way by the onward march of information science and technology in various forms. In recent years, reports of cyber security breach are often heard. New crimes with various modus operandi are unfolded. Many countries have increased their cyber security in order to protect information assets and to ensure business operation. This thesis has collected international and domestic codes and regulations of cyber security, including the security management policy of Taiwan and the regulations from the National Police Agency of the Ministry of the Interior. A questionnaire was circulated among policemen of the Taipei County Government's Police Bureau. The database and the result of the questionnaire are analyzed with the reference from reports of cyber security cognitive education and training of the National Institute of Standards and Technology (NIST). Suggestions on the cyber security training of Taiwan's policemen are also given in the thesis.

Keywords: Cyber Security Awareness, NIST, Police Cyber Security.

1. 前言

資通安全問題自古以來就是一個為人類所關注的問題，大到國家社會的安全，小到個人隱私的保護，在不同的年代都會衍生一套符合當時的資通安全處理的方法與技術。例如早在凱撒大帝時代為解決通訊安全而創造出凱撒密碼，即使訊息遭到敵軍攔截也無法解讀通訊內容；在二次大戰期間，敵我雙方各種攻擊計劃、軍情部署等機密資料，為防止外洩或傳送途中被劫走，發展了各種加、解密等機制，使資訊能夠安全的傳送與接收正確的資訊[3]。而隨著各行政機關的電腦化與網際網路傳輸資料的便利，如何加強維護資通安全之責任，確保資訊的機密性、完整性及可用性，是當前各行政機關推動 e 化所應注意的課題。並且隨著民主政治的發展，民眾越來越注重個人的隱私及安全，如果政府機關外流民眾的資料，甚至藉以謀利，則如何建立民眾對政府的信心。而警察機關亦隨著資訊科技的發展進行各項軟、硬體開發供同仁平日勤、業務之需要；但是根據調查各警察機關對資通安全的管理概念不但非常薄弱，甚至對於現有的資訊環境與資安專家的安全認知程度亦有很大的差異[10]。

2. 資通安全認知相關文獻探討

2.1 資通安全管理的意義

對於資通安全管理的定義，Chelsa Russell[1]認為「資訊安全管理是在保護舉凡跟電腦安全有關的所有事物，包括電腦本身及其內容之軟體、應用程式、資料及終端機、印表機、磁帶及磁碟，甚至整個電腦室的安全皆屬之」，因此我們可以說資訊安全管理的最終目的即在於確保資訊的機密性、完整性及可用性。[9]

而現今因為資訊與電腦網路的發達，資訊的傳達亦需依賴通訊網路的傳送，否則如何開展 B2B、B2C 等的電子商務活動，因此資通安全管理是一個全面性的任務，不只是對硬體進行資通安全管理，

亦應包含組織內執行任務的人及其他相關的活動行為。

2.2 資通安全認知

2.2.1 資通安全認知的意義

CNS 17799[8]中提到，為了確保使用者了解資通安全的威脅及問題，並有能力在正常工作中支持組織安全政策，以及訓練使用者各項安全程序和正確使用資訊處理設施，以降低可能的安全風險。因此在現今高度網路化的時代，必須確保以下三點：1.了解他們在組織中的角色和責任。2.了解組織的資通安全政策、程序和實行。3.擁有和負責的業務相關知識其用來保護資訊資源，包括管理、作業和技術的控管，如此組織才能保護資訊的機密性、完整性和可用性。

NIST（National Institute of Standards and Technology）Special Publication 800-16[5]認為認知是改變人或組織態度和觀念的學習過程，以了解資通安全的重要以及違反規則時所反映出的負面結果。在認知活動中，學習者是資訊的接收者，認知依賴著具有吸引力的套裝技術來撼動廣大的聽眾，學習者透過一個短期、立即性和特定性的認知活動來達成學習目的。從學習的觀點來看，認知的影響範圍是短期的，學習層級屬於告知學習者“what”資訊，透過錄影帶、海報或新聞報紙的方式，目標是讓學習者認識和有深刻的記憶，且可以使用是非或選擇的衡量或測試方式來驗收成果。

資通安全認知的成果是設計用來改變或加強安全行為的實行，在 NIST Special Publication 800-50[6]文件中，資通安全認知被定義為：認知就是將注意力著重在安全，認知意指給予個人識別資訊科技安全考量並能相對的作出回應。Chelsa Russell[1]認為，資通安全認知的目的是提昇安全與安全控管重要性的集體認知，資通安全認知訊息必須簡單清楚並讓目標對象容易了解。

有效的資通安全認知方案的設計必須有助於日常的作業流程，並且必須是不間斷的、積極的創新，才能吸引學習者的注意，學習者吸收後才會意識到安全考量。如此才容易改變別人的行為。

2.2.2 資通安全認知對象

所有的人包含管理者、開發者、維護者、和使用者都必須接受資通安全認知的訓練和教育，而訓練和教育必須是選擇性的，以適合個人的職務和需求為主。Robert Held [7]認為，教育使用者可由設計良好的資通安全認知方案來達成，執行的步驟中必須清楚定義對象是誰，並建議分成：高階員工、中階員工、基層員工。NIST Special Publication 800-16[5]中將目標對象分為兩大類，分別是技術性對象和非技術性對象，技術性對象包含：安全專家、管理者、程式設計師；非技術性對象包含：管理者、系統擁有者、其他人員，整理如表 1 所示。

表 1 目標對象種類表（NIST SP 800-16）

技術性對象	非技術性對象
安全專家	管理者
■ 資通安全官	■ 經理/行政
■ 資通安全管理者	■ 技術人員管理者
■ 安全工程師	■ 非技術人員管理者
管理者	系統擁有者
■ 網路	■ 網路(WANs/LANs)
■ 系統	■ 應用系統
■ 資料庫	■ 資料庫
■ 電子郵件/語音信箱	其他人員
程式設計師	■ 法律業務
■ 系統	■ 契約職員
■ 應用系統	■ 人力資源
	■ 一般使用者

2.2.3 資通安全認知內容收集

NIST Special Publication 800-50[6]提到，組織可以利用許多種方法，從眾多的資訊來源中決定到底哪些資通安全認知的資訊是必須，收集這些資訊的方法包含：

一、訪談所有關鍵的群組和組織。

二、整個組織的調查。

三、重新檢閱和評估所有可得的資料，例如現有的認知教材、訓練計劃和參與者名單。

四、分析和認知有關的資料。

五、重新檢閱一般系統和主要應用系統的安全計劃，來確認系統和應用系統擁有者並指派安全負責人。

六、重新檢閱系統目錄和應用程式使用者的身份來判定存取權限。

七、從任何疏忽的、出錯的紀錄裡，重新檢閱發現或建議。

八、和管理者、應用系統擁有者或使用者面談或訪談。

九、分析任何安全事件可能可以知道必須訓練什麼或哪一群人必須訓練。

十、當技術或架構有改變時必須重新檢閱。

十一、從產業、學術、政府部門發行的刊物或訓練與教育機構中了解趨勢。

這些方法均有可能會讓組織提早了解其問題所在，並發揮“及早預防”的作用。

2.2.4 資通安全認知內容

NIST Special Publication 800-50[6]提到，認知素材的建立必須秉持著“那些行為必須被強調”和“那些技術目標對象必須學習且應用”的精神，現今有許多主題在認知的活動中被提及和討論，這些主題包含：密碼的使用和管理，避免病毒、蠕蟲、木馬程式和其他惡意攻擊的政策，不明的電子郵件和郵件之附加檔案，web 的使用，垃圾郵件，資料的備份和保存，社交工程，事件回應，系統環境的改變，存貨和財產的運送，個人使用和獲得的問題，手提式裝置的安全問題，在網際網路傳遞敏感或機密資訊時必須加密，工作中個人所擁有的系統和軟體，系統修正程式，組織系統中支援或允許的軟體，存取控制議題，個人責任，確認通知方式的使用，訪客和實體空間控管，保護有機密考量的資訊，電子郵件規矩等。

NIST Special Publication 800-16[5]提到，隨著 IT 系統的規模越來越大及資訊科技的日新月異，在不考慮 IT 系統的規模及成長的比率之下，一些有效且基礎的 IT 安全計畫及環境，這些項目及概念必須學習與應用在獨立的安全認知程序上用以訓練及教育。其資通安全的內容可分為基礎和知識，以“ABC’s of Information Technology Security,”的 26 個字母排列項目來說明其關係，基礎包含了資通安全相關的字彙和觀念，分別如表 2 所示。

表 2　NIST SP 800-16 資通安全認知項目一覽表

A	工作時知道那些資產是需要保護且具價值的。（例如那些硬體、軟體、資料等）
B	工作的資料與作業，應有的備份措施程序。（例如個人資料定期備份等）
C	當資通安全事件發生時(例如中毒、被入侵)，清楚知道應採取適當回應對策。
D	在工作中知道不同的作業系統有不同單位負責分配（資訊）資源與授權系統權限。
E	知道隨意詢問或查閱同事的私密資料是不道德的。(例如身分證字號、生日)
F	F6 – 清楚防火牆的功能。(例如組織內實施與 Internet 的隔離，防止非本局人員進入)
	F7 – 清楚知道責任區分之機制的用意。(例如在不同的工作職位有不同的權限的分別)
G	清楚知道資通安全是機密性、完整性、可用性為其目標與其所代表之含意。
H	清楚什麼樣的行為稱為駭客。
I	清楚在工作時的行為應有的責任。(例如違反保密協定時之懲戒)
J	瞭解自己在工作職掌中自己的角色及被授權的權責。
K	遵守資通安全措施(例如定期掃毒、更改密碼等)，並能具備資通安全相關知識，意識到可能的威脅。
L	清楚目前國內各項與電腦資訊相關的法令內容。(例如電腦處理個人資料保護法)
M	對於不同工作所賦予的角色責任，其資通安全訓練要求也會有所不同。
N	N15 – 不同的工作性質會有不同層級的存取權限(例如對於某個內部文件只能閱覽，而不能修改)
	N16 – 資訊科技的日新月異，需持續地學習(例如新病毒的防治方法)
O	警察局內各項需要保護且具價值的資訊資產，需建立起責任機制。(例如資產的所有權指派)
P	知道工作中的資通安全政策與程序之內容是描述資通安全的目標與措施
Q	瞭解工作中安全品質控管的措施(例如警察局員警離職時，其密碼及帳戶應立即刪除其使用權限)
R	對於資通安全與投入成本要有成本效益的觀念。
S	是否曾受過資通安全使用、維護、發展的資通安全訓練。
T	.對於資通安全的威脅是無時無刻都會發生，尤其在無預警的狀況下。(例如：警察局的網路流量突然超過負荷，導致網路中斷的情況)。
U	工作中的各項識別之密碼是賦予個人應負之責任，以及對存取進行控制的意義
V	在單位中工作時資通安全環境的脆弱點，會影響到系統的安全(例如：警察局人員缺乏安全認知、未裝有防火牆、防毒軟體等)
W	W25 – 知道浪費的行為會造成警察局資通安全的危機(例如：無人使用之空 IP 位址)
	W26 – 欺瞞的行為會造成警察局資通安全的危機(例如：使用別人的密碼進入系統)
	W27 – 濫用的行為會造成警察局資通安全的危機(例如:利用權限存取公司內部文件洩漏機密)
X	資通安全事件有可能會發生在警察局內未授權人員的身上(例如:記者可隨意使用警察局內部網路)
Y	清楚自身的行為是可以增強或減弱警察局的資通安全環境(例如:定期更換密碼可讓資訊環境更安全，反之則容易遭人破解)
Z	實體與技術上作到獨立的安全環境對於警察局之資通安全事件影響(例如:伺服器建置在不同主機上）的觀念

本研究以美國國家標準技術研究院(National Institute of Standard and Technology，簡稱 NIST) Special Publication 800-16[5]所提出的「ABC’s of Information Technology Security」做為討論之項目。

3. 研究設計與分析

3.1 研究架構

本研究參考文獻經過整理分析所得結果，以 NIST SP 800-16 所提出的「ABC’s of Information Technology Security」做為問卷參考，分為二個項目基本資料（個人背景）及對資通安全認知項目瞭解程度，來探討警察人員對各個資通安全認知項目的瞭解程度，本研究架構如圖 **1** 所示：

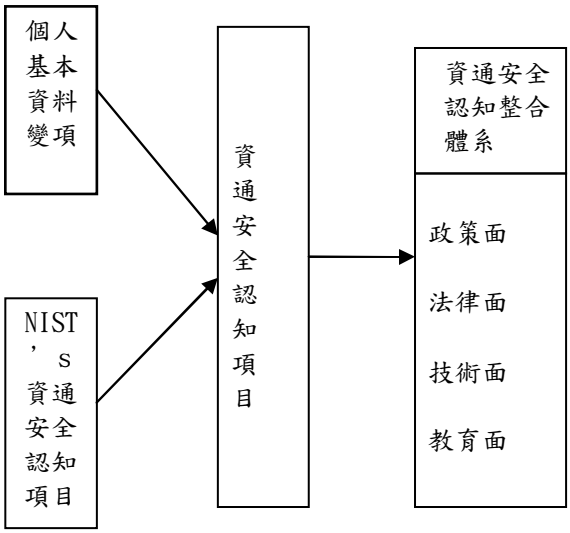

圖 1 研究架構圖

3.2 施測對象

本研究是針對台北縣政府警察局內人員為主，進行量化之研究，其研究範圍與對象分述如下：

一、研究範圍：

針對台北縣政府警察局各單位現職同仁進行資通安全認知之情形進行，以探索對目前資通安全認知項目的瞭解程度，及與人別資料等相關因素間之關係。

二、研究對象：

以台北縣政府警察局警察同仁為對象，包含各分局、各年齡、各種職位以及內、外勤同仁，以隨機抽取之人員作為問卷調查之對象，本次調查共發出 600 份問卷，共回收 513 份問卷（回收率為 85.5%），有效份數共 470 份（78.3%），以 SPSS For Windows 10.0 版進行資料處理與分析。

3.3 信度分析

信度分析用以研究測量量尺的性質，以及組成他們的項目。信度分析程序會計算一些常用的量尺法信度量數，同時也會提供有關量尺中個別項目之間關係的資訊。本研究在信度的測量上採用 Cronbach’s alpha 係數來測量，各表內項目之間平均相關的內部一致性模式。

所有量表共 30 題，所有量表採用 Likert 五點尺度作答，計分方式依之瞭解程度，從「非常不清楚」、「不清楚」、「普通」、「清楚」及「非常清楚」，依次給予 1~5 分，經分析其內部一致性係數在 0.9658，超過努拿利（Nunnally）所以認為研究信度的 alpha 值只需在 0.7 以上即可接受。

4. 分析與討論

4.1 排序分析

以問卷內容中各組間填答之平均數，排序比較出資通安全認知項目中那些項目大多數人員所瞭解的與有待加強的項目。而根據此方法可以得到以下結論：在「知道隨意詢問或查閱同事的私密資料是不道德的」、「清楚在工作時的行為應有的責任」及「瞭解自己在工作職掌中自己的角色及被授權的權責」三項居前三名，顯示大多數人都能知道詢問他人資料是不道德，在工作中能瞭解自己的責任、角色及權責。但相對「清楚目前國內各項與電腦資訊相關的法令內容」、「當資通安全事件發生時，清楚知道應採取適當回應對策」及「是否曾受過資通安全使用、維護、發展的資通安全訓練」居於最後三名，顯見資通安全仍有待加強。另外在資訊人員與非資訊人員其平均數統計分析亦可以發現資訊人員對於資通安全認知，如我們所期望的比非資訊人員在所有的項目中都有較好的認知狀況，亦符合我們原先所期望的，如圖 **2** 所示。

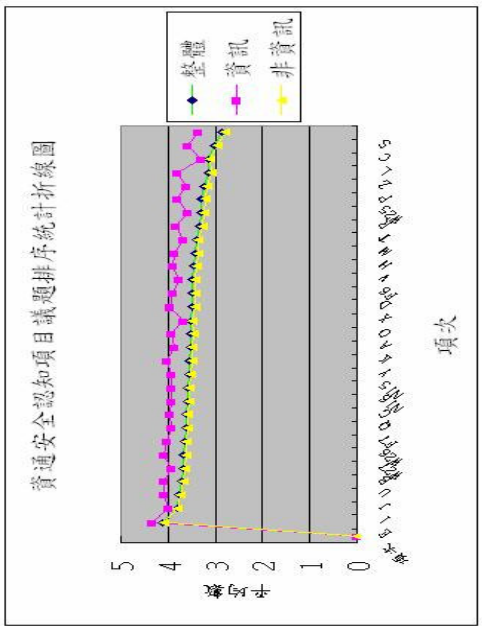

圖 2 資通安全認知項目議題排序統計折線圖

4.2 警察資通安全認知政策面分析

經統計測試發現在台北縣服務年資與年資比較後無太大差異，另教育程度與職務亦有相同的效果，因此在本研究中將服務台北縣的年資與教育程

度由各項統計中刪除。

4.2.1 政策面之標準差、平均數及年齡之分析

分析顯示年齡在 20-30 歲與 31-40 歲之間的比較可以發現有三個項目(I、J、Q)在 20-30 歲比較低，再與 40 歲以上相比較發現除了一個項目(J)外，年紀輕者平均較低，其餘各項皆較年長者平均數來的高。20-30 歲的平均數在五個項目中(C、D、G、O、P)，都可以看出年紀輕者皆比年齡稍長者平均數高，且越年輕者越瞭解資通安全之政策面。

4.2.2 政策面之年資、職務及服務單位之分析

分析顯示年資在 10 年以下者有四個項目(I、J、O、Q)所得的平均數較年資在 10 年以上者為低，其餘項目(C、D、G、P)則為 10 年以下者平均數較高。在職務方面一線以下的員警八個項目(C、D、G、I、J、O、P、Q)均較職務在兩線以上之警官平均數為低。在服務單位部份服務於警察局及分局人員八個項目(C、D、G、I、J、O、P、Q)均較服務於分駐（派出）所平均數高。

4.2.3 政策面之工作性質、接觸電腦頻率之分析

分析顯示工作性質為資訊人員在八個項目(C、D、G、I、J、O、P、Q)平均數均比非資訊人員來的高，接觸電腦頻率方面則為經常使用者的八個項目(C、D、G、I、J、O、P、Q)平均數較高。

4.3 警察資通安全認知法律面分析

4.3.1 法律面之標準差、平均數及年齡之分析

分析顯示年齡在 20-30 歲、31-40 歲與 40 歲以上者，年紀輕者皆比年齡稍長者平均數高，明顯看出越年輕者對於法律面的四個項目(L、W25、W26、W27)越清楚，且是越年輕者越瞭解資通安全之法律面。

4.3.2 法律面之年資、職務及服務單位之分析

分析顯示年資在 10 年以下在兩個項目(W26、W27)所得的平均數較年資在 10 年以上者為低，其餘項目(L、W25)則為 10 年以下者平均數較高。在職務方面一線以下的員警四個項目(L、W25、W26、W27)均較職務在兩線以上之警官平均數為低。在服務單位部份服務於警察局及分局人員四個項目(L、W25、W26、W27)均較服務於分駐（派出）所平均數高。

4.3.3 法律面之工作性質、接觸電腦頻率之分析

分析顯示工作性質為資訊人員在四個項目(L、W25、W26、W27)平均數均比非資訊人員來的高，接觸電腦頻率方面則為經常使用者的四個項目(L、W25、W26、W27)平均數較高。

4.4 警察資通安全認知技術面分析

4.4.1 技術面之標準差、平均數及年齡之分析

分析顯示年齡在 20-30 歲與 31-40 歲之間的比較可以發現除一個項目(B)在 20-30 歲比較低，再與 40 歲以上相比較有十一個項目(A、F6、F7、H、K、R、T、U、V、X、Z)皆較年長者平均數來的高。越年輕者越瞭解資通安全之技術面。

4.4.2 技術面之年資、職務及服務單位之分析

分析顯示年資在 10 年以下者僅在一個項目(X)所得的平均數較年資在 10 年以上者為低，其餘十一個項目(A、B、F6、F7、H、K、R、T、U、V、Z)則為 10 年以下者平均數較高。在職務方面一線以下的員警十二個項目(A、B、F6、F7、H、K、R、T、U、V、X、Z)均較職務在兩線以上之警官平均數為低。在服務單位部份服務於警察局及分局人員十二個項目(A、B、F6、F7、H、K、R、T、U、V、X、Z)均較服務於分駐（派出）所平均數高。

4.4.3 技術面之工作性質、接觸電腦頻率之分析

分析顯示工作性質為資訊人員在十二個項目(A、B、F6、F7、H、K、R、T、U、V、X、Z)平均數均比非資訊人員來的高，接觸電腦頻率方面則為經常使用者的十二個項目(A、B、F6、F7、H、K、R、T、U、V、X、Z)平均數較高。

4.5 警察資通安全認知教育面分析

4.5.1 教育面之標準差、平均數及年齡之分析

分析顯示年齡在 20-30 歲間除了一個項目(E)比其他年齡層低之外，其他的項目(M、N15、N16、S、Y)均比其他年齡層高，所以越年輕者還是越瞭解資通安全之教育面。

4.5.2 教育面之年資、職務及服務單位之分析

分析顯示年資在 10 年以下者在六個項目(E、M、N15、N16、S、Y)所得的平均數較年資在 10 年以上者平均數較高。在職務方面一線以下的員警均比兩線以上之警官平均數為低。在服務單位部份

服務於警察局及分局人員六個項目(E、M、N15、N16、S、Y)均較服務於分駐（派出）所平均數高。

4.5.3 教育面之工作性質、接觸電腦頻率之分析

分析顯示工作性質為資訊人員在六個項目(E、M、N15、N16、S、Y)平均數均比非資訊人員高，接觸電腦頻率方面則為經常使用者平均數較高。

5. 結論

本研究認為警政署居於全國警察機關各項資訊發展之首，有關資通安全認知教育的整合體系亦應由警政署來進行整合與推動，對教材進行整理以節省人力或資訊來源不完整、不正確、無法一致等問題發生；建議可以從下列幾個方向進行。

政策面：

一、確立警察機關資通安全目標：是所有工作的基礎，確定警察機關應該要做到什麼等級的安全，確定目標後成為所有資通安全認知工作的最高指導原則。

二、設定警察機關資通安全政策與程序：根據目標來建立安全的政策與程序，有了依循的準則，則所有的資通安全作為都有標準可遵循。

三、確定警察機關資通安全工作職責/行為責任：建立資通安全工作職責及個人行為責任，畫分工作的權限，防止機密資料外洩。

四、成立警察機關資通安全監控與品質保證單位：有了監控機制即是為了對整個警察機關進行品質保證事宜，提高資通安全認知建立時的成效。

法律面：

一、資通安全相關法律蒐集與案例編撰：由於與資訊相關的法律，隨著資訊與通訊科技的發展不斷更新，而相關法律亦必需更新以符合社會現況，但往往法律修改後未必是員警所知道，因此適時的提供更新法律資訊，方能協助員警保護自己及工作上的方便性。

二、資通安全相關法律推廣：不只是硬梆梆的法律條文，提供多元的管道，如宣導短片、故事書、漫畫等方式皆可，以不同的面貌形式表現出來。

技術面：

一、資訊與通訊技術管理：除瞭解現行系統的狀況及防止其發生資通安全事件之外，隨著資訊與通訊科技的發展更新技術，對引進新技術的評估及未來資通安全事件的防護準備，甚至對於資通訊發展流行的趨勢亦要有所認識，以有效的掌握資訊與通訊的發展。

二、權限控管：對每一項作業建立相關的控制程序，以有效的管控使用者，防止弊端發生。

三、意外處理與監控機制：防止意外事件的發生，並建立起意外發生時的處理步驟，使意外發生的損害降至最低。

四、風險管理：除瞭解自己內部有那些可能產生威脅的地方，亦需由外部人員進行資通安全的評核，以減少資訊人員誤以為已架設了安全的資通環境，即不再加強更新現有資通環境，另由外部人員檢測亦能發現平日疏忽未注意到的細節部份。

教育面：

一、建立資通安全教育資料彙整單位：資料的來源除來自於自行搜集之外，亦需由前三個構面人員隨時提供最新的資訊，建立起資料庫，亦可提供外勤人員參考使用。

二、資通安全教育訓練中心：彙整來自其他構面的資料，整理分類資通安全教育訓練的資料，提出訓練的方式及計畫，不限於固定的場所，最好能做到生活化及多樣，才不致於造成員警的負擔。

三、資通安全教育回饋機制：提出驗證訓練成果的單位，並做為未來改進的資通安全認知教育訓練方式建議。

參考文獻

[1] Chelsa Russell, “Security Awareness – Implementing an Effective Strategy”, GSEC Practical Version 1.4b – Option 1, October 25, 2002.

[2] Courtney Gilbert, “Developing an Integrated Security Training, Awareness, and Education Program”, GSEC Practical Assignment version 1.4b Option 1, June 2003.

[3] Eric Maiwald, “Network Security A Beginner’s Guide”, Second Edition. 陳峰棋譯。2004。資訊安全。學貫行銷股份有限公司。

[4] Lloyd Guyot, “Essential Information Security For Corporate Employees”, SANS GIAC GSEC Practical Version 1.4b Option 1, June, 2003.

[5] Mark Wilson, Dorothea E. de Zafra, Sadie I. Pitcher, John D. Tressler, John B. Ippolito, “Information Technology Security Training Requirements: A Role- and Performance-Based Model”, NIST(National Institute of Standards and Technology), April 1998.

[6] Mark Wilson and Joan Hash, “Building an Information Technology Security Awareness and Training Program”, NIST(National Institute of Standards and Technology), October 2003.

[7] Robert Held, “Security Awareness – are your users “clued in” or “clueless”?”, May 23, 2001.

[8] 經濟部標準檢驗局。資訊技術－資訊安全管理之作業要點。CNS17799。

[9] 劉永禮。2002。以 BS7799 資訊安全管理規範建構組織資訊安全風險管理模式之研究。元智大學工業工程及管理研究所碩士論文。

[10] 賴淑賢。2003。警政資訊安全風險評估與管理－以車輛車牌失竊處理系統為例。中央警察大學資訊管理研究所碩士論文。