資訊安全認知評量之研究

歐芳伶
樹德科技大學資管所
blacknewopel@gmail.com

蕭銘雄
樹德科技大學資管所教授
msshiaw@mail.stu.edu.tw

摘要

網路、通訊應用的快速發展重新改變人們的生活形態，資訊科技儼然已成為現在人工作或生活息息相關的基本配備。行政院主計處於2006年電腦應用概況報告所做的調查，顯示多數組織在安全技術上著力較深，卻忽略了仍需使用者安全意識與習慣的提升，方可達成全面安全管理之功效。本研究欲發展評量資訊安全認知量表，藉以得知組織人員對資訊安全的瞭解程度。本研究採用文獻探討、內容分析法，依據過去的文獻，得知資訊安全認知定義及其構面，再發展可作為測量資訊安全認知量表。其量表可作為衡量人員的資訊安全認知水平，提供未來資訊安全訓練導入參考的依據，並可驗證在受過資訊安全訓練後，認知成效高低之評量。

關鍵詞：資訊安全、資訊安全認知、資訊安全認知評量表

Abstract

The rapid developments of Internet and communication technology application have reconstructed the nature of human life; information technology is the basic infrastructure for modern work and life. In 2006, the Directorate-General of Budget, Accounting and Statistics of the Executive Yuan in Taiwan conducted a computer usage survey. The result has shown that most of the organizations emphasize more on security technology, but ignore the safety awareness and behaviors of users, which are important elements to achieve a thorough safety and secure management. This research intents to develop a information security awareness scale, by which we can measure on what level the organization members understand the information security. Literature review and content analysis method were conducted in this study. Based on literature reviewed, the definition of information security awareness, information literacy, and information security literacy was clearly defined. Such scale could be used to measure the information security awareness level of users, verifying the performance of information security training program.

Keyword: Information security、Information security Awareness、Information security Awareness Scale

1. 前言

1.1 研究背景

在Internet、無線網路、藍芽、3G/4G、WiMax等網路、通訊技術快速發展，加上網路基礎設施大量佈建以及桌上型、筆記型電腦、行動電話、PDA、數位家電等各類資訊、多媒體載具的大量面市與普及，帶動數位內容、行動內容、行動商務等新興服務快速發展。而隨著社會型態、人口結構的改變，無線網路技術逐漸融入日常生活與相關產品，未來透過網路進行的遠距醫療、健康資訊監測、安全監控等服務也將應醞而生。網路、通訊應用的快速發展改變人們接觸資訊的方式，也重新塑造人們的生活形態(資策會, 2007)，資訊科技儼然已成為現在人工作或生活息息相關的基本配備。

我國個人電腦設置數已突破1000萬台，家庭部門的電腦普及率為66.09%，其中網際網路連線比率超過9成(行政院主計處, 2006)。也由於個人電腦已成為家庭溝通及娛樂的中樞，家庭PC使用者也成為愈來愈顯著的攻擊目標。沒有任何電腦、作業系統或軟體能做到完全讓各種類型的攻擊無隙可趁，因而使用者往往無法察覺自己已經曝露於危險之中(CA, 2007)。

行政院主計處於2006年電腦應用概況報告，內容針對國內32,626個民營企業、政府行政機關、公營事業機構、學校及研究機構所做的調查，有94.62%建有資通安全防護措施，較2005年增加5.4%，顯示資安意識普受大家重視。但在近九成五的單位裝有資通安全防護措施下，仍高達51.85%單位遭遇過資訊安全事件，比2005年略升11.3%，顯示資安事件除了防護設施的加強外，尚需配合使用者安全意識

與習慣的提升(行政院主計處, 2006)。

美國電腦安全學會(Computer Security Institute)針對美國大型企業、政府機關與學校資訊部門所進行的電腦犯罪與安全調查報告(Computer Crime and Security Survey)，2007 年間遭受資安攻擊所損失金額達 66,930,950 美元，個人用戶遭受電腦犯罪的比例也比以往增加。美國 CA 軟體公司於 2007 年報告也顯示，家庭、個人電腦使用者正面臨加倍複雜的全新網際網路威脅，個人用戶遭受電腦犯罪比例也比以往增加(CA, 2007)。

然而資訊安全所面臨的問題，為自然所影響的僅佔 15%，而人為的影響卻高達 85%(李東峰, 2001)。在此比例當中，人為因素影響資訊安全發生相關之大，但要如何有效管理這方面的缺失，是值得探討的重點。[9]

1.2 研究動機

隨著全球網路科技之發展，資訊安全工作不僅涉及企業及個人之安危，更影響了國家乃至於全球之政治與經濟運作，資訊安全必須是政府和每個企業及國民共同攜手面對的問題。政府於 2004 年 3 月行政院國家資通安全會報裡，制定了「建立我國通資訊基礎建設安全機制計畫」中，其一主要工作要項「強化國家資通安全認知與訓練推廣」，希望藉由多個單位的主導，來加強全民對於資訊安全認知概念、資訊安全教育訓練和資通安全認證的推動。

由於愈漸增加的資訊安全需求，許多組織已經建立了關於增進資訊安全的專案課程，以確立組織的員工對於資安風險是提高警覺的，進而能保護自己的獲利性(Kruger and Kearney, 2006)。也有越來越多的組織與企業開始導入資訊安全的相關的制度,不論是 BS7799 或 COBIT 等資訊安全標準，都是由組織層面去檢驗資訊安全的機密性、完整性與可用性（曹明玉, 2006）。[25] [12]

在 NIST-SP-800-50 的文獻談到，企業內部中，人就是一個資訊安全弱點與威脅的連結(Wilson and Hash, 2003)，而 BSI 大中國區訓練經理蒲樹盛先生從從各種資安事件中發現，多數組織在安全技術上著力較深，較缺乏全面安全管理概念，尤其是人員的觀念及習慣。由全球推動 ISMS 資訊安全的過程經驗中，歸納出數項成功關鍵因素，其中最基礎且最重要的便是人員的資安觀念及管理知識(http://asia.bsi-global.com/Taiwan/, visited on 2007/10/15)。[28]

近幾年的研究將資訊安全之議題探討向下延伸至使用者的趨勢，以期由最末端的使用者做起，提昇使用者對資訊安全的應變能力。以探討組織資訊安全認知文獻，有曹明玉(2006)探討組織人員本身是否了解資訊安全認知概念的基本意義與內涵的研究。吳倩萍(2006)探討政府機關各層級人員在資訊安全應具備之基礎認知與其行為之關係。余崇倫(2006)探討組織人員對資訊安全方面的認知。劉志銘(2005)發展一套適合使用在資訊安全上的認知模式。在犯罪偵查方面，有楊境恩(2004)研究國內警察人員資訊安全素養對資訊犯罪偵查能力影響。邱士娟(2005)研究員警資通安全的認知訓練及現況。[12] [6] [5] [16] [13] [10]

就整體而言，學術界之關注及研究焦點，仍較少以組織人員資訊安全認知為主的資訊安全相關研究，因此本研究將從最基本以組織人員為出發點，進一步探討資訊安全認知程度，以期望由最根本做起，全面提昇資訊安全認知。

1.3 研究目的

本研究認為，除了技術層面增加軟、硬體設備外，更需要加強使用者資訊安全的基本認知，強化其判斷和反應能力，期盼能正確處理大部分的資訊安全問題。針對這個研究方向，本研究之研究目的為設計資訊安全認知量表。驥希能了解組織人員資訊安全之問題。

2. 文獻探討與基礎理論

2.1 資訊安全定義

依據資訊安全管理系統國際標準 ISO17799 對資訊下的定義為:資訊(Information)意指以各種型態儲存的資料與知識，包括電子方式、文件方式等，如同企業其他重要資產一樣，需要被妥善地保護。(台灣 BSI http://asia.bsi-global.com/Taiwan)

Smith(1989)主張，任何電腦安全政策之廣義目標，必須能保護儲存於系統中資料之機密性(Confidentiality)、完整性(Integrity)與可用性(Availability)。其為資訊安全的基本要素。[27]

a. 機密性：確保資訊只能被經過授權的人才能存取。
b. 完整性：保證資訊和其處理過程的準確性與完整性。
c. 可用性：確保經過授權的使用者，在需要用的時候都可以使用及存取資訊。

所有涉及到「安全」的問題，Gollmann(1999)主張處理下列事項來確保資訊系統軟硬體資料、資訊的機密性、完整性與可用性：[22]

a. 預防(Prevention)：在防止資產發生危險。
b. 發現(Detection)：當安全問題發生時，要有方法可以在最短時間內發現，並知道確切的危險及其嚴重程度。
c. 反應(Reaction)：要在最短時間內使傷害降至最低，損害減至最少，並恢復到正常的情況。

資訊安全的問題是多層面且多元的，可歸納為安全(Security)= 資訊(Information)+ 科技(Technology)+人(People) (Hinde, 2001)。而「資訊系統安全」乃指一切保護資訊系統的資源，包括：硬體、軟體、資料庫，以防止遭受變更、破壞及未授權使用資訊系統資源之控制措施，涵蓋到技術面與組織管理面(吳琮璠, 1996)，應考量的範圍包含電腦軟、硬體、網路、環境的安全技術方面及人員的教育訓練與操作安全觀念等二大類「技術」與「人」的因素(Schneider and Therkalsen, 1990)。[33] [7] [23]

保護資料的安全並不是一件簡單的事，它需要各層次的相關管理來配合(Malisow, 2004)。因此，欲使資訊安全無慮，防護工作並非僅是單純地依賴軟、硬體輔助得以完成，而是需要多方面教育與習慣養成。[18]

2.2 相關資訊安全制度

(1). BS7799

BSI(The British Standards Institution)為英國標準協會創立於 1901 年，為一國際知名標準制定及稽核驗證機構(如 BS 7799、ISO 9000、ISO 14001、OHSAS 18001....)。 BSI 除為 BS 7799 國際標準之制定機構外，亦為國際 UKAS 與國內 TAF 認可之 BS 7799 驗證機構，目前國際上委請 BSI 公司進行 BS 7799 驗證之比例亦高居全球第一。在 ISMS 領域中，BSI 被公認為最公正專業嚴謹之驗證及訓練機構。(台灣 BSI http://asia.bsi-global.com/)

BS7799 資訊安全標準，邀集業界相關領導廠商，為共同追求國際性品質的資訊安全管理系統所共同開發而成，適用於各種產業與組織，是一個包含了各面向的企業資訊安全管理標準。BS7799 係由 BSi、DNV 等認證機構來做審核認證的動作，包括澳大利亞、紐西蘭、荷蘭、挪威及瑞典等國都相繼採用 BS7799 作為資訊安全管理系統的國家標準。BS7799 並於 2000 年 11 月於國際標準組織（ISO）審核通過，成為全球通用與遵循之資訊安全管理系統規範，並於 2000 年 12 月 1 日正式頒佈為 ISO/IEC17799。(蔡興樺, 2001)

以 BS7799 資訊安全管理系統(Information Security Management System, 簡稱 ISMS)標準定義而言: 就是"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。"(台灣 BSI http://asia.bsi-global.com/Taiwan)

BSI 於 1995 年 2 月提出 BS7799 Part I，全名為「Code of practice for information security management」（資訊安全管理之作業要點）；隨後，BSI 於 1998 年公佈 BS7799 Part II，即「 Specification for information security management systems」(資訊安全管理系統規範)，以下分別介紹：

a. Part I ： BS ISO/IEC 17799:2000 BS 7799-1:2000 Information Technology – Code of practice for information security management (資訊安全管理之作業要點)，包括領先企業提出的的相關指導和建議。
b. Part II ： BS 7799-2:2002 Information Technology - Specification for information security management systems (資訊安全管理系統規範)，提供了關於組織資訊 安全管理系統建立、實施和維護的要求。這是正在考慮驗證此標準的組織的必要文件。

BS7799 內容包含 10 大控制類別、36 個控制目標與 127 種控制措施，其結構為：資訊安全範圍、風險審查與風險管理、資訊安全政策、資訊安全管理架構、資訊安全管理系統維護與審查。

中華龍網指出「BS7799-國際資訊安全稽核規範」為 BS7799 包含了所有企業安全政策，從安全政策的擬定、安全責任的歸屬、風險的評估、到定義與強化安全參數及存取控制、防毒策略。根據 BS7799 標準的風險評估包括了兩項系統化的考量(中華龍網股份有限公司網站, visited on 2007/10/9)：

a. IT 安全的破壞造成可能的資訊保密性、真確性與可用性失效之後果，將會導致對企業的傷害。
b. 對各種威脅的防範與合理的控管都會影響這些破壞發生的實際可能性。

BS7799 是一套相當複雜的資訊安全應用與稽核的標準，但不外乎就是控管的觀念。定義一套完整的政策、程序、實施與組織化的架

構，用來提供合理的保障使企業目標得以達成，並避免、偵測或修正無法預期事件所造成的後果。BS7799 的 10 個章節中內容介紹如下(中華龍網股份有限公司網站, visited on 2007/10/9)：

a. 「安全政策」
目標在於提供管理的方向來保障資訊安全。

b. 「安全組織」的目標
1.企業內資訊安全的管理。
2.維持處理組織安全的相關設施與資訊資產由一個可靠的第三單位所控管。
3.維持當資訊處理程序外包（outsourced）給其他組織時的安全。

c. 加上防止侵入程式
妥善配置防禦軟件，可敏捷地確認攻擊模式，然後在警號響起之時，立即抵禦黑客。

d. 「資產分類與控制」
為了維持對企業資產適當的保護及確保資訊資產可得到一個相當程度的保障。

e. 「人員安全」
為了要降低人為錯誤、竊取、欺騙、及濫用相關設施的風險，來確保使用者意識到資訊安全的威脅；為了確保在正常工作程序中資訊的安全與降低安全意外事件的損害並從其中習得相關經驗。

f. 「實體與環境安全」
主要是為了避免未授權之存取、破壞與影響企業的建築或資訊；避免損失、或對資產的破壞與阻礙企業活動的進行；避免對資訊及其處理設施的破壞或竊取。

g. 「電腦與網路管理」要達成
1.確保正確與安全資訊處理設備之運作。
2.把系統的失誤降到最低。
3.保護軟體和資訊的真確性。
4.維持資訊處理與通訊的正確性與可用性。
5.確保資訊在網路上的保全與保護支援的基礎建設。
6.避免對資產的損害與中斷企業活動。
7.避免資訊在組織間傳遞時的中斷、竄改與誤用。

h. 「系統存取控制」要達成
1.資訊存取控制。
2.避免資訊系統未授權之存取。
3.網路服務的保護。
4.避免電腦未授權之存取。
5.偵測未授權之活動。
6.確保行動運算與電信網路設施的安全。

i. 「系統開發與維護」要做到
1.確保安全被內建在運作的系統中。
2.避免使用者資料在應用系統中被中斷、竄改與誤用。
3.保護資訊的授權、機密性與真確性。
4.確保所有的 IT 專案與相關支援活動都在安全的考量下進行。
5.維護應用系統軟體與資料的安全。

j. 「企業持續運作規劃」
要降低對企業活動的阻礙與防止關鍵企業活動受到嚴重故障或災害的影響。

k. 「遵行」
1.避免違反民、刑事法律、規範、或任何安全要求契約上的義務。
2.確保系統運作遵循組織的安全政策與標準。
3.把系統稽核過程之效能極大化與影響最小化。

(2). COBIT

COBIT(Control Objectives for Information and Related Technology，資訊及相關技術之管理與控制)是國際電腦稽核協會（ISACA）於 1995 年所擬定的作業規範，是一套資訊系統稽核與控制標準，源自於 ISACF 之控管目標，加入現有及合併的國際技術、專業、政府機構與標準制訂單位等。

COBIT 將資訊技術控管與營運目標緊密聯結，提供了一個涵蓋階段及作業程序的實際架構，及對細部工作的可行性和邏輯性的結構。所謂「最佳運作模式」之專業表現，可讓資訊投資最佳化及提供何處可能出錯之判斷標準。其主題為企業導向，不僅只設計為使用者及稽核所用，更是一份可供管理階層及業務營運主管使用的詳盡準則。COBIT 之資訊技術控管架構分為四個階段：規劃與組織、取得與建置、交付與支援、監控，以「階段」的區分符合企業結構及管理或資訊作業之生命週期模式(COBIT, 1998)。最高層次資訊技術控管各階段定義如下：[20]

a. 規劃與組織:
涵蓋為達成營運目標，應有之資訊技術策略規劃；為實現策略性遠景，應有之計畫、溝通及管理；除適當之資訊技術建構外，應有適當之組織配合。

b. 取得與建置:
涵蓋為實現資訊技術策略規劃，應確認、

開發或購置資訊技術解決方案，其施行並應與營運活動整合；變更及維護現有系統。

c. 交付與支援:
與實際提供所需之服務有關，涵蓋作業安全、持續訓練；確保服務之提供，建立必要之支援作業；以及應用系統處理之控制。

d. 監控:
經常評估所有資訊技術作業以確保品質及控管制度之落實。此階段提供了管理階層對組織控管程序的整體觀，及內部及外部稽核的另一審計軌跡。

依其作業程序可再細分為 34 項高層控管目標。此架構涵蓋了所有的必須資訊和技術。藉由此 34 項高層控管目標，業務營運主管可確保採用適當的資訊技術環境控管機制。對映於此 34 項高層控管目標，另有 318 項細部控管目標的資訊技術程序稽核準則，可供管理階層及稽核人員參考(ISACA, 2003)。

2.3 資訊安全認知

2.3.1 認知定義

Wangler(1992)認為，「認知」是個體以其感官系統，對外來刺激的一種解釋與反應，而且認知是相當主觀的，個體會依其經驗與社會化之過程，對目標、情況、人或群體會產生不同的認知與反應；依 Wangler 所見，「認知」會造成個體在組織中對前情境的觀點不一致，進而影響個體行為、績效，造成共識或團隊合作的阻礙。由 Wangler 的論點可知，經由探索當事人對某項事物「認知」的看法，即可預測其心理層面潛在的企圖或是行為的方向(李長貴, 1998)。[8]

認知是在處理問題時，由認識問題到了解事件的本質，繼而尋求已知之解決方案，這一連串的思考活動，就是認知的活動，是個體對其週遭情境環境所感受到對人、事、物、情況的瞭解(吳倩萍, 2006)。[6]

NIST Special Publication 800-16 從資訊安全之角度解釋認知，認為認知不等同教育訓練，認知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(NIST, http://www.nist.gov/)。

資訊安全認知是給予人員明白了解 IT 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，必須針對組織內所有使用者。因為安全失效會對每個人有潛在不利的後果，可讓人員體認出資訊安全的關鍵性(曹明玉, 2006)。[11]

2.3.2 NIST Special Publication 800-16

NIST (National Institute of Standard and Technology)美國國家標準技術學會隸屬美國商業部中的技術行政部門，為美國民營企業中受國家認可的一個發展資訊安全文獻與技術的組織。美國國家標準技術學會的先進技術計劃，是透過私人研究及開發夥伴來加速創新技術的發展，以增進全國利益(NIST, http://www.nist.gov/)。

NIST 的資訊技術實驗室(Information Technology Laboratory, ITL)其中的一個分部 CSD (Computer Security Resource Center)電腦安全中心，使命是改善資訊系統安全，其訂定的 NIST Special Publication 800-16「Information Technology Security Training Requirements: A Role- and Performance-Based Model」資訊科技安全的訓練要件，將資訊安全學習歷程(IT Security Learning Continuum)分為三個階段：認知 (awareness) 、訓練 (training) 與教育 (education)。如圖 2-1 所示。

根據圖 2-1 介紹的資訊安全學習歷程，「認知」階段讓所有的員工都必須具備有關於資訊安全知識。它的目的在於呈現資訊安全上簡單的重點，呈現未來允許個人去識別資訊科技之利害關係與相對應的反應。

「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」是經由任何方式與資訊系統有關的員工都需要了解，包括承包商等。在現今的環境中，代表著所有在組織內的員工，都需對重要的資訊安全詞彙與概念有全面性了解，並作為日後訓練的基礎；「訓練」則依照個人在公司特定的角色與責任，來建立員工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，使人員可應付資訊科技未來的威脅與改變，產生有專門知識的資訊安全專家。NIST 也針對認此三階段之教授程度的不同加以比較，闡述如表 2-1 所示，資訊安全認知是重要的。

依據 Ernst & Young 公司的 2004 年全球資訊安全調查(Global Information Security Survey 2004) 針對 51 個國家中 1,233 個組織的調查發現，使用者缺乏安全認知是資訊安全最大的阻礙(Ernst & Young, 2004)。

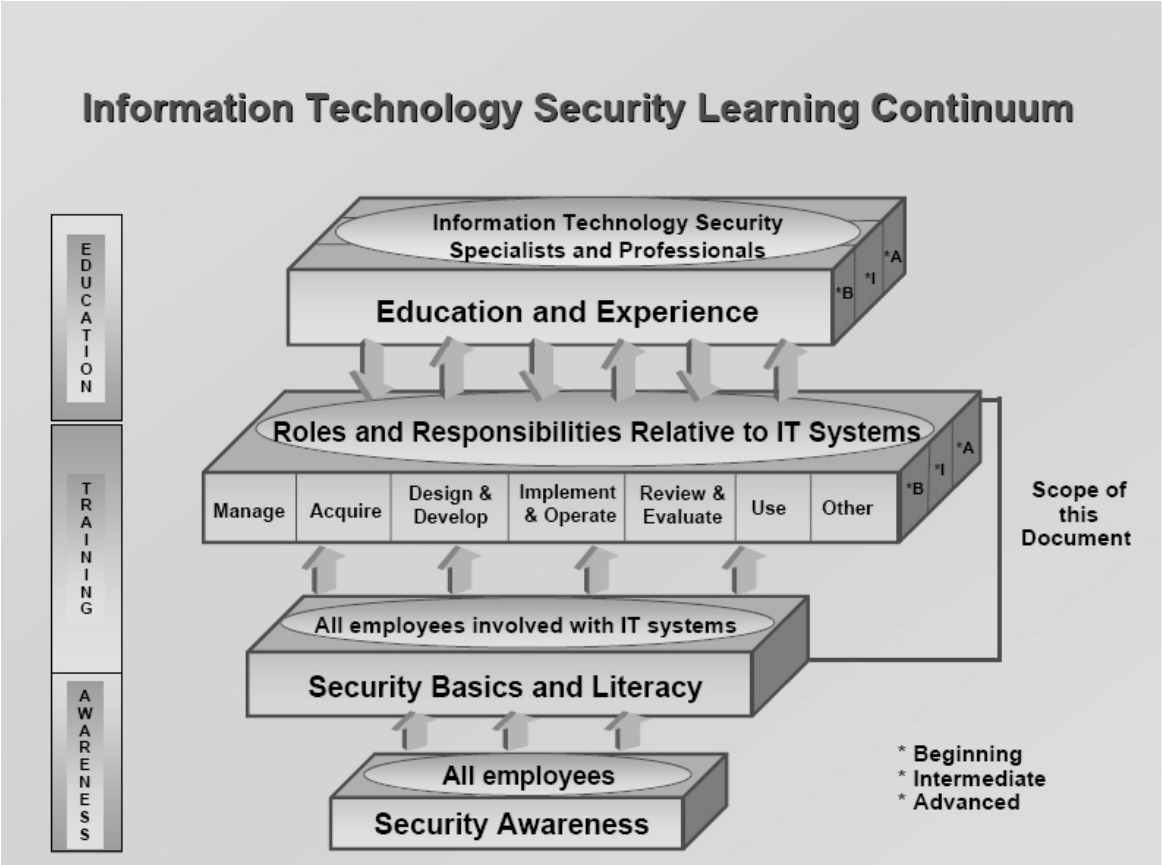

圖 2-1 資訊科技安全的訓練要件
資料來源：NIST Special Publication 800-16

表 2-1 認知、訓練、教育三階段的比較

比較項目	認知(Awareness)	訓練(Training)	教育(Education)
屬性	What	How	Why
層度	Information	Knowledge	Insight
學習目標	Recognition and Retention	Skill	Understanding
教導方法範例	Media - Videos - Newsletters - Posters	Practical Instruction - Lecture/demo - Case Study - Hands-on practice	Practical Instruction - Seminar/discussion - Reading and study - Research
測試方式	True/False Multiple Choice (Identify Learning)	Problem Solving (Apply Learning)	Essay (Interpret Learning)
影響時間範圍	短期	中等	長期

資料來源：NIST Special Publication 800-16

3. 研究方法

3.1 研究架構

在產生研究動機與目的後，即開始蒐集整理資訊安全與資訊安全認知領域的文獻與研究，深入了解目前國內業界導入資訊安全實務對一般組織人員資訊安全認知的應用情形。目前的學術文獻少有這方面的研究，因此，在了

解現有資料與業界情況後，訂定研究主題，以衡量受訪者是否有資訊安全各項概念之基本意義與內涵的認知為主，進行量表內容設計。

本研究根據 Drevin and Kruger and Steyn(2007)資訊通信技術的安全認知六項問題討論與訪談結果深入研究，產生研究架構，如圖 3-1 所示。[26]

該訪談皆遵守 Keeney(1994)所建議之目標定義技術。與受訪者所討論之議題包含以下項目：[32]

a. 其對於資訊和通信技術安全認知議題來說，你認為什麼是重要的?
b. 為了要增進或實現資訊和通信技術安全認知水準，你會怎麼作?
c. 對於目前的資訊和通信技術安全認知水準，你所關心的是什麼?
d. 為了要提升或維持資訊和通信技術安全認知水準，有哪些事是可以被執行的?
e. 欲提升資訊和通信技術安全認知水準，目前的限制條件為何?
f. 如果你必須評估資訊和通信技術安全認知水準，你將會如何進行；另外，你將如何得知可被接受的認知水準為何?

Drevin et al (2007)集中探討資訊和通信技術安全安全認知方面，透過訪談整理價值集中的資訊和通信技術安全認知及關鍵領域。[26]

3.2 資訊安全認知架構解釋

3.2.1 十三個行為目標與六個基礎目標

依據圖 3-1，Drevin et al (2007)訪談結果，圖的左邊是表現關心的目標，透由受訪者訪談結果定義屬於資訊和通信技術安全認知的價值，例如：設備需要上鎖、使用卡片進入是重要的、進入檢測入口後可正常的工作、攜帶筆記型電腦進入應要申報、監視系統應該要被安裝等等，這些受訪者的陳述中，自然安全性被認為是一個問題，經整理後被歸類為「極大化實體存取控制」的行為目標。整理分類後總共為 13 個行為目標，如表 3-1 所示。[26]

圖 3-1 右邊的基礎目標定義方法與行為目標相同，例如：當需要時，資訊應可立即取得、硬體和設備可在工作中正常被使用、資訊應該被定期的備份和儲存在網路上可供即時還原或替代等等，經整理後被歸類為「極大化資訊及硬體設備可用性」之基礎目標。總共歸類為 6 個基礎目標，如表 3-2 所示。

在歸類為基礎目標的過程中，若有同時歸類在兩個類別，則依 Drevin et al (2007)原文中的定義將其歸類在較為適合的類別來作整理。[26]

完成訪談後並整理的資訊和通信技術安全認知基礎目標和已被認同的資訊安全制度 BS7799 目標一致，例如：完整性、機密性和可用性。

3.2.1 六個基礎目標解釋

1. 極大化資訊完整性

完整性可以被定義為保證資訊沒被意外或蓄意改變的需求，且確定資訊是正確和完整的。

a. 硬體：有一些存在大學環境中的潛在威脅可能會造成資料和資訊的損毀或遺失。
b. 人員：使用者意外的錯誤使用。例如：資訊截取錯誤或是刪除檔案或是磁片的數據是會發生的。但是使用者蓄意的行動，可能危急資料的完整性。例如：試驗和檢查標示的改變會損害商業和研究結果，等等。
c. 電腦病毒：潛在的威脅會經由電腦病毒所引起的系統污染。

從集中的評價裡更精鍊出與威脅方面有關係，包括極大化實體存取控制及存取控制邏輯這兩者、安全的對行動設備的使用和負責任的管理電子郵件及網際網路。

2. 極大化資訊機密性

機密性是避免將資訊公開給沒有被授權者使用的一種能力。在大學環境中不公開資料的需求，在於其他盈利組織比較下或許沒有那麼高。不過，對機密的需求仍存在，且對學生和職員個人資料(私人)的保護，和大學所屬資料(秘密)的保護還是重要的。例如：學生系統、金融制度、研究計畫、職員系統和其它。

3. 有效及有效率的使用電子通訊資源

網際網路是連結全世界數百萬台電腦的全球性網路，並且使用戶能夠交換數據、新聞、意見等等的一個全球網路。由許多的網路伺服器形成一個全球資訊網路服務系統，支援特別格式的文件資料，連結其他文件資料、圖形、影像和聲音檔案。一種由網際網路提供的重要服務是資訊傳送或電子郵件的使用。

在大學中使用網際網路和電子郵件是給學術和非學術人員的一種必要資源。電子商務和交易系統是很普遍的，行銷資訊也透過網頁讓未來的學生尋找的到，在全球研究環境中這些設備已是不可或缺的。

電子通訊也在教學中被使用，也被當成是一門學科，且是執行教學活動中的幫助工具。

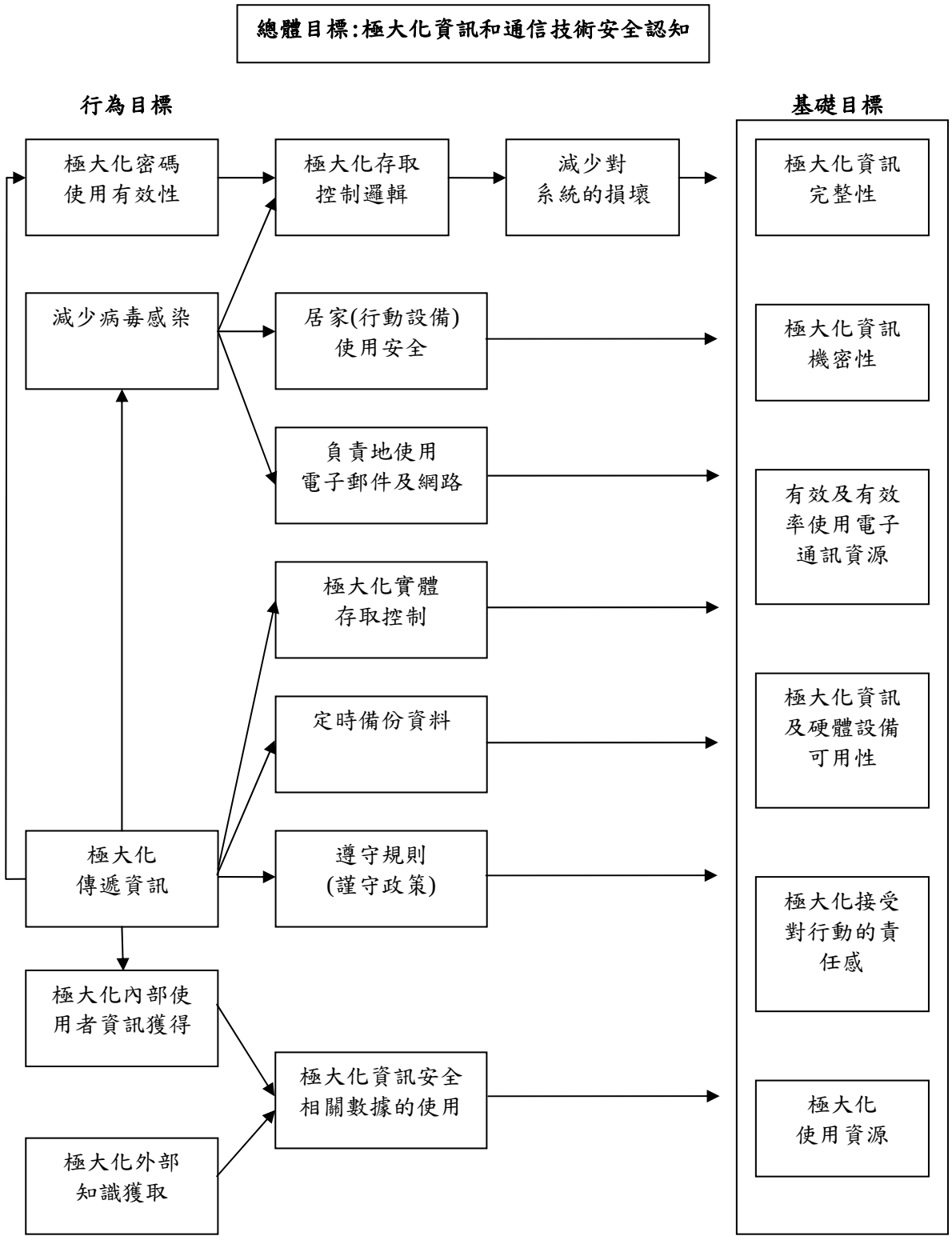

圖 3-1 資訊和通信技術安全認知-方法及目的網絡關係
資料來源: Drevin and Kruger and Steyn(2007)

表 3-1 資訊和通信技術安全認知行為目標

1. 極大化密碼使用的有效性
使用高效密碼並維持密碼保密
當不用電腦時必須登出
減少在網路上使用的密碼組數
2. 極大化存取控制邏輯
使用加密；限制多重登入
正確的系統權限授權
分工、在人員離職後重新置換控制系統程序
3. 減少對系統的損壞
限制存取
4. 減少病毒感染
提防來自居家、行動設備
網路、郵件的病毒
5. 居家行動設備使用安全
遠端存取/數據機；使用密碼
6. 負責地使用電子郵件及網路
使用網路的成本及時間
小心處理陌生郵件及較大的附件
正確的預設值
7. 極大化實體存取控制
減少盜竊；使用安全設備，如監視器
有工作人員離職時，重整登入程序
8. 定時備份資料
減少資料遺失的狀況
設定資料被保存的時間長度條件
正確預設保存資料；重要資料之處理原則
備份設備的可及性
9. 極大化傳遞給員工的資訊量
極大化IT素養
使用溝通管道(張貼文章、佈告欄、溝通聯絡)
辨別重要資訊的原則
何為非法使用軟體的行為
10. 遵守規則(謹守政策)
極大化IT素養；
使用溝通管道(張貼文章、佈告欄、溝通聯絡)
讓風險透明化；使安全之背後意涵明確
11. 極大化內部使用者之資訊獲得
了解使用者回饋資訊
使用內部監督數據
減少知識遺失，如員工離職
12. 極大化外部知識獲取
使用外部資訊報告，如外部監察單位，
Gartner世界最大市場研究及顧問公司
13. 極大化資訊安全相關數據的使用
使用所有可比較的數據

資料來源:Drevin et al (2007)

表 3-2 資訊和通信技術安全認知基礎目標

1. 極大化資訊完整性
資料正確性
遵守正式的資訊和通信技術政策
2. 極大化資訊機密性
確保商業、研究及客戶(學生)的資料機密不外洩
3. 有效及有效率使用電子通訊資源
電子通訊成本最小化
電子通訊資源最大化
最小化電子通訊的負面衝擊
4. 極大化資訊及硬體設備可用性
不間斷的使用;防止資訊損害或漏失
5. 極大化接受對行動的責任感
行為的後果
6. 極大化使用資源
遵守正式的資訊和通信技術政策

資料來源:Drevin et al (2007)

令人遺憾的是網際網路和電子郵件設備把組織和大學暴露在多種危險之中。一些更普遍的危險包括病毒的傳播(最重要的威脅在這個案例研究過程中被指出),使用設備處理民營的商業，擊垮連結的電子郵件，模仿、竊聽等等。可以招致損失的類型例子是對資料的損害、系統和網路、金錢損失、隱私損害，在資訊改變或遺失時的商譽受損。

4. 極大化資訊及硬體設備可用性

可用性的，經常相關的服務等級一致，被用許多不同方式來定義及分類。例如資訊可用性、系統可用性、應用程式可用性、基礎設施可用性等等。為了這項研究的目的，以下的一般型定義會被使用。

可用性是指能夠保証使用者可以在有需要時無時無刻的使用任何資訊。在這個研究裡受訪的大學中，有兩個主要對可用性的影響被定義出來。

備份系統的製作被指為待改進的地方，大多數人員不會定期備份他們的工作。很明顯的，多數人員不知道要備份何種資料，也不知何處和如何去定期的備份。人員被鼓勵將他們的資訊、資料、計畫等等儲存在網路硬碟上，方可自動備份，但很明顯的，這件工作並沒有被確實的做到。適當的實體存取控制的實施將幫助防止資訊的損失及資訊和通信技術資源的損失。

5. 極大化接受對行動的責任感

有多種工作群組和個人對不同有關安全問題的活動有責任。通常，在這個研究中是假定用戶應該對他們的行動負責。

根據簡要的牛津英文字典載明，負責任這

名詞被定義為”把某件事情視為首要，為他負起承諾及承擔罪責；有責任的，讓行為值得依賴，能被信賴”。

它表示如果在大學的使用者不遵守大學的要求和政策，例如：不做定期的備份或在他們的電腦上沒有裝防毒軟體。使用者將對所有的負面結果負責，例如：招致的損失、系統效能降低、客戶信心損失。

在建立一種使用者可以接受他們對自身的行為有責任的文化時，資訊傳輸和安全策略被視為是關鍵因素。

6. 極大化使用資源

資訊技術資源是包含錢，時間和人這三者對支援大學學術性，教育、研究和管理活動的可用性。這些資源是有限的並且應該被以正確的管理使用。

安全犯罪可能對成本有直接影響。(例如：由於資訊、設備或客戶信任的損失。)、時間(例如：處理問題)、和工作人員(例如：做復原工作)。一個區域的資訊傳輸和支持安全政策，再一次在研究過程中被鑑定保証可以讓資源最大化。

3.3 資訊安全認知量表設計

將 Drevin et al (2007)所做的資訊安全認知訪談結果所產生的架構圖中，將 13 個行為目標歸類至 6 個基礎架構中。由 6 個基礎架構中的解釋來分類 13 個行為目標遵循的依據，若有同時歸類在兩個類別，則依 Drevin et al (2007)原文中的定義將其歸類在較為適合的類別來作整理。[24]

再經由表 3-1 行為目標之原文細項及所歸類的基礎架構解釋來產生量表，如表 3-3 所示。

4. 結論

資訊安全除了技術層面增加軟、硬體設備外，更需要加強使用者資訊安全的基本認知，強化其判斷和反應能力。本研究針對此研究方向，採用文獻探討、內容分析法，依據過去的文獻，得知資訊安全認知定義及構面，發展可作為測量資訊安全認知量表。藉由此量表，得知組織人員對資訊安全的瞭解程度。

本研究引用之理論架構與所產出之量表為資訊安全認知之基本意義與內涵，適用於各類型單位，可評量出目前人員資訊安全水準之高低等狀況，藉以分析組織內缺少資訊安全這部份的教育訓練。目前資訊安全認知在國內外少有學術研究及文獻，本研究之量表可作為衡量組織人員的資訊安全認知水平，提供未來資訊教育訓練導入參考的依據；並可驗證在受過資訊安全訓練後，認知成效高低之評量。

受限於研究時間限制，本研究僅以資訊安全認知方面做為測量，未加入組織人員應俱備之技能、資訊安全導入產業之背景及外在因素影響人員資訊安全認知方面。未來研究方向將加入資訊素養能力之構面，探討人員對於資訊安全所應俱備的認知與技能，並進行前測與實測，讓本研究所發展之資訊安全認知量表更完善。

參考文獻

[1]. 中華龍網股份有限公司, BS7799-國際資訊安全稽核規範, http://www.dragonsoft.com/doc/bs7799-intro.php , visited on 2007/10/9。

[2]. 台灣 BSI 官方網站, http://asia.bsi-global.com/Taiwan+InformationSecurity/ShareISMS/index.xalter。

[3]. 行政院主計處, 2006 電腦應用概況 http://www.dgbas.gov.tw/public/Attachment/792617191871.doc。

[4]. 行政院國家資通安全會報, 「建立我國通資訊基礎建設安全機制計畫」, 2004/03。

[5]. 余崇倫, 組織人員對資訊安全認知之研究,中國文化大學資訊管理研究所碩士班, 2006。

[6]. 吳倩萍, 政府機關個人資訊安全認知與行為之探討, 國立台北大學公共行政暨政策學系碩士在職專班, 2006。

[7]. 吳琮璠, 國外政府機構資訊系統安全稽核制度, 存款保險資訊季刊, 1996 年第 10 卷, 第 2 期, PP.21-40。

[8]. 李長貴, 組織行為, 台北, 華泰文化, 1998。

[9]. 李東峰, 企業資訊安全控制制度之研究，第三屆全國資訊管理博士生聯合研討會論文集, 2001, pp.1-22。

[10]. 邱士娟, 員警資通安全的認知訓練及現況, 中央警察大學資訊管理研究所, 2005。

[11]. 國際電腦稽核協會(ISACA), COBIT 資訊及相關技術的管理控制與稽核, 2003/07。

表 3-3 資訊安全認知量表

基礎架構	行為目標	量　　表
極大化 資訊 完整性	極大化 存取控制邏輯	1. 需將資料進行加密。 2. 需限制使用者在同一時間多次的登入。 3. 不同層級的使用者，會有的不同的系統使用權限。 4. 在工作分工時，每個人會有不同的資訊使用權限。 5. 在人員離職後，該人員使用資訊的權限會解除。
	減少 對系統的損壞	6. 不同的使用者，存取資訊權限會有不同。
	減少病毒感染	7. 電腦病毒會經由家中電腦、筆記型電腦及行動設備等進行傳播及感染。 8. 電腦病毒會經由網際網路及電子郵件進行傳播及感染。 9. 進行作業系統漏洞修補可減少病毒入侵。
極大化 資訊 機密性	極大化密碼 使用的有效性	10. 使用高效密碼(Password7個字以上的密碼且英數交錯)並維持密碼的保密。 11. 需減少網路上使用高效密碼(Password)的組數並定期變更。 12. 當不使用電腦時，必須登出個人帳號(例如:XP 作業系統、網路銀行等)。
	居家行動設備 使用安全	13. 需小心使用數據機或網路設備進行遠端存取家中資料及行動設備資料。 14. 如何為家中及行動電腦、網路設備（例如：無線 AP）裝設密碼。
有效及 有效率的 使用電子 通訊資源	負責地使用 電子郵件及 網路	15. 使用網際網路的時間及成本。 16. 如何正確的設定網路系統(例如：個人防火牆)及收發電子郵件(例如：垃圾郵件攔截)。 17. 在收發電子郵件時，對於較大的附件及陌生郵件會謹慎處理。
極大化 資訊及 硬體設備 可用性	極大化實體 存取控制	18. 需要保護工作中所使用的實體設備(例如：減少遺失)。 19. 為保護實體設備的安全，必要時需加裝安全設備(例如：為筆記型電腦加裝安全鎖)。 20. 工作人員離職後，該人員使用實體設備的權限會解除。
	定時備份資料	21. 如何減少資料遺失或毀損的狀況。 22. 如何設定資料需要被保存的時間長度及條件。 23. 如何正確的設定備份以保存資料。 24. 對於重要資料的處理原則。 25. 備份設備的可用性及等級程度(例如：燒錄機使用、燒錄片容量等)。 26. 我瞭解備份資料需定期檢查是否保存完善。
極大化 接受 對行動的 責任感	極大化傳遞 給員工資訊量	27. 如何提升自我資訊素養、資訊管理及知識。 28. 透過觀看張貼文章、佈告欄等方式來吸收與工作相關的資訊方面知識。 29. 如何辨別重要資訊的原則及使用方法。 30. 不使用非法軟體及正版軟體如何使用才不觸法。
	遵守規則 (謹守政策)	31. 提升資訊管理和資訊素養及知識，以達到組織所要求之安全政策。 32. 察看組織內部的張貼文章、佈告欄等方式可了解組織所制定的安全政策。 33. 組織將風險透明化，可幫助員工了解安全事件的威脅、弱點及發生後的損失程度。 34. 我瞭解資訊及系統安全，可保障個人隱私或財產不致損失。
極大化 使用資源	極大化 內部使用者 之資訊獲得	35. 系統或軟體所提供的電腦資訊、效能數據，並知道在安全範圍內如何調整及運用。 36. 在程式中皆有錯誤訊息回報措施，透由網路回報方式來瞭解該軟體的使用者回饋資訊(例如：Windows XP自動錯誤回報功能)。 37. 工作資訊應做好管理及備份措施，減少知識的遺失(例如：誤刪檔案、撰寫標準作業流程等)。
	極大化外部知 識獲取	38. 經由專業研究報告(例如：資策會)，能提供現今資訊安全趨勢。 39. 經由新聞媒體及網站，了解最發生的資訊安全犯罪及防範方法。
	極大化資訊 安全相關 數據的使用	40. 如何判斷具有公信力的資訊安全相關之統計資料，並採納使用。

資料來源:本研究整理

[12].曹明玉, 資訊安全認知評量表之研究, 淡江大學資訊管理學系碩士班,2006。
[13].楊境恩, 國內警察人員資訊安全素養對資訊犯罪偵查能力影響之研究，樹德科技大學資訊管理系碩士班,2004。
[14].資策會, 資訊工業年鑑, 我國資訊軟體暨服務產業發展現況與重要議題,2007。
[15].蒲樹盛,BS7799 全球及台灣目前發展現況, http://asia.bsi-global.com/Taiwan+About/BSINews/BS-7799/ISMS-develop, visited on 2007/10/15。
[16].劉志銘, 資訊安全情境認知模式之研究, 淡江大學資訊管理學系碩士班,2005。
[17].蔡興樺, BS7799f 企業資訊安全管理認證, http://www.informationsecurity.com.tw/feature/view.asp?fid=79, 2001/06。
[18].B. Malisow, 2004, “Valuing Secure Access to Personal Information.”, http://www.securityfocus.com/infocus/1797, visited on 2007/10/9.
[19].CA Transforming IT Management, CA 2007 Internet Threat Outlook http://ca.com/files/SecurityAdvisorNews/ca_2007_internet_threat_outlook_final.pdf。
[20].COBIT, Governance, Control and Audit for Information and Related Technology, 3rd Edition Control Objectives, 1998.
[21].CSI(Computer Security Institute), The 12th Annual Computer Crime and Security Survey, 2007. http://i.cmpnet.com/v2.gocsi.com/pdf/CSISurvey2007.pdf。
[22].D. Gollmann, Computer Security, John Wiley & Sons Ltd.UK, 1999.
[23].E. C. Schneider, and G. W. therkalsen, How Secure Are Your System? , Avenues To Automation, pp.68-72, 1990/11.
[24].Ernst & Young, Global Information Security Survey 2004, http://ics.stpi.org.tw/Abstract/doc/29.pdf, visited on 2007/10/20.
[25].H.A. Kruger and W.D. Kearney, computers & security 25, A prototype for assessing information security awareness, P.289–296 , 2006.
[26].L. Drevin , H.A. Kruger and T. Steyn, Value-focused assessment of ICT security awareness in an academic environment , computers & security 26 p.36–43, 2007.
[27].M. Smith, Computer Security-Threats, Vulnerabilities and Countermeasures, Information Age, pp.205-210, 1989/10.
[28].M. Wilson, and J. Hash, ing an Information Technology Security ” Build Awareness and Training Program”, NIST(National Institute of Standards anTechnology), 2003/10.(NIST-Special Publication 800-50)
[29].NIST Special Publication 500-172, Computer Security Training Guide, 1989/11.
[30].NIST Special Publication 800-16, Information Technology Security Training Requirements: A Role- and Performance-Based Model (supersedes NIST Spec. Pub. 500-172), 1998/04, http://csrc.nist.gov/publications/nistpubs/800-16/800-16.pdf
[31].NIST, http://www.nist.gov/
[32].RL. Keeney, Creativity in decision making with value-focused thinking. Sloan Management Review, Summer:33–41, 1994.
[33].S. Hinde, If You Can Meet With Triumph and Disaster and Treat Those TwoImpostors Just the Same., Computers & Security, 20, PP.657-666, 2001.