組織人員遵守資訊安全規範意圖之探討 - 基於風險、利益及素養觀點

A Study on the Intention of Organizational Staff to Comply with Information Security Norms Based on the Perspectives of Risk, Interest and Literacy

游堯忠
大葉大學資訊管理學系
彰化縣515大村鄉學府路168號
yyj0419@gmail.com

劉定衢
國防大學資訊管理學系
台北市112北投區中央北路二段70號
dingchyu@gmail.com

黃莉涵
國防大學資訊管理學系
台北市112北投區中央北路二段70號
socutegirlsmile@gmail.com

摘要

資訊安全在現今更顯重要，為瞭解組織人員遵守資安規範意圖之影響因素，本研究以分解式計畫行為理論做為研究架構，探討「主觀規範」、「資安態度」、「知覺風險」、「知覺利益」，並加入「資訊安全認知」、「資訊安全素養」來驗證人員「遵守資安規範行為意圖」，歸納影響遵守意圖之主因，提供管理上建議。本研究以陸軍人員為對象，實施電子問卷調查，有效問卷計 402 份，用偏最小平方法（PLS）檢驗結構模型（Structural Model），分析、驗證模型中 8 項假說是否成立，發現各構念對於遵守意圖皆呈現正向顯著影響；各構念強度，以知覺風險最高，資訊安全認知次之，資安態度較低。透過實證結果，本研究提出強化人員遵循資訊安全規定之具體建議，可協助資訊安全政策訂定與改善，以降低組織人員因不遵守資安規定造成之損害。

關鍵詞：資訊安全素養、分解式計畫行為理論、遵守意圖。

Abstract

Information security is even more important in the current internet age. In order to understand the factors influencing organizational personnel’s intention to comply with information security norms, this study used the theory of decomposing planning behavior as the main framework for researching the relationship between "Subjective Norms", "Security Attitude", "Perceived Risk" and "Perceived Interests", adding "Information Security

Awareness" and "Information Security Literacy" as the factors to verify the subjects' compliance with information security. Through concluding the main factor affecting the subjects' behavior, we provided the advice on the management of information security.

This study aimed at the Army personnel, conducting by online electronic questionnaire survey and 402 valid questionnaires were recovered. We used the Partial Least Squares(PLS) way to validate the relationship between eight hypotheses in the structure model, in order to analyze and verify whether the hypotheses in this study were true. It showed that each construct has positively significant impact. Among the constructs, the factor of "Perceived Risk" affected subjects' behavior the most. The second one is "Information Security Awareness" and the last one is "Security Attitude".

Through the empirical results, this study put forward specific suggestions to strengthen staff's compliance with information security, which can help to formulate and improve information security policies, so as to reduce the damage caused by non-compliance of information security regulations.

Keywords: Information security literacy, disaggregated planning behavior theory, compliance intention.

一、前言

隨著資訊科技進步迅速，為使個人在網路空間中依然能受到保護，資訊安全議題逐漸受到重視，許多企業指出他們投入資訊安全支出已逐年上升(Deloitte, 2005; Gordon et al., 2005)；楊勝閎及林淑瓊（2018）指出醫療資訊電子化，並透過各種資通訊科技傳遞，資訊安全議題已成為醫療院所重視的最重要課題；資訊安全的重要性在過去大眾媒體與報章雜誌中雖然獲得強力宣導，令人驚訝是駭客攻擊事件卻持續增長，且未有減少的趨勢(Boss et al., 2009)。基於上述原因，維護資訊安全已成為高層管理的重點(Brancheau et al., 1996; Lohmeyer et al., 2002; Ransbotham and Mitra, 2009)，然而資訊人員或使用者本身如果無法遵照原本公司中資訊安全的規定，即使安全實體環境與資訊安全技術建置再縝密，仍然無法有效減少資安的問題發生(Herath and Rao, 2009)。iThome 在 2018 年調查了企業所面臨的十大資安風險，其中員工疏忽及欠缺資安意識為主要原因，以台積電在 2018 年肇生重大資安事件為例，因新機台內藏有 WannaCry 變種病毒，而安裝人員未按照標準作業程序掃毒，逕行連網而肇生該次事件。故資訊安全在現今社會是非常重要的一環，小至個人大至企業，都應該具有基本的資訊安全意識與認知，才能避免利益上之損失。

而現階段軍事組織面臨著資訊科技與網路快速發展，衍生許多資訊安全議題，對軍事組織及國家安全產生新的衝擊及挑戰。因此，國軍人員在資訊安全意識上，應具備新想法及觀念；尤其是國軍內部的資訊安全事件，大多牽涉到機敏性的問題，所造成的後果不僅是機密資料洩漏或金錢財物損失，更嚴重的是將損及國軍形象及危害國家安全（彭志暐，2017）；現在資安問題最主要的來源當屬「人」的疏忽，孫志忠（2014）整

理出民國 101-102 年空軍通航資聯隊產生之資安事件件數，計有人員誤插 USB 儲存媒體等 3 類 21 件及陸軍各單位在民國 107 年產生之資安事件件數高達 190 件，顯見「人」的因素對國軍內部影響不容忽視。

本研究參考國內外學者的研究後，認為以風險、利益及資安素養等觀點較能符合影響人員遵守資安規定意圖，並以各軍種中人數最多的陸軍為研究對象。因其資安狀況及環境應較其他軍種更為複雜，其所能產生的研究結果，更具指標性及建設性，期藉由探討陸軍人員對資安的素養及風險等知覺，進而找出影響人員違反或遵守資安的重要因素，做為資訊安全政策訂定檢討之參考。

本研究以人員的知覺風險、利益及資安素養等要素探討對態度、認知及意圖的影響，並提供各管理階層在制訂政策內容之參考。本研究目的如下：(1)經由文獻探討，研訂適切之研究方法並設計影響陸軍人員遵守資訊安全意圖之研究架構。(2)探討人員對資安風險、利益及資訊安全素養的認知，是否會影響其對資訊安全的態度、認知及遵守意圖。(3)歸納出影響陸軍人員遵守資訊安全意圖之主要因素，並提供陸軍各單位資安管理方式之建議，以提升整體資訊安全。

二、文獻探討

2.1 資訊安全之威脅

在資訊安全所面臨的威脅事件中，「自然因素」僅佔 15%，屬於「人為因素」高達 85%，其中人為因素裡 80%來自於組織內部員工的無心或是蓄意破壞（盧興義，2004）；黃一婷（2017）指出企業使用資訊安全的實體設備來加強防護以降低被駭客入侵的機率，但大多數的資安問題也都源自於人為的疏失，導致企業遭受駭客攻擊，讓商譽嚴重受損。因此「人」是難以掌控的，假如軍事人員缺乏資訊安全的認知及信念，進而對於遵守產生疑慮，將會影響國家整體安全，羅健銘（2016）在其論文中提到，國軍「資訊安全」是在防護資訊與資訊系統，並對抗非授權連線或資訊修改，以確保國家在執行各項行政或國防事務產生之資訊避免遭受到洩漏或損害。關於「人」這個因素，將是資訊安全威脅之一，需強化國軍人員在資訊安全的認知及遵從性，避免因資安事件產生實質損害及斲傷軍譽之情事發生。

2.2 知覺風險與利益

知覺風險的概念最早是由 Bauer(1960)所提出，發展至今已被用來廣泛的討論消費者行為，認為消費者所採取購買行為都可能產生無法預期的結果，而且結果可能有些是負面的。過去有研究結合其他行為相關理論如科技接受模型、計畫性行為理論、理性行為理論等，來探討資訊系統管理者接受新科技之意圖，亦有研究顯示知覺風險對創新科技的接受行為具有顯著的負面影響(Swaminathan et al.,1999)。Featherman and Pavlou (2003)整合過去的研究並重新定義知覺風險的財務、功能、時間、心理、社會、隱私與加總風險等構面在預測 e-services 的採納(Chang, 2010)。

而在知覺利益部分，過去的研究中各學者對於知覺利益有不同的看法。

Gutman(1982)指出知覺利益被視為一種結果，此結果能增加個人的效用或有助於達到高層次目標的價值。Park et al.(1986)認為利益是指消費者關於產品及服務屬性的個人價值和意義的認知，即消費者認為該產品及服務能夠帶給自己的好處與意義。利益依其內含動機可區分為三個種類：功能性利益(Functional Benefits)、象徵性利益(Symbolic Benefits)以及經驗性利益(Experiential Benefits)。

2.3 資訊安全素養

隨著資訊科技與網路技術的發展與盛行，國軍在內部管理上已逐漸開放各項通資器材使用，也正因為如此，國軍人員倘若缺乏資訊安全素養，國防機密資訊就容易外洩，將對組織造成無法彌補的傷害。國軍資訊安全整備工作，重點在落實資訊安全政策宣導及督管。鄭孫凱（2009）的研究發現，資訊安全的關鍵在於「人」、「制度」及「系統」，國軍一直以來均運用各種內部管理機制，加強所屬人員資安觀念及認知，以提升其資訊安全素養。楊境恩（2004）的研究提到「資訊安全素養」的能力，係指個人除了具備「資訊素養」外，必須能夠體認資訊安全的價值及力量，可以判斷行為的正當性，並熟悉尋求方法及具備評估及綜合資訊安全的能力。

2.4 資訊安全遵守意圖

影響組織之資訊安全程度或潛在的威脅，多數人認為與員工無關(Bulgurcu et al., 2010)，Kessel(2008)指出組織大多採用的資訊安全防護措施是以基本的科技技術或設備來減少風險以及確保資訊安全，容易想到的基礎設備像是與資訊安全有直接相關的防毒軟體、防火牆、網路交換器等資訊設備。Rogers(1975)表示如果個人對提出的建議採取適當的態度和行為即可以避免危險。Bulgurcu et al. (2010)提出員工願意遵循資訊安全政策(Information Security Policy)是增加組織資訊安全的關鍵要素。因此，員工的資訊安全行為意圖大致分為兩方面：程序性控制措施的遵守意圖和技術性控制措施的採用意圖。程序性控制措施遵循意圖包括對組織頒布的資訊安全命令、要求、法律、法規和法令的遵守；技術性控制是指技術性控制措施管控，使員工遵守資安意圖。

2.5 行為意圖相關理論

分解式計畫行為理論：由 Taylor and Todd(1995)提出分解式行為理論(Decomposed Theory of Planned Behavior, DTPB)」，結合 Fishbein and Ajzen(1975)的「理性行為模式（Theory of Reasoned Action, TRA）」、Ajzen(1985)及 Ajzen (1991)提出的「計畫行為理論(Theory of Planned Behavior, TPB)」模型，將影響其因素分解為「態度」、「主觀規範」及「知覺行為控制」三個構念。

Shimp and Kavas (1984)發現，多構念信念架構的提供，比傳統的單構念的架構更具契合度。Taylor and Todd (1995)將計畫行為理論的態度、主觀規範與知覺行為控制三個信念進行分別解構，提出「分解式計畫行為理論」；另據其研究結果顯示，分解式計畫行為模式用來了解使用者採用資訊科技的行為，比起科技接受模式多了「主觀規範」、「自我效能」等因素，對評估影響員工採用資訊科技的因素更準確。

綜合各行為意圖之理論內容，本研究將以分解式計畫行為理論為基礎探討陸軍人員資安行為意圖，並以態度及主觀規範研究官兵之資訊安全態度，以及官兵在採取遵守或違反資安行為時，所感受到其他外在意見時，認為是否該採取遵守或違反此資安行為的考量程度，例如「同儕影響」指的是同事及朋友等對該行為的看法；而「上級影響」指的是長官對該行為的看法，藉以探討出影響意圖之關鍵因素。

三、研究方法

3.1 研究假說推導

3.1.1 知覺風險對資安態度及遵守資訊安全規範意圖的關係

在傳統產業消費中，Huang(1993)指出消費者對農藥使用的知覺風險顯著影響消費者的態度；在網路消費方面，Jarvenpaa et al.(2000)指出即使消費者對於網路店家的印象不是非常良好，如果消費者覺得於該網路商家進行網路購物的風險是低的，即有可能形塑對於網路商家的正面態度，進而影響其網路購物意願；Chang (2010)指出知覺風險是影響消費者對於網路購物態度的重要因素之一，知覺風險越高時，消費者對於網路購物的態度越趨負面。綜上所述，無論在網路上還是現實生活中，知覺風險都會影響到態度，本研究認為，資安態度指的是人員對於資安政策遵守及認同的想法跟態度，就本研究的情境而言，如果能知覺到違反資安規定會產生的風險，應該會對資訊安全態度更正面，因此在人員面臨資安環境中，知覺風險愈高，對於資訊安全態度則愈高；反之，知覺風險愈低，相對於資訊安全態度愈低，因此本研究提出以下假說：

H1-1：人員的知覺風險對資訊安全態度有正向影響。

知覺風險會進而影響到消費者的傾向及購買意願(Shimp and Bearden,1982)。因此，當消費者覺得該購物網站不安全，則知覺其結果可能是負向的，進而影響購買態度(Swaminathan et al.,1999)；若消費者對於網路購物的知覺風險愈低，則購買態度會愈正向(Jarvenpaa et al.,1999)。

以本研究的情境而言，組織人員的資訊安全行為亦是如此，當個人面對遵守資安規定的議題時，所知覺到的風險程度較高時，會認為不遵守規定的後果是較不好的(如：洩密、系統中毒、資安事件、行政處分等)，則個人的知覺風險也就會隨之提高，進而提高人員資訊安全規範遵守意圖。綜合上述討論，因此本研究提出以下假說：

H1-2：人員的知覺風險對資訊安全規範遵守意圖有正向影響。

3.1.2 知覺利益對資安態度及遵守資訊安全規範意圖的關係

在飯店管理中，Kim and Han（2010）研究指出對待客人環境裡，一個人對某一特定知覺利益的感知影響行為的態度；同樣的情境下，他們也發現並驗證了知覺利益、態度和形象等變數之間的關係與顧客購買意願有很大關聯性。知覺風險及知覺利益與態度之

間是有相關聯性。

以本研究情境而言，知覺利益會影響到態度，人員如果能知覺到遵守資訊安全是有利益的，對資訊安全態度應該會是正面的，因此本研究認為，在人員面臨資安的環境中，知覺利益愈高，對於資訊安全態度則愈高；反之，知覺利益愈低，相對於資訊安全態度愈低，因此本研究提出以下假說：

H2-1：人員的知覺利益對資訊安全態度有正向影響。

利益是指消費者關於產品及服務屬性的個人價值和意義的認知，即消費者認為該產品及服務能夠帶給自己的好處與意義(Park et al., 1986)。知覺利益代表消費者個人心理主觀判斷在消費時所獲得之益處(Lovelock, 1983)，簡單來說就是某樣商品帶給消費者的好處。Zeithaml(1988)認為消費者的知覺價值會進一步產生購買意願，且消費者的購買行為通常取決於知覺其所獲得的價值與利益。根據 Youn(2005)的研究顯示，個人知覺其利益程度較高時，更願意在網站上提供個人資料。

以本研究的情境而言，當個人面對遵守資安規定的議題時，所知覺到的利益程度較高時，會認為遵守規定的後果是較好的，能夠帶給自己好處(如：單位榮譽、資安評比、獎勵等)，則個人的知覺利益會隨之提高，進而影響遵守意圖。綜合上述討論，因此本研究提出以下假說：

H2-2：人員的知覺利益對資訊安全規範遵守意圖有正向影響。

3.1.3 資訊安全素養與資訊安全認知的關係

資訊安全素養應指個人在具備操作資訊處理及傳播的工具與系統，包括電腦、媒體系統與網路的基本能力外，且需體認資訊安全價值與力量，並能判斷其正當性，並能瞭解資訊安全本質、管理的特性，熟悉尋求方法並具備評估解釋及綜合資訊安全的能力；Frank et al.(1991)認為資訊安全認知與個人資訊安全知識稱為日常業務中使用的基本素養與應用程式的一般知識。Rhee et al.(2009)指出，個人使用電腦基本能力和相關知識及經驗水準對資訊安全行為會有影響；Zheng et al.(2019)指出缺乏主動性、媒體使用能力不足、媒體選擇不當，是導致軍事院校的學生資訊認知不足的因素，於是有必要透過多種途徑加強這部分學生的資訊素養教育，因此我們假設素養是通過其知識維度直接影響認知。綜合上述討論，因此本研究提出以下假說：

H3：人員的資訊安全素養對資訊安全認知有正向影響。

3.1.4 主觀規範與遵守資訊安全規範意圖的關係

主觀規範說明了個人決定在進行某項行為時，會受到自身想法影響外，也會受到周遭社群環境的影響與壓力，像是父母、朋友或是其他個人認為其重要的關係人認同這項行為的程度。在先前探討遵守組織資安政策之意圖的研究中發現，主觀規範會顯著影響

遵守資安政策之意圖，假如個人發現工作環境周遭的人，像是同事、上司都遵守資安政策，個人去遵守資安政策的意願也相對較高(Chan et al., 2005; Knapp et al., 2006；Johnston and Warkentin, 2010；Ifinedo, 2012)。同樣邏輯套用到本研究中，遵守資訊安全之主觀規範對遵守資安規範之行為意圖會有正向影響。綜合上述討論，因此本研究提出以下假說：

H4：遵守資訊安全的主觀規範對遵守資訊安全規範意圖有正向影響。

3.1.5 態度與遵守資訊安全規範意圖的關係

態度與行為意圖間的關係，除了在先前資訊領域方面的研究中證實態度與行為意圖間確實存在著關聯性外(Herath and Rao, 2009;Pahnila et al., 2007; Venkatesh and Brown, 2001)，在 Ajzen(1985)所提出的計畫行為理論中也指出個人的態度會顯著影響行為意圖。因此，個人若對於自己組織的資安規範有正向的信念的話，將會影響個人遵守資安政策的行為意圖(Bulgurcu et al., 2010; Herath and Rao, 2009; Ng et al., 2009)。套用到本研究上，個人對遵守資安規範之態度越正面的話，個人遵守資安規範的行為意圖也會越高。綜合上述討論，因此本研究提出以下假說：

H5：人員對資訊安全規範之態度對遵守資訊安全規範意圖有正向影響。

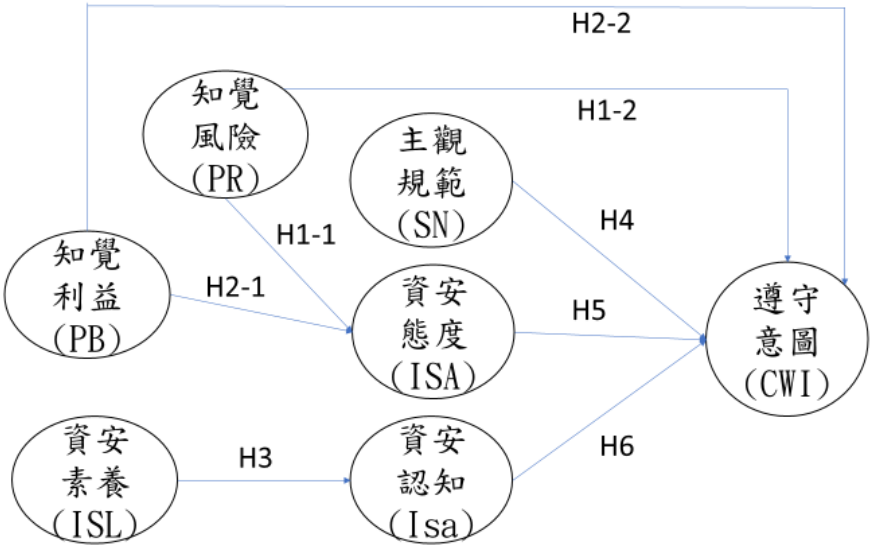
3.1.6 資訊安全認知與遵守資訊安全規範意圖的關係

在過去的研究中指出，員工的資訊安全認知在資訊安全管理中是很重要的一部分(Cavusoglu et al., 2009)，且 Bulgurcu et al.(2010)提出員工願意遵守資訊安全政策為增加組織資訊安全之關鍵要素。因此員工對資訊安全認知(Information Security Awareness)的知識程度高低，就顯得很重要。資訊安全認知的概念是指電腦使用者對資訊的安全認知，其目的在於呈現資訊安全上簡單的重點(Spurling, 1995)，認知使個人對資訊的威脅、攻擊與弱點感到敏感，並可識別出所需保護的資料、資訊與處理的過程。因此，當人員具有較高資訊安全認知，使其對資訊的威脅、攻擊與弱點感到敏感，瞭解違反資訊安全規範嚴重性，因而較不輕易做出違反資訊安全的行為。綜合上述討論，因此本研究提出以下假說：

H6:人員的資訊安全認知對遵守資訊安全規範意圖有正向影響。

3.2 研究模型

本研究根據相關文獻，以分解式計畫行為理論為基礎，建立本研究之研究架構，以主觀規範探討同儕團體及上級影響，並以資安態度探討知覺風險與知覺利益之關係，加入資訊安全認知及資訊安全素養等因素來驗證各受測者對於遵守資訊安全規範行為意圖，基於前節之假說推導過程，共計推導 8 條假說，相關研究模型整理詳如圖一。



圖一：研究架構

3.3 研究變項之概念型定義

根據上述之研究模型，本研究架構共包含七個構念，依序為知覺風險、知覺利益、資安素養、主觀規範、資安態度、資安認知及遵守意圖。各構念之操作型定義如表一所示。

表一：研究變項之操作型定義

研究變數	操作型定義
知覺風險	個人是否能察覺違反資訊安全規定產生之風險程度。
知覺利益	個人是否能察覺遵守資訊安全規定產生對自身利益程度。
資安素養	個人對於是否具操作及判斷資訊處理工具與系統（包括電腦、媒體系統及網路）之自我能力評估感知程度。
主觀規範	個人是否會因外在的環境及內部相關人際關係對資訊安全的影響與壓力程度。
資安態度	個人內在心理是否認同組織所規範之資訊安全政策的感知程度。
資安認知	個人對於資訊安全重要性與面對資安事件處理能力的自我感知程度。
遵守意圖	個人對於遵守資訊安全政策（規定、法律）意願高低的程度。

3.4 資料蒐集與處理

本研究採用量化研究方式驗證研究架構與假說。首先根據過往相關文獻，將所探討之知覺風險、知覺利益、資訊安全素養、資訊安全認知及遵守資訊安全規範行為意圖進行操作化定義，以及參採過往相關研究量表並加以修訂後，編製前測問卷；首先在前測問卷部分以紙本方式發放 50 份，回收後，以項目分析中常見的「極端組檢驗法」及「因

素分析法」兩種方法進行前測分析，其中不具鑑別力之問項，將予以刪除及調整成為正式問卷。

後續透過便利抽樣進行，針對陸軍北、中、南後勤部隊各階級人員，於軍事網路內製作線上問卷系統並透過電子郵件寄送實施調查，正式問卷回收後首先進行無效問卷剔除、反向題轉值等資料清理程序。後續利用 SPSS 進行敘述性統計分析，並利用 SmartPLS 統計軟體，於建模完成後進行兩階段的檢驗，第一階段檢驗量測模型(Measurement Model)，又稱外模式(Outer Model)，使用因素分析、信度分析、收斂效度、區別效度，檢視潛在變數和量測變數之間的關係，以檢驗量表能否真正反映出各研究構念，第二階段檢驗結構模型(Structural Model)，又稱內模式(Inner Model)，使用偏最小平方法，檢視本研究架構自變數與依變數之因果關係，以檢驗本研究假說是否成立。

3.5 信校度檢測與假說檢定

本研究將針對有效樣本進行檢定各構念問卷量表的信效度，以確保在檢定假說之前，各構念是具有良好的信效度表現，研究架構之構念包含知覺風險、知覺利益、資訊安全素養、資訊安全認知及遵守資訊安全規範行為意圖。在信度部分以因素負荷量、Cronbach's Alpha 係數、組合信度(Composite Reliability, CR)與平均變異萃取量(Average Variance Extracted, AVE)來衡量，確保問卷量表具有內部一致性、穩定及可靠；本研究在效度部分以區別效度(Discriminant Validity)及收斂效度(Convergent Validity)進行衡量，確認問卷量表能真實並正確的反應各研究構念。

而在假說檢定部分使用偏最小平方法(Partial Least Square, PLS)檢驗結構模型來衡量研究架構中自變數與依變數之因果關係，以驗證各研究假說。學者蕭文龍（2016）指出，結構方程模式(Structural Equation Modeling, SEM)為社會科學領域中相當盛行的統計方法，而偏最小平方法為其兩大主流技術之一「變異數型式結構方程模式(Variance-based SEM)」所使用的技術。相較另一主流技術共變數型式結構方程模式，具有(1)資料在無分配下可以迴歸分析獲得不錯的估計、(2)需求樣本較小、(3)在無分配機率模式下，迴歸分析不會受到傳統的多元共線性問題的影響等優勢。另有文獻指出，PLS 是基於最小平方法的假設前提，由一系統獨立迴歸來同時最小化線性內部結構關係及外部衡量關係，勝於傳統迴歸的殘差變異數矩陣，而且對於資料的統計分布形態並不要求，以及樣本數不需太多（Lin et al., 2014）。Chin and Newsted (1999)也曾提到 PLS 可用於結構模型複雜、非常態分配、樣本數較小、有多元共線性、及形成性模型與欲檢驗測量指標是否有效等情境。Chin et al. (2003)也提到 PLS 和迴歸分析相似，但能同時分析構念間的結構模式以及構念與衡量變數間的衡量模式關係，和其他多變量分析方法相比， PLS 不論在衡量的尺度或是樣本數量大小以及殘差的分配上的限制均較低。綜上，故本研究選用 PLS 做為主要的資料分析方法。

本研究根據 Bollen and Stine (1992)建議採用拔靴法(Bootstrapping)估計技術，以有限樣本反覆抽樣 5,000 次，利用所獲得之 t 值來推估 p 值，檢驗路徑係數是否達到統計上顯著性（t 值 > 1.96 及 p 值 < 0.05 代表具顯著性），以判斷假說是否成立，並瞭解研究變數之間的關係強度與方向性。

四、資料分析與結果

本研究樣本共計回收 525 份，扣除無效樣本 123 份，總計有效樣本為 402 份，有效問卷比率為 76.57%；無效樣本均為未通過反向題組檢驗。後續使用 SPSS 22.0 進行敘述性統計，並透過 SmartPLS 3.0 進行信度與效度分析、驗證性因素分析及路徑分析並驗證假說。

4.1 樣本人口統計變數分析

為瞭解受測者基本資料，依本次研究調查結果，就正式問卷中有效樣本之人口統計背景變項的基本資料分佈情形，分別敘述如下：(1)性別部分：受測者性別的分佈，男性有 255 人；女性有 147 人，受測者以男性居多。(2)年齡部分：受測者年齡層的分佈，在 20 歲以下有 5 人；21-30 歲有 139 人；31-40 歲有 166 人；41-50 歲有 43 人；51-60 歲有 38 人；61-70 歲有 11 人，調查結果顯示，受測者的年齡以 31-40 歲人數最多，其次依序為 21-30 歲、41-50 歲、51-60 歲、61-70 歲，而 20 歲以下人數最少。(3)民間學歷：受測者教育程度的分佈，學歷為高中職者有 90 人；大學(專科)者有 269 人；學歷為碩、博士者有 43 人。調查結果顯示，受測者教育程度以大學(專科)最多，高中職次之。以上樣本資料顯示符合我國陸軍後勤基層部隊之現況。

4.2 信度與效度分析

本研究針對有效樣本進行檢定各構念問卷量表的信效度，以確保在檢定假說之前，各構念是具有良好的信效度表現，本研究之構念包含知覺風險、知覺利益、資訊安全素養、主觀規範、資安態度、資訊安全認知及遵守資訊安全規範意圖。本研究在信度部分以因素負荷量、Cronbach's Alpha 係數、組合信度（Composite Reliability, CR）與平均變異萃取量（Average Variance Extracted, AVE）來衡量，確保問卷量表具有內部一致性、穩定及可靠；本研究在效度部分以區別效度（Discriminant Validity）及收斂效度（Convergent Validity）進行衡量，確認問卷量表能真實並正確的反應各研究構念。

4.2.1 信度分析

信度是指衡量檢驗問卷量表之一致與穩定性，經「因素負荷量」檢定後，本研究以「組合信度 (CR) 」、「rho_A」及「Cronbach's Alpha」值等 3 項衡量指標進行信度檢驗。其中 Cronbach's Alpha 及 CR 值係以加總後分數來衡量各問項之內部一致性，而 rho_A 值係以結構分數衡量一致性信度(Dijkstra and Henseler, 2015)，此 3 項衡量指標判斷標準均須達 0.7 以上，即代表信度良好(Nunnally, 1978; Homburg and Giering, 1996; Straub et al., 2004; Dijkstra and Henseler, 2015)。

綜上，本研究以 PLS Algorithm 估計技術，經檢驗各構念之 Cronbach's Alpha、CR 值、rho_A 等指標後，其結果均達 0.7 以上，符合信度判斷標準，證明本研究構念和問項具有良好的信度。信度檢驗結果如表二所示。

表二：信度分析表

構念	問項	因素負荷量	Cronbach's Alpha	CR	rho_A	檢驗結果
		> 0.5	> 0.7	> 0.7	> 0.7	
知覺風險 PR	PR1	0.815	0.800	0.883	0.802	通過
	PR2	0.869				
	PR3	0.852				
知覺利益 PB	PB2	0.793	0.810	0.887	0.822	通過
	PB3	0.890				
	PB4	0.868				
資訊安全素養 ISL	ISL1	0.845	0.904	0.926	0.904	通過
	ISL2	0.828				
	ISL3	0.772				
	ISL4	0.806				
	ISL5	0.844				
	ISL6	0.836				
主觀規範 SN	SN1	0.897	0.844	0.906	0.845	通過
	SN2	0.865				
	SN3	0.858				
資安態度 ISA	ISA1	0.848	0.840	0.903	0.844	通過
	ISA3	0.888				
	ISA4	0.873				
資訊安全認知 Isa	Isa2	0.840	0.896	0.923	0.897	通過
	Isa3	0.813				
	Isa4	0.864				
	Isa5	0.874				
	Isa6	0.811				
遵守資安規範意圖 CWI	CWI1	0.700	0.708	0.837	0.726	通過
	CWI3	0.848				
	CWI4	0.831				

資料來源：本研究整理

4.2.2 效度分析

效度檢驗係為衡量問卷量表與欲測量事物之契合度，效度愈高則表示該問卷量表愈是有效，即愈可檢測出所衡量之對象特質或功能。為確認本研究設計之問卷量表可否測出各構念之準確度，以 Anderson and Gerbing (1991)提出之方法，建構效度以衡量模型構念與理論的是否契合，檢定「收斂效度」及「區別效度」兩項指標皆達到檢驗水準，始

可確認為本問卷具有建構效度。

4.2.2.1 收斂效度分析

收斂效度，又稱聚合效度，係指當以多種工具測量同一構念時，構念結果間之相關程度，即指來自於相同潛察變項的觀察變項間的相關程度要高，顯示是否能夠有效的代表該構念。本研究以「因素負荷量」及「平均變異萃取量(AVE)」兩項指標進行收斂效度檢驗，因素負荷量已於信度檢驗時證明各測量變數皆通過判斷標準（因素負荷量> 0.5），如表二。而平均變異萃取量(AVE)為計算潛在變項之各測量變項對該潛在變項的平均變異解釋力，根據 Fornell and Larcker(1981)之判斷標準，AVE 須大於 0.5 才具效度，而 AVE 值愈高，則表示潛在變項具愈高之收斂效度；本研究各構念之 AVE 值均達 0.5 以上，證明本研究具有良好且足夠的收斂效度，檢驗結果如表三。

表三：收斂效度檢驗結果

構念	平均變異萃取量（AVE）	檢驗結果
	> 0.5	
知覺風險(PR)	0.715	通過
知覺利益(PB)	0.725	通過
資訊安全素養(ISL)	0.676	通過
主觀規範(SN)	0.763	通過
資安態度(ISA)	0.757	通過
資訊安全認知(Isa)	0.707	通過
遵守資安規範意圖(CWI)	0.633	通過

資料來源：本研究整理

4.2.2.2 區別效度分析

「區別效度」則用以檢驗不同構念間之相關程度，本研究之判斷標準為各構念自身之平均變異萃取量(AVE)根號值須大於與其他構念之間的相關係數（Fornell and Larcker , 1981），從表四得知，本研究各構念之平均變異萃取量根號值（對角線值，以粗體灰底標示）皆大於構念之間的相關係數（水平與垂直對應之非對角線值），證明各構念之間具有足夠的區別效度。綜上，驗證本研究設計之問卷量表具有足夠的收斂效度與鑑別度。

表四：區別效度表

	知覺風險 (PR)	知覺利益 (PB)	資訊安全素養 (ISL)	主觀規範 (SN)	資安態度 (ISA)	資訊安全認知 (Isa)	遵守資安規範意圖 (CWI)
知覺風險 (PR)	0.841						
知覺利益 (PB)	0.785	0.847					
資訊安全素養 (ISL)	0.619	0.725	0.820				
主觀規範 (SN)	0.698	0.729	0.706	0.871			
資安態度 (ISA)	0.675	0.766	0.814	0.727	0.866		
資訊安全認知 (Isa)	0.796	0.792	0.624	0.722	0.640	0.841	
遵守資安規範意圖 (CWI)	0.791	0.794	0.714	0.755	0.717	0.782	0.797
註：斜對角線值為平均變異萃取量（AVE）開根號，非對角線之其他數值為各構念相關。							

資料來源：本研究整理

4.2.3 假說驗證

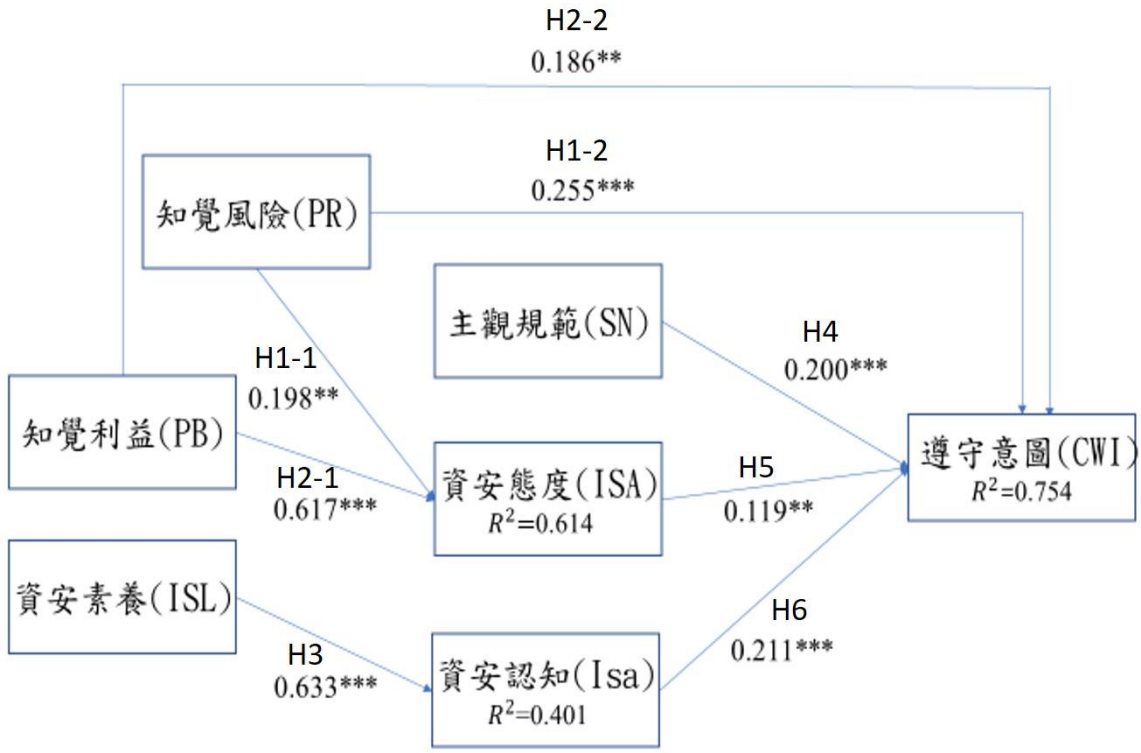
本研究使用偏最小平方法檢驗結構模型衡量模型中 8 項假說之關係，以分析與驗證各研究假說是否成立，本研究取得檢示資料如下：(1)檢驗路徑係數在統計上之顯著性：本研究根據 Bollen and Stine（1992）建議採用拔靴法評估方法，將回收有效樣本反覆抽樣 5,000 次，利用所獲得之 *t* 值推估 p 值，若各變數間路徑數（*t* 值）皆大於 1.96 且 *p* 值小於 0.05，代表具有 95%之信賴區間，並達顯著水準，可依以判斷假說是否成立，並瞭解研究變數之間的關係強度與方向性。(2)結構模型調整後解釋力R^2（R Square Adjusted）：用以判斷自變數對應變數所能夠解釋多少百分比之變異程度，具有多大的解釋力。

本研究將 Bootstrapping 檢驗結果整理成表五，並以表五繪製路徑係數圖（如圖二），假說結果顯著以實線表示，若假說結果不顯著以虛線表示：

表五：研究假說檢驗暨路徑係數表

假說	路徑	路徑係數	P 值	檢驗結果
H1-1	知覺風險→資安態度	0.198	0.003	成立
H1-2	知覺風險→遵守資訊安全規範意圖	0.255	0.000	成立
H2-1	知覺利益→資安態度	0.617	0.000	成立
H2-2	知覺利益→遵守資訊安全規範意圖	0.186	0.002	成立
H3	資訊安全素養→資訊安全認知	0.633	0.000	成立
H4	主觀規範→遵守資訊安全規範意圖	0.200	0.000	成立
H5	資安態度→遵守資訊安全規範意圖	0.119	0.017	成立
H6	資訊安全認知→遵守資訊安全規範意圖	0.211	0.000	成立

資料來源：本研究整理



註：* 表示 P<0.05、**表示 P<0.01、***表示 P<0.001

圖二：研究架構與路徑係數圖

（資料來源：本研究整理）

由本研究結果得知，知覺利益、知覺風險、主觀規範、資安態度及資訊安全認知對遵守資訊安全規範意圖均具有正向顯著關係，且知覺風險及知覺利益亦對資安態度具有正向顯著關係，另資訊安全素養對資訊安全認知亦具有正向顯著關係。

最後，進行模型解釋能力（R^2）分析，R^2值係指觀察變數對潛在變數所能解釋變異量的百分比，亦代表研究模型之預測力，其值介於 0 至 1 之間，當值愈大時，表示此模型的解釋能力愈佳。本研究參採學者 Bliemel et al. （2005）判斷標準（1）調整後 R^2 值 > 0.67，表示模型具實務上解釋力（2）調整後 R^2值 = 0.33，表示模型具中度解釋力（3）調整後 R^2值 < 0.19，表示模型解釋力薄弱。經研究顯示，各構念以資安態度、資訊安全認知及遵守資訊安全規範意圖，其調整後 R^2值分別為 0.614、0.401 及 0.754(如圖二)，顯示本研究各構念在遵守資訊安全規範意圖研究模型上均具有實務上解釋力。

五、結論與建議

本研究以 Taylor and Todd(1995)提出分解式行為理論，探討「主觀規範」、「資安態度」、「資安認知」、「知覺風險」、「知覺利益」及「資訊安全素養」對「遵守資安意圖」之影響，結果發現研究假說架構均獲支持。本研究設計之陸軍後勤人員遵守資訊安全意圖之架構經分析皆達顯著，人員對資安風險、利益及資訊安全素養認知影響其對資訊安全之態度、認知及遵循意圖。

由本研究結果證實，若要讓人員遵守資安意圖，可從增加「主觀規範」、「資安態度」、「資安認知」、「知覺風險」、「知覺利益」及「資訊安全素養」來提高，也就是如何讓人員對資安規範態度正向、讓人員了解不遵守規範必須承擔之風險及遵守可享有之好處、使人員能清楚知道資安事件對組織之傷害而避免違犯規定及肇生資事件。

另本研究在學術貢獻部分，Aurigemma and Mattson (2017)曾以計畫行為理論探討美國國防部人員態度、意圖及主觀行為之間關係，但未提及資安素養及資安認知；蘇建源等人(2010)之行為理論與本文相同，但僅提及「資安素養」加入構念進行探討。綜上結論，本研究在遵守意圖探討是以風險、利益、主觀規範、態度及認知為變項，相較之下更能突顯出本研究之面向多元，且各變項影響更為顯著，故研究結果應更具價值。

透過本研究，將有助於組織採取有效作法以提升人員之資訊安全遵守意圖。針對實務做法之建議，摘述如後

1. 本研究驗證了主觀規範對人員遵守資安意圖的影響。主觀規範係指個人對於組織內重要他人對自身行為的影響，故高階長官應以身作則，由上而下重視遵守各項資安規定及要求；此外亦應強化資訊安全教育，於組織內透過同儕影響逐步形塑資訊安全遵守氛圍。
2. 另對於針對違犯資訊安全相關規定之人員，應採具強度之懲罰措施，讓組織人員明白組織企圖。此外落實資安督導作為，依規定懲處及獎勵，增加其知覺風險考量以遵守資安意圖。另對於遵守規定人員定期獎勵，讓其因自身利益考量，減少違犯資訊安全規定。
3. 人員教育訓練對資安認知具影響效果，故組織應定期辦理資訊安全教育訓練，宣導近期資安威脅及人員違失態樣，並針對違犯規定人員提出檢討，以加強人員資安素養，遵守資安規定。

參考文獻

[1]孫志忠，2014，空軍通資專長人員資訊倫理、對國軍資安政策認知與資訊安全執行成效之研究，南臺科技大學資訊管理研究所碩士論文。

[2]黃一婷，2017，資訊素養與使用者誤點釣魚信件的關聯分析– 以 C 電信公司的使用者為例，國立中正大學會計與資訊科技學系碩士論文。

[3]彭志暐，2018，國軍資訊安全違規事件成因之研究– 最近十年之案例分析，健行科技大學財務金融系碩士論文。

[4]楊境恩，2004，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研究所碩士論文。

[5]楊勝閎、林淑瓊，2018，『影響醫療資訊系統資訊安全關鍵因素之研究』，TANET2018 臺灣網際網路研討會，國立中央大學主辦。

[6]鄭孫凱，2009，空軍人員資訊安全素養之評量與分析，國立臺東大學資訊管理學系碩士論文。

[7]盧興義，2004，危機管理在資訊安全上之研究－以防範「組織內部人員不當竊取」為例，大葉大學事業經營研究所碩士論文。

[8]羅健銘，2016，國軍人員之資訊安全素養及管理規定認知對於違反資安風險行為之研究－以空軍某營區開放使用智慧型手機為例，元智大學資訊管理學系碩士論文。

[9]蘇建源、江婉媚、阮金聲，2010，資訊安全政策實施對資訊安全文化與資訊安全有效性影響之研究。資訊管理學報，(17:4)，pp. 61-87。

[10]蕭文龍，2016，統計分析入門與應門—SPSS 中文版+SmartPLS3(PLS_SEM)，台北：碁峰資訊股份有限公司。

[11 Ajzen, I., 1985, From Intentions to Actions: A Theory of Planned Behavior, Action-control: From Cognition to Behavior, pp. 11-39,Springer, Heidelberg.

[12] Ajzen, I., 1991, The Theory of Planned Behavior. Organizational Behavior and Human Decision Processes (50:2), pp. 179-211.

[13] Anderson,J. C., and Gerbing, D. W., 1991, Predicting the performance of measures in a confirmatory factor analysis with a pretest assessment of their substantive validities. Journal of Applied Psychology (76:5), pp. 732-740.

[14] Aurigemma, S. and Mattson, T., 2017, Privilege or procedure: Evaluating the effect of employee status on intent to comply with socially interactive information security threats and controls. Computers & Security (66), pp. 218-234.

[15] Baumgartner, H. and Homburg, C., 1996, Applications of structural equation modeling in marketing nd consumer research: A review. International Journal of Research in Marketing,(13:2), pp. 139-161.

[16] Bauer, R. A., 1960, Consumer Behavior as Risk Taking. In R. S. Hancock, Dynamic Marketing for a Changing World. Chicago : American Marketing Association, pp. 389-398.

[17] Bollen, K. A., and Stine, R. A., 1992, Bootstrapping Goodness-of-Fit Measures in Structural

Equation Models. Sociological Methods & Research (21:2), pp. 205-229.

[18] Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., and Boss, R. W., 2009, If Someone is Watching, I'll do What I'm Asked: Mandatoriness, Control, and Information Security European Journal of Information Systems (18:2), pp. 151-164.

[19] Brancheau, J. C., Janz, B. D., and Wetherbe, J. C., 1996, Key Issues in Information Systems Management: 1994-95 SIM Delphi Results, MIS Quarterly (20:2), pp. 225-242

[20] Bulgurcu, B., Cavusoglu, H., and Benbasat, I., 2010, Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness MIS Quarterly (34:3), pp. 523-548.

[21] Cavusoglu, H., Cavusoglu, H., Son, J. Y., and Benbasat, I., 2009, Information Security Control Resources in Organizations: A Multidimensional View and Their Key Drivers, UBC Working Paper.

[22] Chan, M., Woon, I., and Kankanhalli, A., 2005, Perceptions of Information Security at the Workplace: Linking Information Security Climate to Compliant Behavior. Journal of Information Privacy and Security (1:3), pp. 18-41.

[23] Chang, A. J. T., 2010, Roles of Perceived Risk and Usefulness in Information System Security Adoption, Proceedings of the 2010 IEEE International Conference on Management of Innovation & Technology, pp 1264-1269.

[24] Chin, W.W. and Newsted, P.R., 1999, Structural equation modeling analysis with small samples using partial least squares. Statistical strategies for small sample research (1:1), pp.307-341.

[25] Chin, W.W., Marcolin, B.L., and Newsted, P.R., 2003, A Partial Least Squares Latent Variable Modeling Approach for Measuring Interaction Effects: Results from a Monte Carlo Simulation Study and an Electronic-mail Emotion/Adoption Study. Information Systems Research (14:2), pp. 189-217.

[26] Dijkstra, Theo K. and Henseler, Jörg., 2015, Consistent Partial Least Squares Path Modeling, MIS Quarterly (39: 2), pp. 297-316.

[27] Deloitte, 2005, Global Security Survey , Deloitte Touche Tohmatsu, London.

[28] Featherman, M. S., and Pavlou, P. A., 2003, Predicting E-Services Adoption: A Perceived Risk Facets Perspective. International Journal of Human-Computer Studies (59:4), pp. 451-474.

[29] Fishbein, M. and Ajzen, I., 1975, Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research, Addison-Wesley, Reading, Massachusetts, United States.

[30] Fornell,C. and Larcker, D, F., 1981, Evaluating Structural Equation Models with Unobservables and Measurement Error. Journal of Marketing Research (18:1),pp. 39-50.

[31] Frank, J., Shamir, B., and Briggs, W., 1991, Security-Related Behavior of PC Users in Organizations. Information & Management (21:3), pp. 127-135.

[32] Gordon, L. A., Loeb, M. P., Lucyshyn, W., and Richardson, R., 2005, CSI/FBI Computer Crime and Security Survey. Computer Security Journal (21:3), pp. 1.

[33] Gutman, J., 1982, A Means-End Chain Model Based on Consumer Categorization Processes.

Journal of Marketing (46:2), pp. 60-72.

[34] Herath, T., and Rao, H. R., 2009, Encouraging Information Security Behaviors in Organizations: Role of Penalties, Pressures and Perceived Effectiveness. Decision Support Systems (47:2), pp. 154-165.

[35] Huang, C. L., 1993, Simultaneous-Equation Model for Estimating Consumer Risk Perceptions, Attitudes, and Willingness-to-Pay for Residue-Free Produce. Journal of Consumer Affairs (27:2), pp. 377-396.

[36] Ifinedo, P.,2012, Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. Computers & Security(31:1), pp. 83–95.

[37] Jarvenpaa, S. L., Tractinsky, J., and Saarinen, L., 1999, Consumer Trust in an Internet Store: A Cross-Cultural Validation. Journal of Computer-Mediated Communication (5:2)

[38] Johnston, A. C., and Warkentin, M., 2010, Fear Appeals and Information Security Behaviors: an Empirical Study. MIS Quarterly (34:3), pp. 549-566.

[39] Kessel, P. V., 2008, Moving Beyond Compliance , Ernst & Young's Global Information Security Survey, London.

[40] Kim, Y., and Han, H., 2010, Intention to Pay Conventional-Hotel Prices at a Green Hotel–a Modification of the Theory of Planned Behavior. Journal of Sustainable Tourism (18:8), pp. 997-1014.

[41] Knapp, K. J., Marshall, T. E., Kelly Rainer, R., and Nelson Ford, F., 2006, Information Security: Management's Effect on Culture and Policy. Information Management & Computer Security (14:1), pp. 24-36.

[42] Lin, H., Fan, W., and Chau, P. Y. K., 2014, Determinants of users' continuance of social networking sites: A self-regulation perspective. Information & Management (51:5), pp. 595-603.

[43] Lohmeyer, D. F., McCrory, J., and Pogreb, S., 2002, Managing Information Security. The McKinsey Quarterly, pp. 12-16.

[44] Lovelock, C. H., 1983, Classifying Services to Gain Strategic Marketing Insights. Journal of Marketing (47:3), pp. 9-20.

[45] Ng, B. Y., Kankanhalli, A., and Xu, Y. C., 2009, Studying Users' Computer Security Behavior: A Health Belief Perspective. Decision Support Systems (46:4), pp. 815-825.

[46] Nunnally, J.C., 1978, Psychometric theory. 2nd Edition, McGraw-Hill, New York.

[47] Park, C. W., Jaworski, B. J., and MacInnis, D. J., 1986, Strategic Brand Concept-Image Management. Journal of Marketing (50:4), pp. 135-145.

[48] Pahnila, S., Siponen, M., and Mahmood, A., 2007, Employees' Behavior Towards is Security Policy Compliance. Proceedings of the 40th Hawaii International Conference on System Sciences - 2007

[49] Ransbotham, S., and Mitra, S., 2009, Choice and Chance: a Conceptual Model of Paths to

Information Security Compromise. Information Systems Research, (20:1), pp. 121-139.

[50] Rhee, H. S., Kim, C., and Ryu, Y. U., 2009, Self-Efficacy in Information Security: Its Influence on end Users' Information Security Practice Behavior. Computers & Security (28:8), pp. 816-826.

[51] Rogers, R. W., 1975, A Protection Motivation Theory of Fear Appeals and Attitude Change1. The Journal of Psychology (91:1), pp. 93-114.

[52] Shimp, T. A., and Kavas, A., 1984, The Theory of Reasoned Action Applied to Coupon Usage. Journal of Consumer Research (11:3) , pp. 795-809.

[53] Spurling, P., 1995, Promoting Security Awareness and Commitment. Information Management & Computer Security (3:2), pp. 20-26.

[54] Swaminathan, V., Lepkowska-White, E., and Rao, B. P., 1999, Browsers or Buyers in Cyberspace? An Investigation of Factors Influencing Electronic Exchange. Journal of Computer-Mediated Communication (5:2), JCMC523

[55] Taylor, S., and Todd, P. A., 1995, Understanding Information Technology Usage: A Test of Competing Models. Information Systems Research (6:2), pp. 144-176.

[56] Venkatesh, V., and Brown, S. A., 2001, A Longitudinal Investigation of Personal Computers in Homes: Adoption Determinants and Emerging Challenges. MIS Quarterly (25:1), pp. 71-102.

[57] Youn, S., 2005, Teenagers' Perceptions of Online Privacy and Coping Behaviors: A Risk–Benefit Appraisal Approach. Journal of Broadcasting & Electronic Media (49:1), pp. 86-110.

[58] Zeithaml, V. A., 1988, Consumer Perceptions of Price, Quality, and Value: A Means-end Model and Synthesis of Evidence. Journal of Marketing (52:3), pp. 2-22.

[59] Zheng, H. Y., Zhang, R. L., and Guo, C. R., 2019, The Information Literacy Assessment of Trainees Based on Cluster Analysis, Proceedings of the 2019 International Conference on Artificial Intelligence and Computing Science (ICAICS 2019), pp. 26-31.

[60] iThome，【iThome 2018 企業資安大調查：資安事件衝擊篇】員工資安意識不足的威脅，比駭客更大(available online at https://www.ithome.com.tw/article/122191)