專 論

機關文檔系統相關人員資安意識調查研究—以桃園市政府為例

A Survey Research on Cybersecurity Awareness of the Electronic Records Management Systems (ERMS) Related Staff: Taoyuan City Government as an Example

劉穎芝 Liu , Yin-Chih
桃園市政府警察局書記
Associate Clerk, Taoyuan Police Department

林巧敏 Lin, Chiao-Min
國立政治大學圖書資訊與檔案學研究所教授兼所長
Professor and Director, Graduate Institute of Library, Information and Archival Studies, National Chengchi University

摘要

隨著電子化文書及檔案的累積，機關文檔系統相關人員對於系統的資安維護扮演第一線的關鍵角色。本研究採用機關文檔及資訊人員資安意識調查問卷，以桃園市政府一級機關之文檔人員及資訊人員為對象，實際調查人員對於文檔系統資安意識認知現況。研究結果顯示機關文檔系統相關人員整體資安意識偏正向，且認知意見趨於一致，多數人最重視且對於機關達成程度最具信心的是「事件通報」，而最不重視的是「存取控制」，但對於機關的達成程度最不具信心的則為「備份機制」。比較資訊人員與文檔人員的資安意識認知程度，在「上網行為」、「事件通報」達顯著差異；比較不同背景，顯示年齡及教育訓練對於資安意識認知程度達顯著差異。

Abstract

With the accumulation of electronic documents and records, the Electronic Records Management Systems (ERMS) related staff including records management and information staff play a key role at the frontline of cybersecurity management. This study used a survey questionnaire on the cybersecurity awareness of ERMS and its respondents were record management and information staff of the first-level departments in Taoyuan City. The results show that the staff's overall cybersecurity awareness are positive and consistent. The facet that most of the staff place the most emphasis on and have the most confidence in the organization's achievement is "incident notification." However, the least emphasized facet is "access control" and the least confident facet is "backup mechanism." To explore the cognition of cybersecurity awareness of record management and information staff, significant differences exist in "online behavior" and "incident notification." In addition, for the cognition of cybersecurity awareness of staff with different backgrounds, significant differences exist in ages and training.

關 鍵 字｜資安意識、文檔系統、電子文件、機關檔案、檔案人員
Keywords｜Cybersecurity Awareness, Electronic Record Management Systems, Electronic Records, Agencies' Records, Record Management Staff

壹、前言

本研究所謂機關文檔系統相關人員，包含文檔及資訊人員。文檔人員是指機關文檔單位之文書管理人員及檔案管理人員，文書管理人員（簡稱文書人員）負責收發文、登記桌、公文時效管制等業務，檔案管理人員（簡稱檔案人員）負責檔案點收、立案編目、檢調、清理、保管、安全維護等業務。此外，因機關文檔系統資安問題亦屬資訊人員權責，故本研究納入資訊人員認知調查，所謂資訊人員包含機關內文書及檔案資訊系統之管理者、機關資通安全負責人員等。

有鑑於資安問題日益重要，本研究根據國內外資安意識相關文獻，擬具機關文檔及資訊人員的資安意識調查問卷，希望瞭解機關人員對於機關文檔資訊系統資安問題之重要性與達成程度的看法，藉此檢討機關文檔資訊系統資安教育訓練問題，以提供現行政策檢討或未來推動人員培訓課程規劃參考。

貳、文獻分析

一、資通安全理念及政策發展

根據行政院《資通安全管理法》，「資通安全」是指「防止資通系統或資訊遭受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，以確保其完整性、機密性及可用性」，包含資訊（information）及通信（或通訊）（communication）兩面向，我國英文官方翻譯為「cybersecurity」（數位發展部資通安全署，2022a），目標在於維持資訊的 3 個主要特性：完整性（integrity）、機密性（confidentiality）及可用性（availability），另外還涉及真實性（authenticity）、可歸責性（accountability）及不可否認性（non-repudiation）（International Organization for Standardization, 2018）。

資通安全國際標準種類繁多，包含網路安全框架 NIST CSF、ISO/IEC 27000 系列及 ISO27100、ISO 27701 等，我國資安標準依據為中華民國國家標準（CNS），主要是參考 ISO 國際標準所訂。經濟部標準檢驗局所訂之 CNS 27001 就是參考 ISO 27001 修訂，為我國資訊安全管理系統（ISMS）系列標準之重要綱要（行政院，2014）。

我國參酌美國《聯邦資訊安全現代化法（Federal Information Security Modernization Act of 2014, FISMA）》，於 2018 年 5 月立法院三讀通過《資通安全管理法》，由行政院公告於 2019 年 1 月 1 日併同其六大子法正式施行，六大子法包含《資通安全管理法施行細則》、《資通安全責任等級分級辦法》、《資通安全情資分享辦法》、《資通安全事件通報及應變辦法》、《特定非公務機關資通安全維護計畫》及《公務機關所屬人員辦理資通安全業務獎懲辦法》，至此我國正式邁向資安法制化階段。除了強調應整合民間及產業力量，推廣全民資安意識之外，尚包含培育資安專才、推動資安科技與產業，發展資安軟硬體技術規範、審驗機制及相關服務等（立法院公報處，2018）。面對日益嚴峻的資安威脅，我國於 2022 年 1 月 19 日總統公布《數位發展部組織法》，特設資通安全署作為我國資通安全政策規劃、計畫核議、督導考核，以及執行國家資通安全防護、演練與稽核業務及通訊傳播基礎設施防護之主責機關（數位發展部資通安全署，2022b），資通安全儼然是維護公共利益及國家安全之重要議題。

二、機關電子檔案資安問題分析

電子檔案涉及的資安議題可分為 6 個面向，分述如下（張文熙，2004）：

（一）傳送安全：以文檔系統而言，就是公文電子交換安全。

（二）人員安全：人員管制是資訊安全基本環

節，人員異動管理亦是帳號管理之基本。另外人員資安認知的加強也是機關的必要手段，一般使用者著重在加強基本操作，主管層級則應加強管理層面之觀念。

（三）設備安全：機房門禁系統可維護實體安全，亦為檔案資訊安全基礎，異地備援機制則是確保設備持續運作及危機管理的有效方式。

（四）網路安全：網路安全的需求對於電子檔案而言更顯重要，尤其現在攻擊手法不斷翻新，相對地，資安手段也要不斷翻新。

（五）檔案產生過程安全：系統可以部分防堵但無法完全防堵人為洩密問題，因此，在資料傳送的各個環節，都應避免發生漏洞。

（六）應用安全：包含應用內容、應用程式及操作安全，可透過防毒軟體、過濾系統、存取控制、非法入侵偵測、系統掃描及行為監控等作業來把關。

有關文檔系統的資安措施分為 4 個面向（國家發展委員會檔案管理局，2019）：

（一）主機管理：包含完善遠端連線軟體及機制、啟用防火牆、盡量不與對外系統共用主機、定期更新、安裝防毒軟體及定期進行全機掃描等。

（二）程式防護：包含用戶端及主機端，皆須檢核存取檔案格式，檔案存取目錄及程式執行目錄可採取不同路徑及應用雜湊值（hash values）來保護程式原始碼。

（三）危機處理：包含設定短、中、長期處理作為，並監看可疑檔案內容之電腦擁有者，修補漏洞或下架可疑程式，並應定期辦理資安鑑定。

（四）系統資訊安全宣導：除了在開發系統時，就應考量資安議題外，加強內部控管機制、釐清資安事件發生原因及強化人員防護意識均為必要措施，而外供應鏈資安威脅持續發生，因此加強委外人員資安意識，也應列入考量（行政院國家資通安全會報技術服務中心，2020）。

三、資安意識探討

資安意識（cybersecurity awareness 或 ICT security awareness）係指認知到資安重要性及瞭解資安問題發生時可能的後果，因而對於資安議題產生態度及相應行為，也是後續進行資安訓練的先備條件（Wilson, de Zafra, Pitcher, Tressler, & Ippolito, 1998 ; Wilson & Hash, 2003）。Hansche（2001）指出資安意識的建立，主要在於提高對於資訊系統安全的認識及瞭解資安漏洞可能的負面影響。Kruger & Kearney（2008）指出一個組織資通安全的良窳，除了仰賴資通科技防護，人員的資通安全活動同等重要，卻易被忽略，而人員資安意識需要循序建立且長期推動，才能有效提升組織的整體資安成效（SANS, 2021）。

有關資安意識之評估，在 NIST Special Publication 800-50 當中提到，資安意識探討的主題包含當前政策、個人責任、個人使用管理（含密碼、網絡使用、擁有的權限及設備）、防範病毒和其他惡意程式、電子郵件使用規則（不明及垃圾郵件及社交工程等）、備份儲存、事件通報、電腦桌面管理及避免資料遭肩窺（shoulder surfing）、系統環境、財產轉移、行動設備安全、機密資料處理及加密傳輸、存取控制等（Wilson & Hash, 2003）。

在國內研究當中，有關資安意識評估工具設計，通常會參考國際資安標準或國外學者設計，佐以邀集國內專家學者共同發展。歐芳伶（2008）以 Drevin, Kruger, & Steyn（2007）的資安意識評估架構為依據，並透過國內專家訪談來發展個人資訊安全認知量表，分為「極大化資訊完整性」、「極大化資訊機密性」、「有效及有效率使用電子通訊資源」、「極大化資訊及硬體設備可用性」、「極大化接受對行動的責任

感」、「極大化使用資源」等 6 大類。此外，吳倩萍（2006）以計畫行為理論為基礎，結合實務經驗主管層級人員及業界顧問之建議，歸納「事件通報」、「電子郵件」、「密碼管理」、「資料保護」、「實體安全」、「清空作業」、「其他」等構面。曹明玉（2006）則以 NIST Special Publication 800-16 當中的「ABC's of Information Technology Security」為基礎，採用疊慧法設計認知評量表，區分為「法律與規範」、「組織與資訊安全」、「系統互聯與資訊分享」、「敏感性」、「風險管理」、「管理控制」、「系統生命週期控制」、「作業控制」、「技術控制」等構面。上述各研究設計不盡相同，但許多基礎構面具共通性，通常不脫離資安的基本要求，也就是資料的完整性、機密性及可用性。

參、研究設計與實施

一、研究方法

本研究採個案調查方式，以政府機關人員為對象，進行機關文檔系統資安意識調查，以瞭解個案研究文檔系統相關人員對於資安意識認知程度及機關達成程度。

本研究設計之調查問卷綜合國內外資訊安全政策要點，參酌符合臺灣情境之現況與陳述，針對機關文檔及資訊人員設計機關調查問卷，並已先透過疊慧法建立專家效度，確立問卷內容。問卷填答分為 2 大部分，一為「資安意識評估題項」，另一為「個人基本資料」。

在「資安意識評估題項」，為分別瞭解人員對於該項議題的重要性及對於機關達成程度的認知，分為「認知重要性」及「機關達成程度」兩個向度，填答主要採用李克特 5 點量表計分，請填答者根據資安議題，分別勾選符合情形之選項，數字越大代表符合情形越高。

在「個人基本資料」，包含性別、年齡、職等職務、最高學歷及教育訓練等，不含具辨識之個資及所屬機關等資料，並放置於問卷最後，將填答干擾降至最小。

二、研究對象

本研究以實施文檔系統約 10 年之桃園市政府為個案分析對象，並以桃園市地方一級機關之文檔人員（文書及檔案）及資訊人員為調查對象進行問卷調查，共 26 局、5 處及 1 委員會，預估母群樣本約 500 至 600 人。參考 Raosoft（2004）對於樣本數量計算，本研究採大樣本抽樣（$n \geq 30$），且希望樣本數佔總母群體數的 10%以上、容許誤差範圍在 10%以內，如果樣本數達到 100 份，則容許誤差範圍預估在 5.32%至 8.13%之間，故評估樣本數至少需達到 100 份以上較為理想。

三、研究流程及資料分析

本研究於正式發放問卷前，邀請 10 人實施第一次前測，確認問卷內容是否便於填答，並以 Cronbach's α 係數值進行信度分析，以次數統計表確認變異性，以評估正式問卷最低樣本數。

正式問卷回收後進行篩檢及整理，剔除填答不完全資料並建檔後，以統計分析軟體 SPSS 20.0 及 SmartPLS 3.3.9 進行資料分析，方法如下：

（一）信效度分析：在信度方面，於前測問卷及正式問卷回收後，採用 Cronbach's α 係數值進行內部一致性的信度分析。在效度方面，則於正式問卷回收後，採用 SEM-PLS 進行驗證性因素分析。

（二）描述性統計：在基本資料部分，以次數分配表、百分比呈現。在填答資料部分，以有效數及遺漏值、次數分配表、百分比、平均數及標準差進行分析。在「機關達成程度」向度，如勾選「不清楚」選項，另

以遺漏值統計。

（三）獨立樣本 t 檢定：包含資訊人員和非資訊人員，以及其他可分為 2 個組別的背景因素包含性別、年齡、教育程度、有無接受教育訓練等，比較是否達顯著差異（$p < .05$）。

（四）多樣本中位數差異檢定（Kruskal Wallis test, K-W test）及 Dunn 檢定（Dunn post hoc test）：用於文書人員、檔案人員、資訊人員、文檔主管和委外人員等 5 個組別之比較，因樣本為非常態分布，當區分為 3 個以上的組別且其中一組未大於 30 個，又變異數同質時，便採用此檢定比較有無顯著差異。

（五）Welch's anova 平均值的強韌性檢定（Robust tests of equality of means） 及 Games-Howell 檢定（Games-Howell post-hoc test）：用於文書人員、檔案人員、資訊人員、文檔主管和委外人員等 5 個組別之比較，因為樣本為非常態分布，當區分為 3 個以上的組別且其中一組未大於 30 個，又變異數不同質時，則採用此檢定比較有無顯著差異。

（六）相關分析：以皮爾森積差相關（Pearson correlation）分析各構面以及「認知重要性」、「機關達成程度」兩個向度之間的關聯程度。

肆、研究結果分析

一、信效度分析

本問卷的信度分析，結果顯示在「認知重要性」向度，問卷總係數值為 .982，各構面係數值在 .739 至 .955 之間，在「機關達成程度」向度，問卷總係數值為 .975，各構面係數值在 .709 至 .914 之間，代表均屬可信至很可信範圍。本問卷的效度分析，有關收斂效度，在「認知重要性」向度，各題項的因素負荷量均大於 0.5，CR 均大於 0.8，在 AVE 部分，除了「帳戶管理」及「存取控制」屬略低可接受範圍（$0.4 \leq AVE < 0.5$），其餘構面 AVE 均大於 0.5；有關區別效度，在「認知重要性」向度，除了「電子交換」的 Cronbach's α 係數值 .758 略低於「電子交換」及「實體安全」相關係數值 .824，其餘任兩構面間的相關係數均小於個別構面的 Cronbach's α 係數值，在「機關達成程度」向度，則任兩構面間的相關係數均小於個別構面的 Cronbach's α 係數值，代表本問卷達到可接受的良好效度。

二、調查對象背景分析

本次調查對象共計 100 名，調查對象基本資料次數統計表詳見表 1。在性別方面以女性居多，計 67 人（67.0%），男性計 33 人（33.0%）。在年齡部分，以 31 至 40 歲最多，計 32 人（32.0%），其次為 41 至 50 歲，計 26 人（26.0%）。

在職等方面，正式公務人員有 73 人（73.0%），其中委任最多，計 51 人（51.0%），薦任計 22 人（22.0%），其他身分則有 27 人（27.0%），其中約僱人員最多有 18 人，另有委外人員 8 人及工友 1 人，委外人員 8 人當中有 7 人是資訊人員、1 人是檔案人員。

在職務方面，以文書人員最多，計 36 人（36.0%），檔案人員次之，計 34 人（34.0%），資訊人員（不含委外）則為居第三，計 19 人（19.0%）。在最高學歷方面，以大學最多，計 59 人（59.0%），其次為碩士，計 19 人（19.0%）。

在教育訓練方面，未接受過教育訓練者計 10 人（10.0%），其中文書人員 7 人，檔案、委外、資訊人員各 1 人。曾受過教育訓練者佔多數，計 90 人（90.0%），所受教育訓練類別則略不相同，以曾共同接受過文書、檔案、資訊（含資安）教育訓練者居多，計 24 人（佔總樣本數 24.0%，佔有教育訓練者 26.7%）；其次為只有資訊（含資安）教育訓練者，計 16 人（佔總樣

表 1　調查對象基本資料次數統計表

n=100

基本資料變項	組別	次數	百分比%	累積百分比%
性別	女 *	67	67.0	67.0
	男	33	33.0	100.0
年齡	18-30 歲	15	15.0	15.0
	31-40 歲 *	32	32.0	47.0
	41-50 歲	26	26.0	73.0
	51-60 歲	25	25.0	98.0
	61 歲以上	2	2.0	100.0
職等	委任 *	51	51.0	51.0
	薦任	22	22.0	73.0
	其他	27	27.0	100.0
	- 工友	1	3.7	3.7
	- 約僱人員 *	18	66.7	70.4
	- 委外人員	8	29.6	100.0
職務	文書人員 *	36	36.0	36.0
	檔案人員	33	33.0	69.0
	資訊人員	19	19.0	88.0
	文檔主管	4	4.0	92.0
	委外人員	8	8.0	100.0
	- 委外資訊人員	7	87.5	87.5
	- 委外檔案人員	1	12.5	100.0
最高學歷	高中（職）	5	5.0	5.0
	專科	15	15.0	20.0
	大學 *	59	59.0	79.0
	碩士	19	19.0	98.0
	博士	2	2.0	100.0
接受教育訓練	否	10	10.0	10.0
	是 *	90	90.0	100.0
	- 只有文書	14	15.6	15.6
	- 只有檔案	13	14.4	30.0
	- 只有資訊（含資安）	16	17.8	47.8
	- 文書 & 檔案	12	13.3	61.1
	- 文書或檔案 & 資訊（含資安）	11	12.2	73.3
	- 文書 & 檔案 & 資訊（含資安）*	24	26.7	100.0

資料來源：作者彙整

*：表示次數最多

本數 16.0%，佔有教育訓練者 17.8%）。而有接受過資訊（含資安）教育訓練者，計 51 人（佔總樣本數 51.0%，佔有教育訓練者 56.7%），超過整體人數的一半。

三、資安意識調查分析

為瞭解機關人員在資安意識各構面的「認知重要性」及「機關達成程度」現況，根據問卷統計結果，分述如下：

（一）帳戶管理

在「認知重要性」向度，平均數為 4.77，標準差為 0.47；有 79.0％認為非常重要，19.3％認為重要，1.5％認為普通，0.2％認為不重要，各題項平均數落在 4.67 至 4.84 之間，標準差落在 0.37 至 0.57 之間。在「機關達成程度」向度，平均數為 4.49，標準差為 0.69；有 59.2％認為完全符合，30.7％認為大部分符合，8.5％認為部分符合，0.7％認為大部分不符合，0.2％認為完全不符合，另外有 0.7％表示不清楚，各題項平均數落在 4.28 至 4.76 之間，標準差落在 0.45 至 0.80 之間。

（二）存取控制

在「認知重要性」向度，平均數為 4.68，標準差為 0.59；有 73.2％認為非常重要，21.8％認為重要，4.7％認為普通，0.1％認為不重要，0.2％認為非常不重要，各題項平均數落在 4.31 至 4.86 之間，標準差落在 0.38 至 0.88 之間。在「機關達成程度」向度，平均數為 4.53，標準差為 0.69；有 61.4％認為完全符合，29.1％認為大部分符合，6.3％認為部分符合，1.1％認為大部分不符合，0.3％認為完全不符合，另外有 1.8％表示不清楚，各題項平均數落在 4.24 至 4.69 之間，標準差落在 0.60 至 0.82 之間。

（三）系統防護

在「認知重要性」向度，平均數為 4.75，標準差為 0.48；有 76.8％認為非常重要，21.1％認為重要，2.1％認為普通。各題項平均數落在 4.64 至 4.84 之間，標準差落在 0.38 至 0.58 之間。在「機關達成程度」向度，平均數為 4.59，標準差為 0.66；有 60.6％認為完全符合，23.6％認為大部分符合，4.7％認為部分符合，1.1％認為大部分不符合，0.1％認為完全不符合，另外有 9.9％表示不清楚。各題項平均數落在 4.21 至 4.79 之間，標準差落在 0.47 至 0.85 之間。

（四）行動安全

在「認知重要性」向度，平均數為 4.78，標準差為 0.45；有 79.0％認為非常重要，19.5％認為重要，1.5％認為普通。各題項平均數落在 4.74 至 4.81 之間，標準差落在 0.42 至 0.49 之間，在「機關達成程度」向度，平均數為 4.50，標準差為 0.67；有 56.0％認為完全符合，31.5％認為大部分符合，6.5％認為部分符合，1.0％認為大部分不符合，無填答者認為完全不符合，另外有 5.0％表示不清楚。各題項平均數落在 4.44 至 4.56 之間，標準差落在 0.67 至 0.68 之間。

（五）上網行為

在「認知重要性」向度，平均數為 4.77，標準差為 0.45；有 79.0％認為非常重要，19.4％認為重要，1.6％認為普通。各題項平均數落在 4.63 至 4.87 之間，標準差落在 0.34 至 0.58 之間，在「機關達成程度」向度，平均數為 4.53，標準差為 0.65；有 57.6％認為完全符合，31.4％認為大部分符合，5.9％認為部分符合，0.4％認為大部分不符合，0.1％認為完全不符合，另外有 4.6％表示不清楚。各題項平均數落在 4.23 至 4.78 之間，標準差在 0.42 至 0.73 之間。

（六）電子交換

在「認知重要性」向度，平均數為 4.77，標準差為 0.50；有 80.2％認為非常重要，17.6％認為重要，1.8％認為普通，0.2％認為不重要，0.2％認為非常不重要。各題項平均數落在 4.72 至 4.82 之間，標準差落在 0.39 至 0.60 之間，在「機關達成程度」向度，平均數為 4.61，標準差為 0.62；有 62.0％認為完全符合，28.2％認為大部分符合，2.0％認為部分符合，0.8％認為大部分不符合，0.4％認為完全不符合，另外有 6.6％表示不清楚。各題項平均數落在 4.38 至 4.80 之間，標準差落在 0.40 至 0.85 之間。

（七）實體安全

在「認知重要性」向度，平均數為 4.76，標準差為 0.45；有 76.8％認為非常重要，22.1％認為重要，1.1％認為普通，沒有填答者認為不重要或非常不重要。各題項平均數落在 4.60 至 4.85 之間，標準差落在 0.36 至 0.59 之間，在「機關達成程度」向度，平均數為 4.64，標準差為 0.60；有 66.9％認為完全符合，24.4％認為大部分符合，3.9％認為部分符合，0.5％認為大部分不符合，0.1％認為完全不符合，另外有 4.2％表示不清楚。各題項平均數落在 4.19 至 4.81 之間，標準差落在 0.40 至 0.90 之間。

（八）備份機制

在「認知重要性」向度，平均數為 4.70，標準差為 0.52；有 72.6％認為非常重要，24.4％認為重要，3.0％認為普通。各題項平均數落在 4.60 至 4.80 之間，標準差落在 0.44 至 0.59 之間，在「機關達成程度」向度，平均數為 4.37，標準差為 0.82；有 48.8％認為完全符合，28.4％認為大部分符合，9.6％認為部分符合，1.4％認為大部分不符合，1.0％認為完全不符合，另外有 10.8％表示不清楚。各題項平均數落在 4.19 至 4.56 之間，標準差落在 0.74 至 0.93 之間。

（九）遵守政策

在「認知重要性」向度，平均數為 4.70，標準差為 0.49；有 71.7％認為非常重要，26.8％認為重要，1.5％認為普通。各題項平均數落在 4.64 至 4.76 之間，標準差落在 0.45 至 0.56 之間，在「機關達成程度」向度，平均數為 4.61，標準差為 0.64；有 64.0％認為完全符合，24.7％認為大部分符合，4.3％認為部分符合，0.8％認為大部分不符合，0.2％認為完全不符合，另外有 6.0％表示不清楚。各題項平均數落在 4.36 至 4.78 之間，標準差落在 0.49 至 0.77 之間。

（十）事件通報

在「認知重要性」向度，平均數為 4.82，標準差為 0.40；有 82.7％認為非常重要，16.7％認為重要，0.6％認為普通。各題項平均數落在 4.76 至 4.85 之間，標準差落在 0.36 至 0.47 之間，在「機關達成程度」向度，平均數為 4.70，標準差為 0.49；有 66.3％認為完全符合，24.7％認為大部分符合，1.3％認為部分符合，另外有 7.7％表示不清楚。各題項平均數落在 4.68 至 4.72 之間，標準差落在 0.48 至 0.51 之間。比較發現各題項之間差異不大，平均數皆大於 4，標準差皆小於 0.60。

整體而言，在「認知重要性」向度，平均數為 4.74，標準差為 0.49；有 76.5％認為非常重要，21.3％認為重要，2.1％認為普通，0.05％認為不重要，0.05％認為非常不重要，也就是認為不重要或非常不重要趨近於零。各構面平均數介於 4.68 至 4.82 之間，標準差介於 0.40 至 0.59 之間，其中以「事件通報」的平均數最高（M=4.82, SD=0.40），「存取控制」的平均數最低（M=4.68, SD=0.59）。在「機關達成程度」向度，平均數為 4.57，標準差為 0.66；有 61.3％認為完全符合，27.1％認為大部分符合，5.3％認為部分符合，0.8％認為大部分不符合，0.2％認為完全不符合，另外有 5.3％表示不清楚，其中不清楚比例最高的前 3 名分別是「備份機制」（10.8％）、「系統防護」（9.9％）及「事件通報」（7.7％），若將填答不清楚選項的人員以職務身分區分，則占比依高至低排序為文書人員（7.30％）、檔案人員（6.60％）、委外人員（5.41％）、資訊人員（0.55％）。若將填答不清楚的選項以遺漏值處理，則有 64.7％認為完全符合，28.6％認為大部分符合，5.6％認為部分符合，0.8％認為大部分不符合，0.3％認為完全不符合。各構面平均數介於 4.37 至 4.70 之間，標準差介於 0.49 至 0.82 之間，其中亦是「事件通報」構面的平均數最高（M=4.70, SD=0.49），另外在「備份機制」構面的平均數最低（M=4.37, SD=0.82），詳見表 2。

表 2　文檔系統資安意識調查結果統計分析表

構面	向度	有效數	選項	次數	百分比%	平均數	標準差
帳戶管理	認知重要性	600	非常重要	474	79.0	4.77	0.47
			重要	116	19.3		
			普通	9	1.5		
			不重要	1	0.2		
			非常不重要	0	0.0		
	機關達成程度	596	完全符合	356	59.2	4.49	0.69
			大部分符合	184	30.7		
			部分符合	51	8.5		
			大部分不符合	4	0.7		
			完全不符合	1	0.2		
			不清楚	4	0.7		
存取控制	認知重要性	1000	非常重要	732	73.2	4.68	0.59
			重要	218	21.8		
			普通	47	4.7		
			不重要	1	0.1		
			非常不重要	2	0.2		
	機關達成程度	982	完全符合	614	61.4	4.53	0.69
			大部分符合	291	29.1		
			部分符合	63	6.3		
			大部分不符合	11	1.1		
			完全不符合	3	0.3		
			不清楚	18	1.8		
系統防護	認知重要性	900	非常重要	691	76.8	4.75	0.48
			重要	190	21.1		
			普通	19	2.1		
			不重要	0	0		
			非常不重要	0	0		
	機關達成程度	811	完全符合	546	60.6	4.59	0.66
			大部分符合	212	23.6		
			部分符合	42	4.7		
			大部分不符合	10	1.1		
			完全不符合	1	0.1		
			不清楚	89	9.9		
行動安全	認知重要性	200	非常重要	158	79.0	4.78	0.45
			重要	39	19.5		
			普通	3	1.5		
			不重要	0	0.0		
			非常不重要	0	0.0		

構面	向度	有效數	選項	次數	百分比%	平均數	標準差
上網行為	機關達成程度	190	完全符合	112	56.0	4.50	0.67
			大部分符合	63	31.5		
			部分符合	13	6.5		
			大部分不符合	2	1.0		
			完全不符合	0	0.0		
			不清楚	10	5.0		
	認知重要性	700	非常重要	553	79.0	4.77	0.45
			重要	136	19.4		
			普通	11	1.6		
			不重要	0	0.0		
			非常不重要	0	0.0		
	機關達成程度	668	完全符合	403	57.6	4.53	0.65
			大部分符合	220	31.4		
			部分符合	41	5.9		
			大部分不符合	3	0.4		
			完全不符合	1	0.1		
			不清楚	32	4.6		
電子交換	認知重要性	500	非常重要	401	80.2	4.77	0.50
			重要	88	17.6		
			普通	9	1.8		
			不重要	1	0.2		
			非常不重要	1	0.2		
	機關達成程度	467	完全符合	310	62.0	4.61	0.62
			大部分符合	141	28.2		
			部分符合	10	2.0		
			大部分不符合	4	0.8		
			完全不符合	2	0.4		
			不清楚	33	6.6		
實體安全	認知重要性	1400	非常重要	1076	76.8	4.76	0.45
			重要	309	22.1		
			普通	15	1.1		
			不重要	0	0.0		
			非常不重要	0	0.0		
	機關達成程度	1341	完全符合	936	66.9	4.64	0.60
			大部分符合	342	24.4		
			部分符合	54	3.9		
			大部分不符合	7	0.5		
			完全不符合	2	0.1		
			不清楚	59	4.2		

構面	向度	有效數	選項	次數	百分比%	平均數	標準差
備份機制	認知重要性	500	非常重要	363	72.6	4.70	0.52
			重要	122	24.4		
			普通	15	3.0		
			不重要	0	0.0		
			非常不重要	0	0.0		
	機關達成程度	446	完全符合	244	48.8	4.37	0.82
			大部分符合	142	28.4		
			部分符合	48	9.6		
			大部分不符合	7	1.4		
			完全不符合	5	1.0		
			不清楚	54	10.8		
遵守政策	認知重要性	600	非常重要	430	71.7	4.70	0.49
			重要	161	26.8		
			普通	9	1.5		
			不重要	0	0.0		
			非常不重要	0	0.0		
	機關達成程度	564	完全符合	384	64.0	4.61	0.64
			大部分符合	148	24.7		
			部分符合	26	4.3		
			大部分不符合	5	0.8		
			完全不符合	1	0.2		
			不清楚	36	6.0		
事件通報	認知重要性	300	非常重要	248	82.7	4.82	0.40
			重要	50	16.7		
			普通	2	0.6		
			不重要	0	0.0		
			非常不重要	0	0.0		
	機關達成程度	277	完全符合	199	66.3	4.70	0.49
			大部分符合	74	24.7		
			部分符合	4	1.3		
			大部分不符合	0	0.0		
			完全不符合	0	0.0		
			不清楚	23	7.7		
整體構面	認知重要性	6700	非常重要	5126	76.50	4.74	0.49
			重要	1429	21.33		
			普通	139	2.07		
			不重要	3	0.05		
			非常不重要	3	0.05		

構面	向度	有效數	選項	次數	百分比%	平均數	標準差
	機關達成程度	6342	完全符合	4104	61.25	4.57	0.66
			大部分符合	1817	27.12		
			部分符合	352	5.25		
			大部分不符合	53	0.79		
			完全不符合	16	0.24		
			不清楚	358	5.34		

資料來源：作者彙整

四、不同背景職務資安意識之差異分析結果

本研究區分為資訊人員（含委外或不含委外）和非資訊人員 2 個組別，及其他可分為 2 個組別的因素，包含性別、年齡、教育程度、有無接受教育訓練及有無接受資訊教育訓練等，以獨立樣本 t 檢定分析比較不同背景的資安意識程度有無顯著差異。結果顯示整體構面達顯著差異的為年齡及教育訓練因素，但不限於資訊教育訓練。其中超過 40 歲者資安意識大於 40 歲以下（t= -3.06, p=.003 ＜ .01），有教育訓練大於無教育訓練（t= 2.09, p=.040 ＜ .05），其餘因素均無顯著差異。

在個別構面部分，達顯著差異的各有不同，在年齡方面僅「事件通報」未達顯著差異（t= -1.25, p=.216 ＞ .05），其餘構面皆達顯著差異，超過 40 歲者大於 40 歲以下。在教育訓練方面，「存取控制」（t=3.11, p=.002 ＜ .01）、「上網行為」（t=2.10, p=.039 ＜ .05）、「電子交換」（t=2.09, p=.040 ＜ .05）等 3 構面達顯著差異，有教育訓練大於無教育訓練，其餘未達顯著差異；在「事件通報」構面，資訊人員（不含委外）大於非資訊人員（t=4.04, p=.000 ＜ .001），詳見表 3。

為進一步比較不同職務身分的資安意識程度，細分文書人員、檔案人員、文檔主管、資訊人員和委外人員等 5 組身分，以多樣本中位數差異檢定及 Dunn 檢定、Welch's anova 平均值的強韌性檢定及 Games-Howell 檢定進行分析，結果顯示在「上網行為」構面，檔案人員（不含委外）的資安意識大於委外人員（含資訊及檔案）；在「事件通報」構面，資訊人員（不含委外）的資安意識大於文書人員，詳見表 4。

五、相關分析

為瞭解各構面之間，以及「認知重要性」、「機關達成程度」之間的關聯程度，以皮爾森積差進行相關分析，則得出以下結果：

（一）構面相關分析

在「認知重要性」向度，各構面均為顯著正相關，其中「存取控制」和「系統防護」、「上網行為」和「電子交換」、「電子交換」和「實體安全」、「備份機制」和「遵守政策」之間呈現高度正相關（r ≧ 0.8, p ＜ .001），其餘各構面之間呈現中度正相關（r ≧ 0.4, p ＜ .001）。在「機關達成程度」向度，各構面亦均呈現顯著正相關，其中在「存取控制」和「系統防護」之間呈現高度正相關（r ≧ 0.8, p ＜ .001），「行動安全」和「遵守政策」之間呈現低度正相關（r ＜ 0.4, p ＜ .001），其餘各構面之間呈現中度正相關（r ≧ 0.4, p ＜ .001），詳見表 5、6。

表 3　不同背景職務資安意識構面 t 檢定結果

構面	組別	平均數	標準差	t 值	顯著性
帳戶管理	資訊人員（含委外） 非資訊人員	4.79 4.76	0.29 0.33	0.43	.671
	資訊人員（不含委外） 非資訊人員	4.82 4.76	0.29 0.33	0.73	.466
	女 男	4.76 4.80	0.34 0.27	-0.68	.496
	年齡≦ 40 歲 年齡＞ 40 歲	4.67 4.86	0.35 0.26	-2.93	.004**
	大學以下 碩士以上	4.79 4.70	0.32 0.34	1.18	.241
	有教育訓練 無教育訓練	4.79 4.60	0.31 0.40	1.80	.075
	有資訊教育訓練 無資訊教育訓練	4.82 4.75	0.26 0.35	1.04	.300
存取控制	資訊人員（含委外） 非資訊人員	4.56 4.72	0.40 0.36	-1.87	.065
	資訊人員（不含委外） 非資訊人員	4.65 4.72	0.41 0.36	-0.77	.445
	女 男	4.70 4.64	0.36 0.41	0.83	.406
	年齡≦ 40 歲 年齡＞ 40 歲	4.55 4.80	0.41 0.29	-3.37	.001**
	大學以下 碩士以上	4.71 4.57	0.39 0.31	1.59	.115
	有教育訓練 無教育訓練	4.72 4.34	0.35 0.43	3.11	.002**
	有資訊教育訓練 無資訊教育訓練	4.74 4.69	0.34 0.38	0.75	.456
系統防護	資訊人員（含委外） 非資訊人員	4.74 4.75	0.34 0.38	0.63	.907
	資訊人員（不含委外） 非資訊人員	4.85 4.75	0.26 0.38	1.39	.173
	女 男	4.74 4.76	0.39 0.34	-0.33	.740
	年齡≦ 40 歲 年齡＞ 40 歲	4.65 4.83	0.40 0.32	-2.55	.013*
	大學以下 碩士以上	4.77 4.67	0.37 0.37	1.11	.268

構面	組別	平均數	標準差	t 值	顯著性
	有教育訓練 無教育訓練	4.77 4.57	0.36 0.41	1.63	.106
	有資訊教育訓練 無資訊教育訓練	4.81 4.71	0.32 0.41	1.34	.186
行動安全	資訊人員（含委外） 非資訊人員	4.73 4.79	0.49 0.38	-0.64	.526
	資訊人員（不含委外） 非資訊人員	4.82 4.79	0.51 0.38	0.24	.810
	女 男	4.77 4.79	0.44 0.35	-0.22	.827
	年齡≦ 40 歲 年齡＞ 40 歲	4.65 4.89	0.50 0.27	-2.91	.005**
	大學以下 碩士以上	4.80 4.67	0.42 0.37	1.37	.175
	有教育訓練 無教育訓練	4.82 4.40	0.36 0.66	1.97	.078
	有資訊教育訓練 無資訊教育訓練	4.84 4.78	0.31 0.41	0.81	.422
上網行為	資訊人員（含委外） 非資訊人員	4.75 4.78	0.34 0.39	-0.34	.735
	資訊人員（不含委外） 非資訊人員	4.89 4.78	0.21 0.39	1.70	.095
	女 男	4.78 4.76	0.39 0.34	0.23	.818
	年齡≦ 40 歲 年齡＞ 40 歲	4.67 4.87	0.42 0.31	-2.69	.009**
	大學以下 碩士以上	4.80 4.69	0.38 0.37	1.20	.232
	有教育訓練 無教育訓練	4.80 4.54	0.36 0.41	2.10	.039*
	有資訊教育訓練 無資訊教育訓練	4.86 4.73	0.28 0.44	1.63	.109
電子交換	資訊人員（含委外） 非資訊人員	4.78 4.77	0.36 0.35	0.05	.961
	資訊人員（不含委外） 非資訊人員	4.86 4.77	0.26 0.35	1.06	.292
	女 男	4.77 4.78	0.34 0.36	-0.04	.972
	年齡≦ 40 歲 年齡＞ 40 歲	4.69 4.85	0.38 0.30	-2.19	.031*

構面	組別	平均數	標準差	t 值	顯著性
	大學以下 碩士以上	4.78 4.76	0.33 0.40	0.32	.750
	有教育訓練 無教育訓練	4.80 4.56	0.34 0.37	2.09	.040*
	有資訊教育訓練 無資訊教育訓練	4.86 4.72	0.30 0.38	1.80	.077
實體安全	資訊人員（含委外） 非資訊人員	4.73 4.77	0.33 0.36	-0.45	.651
	資訊人員（不含委外） 非資訊人員	4.80 4.76	0.26 0.36	0.46	.644
	女 男	4.75 4.77	0.35 0.36	-0.17	.868
	年齡≦ 40 歲 年齡＞ 40 歲	4.67 4.84	0.40 0.27	-2.40	.019*
	大學以下 碩士以上	4.78 4.70	0.35 0.35	0.79	.434
	有教育訓練 無教育訓練	4.79 4.48	0.33 0.46	2.06	.066
	有資訊教育訓練 無資訊教育訓練	4.82 4.75	0.29 0.37	1.11	.272
備份機制	資訊人員（含委外） 非資訊人員	4.75 4.68	0.36 0.44	0.69	.488
	資訊人員（不含委外） 非資訊人員	4.78 4.68	0.36 0.45	0.91	.367
	女 男	4.67 4.76	0.45 0.37	-1.02	.313
	年齡≦ 40 歲 年齡＞ 40 歲	4.58 4.80	0.43 0.40	-2.57	.012*
	大學以下 碩士以上	4.69 4.72	0.44 0.36	-0.34	.738
	有教育訓練 無教育訓練	4.72 4.50	0.41 0.50	1.54	.126
	有資訊教育訓練 無資訊教育訓練	4.78 4.64	0.35 0.48	1.50	.141
遵守政策	資訊人員（含委外） 非資訊人員	4.74 4.69	0.39 0.44	0.50	.622
	資訊人員（不含委外） 非資訊人員	4.81 4.69	0.33 0.44	1.28	.209
	女 男	4.68 4.74	0.45 0.38	-0.71	.503

構面	組別	平均數	標準差	t 值	顯著性
	年齡≦ 40 歲 年齡＞ 40 歲	4.59 4.81	0.46 0.36	-2.63	.010*
	大學以下 碩士以上	4.70 4.70	0.44 0.36	0.04	.969
	有教育訓練 無教育訓練	4.72 4.50	0.41 0.53	1.29	.226
	有資訊教育訓練 無資訊教育訓練	4.77 4.67	0.38 0.44	1.17	.245
事件通報	資訊人員（含委外） 非資訊人員	4.91 4.79	0.24 0.38	1.87	.065
	資訊人員（不含委外） 非資訊人員	4.98 4.79	0.76 0.38	4.04	.000*
	女 男	4.80 4.87	0.38 0.31	-0.96	.340
	年齡≦ 40 歲 年齡＞ 40 歲	4.77 4.86	0.37 0.34	-1.25	.216
	大學以下 碩士以上	4.82 4.79	0.35 0.37	0.38	.705
	有教育訓練 無教育訓練	4.84 4.67	0.34 0.47	1.44	.152
	有資訊教育訓練 無資訊教育訓練	4.89 4.77	0.28 0.40	1.60	.115
整體構面	資訊人員（含委外） 非資訊人員	4.73 4.75	0.29 0.34	-0.28	.782
	資訊人員（不含委外） 非資訊人員	4.81 4.75	0.24 0.34	0.94	.354
	女 男	4.74 4.75	0.33 0.31	-0.17	.864
	年齡≦ 40 歲 年齡＞ 40 歲	4.64 4.83	0.35 0.27	-3.06	.003**
	大學以下 碩士以上	4.76 4.68	0.33 0.31	0.97	.333
	有教育訓練 無教育訓練	4.77 4.50	0.31 0.40	2.53	.013*
	有資訊教育訓練 無資訊教育訓練	4.81 4.71	0.26 0.35	1.39	0.17

資料來源：作者彙整

*：p ＜ .05 **：p ＜ .01

表 4　不同職務人員資安意識構面 K-W 檢定與 Welch's ANOVA 差異分析摘要表

構面	組別	平均數	標準差	Levene 檢定	K-W/Robust 檢定	Dunn/Games-Howell 檢定
帳戶管理	1. 文書人員	4.73	0.36	.549	.589	
	2. 檔案人員	4.81	0.30			
	3. 資訊人員	4.82	0.29			
	4. 文檔主管	4.63	0.30			
	5. 委外人員	4.75	0.32			
存取控制	1. 文書人員	4.65	0.41	.181	.072	
	2. 檔案人員	4.81	0.27			
	3. 資訊人員	4.65	0.41			
	4. 文檔主管	4.61	0.43			
	5. 委外人員	4.42	0.36			
系統防護	1. 文書人員	4.68	0.42	.018*	/.128	
	2. 檔案人員	4.84	0.32			
	3. 資訊人員	4.85	0.26			
	4. 文檔主管	4.64	0.45			
	5. 委外人員	4.50	0.38			
行動安全	1. 文書人員	4.69	0.45	.002*	/.039*	未達顯著
	2. 檔案人員	4.92	0.22			
	3. 資訊人員	4.82	0.51			
	4. 文檔主管	4.50	0.41			
	5. 委外人員	4.56	0.42			
上網行為	1. 文書人員	4.68	0.48	.000*	/.011*	2 > 5
	2. 檔案人員	4.92	0.18			
	3. 資訊人員	4.89	0.21			
	4. 文檔主管	4.54	0.41			
	5. 委外人員	4.45	0.37			
電子交換	1. 文書人員	4.68	0.40	.000*	/.091	
	2. 檔案人員	4.89	0.22			
	3. 資訊人員	4.86	0.26			
	4. 文檔主管	4.55	0.44			
	5. 委外人員	4.60	0.49			
實體安全	1. 文書人員	4.67	0.43	.000*	/.154	
	2. 檔案人員	4.76	0.24			
	3. 資訊人員	4.78	0.26			
	4. 文檔主管	4.65	0.39			
	5. 委外人員	4.70	0.44			
備份機制	1. 文書人員	4.60	0.50	.176	.455	
	2. 檔案人員	4.76	0.38			
	3. 資訊人員	4.78	0.36			
	4. 文檔主管	4.65	0.47			
	5. 委外人員	4.70	0.37			
遵守政策	1. 文書人員	4.60	0.49	.001*	/.405	
	2. 檔案人員	4.78	0.37			
	3. 資訊人員	4.81	0.33			
	4. 文檔主管	4.71	0.48			
	5. 委外人員	4.60	0.49			

構面	組別	平均數	標準差	Levene 檢定	K-W/Robust 檢定	Dunn/Games-Howell 檢定
事件通報	1. 文書人員	4.71	0.43	.000*	/.016*	3 > 1
	2. 檔案人員	4.87	0.31			
	3. 資訊人員	4.98	0.08			
	4. 文檔主管	4.75	0.50			
	5. 委外人員	4.75	0.39			
整體構面	1. 文書人員	4.67	0.40	.000*	/.122	
	2. 檔案人員	4.84	0.22			
	3. 資訊人員	4.81	0.24			
	4. 文檔主管	4.64	0.41			
	5. 委外人員	4.56	0.34			

資料來源：作者彙整　　*：p < .05

表 5　認知重要性構面 Pearson 積差相關分析表

構面	帳戶管理	存取控制	系統防護	行動安全	上網行為	電子交換	實體安全	備份機制	遵守政策	事件通報
帳戶管理	1									
存取控制	.691**	1								
系統防護	.731**	.822**	1							
行動安全	.718**	.752**	.742**	1						
上網行為	.657**	.673**	.759**	.703**	1					
電子交換	.646**	.727**	.789**	.709**	.825**	1				
實體安全	.735**	.708**	.756**	.687**	.732**	.824**	1			
備份機制	.721**	.738**	.701**	.674**	.664**	.734**	.770**	1		
遵守政策	.684**	.714**	.723**	.578**	.671**	.696**	.763**	.830**	1	
事件通報	.644**	.545**	.643**	.469**	.612**	.745**	.737**	.679**	.727**	1

資料來源：作者彙整　　**：p < .001

表 6　機關達成程度構面 Pearson 積差相關分析表

構面	帳戶管理	存取控制	系統防護	行動安全	上網行為	電子交換	實體安全	備份機制	遵守政策	事件通報
帳戶管理	1									
存取控制	.660**	1								
系統防護	.540**	.824**	1							
行動安全	.462**	.593**	.583**	1						
上網行為	.498**	.659**	.698**	.715**	1					
電子交換	.451**	.646**	.641**	.548**	.647**	1				
實體安全	.579**	.723**	.706**	.601**	.684**	.648**	1			
備份機制	.471**	.645**	.687**	.551**	.603**	.623**	.615**	1		
遵守政策	.521**	.518**	.587**	.379**	.497**	.452**	.591**	.498**	1	
事件通報	.461**	.514**	.594**	.482**	.550**	.542**	.698**	.620**	.624**	1

資料來源：作者彙整　　**：p < .001

（二）向度相關分析

在「認知重要性」及「機關達成程度」兩個向度之間，均呈現顯著正相關，其中「帳戶管理」呈現低度正相關（$r < 0.4, p < .001$），其餘向度整體構面及各構面之間呈現中度正相關（$r \geq 0.4, p < .001$），詳見表 7。

伍、結論與建議

一、結論

綜合問卷調查結果，歸納以下結論：

（一）整體資安意識偏正向且趨於一致

在「認知重要性」向度，有 76.5％認為非常重要，21.3％認為重要，2.1％認為普通，0.05％認為不重要，0.05％認為非常不重要。在「機關達成程度」向度，有 61.3％認為完全符合，27.1％認為大部分符合，5.3％認為部分符合，0.8％認為大部分不符合，0.2％認為完全不符合，另外有 5.3％表示不清楚。本次調查結果顯示，人員整體資安意識偏正向且趨於一致。

（二）最受重視且最具信心為「事件通報」，最不重視為「存取控制」，最不具信心為「備份機制」

在「認知重要性」向度，以「事件通報」的平均數最高，「存取控制」的平均數最低。在「機關達成程度」向度，亦是「事件通報」的平均數最高，「備份機制」的平均數最低。可知人員最重視且對於機關達成程度最具信心的皆為「事件通報」構面，多數人最不重視「存取控制」構面，而多數人對於機關達成程度最不具信心的是「備份機制」構面。

（三）「認知重要性」向度略高於「機關達成程度」向度，兩向度及構面之間達顯著正相關

在「認知重要性」向度，各構面呈現中度至高度正相關，在「機關達成程度」向度，各構面呈現低度至中度正相關，而「認知重要性」及「機

表 7　認知重要性及機關達成程度構面 Pearson 積差相關分析表

「認知重要性」/「機關達成程度」兩個向度之間構面	相關係數
帳戶管理	.388**
存取控制	.529**
系統防護	.553**
行動安全	.436**
上網行為	.428**
電子交換	.400**
實體安全	.648**
備份機制	.517**
遵守政策	.632**
事件通報	.475**
整體構面	.565**

資料來源：作者彙整　　**：$p < .001$

關達成程度」兩個向度之間呈現低度至中度正相關，代表各構面之間互有關連性，整體而言，「認知重要性」向度的分數均高於「機關達成程度」。

（四）對於機關在資安作業上的符合程度，約有5%不清楚的比例

在「機關達成程度」向度，約有 5%不清楚的比例，其中較不清楚的前 3 名是「備份機制」（10.8%）、「系統防護」（9.9%）及「事件通報」（7.7%），而「備份機制」也是人員最不具信心的構面。若將填答不清楚選項的人員以職務身分區分，則占比依序為文書人員（7.30%）、檔案人員（6.60%）、委外人員（5.41%）、資訊人員（0.55%），顯見資訊人員不清楚的比例最小。

（五）年齡及教育訓練是影響資安意識程度的重要因素

本研究結果顯示，性別及教育程度對於資安意識程度沒有顯著影響。另外，若將基本資料當中的年齡區分為 40 歲以下及超過 40 歲 2 個組別，則僅「事件通報」無顯著差異，其餘構面均達顯著差異，僅，40 歲以下者顯著低於超過 40 歲。當區分為「有接受教育訓練」和「無接受教育訓練」2 個組別時，整體構面達顯著差異，另在「存取控制」、「上網行為」、「電子交換」等 3 個構面亦達顯著差異，有接受教育訓練顯著高於未接受教育訓練，調查結果得知，年齡及教育訓練是影響資安意識程度的重要因素。

（六）在部分構面，資訊人員（不含委外）的資安意識程度相對較高，而文書人員、委外人員的資安意識程度相對較低

資訊人員和非資訊人員（含委外）無顯著差異，但若將委外人員排除，比較資訊人員（不含委外）和非資訊人員，則在「事件通報」，資訊人員（不含委外）比非資訊人員更加重視。當細分為文書人員、檔案人員、資訊人員、文檔主管和委外人員 5 個組別時，同樣地，在「事件通報」，資訊人員（不含委外）顯著高於文書人員。另外在「電子交換」，檔案人員（不含委外）顯著高於委外人員（含辦理資訊或檔案業務）。

本研究調查初衷，是先進行量化方面的初探，期望後續能有更多研究者投入，以發現更多影響資安意識因素。而從整體加以檢視可發現，人員整體資安意識偏正向且趨於一致，而影響資安意識程度的因素，主要聚焦在年齡差異及是否接受教育訓練，且不限於資訊教育訓練。另在性別、教育程度及不同職務身分等因素上，未對資安意識構成重大影響。

二、建議

綜合結論，對於機關的歸納建議如下：

（一）優先加強非資訊人員含「事件通報」等資安教育訓練內容

本研究結果顯示，雖然不同職務人員在整體資安意識無顯著差異，且「事件通報」整體平均數最高，但經分組分析後，發現不同職務人員對於「事件通報」的資安意識程度有所不同，而其中資訊人員顯著高於非資訊人員，尤其高於文書人員。顯示對於資訊人員來說，資安異常事件通報是很重要的，但資安異常事件仍需仰賴非資訊人員遇到是類情況通報，故提升非資訊人員對於「事件通報」的重視程度有其必要。另外在「機關達成程度」向度當中，不清楚機關運作情形由高至低依序是「備份機制」、「系統防護」、「事件通報」、「電子交換」及「遵守政策」等構面，且不清楚的人員以文書人員最多，其次為檔案人員及委外人員。故建議對於非資訊人員，尤其是文檔及委外人員，可優先加強相關資安教育訓練內容。

（二）應確認機關教育訓練覆蓋率，尤其文書人員、委外人員

本研究結果顯示，委外人員有極大比例從事資訊相關業務，資訊人員和非資訊人員（含委外）資安意識程度無顯著差異，但若將委外人員從資訊人員當中排除，則資訊人員（不含委外）在「事件通報」的資安意識高於非資訊人員。而委外人員在「電子交換」的資安意識顯著低於檔案人員；文書人員則在「事件通報」顯著低於資訊人員（不含委外）；同時文書人員在「機關達成程度」向度填答不確定比例最高，也是未接受教育訓練比例最高的一群。這些細微差異，代表在一個機關可能高達 9 成的人員至少受過 1 種以上的教育訓練且整體資安意識偏高時，少部分文書人員、委外人員卻有可能成為潛在威脅對象。應確認機關教育訓練覆蓋率，尤其特別應關注文書人員、委外人員是否有完善教育訓練管道，以預防少數人員成為機關資安防護中的不確定因子。

（三）定期評估機關人員的資安意識

本研究結果顯示，人員整體資安意識偏正向且一致，但不同背景因素的人員，則在個別構面存有部份歧異，這是由於雖然資安意識已具共識，但不同職務人員之間，因所涉及業務不同，必然產生認知上的些微差異，而持續弭平歧異並取得最大共識，是資安議題永遠追求的目標。如果一味針對「已知」的資安內容進行重複無變化的教育訓練，未找出的「未知」部分則易淪於形式。建議機關可參考本研究所擬出資安意識構面題項，定期評估機關人員的資安意識，作為安排機關資訊教育訓練內容的基礎。

（四）由資訊人員協同相關職務人員共同規劃含資安議題之職務訓練

研究結果顯示，教育訓練確實對於資安意識有正面影響，但不限於資訊教育訓練，由於資安作業涉及職務的各個層面，目前一般公務機關都會要求正職人員至少每年須上一定時數的資安教育訓練，但往往內容單一，易在訓練上形成瓶頸，建議可由資訊人員協同相關職務人員共同規劃，將資安議題融入於不同人員的職務訓練當中，可增強人員的理解及接納。例如在文書教育訓練、檔案教育訓練當中，加入資安議題內容及因應實務情境之舉例，可更兼具效益及實用性。

參考文獻

立法院公報處（2018）。*立法院公報，107(52)*，109-113。檢自 https://lis.ly.gov.tw/lgcgi/lypdftxt?xdd!cec9c7c6c7c8cbcecac881cecfc8cfcacdcfcec4cfcecfc6c4cfcececc (Jul. 18, 2023)

行政院（2014）。CNS 27001：資訊技術－安全技術－資訊安全管理系統－要求事項。檢自 https://nicst.ey.gov.tw/Page/7CBD7E79D558D47C/45d1f417-ca0c-4b30-aafa-ffeb9070a257 (Mar. 4, 2022)

行政院國家資通安全會報技術服務中心（2020）。資安趨勢與案例研討。檢自 https://www.motc.gov.tw/uploaddowndoc?file=bussiness/202009041421300.pdf&filedisplay=202009041421300.pdf&flag=doc (Oct. 28, 2021)

吳倩萍（2006）。*政府機關個人資訊安全認知與行為之探討*（未出版之碩士論文）。國立臺北大學，新北市。

國家發展委員會檔案管理局（2019）。文檔系統資訊安全宣導。檢自 https://www.archives.gov.tw/Download_File.ashx?id=17228 (Oct. 28, 2021)

張文熙（2004）。檔案資訊安全之探討。檢自 https://pearl.archives.gov.tw/Publish.aspx?cnid=104425&p=4587 (Oct. 21, 2021)

曹明玉（2006）。*資訊安全認知評量表之研究*（未出版之碩士論文）。淡江大學，新北市。

數位發展部資通安全署（2022a）。資通安全管理法中英對照表。檢自 https://moda.gov.tw/ACS/laws/regulations/522 (Jul. 18, 2023)

數位發展部資通安全署（2022b）。歷史沿革。檢自 https://moda.gov.tw/ACS/aboutus/history/608 (Jul. 18, 2023)

歐芳伶（2008）。*個人資訊安全認知量表設計之研究*（未出版之碩士論文）。樹德科技大學，高雄市。

Drevin, L., Kruger, H. A., & Steyn, T. (2007). Value-focused assessment of ICT security awareness in an academic environment. *Computers & Security, 26(1)*, 36-43. Retrieved from https://doi:10.1016/j.cose.2006.10.006 (Nov. 28, 2021)

Hansche. (2001). Designing a Security Awareness Program: Part 1. *Information Systems Security, 9*(6), 1-9. Retrieved from https://doi.org/10.1201/1086/43298.9.6.20010102/30985.4 (Nov. 28, 2021)

International Organization for Standardization. (2018). *ISO/IEC 27000:Information technology-Security techniques-Information security management systems-Overview and vocabulary* (ISO Standard No. 27000:2018). Retrieved from https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html (Oct. 21, 2021)

Kruger, H. A., & Kearney, W. D. (2008). Consensus ranking-An ICT security awareness case study. *Computers & Security, 27(7)*, 254-259. https://doi.org/10.1016/j.cose.2008.07.001(Nov. 28, 2021)

Raosoft, Inc. (2004). Sample Size Calculator. Retrieved from http://www.raosoft.com/samplesize.html (Mar. 4, 2022)

SNAS. (2021). *Measuring Program Maturity*. Retrieved from https://www.sans.org/security-awareness-training/resources/maturity-model/ (Nov. 28, 2021)

Wilson, M., de Zafra, D. E., Pitcher, S. I., Tressler, J. D., & Ippolito, J. B. (1998). *Information technology security training requirements: A role-and performance-based model(NIST Special Publication 800-16)*. Retrieved from https://apps.dtic.mil/sti/citations/ADA391650 (Nov. 28, 2021)

Wilson, M., & Hash, J. (2003). *Building an Information Technology Security Awareness and Training Program (NIST Special Publication 800-50).* Retrieved from https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-50.pdf (Oct. 28, 2021)