游佳萍、趙慕芬、林美齡 (2023),「台灣公部門與私部門建置資訊安全策略進行變革之重要驅動力」,*資訊管理學報*,第三十卷,第三期,頁 287-314。

台灣公部門與私部門建置資訊安全策略進行變革之重要驅動力

游佳萍
淡江大學資訊管理學系

趙慕芬*
淡江大學企業管理學系

林美齡
淡江大學資訊管理學系

摘要

組織頻頻發生資訊安全事件,會損害競爭力,因此,對資訊安全策略的重視,已經是基本工作。組織強化資安,建置或推動資安策略,實質上是在進行組織變革,促使組織脫離現狀,進行變革的力量,稱為驅動力(driving forces)。而組織進行資安強化時,有哪些重要的驅動力,為本研究探討重點。本研究採用環境掃描工具 PEST 中政治法令、經濟成本、社會文化,以及技術科技四個構面,作為分析架構。深度訪談三位資訊安全顧問,取得 15 個個案的相關資訊,利用內容分析法整理訪談資料,以了解 PEST 四個構面對資訊安全策略,所扮演的推手角色。本研究有幾個發現:第一,社會文化是影響公部門資安策略的首要構面,對於私部門而言,首要構面則是技術科技;第二,公、私部門都重視員工資訊安全認知、顧問的專業資安技術以及資訊安全投資成本等。第三,在技術科技構面中,對公部門、私部門的金融與高科技產業產生影響的指標,較為分歧。最後,從宏觀環境分析的角度來觀察,公私部門面對資訊安全議題時,較為著重的環境因素。本研究結果可以幫助公部門與私部門制定更有效率的資安策略。

關鍵詞: 資訊安全策略、PEST 分析、內容分析、公部門、私部門

* 本文通訊作者。電子郵件信箱:cmf@mail.tku.edu.tw

2022/11/30 投稿;2023/01/18 第一次修訂;2023/03/03 第二次修訂;2023/04/10 第三次修訂;2023/04/11 接受

Yu, C. P., Chao, M. F., & Lin, M.L. (2023). The Major Driving Forces behind Taiwan's Public and Private Sectors' Information Security Strategies, *Journal of Information Management*, 30(3), 287-314.

The Major Driving Forces behind Taiwan's Public and Private Sectors' Information Security Strategies

Chia-Ping Yu
Department of Information Management, Tamkang University

Mu-Fen Chao*
Department of Business Administration, Tamkang University

Mei-Ling Lin
Department of Information Management, Tamkang University

Abstract

This study investigates the need for an information security strategy due to the harm frequent information security incidents cause to a company's competitiveness and the impetus for its transformation. Based on the PEST framework, three information security consultants were interviewed for 15 cases, and content analysis was used to analyze the data. This study found: First, the public and private sectors value information security awareness, consultant skills, and investment costs equally. Second, technology dominates information security strategy in the private sector, while social culture dominates in the public sector. Thirdly, public and private financial and high-tech industry indicators differ among technology components. Finally, the environmental factors are most significant to the public and private sectors when addressing information security issues from a macro perspective. This study provides valuable insights for the public and private sectors to develop effective information security strategies.

Keywords: Information security strategy, PEST analysis, Content analysis, Public sector, Private sector

* Corresponding author. Email: cmf@mail.tku.edu.tw

2022/11/30 received; 2023/01/18 1st revised; 2023/03/03 2nd revised; 2023/04/10 3rd revised; 2023/04/11 accepted

壹、緒論

資訊科技的發展與應用普及，已改變人們生活和工作方式。隨著對資訊技術日益依賴，接踵而至的則是資訊安全(簡稱資安)問題。資安意指維護資訊的保密、完整及可用性(Niemimaa & Niemimaa 2017)。根據趨勢科技研究，2021 年偵測到的全球勒索攻擊數量，台灣位列在全球前十名、亞洲區前五名。2021 年最常遭受勒索攻擊的前三大產業，分別是政府機構、銀行與醫療產業；2022 年則為高科技製造業、政府機構與醫療產業。顯示資安問題，對公部門與私部門都是重要議題。

2019 年為台灣在資安的重要里程碑，政府將資安規定位階提高到法令層級，並將納管對象擴大到特定的非公務機關，對技術面應變事項及控制措施，有更明確的指引(行政院國家資通安全會報 2019、2021)。行政院從 2019 年起，為加強維護中央機關的資安，規定各部會施政計畫在十億元以上者，資安預算佔該部會資訊預算的 5%；一至十億元之間者，資安預算佔比 6%；一億元以下則資安預算佔比 7%。由此可看出，台灣公部門對資安的重視日益提升(行政院國家資通安全會報 2019)。2021 年通過行政院組織調整法案，增設數位發展部，整合電信、資訊、資安、網路、傳播五大領域，統籌基礎建設、環境整備及資源應用，加速促進數位轉型，做好資安維護工作。針對金融業，金管會以非強制性經濟誘因，誘使金融業重視資安(行政院國家資通安全會報 2021)，例如資安做得好的金融業，申請開辦業務時，比較不會被駁回；計算存款保險費率時，可適用較低費率。

自 2018 年，iThome 以臺灣區政府一級機構、大專院校 IT 和 2 千大規模的企業資安主管為對象，進行調查。根據其調查資訊，可一窺台灣公部門與私部門的資安現況。各產業平均資安投資金額彙總於表 1，金融業與其他產業相比，對於資安有較高的需求，也傾向投資更多資源(Tsai & Su 2021)。受到資訊安全法的強制規定，公部門於資安上的投資金額也相當可觀，且呈現逐年上升態勢。

表 1：各產業機構平均資安投資金額(單位：新台幣)

產業別	2018 投資金額	2019 年 投資金額	2020 年 投資金額	2021 年 投資金額
金融	4,613 萬元	3,839 萬元	2,279 萬元	2,207 萬元
政府機關	1,238 萬元	1,040 萬元	1,725 萬元	2,009 萬元
醫療	418 萬元	1,113 萬元	806 萬元	407 萬元
高科技製造	415 萬元	452 萬元	310 萬元	568 萬元

資料來源：本研究整理自 iThome 2018~2022 資安大調查

資安事件極可能嚴重衝擊組織，資安事故的預防成本低於發生危機後的補救成本。資安初始是為確保資訊系統執行時的安全管制，ISO2700 與 ISO20000 與此相關；歐盟提出 GDPR(General Data Protection Regulation 一般資料保護規範)是為在商業交易下，妥善保護消費者資訊(Drozd 2016; Lin, Lin, & Wu 2016)；製造業為確保生產品質與效率，大量使用資訊科技收集生產資料並進行應用，增加資安活動不同的控制方法，ISO90001 針對此部分進行添補(Kinnunen & Siponen 2018)。資安策略是因應業務、法令及監管需求，提供對組織資安的管理方向

（ISO/IEC 2013）。考量外部環境，評估現況和自我能力，制定有效的資安策略，對組織而言十分重要。在資安標準或業界規範上，組織常以檢核表列出資安規則，以符合國際標準，如 ISO/IEC 27000/27001/ 27002, BS7799, NIST-SP800, PCI-DSS 等。這些標準常僅提供一般通用的建議或方針，組織須根據自身需求擬定具體資安規範及實施細則(Kinnunen & Siponen 2018; Niemimaa & Niemimaa 2017)。為了落實資安策略的管控活動，資料保護、加密、網路防護與偵測等相關技術，也紛紛被提出(Rastogi & Trivedi 2016; Vintilă, Gherghina, & Toader 2019)。資安的投資成本研究上，Deane et al. (2019)和 Ryan & Ryan (2006)曾經研究投資成本與資安效果之間的相關性。Kissoon (2020)、Ermicioi & Liu (2021)與 Jerman-Blažič & Tekavčič (2012)計算資安投資的邊際收益來確定投資資安的最佳金額，再行形成決策。此外，資安策略的制定與地區文化、教育水平、資安意識等因素有著密不可分的關係(Babatunde & Adebisi 2012; Stewart & Jürjens 2017; Balozian & Leidner 2017)。

過往研究常聚焦於資安策略內容與施行成本，對於促使組織推行資安策略的外部環境驅動力，鮮有系統性的分析。組織制定有效決策時，需將內部能力或資源，與外部環境相互配合(Johnson, Whittington, & Scholes 2011)。Aguilar (1967)指出高階主管可進行環境掃描(environment scanning) 獲取外部環境資訊，還提出「ETPS」(Economic, Technical, Political & Social)作為掃描環境的工具。經歷 1980 年代學者，包括 Fahey, Narayanan, Morrison, Renfro, Boucher, Mecca & Porter，將此掃描工具重新分類，而有 PEST, PESTLE, STEEPLE 等架構。其中 PEST(Politics, Economic, Society, Technology)是最普及的掃描工具(Rastogi & Trivedi 2016)，提供組織關於外部環境的整體總覽(Babatunde & Adebisi 2012)。

PEST 嘗試縮小外部環境，找出根本問題 (Peng & Nunes 2007)，協助組織識別、評估外部機會與威脅 (Talib et al. 2014)。強化資安時，無論是建立規範、落實資安政策，或投入資源開發資安系統，均為組織變革。改變現狀打破均衡，需要增加脫離現狀的驅動力(driving forces)(Robbins & Judge 2022)，許多驅動力存在於外部環境。組織為強化資安或建置資安策略，而進行環境掃描時，屬於特定情境。爰此，本研究採用 PEST 架構，作為掃描工具，分析當前公私部門所面對的資安環境，以了解公部門與私部門組織進行資安強化時，有哪些重要的驅動力。

現今混合辦公成為常態，雲端運用也愈發普及，都更突顯資安策略對組織的重要性。然而，以往鮮少研究有系統地探討，有哪些環境因素會驅動組織進行強化資安的變革，抑或是不同產業是否會有不同的考量因素。有鑒於這項議題在資安研究中仍屬少見，本研究嘗試以 PEST 環境架構做為分析工具，進行探索性研究，聚焦探討台灣公部門與私部門執行資安策略時偏重考慮的因素，並進行公部門與私部門差異分析，做為組織建置或推動資安策略時，宜納入考量的環境指標。

貳、文獻探討

一、資訊安全

為制定資安策略，組織須建立完整框架，實施資安管理(Chen, Li, & Yin 2021)。Kang & Hovav (2020)將資安策略定義為「決定如何有效部署及應用適當的資安技術和措施，以防禦組織的資訊基礎結構。透過安全機制的機密性、完整性和可用性，以最小成本和效力來抵禦內部和外部威脅，達到最好的成效」。由此可知，資安活動包含人、組織、科技與環境之間的互動，組織倚靠環境生存，但環境也可能是威脅的來源，對組織會造成一定程度的衝擊與影響(Johnson et al. 2011)。

國內外陸續制定資安標準，協助組織因應不同產業特色，推動資安。依時序為：(1)BS10012 為全球第一個個人資訊管理國際標準，於 2009 年由 BSI(British Standards Institution 英國標準協會)制定，旨在保護個資(Lin et al. 2016)，規範個資蒐集、處理、利用等程序。(2)國際標準組織為增強 ISO27001 隱私安全，於 2011 年發布 ISO29100 資安技術-隱私框架標準，協助組織定義、辨識並保護資通系統中的個資，具體說明在資通系統中如何保護個人的身份訊息 (Drozd 2016)。(3)基於雲端網路的日益發達，2014 年發展出第一個公有雲保護個人資訊的國際標準 ISO 27018:保護雲端個人隱私資料，以提升使用者對雲端服務的信任。 (4) 2016 年歐盟特別制定的 GDPR 規範增強個人資料隱私、資料權力，和釐清資料控制者的責任和義務。在歐盟境內設立據點的公司，和對歐盟境內提供產品、服務的境外公司，都必須遵守法規以保障歐盟民眾的個人資料。(5)為了與 GDPR 接軌，2019 年發布 ISO27701 隱私資訊管理為 ISO29100 隱私安全的進階版，對於控制和處理個資者分別列出實務指引與要求。

過往資安實務做法的相關研究，有二大方向(Hartman, Flinn, & Beznosov 2002; Kemp & Kemp 2005; Bulgurcu, Cavusoglu, & Benbasat 2010; Puhakainen & Siponen 2010)：第一是規範面，指的是組織在制度與政策上建立完整的資安政策，以帶動組織整體的資安意識，讓組織成員有可遵循的規範。例如 Kemp & Kemp (2005) 曾提到，資安政策規範是組織實施資安管理最主要的機制，可以提供資訊使用者一套管理標準以保障資訊安全。組織資安策略的提出，應該考慮政府的法令規範，以及產業標準的影響(Bulgurcu et al. 2010; Puhakainen & Siponen 2010)。Hartman et al. (2002) 也認為應該落實資安政策，以實現資安目標。Diamantopoulou, Tsohou, & Karyda (2020) 則指出，資安政策是為了幫助使用者在執行日常工作時，可以確保資訊安全性的一個遵循標準。組織可藉由建置資安策略，而逐步建立組織的資訊安全文化，加強組織人員的資安認知 (Shadbad & Biros 2022) 。

第二則著重於資源配置，係指組織需投入充足經費、人力設備等資源，才能推行資安系統的開發與執行。Hartman et al. (2002) 強調，應該以管理面的思維對資源配置與安全控管進行完整規劃，以求資安效益最佳化。在資安控管與資訊存取便利性之間，取得平衡，使資源利用度達到最大化。例如，對資安的控管應該

包含，組織身處的市場、資本、人力資源、客戶、產品，以及安全控管等層面，進行整體的控管規畫(Puhakainen & Siponen 2010)。而人力資源是組織發展的重要關鍵指標之一，組織必須重新調整人力資源的價值以及人力資源配置(Hartman et al. 2002; Puhakainen & Siponen 2010)。

二、環境掃描與 PEST 架構

組織倚靠環境生存,但環境也可能是威脅的來源,對組織會造成衝擊與影響,因此評估外部環境，有助於組織使用策略抓住機會並避免威脅，也可提高組織獲利能力(Johnson et al. 2011; Babatunde & Adebisi 2012)。企業掃描環境，以更好地理解會對其未來產生衝擊的外部驅力或事件(Jogaratnam & Law 2006)，發展與執行對其成長有益的策略(Chebo & Kute 2019)。Fahey & Christensen (1986)指出，進行環境掃描時，有 2 個方式：outside-in 與 inside-out。outside-in 方式為宏觀觀點(macroperspective)，聚焦於環境中所有的長期趨勢；inside-out 方式是微觀觀點(microperspective)，聚焦於環境中組織需要注意的近期影響。PEST 是較為普及的掃描工具(Rastogi & Trivedi 2016)。

環境分為一般環境與作業環境，一般環境由多個作業環境組成(Bourgeois III 1980)。PEST 將具有影響力的環境構面分為：政治法令、經濟成本、社會文化與技術科技 (Babatunde & Adebisi 2012; Gupta 2013)。會直接影響組織的作業環境，也需列入環境因素，如供應商等利害關係人(Fleisher & Bensoussan 2003; Ho 2014)。Gluckman (2014)分析中國私人航運業時，曾將「許多世界頂級私人飛機製造商試著提高在大陸的知名度，有些與中國製造商進行合作，一起建造飛機」列為經濟環境因素。由此可知，對不同產業組織而言，面對宏觀面的環境因素時，需要依據行業別的微觀因素，採取相對應的策略。本研究探究公私部門的資安驅動力，公私部門的作業環境因素並不相同，採用 PEST 架構進行分析時，會著重於可能對資安變革具有直接影響的一般環境(宏觀)與作業環境因素(微觀)。本研究探討 PEST 的四個構面，分別說明如下：

第一、政府政策對基礎設施具重大影響(Babatunde & Adebisi 2012)，也會影響特定產業的發展(Rastogi & Trivedi 2016)，還會涉及各種形式的政治遊說活動(Ho 2014)，政府在商業經濟環境中具有舉足輕重的地位(Rastogi & Trivedi 2016)。政策因素通常包括勞動法、環境法、租稅政策、貿易限制(Babatunde & Adebisi 2012) 、監管機構制定特定行業法規 (Rastogi & Trivedi 2016)。政治因素常和法令有關(Vintilă et al. 2019)，法令因素通常包括安全標準、勞動法等(Rastogi & Trivedi 2016)。監管機構也會針對特定產業制定規範，組織必須分析環境中的法令因素，制定得宜策略(Bulgurcu et al. 2010)。國內公私部門都必須依照政府所制定的《資通安全管理辦法》，推行並維護組織資安品質。公部門必須遵守《資通安全責任等級分級辦法》與《特定非公務機關資通安全維護計劃實施情形稽核辦法》，公務組織人員必須遵守《公務機關所屬人員資通安全事項獎懲辦法》。而

私部門金融業則必須遵守《資通安全事件通報及因應辦法》與《資通安全情資分享辦法》。

第二、關於資安投資策略與其有效性，過去研究有三大方向：(1)為確認組織在資安的投資成效，Hausken (2006)提出資安投資的四個關鍵績效指標(Key Performance Indicators， KPI)，分別是成長學習、內部流程、客戶指標與財務指標。內部流程的改進會影響客戶滿意度，財務績效將會隨著客戶滿意度提高(Kong, Kim, & Kim 2012)。(2)量化資安風險和選擇最佳資安投資技術。考量資安事件的潛在風險，包含發生可能性及潛在損害後，依照組織可接受的安全程度進行資安投資。Kissoon (2020)與 Ermicioi & Liu (2021)提出經濟模型，計算資安投資邊際收益，以確定資安的最佳投資金額。Ryan & Ryan（2006）將安全性視為風險的反轉，建立藉由預期損失風險來量測安全性收益的定量方法。Jerman-Blažič & Tekavčič (2012)提出綜合模型，衡量每種資安措施的成本與收益，將比較各個措施之後，再行形成決策。(3)以資安發展的階段，提出投資計畫。例如，組織資安政策的聲明與文件撰寫，控制措施的建立等，這些都會衍生顧問諮詢成本(Deane et al. 2019)。進行後續維護時，聘請顧問輔導成本較高，有些組織會以成本較資安健診的方式，幫助組織發現潛在的資安危機 (Ilvonen 2013)。負責健診的技術實驗室，提供例如弱點掃描分析、特定產業合規檢測、網路滲透測試、資安記錄覆核等服務(Deane et al. 2019)。此外，組織在資訊安全上所需要用到的軟硬體設備，也都是在成本上必須考量的一環。

第三、社會文化因素通常包括國家和地區文化、社會生活方式、教育水平、社會流動性(Jobber & Ellis-Chadwick 2016)、健康意識、人口成長率、態度和對安全的重視(Babatunde & Adebisi 2012)等要素。Stewart & Jürjens (2017)將人類活動，視為資安最關鍵因素。除了來自外界的資安風險之外，越來越多組織體認到員工是防範資安問題不可忽視的內部威脅(Balozian & Leidner 2017)。Puhakainen & Siponen (2010)證實，資安意識培訓對員工行為有積極影響；Bulgurcu et al. (2010)指出可以透過獎懲來加強員工遵守資安政策；Da Veiga (2016) 發現員工閱讀並信任資安政策，對資安文化具有積極影響。在建立資安文化上，Sherif, Furnell, & Clarke (2015)提出五個影響變數，即資訊安全行為、資訊安全教育、意識和資訊安全接受度。

第四、技術因素包括與技術有關的所有活動，如研究與開發、自動化、技術創新與突破(Vintilă et al. 2019)、技術基礎設施 (Ho 2014)、許可和專利以及影響外部環境技術變化等要素(Rastogi & Trivedi 2016)。Orehek & Petric (2021)認為能正確操作資訊系統，是項關鍵技術技能。擁有維持資訊系統運作的能力，有助於減少系統故障，提高系統可用性。資安的重要技術包括對資安活動研發新技術、使用自動化科技管理等創新和突破的技術(Rastogi & Trivedi 2016)。PEST 四大構面下，再細分為 22 項指標。

參、研究方法

本研究探討驅動組織進行資安變革之環境因素，以及不同產業是否會有不同的考量因素。組織進行環境掃描或預測時，最精巧的(most sophisticated)方式，是於直線主管之外，另行設置獨立單位(Fahey, King, & Narayanan 1981)。因而，本研究採用 PEST，訪談獨立於組織之外的資安顧問，以獲取完整之外部驅動力。本研究使用質性方法，以深度訪談與內容分析法，收集資料與分析，探討組織建置推動資安策略應考量因素。金融業、政府機關、醫療與高科技業的資安投入金額，高於其他產業(請見表 1)，因此本研究以此 4 類組織為研究範圍。

一、訪談個案

本研究利用深度訪談收集資料，訪談問題根據PEST 架構之四大構面而設計，包含宏觀的一般環境與微觀之產業作業環境。訪談資料以加密方式儲存，以保護個案資訊。本研究共訪談 3 位資安顧問(分別為顧問 A、B 與 C)，皆曾任職於四大會計師事務所。台灣六成左右的上市櫃公司是在此四大事務所輔導下，獲取資安國際認證。資安顧問並非組織內部成員，而是組織外部稽核或監督者，較能客觀陳述組織在推動資安策略時面臨的情境，且可觀察跨組織的資安現象。資安為專業性高的議題，本研究透過資安顧問在現場第一手的客觀觀察，取得資料，除了可以摒除組織內部的主觀意見之外，專業的可信度也因而提高。

此 3 位顧問輔導對象以金融業和政府機關為主，輔導超過 50 個組織。顧問 A 輔導工作年資四年，主要輔導對象為政府單位，曾參與 32 個公家機構的輔導。顧問 B 年資為 3 年，具有輔導台灣前十大銀行之經歷，客戶群以金融業為主。顧問 C 工作年資 12 年，曾輔導 10 個組織從導入、建置到後續完善，輔導對象為政府部門和私人機構各占比一半。三位顧問中，顧問 A 與 B 為管理背景，顧問 C 為技術背景出身，文辭精簡扼要，致使受訪時間較簡短。

受訪顧問針對所輔導個案，進行分享。顧問 A 提供 8 個個案，但有 1 個案主要輔導工作並非資安，故予以剔除；顧問 B 提供 4 個個案皆為有效個案；顧問 C 提供 4 個個案均為有效個案。本研究收集 15 個有效個案，相關資訊列於表 2，其中有 8 個公部門(7 個政府單位，1 個醫療單位)，7 個私部門(4 家金融機構，3 家高科技業)。本研究定義個案證照持有時間 1-5 年為短期、6-10 年為中期、10 年以上為長期。表 2 說明本研究資料來源之個案主，稽核範圍以資訊單位為主要對象。此 15 個個案，公私部門均有且業態分布均勻；持照年限從已長期持有到尚在導入期欲取得認證者，兼而有之；組織規模不論從資本額或是員工數來看，大小錯落有致，充分表現出個案具有充分的代表性。

二、內容分析

本研究參考 Neuendorf (2017)的步驟，進行資料分析。第一步驟，選用 PEST 環境架構，作為資安環境要素之分類基礎；第二步，根據研究設計與 PEST 環境

架構，將編碼類目分為四類。第三步驟，將訪談內容進行資料分析，訪談內容經過斷句，才進一步分析資料。訪談內容為連續性資料，正式編碼時，須分割成許多斷句，一個斷句僅能包括一個意義。斷句的方法，本研究採用釐清文意斷句。依據文獻定義和分類規則(請見附錄 1)，建立資安策略需考量的環境要素類別與指標。分類過程，若有無法對應的項目時，則修正分類指標。所有項目指標，都至少經歷三次比對與討論。經歷第一至第三步驟後，本研究將資安策略環境驅動力以 PEST 架構分為四類：政治法令、經濟成本、社會文化與技術科技。每個構面均在細分指標，共計有 22 個指標，每個指標名稱與定義說明，請見表 4。根據斷句內容的文意，以及是否出現攸關關鍵字，將訪談內容劃分歸類於各個指標。

第四步驟，本研究選用 3 位研究人員作為編碼員，經過訓練，確認信度與效度後，進行正式編碼。3 位編碼員均為資管碩士生，皆修過資安課程或受過相關訓練，其中一位編碼員擁有 ISO27001 資訊安全管理系統主導稽核員的證照。起初先由二位研究員做共同訓練，每次隨機抽取十個連續斷句作為訓練文件，各自編碼後，再與第三方進行比對，尚未達標前，必須重複執行編碼訓練和議論，三人正確率達標後，才能進行獨立編碼。本研究採用百分比一致性(percent agreement)進行結果計算，要求正確率需大於或等於 90%。PEST 環境架構方面經 4 次訓練後，達至 0.9 的信度標準。

在信度效度上，本研究具有編碼者信度(intracoder reliability)、編碼者間信度(intercoder reliability)、表面效度(face validity)與語意效度(semantic validity)。本研究編碼者一致性達到 0.902，具有足夠編碼者信度；PEST 架構因素經過 4 次訓練後，編碼者間的信度達到 0.904；本研究旨在探討環境影響資安策略的要素，使用 PEST 環境架構作為內容分析的基礎，所用工具能衡量研究主題，即具有表面效度(Krippendorff 2018; Neuendorf 2017)；分析文本中有意義的單元僅對應一項編碼，且與其他編碼互斥，具有語意效度(Krippendorff 2018; Neuendorf 2017)。本研究訪談內容經編碼者與受訪者查核，再交由訓練合宜的編碼者進行整理斷句，並將每次編碼討論的細項、定義、關鍵字等，紀錄至編碼書(code book)中，協助釐清編碼者在語意判斷上的準則。

表 2：本研究資料來源個案組織與訪談相關資訊

	編號	資安責任等級/行業別	組織人數(資本額)	認證	受稽單位	證照持有時間	逐字稿時間	顧問(資料來源)
公部門	A01	A	約 130000 人	資訊安全後期階段 ISO27000	資訊單位	長期	約 1 小時	A
	A03[a]	B	約 5000 人	資訊安全後期階段 ISO27001	資訊單位	長期	約 1.5 小時	A
	A05		約 800 人	資訊安全後期階段 ISO27001	資訊單位	短期	約 1 小時	A
	A07		約 700 人	資訊安全後期階段 ISO27001	業務單位	長期	約 30 分鐘	A
	A06		約 700 人	資訊安全後期階段 ISO27001	資訊單位	短期	約 1 小時	A
	A02		約 600 人	資訊安全後期階段 ISO27001	資訊單位	短期	約 2 小時	A
	A04		約 300 人	資訊安全後期階段 ISO27001	資訊單位	短期	約 1 小時	A
	A08	C	700~600 人	資訊安全前期階段 ISO 9001 、ISO 17025	資訊單位	無	約 30 分鐘	C
私部門	B01	金融	約 10000 人(750 億)	資訊安全後期階段 ISO27001	資安部門	中期	約 1 小時	B
	B02		約 20000 人(1000 億)	資訊安全後期階段 ISO27001	資安部門	中期	約 1 小時	B
	B03		約 1500 人(300 億)	資訊安全後期階段 BS10012	業務單位	短期	約 1.5 小時	B
	B04		約 2000 人(570 億)	資訊安全後期階段 BS10012	全組織	短期	約 1.5 小時	B
	B05	高科技製造	約 200 人(4.5 億)	資訊安全前期階段	資訊單位	無	約 30 分鐘	C
	B06		約 300 人(6.9 億)	資訊安全前期階段 ISO 9001、13485、14001、45001	系統整合業務部	無	約 30 分鐘	C
	B07		約 300 人(1.5 億)	資訊安全後期階段 ISO9001,+ISO27001	資訊單位、客服中心	短期	約 1.5 小時	C

註 a:醫療單位

肆、資料分析與結果

本研究針對推動資安策略，探究環境中的驅動因素，採 PEST 為環境掃描工具，掃描範圍包含宏觀的一般環境與微觀之產業作業環境。宏觀觀點聚焦於環境中長期趨勢，微觀關注環境中組織需注意的近期影響(Fahey & Christensen 1986)。本研究收集 15 個有效個案組織資料，以 7 個政府單位與 1 個醫療機構，共計 8 個，作為公部門代表；4 個金融與 3 個高科技業，共計 7 個企業，代表私部門。

一、公私部門資安策略的宏觀與微觀環境指標

公部門訪談內容共有 954 個斷句，刪除 216 個與環境無關者，738 個屬於本研究範疇。私部門資料有 701 個斷句，刪去 141 個後保留 560 個。訪談內容經斷句、編碼、比對、分類後，依 PEST 架構分四大構面，於政治法令環境再細分為 4 個指標，經濟成本細分為 4 個指標，社會文化細分為 7，技術科技細分為 7。

表 3：公私部門資安策略宏觀/微觀環境指標資料彙總

Type	PEST	公部門	私部門
宏觀	P01 國內政策與法規	6.91%	8.21%
	P02 國際認證	7.45%	5.71%
	P03 投標契約書內容與規定	3.25%	2.68%
	E04 市場趨勢	0.54%	2.14%
	S01 產業慣例	6.10%	6.79%
	S02 產業資安責任	8.13%	4.29%
	S07 重大事件	1.36%	2.14%
	T01 電腦系統結構	0.81%	1.07%
	T03 駭客攻擊手法與資安事故因應	5.83%	2.32%
	T04 基礎設施	3.66%	2.14%
微觀	P04 獎懲制度	0.27%	0.00%
	E01 資訊安全投資成本	7.72%	7.68%
	E02 資訊安全準備金	1.36%	0.71%
	E03 績效	1.08%	2.86%
	S03 人力資源	1.36%	2.14%
	S04 資訊安全認知與態度	15.85%	12.68%
	S05 溝通與討論	2.57%	2.14%
	S06 教育訓練	4.07%	4.82%
	T02 顧問專業資安輔導	12.20%	20.18%
	T05 委外廠商的控管	4.07%	2.50%
	T06 技術人員與專業技術能力	2.57%	2.86%
	T07 系統技術檢測與演練	2.85%	3.93%

政治法令 4 個指標中，3 個指標屬於長期趨勢的宏觀環境指標：P01 國內政策與法規、P02 國際認證、P03 投標契約書內容與規定，僅有 P04 獎懲制度，此一指標為需要注意的近期影響，屬於微觀指標。公部門 738 斷句中，51 個與國內政策與法規攸關，占比 6.91%，為政治法令中佔比最高者，故命名為 P01。經濟成本環境 4 個指標中，僅有市場趨勢屬於宏觀，在公部門中佔比最低，僅 0.54%，而將此指標編號為 E04；微觀指標有 E01 資訊安全投資成本、E02 資訊安全準備金與 E03 績效。社會文化 7 個指標，3 個屬於宏觀，4 個是微觀。技術科技構面共有 7 個指標，3 個屬於宏觀，微觀指標有 4 個。相關資訊，請見表 3。政治法令構面，4 個中有 3 個屬於宏觀指標；經濟成本構面 4 個指標，3 個屬於微觀指標；社會文化與技術科技構面，指標分布較為平均。本研究 PEST 四個構面，22 個指標中，屬於宏觀者計有 10 個，微觀指標共有 12 個。

在建置或推動資安策略議題上，公部門 738 個斷句內容，有 45.46%與宏觀指標攸關，私部門 560 個斷句中，屬於宏觀者占比 39.46%。公、私部門斷句資料中，屬於微觀指標者，百分比分別為 54.54%與 60.54%。

二、公私部門資安策略的環境指標分析

公部門 738 個斷句中，132 個屬於政治法令(占比 17.89%)，出現最多為「國際認證」，「國內政策與法規」次之；79 個屬於經濟成本(10.70%)，出現最多的與「資訊安全投資成本」相關；291 個屬於社會文化(39.43%)，出現最多的與「資訊安全認知與態度」相關，「產業資安責任」次之；236 個屬於技術科技(31.98%)，出現最多的與「顧問專業資安輔導」相關，「駭客攻擊手法與資安事故因應」次之。私部門的資料分析結果，共有 560 個攸關斷句， 93 個屬於政治法令(16.61%)，出現最多的為「國內政策與法規」，「國際認證」次之；75 個為經濟成本(13.39%)，出現最多的與「資安投資成本」相關，「績效」次之；196 個歸類為社會文化(35.00%)，出現最多的為「資安認知與態度」，「產業慣例」次之；196 個屬於技術科技(35.00%)，出現最多的與「顧問專業資安輔導」相關，「系統技術檢測與演練」次之。相關資訊，請見表 4。

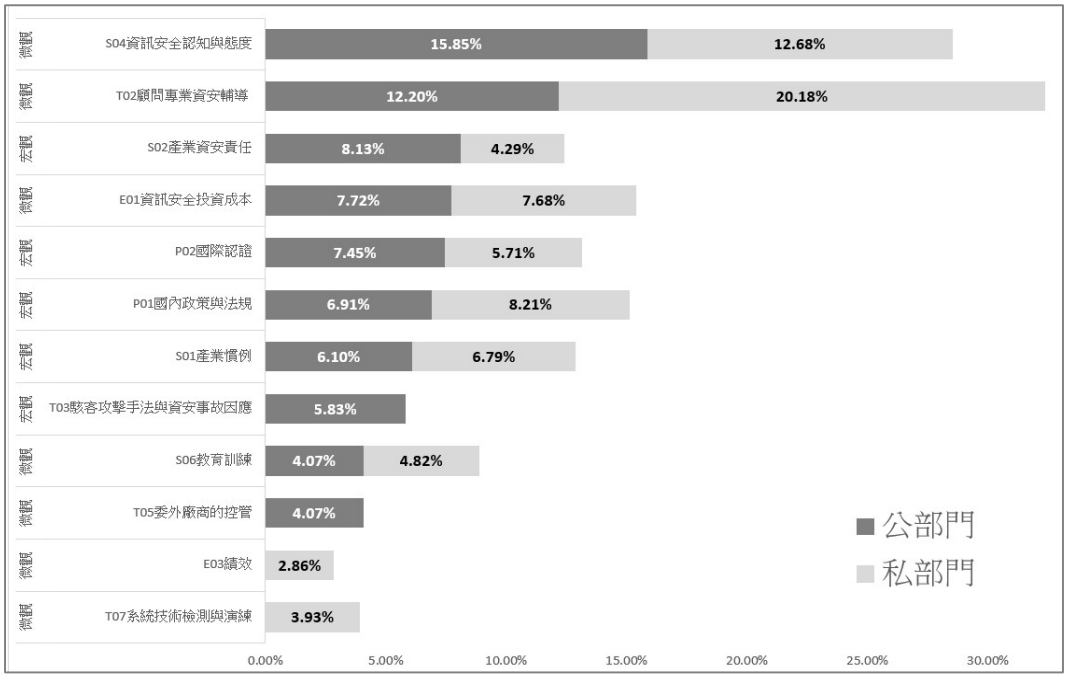
公部門在資安策略中，考量的前十大環境指標(詳見圖 1)分別為：資訊安全認知與態度、顧問專業資安輔導、產業資安責任、資訊安全投資成本、國際認證、國內政策與法規、產業慣例、駭客攻擊手法與資安事故因應、委外廠商的控管、教育訓練。其中，委外廠商的控管與教育訓練此二指標，並列為第 9。此十項指標，有四項來自社會文化環境：資訊安全認知與態度、產業資安責任、產業慣例、教育訓練，分別名列第 1、3、7 與 9；三項來自技術科技環境：顧問專業資安輔導、駭客攻擊手法與資安事故因應、委外廠商的控管，分別名列第 2、8、9；二項來自政治法令環境：國際認證、國內政策與法規，分別名列第 5 與 6；僅有一項來自經濟成本因素，資訊安全投資成本，排名第 4。綜而觀之，在外界顧問觀察中，公部門推動資安策略時，主要的環境驅動力，來自社會文化，技術科技次之，政治法令第三，經濟成本則是最後。

私部門在資安策略中，考量的前十大環境指標(詳見圖 1)分別為：顧問專業資安輔導、資訊安全認知與態度、國內政策法規、資訊安全投資成本、產業慣例、國際認證、教育訓練、產業資安責任、系統技術檢測與演練、績效以及技術人員的專業能力。其中有二項指標並列第 10：績效、技術人員的專業能力。此 11 項指標，有四項來自社會文化環境：資訊安全認知與態度、產業慣例、教育訓練、產業資安責任，分別名列第 2、5、7 與 8；三項來自技術科技環境：顧問專業資安輔導、系統技術檢測與演練、技術人員的專業能力，分別名列第 1、9、10；二項來自政治法令環境：國內政策法規、國際認證，分別名列第 3 與 6；二項來自經濟成本因素：資訊安全投資成本、績效，排名分別為第 4 與 10。綜而觀之，在外界顧問觀察中，私部門資安策略最要考量的環境因素，為社會文化，技術科技次之，政治法令第三，經濟成本則是最後。

表 4：公私部門資安策略環境指標相關資料彙總

指標	分析數量		PEST 編碼百分比	編碼細項百分比	
	公部門	私部門		公部門	私部門
*P01 國內政策與法規**	51	46	政治法令 公部門: 17.89% 私部門:16.61%	6.91%	8.21%
*P02 國際認證**	55	32		7.45%	5.71%
*P03 投標契約書內容與規定**	24	15		3.25%	2.68%
P04 獎懲制度	2	0		0.27%	0.00%
E01 資訊安全投資成本	57	43	經濟成本 公部門: 10.70% 私部門:13.39%	7.72%	7.68%
E02 資訊安全準備金	10	4		1.36%	0.71%
E03 績效	8	16		1.08%	2.86%
*E04 市場趨勢**	4	12		0.54%	2.14%
*S01 產業慣例**	45	38	社會文化 公部門: 39.43% 私部門:35.00%	6.10%	6.79%
*S02 產業資安責任**	60	24		8.13%	4.29%
S03 人力資源	10	12		1.36%	2.14%
S04 資訊安全認知與態度	117	71		15.85%	12.68%
S05 溝通與討論	19	12		2.57%	2.14%
S06 教育訓練	30	27		4.07%	4.82%
*S07 重大事件**	10	12		1.36%	2.14%
*T01 電腦系統結構**	6	6	技術科技 公部門: 31.98% 私部門:35.00%	0.81%	1.07%
T02 顧問專業資安輔導	90	113		12.20%	20.18%
*T03 駭客攻擊手法與資安事故因應**	43	13		5.83%	2.32%
*T04 基礎設施**	27	12		3.66%	2.14%
T05 委外廠商的控管	30	14		4.07%	2.50%
T06 技術人員與專業技術能力	19	16		2.57%	2.86%
T07 系統技術檢測與演練	21	22		2.85%	3.93%

*宏觀指標 資料來源:本研究



資料來源:本研究

圖 1：影響公、私部門資訊安全策略的前十大指標

組織建置推動資安策略時，過往研究在 PEST 環境架構下，共指出有 22 項指標，會對其產生影響。而本研究經過梳理後發現，台灣公私部門建置推動資安策略時，會重視的環境指標，縮減為 15 項。相關資訊，請見表 5。表中整理過往相關文獻，界定 PEST 四大構面下，會影響資安策略的環境指標及定義(相關說明請見附錄 1)。在 22 項指標中，發現有 7 項指標，重要性較低。

政治法令構面刪除了 2 項指標：「投標契約書內容與規定」與「獎懲制度」。對照訪談相關內容，發現研究個案都已處於資安策略的建置或推動階段，而非規畫階段，而使投標契約書內容與規定，顯得較不重要。公私部門多會遵循國內政策與法規，內部人員也多會遵守組織資安規定，獎懲制度已經融入日常資安管控活動中，而非影響策略建置或推動的重要指標。經濟成本構面下，「資訊安全準備金」與「市場趨勢」，此 2 項指標，也被刪除。由於公部門的預算制度，以及金融業與高科技業長期穩定地對資安投入預算，因此經濟成本上，較為重視資訊安全投資成本與績效。對資安進行收支計算的資訊安全準備金，則因無法估算資安投資收益而刪除。社會文化這一構面，研究個案對各項指標的重視程度，會隨著組織類型而有所不同。例如，「產業慣例」與「教育訓練」是公部門的重要指標，私部門較看重「溝通與討論」。在社會文化構面下，刪除「人力資源」此項指標。Hartman et al. (2002) 以及 Puhakainen & Siponen (2010) 雖然指出組織必須重新調整人力資源配置，以進行組織發展。然而，根據訪談資訊透漏，台灣公私部門在建置推動資安策略時，常仰賴外界專業顧問與現有人力，較不傾向調整組織結構或重新配置人力資源。技術科技構面中，刪除了 2 項指標：「電腦系統結構」與「基礎設施」，顯示公私部門對於外部環境中，現行的資安軟硬體介面結構與功能，以及基礎設備的相關變化，重視度不高。

表 5：資安研究文獻與 PEST 環境架構相關者

構面	指標與定義	組織		出處
		公部門	私部門	
政治法令 (Politics)	國內政策與法規*：中央政府單位為積極推動國家資通安全政策，加速建構國家資通安全環境以保障國家安全、維護社會公共利益所制定的政策與規範。	v	v	Bulgurcu et al. 2010; Babatunde & Adebisi 2012; Rastogi & Trivedi 2016; Vintilă et al. 2019; Diamantopoulou et al. 2020; Kang & Hovav 2020
	國際認證*：國際標準化組織、英國標準協會等具公信力團體所制定的資訊安全相關國際標準認證。	v		
	投標契約書內容與規定*：投標單位按照組織招標書的條件和要求。			
	獎懲制度：政府對資安管控的罰則或獎勵制度。			
經濟成本 (economic)	資訊安全投資成本：預期為組織可能帶來的利益與好處，所投入於資訊安全項目上的資金花費。	v	v	Jerman-Blažič & Tekavčič 2012; Kong et al. 2012; Ilvonen 2013; Rastogi & Trivedi 2016; Deane et al. 2019; Kissoon 2020; Ermicioi & Liu 2021; Jouini, Raba, & Khedri 2021
	資訊安全準備金：針對一段時期所需的收入和支出做出預測和規劃。			
	績效：一定時期內的工作行為、方式、結果及其產生的客觀影響。	v	v	
	市場趨勢*：對一個或多個有確定的意義市場，所做的持續反映。			
社會文化 (society)	產業慣例*：產業中多數組織共同的價值觀、處事方式和信念等內化認同表現出來的行為方式。	v		葉桂珍、張榮庭 2006; Bulgurcu et al. 2010; Puhakainen & Siponen 2010； Babatunde & Adebisi 2012; Sherif et al. 2015;
	產業資安責任*：聚焦的資安重點會因產業別，而有所不同。	v	v	
	人力資源：資安推動所需之專業人力、人員流動、人才培訓或人力短缺等。			

	資訊安全認知與態度：不同產業的資安問題意識。	v	v	Da Veiga 2016; Rastogi & Trivedi 2016; Jobber & Ellis-Chadwick 2016; Babatunde, Stewart, & Jürjens 2017; Balozian & Leidner 2017; Yu, Chu, & Lu 2018; 陳志誠等人 2018
	溝通與討論：針對問題的提出、說明或解決辦法與他人或團體建立互動式的討論方式。例如：資安事件通報平台、資安大會…。		v	
	教育訓練：有經驗者以系統化的方式引導學習者了解資安，以達到執行資安活動的目標。	v		
	重大事件*：對組織將產生嚴重傷害或影響的資安相關事件。	v	v	
技術科技 (technology)	電腦系統結構*：能在機器上正確運行所應具有的軟體和硬體介面結構和功能。			黃士銘、張碩毅、蘇耿弘 2006; Ho 2014; Rastogi & Trivedi 2016; Vintilă et al. 2019; Orehek & Petric 2021; Shadbad & Biros 2022
	顧問專業資安輔導：顧問協助組織導入資安的國際標準的能力。	v	v	
	駭客攻擊手法與資安事故因應*：資安事件發生後，組織針對資安事故做出的處理和應對。		v	
	基礎設施*：資訊服務運作之重要基礎設備。			
	委外廠商的控管：外包程序的控制與管理措施，包括文件紀錄、制定標準作業程序、擬定測試計畫等。		v	
	技術人員的專業能力：資安技術人員對機器、硬體、系統運用的技巧。	v	v	
	系統技術檢測與演練：找出系統漏洞，針對弱點加以修正與改進的相關技術。或預演攻擊事件發生時，測試其應對策略能否進行有效的防技術工具。	v	v	

*宏觀指標 「V」表示該指標排名在十名之內 資料來源:本研究

三、再探私部門資安策略環境指標

本研究中的私部門，包含金融業與高科技業。這二個產業對資安投資的金額與時程差異頗大，相關資訊請見表 2。金融業投入較早，金額遠大於高科技業，雖然金融業近年資安投資金額已逐漸下降，但絕對金額仍高於高科技業。根據趨勢科技研究，2021 年偵測到最常遭受勒索攻擊的產業，金融名列第 2，但 2022 年，已經從前 3 名中除名；反觀原本一直未進入前 3 名的高科技業，2022 年甫一入榜，即位居遭受勒索攻擊產業的第 1 名。本研究有效個案中，共有 7 個私部門組織。4 個為金融業，均處於資訊安全後期階段；3 個為高科技業，都還在資訊安全前期階段。因而將本研究之私部門，劃分為金融與高科技業，進行探究。私部門的資料分析結果顯示，屬於 PEST 環境的斷句共有 560 個，金融業有 369 個，高科技業有 191 個。

金融業 369 個斷句中，60 個屬於政治法令(占比 16.26%)，出現最多的為「國內政策與法規」,「國際認證」次之；51 個屬於經濟成本(占比 13.82%)，出現最多的與「資安投資成本」相關,「績效」次之；140 個屬於社會文化(占比 37.94%)，出現最多的為「資安認知與態度」,「產業慣例」次之；118 個屬於技術科技(占比 31.98%)，出現最多的與「顧問專業資安輔導」相關,「技術人員與專業技術能力」次之。高科技業 191 個中，33 個屬於政治法令(占比 17.28%)，出現最多的為「國內政策與法規」,「國際認證」次之；24 個屬於經濟成本(占比 12.57%)，出現最多的與「資安投資成本」相關,「市場趨勢」次之；56 個屬於社會文化(占比 29.32%)，出現最多的為「資安認知與態度」,「產業慣例」次之；78 個屬於技術科技(占比 40.84%)，出現最多的與「顧問專業資安輔導」相關,「技術人員與專業技術能力」次之。高科技業中技術科技構面指標的重要性，高於金融業；社會文化構面指標的重要性，則低於金融業。此二產業的前十大指標，整理於圖 2 中。

專業顧問資安輔導、資訊安全認知與態度，在金融或是高科技業中，都是同列第 1 與第 2 名(請見圖 2)。資安投資成本、產業慣例、國內政策與法規、國際認證，以及教育訓練，在金融業重要性分屬第 3 到 7。上述 5 項指標，在高科技業的重要性，也擠身進入前十大，位居分別為 5、8、3、6、10。

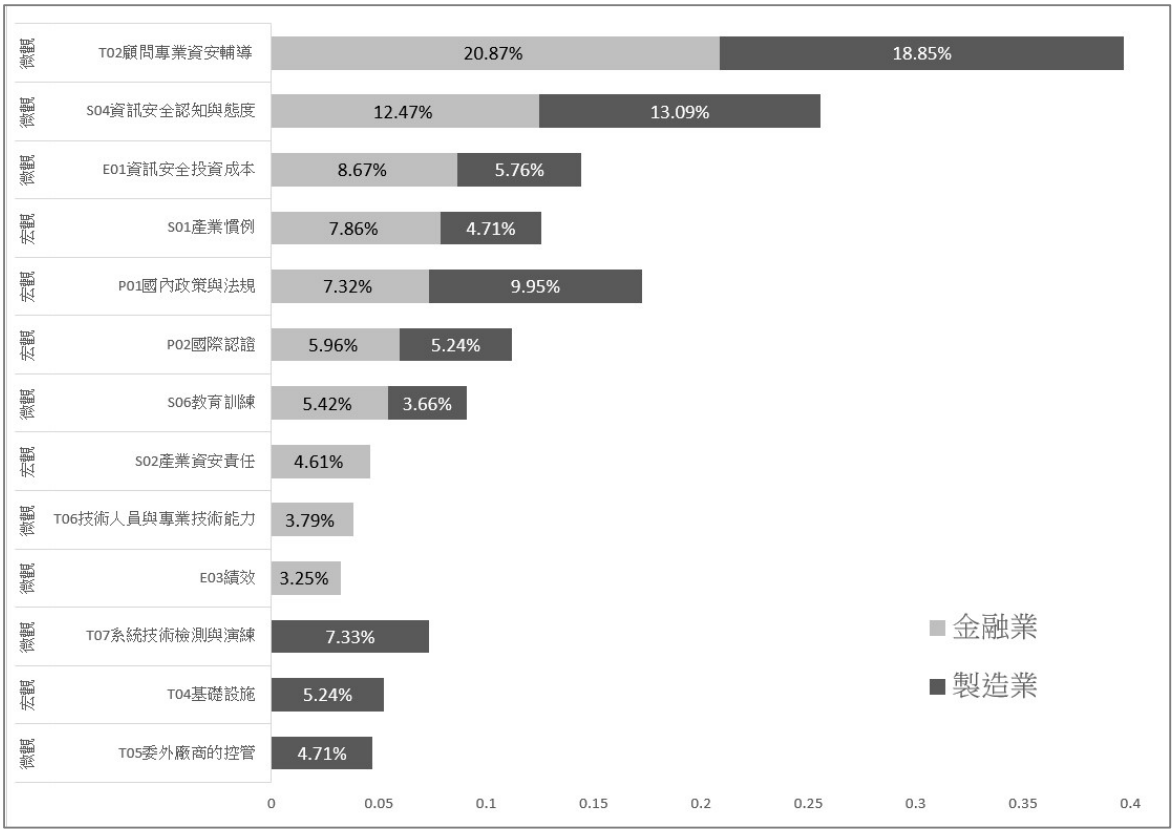
金融業排名末 3 名指標，分別為產業資安責任、技術人員與專業技術能力，以及績效。而此 3 項指標，並不受高科技業重視。產業資安責任，意指聚焦的資安重點會因產業別，而有所不同。金融業比起其他產業，除了一般資安議題之外，更重視客戶的隱私保護，因而這項指標會排名較高。在技術人員與專業技術能力這項指標中，比對深度訪談中資訊之後，發現有些金融機構願意設置資安單位，專責資安事務，但招聘人員時，往往因工作規範與應徵者條件無法吻合，致使不易晉用新人，人手不足。而對資安已然投入許多資金的金融業而言，對績效指標的重視，也不難理解。

高科技業者重視，但未進入金融業前十大指標者，共有 3 項：系統技術檢視與演練、基礎設施，以及委外廠商的控管。此 3 項指標在高科技業中的重要性，排名分別為第 4、6、8。由於本研究中的高科技業正好均處於資訊安全前期階段，而金融業都

位居資訊安全後期階段。因而，雖然觀察到高科技業特別重視這 3 項指標，但是對於差異起因，是來自產業別的不同，或是資訊安全階段不同而引發，則無法有定論。

四、公私部門資安策略環境指標綜論

綜觀公私部門此 3 類型組織，排名前面的指標，有其共同性。像是顧問專業資安輔導、資訊安全認知與態度、資訊安全投資成本、國內政策與法規、國際認證，上述 5 項，無論在那一類型組織，都受到高度重視。產業慣例、教育訓練此 2 項，雖也普遍受到重視，但是重要度較低。以上現象分述於後。



資料來源:本研究

圖 2：影響金融業與高科技業資訊安全策略的前十大指標

公部門中較不同於其他組織的指標有 3 項：產業資安責任、駭客攻擊手法與資安事故因應，以及委外廠商的控管，排名分別為 3、8、9。梳理訪談資料後發現，由於公部門必須遵守《資安管理辦法》，並對應《公務機關所屬人員資通安全事項獎懲辦法》，因而比私部門更重視產業資安責任歸屬與釐清。其次，是在發生重大駭客攻擊和資安事件時，公部門成員除了必須究責之外，此攻擊或事件還會成為其他公部門組織單位重要的資安管理參考。因此，公部門對「駭客攻擊手法與資安事故因應」，重視度較高。最後，在委外管理的部分，由於公部門的資安系統涉及許多外包工作，從發包、建置、驗證、維護等，各個資訊系統發展階段，都涵蓋許多資安的管控。除此之外，舊有資訊系統的限制，也會是資安外包工作的一大疑慮。故「委外廠商的控管」此一指標，對於公部門而言，會相當重要。

第二、金融業較不同的指標為：產業資安責任、技術人員與專業技術能力、績效，排名分別為 8、9、10。相較於其他類型組織，金融業必須遵守《資通安全事件通報及因應辦法》，在法規上有十分明確的管控，因此，金融業在產業資安責任的重視，遠遠超過高科技製造業。除此之外，為了維護客戶資料與服務流程安全，金融業不能只依靠科技，還須培訓專業人才和提升資安意識。然而，專業人才招募、培育不易且流動率高，因此「技術人員與專業技術能力」成為金融業重視的指標之一。最後，相較於公部門與製造業，金融業多年投入資安推動且資金龐大，因此更專注於長期績效的稽核與檢驗，以作為日後長期改善資安策略的重要參考依據。

高科技業者與其他類型組織不同的指標，共有 3 項：系統技術檢視與演練、基礎設施，以及委外廠商的控管，排名分別為第 4、6、8。相較於金融以及公部門，高科技業為了維護製造品質，較為注重實際製造活動中，每個環節系統技術之檢視與演練，以確保採用的資安技術或系統，能隨時監測資安品質並降低資安風險。再者，在製造的過程中，高科技製造業的許多硬體設備，必須仰賴穩定且安全的基礎設施，才能讓製造設備穩定且安全的運作。因此，基礎設施此一指標，成為製造業建置或推動資安策略時的重要環境指標。最後，高科技製造業會面對許多的委外單位，例如原物料供應商廠商、外包廠商、下游協力廠商等，在建置資安系統時，也需要將委外廠商的控管，考量在內 。

五、公私部門建置資安策略之重要環境驅動力指標

資訊安全認知與態度，是指不同產業存在不同的資安問題意識。此一指標與外界顧問進行資安輔導時的專業建議，無論對公部門或私部門而言，都是數一數二的重要(請見圖 1)。尤其是資訊安全認知與態度的重要性，本研究的結果與 iThome 自 2018 年以來進行調查所顯示之情形，相互吻合。

資訊安全投資成本這項指標，在公部門或私部門的影響力，均名列第 4，顯現成本效益分析，對公或私部門而言，仍是重要考量。國際認證雖然在公、私部門都列名第 6，但是在公部門受到的重視度(7.45%)，比私部門(5.71%)高。公部門比私部門更注重國際認證，可能是公部門所受到的國內政策與法規環境限制所致。根據資安法規定，屬於 A 或 B 等級的公部門，必須通過 ISO27001 國際認證。

公部門與私部門在建置或推動資安策略時，公部門經常仰賴外包廠商建置、維護、處理漏洞與更新等事宜。根據法令規定公部門將資安事務委外時，外部廠商必須已取得 ISO27001 國際認證，才符合委外資格。

在公部門中，產業資安責任、駭客攻擊手法與資安事故因應，以及委外廠商的控管，此 3 項指標與私部門的重要性，分歧較大。公部門對上述 3 項指標的重視度，高於私部門。這是因為公部門資安系統不僅經常是外包建置，而且若出現資安事故，只要不是公部門員工操作不當(例如開啟不明郵件、亂插 USB、隨便瀏覽奇怪網站等)，就不會有內部人員被究責。資安事故的責任，由外包廠商承擔。因此公部門員工會遵守規定，謹慎操作。但是對資安系統老舊需要更新、可能存在漏洞等問題，關心度較低。爬梳深度訪談內容，有多位受訪者提及，公部門中有些主管雖然意識到有資安問

題，但抱持較消極的處理態度，只要還未爆發或還未上媒體，就不會處理。公部門選用顧問公司時，會先公開招標，再進行議價。尋找合乎法令規定、配合度佳且能承擔責任的外包廠商，對公部門而言，重要性較高。若出現較重大資安事故，除究責原來外包廠商之外，仍利用外包解決駭客攻擊或資安事故。

顧問專業資安輔導，為私部門重視度最高的指標；國內政策與法規，名列第 3；產業慣例，則名列第 5；系統技術檢測與演練與技術人員，以及專業技術能力，分列第 9 與第 10。梳理訪談資訊後，發覺此 5 者有關連性存在。私部門在建置或推動資安策略時，會仰賴有輔導同業經驗的資安顧問，是有 4 個主要原因：(1)國內政策法規上細節不明確，需要有經驗的顧問協助組織訂定明確的內部規範與作業流程；(2)私部門相對重視稽核，會試圖找出資安缺陷並設法解決問題。私部門較願意尋找外部助力，透過第三方專業實驗室的儀器設備，檢測系統潛在的資安漏洞與風險，發現問題後會先進行弱點修補，再進行第二次複掃；(3)組織重視法遵，特別是金融機構的法務部門都會謹慎確認組織內部規範與流程，是否符合法規；(4)金融機構於個資隱私規範上，重視的為歐盟之 GDPR。GDPR 不屬於驗證公司(BSI、SGS)的範疇，需仰賴專業顧問協助審閱，公司有無違反 GDPR 條款要求。

雖較不受公部門重視，但仍進入私部門前十大的指標，共有 3 項：系統技術檢視與演練、績效，以及技術人員的專業技術能力。比對深度訪談資訊後，發現私部門，尤其是金融業，意識資安事故可能會讓組織付出高昂代價，所以在系統技術檢視與演練上，對於找出漏洞、發掘弱點並改進之意識程度高。而績效考量下，難以事先計算投資報酬率的資安，不易吸引私部門率先投入資金，往往需要同業擔任領頭羊。私部門雖然願意增設或擴編資安單位，往往囿於不易招聘到適合人員，而使技術人員的專業技術能力，成為私部門的第 10 名指標。編制較小組織，例如銀行分行，經常僅有一位人員負責資安，除了要管理關鍵基礎設施與網路等工作，還要完成資安相關事務，且經常無職務代理人，資安人力編制顯得吃緊。

伍、結論

過往研究探討組織資安議題之外部環境時，常是分別就政治法令、經濟成本、社會文化或技術科技等單一構面，探討其對組織的影響。鮮少研究進行系統全面探討，驅動組織進行強化資安的環境因素，以及不同類型組織是否會有不同因素，因而本研究以 PEST 環境架構做為分析工具，進行探索性研究。

首先，環境指標中，關注於一般環境的中長期趨勢者，為宏觀指標；聚焦作業環境，組織需要注意的近期影響，則是微觀指標。研究發現，在建置或推動資安策略時，公私部門較常談論的是微觀指標，顯示建置或推動資安策略時，毋論公私部門皆較重視作業環境。對於宏觀指標的重視，公部門高於私部門，揭示公部門對於一般環境中的長期趨勢，較為關切。

其次，綜合觀察各個構面下，公私部門不同類型組織，在建置推動資安策略時，所重視的環境指標。研究發現影響公部門資安策略的環境指標來源，首要為社會文化，技術科技次之，政治法令第三，經濟成本為最後。影響私部門資安策略的環境指

標重要性，技術科技與社會文化並列第一，政治法令與經濟成本，分列第三與第四。這四大構面對資安策略的影響，由研究資料可以歸納如下：

第一、政治法令方面，公私部門建置推動資安策略的主要受兩個宏觀指標影響，分別為國內政策與法規，以及國際認證。公部門考量機關的業務、系統、層級等，將資安責任等級分為 A 至 E 五等，訂定各自資安責任。行政院資安處要求，資安程度等級為 A 或 B 的機關，必須導入並通過 ISO27001 驗證。台灣公部門較特別的機制為資安情資分享，藉由分享情資改善稽核報告，增強各機關對資安的預警能力。當機關首長認為資安重要性極高，則會透過大型會議展開推動工作。當組織變革由高階主管展現承諾，由上而下推動時，會對組織資安策略的發展，具有重大實質幫助。目前國內公部門管理階層會依據資安標準要求行事，成員對外界資安顧問的專業資安輔導，配合度高。為了使得公部門持續發展資安，相關單位宜善用資安管理政策與辦法，引導公部門人員積極參與資安的工作，培養組織成員資安素養，進而取得高品質的資訊安全成效。私部門則因產業特性不同，受到不同資訊安全、隱私安全、網路安全，以及產業標準的影響。例如，國際標準機構特別為銀行、保險公司、信用卡公司制定 ISO27015，協助金融服務組織內部的資安管理。

第二、經濟成本構面中，公、私部門都十分重視「資訊安全投資成本」這個微觀指標。而在資安上已經多年連續投注高額資金的金融業，會較特別在意績效。然而，資安的投資不易進行成本效益分析，建置或實施資安系統，所需資源，可以量化且計算得到。然而，推動資安所帶來的效益，則不易得知。只要沒有發生資安事故，就無法知道損失金額，況且有些損失，例如商譽受損，是不易量化的。因此，對於容易得知的資訊安全投資成本，就成了經濟成本構面中，唯一備受重視的指標。

第三、社會文化的資安策略擬定著重微觀指標，並且需要依據不同的社會文化而制定。本研究的資料顯示，社會文化因素中，資安認知與態度以及顧問專業資安輔導，對公私部門資安策略都有重要的影響。不同產業間的資安問題意識，為組織建置或推動資安策略，進行變革的重要環境指標。同業之間對資安問題的重視與應對，往往會相互影響。在建置推動資安策略時，公私部門對外部專業資安顧問，均仰賴其輔導。事實上，台灣六成左右的上市櫃公司，確實是在四大事務所輔導下，獲取資安國際認證。在產業資安責任指標上，公部門資安策略的制定、推動、控制與缺失檢討等活動，常仰賴或聚焦於外包廠商；金融業除一般資安議題，還須重視保護客戶隱私。

第四、技術科技方面，宏觀與微觀指標都將影響公、私部門在設置資安策略。宏觀指標中，有駭客攻擊手法與資安事故因應、委外廠商的控管，是公部門擬定資安技術科技策略的重要指標。私部門的高科技業者，重視兩項宏觀指標：基礎設施與委外廠商的控管。在微觀指標的部分，公私部門都會借助外界專業顧問，幫其將不明確的法規規範，化身為明確的內部作業流程。影響部門面對的部分資安政策與法令規定較為模糊，對於如何將其落實於實際資安管控工作中，會倚重外界專業顧問。私部門採取的實務做法是，透過參考業界其他組織的實務管控辦法，與專家討論後，訂定適合自身組織的執行方案，以確保組織人員在工作中，都能有清楚的準則可供依循。

綜合研究發現，建置推動或執行資安策略上，會驅動公私部門的環境指標確實有所不同。在實務上，首先，政府機關若欲針對不同部門組織，驅使其強化資安時，可給予不同的環境因素刺激。其次，組織在制定資安策略時，宜充分了解自身情形與期待事項，尤其要優先解決影響程度大或較脆弱的環節。組織也要對資安輔導顧問業，有一定的熟識度，才能選擇合適顧問，為組織資安策略訂立明確時程及具體執行項目的有效策略。再者，建置推動資安策略過程中，須不斷釐清方向，視發展階段了解重要環境指標，以避免資安策略的疏漏與確保其可行性。此外，毋論何種類型組織，所面臨的資安問題，會隨著資安技術的進步、參與人員的資安問題意識改變，以及組織所處的資安發展階段，而有所不同。組織宜注意關注自身狀況，聚焦於目前資安策略所需要關注的環境指標。最後，由於本研究是資安驅動力的探索性研究，本研究結果一方面有助於提供政府驅動產業加入資安活動的參考，以提升整體產業與國家的資安投入。另一方面，各個產業也能根據本研究的結果，參考其重要環境因素對組織的可能影響，進而提早思考資安策略的方向。

本研究以 PEST 架構為根基，同時考慮多個構面，分析公部門、金融業與高科技製造業的資安議題，在資安策略上，提供了一個廣泛的探究基礎。雖以嚴謹的態度與方法進行，但在實際的研究過程中，仍不免有下列限制。第一，目前市場上越來越多產業意識到資安的重要性，也相繼投入資源，以增進組織的資訊安全。而本研究目標鎖定在公部門(包括醫療)、金融與高科技業組織，以這三類型對資安需求較為急迫的個案主為研究對象。雖然可提供學術上豐富的資料收集，但研究對象若為其他產業別時，本研究之結果，有可能需要再加以修正。第二，本研究之研究個案皆為台灣組織，國家區域文化、生活習慣等，特別是資安風險意識，可能與其他國家地區有所不同，因此，對應到其他國家或是跨文化的其他組織，是否仍呈現相同結果，也值得後續研究探討。第三、本研究透過訪談專業資安顧問，而取得研究資料。雖然專業顧問為客觀觀察者，但是受訪時，是否能以豐富語彙充分說明個案情形，會對本研究產生影響。第四、推動資安策略時，取得資安認證是極為常見的方法，因此本研究取樣上，以取得資安認證或推動資安認證的組織，為重要篩選條件。然而，這樣的抽樣方式恐會對研究發現，產生影響或限制。而本研究之研究對象，個別組織所處的資訊安全階段與採用的資安推動方法不盡相同，組織目標或內部資源等，對個別組織推動資安有何影響？這個問題將對於實務上，資安的推動具有重要參考價值，值得未來研究持續深入發掘。

參考文獻

行政院國家資通安全會報(2019)，*國家資通安全發展方案(106 年至 109)*，https://www.tcrc.edu.tw/files/0news/106-109%E5%B9%B4%E5%9C%8B%E5%AE%B6%E8%B3%87%E9%80%9A%E5%AE%89%E5%85%A8%E7%99%BC%E5%B1%95%E6%96%B9%E6%A1%88.pdf

行政院國家資通安全會報(2021)，*國家資通安全發展方案(110 年至 113)*, https://cloudschool.chc.edu.tw/open-message/074738/get-file/6041e464285d5d58af198572.pdf

陳志誠、林淑瓊、劉用貴、趙乃青(2018)，「BYOD 導入企業之關鍵管理因素：組織資訊安全管理觀點」，*資訊管理學報*，第二十五卷，第一期，頁 76-102。

黃士銘、張碩毅、蘇耿弘(2006)，「企業導入 BS7799 資訊安全管理系統之關鍵成功因素－以石化產業為例」，*資訊管理學報*，第十三卷，第二期，頁 171-192。

葉桂珍、張榮庭(2006)，「企業之資訊安全策略與其產業別及資訊化程度關係探討」，*資訊管理學報*，第十三卷，第二期，頁 113-143。

Aguilar, F. J. (1967). *Scanning the Business Environment*, Macmillan, New York.

Babatunde, B. O. & Adebisi, A. O. (2012). Strategic Environmental Scanning and Organization Performance in a Competitive Business Environment, *Economic Insights-Trends & Challenges*, 64(1), 24-34.

Balozian, P. & Leidner, D. (2017). Review of IS security policy compliance: Toward the building blocks of an IS security theory, *The DATA BASE for Advances in Information Systems*, 48(3), 11-43.

Bourgeois, III L. J. (1980). Strategy and Environment: A Conceptual Integration, *The Academy of Management Review*, 5(1), 25-39.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness, *MIS Quarterly*, 34(3), 523-548.

Chen, H., Li, Y., & Yin, J. (2021). Understanding employees' adoption of the Bring-Your-Own-Device (BYOD): the roles of information security-related conflict and fatigue, *Journal of Enterprise Information Management*, 34(3), 770-792

Chebo, A. K. & Kute, I. M. (2019). Strategic process and small venture growth: The moderating role of environmental scanning and owner-CEO, *Journal of Small Business Strategy,* 29(3), 60-77.

Da Veiga, A. (2016). Comparing the information security culture of employees who had read the information security policy and those who had not, *Information & Computer Security*, 24(2), 139-151.

Deane, J.K., Goldberg, D.M., Rakes, T.R., & Rees, L.P. (2019) The effect of information security certification announcements on the market value of the firm, *Information Technology and Management*, 20, 107-121.

Diamantopoulou, V., Tsohou, A., & Karyda, M. (2020) From ISO/IEC 27001:2013 and ISO/IEC 27002:2013 to GDPR compliance controls, *Information & Computer Security*, 28(4), 645-662

Drozd, O. (2016). Privacy pattern catalogue: a tool for integrating privacy principles of ISO/IEC 29100 into the software development process, *Part of the IFIP Advances in*

Information and Communication Technology book series (Tutorials, volume 476), Springer, Cham.

Ermicioi, N. & Liu, X.M. (2021). An Interdisciplinary Study of Cybersecurity Investment in the Nonprofit Sector, *American Journal of Management*, 21(5), 39-50.

Fahey, L., King, W. R., & Narayanan, V. K. (1981). Environmental scanning and forecasting in strategic planning—the state of the art, *Long range planning*, 14(1), 32-39.

Fahey, L. & Christensen, H. K. (1986). Evaluating the research on strategy content, *Journal of Management*, 12(2), 167-183.

Fleisher, C.S. & Bensoussan, B.E. (2003). *Strategic and Competitive Analysis: Methods and Techniques for Analyzing Business Competition*, Prentice Hall, New Jersey.

Gluckman, R. (2014). Buzzing around China, *Forbes Asia*. April: 18-21.

Gupta, A. (2013). Environment & PEST analysis: an approach to the external business environment, *International Journal of Modern Social Sciences*, 2(1), 34-43.

Hartman, B., Flinn, D. J., & Beznosov, K. (2002). *Enterprise Security with EJB and CORBA (Vol. 16)*, John Wiley & Sons, New Jersey.

Hausken, K. (2006). Income, interdependence, and substitution effects affecting incentives for security investment, *Journal of Accounting and Public Policy*, 25(6), 629-665.

Ho, J. K. K. (2014). Formulation of a systemic PEST analysis for strategic analysis, *European Academic Research*, 2(5), 6478-6492.

Ilvonen, I. (2013). Information security assessment of SMEs as coursework–learning information security management by doing, *Journal of Information Systems Education*, 24(1), 53-62.

ISO/IEC (2013). Information technology–Security techniques–Code of practice for information security controls (ISO/IEC 27002), Geneva, Switzerland: ISO.

Jerman-Blažič, B. & Tekavčič, M. (2012). Managing the investment in information security technology by use of a quantitative modeling, *Information Processing & Management*, 48(6), 1031-1052.

Jobber, D. & Ellis-Chadwick, F. (2016). *Principles and Practice of Marketing* (8th Ed.), McGraw-Hill Education, London.

Jogaratnam, G. & Law, R. (2006). Environmental scanning and information source utilization: exploring the behavior of Hong Kong hotel and tourism executives, *Journal of Hospitality & Tourism Research*, 30(2), 170-190.

Johnson, G., Whittington R., & Scholes K. (2011). *Exploring corporate strategy: text & cases* (9th Ed.), Pearson education, London.

Jouini, M., Rabai, L.B.A., & Khedri, R. (2021) A quantitative assessment of security risks based on amultifaceted classification approach, *International Journal of Information Security*, 20, 493-510

Kang, M. & Hovav, A. (2020). Benchmarking Methodology for Information Security Policy (BMISP): Artifact Development and Evaluation, *Information Systems Frontiers*, 22, 221-242

Kemp, M. & Kemp, M. (2005). Beyond trust: security policies and defence-in-depth, *Network Security*, 2005(8), 14-16.

Kinnunen, H. & Siponen, M. (2018). Developing organization-specific information security policies by using critical thinking, *Proceedings of the 22nd Pacific Asia Conference on Information Systems*, Yokohama, Japan.

Kissoon, T. (2020). Optimum spending on cybersecurity measures, *Transforming Government: People, Process and Policy*, 14(3), 417-431.

Kong, H.K., Kim, & Kim, J. (2012). An analysis on effects of information security investments: a BSC perspective, *Journal of Intelligent Manufacturing*, 23(4), 941-953.

Krippendorff, K. (2018). *Content analysis: An introduction to its methodology*, Thousand Oaks, Sage publications, CA.

Lin, I. C., Lin, Y. W., & Wu, Y. S. (2016). Corresponding Security Level with the Risk Factors of Personally Identifiable Information through the Analytic Hierarchy Process, *Journal of Computers*, 11(2),124-131

Neuendorf, K. A. (2017). *Content analysis guidebook*, 2nd Thousand Oaks, Sage, CA.

Niemimaa, E. & Niemimaa, M. (2017). Information systems security policy implementation in practice: From best practices to situated practices, *European Journal of Information Systems*, 26(1), 1-20

Orehek, S. & Petric, G. (2021) A systematic review of scales for measuring information security culture, *Information & Computer Security*, 29(1), 133-158

Peng, G. C. A. & Nunes, M. B. (2007). Using PEST analysis as a tool for refining and focusing contexts for information systems research, *6th European Conference on Research Methodology for Business and Management Studies*, Lisbon, Portugal.

Puhakainen, P. & Siponen, M. (2010). Improving employees' compliance through information systems security training: an action research study, *MIS Quarterly*, 34(4), 757-778.

Rastogi, N. & Trivedi, M. (2016). PESTLE technique–a tool to identify external risks in construction projects, *International Research Journal of Engineering and Technology,* 3(1), 384-388.

Robbins, S. P. & Judge, T. (2022). *Organizational Behavior* (19th Ed.), NY: Pearson New York.

Ryan, J. J. & Ryan, D. J. (2006). Expected benefits of information security investments, *Computers & Security*, 25(8), 579-588.

Shadbad, F.N. & Biros, D. (2022). Technostress and its influence on employee information security policy compliance, *Information Technology & People*, 35(1), 119-141

Sherif, E., Furnell, S., & Clarke, N. (2015). A Conceptual Model for Cultivating an Information Security Culture, *International Journal for Information Security Research*, 5(2), 565-573.

Stewart, H. & Jürjens, J. (2017). Information security management and the human aspect in organizations, *Information and Computer Security*, 25(5), 494-534.

Talib, M. S. B., Hamid, A. B. A., Zulfakar, M. H., & Jeeva, A. S. (2014). Halal logistics PEST analysis: the Malaysia perspectives, *Asian Social Science,* 10(14), 119-131.

Tsai, C.H. & Su, P.C. (2021) The application of multi-server authentication scheme in internet banking transaction environments, *Information Systems and eBusiness Management*, 19(1), 77-105.

Vintilă, G., Gherghina, S. C., & Toader, D. A. (2019). Exploring the Determinants of Financial Structure in the Technology Industry: Panel Data Evidence from the New York Stock Exchange Listed Companies, *Journal of Risk Financial Management*, 12(4), 163-180.

Yu, C.P., Chu, C.P., & Lu, P.H. (2018). Applying a Security Management Mechanism to a System Development Lifecycle, *International Journal of E-Adoption*, 10(1), 1-17.

附錄 1

政治法令(Politics)			
指標	**定義**	**關鍵字**	**參考文獻**
P01 國內政策與法規	中央政府單位為積極推動國家資通安全政策，加速建構國家資通安全環境以保障國家安全、維護社會公共利益所制定的政策與規範。	資通安全法、資安法、銀行法、證券法、保險法、PDPA	Bulgurcu et al. 2010; Babatunde & Adebisi 2012; Rastogi & Trivedi 2016; Vintilă et al. 2019; Diamantopoulou et al. 2020; Kang & Hovav 2020
P02 國際認證	國際標準化組織、英國標準協會等具公信力團體所制訂的資訊安全相關國際標準認證。	通過驗證、ISO、BS	
P03 投標契約書內容與規定	投標單位按照組織招標書的條件和要求。	無敵條款、投標書、RFP、專案管理、時程	
P04 獎懲制度	政府對資安管控的罰則或獎勵制度。	績效考核、考績、記點	
經濟成本(economic)			
E01 資訊安全投資成本	預期為組織可能帶來的利益與好處，所投入於資訊安全項目上的資金花費。	購買設備、軟體、投資	Jerman-Blažič & Tekavčič 2012; Kong et al. 2012; Ilvonen 2013; Rastogi & Trivedi 2016; Deane et al. 2019; Kissoon 2020; Ermicioi & Liu 2021; Jouini et al. 2021
E02 資訊安全準備金	針對一段時期所需的收入和支出做出預測和規劃。	採購清單、預算	
E03 績效	一定時期內的工作行為、方式、結果及其產生的客觀影響。	投資報酬率、淨現值.邊際效益	
E04 市場趨勢	對一個或多個有確定的意義市場，所做的持續反映。	陌生開發、淺在市場、市場競爭	
社會文化 (society)			
S01 產業慣例	產業中多數組織共同的價值觀、處事方式和信念等內化認同表現出來的行為方式。	文化、文化變革	葉桂珍、張榮庭 2006; Bulgurcu et al. 2010; Puhakainen & Siponen 2010; Babatunde & Adebisi 2012; Sherif et al. 2015; Da Veiga 2016; Rastogi & Trivedi 2016; Jobber & Ellis-Chadwick 2016; Babatunde, Stewart, & Jürjens 2017; Balozian & Leidner 2017; Yu et al. 2018; 陳志誠等人 2018
S02 產業資安責任	聚焦的資安重點會因產業別，而有所不同。	組織結構、職責、分工、政治鬥爭與權力衝突 、人員內鬥	
S03 人力資源	資安推動所需之專業人力、人員流動、人才培訓或人力短缺等	流動、輪調、離職、人力資源、招募	
S04 領導理念	領導者的觀點、看法和信念	領導者問題、想法. 主管	
S05 資訊安全認知與態度	不同產業的資安問題意識、判斷和想法，以及員工對環境的認知能力以及了解程度，和他們的看法和信念。	廠商、員工認為、不想做、增加工作、監督廠商、陪同監督	
S06 溝通與討論	提出問題、說明或解決辦法與他人或團體建立互動式的討論方式。例如：資安事件通報平台、資安大會…。	談論、議論	
S07 教育訓練	有經驗者以系統化的方式引導學習者了解資安，以達到執行資安活動的目標。	教育背景、在職訓練、職前訓練	

S08 重大事件	對組織將產生嚴重傷害或影響的資安相關事件。	洩漏資料. 廣告和媒體.同業連鎖效應	
技術科技(technology)			
T01 電腦系統結構	能在機器上正確運行所應具有的軟體和硬體介面結構和功能。	寫死、無法更動	黃士銘等人 2006; Ho 2014; Rastogi & Trivedi 2016; Vintilă et al. 2019; Orehek & Petric 2021; Shadbad & Biros 2022
T02 顧問專業資安輔導	顧問協助組織導入資安的國際標準的能力。	專案管理、顧問、內部稽核	
T03 駭客攻擊手法與資安事故因應	資安事件發生後，組織針對資安事故做出的處理和應對。	資訊安全事故管理與處理、通報對象、事件等級、駭客攻擊、跳板	
T04 基礎設施	資訊服務運作之重要基礎設備。	防火牆、監控系統、同步備份、加密	
T05 委外廠商的控管	外包程序的控制與管理措施，包括文件紀錄、制定標準作業程序、擬定測試計畫等。	廠商、管控措施	
T06 技術人員與專業技術能力	資安技術人員對機器、硬體、系統運用的技巧	程式撰寫、專業技術能力	
T07 系統技術檢測與演練	找出系統漏洞，針對弱點加以修正與改進的相關技術。或預演攻擊事件發生時，測試其應對策略能否進行有效的防技術工具。	滲透測試、弱點掃描、資安健診、營運持續計畫演練、紅隊演練	