華岡法粹／*Hwa Kang Law Review*
Vol. 74 (2023), pp. 1-62
DOI10.6868/HKLR.202306_(74).01

資訊安全長之設置與責任初探

The Establishment and Responsibilities of Chief Information Security Officer

余 啓 民*
Chi-Min Yu

摘 要

數位經濟已成為各國經濟發展重心，COVID-19 疫情更促使各行各業競相投入數位轉型，但資通訊科技日新月異與資料多元應用也使得資訊安全問題日趨嚴峻。資訊安全風險已是當前企業營運之重大挑戰，然而資訊安全風險管理涉及眾多層面與考量因素。面對資訊安全風險對企業帶來的威脅，建立充分對應相關風險的管理機制，成為資訊安全風險問題對應上的重要工作。對此，企業如何藉由設置「資訊安全長」，將資訊安全風險與企業經營加以連結，甫能充分判斷資訊安全事件對企業營運所產生的實際影響範圍與影響程度。美國「聯邦資訊安全管理法」強調「資訊安全長」的重要，帶動主要國家制定相近規範，而我國「資通安全法」亦首見於法律層級明訂「資通安全長」之設置要求。在非公務機關層面，金管會於「金融資安行動方案」及「金融資安行動方案 2.0」中提出及擴大資訊安全長之設置要求，並採取分階段及分級方式加以推動。在個人資料保護議題受到重視並衍生應否設置隱私長／個人資料保護官之討論時，我國亦可參酌資訊安全長的設置要

投稿日期：112.04.10　　接受刊登日期：112.05.23　　最後修訂日期：112.05.28

*　東吳大學法學院副教授，美國南美以美大學法律暨法學博士。
Associate Professor, Soochow University, School of Law, J.D & S.J.D, Southern Methodist University, School of Law.

求，以分層分級方式逐步推動此一機制，協助企業在全力發展之餘，可得有效兼顧發展過程中所出現的資訊安全風險之管理需求。

關鍵詞：數位經濟；資訊安全；資訊安全風險；資訊安全長；聯邦資訊安全管理法；資通安全法；金融資安行動方案

目　次

壹、前言

考量資通訊科技日新月異與資料應用多元化下衍生的問題日益增加，「資訊安全」（Information Security）開始成為不容企業忽視的重要議題。依據 PwC 於 2022 年 9 月發布的「全球數位信任洞察報告」（Global Digital Trust Insights Survey），PwC 分析全球 65 國、合計 3,522 家企業，研究成果顯示在過去三年全球約有 27 %的企業曾發生資料外洩事件，而因資訊安全事故所遭受的損害金額平均在 100 萬至 2,000 萬美元之譜[1]。

在數位轉型（Digital Transformation）浪潮席捲全球下，全球企業無不爭先投入數位化及轉型工作藉以維持成長，但此舉卻可能招來企業難以有效防範新興的資訊安全威脅與資料不當利用風險，造成重大的財務與商譽損失。諸如美國最大輸油管線業者 Colonial Pipeline 在 2021 年遭到勒索病毒攻擊，導致其營運系統因攻擊行為而被迫關閉數日，也造成美國東岸地區發生嚴重的燃油短缺，由此可見資訊安全問題的嚴重性[2]。

「資料經濟」（Data Economics）已是當前國際間密切討論的議題，資料已與物質與能源並列為重要的經濟資源，而資料與其他經濟資源的最大差異，在於資料並不因使用行為而出現消耗情形，反而可以不斷的重組而再利用，同時資料越經使用，其價值也將越高。伴隨資料量的急遽增加，數位創新固然有助於將用戶個人資料轉化為具競爭力的成果，惟如何有效保護包括個人資料在內的各類資料，並衡平資料利用行為衍生的法律爭議，亦相形重要。隨著資訊安全與個人資料保護成為各個國

1 PwC, A C-suite united on cyber-ready futures: Findings from the 2023 Global Digital Trust Insights 10-11 (2023), *available at* https://www.pwc.com/gx/en/issues/cybersecurity/global-digital-trust-insights.html (last visited June 12, 2023).

2 Sean Michael Kerner, *Colonial Pipeline hack explained: Everything you need to know*, *available at* https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know (last visited June 12, 2023).

家共通關注的議題，本文自「資訊安全長」（Chief Information Security Officer）角度出發，分析國際及我國立法針對資訊安全長此一重要性角色的設置規範與相關要求，並進而思考在個資保護受到重視下，隱私長／個人資料保護官此一角色之關聯推動議題，以期助益國內各界思考及有效因應資訊安全風險所帶來之重大挑戰。

貳、資訊安全長之重要性與設置規範分析

一、資訊安全風險頻生突顯「資訊安全長」之價值

（一）資訊安全風險已是當前企業營運之重大挑戰

公、私部門日常營運上無不面臨著各項風險，就「風險」（Risk）一詞而言，其泛指任何可能影響企業達到其管理或控制目標的威脅或障礙。企業如何有效識別風險、可得承受多少風險以及如何降低或轉移風險，均屬於企業風險管理之範疇[3]。長期關注內部控制與風險管理的COSO委員會（Committee of Sponsoring Organizations of the Treadway Commission, COSO）[4]，在其發布的「企業風險管理－整合架構」（Enterprise Risk Management - Integrated Framework）文件中，將企業風險管理定義為「遍及企業各個層面之流程，該流程受到企業董事會、

3 廖君美，企業風險管理與資訊安全機制設計，財金資訊季刊，第 75 期，頁 27，2013 年 7 月。

4 1970 至 80 年代美國發生許多不實財務報表事件，導致投資人對財務報表資訊喪失信心，為找回投資人的信心與恢復市場秩序，在美國會計師協會、會計學會、財務主管協會、管理會計人員協會及內部稽核協會等眾多機構支持下，美國於 1985 年成立「不實財務報導全國委員會」（National Commission on Fraudulent Financial Reporting），此委員會又被稱為 Treadway 委員會，並由 Treadway 委員會贊助成立 COSO 委員會，投入內部控制等相關議題之研究工作。林淑芸、金旻姍，美國 COSO 內部控制相關報告之介紹，證券暨期貨月刊，第 33 卷，第 6 期，頁 6，2015 年 6 月。

管理階層或其他人員之影響，用以制定策略、辨認可能影響企業之潛在事項、管理企業之風險，使其不超過企業之風險承受範圍，以合理保證其目標之達成」[5]。

COSO 委員會於 90 年代發布「內部控制報告」，雖將「風險評估」納入內部控制之組成要素，然而，在企業經營實務上，必須可得於「企業成長」、「企業報酬」與「企業風險」三者之間取得最適平衡，以訂定策略及目標。有鑑於此，COSO 另發布「企業風險管理－整體架構」報告，由原先「內部控制報告」之三大目標，擴充為「策略」、「營運」、「報導」及「遵循」等四大目標，並將原先「內部控制報告」之五大要素，擴充為「內部環境」、「目標設定」、「事件辨認」、「風險評估」、「風險因應」、「控制活動」、「資訊與溝通」及「監督」等八大要素[6]。

企業在享受資訊化便利性的同時，必須留意相關資訊資產是否受到妥善保護，關注可能潛藏的資訊安全風險，並思考如何善用有限的資源落實資訊安全管理，相關事務無疑是所有企業共同面臨的重大挑戰。為因應日新月異的資訊環境所帶來的資訊安全風險，成立資訊安全專責單位並思考設置資訊安全長，看似成為公、私部門的必經道路，預跳脫傳統的資訊框架，並以全方位的角度為公、私部門發現可能發生的潛在資訊安全風險。

（二）資訊安全風險管理涉及眾多層面與考量因素

1. 資訊安全風險管理概念

由於各式各樣的資訊，包括個人健康紀錄、位置資料、用電資料等，越來越容易被複製且被分享至全球各地，使得維護資訊安全與保障隱私變得越來越困難，同時也產生資料剖繪（Profiling）、特定族群歧視、刻

5 廖君美，同註 3，頁 27-28。

6 王宏瑞，淺談美國 COSO 委員會之「企業風險管理－整合架構」報告，集保結算所月刊，第 225 期，頁 13，2016 年 4 月。

意排除或喪失資料自我控制等負面影響[7]。

面對資訊安全風險對企業帶來的威脅，建立充分對應相關風險的管理程序成為包括資訊安全風險在內，各項風險問題對應上的重要工作。就管理程序一詞而言，其係指透過一套有系統的方法，來達到以下的三大目的：（1）管控或降低資訊安全意外事件所可能造成的損失：風險管理要能夠辨識出可能發生的意外事件或風險，並採取適當回應，以使得可能的損失被控管在一個可接受的範圍內。（2）提升資訊安全措施的成本效益：風險管理的方法要能夠協助企業或組織，在需要控管某項風險時，能夠找到最有成本效益的措施來進行控管。（3）滿足法規或是利害關係人（如客戶與消費者團體）的相關要求[8]。

企業經營上一旦發生重大資訊安全事件，即無可避免地對企業營運造成損失，此時企業內部若欠缺諸如「資訊安全長」此一角色，無法將資訊安全風險與企業業務經營加以連結及評估，就無法充分判斷資訊安全事件對企業營運所產生的影響範圍與實際影響程度。

2. 資訊安全風險之評鑑

以法務部「法務部及所屬機關資訊安全風險評鑑管理規範」為例，此一規範表明風險評鑑作業的首要工作，係建立所謂的「風險管理全景」，亦即識別組織內、外各方面的資訊安全需求，包括資訊安全政策以及法令、法規、規章與合約以及其他可能影響資訊安全之事務，以利界定風險評鑑範圍並執行風險評鑑作業[9]。

而「風險評鑑範圍」之具體界定，則有必要分別定義「風險準則」

---

7 葉志良，大數據應用下個人資料定義的檢討：以我國法院判決為例，資訊社會研究，第 31 期，頁 3-4，2016 年 7 月。

8 查士朝，資訊安全風險管理介紹，頁 7，http://www.im.ntu.edu.tw/~tsay/dokuwiki/lib/exe/fetch.php?media=courses:sem2009:20090410cha.pdf（最後瀏覽日期：2023 年 6 月 12 日）。

9 法務部及所屬機關資訊安全風險評鑑管理規範第 4 點第 1 項本文。

（Risk Criteria）、「風險等級」（Level of Risk）及「風險接受準則」（Risk Acceptable Criteria）。風險準則係指評估風險顯著性時所用的評估條件及其評估方法，若評估方式採用所謂的「定性」作法，則其評估條件應考量：（1）弱點；（2）威脅；及（3）衝擊等三個項目。風險等級則是指以風險評估條件評估結果之總合方式表示之風險顯著性。而最後的風險接受準則，則是指機關用以決定留置或承受風險之原則，機關所應考量影響風險接受準則，其項目包括：（1）業務需求及目標；（2）法律、法令、規章及契約方面之要求;（3）智慧財產權（Intellectual Property Right, IPR）;（4）資源分配狀況；（5）技術成熟度；（6）經費預算；（7）社會與輿論因素[10]。

3. 資訊安全風險之處理

法務部「法務部及所屬機關資訊安全風險評鑑管理規範」針對「風險處理」一事，明訂可採用之風險改善方式包括：（1）規避風險；（2）降低風險發生機率；（3）降低風險影響程度；（4）轉移風險；（5）接受風險等五者[11]。若風險項目係超過「可接受風險等級」，規範要求應擬訂風險改善計畫，並明訂風險改善計畫之擬訂，應預估完成後殘餘風險是否可降低至可接受風險值以下，並考量所需資源、優先順序、責任分配等因素，至少包含下列內容：（1）風險項目；（2）採取之控制方法；（3）所需投入資源；（4）相關負責人員；（5）預估完成日期[12]。此外，針對所採用的風險改善計畫，其應符合整體資訊安全目標。同時風險改善計畫執行結束後，應重新評估殘餘風險是否均已降低至可接受風險值以下[13]。

---

10 法務部及所屬機關資訊安全風險評鑑管理規範第 4 點第 1 項第 1 款至第 3 款。
11 法務部及所屬機關資訊安全風險評鑑管理規範第 5 點第 1 項。
12 法務部及所屬機關資訊安全風險評鑑管理規範第 5 點第 2 項。
13 法務部及所屬機關資訊安全風險評鑑管理規範第 5 點第 3 項、第 4 項。

（三）資訊安全風險管理突顯「資訊安全長」之價值與必要性

資訊安全不應只有「資訊系統」安全的思維，過度執著於資訊系統本身，常會忽略企業營運其他構面所潛在的安全風險。企業實有要將其納入企業風險管理系統的範疇，從資訊安全管理、資訊治理到企業治理一以貫之，以期維護企業的永續發展[14]。

在資訊安全議題日益複雜下，連帶突顯出「資訊安全長」的價值與重要性。蓋資訊安全長除了符合法律遵循要求，作為稱職的資訊安全長，必須能夠定義資訊安全角色與職掌功能，也必須了解企業所面臨的風險並連結績效指標，最後更要知道如何配合業務發展策略，投入相對應之資源。易言之，身為企業高階主管的資訊安全長，已經不能和以往定義的資訊安全部門主管一樣，只偏重資訊安全技術與縱深防護而已，思考角度應由傳統的技術思維，進一步轉變為企業之營運思維[15]。

隨著數位化程度的普遍提升，嶄新資通訊技術為企業帶來更多的創新發展可能，但同時也增加不安全系統可能導致的風險。特別是數位化打破數位與物理世界的界線，電力網路、水利系統與工廠設施等重要基礎設施，均逐步採用物聯網等數位技術取代傳統的類比控制系統，無形中也使得資訊安全風險急遽升高。為因應此一數位化浪潮下的重大挑戰，使資料管理人（企業）確實擔負保護資料之責，美國白宮於 2023 年 3 月發布「國家資安策略」（National Cybersecurity Strategies），揭示未來十年的資訊安全發展策略，除強調將持續推動資訊安全技術與設備的開發，亦表明美國應重新檢討相關法律，促使企業就其因為軟體漏洞等未落實資訊安全所成的損害負起相關責任[16]。無論是產業發展層面抑

14 廖君美，同註 3，頁 31。

15 黃彥棻，有獲利的企業，年底前都要設立資安長，https://www.ithome.com.tw/news/155142（最後瀏覽日期：2023 年 6 月 12 日）。

16 THE WHITE HOUSE, NATIONAL CYBERSECURITY STRATEGIES 9 (2023).

或法制政策層面，均顯示企業設置「資訊安全長」實有其必要性。

二、「資訊安全長」之概念、職責與設置必要性

（一）資訊安全長的定義與主要職責

1. 資訊安全長之定義

資訊安全長（Chief Information Security Officer, CISO）簡言之係指「負責企業內部組織資訊與資料安全之高層管理人員」[17]。在網路高度普及以及嶄新技術如大數據、雲端計算與人工智慧等快速發展下，加諸資料跨境流通與儲存成為常態，均使得資訊安全長此一角色的重要性日益提升。資訊安全長除了應對資料外洩風險與其他安全事件，資訊安全長亦經常負責評估、預測與積極管理企業營運上持續出現的威脅，藉由與不同部門的高階管理人員進行合作，以便使資訊安全管理計畫得與企業業務發展目標保持一致，並減輕各種安全威脅帶來的風險[18]。

2. 資訊安全長之職責

就資訊安全長職責而言，現時多數討論經常引用 90 年代於花旗集團（Citigroup）擔任資訊安全長的 Stephen Katz 所界定的職責範圍。Katz 將資訊安全長所負職責區分為下述八者：

（1）**資安操作**（Security Operations）

針對立即出現的威脅進行即時分析，同時針對問題發生時的情況進行識別與分類。

---

17 Josh Fruhlinger, *How the CISO role is evolving*, *available at* https://www.csoonline.com/article/3332026/what-is-a-ciso-responsibilities-and-requirements-for-this-vital-leadership-role.html (last visited June 12, 2023).

18 范國華，業者該如何適應跨國資訊安全相關法規及其守法方法，https://www.lexology.com/library/detail.aspx?g=e1570392-d100-4b84-8386-f0f6b096cf3e（最後瀏覽日期：2023 年 6 月 12 日）。

（2）**網路風險與網路情報**（Cyber Risk and Cyber Intelligence）

針對持續發展中的安全性威脅保持第一手狀態的瞭解，並使董事會知悉可能因併購或其他重大營運行動所可能導致的潛在資安問題。

（3）**資料漏失與詐欺預防**（Data Loss and Fraud Prevention）

確保企業內部人員不致誤用或竊取資料。

（4）**資安建構**（Security Architecture）

規劃、採購與推動資安相關軟、硬體設備，確保 IT 與網路基礎架構係以最佳安全性實作方式為目標進行設計。

（5）**身分與存取管理**（Identity and Access Management）

確保僅有獲得授權的人員擁有管制資料與系統的存取權限。

（6）**計畫管理**（Program Management）

實際運作有助於緩解風險的計畫或專案，例如定期性的系統漏洞修補，以利在資安需求上維持領先地位。

（7）**調查與取證**（Investigations and Forensics）

在外洩事件發生時確認究竟發生何等問題，若係發生於企業內部，除處理責任歸屬，亦應規畫如何避免相同問題再度發生。

（8）**治理**（Governance）

確認上述所有事項均可得順利運作，並取得所需資源，同時使企業領導高層理解相關事項的重要性[19]。

（二）要求企業應設置「資訊安全長」的重要性與必要性

為統籌並加速我國資訊通訊安全基礎建設，以強化資通訊安全能力，「國家安全會議」於 2000 年研提「建立我國通資訊基礎建設安全機

19 Fruhlinger, *supra* note 17.

制」建議書，行政院並於 2001 年 1 月第 2718 次院會核定通過第一期資通安全機制計畫，成立行政院「國家資通安全會報」，積極推動我國資通安全基礎建設工作[20]。

國家資通安全會報主責制定我國資通安全政策、推動資安事件通報應變機制並進行跨部會資通安全事務的督導與協調，以強化整體資通訊安全防禦與災後應變能力。為促進資訊通訊安全發展，國家資通安全會報持續推動「國家資通安全發展方案」，其中在第二期發展計畫時，除成立「國家資安監控中心」（National Security Operations Center, NSOC）外，也首次提出設置「資訊安全長」（CISO）之倡議，藉以落實資訊安全長責任制度，強化資通安全防護及管理之責。

特別是在當今的全球化時代，企業的經營觸及不以臺灣為限時，勢必伴隨資料的傳輸而有觸及業務所及國家的網路安全、資訊安全或個人資料保護立法。另一方面，隨著網路事件所帶來的威脅與影響持續增加，主要國家也開始意識並持續嘗試通過監管立法，要求公、私部門應設置包括「資訊安全長」在內的必要人力，以解決當前已普遍出現的資訊安全風險[21]。

以私部門要求為例，美國紐約州金融服務署（New York State Department of Financial Services）於 2017 年發布「金融服務業網路安全規範」（23 NYCRR Part 500）[22]，成為目前美國金融監理機關針對防範網路攻擊唯一法律層級的資通安全規範，要求金融機構應指定「資訊安全長」負責執行與監督、強化資訊安全計畫及政策。新加坡於 2018 年通過網路安全法（Cybersecurity Act），並該法第 4 條中規定網路安全總

20 數位發展部資通安全署，行政院國家資通安全會報緣起背景，https://moda.gov.tw/ACS/nicst/background/658（最後瀏覽日期：2023 年 6 月 12 日）。

21 同註 18。

22 New York State, *Proposed Second Amendment to 23 NYCRR Part 500*, *available at* https://www.dfs.ny.gov/industry_guidance/cybersecurity (last visited June 12, 2023).

監（Commissioner of Cybersecurity）、副總監（Deputy Commissioner）及一位以上的網路安全助理總監（Assistant Commissioner of Cybersecurity）與網路安全人員之設置，具體明確彼此權限及任務從屬關係以共同合作推動資安政策[23]。近期，新加坡金融管理局（Monetary Authority of Singapore）於 2021 年修正發布「技術風險管理指引」（Guidelines on Risk Management Practices - Technology Risk）[24]，明訂董事會和高階管理層應確保任命具有必要經驗和專業知識的資訊長和資安長，負責管理技術和網路風險；董事會應具有相關知識的成員，以對技術和網路風險進行有效監督。

三、我國資通安全法首見法律層級「資訊安全長」概念

（一）資通安全管理法之制定沿革與目標

隨著全球進入網路高度發達時代，世界各國對於資訊安全之防護與立法更是看中其重要性，尤其是各國家建立國家層級的資安管理法規，並設立專門部門或機關加以管理。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，我國於 2018 年 6 月制定「資通安全管理法」。

在資通安全管理法制定前，國內與資通安全有關的規範，在公務機關部分，除適用對象較為廣泛之刑法妨害電腦使用罪罪章及個人資料保護法等外，另有行政院及所屬各機關資訊安全管理要點、行政院及所屬各機關資訊安全管理規範、國家資通安全通報應變作業綱要等規定[25]。

---

23 潘元偵，淺談新加坡網路安全法－以網路安全總監為核心，科技法務透析，第 31 卷，第 8 期，頁 15-17，2019 年 8 月。

24 Monetary Authority of Singapore, *Guidelines on Risk Management Practices - Technology Risk*, *available at* https://www.mas.gov.sg/regulation/guidelines/technology-risk-management-guidelines (last visited June 12, 2023).

25 資通安全管理法草案總說明。

然而前述規定中，屬法律者，其規範目的各異，而適用時或僅就實害之結果進行處罰，或其保護客體僅以特定類型之資料為限，並非針對資通安全管理為整體考量而制定；其餘規定對資通安全管理雖定有較細節之規範，但其位階較低，且規定分散，適用上難免不足。至於適用於非公務機關之規定，因其立法目的不同，其適用範圍、保護客體與規範對象亦有差異，無法作為各非公務機關共通遵循之標準，難以帶動其整體資通安全能量。此外，無論是適用於公務機關或非公務機關之規定，均無以資通安全為主要考量，並要求以風險管理為核心，建立完整資通安全維護計畫及通報應變相關機制者，此現況與國際上目前資通安全管理之趨勢尚有落差[26]。

資通安全的確保除能塑造鼓勵持續創新之環境外，對國家安全及社會公益之確保亦有其重要性。近年來，對於公務機關或關鍵基礎設施等進行網路攻擊之情形時有所聞，由於公務機關所承擔之公共任務，及關鍵基礎設施提供者等非公務機關所維運或提供之服務，均對國家安全、民眾生活、經濟活動等有重大影響，該等機關如未能考量自身資通安全風險，進而決定資通安全管理之作法，逐步提升自身資通安全能量，一旦其遭受惡意攻擊，恐造成難以回復之損害。從而制定一部協助公務機關及受規範的非公務機關認知自身資通安全風險並加以因應，訂定及實施資通安全維護計畫以確保其資通安全、逐步提升自身資通安全能量之專法實有其必要性。基此，為提升我國整體資通安全環境及資通安全意識，保障國家安全與公共利益，國內遂正式制定及通過「資通安全管理法」[27]。

（二）該法第 11 條明訂應設置「資通安全長」

依資通安全管理法第 11 條規定「公務機關應置資通安全長，由機

26 同前註。

27 同前註。

關首長指派副首長或適當人員兼任，負責推動及監督機關內資通安全相關事務」。觀察該條之立法理由，其指出「為確保有效推動資通安全維護事項，公務機關應置資通安全長，由其成立相關推動組織及督導推動相關工作。考量資通安全長如由副首長擔任，更能提升資通安全於機關中之重要性，參考美國 2014 年聯邦資訊安全現代化法（Federal Information Security Modernization Act of 2014）關於資訊長應指定資深資安專責人員負責相應事務規定之意旨，爰為本條規定」。

資安作業是一套龐大的分工合作體系，因此精準治理架構是決定資安作業能否有效的關鍵。資通安全管理法實施後，陸續依據資通安全管理法制定「資通安全管理法施行細則」、「資通安全責任等級分級辦法」、「資通安全事件通報及應變辦法」、「特定非公務機關資通安全維護計畫實施情形稽核辦法」、「資通安全情資分享辦法」及「公務機關所屬人員資通安全事項獎懲辦法」等配套子法。其中依資通安全管理法第 22 條規定所制定的「資通安全管理法施行細則」，細則第 6 條規定母法第 10 條、第 16 條及第 17 條所稱之資通安全維護計畫，其所應包括的事項中，亦明文列入「資通安全長之配置」。

四、源自美國 FISMA 之「資訊安全長」機制設計

（一）美國資訊安全立法發展

美國資訊安全法規可追溯至 1929 年聯邦紀錄法（Federal Records Act），1942 年的聯邦報告法（Federal Records Act）更闡明資訊資源管理（Information Resources Management, IRM）由白宮之「管理與預算辦公室」（Office of Management and Budget, OMB）之前身「預算局」（Bureau of Budget）主責；為因應 1952 年起美國「國家安全局」（National Security Agency, NSA）對「機密性」的要求與規範，1985 年 12 月 OMB 以 A-130 公告的附件三（Appendix III）正式啟動資訊安全管理法制化的工作項目

[28]。

隨著資訊化之日益普及，面對多面向的網路威脅議題，1998 年 5 月柯林頓總統以第 63 號總統決策令（Presidential Decision Directive, PDD）將美國根基於「機密性」的電腦系統安全（Computer System Security）擴增至要求「機密性」、「完整性」與「可用性」之資訊安全，在「政府以身作則」的方針下，美國於 2002 年 12 月正式頒布「聯邦資訊安全管理法」（Federal Information Security Management Act, FISMA），並提出設置資訊安全長要求[29]。

繼 2002 年制定 FISMA，2009 年歐巴馬總統簽署「網路空間政策評估報告」，強調保障美國政府之網路系統安全。911 事件後為因應恐怖攻擊，美國成立「國土安全部」（Department of Homeland Security, DHS）。FISMA 配合「網路空間政策評估報告」及「國土安全部」之成立，分別於 2012 年與 2014 年進行兩次修正，將該法納入「國土安全部」為管理角色之一，要求其對資安事件進行通報，並修正法名稱為「聯邦資訊安全現代化法」（Federal Information Security Modernization Act of 2014, 44 USC 3554: Federal agency responsibilities），授權給美國國土安全部對於各公務機關進行監督與管理、管制重大資安事件之通報與受到侵害時之處置[30]。

---

28 樊國楨、林惠芳、黃健誠，資訊安全法制化初探之一：根基於美國聯邦資訊安全管理法，資訊安全通訊，第 18 卷，第 1 期，頁 23，2012 年 1 月。

29 Daniel M. Whitea1, *The Federal Information Security Management Act of 2002: A Potemkin Village*, 79 FORDHAM L. REV. 369, 381-382 (2011); Chelsea C. Smith, *Hacking Federal Cybersecurity Legislation: Reforming Legislation to Promote the Effective security of Federal. Information Systems*, 4 NAT'L SEC. L.J. 345, 365 (2016).

30 國家實驗研究院科技政策研究與資訊中心，各國家對資通安全立法與管理概述，https://iknow.stpi.narl.org.tw/Post/Read.aspx?PostID=18377（最後瀏覽日期：2023 年 6 月 12 日）。

（二）2014 年 FISMA 修正重點與資訊安全長規定

觀察 2014 年「聯邦資訊安全現代化法」的修正重點，其包括：1. 賦與國土安全部長監督管理職掌；2. 調整各機關提出年度報告之內容；3. 增加對重大資安事件進行通報之要求與相關規定；及 4. 增加資訊安全系統測試及關於資訊受侵害時之相關規定等四者。簡要分析如下：

1. 賦與國土安全部長監督管理職掌

將 FISMA 監督管理聯邦各機關資安政策及實施者，由原本之「管理及預算局」（Office of Management and Budget, OMB）局長，改為與「國土安全部」（DHS）部長應隨時互相磋商，共同進行監督管理。職掌包括：（1）DHS 部長協助 OMB 局長執行任務；（2）訂定並監督綜合作業指令之實施；（3）監督聯邦各機關資安政策及實施；（4）召集各機關主管開會，以落實資安政策及實施；（5）協調跨部門資安工作事項；（6）提供各機關資安管理與技術上之協助。當「聯邦資訊安全現代化法」生效兩年後，前述兩位監管最高負責人，應提出政府機構採用診斷式科技及其他精密安全儀器後之效果分析[31]。

2. 調整各機關提出年度報告之內容

對於各機關應向有關監督機關提出年度報告之要求，其內容由原本關於資安政策及措施等執行情形，與預算及資源之運用狀況，調整為關於資安事件之報告。報告內容主要為：（1）重大資安事件之情形與處理狀況；（2）資安事件之統計數量及其影響程度；（3）涉及個人資料受侵害之重大資安事件之相關情形[32]。

---

31 立法院，外國法案介紹－資通安全管理法，頁 20，https://npl.ly.gov.tw/do/www/FileViewer?id=8520（最後瀏覽日期：2023 年 6 月 12 日）。

32 同前註，頁 20-21。

3. 增加對重大資安事件進行通報之要求與相關規定

為因應對重大資安事件進行通報之要求，2014 年「聯邦資訊安全現代化法」規定管理及預算局應訂定「重大資安事件指導原則」，並應向國會報告。此外，發生重大資安事件之機關應於相當確定事件發生後 7 天內，向國會相關權責委員會進行初次通報，並於合理時間內，再次提出詳細報告[33]。

4. 增加資訊安全系統測試及關於資訊受侵害時之相關規定

2014 年「聯邦資訊安全現代化法」除增訂資訊安全系統之定期測試，應包括使用符合標準之自動化儀器在內外，另要求當資訊系統內之資料受到侵害時，應有相當處置措施。管理及預算局應確認關於資料受侵害時之通報政策與指引是否適時更新。受侵害之聯邦機關發現資料遭到無權取得或存取後 30 日內，向國會報告下列事項：（1）侵害發生之原因；（2）預估受侵害影響之當事人數量；（3）是否及何時告訴當事人，並說明可能延遲告知時間之原因[34]。

為強化各單位資訊安全管理並確保相關要求之落實，FISMA 於第 3554 條遂規定「應向根據第 3506 條所設立的機關資訊安全長授予確保遵循本條規定之權力」[35]。而其具體所被授權的權力則包括：

（1） 履行資安長於在本條項規定之職責；

（2） 具備管理本條所述職責所必需的專業資格，包括培訓與經驗；

（3） 將資訊安全職責作為該人員之主要職責；且

（4） 領導一個肩負職務與資源的辦公室，協助確保機構遵循本條規定

---

33 同前註，頁 21。

34 同前註。

35 (3) delegate to the agency Chief Information Officer established under section 3506 (or comparable official in an agency not covered by such section) the authority to ensure compliance with the requirements imposed on the agency under this subchapter.

[36]。

除上述四款事項，FISMA 亦要求確保資安長應予機關其他高階人員進行互動與協調，每年向機關負責人報告資訊安全計畫的有效性[37]。

（三）主要國家亦多制定相仿規範

綜觀國際近年涉及資通安全的法制政策，主要國家多以制定專法之方式針對資通安全議題進行規範。除前已述及的美國「聯邦資訊安全現代化法」，其他重要關聯立法還包括日本在 2014 年制定「網路安全基本法」、德國在 2015 年通過「資訊科技安全法」、韓國資訊安全署在 2016 年提出「資訊與通訊基礎設施保護法」（Laws on the Internet and Information Security of Korea）、中國大陸在 2017 年制定實施「網絡安全法」，英國於 2018 年發布之「電子通訊網路與資訊系統規則」（The Network and Information Systems Regulations 2018）及 2019 年新加坡制定「網路安全法」等。

而在國際組織方面，歐盟亦曾訂定「網路與資訊系統安全指令」（Directive on Security of Network and Information Systems, NIS Directive），透過專法之制定，協助公務機關及關鍵基礎設施提供者等非公務機關，認知自身資通安全責任、進而理解並因應資通安全風險，增進自身資通安全能力。

---

36 (i) carry out the Chief Information Officer's responsibilities under this section;
(ii) possess professional qualifications, including training and experience, required to administer the functions described under this section;
(iii) have information security duties as that official's primary duty; and
(iv) head an office with the mission and resources to assist in ensuring agency compliance with this section;

37 (5) ensure that the agency Chief Information Officer, in coordination with other senior agency officials, reports annually to the agency head on the effectiveness of the agency information security program, including progress of remedial actions;

五、非公務機關層面之「資訊安全長」設置規範分析

（一）「金融資安行動方案」提出設置「高階資安長」構想

資訊安全受到主要國家共同重視，也逐步成為近年國內各界強調的事項。除公務機關外，在非公務機關部分亦日益重視資訊安全專責人員之設置，並基此進一步要求應設置資訊安全長。特別是就「金融機構」而言，資訊安全同時涉及法令遵循、內稽內控以及風險管理等多重因素，成為金融機構業務發展上的關鍵事項。在正式推動金融機構「資訊安全長」前，要求配置「適當資訊安全人力資源」在國內金融界已行之有年。

考量資訊安全的重要性日益提升，金管會在 2020 年 8 月發布「金融資安行動方案」，以推動安全便利不中斷的金融服務為主要目標。金管會於方案中提出「強化資安監理」、「深化資安治理」、「精實資安韌性」及「發揮資安聯防」四大構面，並具體提列 36 項執行措施[38]。其中在「強化資安監理」部分，具體執行措施包括「型塑金融機構重視資安的組織文化」，此項並細分為：1. 增進經營階層對資安的監督職能；及 2. 定期檢視資安風險因子與金融監理工具連結之有效性[39]。

針對增進經營階層對資安的監督職能，「金融資安行動方案」表明「要求金融機構應成立資安專責單位並將資安辦理情形定期提報董事會，惟為再提升其對資安議題之決策能量，推動增設『高階資安長』統籌資安政策推動協調與資源調度，直接向董事會報告；並增納專業人員參與董事會運作，特設董監事資安課程，以增進對資安情勢掌握並實質將資安議題納入經營決策考量因子，帶動機構重視資安的組織文化」，

38 金融監督管理委員會編，金融資安行動方案，頁 14，金融監督管理委員會，2020 年 8 月。

39 同前註，頁 15。

要求金融機構應於其管理階層設置「高層資安長」，加強要求所謂的「內部控制三道防線」之落實，結合由外而內、從上而下的推升力道，內化資安監理思維，以進而型塑重視資安的組織文化[40]。

金管會「金融資安行動方案」中有關「資訊安全長」之推動

構面	工作項目	工作小項	執行措施	執行期程	說明
強化資安監理	型塑金融機構重視資安的組織文化	增進經營階層對資安的監督職能	（1）推動一定規模金融機構或純網銀設置資安長	二年	參考美國 NYDFS、歐盟 EBA 等要求金融機構應獨立資安職能、指定資安長及向經營階層（董事會）報告與問責等政策方向，本會雖已要求金融機構應成立資安專責單位並將資安辦理情形定期提報董事會，惟為再提升其對資安議題之決策能量，推動一定規模金融機構或純網銀設置高階資安長（副總經理，得兼任）統籌資安政策推動協調與資源調度，向董事會報告，並增納專業人員參與董事會運作，辦理董監事資安課程，增進董事會成員對資安情勢掌握並實質將資安風險納入經營決策考量，帶動重視資安的組織文化。
			（2）鼓勵遴聘具資安背景之董事、顧問或設置資安諮詢小組	二年	
			（3）開辦董監事資安教育訓練專設課程	一年	

資料出處：金管會「金融資安行動方案」（2020）

（二）「金融資安行動方案 2.0」擴大資訊安全長之設置要求

繼 2020 年 8 月發布「金融資安行動方案」，為因應業務發展與科技

40　同前註，頁 11。

進步，持續提升金融機構資安防護能量，金管會持續審視金融科技發展趨勢、國內外資安情勢變化及實務運作情形，並參考國際資安監理政策，於 2022 年 12 月再度發布「金融資安行動方案 2.0」，促使金融資訊安淨可得持續精進，並以擴大適用、落實與深化及鼓勵前瞻作為持續精進方向，訂定達 40 項重要措施[41]。

針對「金融資安行動方案 2.0」的重點，金管會首先即指出係「擴大資安長設置，定期召開資安長聯繫會議」，對此，金管會表示自「金融資安行動方案」發布後，修訂各業別內部控制規範，要求銀行及一定規模以上金融機構設置副總經理層級以上之資安長。考量電子交易達一定比例者，其資安防護對整體營運影響亦高，爰併納入推動設置資安長範圍，統籌資安政策推動協調與資源調度。另為強化資安長職責，規劃另定期辦理資安長聯繫會議，就當前資安情勢、推動策略及關鍵議題等共同研商，並增進金融機構間交流與聯防[42]。

析言之，我國於 2011 年 9 月間陸續修正「金融控股企業及銀行業內部控制及稽核制度實施辦法」、「保險業內部控制及稽核制度實施辦法」及「證券暨期貨市場各服務事業建立內部控制制度處理準則」，並發布相關令釋，要求銀行業及符合一定條件之保險企業、證券期貨各服務事業，應於 2022 年 3 月底前指派副總經理以上或職責相當之人兼任資訊安全長，綜理資訊安全政策推動及資源調度事務。而截至 2022 年第 3 季為止，已有 40 家本國銀行、21 家證券商及 12 家保險企業，共計 73 家金融機構設置副總經理層級以上之資訊安全長[43]。

---

41 金融監督管理委員會，金管會發布「金融資安行動方案 2.0」，引導金融資安持續精進，https://www.fsc.gov.tw/ch/home.jsp?id=96&parentpath=0,2&mcustomize=news_view.jsp&dataserno=202212270001&dtable=News（最後瀏覽日期：2023 年 6 月 12 日）。

42 同前註。

43 金融監督管理委員會編，金融資安行動方案 2.0，頁 12，金融監督管理委員會，2022 年 12 月。

金管會「金融資安行動方案 2.0」中有關「資訊安全長」之推動

構面	工作項目	工作小項	執行措施	執行期程	說明	與 1.0 關聯性
強化資安監理	型塑金融機構重視資安的組織文化	增進經營階層對資安的監督職能	（1）推動一定規模或電子交易達一定比例之金融機構設置資安長	2024 年	參考美國 NYDFS、歐盟 EBA 等要求金融機構應獨立資安職能、指定資安長及向經營階層（董事會）報告與問責等政策方向，本會繼要求金融機構應成立資安專責單位並將資安辦理情形定期提報董事會後，為再提升其對資安議題之決策能量，推動要求一定規模金融機構或純網銀設置副總經理層級以上之資安長，統籌資安政策推動協調與資源調度，向董事會報告，並增納專業人員參與董事會運作，辦理董監事資安課程，增進董事會成員對資安情勢掌握並實質將資安風險納入經營決策考量，帶動重視資安的組織文化。	擴大適用
			（2）鼓勵遴聘具資安背景之董事、顧問或設置資安諮詢小組	持續		延續
			（3）開辦董監事資安教育訓練專設課程	持續		延續
			（4）辦理資安長聯繫會議	2023 年		新增

資料出處：金管會「金融資安行動方案 2.0」（2022）

（三）後續推動情形觀察

1. 金融控股企業及銀行業內部控制及稽核制度實施辦法之修正

以根據金融控股企業法第 51 條、銀行法第 35 條之 1 第 1 項、信用合作社法第 21 條第 1 項、票券金融管理法第 43 條及信託業法第 42 條

第 3 項受權制定的「金融控股企業及銀行業內部控制及稽核制度實施辦法」為例，辦法第 3 條第 1 項規定「金融控股企業及銀行業應建立內部控制制度，並確保該制度得以持續有效執行，以健全金融控股企業（含子企業）與銀行業經營」，同條第 2 項同時要求「金融控股企業（含子企業）與銀行業應規劃整體經營策略、風險管理政策與指導準則，並擬定經營計畫、風險管理程序及執行準則」。

為落實上述規定，辦法第 38 條復規定「銀行業之風險控管機制應包括下列原則：一、應依其業務規模、信用風險、市場風險與作業風險狀況及未來營運趨勢，監控資本適足性。二、應建立衡量及監控流動性部位之管理機制，以衡量、監督、控管流動性風險。三、應考量整體曝險、自有資本及負債特性進行各項資產配置，建立各項業務風險之管理。四、應建立資產品質及分類之評估方法，計算及控管大額暴險，並定期檢視，覈實提列備抵損失。五、應對業務或交易、資訊交互運用等建立資訊安全防護機制及緊急應變計畫」，明文納入建置「資訊安全防護機制」之要求。

有鑑於資訊風險日益升高，金管會為強化企業資訊安全管理，修正「金融控股企業及銀行業內部控制及稽核制度實施辦法」並增訂第 38 條之 1 規定。依新設規定，「銀行業應指派副總經理以上或職責相當之人兼任資訊安全長，綜理資訊安全政策推動及資源調度事務。設置資訊安全專責單位及主管，不得兼辦資訊或其他與職務有利益衝突之業務，並配置適當人力資源及設備。但主管機關對信用合作社及票券金融企業另有規定者，依其規定。

銀行業前一年度經會計師查核簽證之資產總額達新臺幣一兆元以上者，應設置具職權行使獨立性之資訊安全專責單位，並指派協理以上或職責相當之人擔任資訊安全專責單位主管。

銀行業資訊安全專責單位負責規劃、監控及執行資訊安全管理作業，每年應將前一年度資訊安全整體執行情形，依第 27 條第 1 項規定

辦理內部控制制度聲明書之出具、揭露及公告申報，並由資訊安全長聯名出具。

銀行業資訊安全專責單位人員，每年至少應接受十五小時以上資訊安全專業課程訓練或職能訓練。總機構、國內外營業單位、資訊單位、財務保管單位及其他管理單位之人員，每年至少須接受三小時以上資訊安全宣導課程。

中華民國銀行商業同業公會全國聯合會、有限責任中華民國信用合作社聯合社及中華民國票券金融商業同業公會應訂定並定期檢討資訊安全自律規範。

適用第二項規定之銀行業，應於符合適用條件起六個月內調整」。

金管會指出上述有關修正規定，係參考美國紐約州金融署發布之「金融服務業網路安全規範」（Part 500）相關規定，增要求銀行業資訊安全專責單位應將資訊安全整體執行情形提報董事會，並由資訊安全專責單位主管與董事長、總經理、總稽核聯名出具資訊安全聲明書。而資訊安全整體執行情形的內容，至少應包括依據資訊安全防護機制與緊急應變計畫等執行情形，以及相關同業公會所訂資訊安全規範之遵循情形[44]。

2. 分階段及分級推動之「資訊安全長」新制

在修正「金融控股企業及銀行業內部控制及稽核制度實施辦法」並增訂第 38 條之 1 規定下，金管會基此分階段要求國內上市及上櫃企業應設立資訊安全單位。金管會在 2021 年 12 月 28 日修正「公開發行企業建立內部控制制度處理準則」，依修正後準則第 9 條之 1 第 1 項規定「公開發行企業應配置適當人力資源及設備，進行資訊安全制度之規

44 行政院公報資訊網，金融控股企業及銀行業內部控制及稽核制度實施辦法部條文修正說明，頁 21，https://gazette.nat.gov.tw/EG_FileManager/eguploadpub/eg024060/ch04/type1/gov36/num10/images/AA.pdf（最後瀏覽日期：2023 年 6 月 12 日）。

劃、監控及執行資訊安全管理作業。符合一定條件者，本會得命令指派綜理資訊安全政策推動及資源調度事務之人兼任資訊安全長，及設置資訊安全專責單位、主管及人員」，同條第 2 項並規定「前項一定條件，由本會定之」。

基於上述規定，金管會將上市（櫃）企業依其收入規模分成三級，以循序漸進方式推動包括資安長在內的資通安全管控機制，並要求下列三類事業，應在 2022 年底前指派資訊安全長並設置資訊安全單位，包含資訊安全專責主管及至少兩名資訊安全專責人員，分別為：

（1） 實收資本額達新臺幣 100 億元以上之上市（櫃）企業；

（2） 前一年底屬於臺灣 50 指數成分之上市（櫃）企業；

（3） 主要經營電子商務媒介商品或服務之上市（櫃）企業。

金管會證券暨期貨管理局指出截至 2022 年 4 月底為止，國內計有 113 家上市（櫃）企業符合指出上述三類條件。

第二階段則是前者三類以外之其餘上市櫃企業，除最近三年稅前純益連續虧損或最近一年度每股淨值低於面額者外，應於 2023 年底前配置資訊安全主管及資訊安全人員。

分級	分級標準	資安單位暨人力編制	實施時程
第一級	符合下列條件之一者： 1. 資本額 100 億元以上 2. 前一年底屬臺灣 50 指數成分企業 3. 藉電子方式媒介商品所有權移轉或提供服務（如電子銷售平臺、人力銀行等）收入占最近年度營業收入達 80 %以上，或占最近二年度營業收入達 50 %以上者	應設資安長及設置資安專責單位（包含資安專責主管及至少 2 名資安專責人員）	2022 年底設置完成
第二級	第一級以外之上市（櫃）企業，最近三年度之稅前純益未有連續虧損，且最近年度財務報告每股淨值未低於面額者	資安專責主管及至少 1 名資安專責人員	2023 年底設置完成
第三級	第一級以外上市（櫃）企業，最近 3 年度稅前純益有連續虧損，或最近年度每股淨值低於面額	至少 1 名資安專責人員	鼓勵設置

六、小結

在跨入數位時代後，數位經濟已成為各國經濟發展重心，而近期的COVID-19 疫情更促使各行各業競相投入數位轉型，不分傳統產業或數位化事業，各個產業如今都與數位科技高度相關，使得「資訊安全」成為當前企業治理上的重要環節。

隨著網際網路及資通科技快速發展與普及，資通科技相關應用，已被世界各國視為協助產業經濟轉型、提升國家競爭力及有效解決社會發展議題的關鍵，各國亦紛紛致力於資通政策的規劃，以期建構公開及有效率的數位環境，藉由科技化服務，提升民眾生活品質、維護公共利益、帶動產業發展及國家整體競爭力。惟網路給人們日常生活帶來便利的同時，貫通系統或服務的應用所引發之網路犯罪、個人資料保護等資通安全課題，也逐漸成為影響社會安定與國家安全之隱憂[45]。在此一背景及發展趨勢下，設置「資訊安全長」開始成為公、私部門因應資訊安全問題的重要對策。

伴隨新興科技引發的嶄新網路安全問題，近年國際組織及主要國家無不採取更為嚴謹的保護資通安全政策，先進國家已將各種資訊安全議題提升至國家安全層次，並制定專門立法加以規範。各國透過專法之制定，得以採取適當法律手段，以逐步提升資通安全能量及協助關鍵基礎設施提供者在內之非公務機關，其營運或提供之服務，得以認知自身資通安全責任與因應資通安全風險，增進自身資通安全能力。而相關要求事項中，即包括要求設置「資訊安全長」。

資訊安全長除了掌握關鍵技術，從而使得企業具備韌性、營運不中斷外，也要擺脫以往資訊安全長僅執行稽核檢視的舊觀念。現代的資訊安全長打造一個立體呈現網路安全的資安建築藍圖，不僅要納入企業合作的上、中、下游廠商，也必須搭配企業的組織架構、管理制度和相關

45 同註 31。

技術，甫能建構完整的資訊安全體系[46]。由於金融業向為受到高度監管的產業，我國諸多資訊安全法制政策規範，往往都是在金融業試行後，再廣泛推動至其他產業，因此金管會在「金融資安行動方案 2.0」所揭示、包括資訊安全長設置要求與推動重點，也可以作為其他產業思考有無必要設置資訊安全長時之參考。

參、隱私長（個人資料保護官）機制之對照觀察

一、個人資料外洩事件頻傳帶動保護需求

（一）國際指標性個案

知名軟體公司 Intact 分析 2004 年後用戶個人資料外洩超過 3 萬筆之事件，研究發現網路使用者個人資料外洩最為嚴重的年度為 2011 年，其次分別是 2013 年與 2019 年。而導致用戶個人資料發生外洩情形的主要原因，包括遭到駭客入侵、資安防護意識欠佳以及用戶個人資料儲存裝置遭到盜取或發生遺失等情形[47]。

若以「個別企業」而言，無論是統計期間的資料外洩次數，或是外洩資料筆數，最多者均為 Facebook，總計發生 5 次大規模用戶個人資料外洩情形，並外洩高達 8.645 億筆用戶個人資料。其次分別是 Marriott International 外洩用戶個人資料 5.052 億筆、MongoDB 外洩 4.77 億筆、AOL 外洩 9,200 萬筆以及 JP Morgan Chase 外洩 7,860 萬筆個人資料[48]。

Business Insider 在 2021 年 4 月指出社交媒體平臺 Facebook 逾 5 億的用戶個人資料被公開於駭客論壇，遭到洩露的資料包括了用戶的

46 同註 15。

47 Intact, *Visualising the Biggest Data Breaches in History*, *available at* https://www.intactsoftware.com/blog/visualising-biggest-data-breaches-history/ (last visited June 12, 2023).

48 *Id.*

Facebook 帳號、姓名、所在國家／地區、電話號碼及電子郵件等，而受害用戶更遍及 106 個國家。總數達 5.33 億的外洩用戶個人資料，包括 3,200 萬美國用戶、1,100 萬英國用戶及 600 萬印度用戶，甚至 Facebook 創辦人 Mark Zuckerberg 的個人電話號碼也遭到外洩[49]。

事實上 Facebook 已多次發生用戶個人資料洩露事件及不當利用用戶個人資料爭議。Facebook 曾將 8,000 萬用戶數據與劍橋分析公司（Cambridge Analytica）進行分享，而後者則將這些數據用於 2016 年美國大選政治廣告，嚴重違反了 Facebook 的服務條款。Mark Zuckerberg 承認對此事負有責任並道歉。隨後，美國聯邦貿易委員會（Federal Trade Commission）對此事展開調查，並對 Facebook 開出 50 億美元罰單[50]。

（二）國內近期案例

個人資料外洩事件在我國時有所聞，而近期更是受到各界矚目。2023 年 1 月媒體報導駭客於國外網路論壇披露華航會員個人資料，先後於 2023 年 1 月 4 日和 1 月 11 日，陸續釋出 10 筆和 50 筆、總計 60 筆涵蓋政界、商界與藝能界等知名人士個人資料，而遭到外洩的個人資料除華航會員編號外，還包括中英文姓名、出生年月日、電子郵件與手機號碼等[51]。

和泰汽車旗下共享汽機車平臺 iRent 於 2023 年 1 月出現個資外洩事件，由於資料庫超過 9 個月未進行加密，在任何人均能自由查閱下，導致至少 10 萬名客戶的個人資料，包括身份證明文件、信用卡號碼簽名與租車情況等遭到外洩，交通部公路總局清查發現 iRent 外洩多達 40

49 Aaron Holmes, *533 million Facebook users' phone numbers and personal data have been leaked online, available at* https://www.businessinsider.com/stolen-data-of-533-million-facebook-users-leaked-online-2021-4 (last visited June 12, 2023).

50 *Id.*

51 黃立偉，華航 60 筆會員個資遭駭客公布　清查與資料庫不盡相符，https://news.pts.org.tw/article/618913（最後瀏覽日期：2023 年 6 月 12 日）。

萬筆個人資料，依個人資料保護法處罰新臺幣 20 萬元[52]。

二、各國個人資料保護立法普遍受歐盟 GDPR 影響

（一）各國近期立法深受歐盟影響

在個人資料外洩事件頻傳下，各國無不開始重視個人資料保護立法，著手制定或修訂相關法制。而當前國際可見的個人資料保護立法，幾無例外地均受到歐盟 GDPR 的影響。

過去多年因為物聯網（The Internet of Things）和大數據（Big Data）等新興科技的發展，規範需求日增，歐盟在 2012 年 1 月提出 GDPR 草案，嘗試將歐盟既有的 1995 年的個資保護指令（Data Protection Directive 95/46/EC）、歐盟 ePrivacy 保護指令和歐盟 Cookies 指令等數者予以整合，建立起更為完整嚴謹的個人資料保護法制，最終達成 GDPR 此一成果[53]。

歐盟 GDPR 除普遍適用於 28 個歐盟會員國，對會員國政府與人民有全面拘束力之法律效果。另外根據歐洲經濟區（European Economic Area, EEA）協定第 7 條規定，非歐盟會員國之冰島，列支敦士登和挪威，亦應適用 GDPR。而近期國際法制發展更顯示在 GDPR 正式實施後，主要國家針對個人資料保護立法所展開的制定或修正工作，幾近全數受到歐盟 GDPR 之深遠影響[54]。

---

52 數位時代，iRent 個資外洩，公總罰 20 萬、新北交通局也罰 9 萬！為何引發 40 萬用戶資安危機？，https://www.bnext.com.tw/article/73974/hota-irent-customer-data-exposed-response-security-information（最後瀏覽日期：2023 年 6 月 12 日）。

53 劉靜怡，淺談 GDPR 的國際衝擊及其可能因應之道，月旦法學雜誌，第 286 期，頁 6，2019 年 3 月。

54 PAUL CRAIG & GRÁ INNE DE BÚ RCA, THE EVOLUTION OF EU LAW 932-933 (2021).

（二）歐盟 GDPR 之重點

1. 一套調適而統一的法律框架

GDPR 係採取「規則」（Regulation）位階，不僅促進了規範層面的一體適用，亦可望助益歐盟單一數位市場（Digital Single Market）之推動。GDPR 將解決現行資料保護指令於歐盟成員國之間執行狀況分歧的情形，確保新法於所有成員國適用上的一致性。GDPR 並引進備受矚目的「一站式機制」（One Stop Shop），執委會（European Commission）指出此舉將有助於企業節省 27 億歐元、用於與隱私主管機關往來的費用支出[55]。

GDPR 在體制上採取歐盟法中的「規則」此種規範型態，也就是直接透過歐洲議會（European Parliament）與歐盟理事會（European Council）決議通過的「規則」立法模式，不必再經過歐盟各會員國內國法的轉換，直接對各會員國產生拘束力，以便調和歐盟各會員國之間彼此分歧的法律規定，一則減輕私部門的法規遵循成本，再則也進一步強化個人的資訊自主控制權[56]。

2. 提供於歐盟市場實際運作的所有企業均屬公平之競爭環境

GDPR 要求歐盟以外的企業，若該企業所提供的商品或服務涉及歐盟區域內的個人資料或針對特定個人進行監測，即必須與歐盟境內企業適用相同的規範。設立於歐盟境外、但於歐盟境內存在實際活動的企業，其在特定情形下必須於歐盟境內任令一名代表，以利歐洲公民及隱私主管機關與之接觸或代表其位於境外的企業[57]。

---

55 郭戎晉，自歐盟執委會及成員國視角談一般資料保護規則（GDPR）之實施與課題，科技法律透析，第 30 卷，第 4 期，頁 28-29，2018 年 4 月。

56 劉靜怡，同註 53，頁 6。

57 同前註，頁 29。

3. 強化個人資料處理行爲之要求

1995 年歐盟個資保護指令對於同意的要求，並未明確規定是「明示」或「默示」，但 GDPR 的規範方向，則是強化資料主體之同意。根據 GDPR 的第四條規定，先要求同意必須符合由資料主體自主授予（Freely Given）、具體（Specific）、知情（Informed）以及明確（Unambiguous）的條件，方能取得並處理個人資料，尤其是針對敏感性資料（Sensitive Data），GDPR 則是特別要求必須明確清楚（Explicit）。其次，GDPR 本條規定也要求資料主體的同意方式，必須以「聲明」（Statement）方式為之，或是以「清楚的積極行為」（Clear Affirmative Action）為之。而且，資料控制者必須負擔證明已取得資料主體同意的責任，若是資料主體保持沉默、未表示意見或無作為等情形，自然皆不構成前述「同意」[58]。

4. 導入隱私設計及隱私預設概念

考量商業服務型態及科學技術應用日新月異，歐盟期待藉由導入「隱私設計」（Privacy by Design）及「隱私預設」（Privacy by Default）要求，建立嶄新的個人資料保護原則，以利於產品或服務發軔之際，即力求採行創新解決方案對應嗣後可能出現的隱私保護問題[59]。

GDPR 前言第 78 點特別提及上述兩項要求，要求資料控制者應該採取合乎上述原則的內部政策或措施，以便落實個人資料保護的要求，這也是過去歐盟個資保護指令中並未特別明文化的個資保護要求。同時，GDPR 的第 25 條也進一步落實上述資料保護設計制度，規定「考量現有技術、資料處理成本、性質、範圍、脈絡和處理目的，以及資料處理對自然人的權利和自由帶來的不同可能性和嚴重程度的風險，資料控制者應在決定處理方式和進行處理的同時，以有效之方式，採取例如

58 同前註，頁 7。

59 郭戎晉，同註 55，頁 29。

匿名化等適當技術和組織措施，為實現資料最小化等資料保護原則而設計的適當技術性與組織性措施，並在處理中融入必要保障，以符合本規則要求與保護資料主體權利」。上述規定，可以說是進一步充實了資料控制者與處理者的資料保護義務內涵[60]。

5. 更爲強化的個人權利保障

GDPR 導入全新的透明度（Transparency）要求，強化本人所享有的知情、訪問及刪除（包括被遺忘權的導入）等權利；新制同時要求同意必須出於明確且肯定地傳達同意的行為，並強化兒童於網路環境下的隱私保護。規則前言特別強調「緘默」及「不為表示」等過往實務慣行的預設同意作法，將不再被視為有效之同意[61]。

被遺忘權或刪除權的明文化，是 GDPR 相當值得注意的重點。GDPR 增加被遺忘權此一權利的目的，在於賦予資料主體更有效地控制其個人資料的權利基礎，但是，這個權利，也更凸顯出歐洲與美國兩者在資料刪除此一課題上的不同立場。在 1995 年歐盟個人資料保護指令中，其實已經規範了資料主體可要求查閱、複製資料控制者所擁有的個人資料的權利，倘若個人資料不正確或不完整時，資料當事人即可要求就其個人資料予以更正、刪除或封鎖。GDPR 則是更進一步地針對被遺忘權予以更為明確的規範，也就是除了資料不正確或不完整時，可行使上述權利外，當滿足該條所列其他理由時，資料主體亦有權要求資料管理者在無不當延誤的情況下，刪除其個人資料[62]。

6. 賦予本人對個人資料享有更大的自主掌控權

GDPR 創造「資料可攜」（Data Portability）此一全新的權利概念，允許公民有權向企業或機構要求提供其立於當事人同意或契約基礎上

60 劉靜怡，同註 53，頁 12-13。
61 郭戎晉，同註 55，頁 29-30。
62 劉靜怡，同註 53，頁 11。

自本人取得的個人資料，同時允許在技術互通的前提下，要求將個人資料移轉至另一企業或機構。新法同時支持個人資料於歐盟境內的自由移轉，避免資料本身的「鎖死」（lock-in）情事，此舉將有助於企業之間的良性競爭，進而催生更多的嶄新應用[63]。

在資料大量產製與處理的時代，「資料所有權」（Data Ownership）歸屬，是常見的爭議。GDPR 規定的特色，除了對資料控制者與處理者的規範更加嚴格之外，也同時賦予使歐盟公民針對自己的個人資料，可以擁有更高的自主權，而個資自主權的最新落實方式之一，則包括「資料可攜」此一過去未曾明文化的權利，規定於 GDPR 第 20 條之中。簡言之，所謂資料可攜權，就是指資料主體可以行使在不同服務提供者之間移動個資的權利，例如網路用戶可以將其個人資料和其他相關資料，例如從某一個網路服務供應商（ISP）轉移至另外一個 ISP[64]。

7. 對應資料外洩問題更強而有力的保護機制

GDPR 制定一套對應個人資料事故的全面性規範，除明確界定何謂個資事故，並明訂當事故發生並對本人權利與自由構成危害時，業者負有最遲應於 72 小時內通知隱私主管機關之義務。另於特定情況下，其亦須主動通知個資事故所涉及的相關利害關係人[65]。

相對地，在個資外洩時所產生的對資料主體之通知義務，首先必須符合第 34 條第 1 項之「可能導致自由或權利的高度風險」，方啟動通知程序，第 34 條第 3 項並規定三種可以豁免通知的事由，亦即通知義務和資料管理者負擔之間，嘗試取得平衡[66]。

63 郭戎晉，同註 55，頁 29-30。
64 劉靜怡，同註 53，頁 10。
65 郭戎晉，同註 55，頁 29-30。
66 劉靜怡，同註 53，頁 10。

8. 賦予歐盟所有隱私主管機關處罰之權

GDPR 使歐盟所有的隱私主管機關均有權對資料蒐集者與處理者處以罰金，在現行指令之下，並非所有隱私主管機關均享有該等權利，此一變革將有助於各成員國更有效率地執行及落實 GDPR。新規下的罰鍰最高將達到 2,000 萬歐元或系爭企業全球年營業額的 4 %，並以二者較高者為準[67]。

9. 明確化責任條款，促使資料控制者及處理者擁有更大的操作彈性

執委會指出 GDPR 已由指令的「通知制度」（System of Notification）轉變為所謂的「問責原則」（Principle of Accountability），並將根據風險的高低執行一套富有彈性之義務／責任要求。GDPR 導入一項新興工具：資料隱私衝擊分析（Data Protection Impact Assessment, DPIA），助益於進行個人資料處理行為之前詳細評估潛藏的風險；新制並明確化資料處理者所負責任，以及控制者於選擇處理者時所應擔負之責[68]。

三、應否設置隱私長／個人資料保護官機制受到重視

（一）歐盟 GDPR 之個人資料保護官設計廣泛影響各國立法

歐盟 GDPR 的嚴格規範與高額處罰設計，使得各國公、私部門均審慎看待該法的遵循工作。根據 Veritas 在 GDPR 正式生效前所作調查，86 %的企業擔心未遵守 GDPR 規定將對其業務產生重大影響，其中更有 20 %企業擔憂若未能符合要求恐將造成企業面臨高額處罰甚至因而破產。Veritas 所作調查同時指出 GDPR 嚴峻規定使得事業因此支出的法

67 郭戎晉，同註 55，頁 30。

68 同前註，頁 30-31。

遵費用平均達到 130 萬歐元，恐非財力相對有限的中小企業所能負擔[69]。

歐盟 GDPR 的重要設計，包括：1. 適用事項範圍；2. 法域適用範圍；3. 適用之客體、行為及相關主體；4. 個資保護基本原則；5. 控管者（蒐集主體）及處理者（受託者）義務；6. 個人資料主體權利；7. 個人資料之跨境傳輸規範；8. 有關請求損害賠償救濟與行政裁罰規範等，無不實質影響各國法制設計[70]。

另一受到重視的設計，則是「個人資料保護官」（個人資料保護官）的設置要求，以 GDPR 為例，該法第 37 條明訂應指定個人資料保護官的三種情形，包括：1. 公務機關（不包括行使司法權之法院）；2. 核心業務涉及定期且系統性地大規模監控資料主體之資料控制者或處理者；3. 核心業務涉及大規模處理特種個人資料之資料控制者或處理者。除應指定個人資料保護官之情形，GDPR 亦詳加規定個人資料保護官之資格／職能、個人資料保護官所負職責與獨立性要求，並針對個人資料保護官有關事項發布實務操作指引。

GDPR 面臨數據資料全球化現象，擴大法域適用範圍和增設多層次之權利義務規定，讓我國個人資料保護法於進行解釋及修法活動，有豐沛之外國立法例足供參考。惟我國也面臨各種智慧型手機、APP 軟體、生物特徵辨識、雲端服務、大數據分析、物聯網、人工智慧技術（機器人、自動駕駛）等等科技應用成果，出現於各種政府服務或商業應用領域，甚至已形成所謂的數位經濟（Digital economy），伴隨產生個人資料保護與管理議題之解決方案需求，讓我國個人資料保護法的成長，更需借鏡 GDPR 法制之實踐經驗[71]。若可藉由參考歐盟法制並導入個人資料

69 VERITAS, THE VERITAS 2017 GDPR REPORT 2 (2017) *available at* https://m.moam.info/the-veritas-2017-gdpr-report_647a3ed8097c4768028c9379.html?utm_source=slideleged end (last visited June 12, 2023).

70 Michael L. Rustad & Thomas H. Koenig, *Towards a Global Data Privacy Standard*, 71 FLA. L. REV. 365, 390-393 (2019).

71 李世德，GDPR 與我國個人資料保護法之比較分析，臺灣經濟論衡，第 16 卷，

保護官機制，不僅有助於臺灣獲得歐盟 GDPR 的適足性認定資格，對於我國應如何重新整備既有的個人資料保護法制與實務運作，也可望將帶來助益。

（二）個人資料保護官在我國之相關推動倡議

我國於 2022 年 5 月發布「國家人權行動計畫」，國家人權行動計畫所提出優先推動的八大議題中，包括強調個人資料保護的「數位人權」[72]，國家人權行動計畫同時指出現時已有國際個人資料立法要求公務機關及非公務機關應設置「個人資料保護官」（Data Protection Officer，以下簡稱個人資料保護官），未來我國個人資料保護法（以下簡稱個人資料保護法）是否有增設個人資料保護官機制之必要，將於個人資料保護法修法時一併研議[73]。

我國個人資料保護法與歐盟 GDPR 皆師承「經濟合作暨發展組織」（Organisation for Economic Cooperation and Development, OECD）的個人資料保護八大原則，而我國個人資料保護法的研修過程，不少條文意旨係參考 GDPR 前身之歐盟資料保護指令（Directive 95/46/EC4）的相關規定，故 GDPR 與我國個人資料保護法比較分析時，將可發現二者具有相似之處[74]。另一方面，為與國際個人資料保護水平接軌，我國刻正評估取得歐盟執委會適足性認定資格並積極檢討個人資料保護法相關規定之修正必要[75]。

基此，無論是自我國個人資料保護法之立法沿革，或是就與歐盟法制接軌角度而言，國內實有必要考慮參考歐盟 GDPR 中有關個人資料保

第 3 期，頁 93，2018 年 9 月。

72 行政院編，國家人權行動計畫，頁 14，行政院，2022 年 5 月。

73 同前註，頁 88。

74 李世德，同註 71，頁 70。

75 國家發展委員會，歐盟對台歐展開 GDPR 適足性對話表示歡迎，https://www.ndc.gov.tw/nc_27_32174（最後瀏覽日期：2023 年 6 月 12 日）。

護官之設計，並評估導入國內之必要性。

四、我國個人資料保護法相關規定之觀察

（一）公務機關

個人資料保護法第 18 條規定「公務機關保有個人資料檔案者，應指定專人辦理安全維護事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏」，基於本條規定，所有公務機關均負依設置「專人」負責個人資料保護法相關要求之義務。

個人資料保護法施行細則第 25 條進一步規定「本法第 18 條所稱專人，指具有管理及維護個人資料檔案之能力，且足以擔任機關之個人資料檔案安全維護經常性工作之人員」。「公務機關為使專人具有辦理安全維護事項之能力，應辦理或使專人接受相關專業之教育訓練」。

另依「行政院及所屬各機關落實個人資料保護聯繫作業要點」[76]，為防止非公務機關個人資料檔案外洩，加強所屬中央目的事業主管機關對非公務機關個人資料保護之監管，以落實個資保護。

非公務機關個人資料檔案之安全維護。

（二）非公務機關

1. 國內合計 15 部中央目的事業個人資料保護法配套子法納入指定專人規定

非公務機關部分，個人資料保護法本身並未如公務機關直接明訂應指定「專人」辦理諸如第 18 條要求之事項，惟個人資料保護法第 27 條第 1 項規定「非公務機關保有個人資料檔案者，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏」，同條第 2 項及

76 行政院 110 年 8 月 11 日院授發協字第 1102001106 號函訂定。

第 3 項分別規定「中央目的事業主管機關得指定非公務機關訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法」;「前項計畫及處理方法之標準等相關事項之辦法，由中央目的事業主管機關定之」。

基於上述規定，國內各目的事業主管機關歷來依據個人資料保護法第 27 條第 3 項規定授權所制定之配套子法中，不乏明文要求「指派專人」辦理個人資料檔案安全維護等相關事項之例。現時國內依個人資料保護法第 27 條規定授權、明文規定所轄目的事業應指定專人之個人資料保護法子法（個人資料檔案安全維護管理辦法），現階段計有 15 部法規[77]。

2. 相關配套子法之指定專人規定分析

現階段國內共計 15 部中央目的事業個人資料保護法配套子法納入「指定專人」規定，其針對專人指定之設計與經指定之專人的具體要求分析如下：

（1）勞動部：人力仲介業個人資料檔案安全維護計畫及處理辦法

辦法第 4 條第 1 項規定「人力仲介業就個人資料檔案安全維護管理，應指定專人或建立專責組織負責，並配置相當資源。」

同條第 2 項進一步規定「前項專人或專責組織之任務如下：

一、訂定個人資料保護管理原則，將其所蒐集、處理及利用個人資料之依據、特定目的及其他相關保護事項公告，使其所屬人員瞭解。

二、規劃、訂定、修正及執行本計畫。

三、定期對所屬人員施以基礎認知宣導或專業教育訓練，使其瞭解個人資料保護相關法令規定、責任範圍、管理措施或方法。」

77 國家發展委員會，個人資料保護專區，https://pipa.ndc.gov.tw/News.aspx?n=39982462BE4D486C&sms=8D016F8982417771（最後瀏覽日期：2023 年 6 月 12 日）。

（2）勞動部：人力供應業個人資料檔案安全維護計畫及處理辦法

辦法第 4 條第 1 項規定「人力供應業者就個人資料檔案安全維護管理，應指定專人或建立專責組織負責，並配置相當資源。」

同條第 2 項進一步規定「前項專人或專責組織之任務如下：

一、規劃、訂定、修正及執行本計畫。

二、訂定個人資料保護管理原則，將其所蒐集、處理及利用個人資料之依據、特定目的及其他相關保護事項公告，使其所屬人員瞭解。」

（3）財政部：公益彩券發行機構個人資料檔案安全維護管理辦法

辦法第 3 條第 1 項規定「發行機構就個人資料檔案安全維護管理應指定專人或建立專責組織，並配置相當資源。」

同條第 2 項進一步規定「前項專人或專責組織之任務如下：

一、規劃、訂定、修正與執行本計畫及業務終止後個人資料處理方法等相關事項。

二、訂定個人資料保護管理政策，將其所蒐集、處理及利用個人資料之依據、特定目的及其他相關保護事項，公告使其所屬人員均明確瞭解。

三、定期對所屬人員施以基礎認知宣導或專業教育訓練，使其明瞭個人資料保護相關法令之規定、所屬人員之責任範圍及各種個人資料保護事項之方法或管理措施。

四、定期就執行任務情形向發行機構代表人或經其授權之人員提出書面報告。」

（4）財政部：保稅倉庫及物流中心個人資料檔案安全維護管理辦法

辦法第 3 條第 1 項規定「保稅倉庫及物流中心就個人資料檔案安全維護管理應指定專人或建立專責組織，並配置相當資源。」

同條第 2 項進一步規定「前項專人或專責組織之任務如下：

一、規劃、訂定、修正與執行本計畫及業務終止後個人資料處理方法等相關事項。

二、訂定個人資料保護管理政策，將其所蒐集、處理或利用個人資料之依據、特定目的及其他相關保護事項，公告使其所屬人員均明確瞭解。

三、定期對所屬人員施以基礎認知宣導或專業教育訓練，使其明瞭個人資料保護相關法令規定、所屬人員責任範圍及各種個人資料保護事項之方法或管理措施。

四、定期就執行任務情形向保稅倉庫及物流中心代表人或經其授權人員提出書面報告。」

（5）財政部：記帳士與記帳及報稅代理人個人資料檔案安全維護管理辦法

辦法第 3 條第 1 項規定「記帳士、記帳及報稅代理人就個人資料檔案安全維護管理應指定專人或建立專責組織，並配置相當資源。」

同條第 2 項進一步規定「前項專人或專責組織之任務如下：

一、規劃、訂定、修正與執行本計畫及業務終止後個人資料處理方法等相關事項。

二、訂定個人資料保護管理政策，將其所蒐集、處理或利用個人資料之依據、特定目的及其他相關保護事項，公告使其所屬人員充分瞭解。

三、定期對所屬人員施以基礎認知宣導或專業教育訓練，使其明瞭個人資料保護相關法令之規定、所屬人員之責任範圍及各種個人資料保護事項之方法或管理措施。

四、定期就執行前三款任務情形向記帳士、記帳及報稅代理人或其授權人員提出書面報告。」

（6）財政部：菸酒事業個人資料檔案安全維護管理辦法

辦法第 4 條第 1 項規定「菸酒事業就個人資料檔案安全維護管理應指定專人或建立專責組織，並配置相當資源。」

同條第 2 項進一步規定「前項專人或專責組織之任務如下：

一、規劃、訂定、修正與執行本計畫及業務終止後個人資料處理方法等相關事項。

二、訂定個人資料保護管理政策，將其所蒐集、處理及利用個人資料之依據、特定目的及其他相關保護事項，公告使其所屬人員均明確瞭解。

三、定期對所屬人員施以基礎認知宣導或專業教育訓練，使其明瞭個人資料保護相關法令之規定、所屬人員之責任範圍及各種個人資料保護事項之方法或管理措施。

四、定期就執行任務情形向菸酒事業代表人或經其授權之人員提出書面報告。」

（7）財政部：報關業個人資料檔案安全維護管理辦法

辦法第 3 條第 1 項規定「業者就個人資料檔案安全維護管理得指定專人或建立專責組織，並配置相當資源。」

同條第 2 項進一步規定「前項專人或專責組織之任務如下：

一、規劃、訂定、修正與執行本計畫及業務終止後個人資料處理方法等相關事項。

二、訂定個人資料保護管理政策，將其所蒐集、處理或利用個人資料之依據、特定目的及其他相關保護事項，公告使其所屬人員均明確瞭解。

三、定期對所屬人員施以基礎認知宣導或專業教育訓練，使其明瞭個人資料保護相關法令規定、所屬人員責任範圍及各種個人資料保護事項之方法或管理措施。

四、定期就執行任務情形向報關業代表人或經其授權人員提出書面報告。」

（8）交通部：民用航空事業個人資料檔案安全維護計畫及處理辦法

辦法第 3 條第 1 項規定「業者就個人資料檔案安全維護管理得指定專人或建立專責組織，並配置相當資源。」

同條第 2 項進一步規定「前項專人或專責組織之任務如下：

一、規劃、訂定、修正與執行本計畫及業務終止後個人資料處理方法等相關事項。

二、訂定個人資料保護管理政策，將其所蒐集、處理及利用個人資料之依據、特定目的及其他相關保護事項，公告使其所屬人員均明確瞭解。

三、定期對所屬人員施以基礎認知宣導或專業教育訓練，使其明瞭個人資料保護相關法令之規定、所屬人員之責任範圍及各種個人資料保護事項之方法或管理措施。」

（9）交通部：汽車運輸業個人資料檔案安全維護計畫及處理辦法

辦法第 4 條第 1 項規定「業者就個人資料檔案安全維護管理得指定專人或建立專責組織，並配置相當資源。」

同條第 2 項進一步規定「前項專人或專責組織之任務如下：

一、規劃、訂定、修正與執行本計畫，包括業務終止後個人資料處理方法等相關事項。

二、定期就執行情形向管理人報告。

三、依據稽核人員就執行之評核進行檢討改進，並向管理人及稽核人員提出書面報告。

四、訂定個人資料保護管理政策，將其所蒐集、處理及利用個人資料之依據、特定目的及其他相關保護事項，公告使其所屬人員均明確瞭

解。

五、定期對所屬人員施以基礎認知宣導或專業教育訓練，使其明瞭個人資料保護相關法令之規定、所屬人員之責任範圍及各種個人資料保護事項之方法或管理措施。」

（10）交通部：停車場經營業個人資料檔案安全維護計畫及處理辦法

辦法第 3 條第 1 項規定「停車場經營業就個人資料檔案安全維護管理，應指定專人或建立專責組織負責。」

同條第 2 項進一步規定「前項專人或專責組織之任務如下：

一、規劃、訂定、修正與執行維護計畫及業務終止後個人資料處理方法等相關事項，並定期向停車場經營業負責人報告。

二、訂定個人資料保護管理政策，將其所蒐集、處理及利用個人資料之依據、特定目的及其他相關保護事項，公告使其所屬人員均明確瞭解。

三、定期對所屬人員施以基礎認知宣導或專業教育訓練，使其明瞭個人資料保護相關法令之規定、所屬人員之責任範圍及各種個人資料保護事項之方法或管理措施。」

（11）交通部：船舶運送業個人資料檔案安全維護計畫及處理辦法

辦法第 3 條第 1 項規定「業者就個人資料檔案安全維護管理得指定專人或建立專責組織，並配置相當資源。」

同條第 2 項進一步規定「前項專人或專責組織之任務如下：

一、規劃、訂定、修正與執行維護計畫及業務終止後個人資料處理方法等相關事項。

二、訂定個人資料保護管理政策，將其所蒐集、處理及利用個人資料之依據、特定目的及其他相關保護事項，公告使其所屬人員均明確瞭解。

三、定期對所屬人員施以基礎認知宣導或專業教育訓練，使其明瞭個人資料保護相關法令之規定、所屬人員之責任範圍及各種個人資料保護事項之方法或管理措施。」

（12）教育部：私立高級中等以下學校及幼兒園個人資料檔案安全維護計畫實施辦法

辦法第 5 條規定「學校及幼兒園得指定或設管理單位，或指定專人，負責個人資料檔案安全維護；其任務如下：

一、訂定及執行安全維護計畫。

二、定期就個人資料檔案安全維護管理情形，向管理人提出書面報告。

三、依據稽核人員就安全維護計畫執行之評核，於進行檢討改進後，向管理人及稽核人員提出書面報告。」

（13）教育部：私立專科以上學校及私立學術研究機構個人資料檔案安全維護計畫實施辦法

辦法第 5 條規定「學校、機構得指定或設管理單位，或指定專人，負責個人資料檔案安全維護；其任務如下：

一、訂定及執行安全維護計畫，包括業務終止後個人資料處理方法。

二、定期就個人資料檔案安全維護管理情形，向管理人提出書面報告。

三、依據稽核人員就計畫執行之評核，於進行檢討改進後，向管理人及稽核人員提出書面報告。

（14）教育部：海外臺灣學校及大陸地區臺商學校個人資料檔案安全維護計畫實施辦法

辦法第 7 條規定「境外臺校得指定或設管理單位，或指定專人，負

責個人資料檔案安全維護；其任務如下：

一、訂定及執行安全維護計畫，包括業務終止後個人資料處理方法。

二、定期就個人資料檔案安全維護管理情形，向管理人提出書面報告。

三、依據稽核人員就計畫執行之評核，於進行檢討改進後，向管理人及稽核人員提出書面報告。

（15）行政院公共工程委員會：工程技術顧問業個人資料檔案安全維護計畫及處理辦法

辦法第 3 條第 1 項規定「顧問公司就個人資料檔案安全維護管理得指定專人或建立專責組織，並配置相當資源。」

同條第 2 項進一步規定「前項專人或專責組織之任務如下：

一、規劃、訂定、修正與執行維護計畫及業務終止後個人資料處理方法等相關事項。

二、訂定個人資料保護管理政策，將其所蒐集、處理及利用個人資料之依據、特定目的及其他相關保護事項，公告使其所屬人員均明確瞭解。

三、定期對所屬人員施以基礎認知宣導或專業教育訓練，使其明瞭個人資料保護相關法令之規定、所屬人員之責任範圍及各種個人資料保護事項之方法或管理措施。」

3. 個人資料檔案安全維護計畫辦法有關專人所負任務綜合比較

觀察上述 15 部個人資料保護法子法，經指定的專人所將承擔之任務，整體而言共有六款事項受到採納，分別為：

（1） 規劃、訂定、修正及執行個人資料保護計畫（安全維護計畫）；

（2） 訂定個人資料保護管理原則(管理政策)並公告使所屬人員瞭解；

（3） 規劃、訂定、修正與執行業務終止後個人資料處理方法；

（4） 定期對所屬人員施以基礎認知宣導或專業教育訓練；

（5） 定期就執行任務情形向代表人或經其授權之人員提出書面報告；
（6） 依據稽核人員就執行之評核進行檢討改進，並向管理人及稽核人員提出書面報告。

觀察我國個人資料保護法，個人資料保護法第 18 條規定公務機關應指定專人，同時特定公務機關基於中央目的事業主管機關所制定的 15 部個人資料保護法子法，亦負有指定專人之義務。但現行個人資料保護法中並未直接使用「個資保護官」用語。

五、現時主要國家立法中之有關規範分析

（一）個人資料保護官之設置

1. 歐盟

GDPR 規定資料控制者或資料處理者應指定個人資料保護官的三種情形：

（1） 從事個人資料處理行為之公務機關，但不包括行使司法權之法院；
（2） 依其本質、範圍及／或其目的，核心業務涉及定期且系統性地大規模監控資料主體之資料控制者或資料處理者；
（3） 核心業務涉及大規模處理特種個人資料之資料控制者或資料處理者[78]。

除上述三種特定情形，GDPR 另規定成員國亦得以法律明訂資料控制者或資料處理者應指定設置個人資料保護官之情形。若資料控制者或資料處理者違反 GDPR 的任命要求，即可能面臨 1,000 萬歐元或最高以全球營收 2 %計算之罰款[79]。

78 GDPR 第 37 條第 1 項。
79 GDPR 第 83 條。

2. 泰國

依泰國個人資料保護法規定，資料控制者或資料處理者於下述三種情形應指定個人資料保護官：

（1） 經個人資料保護委員會公告之公務機關；

（2） 經個人資料保護委員會公告，考量其個人資料蒐集、利用與揭露行為狀況而有定期監控其個人資料及系統必要性之資料控制者或資料處理者；

（3） 核心業務涉及依第 26 條規定蒐集、利用與揭露特種個人資料之資料控制者或資料處理者[80]。

3. 韓國

依韓國個人資料保護法規定，個人資料控制者應指定一名「隱私官」（PrivacyOfficer；亦即個人資料保護官），全面負責個人資料處理工作[81]。由於韓國法將個人資料控制者定義為「直接或間接處理個人資料並將個人資料檔案作為其活動一部分進行操作的事業單位、法人、組織及個人等」，基此，凡該當前揭個人資料控制者定義的公務機關與非公務機關，均負有任命個人資料保護官之義務。

4. 新加坡

新加坡個人資料保護法規定「『機構』（Organisation）必須指定一名或多名個人，負責確保該機構遵循本法」[82]。依同法法所作定義，機構一詞包括「任何個人、企業、協會或團體、企業或非法人組織」，同時前述的機構概念，並不論其是否根據新加坡法律成立或受到新加坡法律認可，或居住於新加坡，或在新加坡設有辦事處或營業地點。

---

80 泰國個人資料保護法第 41 條第 1 項。

81 韓國個人資料保護法第 31 條第 1 項。

82 新加坡個人資料保護法第 11 條第 3 項。

（二）個人資料保護官之職責

1. 歐盟

符合資格要求並經資料控制者或資料處理者正式任命之個人資料保護官，依 GDPR 規定，其所負職責包括：

（1） 針對依 GDPR 及歐盟會員國個人資料保護內國立法負有執行法律遵循義務之資料控制者、資料處理者或其職員，提供資訊或諮詢；

（2） 針對依 GDPR、歐盟會員國個人資料保護內國立法以及自身所訂個資保護政策負有落實保護責任之資料控制者或資料處理者，監督其實際遵循情形，包括責任分配、提高認知及培訓職員對於個人資料之處理，以及相關審計事項之遵循工作；

（3） 於接獲隱私衝擊分析（Data Protection Impact Assessment，以下簡稱 DPIA）請求時，提供建議並依 GDPR 第 35 條規定監督 DPIA 之執行；

（4） 與監管機關進行合作；

（5） 針對包括第 36 條所規定之事前諮詢（Prior Consultation）及適當情形下之其他任何事項之諮詢，擔任對應監管機關之連絡窗口[83]；

由於資料當事人依 GDPR 得就與資料處理與 GDPR 賦予資料當事人之權利等有關事項聯繫個人資料保護官，故個人資料保護官之職掌範圍還包括資料當事人權利請求之處理。

2. 泰國

依泰國個人資料保護法規定，符合資格要求並經資料控制者或資料處理者正式任命之個人資料保護官，其所負職責包括：

（1） 就該法之法律遵循向資料控制者或資料處理者提供建議，包括資

83 GDPR 第 39 條第 1 項。

料控制者或資料處理者之內部員工或外部之服務提供者；

（2） 審視資料控制者或資料處理者，包括其內部員工或外部服務提供者在個人資料蒐集、利用或揭露方面之情形，以利該法要求之確實遵循；

（3） 當資料控制者或資料處理者，包括其內部員工或外部服務提供者在個人資料蒐集、利用或揭露上遭遇問題時，與個人資料保護委員會進行協調與合作；

（4） 針對於履行本法規定之職責過程中所知悉或獲取之個人資料保守秘密[84]。

3. **韓國**

韓國個人資料保護法第 31 條第 2 項明訂個人資料保護官所應承擔的七款職責事項：

（1） 制定並實施個人資料保護計畫；

（2） 定期針對個人資料處理行為之現狀與做法進行查核，並改善不足之處；

（3） 與個人資料處理行為有關之投訴與求償之處理；

（4） 建立防止個人資料洩露、濫用及誤用之內部控制機制；

（5） 制定並實施個人資料保護教育計畫；

（6） 保護、控制與管理個人資料檔案；

（7） 其他由總統令所規定、適當處理個人資料之職掌事項[85]；

考量個人資料保護法本身無法就所有事項鉅細靡遺加以規範，韓國法規定可透過「總統令」方式，就適當處理個人資料之事項另行規定。在 2011 年制定個人資料保護法後，韓國政府也旋即於同年 9 月由總統發布「個人資料保護法施行令」（Enforcement Decree of the Personal

84 泰國個人資料保護法第 42 條第 1 項。

85 韓國個人資料保護法第 31 條第 2 項。

Information Protection Act）。其中施行令第 32 條即進一步就個人資料保護官之職責與資格要求等事項進行規定。依韓國個人資料保護法施行令規定，「個人資料保護法中所稱之「總統令規定之其他職責，係指下列事項：

（1） 根據第 30 條規定制定、修改與實施隱私權政策；

（2） 維護與個人資料保護有關之資料；

（3） 銷毀業已滿足處理目的或已逾保存期限之個人資料[86]。

4. 新加坡

新加坡個人資料保護法規定揭示個人資料保護官負有確保該機構確實遵循新加坡個人資料保護法規定之責[87]。此外，依據新加坡個人資料保護主管機關：個人資料保護委員會（Personal Data Protection Commission, PDPC）所發布的「個人資料保護法關鍵概念諮詢指引」（Advisory Guidelines on Key Concepts in the Personal Data Protection Act）規定，個人資料保護官在個人資料保護法下之具體職責還包括：

（1） 與最高管理階層與業務部門進行合作，為機構制定與實施適當的個人資料保護政策；

（2） 編製（或指導編製）個人資料清冊；

（3） 進行個人資料保護衝擊評估；

（4） 監控與報告個人資料保護有關風險；

（5） 提供有關個人資料保護法律遵循之內部培訓；

（6） 與利害關係人就個人資料保護事宜進行接觸；

（7） 與機構之資料治理與網路安全負責人進行合作；

（8） 支持機構之創新活動。

---

86 韓國個人資料保護法施行令第 32 條。

87 新加坡個人資料保護法第 11 條第 3 項。

（三）個人資料保護官之資格要求

1. 歐盟

針對個人資料保護官之任命，GDPR 第 37 條第 5 項規定應依據專業資格能力，特別是有無具備個人資料保護立法之專業知識，以及能否完成相關職務能力為準。此外，個人資料保護官可得為資料控制者或資料處理者之內部職員，亦可由基於服務契約完成職務之外部人員擔任[88]。

2. 泰國

有關個人資料保護官之資格／職能要求，泰國個人資料保護法規定授權個人資料保護委員會按個人資料保護有關知識或專長，制定及公布個人資料保護官之具體資格／職能要求。與 GDPR 相同，規定經任命之個人資料保護官可得為資料控制者或資料處理者之內部職員，亦可為基於服務契約完成職務之外部人員[89]。

3. 韓國

韓國個人資料保護法規定資料控制者的資料條件為：（1）企業負責人或代表人；或（2）董事及高階人員。若無董事或高階人員時，則為從事個人資料處理相關工作之部門負責人[90]。

4. 新加坡

依據新加坡個人資料保護委員會「個人資料保護法關鍵概念諮詢指引」規定，機構根據新加坡個人資料保護法所指定的個人資料保護官，其應具備下列條件：

（1） 充分熟練及知識淵博；

（2） 不必然為內部職員，但須具備充分的權力履行其作為個人資料保

88 GDPR 第 37 條第 5 項、第 6 項。

89 泰國個人資料保護法第 41 條第 6 項、第 7 項。

90 泰國個人資料保護法第 41 條第 6 項、第 7 項。

護官之職責；

（3） 機構應確保經任命的個人資料保護官經過培訓與認證；

（4） 理想情況下個人資料保護官應為機構最高管理階層之一員，或直接向最高管理階層報告，藉以確保其個人資料保護政策之有效制定與實施。

六、國內後續思考議題

觀察個人資料保護國際立法例，部分國家如韓國與新加坡全面要求「所有」的公務機關及非公務機關應設置個人資料保護官，但亦有部分立法例在「非公務機關」部分，並未全面要求設置個人資料保護官，而是有條件的推動。

以歐盟 GDPR 為例，該法第 37 條採取所謂的「分級」設計，僅符合條件的資料控制者與資料處理者應須設置個人資料保護官，而其所採取的分級標準則包括：（一）核心業務是否涉及定期且系統性地大規模監控資料主體；以及（二）核心業務是否涉及大規模處理特種個人資料兩者。可見歐盟係有意地將保有個人資料數量較少的資料控制者，排除於設置個人資料保護官要求之列。

本文認為此一思維亦可為我國所採，蓋國內向來是以「中小企業」為主，依據經濟部發布資料，2021 年我國企業總數為 1,613,281 家，其中中小企業為 1,595,828 家，中小企業占比達到 98.92 %[91]。儘管特定行業別仍可能保有大量個人資料，但多數行業，特別是製造業等傳統產業，往往是以內部員工個人資料為主，而無太多的外部人員個人資料。

中小企業除財力相對有限外，在員工方面亦可能因人力吃緊而難以設置個人資料保護官。儘管依中小企業發展條例第 2 條第 2 項授權制定的「中小企業認定標準」，標準第 2 條規定中小企業指依法辦理企業登

91 經濟部統計處編，110 年經濟統計年報，頁 125，經濟部統計處，2022 年 5 月。

記或商業登記，實收資本額在新臺幣一億元以下，或經常僱用員工數未滿 200 人之事業。員工人數在百人以上仍可能視為中小企業，但對多數中小企業而言，員工人數往往不多，甚至多數民眾所認知的中小企業，是經常僱用員工數未滿五人的「小規模企業」。有無必要要求中小企業設置個人資料保護官，若納入其應有的門檻為何，值得國內加以重視。

觀察國內在資訊安全長的推動經驗，若考慮推動個人資料保護官機制，「非公務機關」部分應無須全面要求設置個人資料保護官，在分級原則設計上，應可參考當前資訊安全長的分級原則設計，明確應設置個人資料保護官的非公務機關對象。

肆、結語

數位經濟已成為各國經濟發展重心，而近期的 COVID-19 疫情更促使各行各業競相投入數位轉型，不分傳統產業或數位化事業，各個產業如今都與數位科技高度相關，使得「資訊安全」成為當前企業治理上的重要環節。資通訊科技日新月異與資料多元應用使得資訊安全問題日益增加，PwC 研究成果即顯示過去三年全球約有 27 %的企業曾發生資訊安全事件。

資訊安全風險已是當前企業營運之重大挑戰，近年來國內持續發生資訊安全事件，造成大的金錢損失及聲譽受損，除了企業人員本身資訊安全意識不足之外，欠缺專業資訊安全人才更是企業備感棘手之關鍵問題。然而資訊安全風險管理涉及眾多層面與考量因素。面對資訊安全風險對企業帶來的威脅，建立充分對應相關風險的管理機制，成為資訊安全風險問題對應上的重要工作。企業內部若欠缺諸如「資訊安全長」此一角色，無法將資訊安全風險與企業業務經營加以連結及評估，即無法充分判斷資訊安全事件對企業營運所產生的影響範圍與實際影響程度。

美國「聯邦資訊安全管理法」（FISMA）提出「資訊安全長」機制設計後，帶動主要國家推動相仿規範，而我國規範公務機關之「資通安

全管理法」亦首見於法律層級明訂「資通安全長」之設置要求。在 2022 年數位發展部成立後，該法已由資通安全署主責並積極規劃因應需求進行修法。本文建議在未來修法時能進一步落實公務機關資安標準之實踐，如新版 ISO/IEC 27001:2022 標準，因為新版標準已經整合資訊安全及個資保護之因應。另外在政府先於企業的政策下，對於資通安全長的設置與責任，似可參考國外法制，如與新加坡之網路安全總監制度比較，建立分層負責相互合作規範。

在非公務機關層面，金管會於 2020 年 8 月發布的「金融資安行動方案」提出設置「高階資安長」構想，2022 年 12 月「金融資安行動方案 2.0」更擴大資訊安全長之設置要求。觀察修正後的金融控股企業及銀行業內部控制及稽核制度實施辦法，其係採取分階段及分級推動之「資訊安全長」新制。金管會將上市（櫃）企業依其收入規模分成三級，以循序漸進方式推動包括資安長在內的資通安全管控機制。基此新制設計，三類事業應於 2022 年底前指派資訊安全長並設置資訊安全單位，包含資訊安全專責主管及至少兩名資訊安全專責人員：一、實收資本額達新臺幣 100 億元以上之上市（櫃）企業；二、前一年底屬於臺灣 50 指數成分之上市（櫃）企業；及三、主要經營電子商務媒介商品或服務之上市（櫃）企業。金管會對於資訊安全長設置的要求，本文建議未來可以擴及至非公開發行之商業組織型態，要求將資訊安全與個資保護併入公司治理環節要求，建立資訊安全及個人檔案維護標準，並以目的事業主管機關為核心，建立資安聯防與通報機制，以有效強化事變因應能力。至於公開發行公司及上市（櫃）公司，本文建議可於董事會下設「公司治理委員會」，就資訊安全、個資保護等事項進行規劃，要求內稽與外稽，並定期向該委員會報告。

在個人資料保護議題日益受視之際，並帶動應否設置隱私長／個人資料保護官之討論時，本文建議我國似可參酌當前資訊安全長的設置要求，評估以分級方式逐步推動隱私長／個人資料保護官。不過資訊安全

事件並不能與個資外洩事件完全劃上等號，兩者仍有維護管理上之區別。觀察國內企業資訊安全人員，過往大抵隸屬於企業資訊部門，且多數並非資訊安全相關專業領域出身。受限於資訊單位層級及自身認知，早期的資訊安全人員往往無法立於企業整體構面思考資訊安全問題，無可避免造成企業存在著資訊安全管理上的不足及盲點。在設置資訊安全長逐漸成為各個企業經營上不可或缺的事項時，資訊安全長及專責人員惟有跳脫傳統的資訊框架，以全方位的角度為企業識別並管理可能出現的潛在風險，進而規劃符合企業業務發展需求的資訊安全體系，甫能協助企業在全力發展之餘，亦可得有效兼顧發展過程中所出現的資訊安全風險之管理需求。

另一方面，資訊安全的有效維護亦必須解決資安人才問題，根據美國網路安全教育中心所作調查，2015 年全球資安人才需求約為 150 萬人，2022 年時需求擴大為 180 萬人，資安人才短缺問題是各國網路安全建設面臨的共同難題。我國目前依照數位發展部之組織執掌分工，有關協助規劃及培育資通安全專業人才並推廣全民資通安全意識，係屬國家資通安全研究院之業務範圍。本文建議未來該院似宜積極與產業發展署及民間公協會組織合作研議，共同就產業資安人才培訓與資格認證進行規劃與實踐，也唯有公私協力，才能落實產業資安化之最大利益發揮。

參考文獻

中文

一、專書

行政院編，國家人權行動計畫，行政院，2022 年 5 月。

金融監督管理委員會編，金融資安行動方案，金融監督管理委員會，2020 年 8 月。

金融監督管理委員會編，金融資安行動方案 2.0，金融監督管理委員會，2022 年 12 月。

經濟部統計處編，110 年經濟統計年報，經濟部統計處，2022 年 5 月。

二、期刊論文

王宏瑞，淺談美國 COSO 委員會之「企業風險管理－整合架構」報告，集保結算所月刊，第 225 期，頁 8-33，2016 年 4 月。

李世德，GDPR 與我國個人資料保護法之比較分析，臺灣經濟論衡，第 16 卷，第 3 期，頁 69-93，2018 年 9 月。

林淑芸、金旻姍，美國 COSO 內部控制相關報告之介紹，證券暨期貨月刊，第 33 卷，第 6 期，頁 5-12，2015 年 6 月。

郭戎晉，自歐盟執委會及成員國視角談一般資料保護規則（GDPR）之實施與課題，科技法律透析，第 30 卷，第 4 期，頁 28-38，2018 年 4 月。

葉志良，大數據應用下個人資料定義的檢討：以我國法院判決為例，資訊社會研究，第 31 期，頁 1-36，2016 年 7 月。

廖君美，企業風險管理與資訊安全機制設計，財金資訊季刊，第 75 期，

頁 27-31，2013 年 7 月。

劉靜怡，淺談 GDPR 的國際衝擊及其可能因應之道，月旦法學雜誌，第 286 期，頁 5-31，2019 年 3 月。

樊國楨、林惠芳、黃健誠，資訊安全法制化初探之一：根基於美國聯邦資訊安全管理法，資訊安全通訊，第 18 卷，第 1 期，頁 3-26，2012 年 1 月。

潘元偵，淺談新加坡網路安全法－以網路安全總監為核心，科技法務透析，第 31 卷，第 8 期，頁 13-19，2019 年 8 月。

英文

一、專書

CRAIG, PAUL & BÚ RCA, GRÁ INNE DE, THE EVOLUTION OF EU LAW (OXFORD UNIVERSITY PRESS, NEW YORK, 2021).

THE WHITE HOUSE, NATIONAL CYBERSECURITY STRATEGIES (UNITED STATES. WHITE HOUSE OFFICE, 2023).

二、期刊論文

Rustad, Michael L. & Koenig, Thomas H., *Towards a Global Data Privacy Standard*, 71 FLA. L. REV. 365-453 (2019).

Smith, Chelsea C., *Hacking Federal Cybersecurity Legislation: Reforming Legislation to Promote the Effective security of Federal. Information Systems*, 4 NAT'L SEC. L.J. 345-385 (2016).

Whitea1, Daniel M., *The Federal Information Security Management Act of 2002: A Potemkin Village*, 79 FORDHAM L. REV. 369-405 (2011).

Abstract

The digital economy has become the focus of economic development in various countries. The COVID-19 epidemic has prompted all industries to invest in digital transformation. However, the rapid changes in information and communication technology, together with the multiple applications of data have also aggravated information security issues. Information security risk has become a major challenge for current business operations, but its management involves many levels and considerations.

Facing the threats brought by information security risks to enterprises, establishing a management mechanism that adequately responds to relevant risks has become an important task in dealing with information security risk issues. In particular, whether and how an enterprise can link information security risks with business operations by setting up a “Chief Information Security Officer” to fully judge the actual scope and degree of impact of information security incidents on business operations.

The Federal Information Security Management Act of the United States emphasizes the importance of the “Information Security Officer”, while leading major countries also formulate similar regulations. Taiwan’s Cyber Security Management Act is the first to clearly stipulate the establishment requirements of the “Chief Information Security Officer” at the legal level. At the level of non-government agencies, the Financial Supervisory Commission proposed and expanded the requirements for setting up chief information security officers in the “Financial Security Action Plan” and “Financial Security Action Plan 2.0”, as well as adopted a phased and hierarchical approach to promote it.

When the issue of personal data protection is taken seriously and leads

to discussions on whether to set up a privacy officer/personal data protection officer, our country can also refer to the requirements for the establishment of an information security officer, and gradually promote this mechanism in a hierarchical manner. The establishment of an information security officer will gradually become an indispensable item in the operation of each enterprise, assisting enterprises to fully develop while effectively accommdating the management needs of information security risks that arise during the development process.

Keywords: Digital Economy, Information Security Risk, Chief Information Security Officer, FISMA, Cyber Security Management Act, Financial Security Action Plan