美國各州逐步研議透過立法豁免企業資安事件賠償責任

美國各州逐步研議透過立法豁免企業資安事件賠償責任

資訊工業策進會科技法律研究所

2024年06月10日

為鼓勵企業採用資安標準與框架，美國已有幾州開始透過立法限縮企業資安事件賠償責任，企業若能舉證證明已符合法令或遵循業界認可之資安框架和標準，則於資安攻擊事件所致損害賠償訴訟中，將無需承擔賠償責任。

壹、事件摘要

為避免有心人士於未取得經授權下近用網路和敏感資料，企業往往投入大量資源打造資安防護架構，惟在現今網路威脅複雜多變的環境下，仍可能受到惡意資安攻擊，導致資料外洩事件發生，導致企業進一步面臨訴訟求償風險，其中多數指控為未實施適當的資安措施。為此美國佛羅里達州和西維吉尼亞州研議透過立法限縮企業之資安事件賠償責任，以鼓勵企業採用資安標準、框架與資安相關法令。

貳、重點說明

繼美國俄亥俄州[1]、猶他州[2]和康乃狄克州[3]相繼頒布法令，讓已實施適當安全維護措施之企業，豁免資安攻擊所致資料外洩之損害賠償責任，佛羅里達州和西維吉尼亞州近期亦提出相似法案，以下介紹兩州法案之重點：

一、佛羅里達州

美國佛羅里達州於2023年11月公布《資安事件責任法案》（H.B 473: Cybersecurity Incident Liability）[4]，法案納入「安全港條款」（Safe Harbor），當企業遭受資安攻擊致生個資外洩事件，如可證明已遵循產業認可的資安標準或框架，實施適當的資安措施與風險控管機制，則可免於賠償責任，以鼓勵企業採納資安標準或框架。

為適用安全港條款，企業須遵循佛羅里達州資訊保護法（The Florida Information Protection Act），針對資料外洩事件，通知個人、監管機關和消費者，並建立與法案內所列當前產業認可的資安標準、框架，或是特定法令規範之內容具一致性的資安計畫（Cybersecurity Programs）：

（一）當前產業認可的資安標準、框架

1. 國家標準暨技術研究院（National Institute of Standards and Technology, NIST）改善關鍵基礎設施資安框架（Framework for Improving Critical Infrastructure Cybersecurity）。
2. NIST SP 800-171－保護非聯邦系統和企業中的受控非機密資訊。
3. NIST SP 800-53 和 SP 800-53A－ 資訊系統和企業的安全和隱私控制/ 評估資訊系統和企業中的安全和隱私控制。
4. 聯邦政府風險與授權管理計畫（Federal Risk and Authorization Management Program, FedRAMP）安全評估框架。
5. 資安中心（ The Center for Internet Security, CIS）關鍵安全控制。[5]
6. ISO/IEC 27000系列標準。
7. 健康資訊信任聯盟（The Health Information Trust Alliance, HITRUST）通用安全框架（Common Security Framework）[6]。
8. 服務企業控制措施類型二（Service Organization Control Type 2, SOC 2）框架。
9. 安全控制措施框架（Secure Controls Framework）。
10. 其他類似的產業標準或框架。

（二）特定法令規範

企業（entity）如受以下法令規範，亦得適用安全港條款，如法令有修訂，企業應在發布修訂後的一年內更新其資安計畫：

1. 健康保險可攜與責任法（The Health Insurance Portability and Accountability Act, HIPAA）之安全要求。
2. 金融服務現代化法（The Gramm-Leach-Bliley Act）第五章。
3. 2014 年聯邦資訊安全現代化法（The Federal Information Security Modernization Act of 2014）。
4. 健康資訊科技促進經濟和臨床健康法（The Health Information Technology for Economic and Clinical Health Act, HITECH）之安全要求。
5. 刑事司法資訊服務系統 （The Criminal Justice Information Services, CJIS）安全政策。
6. 州或聯邦法律規定的其他類似要求。

該法案雖於2024年3月5日經佛羅里達州參議院三讀通過，但於2024年6月26日遭州長否決[7]，其表示法案對於企業的保障範圍過於廣泛，如企業採取基礎的資安措施與風險控管機制，便得主張適用安全港條款，將可能導致消費者於發生個資外洩事件時，無法受到足夠的保障。州政府鼓勵利害關係人與該州網路安全諮詢委員會（Florida Cybersecurity Advisory Council）合作，探求法案的替代方案，以保護消費者資料。

二、西維吉尼亞州

美國西維吉尼亞州於2024年1月29日提出眾議院第5338號法案[8]，修訂西維吉尼亞法典（Code of West Virginia），增訂第8H章資安計畫安全港條款（Safe Harbor for Cybersecurity Programs），如企業符合業界認可的資安標準、框架或依特定法令建立與實施資安計畫，包含個人資訊和機敏資料的管理、技術和企業保障措施，將能夠於侵權訴訟中，主張適用避風港條款。

法令內明列評估企業所建立的資安計畫規模和範圍是否適當之要素，包含：

1. 企業的規模和複雜性；
2. 企業的活動性質和範圍；
3. 受保護資訊的敏感性；
4. 使用資安防護工具之成本和可用性；
5. 企業可運用的資源。

（一）當前產業認可的資安標準、框架

除與佛羅里達州法案所列舉業界認可的資安標準之前六項相同，另增加：

1 NIST SP 800-76-2個人身分驗證生物辨識規範（Biometric Specifications for Personal Identity Verification）[9]。

2. 資安成熟度模型認證（The Cybersecurity Maturity Model Certification, CMMC）至少達到第2級，並經外部驗證（external certification）。

（二）特定法令規範

除與佛羅里達州法案所列舉特定法令之前四項相同，另增加：由聯邦環境保護局（Environmental Protection Agency, EPA）、資安暨基礎設施安全局（Cybersecurity and Infrastructure Security Agency, CISA）或北美可靠性公司（North American Reliability Corporation）[10]所採用任何適用於關鍵基礎設施保護的規則、法規或指南。

惟目前法案已於2024年3月27日被西維吉尼亞州長否決[11]，其表示透過安全港條款鼓勵企業實踐資安框架雖立意良好，但也可能遭濫用而帶來不當影響，例如TikTok等大型國際企業，如在違背公民意願情況下共享個人資料時，將免於訴訟，恐有損其公民權益，未來州政府將與利害關係人持續進行協商。

參、事件評析

佛羅里達州和西維吉尼亞州近期同步公布有關限制企業於資安事件之責任相關法案，內容亦為相似，西維吉尼亞州之法案目前已遭否決，主要係擔心該豁免條款遭到不當濫用；佛羅里達州之法案亦因對於企業保障過廣與無法保障消費者個資安全考量，而遭州長否決。

法案中明列受產業普遍認可的資安標準、框架與政府所頒布特定法令，有助企業明確遵循與採納，建立與實施資安計畫，惟如何舉證所建立之資安計畫或實施之資安措施，與法案所列之資安標準、框架，或是特定法令規範，具有實質上的一致性，仍不明確，將可能阻礙企業於訴訟上行使抗辯與主張責任豁免權。未來美國如何權衡產業穩健發展與民眾個資保障，仍有待持續觀察。

[1] Chapter 1354 - Ohio Revised Code, Ohio Laws, https://codes.ohio.gov/ohio-revised-code/chapter-1354 (last visited May 24, 2024).

[2] Part 7 Cybersecurity Affirmative Defense Act, Utah StateLegislative, https://le.utah.gov/xcode/Title78B/Chapter4/78B-4-P7.html (last visited May 24, 2024).

[3] Frederick Scholl, Connecticut's New Breach Notification and Data Security Laws: Carrots and Sticks, Quinnipiac University, July,1,2021, https://www.qu.edu/quinnipiac-today/connecticuts-new-breach-notification-and-data-security-laws-2021-07-01/ (last visited May 24, 2024).

[4] CSHB 473-Cybersecurity Incident Liability, The Florida Senate, https://www.flsenate.gov/Session/Bill/2024/473 (last visited Jun. 28, 2024).

[5] 資安中心（ The Center for Internet Security, CIS）為美國非營利組織，負責推動CIS Controls，針對實際發生的資安攻擊行為提供防禦建議，

作為企業保護 IT 系統和資料時可參考之最佳實務作法。資料來源：About us, Center for Internet Security, https://www.cisecurity.org/about-us (last visited Jun. 6, 2024).

[6] What is HITRUST?, Schneider Downs, https://schneiderdowns.com/cybersecurity/what-is-hitrust/ (last visited May 24, 2024).

[7] Governor of Florida, *Vote letter for House Bill 473*(2024), https://www.flgov.com/wp-content/uploads/2024/06/Veto-Letter_HB-473.pdf (last visited Jun. 28, 2024).

[8] 2024 REGULAR SESSION ENROLLED Committee Substitute for House Bill 5338, WEST VIRGINIA LEGISLATURE,https://www.wvlegislature.gov/Bill_Status/bills_text.cfm?billdoc=hb5338%20sub%20enr.htm&yr=2024&sesstype=RS&i=5338 (last visited May 24, 2024).

[9] NIST SP 800-76-2 Biometric Specifications for Personal Identity Verification, National Institute of Standards and Technology, https://csrc.nist.gov/pubs/sp/800/76/2/final (last visited May 24, 2024).

[10] 北美電力可靠性公司（North American Electric Reliability Corporation, NERC），為一家非營利機構，致力推動關鍵基礎設施保護相關標準，以強化北美大規模電力系統（亦即電網）的可靠性和安全性，資料來源：https://www.nerc.com/Pages/default.aspx (last visited May 24, 2024).

[11] Governor of West Virginia, *Enrolled Committee Substitute for House Bill 5338*(2024), https://www.wvlegislature.gov/Bill_Text_HTML/2024_SESSIONS/RS/veto_messages/HB5338.pdf (last visited May 24, 2024).

你可能會想參加

→ 製造業及技術服務業個資保護及資安落實－經濟部工業局112年企業個人資料保護暨資訊安全宣導說明會
→ 【已額滿】2023科技研發法制推廣活動—科專個資及反詐騙實務講座
→ 供應鏈資安國際法制與政策趨勢分享會
→ 【實體】數位發展部數位經濟相關產業個資安維辦法說明會（南部場）
→ 【線上】數位發展部數位經濟相關產業個資安維辦法說明會（南部場）
→ 數位發展部數位產業署113年資訊服務業安維計畫常見問題分享說明會
→ 商業服務業個資保護宣導說明會
→ 個人資料保護新思維企業法遵論壇
→ 【實體】2024科技研發法制推廣活動— 科專個資及反詐騙實務講座
→ 【直播】2024科技研發法制推廣活動— 科專個資及反詐騙實務講座
→ 中部場–商業服務業個資保護工作坊
→ 南部場–商業服務業個資保護工作坊
→ 北部場–商業服務業個資保護工作坊
→ 數位發展部數位產業署113年資訊服務業者個資安維辦法宣導說明會

阮韻蒨
副法律研究員 編譯整理

上稿時間：2024年07月

文章標籤

推薦文章