| 2024-05-10 | 香港商報 | A02 | 香江評論 | 建評 | 葛珮帆

須加強資訊系統監督

政府部門及公營機構近年接二連三發生外洩市民個人資料事故，引起公眾對私隱安全問題的關注。無論如何，這接連事件已充分反映涉事人員對網絡安全及保護個人私隱方面不夠重視和意識不足。筆者認為，時至今日，資訊系統已成為政府各個部門業務運作的核心，部門管理層實在不能只把其資訊系統視作單純技術問題，只交給技術團隊或服務承辦商處理，而應該直接對其資訊系統加強監督。

繼公司註冊處及機電工程署後，消防處日前亦公布發生有外洩消防處屬員和市民個人資料風險的事故。綜觀近年選舉事務處、數碼港、消委會、公司註冊處及機電工程署等先後發生的同類事件，出現市民個人資料外洩的原因主要是管理及人為因素。據此，本人提出以下四項建議：

一，鑒於相關事件發生後，各政府部門和公營機構多遲遲未有通報個人資料私隱專員公署、媒體及受害人，情況並不理想，同時，亦反映各政府部門及公營機構對網絡安全的重視程度及執行力不足，因此，當局應就事故進行徹查並追究責任。

二，現時政府各部門均設有部門資訊科技保安主任及資訊保安事故應變小組，分別領導該部門的整體資訊保安管理，和處理日常所有事項，以準備、偵測和應對所有資訊保安事件及事故。當局應責成各政府部門首長及資訊科技部門須對其電

腦系統的保安工作問責，以保障系統網絡及資訊安全，如發現有人為疏忽或違規，相關人員須作紀律處分。

密切監察網絡保安威脅

三，目前所有政府資訊科技項目在系統上線前，必須進行「保安風險評估和審計」（SRAA），但 SRAA 並沒有評估系統是否向公眾披露過多和不必要的個人數據，因此，政府有必要在所有資訊科技項目中引入「隱私數據評估和審計」，以確保系統不會向公眾披露過多和不必要的個人數據。

四，未來「數字政策辦公室」須密切監察網絡攻擊的趨勢和保安威脅，適時發出警報通知，並提高各政府部門網絡及資訊安全的即時應變能力和防範意識。

此外，單就機電工程署洩漏疫情時「圍封強檢」期間收集的 17000 名市民個人資料事故，筆者強調，政府部門不應把個人私隱數據長期儲存在雲端系統，若因情況緊急，亦應把儲存時間盡量縮短，涉事人員完成數據處理後，應盡快移除數據。政府亦應督促各部門安排指定人員定期監測及監管涉及個人私隱敏感數據的存儲，以定期刪除敏感個人數據，並就數據安全進行內部演練，主動識別和解決潛在風險或漏洞，強化安全防護能力。

立法會議員