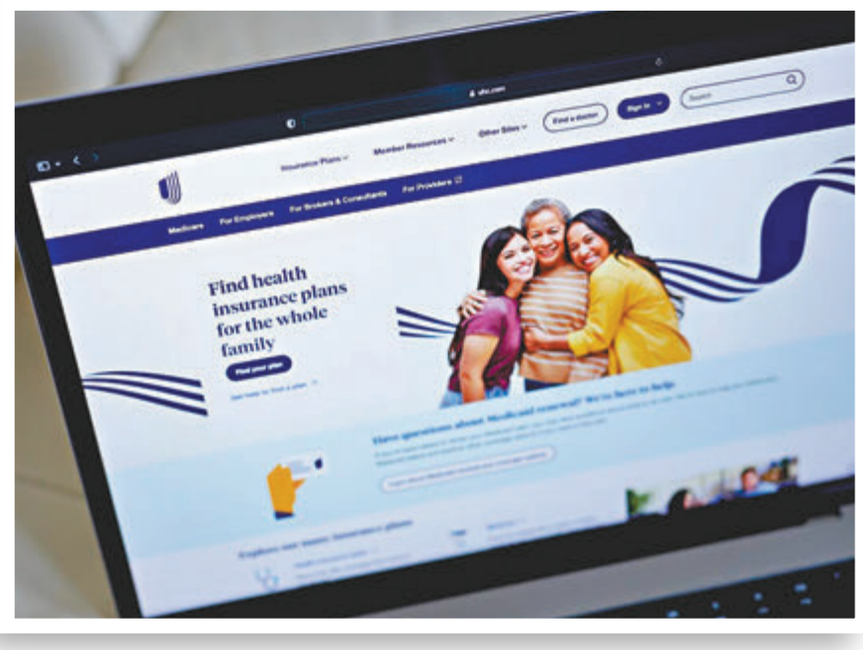
欠完善「第三方風險管理」 涵蓋醫療物流等多個行業

逾六成美企經歷客戶資料外洩

香港文匯報訊　全球多地企業的客戶私隱外洩問題近年愈趨嚴重，第三方服務商的風險尤其引人關注。負責第三方服務商風險管理的美國企業Prevalent周三（5月8日）發布最新報告，發現過去一年，全美約有61%企業經歷第三方資料外洩或網絡安全事件，該比例按年增幅達49%，從2021年至今更是增加了3倍。報告指出，許多企業沒有制訂完善的「第三方風險管理」（TPRM）計劃，這一問題現時需要重視。



◆美醫療保險集團「聯合健康集團」遭黑客勒索，大量客戶數據被竊。　網上圖片

今次調查於今年2月至3月進行，Prevalent訪問全美數十個行業不同企業的資訊安全、資料私隱、風險管理、採購和資訊科技服務主管，相關企業的供應鏈涵蓋全美約50萬間第三方服務供應商。公司執行主任希克基表示，「最引人矚目的不是安全事件的數量，是其涵蓋的規模，它影響了涵蓋醫療、物流、訊息管理等多個行業，外洩了數百萬人的敏感紀錄。」

Prevalent運營主管希伯特稱，企業若配有完善的TPRM計劃，可以明顯降低第三方服務商外洩客戶資料的風險，但調查發現，約半數企業仍依賴傳統的電子表格，或是使用各類單一工具評估類似風險，「這種做法缺乏協調」。希伯特也稱，受訪企業約60%沒有專門的TPRM平台，只有三分之一的企業會妥善協調TPRM計劃。

企業平均與逾3000服務商合作

受訪企業平均每間與3,200個第三方服務商合作，不過企業平均只對其中三分之一完成風險評估。調查指出，超過62%的受訪企業坦言人手不足，是其加強評估第三方風險、避免客戶資料外洩的最大障礙。企業平均需要將現有負責相關事務員工增加一倍，才能較好監督第三方服務商的運作。

缺乏外洩資料後補救措施

希伯特還指出，多數企業還缺乏第三方服務商外洩客戶資料後的整體補救措施，「令我們驚訝的是，主動追蹤資料外洩風險的企業，與積極補救資料外洩風險的企業數目有明顯差距，只有46%的企業表示，會就TPRM計劃發現的風險進行修復，這一比例非常低：這是降低資料外洩風險的必要階段。」

調查報告也顯示，目前只有5%的企業在TPRM計劃中使用了人工智能（AI）技術，但有61%的企業正研究AI技術在TPRM的應用。Prevalent建議，企業可以組建跨部門TPRM團隊，圍繞單一平台實現TPRM流程自動化、提升工作效率的同時，亦加強資料外洩風險管控。

黑客專攻服務商 骨牌效應殃及多間企業

香港文匯報訊　第三方服務商往往同時為多間企業服務，一旦遭受黑客攻擊導致數據外洩，便會掀起骨牌效應，波及眾多不同企業的客戶。美國信息技術專業網站Spiceworks引述專家分析，黑客通常會尋找第三方服務商的供應鏈缺口，試圖「以最少成本獲得最高額回報」，呼籲企業應當與第三方持份者持續溝通，更快識別、監控並減輕網絡風險。

網絡安全公司SecurityScorecard指出，2023年5月，文件開發傳輸平台MOVEit發現存在漏洞，由於該平台被北美為主的全球多地政府、金融機構和私企作信息收發用途，黑客對MOVEit的攻擊造成嚴重後果，截至去年底合共影響2,611間企業或機構，信息外洩受害人數估計至少達8,500萬人，MOVEit事件展現了攻擊第三方平台的破壞力，一個漏洞可以導致數以千計企業同時被攻擊，造成難以估計的損失。

美國網絡安全培訓機構KnowBe4創辦人科隆解釋稱，使用第三方服務處理客戶資料很常見，有助企業提升效率，但想要降低數據外洩風險，需要企業時常留意。企業要注意與第三方服務確認數據保護協議，以及資料管理時限。部分資料應當以匿名形式儲存，並定期進行檢查。

◆黑客攻擊MOVEit影響逾2,600企業。圖為MOVEit網頁。　網上圖片

澳私隱專員：第三方服務商合作條款存漏洞

香港文匯報訊　澳洲私隱專員辦公室周日（5月5日）發布報告顯示，該部門於過去6個月內，收到483宗企業外洩用戶個人資料報告，以及121宗「二次資料外洩」報告，即一間公司的客戶資料外洩、影響到該客戶在另一間公司的業務。私隱專員金德指出，第三方服務商與企業合作時，通常缺乏私隱標準相關條款，「這些服務商現時是客戶資料外洩的真正弱點，需要企業和機構重視。」

金德指出，私隱專員辦公室建議企業與第三方服務商合作時多加留意，「企業和機構要確認保護客戶的個人資料，它們需要與第三方服務商簽訂私隱保護合約，或是通過詳細調查，確保企業指導第三方服務商採取了什麼措施，保證用戶的個人資料安全。」

資料被閒置後外洩

金德稱，她並不擔心業界抵制當局立法加強私隱保護，但擔憂部分企業和機構收集個人資料後便將其閒置，成為私隱外洩潛在來源，「我們看到每次個人資料外洩事件發生時，外洩的資料數目很多，也許其中一些已經無需由特定企業或機構保留。應對這種『過度收集數據』問題，企業和機構需要改變習慣。」

歐盟早前頒布嚴格的數據保護法案，要求跨國企業遵守。金德認為，澳洲等國家和地區應當仿效該作法，加強私隱保障法案中監管機構的權力，「監管機構的角色非常關鍵，我們已經看到在歐洲，積極執行私隱保護法案確實可以改變部分企業的商業模式。」

澳洲司法部長德雷福斯早前表示，在公民個人私隱頻繁受到攻擊的時代，推動相關法律改革很重要。德雷福斯稱，澳洲政府計劃8月修訂私隱保護法案，測試企業和機構是否正確收集及使用客戶資料，亦考慮設定企業保留用戶個人資料的最長期限。

醫療保險集團遭黑客勒索 支付1.7億贖金

香港文匯報訊　美國多間企業今年發生客戶私隱數據外洩事件，全美第五大企業、醫療保險集團「聯合健康集團」（UnitedHealth Group）今年2月遭到黑客勒索，大量客戶數據被竊取，公司不得不支付高達2,200萬美元（約1.7億港元）的贖金。美國運通與美國銀行也先後因第三方服務商被黑客攻擊，導致用戶資料外洩，涉及多項用戶敏感交易數據。

聯合健康集團行政總裁惠蒂上周三（5月1日）出席國會參議院聽證會，他承認被黑客攻擊的是子公司「Change Healthcare」服務系統，每年處理多達150億宗醫療相關交易，涉及美國三分之一的患者就醫紀錄。惠蒂坦言，公司向黑客團體BlackCat以加密貨幣比特幣支付贖金，承認公司需要盡力保護患者的健康資料，他為此作出「歷來最艱難的決定之一」。

美國運通卡客戶資料被竊

美國運通今年3月通報，由於一間負責處理信用卡交易的第三方服務商系統被黑客入侵，美國運通部分會員的資料外洩，包括信用卡卡號、姓名、信用卡到期日等。美國運通表示，公司已向受影響的客戶發出警示，提醒客戶及時上報任何可疑的信用卡交易。

美國銀行合作的第三方服務商、保險管理服務公司IMS去年10月被黑客攻擊，導致美國銀行多名客戶資料外洩。得州檢方報告稱，外洩資料涵蓋至少5.7萬宗敏感交易數據，以及客戶的銀行賬戶、信用卡卡號、社會安全號碼、出生日期和聯絡資料等。

AI研發存私隱憂慮　專家籲度身打造保障規定

香港文匯報訊　人工智能（AI）技術近年迅速發展之際，對私隱保障的擔憂亦浮現。美國律師行Greenspoon Marder創新及技術業務合夥人舍爾與本齊盧奇在路透社撰寫評論稱，需要利用大量數據訓練演算法的AI技術，無可避免存在私隱方面的憂慮，立法者和技術人員應推動爲AI技術度身打造的私隱保障規定，保護民眾的個人資料安全。

分析指出，AI技術用於訓練演算法的數據中，包含大量個人資料，相關資料的收集、儲存和使用，都與傳統互聯網技術的個人資料收集及保護模式截然不同。AI技術還可能利用總結大量數據，透過用戶的指令「推算」用戶的敏感信息，包括他們的住址、工作、家庭情況，以及個人喜好和習慣等，這些推算得到的資料不排除未經用戶授權，便會被轉移甚至外洩。

僅10%企業擁衡量AI風險系統

全球市場諮詢公司Coleman Parkes今年初一項研究，訪問300名美國生成式AI專家，當中80%對AI技術的私隱保障問題感到擔憂。報告指出，專家們認爲現時只有約10%的科企，擁有可靠的系統衡量AI大型語言模型（LLM）的私隱風險，多數企業在運用AI技術時，存在私隱保障不足問題。

舍爾與本齊盧奇分析，解決AI私隱問題需多方面合作。立法者需要就AI資料處理技術制訂嚴格法規，並要求開發人員披露演算法所需資料的來源、提升訓練演算法的透明度。

分析也認爲，當局應鼓勵科技從業者和普通民眾參與公共討論，就監管AI技術、避免私隱外洩制訂法律框架，在公共安全與保護個人私隱之間實現平衡，「AI私隱問題是我們所處時代最大挑戰之一，我們必須確保我們對技術進步的追求，不會以犧牲私隱權爲代價。」