Feature

您的個人資料有多安全?
How Safe Is Your Private Information?

作者: **Joanne Joseph, CISA,** is an IT auditor in Atlantic LNG Company of Trinidad & Tobago. In 2005, while at BP Trinidad & Tobago, Joseph was the IT representative on a cross-functional team that was formed to develop the local data privacy policy and promote information security awareness among the user community.

譯者: 陳立群, CISM,CISA,CISSP,PMP, 中華民國電腦稽核協會理事,Taiwan CISM Coordinator,中華電信數據通信分公司政府網路處

從流行和演進的技術觀點，電子資料隱私性是全球議題且和隱私權損害與資料跨邊界於網際網路與使用無線裝置(例如行動電話、互動電視、全球衛星定位系統 [GPSs])傳輸、儲存與使用的資訊安全受到大眾持續的關注。從這些來源捕捉的電子資料可能被用來做非計畫中的目的使得使用這些服務的個人受害。根據 Ponemon 研究院(Ponemon Institute)執行的研究[1]顯示行動裝置與無所不在的存取敏感的個人資料造成數位時代的重大個資風險。

本文從隱私權侵害探討其威脅和保護客戶資料所普遍實施的政策與保護措施。

哪些個人資料遭遇風險?

個人資料遭遇的風險的例子包含但不限於姓名、生日、住家地址、電話號碼、種族、性傾向、政黨、宗教、社會安全號碼、不同系統的識別號碼、客戶信用卡資訊、申請工作的健康資訊、資格和經驗、受雇表現評價、網際網路瀏覽記錄和電子郵件等。

隱私權情報交換所(Privacy Rights Clearinghouse)描述在 2005 至 2012 年間組織的個人資料安全損害事件由於：[2]

- **非故意的揭露**—資訊不慎地被送到錯誤的收件者。
- **內賊的資訊（Insider information）**—資料被具有合法存取權限的人蓄意洩漏。
- **實體文件(Physical documents)**—紙本資訊遭遺失、拋棄或偷竊。
- **可攜式裝置（Portable devices）**—筆記型電腦、硬碟、隨身碟、光碟和智慧型手機遺失、拋棄或遭竊。

甚麼是隱私權

在企業經營時，組織必須取得關於個人、公司和其他機構的個人資料。隱私權是指「免於遭受未經授權的打擾」("freedom from unauthorized intrusion.")[3]。

隱私權保護根據使用者、客戶與員工三個面向管理：在使用者面向，期望其個人紀錄受到保護不被未經授權的個人或個體侵害。由客戶之面向，當業務執行時，信賴與信用必須被維護。而從員工的角度，必須確保其隱私資訊不會在未經員工同意下遭揭露。

當敏感資料處理時，必須實施額外的保護措施，特別是資料傳輸時的強韌加密與記錄存取敏感資訊。然而，最佳的防禦措施並非實施技術上的安全控制措施，而是辦理資訊安全訓練與認知。對於服務提供者和組織，鼓勵使用者對於安全有認知將是主要關心的事。在資訊安全中，使用者被認為在確保資訊機密上是脆弱的一環。在 2005 年到本文撰寫的 2012 年間，有 364 個案例導因於內賊洩漏的資訊造成資料外洩[4]。

隱私資料法規:保護的措施

近年來，在公開報導的違反個資事件後，為了提供安全給使用者、客戶與員工以防其資料可能被竄改、其隱私在資料安全事件可能遭外洩，新的法規已經制訂。

於 1972 年由美國衛生、教育與公眾服務部(US Department of Health, Education and Welfare)制訂的公平資訊實務法(The Code of Fair Information Practices)提供後續法規例如美國資料隱私權法 (US Data Privacy Act (1974)) 和英國資料保護法(UK Data Protection Act (1998))的基礎。公平資訊實務法根據以下五個原則制訂:[5]

- *必須提供個人資料記錄保存制度。*
- *必須提供個人知道其個資被記錄與如何使用的資訊。*
- *因某一目的而取得的個人資訊不能在沒有取得當事人同意下使用或利用於其他用途，必須要有方法防止上述情形發生。*
- *必須提供修正或增補個人可識別資訊的記錄之方式。*
- *任何組織產生、維護、使用或散播可識別個人資料紀錄必須確保資料特定使用目的的可信賴性並且必須採取預防措施防止資料的誤用。*

美國與英國法律框架支援良好隱私實務已經擴展包括業界特定的法規以因應和特定型態資料相關的內在風險。這些實務的例子包括:

- 1999 年美國針對金融機構制訂的 THE GRAMM-LEACH-BLILEY ACT (GLBA)[6] 法案
- 美國於 2002 年頒佈的沙賓法案(THE SARBANES-OXLEY ACT[7])，也被稱為「上市公司會計改革和投資人保護法案與稽核可規則性與責任法」(the Public Company Accounting Reform and Investor Protection Act and Corporate and Auditing Accountability and Responsibility Act)
- 2006 年美國針對健康保險公司與醫療提供者制訂的健康保險可攜性和責任法案(THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT,HIPAA[8])。
- 2003 年的英國隱私和電子通訊法(歐盟指令) UK PRIVACY AND ELECTRONIC COMMUNICATIONS REGULATIONS (EC Directive)[9] of 2003 禁止未事先經用戶同意下直接透過電話、電子郵件或文字訊息行銷。

英國和美國立法的管理需求結合對於隱私與資訊安全成長的關注，已經觸發公司和政府機構朝向符合國家法律或者國家間彼此的協議。法律上的規定與符合性的標準[10]是外部驅動指令[11]的範例，能提供跨國際疆界的隱私權政策框架[12]並設計藉由禁止未經授權揭露個人資訊來保護個人隱私權益。在法律框架內，額外的關心是組織通知當事者其個人資料已經洩漏的責任。在美國此法規於不同洲有所不同，但一般來說若資料未經加密（亦即可用明文讀取）必須強制實施。美國的洲議會國家聯盟（ The National Conference of State Legislatures)維護已頒佈與已提出的安全侵害通報法律清單[13]。歐洲網路與資訊安全署(The European Network and Information Security Agency,ENISA)於 2011 年 1 月出版歐洲國家資料外洩通報法律（data breach notification laws)報告，此份報告陳述在大部分歐盟國家資外洩通報並未強制實施，因為大部分成員國仍在準備調整至 2009 年 11 月歐盟通過的電信法規改革包裹法案[14]，此改革包裹法案需要歐盟成員國將資料外洩通報法規引介至其本國立法。

為了有效地實施立法框架的政策以因應技術風險，業界特定的標準已經浮現。這些標準根據產業風險剖繪更新，並且出版作為實施數位維運的基準。

這些標準的例子包括:

- 付款卡片工業資料安全標準 PAYMENT CARD

INDUSTRY DATA SECURITY STANDARD (PCI DSS)[15]
- 美國國家標準和技術研究 (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)[16]
- ISO/IEC 27001 資訊技術-安全技術-資訊安全管理系統 - 要求事項 (ISO/IEC 27001 Information technology—Security) techniques—Information security management systems—Requirements)

隱私資料外洩如何發生？

在數位通訊中，常常發生敏感個人資訊未經授權存取或是因不注意而揭露。資訊安全上這些利用的進入點範例如表 1 顯示：

隱私資料外洩

有時資料安全侵害和偽冒身分或是洩漏被認為是機密或秘密的資訊的報導使得企業、名流與政府官員於大庭廣眾丟臉

孤獨和隱私對於個人已經變得更重要，但現代企業和發明帶來痛苦和憂傷,遠比只是對身體健康的損害來得大。[17]

近期發生資料安全事件的媒體報導其例子涵蓋部門包括以下：

- 谷哥違反英國資料隱私權協議(2012 年 7 月)[18]
- 美國聯邦貿易部對 WYNDHAM 大飯店資料損害事件提起訴訟(2012 年 6 月)[19]
- 安大略選舉發現選舉個人資料損害 (2012 年 7 月)[20]

ISACA 白皮書強調做壞事的人為了犯罪的目的可使用定位系統追蹤個人行蹤的風險，這類型的資訊是高度個人化且應該被歸類為敏感並且應該恰當地限制存取 [21]

每次人們於店家簽署折扣卡或填完表格以取得某些優惠服務，個人資料在未知之處增長的可能就增加。對某些範圍，保護個人資料大部分倚賴每個人。

對損害預作準備

對於使用者教育關鍵資訊安全觀念，例如社交工程、電子隱私 e-privacy 和網際空間安全（cybersecurity)很重要。

關於公司監控、存取數位通訊和電子檔案應該只有在合法的業務理由下執行，例如技術維護、監視系統安全、符合公司政策和/或是法律規定、調查不端行為、欺騙或犯罪的辯解與申訴。使用者應被告知其電子通訊可能因為上述理由而被存取。

當資料被用來做為行銷目的，個人應該在任何時間有機會決定不參與此項安排。

針對資料保管者其功能與角色提供特別的訓練很重要，以確保在其責任下對資料提供適當的防護措施。資料保管者承擔對於敏感性資料的存取准駁以及適當的資料機密分級之責任。

執行定期的資訊安全覆核、稽核、資料隱密性政策和程序與主動監控新安全弱點可協助確保維護適當的資料保護標準。啟動資訊安全成功建置的關鍵策略是高階管理者的支援。

表 1—資訊安全威脅範例	
威脅	**範例**
馬虎的用戶	• 在社群網站 透過標示照片或影片交換個人資料 (臉書, LINKEDIN 和推特 TWITTER) • 在公眾網站上傳圖像、影片與聲音記錄或文件
社交工程	• 被騙提供個人資料或透過語音通訊(例如在講電話過程)向陌生人洩漏敏感資訊 • 透過虛構或匿名身分達到蒐集網路上其他人資訊的目的
不恰當的資料處理	• 提供特定目的使用的資料,透過故意的竄改或非故意的誤用使用於其他用途
將訊息送到錯誤的收件者	• 由於人為疏失將電子郵件與語音郵件訊息散播給非計畫中的收件
弱邏輯存取控制	• 於使用中弱通行碼/無通行碼保護
實体安全的破壞	• 遺失或被竊取的筆電行動裝置與可攜式儲存設備 LOST/STOLEN LAPTOPS, MOBILE DEVICES AND PORTABLE DISK STORAGE
利用從監控的裝置蒐集的資訊	• 藉由撥號者識別碼特徵從電話號碼指出發話來源 • 監視相機與記錄裝置用於捕捉個人移動因此特定事件將來可以重播或揭露 • 隱藏式的小型電子裝置秘密地錄製受禁止的影像 • 用戶活動的記錄（例如網際網路瀏覽歷史,小型文字檔案(cookies),電子郵件,印表機和傳真機日誌)
不安全的網路連接	• 花很多時間在作商務旅行的人其不安全的撥接和粗心的無線網路使用 • 透過遠端連接不安全地存取公司資料庫（例如資料傳輸未經加密） • 通訊流量的攔截與竊聽（例如利用藍芽技術的漏洞) • 連接至產品或存貨清單、識別證、護照或行李並用於個人追蹤和檢歷的 射頻識別標籤
惡意程式	• 未經保護的家用電腦（攻擊者更喜歡) • 藉由電子郵件交換附加檔案,透過網站廣告或網路連結下載 ，使用惡意軟體存取電腦而取得控制權
系統除役	• 系統中的敏感資訊未經適當抹除而遭棄置 SENSITIVE INFORMATION REMAINING ON SYSTEMS THAT ARE DISPOSED OF WITHOUT PROPER ERASURE

結論

隨著通信技術不斷演進，源自於個人資料的安全侵害，考慮到損失的範圍與種類，必須由隱私專家[22]執行持續性的風險評估。並配合這樣的努力，需要更嚴格的政策與規定降低不斷成長的威脅。根據前美國司法部部長 Earl Warren 表示"電子通訊驚人的進步造成了個人隱私更大的危險,"[23]，因此，個人資訊保護和安全對於能影響對抗隱私權侵害的政策與法律發展的隱私權專家必須是優先考慮的事情。隱私權法律在許多國家仍處在嬰兒期，每個主要個體應該持續參加防止與偵測個人資料的濫用的行動。持續的資訊安全作戰必須恰當地教育使用者關於其個人資料遭竊以及保護個人資料的控制措施。在使用者認知行動的關鍵成功因素是 C-階層(C-level)支援-藉由範例與可歸責性展現給領導階層。此任務可透過和非營利性隱私權保護組織的利害關係人伙伴關係延伸宣傳至公眾資訊媒體而普遍地教育使用者。簡而言之，資料隱私權是每一個人的責任。

資料隱私是每一個人的責任

ENDNOTES

1. *onemon Institute, "2012 Confidential Documents at Risk Study," July 2012, www.ponemon.org/blog/post/2012-confidential-documents-at-risk-study*
2. *Privacy Rights Clearinghouse, "Chronology of Data Breaches, Security Breaches 2005–Present," 2005, https://www.privacyrights.org/data-breach*
3. *Merriam Webster's Collegiate Dictionary, www.webster.com*
4. *Op cit, Privacy Rights Clearinghouse*
5. *Health, Education, Welfare (HEW), Advisory Committee on Automated Data Systems, The Code of Fair Information Practices, http://epic.org/privacy/consumer/code_fair_info.html*
6. *Tech Target, "The Gramm-Leach-Bliley Act," http://searchcio.techtarget.com/definition/Gramm-Leach-Bliley-Act*
7. *SOX-online, "Sarbanes-Oxley Act," www.sox-online.com/sarbanes_and_oxley.html*
8. *Health Insurance Portability and Accountability Act(HIPAA), http://samples.jbpub.com/9780763766207/66207_CH02_McConnell.pdf*
9. *"UK Privacy and Electronic Communications Regulations :E-mail, Faxes, Phone Calls, and Cookies,"http://www.the-dma.org/international/articles/UKElectronicprivacyreg.PDF*
10. *Axelrod, C. Warren; Jennifer L. Bayuk; Daniel Schutzer; Enterprise Information Security and Privacy, Artech House, 2009, appendix A*
11. *The expression "externally driven mandates" refers to changes that are driven or mandated by an external source (e.g., regulatory requirements, industry standards).*
12. *Forrester Research, "Forrester's Global Data Protection and Privacy Heat Map," 2011, http://heatmap.forrestertools.com*
13. *National Conference of State Legislatures, www.ncsl.org/issues-research/telecom/security-breach-notification-laws.aspx*
14. *European Network and Information Security Agency, European Union, 2011, www.enisa.europa.eu/activities/identity-and-trust/risks-and-data-breaches/library/deliverables/dbn*
15. *PCI Security Standards Council, www.pcisecuritystandards.org*
16. *National Institute of Standards and Technology, www.nist.gov/index.html*
17. *Brandeis, Louis D.; Samuel D. Warren; "The Right to Privacy," Harvard Law Review, vol. IV, no. 5, December 1890, http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm*
18. *BBC News Technology, "Google 'in Breach' of UK Data Privacy Agreement," 2012, www.bbc.co.uk/news/technology-19014206*
19. *Borden, Sarah; "Wyndham Hotels Data Breach," Bloomberg.com, 2012*
20. *CBC News, "Elections Ontario Discovers Privacy Breach of Voter Data," 2012, www.cbc.ca/news/canada/windsor/story/2012/07/16/toronto-elections-ontario-privacy-breach.html*
21. *ISACA, Geolocation: Risk, Issues and Strategies, 2012, www.isaca.org/research*
22. *Nonprofit privacy organizations as well as enterprise representatives from human resources, security, IT, internal audit, records management, legal and other function with aspects of their roles dedicated to dat privacy*
23. *Warren, Earl; www.judiciary.senate.gov/hearings/estimony.cfm?id=e655f9e2809e5476862f735da16302cc&it_id=e655f9e2809e5476862f735da16302cc-0-0*

Quality Statement:

This Work is translated into Chinese Traditional from the English language version of Volume 2, 2013 of the ISACA Journal articles by the Taiwan Chapter of the Information Systems Audit and Control Association (ISACA) with the permission of the ISACA. The Taiwan Chapter assumes sole responsibility for the accuracy and faithfulness of the translation.

品質聲明：

ISACA臺灣分會在ISACA總會的授權之下，摘錄ISACA Journal 2013,Volume 2中的文章進行翻譯。譯文的準確度及與原文的差異性則由臺灣分會獨立負責。

Disclaimer:

The ISACA Journal is published by ISACA. Membership in the association, a voluntary organization serving IT governance professionals, entitles one to receive an annual subscription to the ISACA Journal.

Opinions expressed in the ISACA Journal represent the views of the authors and advertisers. They may differ from policies and official statements of ISACA and/or the IT Governance Institute and their committees, and from opinions endorsed by authors' employers, or the editors of this Journal. ISACA Journal does not attest to the originality of authors' content.

Instructors are permitted to photocopy isolated articles for noncommercial classroom use without fee. For other copying, reprint or republication, permission must be obtained in writing from the association. Where necessary, permission is granted by the copyright owners for those registered with the Copyright Clearance Center (CCC), 27 Congress St., Salem, MA 01970, to photocopy articles owned by ISACA, for a flat fee of US $2.50 per article plus 25¢ per page. Send payment to the CCC stating the ISSN (1526-7407), date, volume, and first and last page number of each article. Copying for other than personal use or internal reference, or of articles or columns not owned by the association without express permission of the association or the copyright owner is expressly prohibited.

免責聲明：

ISACA Journal係由ISACA出版。ISACA 為一服務資訊科技專業人士的自願性組織，其會員則有權獲得每年出版的ISACA Journal。

ISACA Journal收錄的文章及刊物僅代表作者與廣告商的意見，其意見可能與ISACA以及資訊科技治理機構與相關委員會之政策和官方聲明相左，也可能與作者的雇主或本刊編輯有所不同。ISACA Journal 則無法保證內容的原創性。