資訊時代，隱私已死？標準有話說

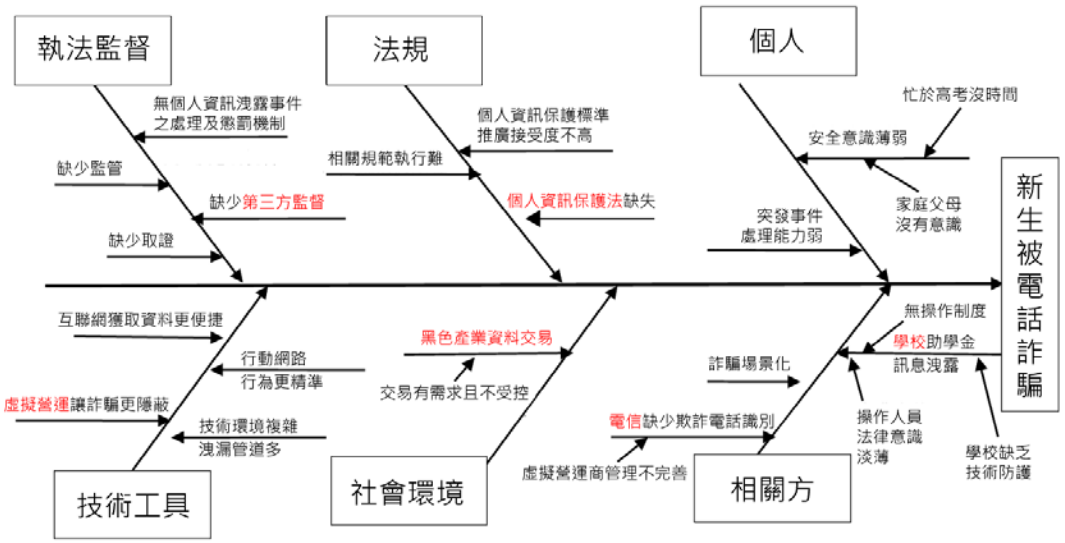
原文刊載於 BSI 中國的《標準+》期刊第 20 期，本文經 BSI 台灣編譯。

撰文：BSI 英國標準協會
潘 蓉
亞太區首席標準專家

全球爆發的勒索病毒「永恆之藍」餘音未消，加之 2016 年發生的網路安全、隱私洩露等重大事件帶給人們的驚恐與反思仍彌留至今，比如：國際上的雅虎資料洩露事件，大陸山東臨沂準大學生徐玉玉遭遇電信詐騙自殺身亡事件等等。

互聯網與資訊技術的高速發展，為民眾帶來便利之時，卻也有一部分不幸淪為受害者。作為一個資料治理工作者，感性、同情、轉知教育孩子與他人之外，也用系統化思維從個人、組織、社會與產業、法規與標準推廣進行了具體實施層面的思考。

以震驚社會的新生「徐玉玉事件」為例，先用一張魚骨圖來思考其被騙的原因：



[點擊可查看大圖]

下面看看具體的分析與應對建議：

1　個人

從個人來看，缺少防範意識，不知曉詐騙的通用伎倆，如通過口音、來電號碼、轉帳請求等判斷詐騙傾向，涉及轉帳等重大事項操作未經查核確認。

倡議全民增強資訊時代的安全意識，瞭解使用設備的安全防範技巧，對於收集個人資料隱私的環節要求明確用途和控制手段，對於錢財的轉移設定不同控制許可權，比如大額支付雙人操作。

2　資料鏈

從資料鏈的相關方來看，學校存有大量學生資料，本案例涉及採集了學生的完整身份資訊，也有助學金發放等即時精準行為資訊，是否有規章制度要求從採集、儲存、處理、傳輸、使用、銷毀等保護個人資訊，操作人員是否有相關意識，在上述環節操作注意防止洩露，學校是否有相適應的技術措施防止來自網路的攻擊，給駭客留下方便之門？

電信營運商作為詐騙電話傳送媒介，是否對虛擬營運商的管理做到實名制？如何監管虛擬營運商的運作？對於欺詐電話有沒有反欺詐機制和消費者提醒？電信掌握著消費者精準的個人身份與地點、通訊資訊，是高價值的資料金礦也是罪犯垂涎之地。

類似筆者去過的一個智慧制卡機構，看到各地社會基金保險局委託製作個人社保卡，在資料的傳送、實體卡的運輸、裝箱單的要求方面，居然嫌麻煩，要求制卡商明文列印姓名、身份證號、社保卡號、電話等資訊作為裝箱單，這些擁有大量個人敏感資訊的國家機關因為沒有商業公司供應鏈的強制要求，反而是資訊安全管理的漏洞。

本案例詐欺犯能精準運用場景詐騙，說明獲取了完整的個人身份資料和即時行為資料，這些資料的獲取與利用是產業化運作的結果，資料黑色產業依靠互聯網、巨量資料技術，以非法交易獲取個人資料，最後使用虛擬營運商的服務偽裝騙取受害人。

！ 提倡：

擁有大量個人資料的組織：

- 實施資訊安全管理及個人資料保護標準；
- 明確資訊安全責任人，也可設立首席隱私官；
- 建立內控制度防範操作風險；
- 建立內稽制度，發現洩露風險及時糾正；
- 建立個人資料洩露的報告、處理、賠償機制；
- 自建或依靠協力廠商的能力，建立動態的風險監控與防範機制。

3 法律標準

從法規標準層面看，自 6 月 1 日開始，大陸《網路安全法》正式實施。作為大陸第一部關於網路安全的綜合性法律，保護公民個人資訊安全是其重要內容。《網路安全法》正式實施後，又有什麼合適的工具幫助落地？

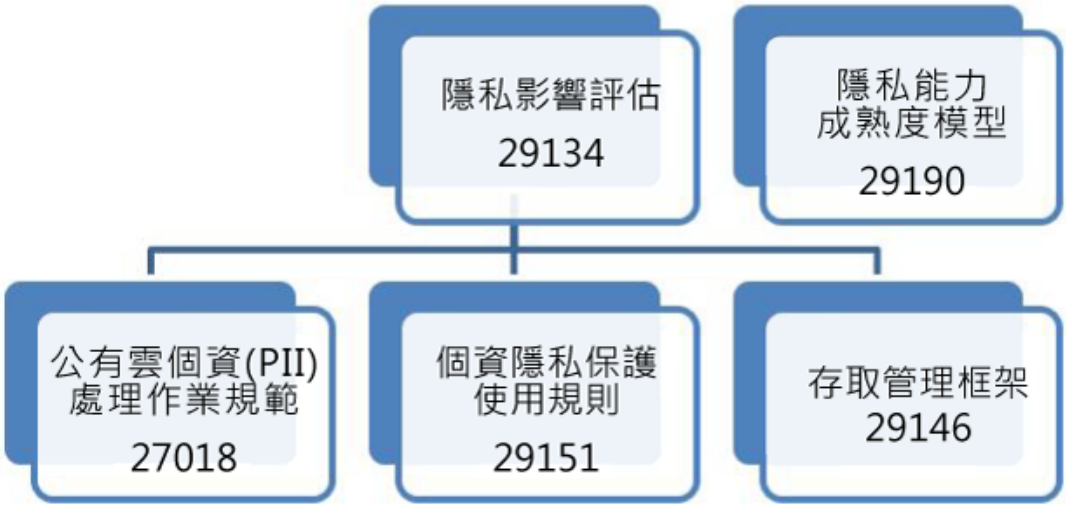
BS 10012:2017 ——個人資訊管理標準則是對 BS 10012:2009 版的修訂，此次修訂符合 2016 年 4 月 14 日正式通過的歐盟一般資料保護法案(GDPR) 的要求，並為全面資料治理中的個人資訊保護提供了一個良好框架；《資訊安全技術公共及商用服務資訊系統個人資訊保護指南》明定了個人敏感與一般資訊，也規範了資料生命週期的操作要求，但不是強制標準，宣傳推廣與接受度受限；金融電信等有行業規範要求保護個人資訊，隨著雲端、大數據、物聯網、行動通信等技術的發展，各類 APP 的安裝，越來越多的個人資訊在民眾不知道的情況下被收集被利用；在呼喚個人資訊保護法的國家基本大法頒布的同時，我們看到更

務實的做法是借鑒國際標準，融合行業要求，推動個人資訊保護的最佳實務認知。

建議推廣與訓練國際、國內標準作為個人資料保護的起點。

目前在個人隱私資料保護方面，可以參考國際標準將操作規範與指南具體化：

- ISO 29100:2011 資訊安全技術-隱私框架標準



與隱私保護相關的技術與應用類標準還有：

- ISO 27017：雲端服務之資訊安全作業規範
- ISO 27018：雲端服務之個資保護作業規範
- BS 10012:2017：個人資訊管理
- ISO 19608：制定安全與隱私功能要求之指南
- ISO 29191:2012：部分匿名及部分去連結鑑別之要求
- ISO 27040：儲存安全

與行業應用相關的標準有：

- ISO 27799：健康資訊安全管理
- ISO 27015：金融服務的資訊安全管理

- ISO 27019：能源行業的資訊安全管理
- ISO 27011：電信營運商的資訊安全管理

與資料取證相關的標準有：

- ISO 27037：數位證據的識別、收集、獲取與保全
- ISO 27042：數位證據的分析與解釋指南
- ISO 27043：事件調查原則和過程指南
- ISO 30121：數位取證風險框架的治理

社會環境中資料黑色產業盛行，中國互聯網協會 《中國網民權益保護調查報告 2016》顯示，近一年時間，大陸 6.88 億網路用戶因垃圾短信、詐騙資訊、個人資訊洩露等造成的經濟損失估算達 915 億人民幣。

對於黑色產業的盛行，倡議全民監督，發現資料洩露就舉報，結合平臺工具利用大數據治理資料黑色產業，形成眾治的力量；行業或協會組織採用各種新型手段場景化、移動、即時、及時促進全民防詐騙防風險的意識。

4 執法監督

從執法監督來看，目前大陸沒有專門的機構負責監控個人資料的使用情況，據騰訊研究院法律研究中心首席研究員蔡雄山在「網路空間治理創新」沙龍上介紹，歐盟每個成員國都設立了專門的資料保護局監督個人資料保護的執行情況，審批資料的流動，擁有檢查和處罰的權利；以美國為代表的是基於行業自律，通過產業協會、互聯網協會，及驗證機構等進行個人資料保護的驗證，是行業與市場認可的機制。鑒於現有的國際標準，歐盟與美國供應鏈及資訊流通的要求，及國內的現有的行業規範、協力廠商認證資源。

建議推動協力廠商的個人資訊保護驗證監督工作，發揮中立、市場的力量監督標準、規範、法規的執行。

5 技術工具

從技術工具來看，所謂道高一尺魔高一丈，大數據蘊藏著價值，也為隱蔽攻擊提供了空間。

建議產業政策應鼓勵和支援大數據安全技術研究的企業，從攻、防、取證、稽核開發應用新技術，以大數據治理資料洩露；應鼓勵和支持理論與標準化研究人員歸納整理最佳實務，及時頒布管理與技術標準，提升行業、社會的資料治理水準。

媒體的覺醒，喚起民眾的意識，更應喚起法規標準的跟進，每個角色都應盡職盡責保護一個安全的資料天空。●

延伸閱讀

本文章從國際上的日常案例出發，以不同角度與層面分析隱私與資料治理的現狀，並從 BS 10012 個人資訊管理國際標準延伸，提供實質的應對建議，亦點出法令法規與標準在個資管理的關鍵性。

從金融業、公部門到各產業界，已被全球廣泛運用的 BS 10012 標準在 2017 年 4 月正式改版，您可以進一步透過 BSI Taiwan 個資管理專家 – 章鈺 (Oscar) 的最新文章，深入了解本次改版的緣起、脈絡與驗證/轉證重要時程...

【從新版 BS 10012:2017 標準看資訊治理要求】

<閱讀全文>