信用卡業者與持卡人一定要知道的資料安全事項

國際信用卡組織訂定一個安全規範 PCI (Payment Card Industry)，這個 PCI 資料安全規範要求所有信用卡會員、 商店、服務提供者，在儲存、處理、與傳遞持卡人資料時需要做到的安全事項。

PCI 裡定義了六大類安全議題, 共包括 12 項要求 (Requirements), 簡述如下:

建置與維護一個安全的網路
要求一: 使用防火牆
要求二: 不要使用系統內定的密碼及參數

保護持卡人資料
要求三: 保護儲存起來的資料
要求四: 在公用網路上傳輸持卡人資料及敏感性的資訊一定要加密

弱點管理
要求五: 使用與定期更新防病毒程式
要求六: 發展與維護安全系統與應用程式

使用強壯的存取控制機制
要求七: 只讓有業務上需要的人才能存取資料
要求八: 每一個人都使用不同的 ID
要求九: 限制實體上的接觸資料

定期稽查與測試網路
要求十: 追蹤與稽查所有存取網路資源與持卡人資料的動作
要求十一: 定期的測試安全系統與流程

維持資訊安全政策
要求十二：維持一個能滿足資訊安全的政策

我們先來看比較令人好奇的要求三: 保護儲存起來的資料，PCI 的要求是這樣的:

加密(Encryption)是最好的保護機制，因爲即使有人能夠破解層層保護關卡而取得加密過的資料，沒有破解加密方法, 他也無法讀懂這些資料。
1. 除非業務上的需要及法律上的要求，應儘量限制資料儲存的時間與範圍
2. 不要儲存後續要用來授權的認證資料

(1) 不要儲存卡片磁條(或晶片)裡的全部內容
(2) 不要儲存卡片驗證碼 (CVV2 or CVC2)
(3) 不要儲存個人驗證碼 (PIN, PVV)

3. 顯示(Display)資料時要遮蓋起來(Mask) (最多顯示前面六碼與後面四碼)
4. 敏感性的持卡人資料儲存時要將其亂碼成無法閱讀的格式 (包括可攜式的磁碟, 備份媒體等), 應使用下列方式來亂碼:
(1) 單向的 Hash (如 SHA-1)
(2) 截斷 (Truncation)
(3) 堅固的加密演算法, 例如 Triple-DES 128-bit, AES 256-bit 與金鑰(key)管理程序
5. 保護加密金鑰以防洩漏與誤用
(1) 只允許最少的存取金鑰的人員
(2) 只允許最少的存放金鑰的地點與方式
6. 金鑰管理之程序與流程的文件與執行
(1) 堅固金鑰的產生
(2) 安全的金鑰發送
(3) 安全的金鑰保管
(4) 定期換金鑰
(5) 舊金鑰的銷毀
(6) 金鑰管理權限分散 (兩人以上, 每人僅知道一部分內容)
(7) 預防無授權的金鑰替換
(8) 已知或有安全疑慮的金鑰應立即換掉
(9) 舊的或無效的金鑰應撤銷 (主要指 RSA Keys)
(10) 金鑰保管人必需簽署文件同意其知道並接受金鑰保管人的責任

上述是 PCI 規範中對持卡人資料在電腦儲存時的安全要求. 我們不知道台灣相關業者(主要指發卡銀行, 當然還包括提供信用卡交易相關的資訊平台或系統廠商, 商家…等)是否完全遵照規定保護好我們的個人資料. 例如網路購物, 一定會留下信用卡號及個人基本資料, 我們不知道這些商家是如何儲存我們的資料的, 萬一資料檔案遭竊或遺失, 誰知道後續會發生什麼事情.

參考資料:
http://usa.visa.com/download/business/accepting_visa/ops_risk_management/cisp_PCI_Data_Security_Standard.pdf
http://www.asiapeak.com/download/SecureDB_VisaMasterCard.pdf
http://www.asiapeak.com/download/loyalty_lab.pdf