ISSN 1023-2842
中山管理評論　2016 年十二月號
第二十四卷第四期　p.663-703
DOI: 10.6160/2016.12.01

# eTrust 網路銀行個資事件

# Personal Information Leakage on eTrust Netbanking

游士瑩 *Shih-Yin Yu*
上海交通大學凱原法學院經濟法研究所
Institute for Economic Law,
KoGuan Law School of Shanghai Jiao Tong University

蘇雅惠*[*] *Yea-Huey Su*
國立中央大學資訊管理學系
Department of Information Management,
National Central University

林裕得 *Yu-De Lin*
旭得數位有限公司
ZID CO., LTD

連文雄 *Wen-Shiung Lian*
國立中央大學資訊管理學系
Department of Information Management,
National Central University

本文引用格式建議：游士瑩、蘇雅惠、林裕得、連文雄，2016，「eTrust網路銀行個資事件」，中山管理評論，24卷4期：663~703。
Suggested Citation: Yu, S. Y., Su, Y. H., Lin, Y. D., and Lian, W. S., 2016, "Personal Information Leakage on eTrust Netbanking," **Sun Yat-sen Management Review**, Vol. 24, No. 4, 663-703.

[*] 通訊作者：蘇雅惠，suesu@mgt.ncu.edu.tw

# 摘要

本個案是一個真實事件的管理層級之圖書館個案，藉由本教學個案讓學生可以學習個人資料保護以及資訊安全管理等相關議題。行動數位時代，個資保護已然成為顯學，資訊安全議題不再只是管控流程的作業層級議題，而是公司政策的管理議題。自 1997 年以來，中信銀進行 e 化及資安建置，然而在此次由 ptt 鄉民揭露的個資外洩事件中，卻凸顯了其資安管理的問題。資安管理的本質其實是代理問題，代理問題其實涉及一個公司資訊部門定位與資安人力成本議題，透過對於檢討中信銀內部資安管理制度與落實內控流程，讓學生得以進一步理解資訊人在金融業其實不宜只是支援角色，而是應該做領頭羊角色，以因應制度或環境快速變遷。而在整個危機處理過程中，看似完美堪為典範的危機處理背後，卻仍有不小的隱憂存在，究其根本原因是現行制度下的成本議題－個資外洩所必須付出的代價對金控公司而言其實微不足道，本個案透過討論銀行對於成本的權衡取捨行為，讓學員得以重新思考成本的意義。

**關鍵詞：**個資保護、資訊安全管理、代理問題、內控流程、成本權衡取捨

# Abstract

In this library case we pursue the objectives for students to realize the issues related to personal information protection and information security management. It has been more matter for the issue of personal information protection since the mobile age. Information system security is a management-oriented rather than an operation-oriented or a technology-oriented issue. The event of personal information leakage on eTrust netbanking has led the critical problems about information security within CTBC Bank. The nature of information security management is an agent problem which involves the positioning of MIS department and the philosophy for human cost within a company. By discussing the internal control processes of CTBC Bank, the case looks at the challenges CTBC facing in a dynamic environment to regard MIS department not as a supporting role but a creating one. This case is also a good vehicle to focus on the cost tradeoff issues for students to rethink of the nature

of cost for a finance holding company.

**Keywords:** Personal Information Protection, Information Security Management, Agency Theory, Internal Control Process, Cost Tradeoff

# 壹、事情是從 ptt 開始的…

2013 年 5 月 13 日晚上九點左右，一位 ptt 鄉民貼文爆卦 (詳見圖 1-1)[1] 指出，因接到不認識的房仲業者打到他家的室內電話詢問，讓他驚覺自己的個資可以透過 Google 被查詢到。ptt 鄉民們紛紛於此貼文下方留言熱議到凌晨左右，時值 5 月 10~16 日「鍵盤開戰行動[2]」事件，台灣與菲律賓兩國駭客陸續攻擊或癱瘓對方重要官方網站 (但不包含交通、金融、醫療資源等民生必需相關網站[2])，因此有兩位鄉民嘲諷「其實是菲律賓駭客搞的[1]」「菜鳥工程師快推給菲律賓就可以無事了[1]」

Disp BBS guest 註冊 登入(i) 線上人數: 3100 回列表
(←) 分享
※ 本文轉寄自 ptt.cc 更新時間: 2013-05-14 06:15:09
作者 iam186 (iam186) 看板 Gossiping
標題 [爆卦] 某銀行疑似洩漏個資
時間 Mon May 13 21:04:25 2013

因今天某房仲打到我家室內電話來問是否持有某新竹的房產.
但就很好奇他是怎麼取得我家的電話的.
[C 他說他是 google 來的,還說我可以自己 google 看看.
結果 google 下去不得了了~~
大家快來看看自己繳費時有沒有留下電話歐!
http://ppt.cc/KirT

應該是不知哪個死菜兵第一天寫程式
撈錯 table,開心的跑完 for 迴圈也不上線首驗
就這樣把大家的資料公諸於世
大家進去檢查一下吧,option 裡面大約有四千多筆資料

圖 1-1 一位 ptt 鄉民貼文「 [爆卦] 某銀行疑似洩漏個資」之本文[1]
資料來源：註腳1 http://disp.cc/b/337-5GSB

[1] http://disp.cc/b/337-5GSB (access date: 2016/4/12)
[2] 此為 2013 年 5 月 9 日上午廣大興事件－台灣的民間漁船廣大興號遭菲律賓海巡署的公務船以機槍射擊造成船長中彈身亡事件－所引發的台菲兩國網路駭客於 5/10 開始之網路戰爭行為後續事件。https://zh.wikipedia.org/wiki/鍵盤開戰行動 (access date: 2016/4/12)

次日新聞指出：用戶在中信銀 eTrust 網路銀行 (下文簡稱 eTrust) 繳費中心網頁下拉常用繳費項目時，顯現數量眾多的個人資料[3]。「……此事件於 ptt 上爆料之後，隨即於網路間傳開，有科技部落客連上 eTrust，發現洩漏的個資包含姓名、電話號碼、手機號碼、身份證號碼、信用卡卡號、人壽保險號碼、交通違規罰款編號、車主身分證字號、出生年月日……等，估計約有五萬七千多筆，並且不需要登入網站即可看見。」[3]

中信銀商業銀行 (下文簡稱中信銀) 於 5 月 14 日發布新聞稿表示「接獲客戶通知後，在 5 月 13 日晚上 10 點就已經緊急關閉該繳費中心網頁，並聯繫 Google 刪除暫存的網頁」[4]，新聞稿中證實繳費網頁出錯，但否認有網銀交易資訊外洩[4]。

eTrust 此個資外洩事件，是新版《個人資料保護法》 (下文簡稱個資法) 自 2012 年 10 月 1 日正式實施後發生的第一起銀行個資外洩事件[4]。狀況顯示個資已經被 Google 收錄，因此引發銀行用戶對個資安全的疑慮。

# 貳、We Are Family

中信銀金融控股 (股) 公司 (下文簡稱中信銀) 成立於 2002 年 5 月 17 日，最初由中信銀以股份轉換方式成立，企業總部設於臺灣臺北市，全球員工人數超過 15,000 人。中信銀是中信銀全資擁有的子公司，前身為由辜振甫先生發起成立於 1966 年的「中華證券投資公司」，2014 年 7 月為止，為臺灣第一大信用卡發卡銀行。1999 年 12 月，中信銀開辦網路銀行服務。[5, 6, 7]

中信銀官網公佈自 2005 年伊始連年得獎記錄，2012 年官網條列國內共 29 與國外共 34 單位頒給的獎項。例如：中信銀於 2012 年元月榮獲歐洲貨幣雜誌 (Euromoney, January 2012) 評選為「臺灣最佳本國財富管理銀行 (Best Local Private Bank)」、「最佳客戶資料保密與安全機制服務 (Best for Privacy and Security)」、以及「最佳高資產客戶銀行服務 (Net Worth Specific Services—

[3] https://tw.news.yahoo.com/中國信託網路銀行疑個資外洩-五萬多筆資料看光光-025435160.html (access date: 2016/4/12)
[4] http://www.ithome.com.tw/node/80425 (access date: 2016/4/12)
[5] http://www.ctbcholding.com/abo_intro.html (access date: 2016/4/12)
[6] https://zh.wikipedia.org/wiki/中國信託金融控股 (access date: 2016/4/12)
[7] https://zh.wikipedia.org/wiki/中國信託商業銀行 (access date: 2016/4/12)

super affluent US$500,000 to 1 million )」。[8]

展望未來，中信銀控將秉持著「We are family」的品牌精神，「守護與創造」的企業使命以及「關心、專業、信賴」的品牌特質，為客戶提供更方便的服務管道和更多元的金融服務，打造臺灣第一、亞洲領先的領導品牌，成為客戶心目中最值得信賴的金融服務機構。[5]

# 參、中信銀之 e 化及資訊安全管理

1997 年至 2001 年間，中信銀導入 Financial Network Service (FNS) 系統。1999 年 12 月，中信銀開辦網路銀行服務。2002 年中信銀重金投資、拍攝的「感謝廣告」影片，主要是向推動 e 化的員工表示謝意。這一項投資 10 億元、歷時 3 年 (從 1997 年開始、2001 年 1 月上線 FNS) 的企業 e 化改造工程，讓中信銀從此脫胎換骨，不僅加速了新服務上市和業務流程，也奠定了未來邁向國際的基礎。1994 年中信銀剛改制，一切都還在摸索階段，當時金融界的 IT 應用仍傾向保守，而最賺錢銀行的幕後 IT 推手則是張汝恬，她於 1996 年借調到中信銀，因表現良好，於是被董事長辜濂松直接延攬到企業內部。從中信銀的公司年報顯示，張汝恬於 2010/4/12~2012/6/29 擔任資訊長 (CIO)，而中信銀 2013 年報內的組織圖已經沒有資訊長一職了。[9, 10]

2008 年左右，中信銀資訊管理部協理張碩暉表示：「中信銀的 IT 部門，成立之初就被要求要支援業務，4、5 年前更被要求要實現業務的發展，在這樣的情況下，IT 人員當然會瞭解業務的需求。2 年前，中信銀的 IT 組織再造，將原來集中式的資訊管理，改為視需要來和業務串連，至今變成只要和業務有關的應用，IT 的老闆就是各事業單位的主管，IT 思維當然會符合業務的需求。中信銀每年會選一個年度的重要創新業務，在這項業務上，不僅要衝第一家、也要衝最快，對 IT 來說，就是資訊系統要能跟得上，像在 1974 年推出國內第一張信用卡、1990 年是第一家獲准到國外設立據點的民營金融機構等。而 1994 年成立台灣第一家無人銀行，也讓網路和通路開始展開密不可分的關係。一開始是因為要推自動化設備才建置無人銀行，所以中信銀的網路銀行甚至還提供客戶撥接網路的服務，到了 2000 年，政府核准網路銀

[8] http://www.ctbcholding.com/honor12.html (access date: 2016/4/12)
[9] http://www.ithome.com.tw/node/28216 (access date: 2016/4/12)
[10] http://www.ctbcholding.com/ir_index.html (access date: 2016/4/12)

行，才在網路上提供服務。」[11]

2009 年左右，中信銀拉高了資安委員會 (Security Review Board) 的層級，成為更符合現況的資安政策，該組織是直接報告到作業風險層級，任何資安政策在各部門要如何落實、執行都會透過這個委員會形式的主管機構來形成一個機制，其中包含了資訊、人事、稽核、法務、事業單位、風控代表等，原來是只有在中信銀體系裡建立，如今已經拉到金控的階層，並且會與金控的其他子公司進行意見交換、彼此分享。[12]

而與資訊安全管理制度相關的銀行必定遵守的「金融機構辦理電子銀行業務安全控管作業基準 (下文簡稱安控法)」以及「中信銀內控內稽制度」，則分別摘錄於附錄 A5 及附錄 A6。

# 肆、中信銀 eTrust 網路銀行客戶個人資料外洩事件

2013 年 5 月 13 日晚上九點左右，一位 ptt 鄉民發文指出自己的個資可以在 Google 上輕易地被搜尋到，因而被鄉民們接力揭露此次 eTrust 客戶個人資料外洩事件。鄉民們發現在 eTrust 網站的繳費中心可隨意檢視大筆其他用戶的資料，而看過這些資料的部落客重灌狂人表示，繳費資料紀錄包含姓名、家中電話、手機、信用卡號等等總共有 5 萬 7000 多筆[13]。此部落客在自己的部落格發文說明此個資外洩事宜，並於文章一開始先表示「5/13 晚上 10:30 PM 更新：在文章發出去後沒多久，中信銀就把洩漏個資的網頁整個撤掉了，後來去查 Google，似乎還有少部分資訊還搜尋得到！但是在今天之前，有多少人看過、蒐集了這些已經暴露不知道多久的資料…沒人知道。」[14] 此部落客在其文章中，附上 eTrust 網站資料外洩的相關畫面截圖 (如圖 1-2～圖 1-7 所示)[14]。

[11] http://www.cio.com.tw/article_in.aspx?aid=398 (access date: 2016/4/12)
[12] http://www.informationsecurity.com.tw/article/article_detail.aspx?aid=5462#ixzz45aaZKo8r (access date: 2016/4/12)
[13] http://www.ithome.com.tw/node/80303 (access date: 2016/4/12)
[14] https://briian.com/10793/chinatrust-credit-card.html (access date: 2016/4/12)

打開之後，看起來是很正常的網頁，但是點一下選單，卻….


圖 1-2 部落客之部分截圖與說明一 [14]

資料來源：註腳14 https://briian.com/10793/chinatrust-credit-card.html

一堆不認識的人名、電話號碼就出現了。


圖 1-3 部落客之部分截圖與說明二 [14]

資料來源：註腳14 https://briian.com/10793/chinatrust-credit-card.html

代繳汽車燃料使用費的相關個資：


圖 1-4 部落客之部分截圖與說明三 [14]

資料來源：註腳14 https://briian.com/10793/chinatrust-credit-card.html

代繳中華電信手機費用的相關個資：

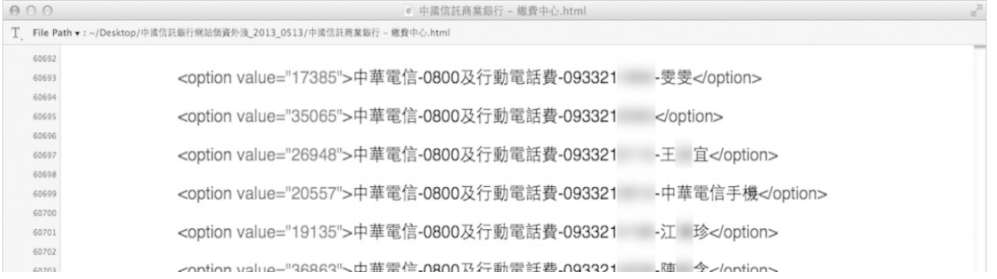


圖 1-5 部落客之部分截圖與說明四 [14]

資料來源：註腳14 https://briian.com/10793/chinatrust-credit-card.html

代繳信用卡卡費的相關個資，上面被遮住的都是信用卡卡號：

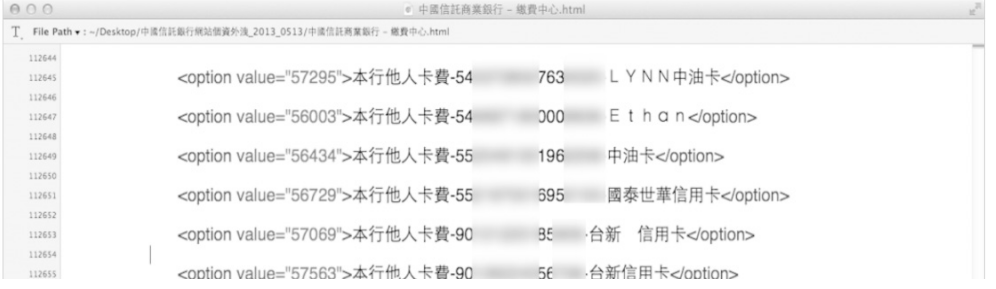


圖 1-6 部落客之部分截圖與說明五 [14]

資料來源：註腳14 https://briian.com/10793/chinatrust-credit-card.html

看樣子中國信託銀行網站的個資外洩問題**並不是最近兩天菲律賓駭客攻擊的成果**，**因為早就可以在 Google 上搜尋到姓名與電話號碼了！應該已經洩漏很久了…。**


圖 1-7 部落客之部分截圖與說明六 [14]

資料來源：註腳14 https://briian.com/10793/chinatrust-credit-card.html

5 月 14 日一平面媒體報導：「中信銀公關系統今凌晨回應指出，經內部查證，網銀繳費中心交易系統確實有異常，已先將該系統關閉，但外洩資料均為客戶自行設定的繳費項目 (如電費、水費) 及代號，並無任何客戶姓名與帳號資料外洩。」[15] 該媒體並報導：「5 月 13 日中信銀網銀約在十時於首頁公告：『由於目前交易量大，交易回應速度稍慢，若有無法登入網路銀行的情況，請您稍後再試，造成不便，敬請見諒。』」[15]。

該報導繼續指出：「針對 ptt 相關內容，中信銀公關系統回應，昨晚確有接獲客戶電話，反映網銀交易系統個資外洩，經調查，發現繳費中心交易系統確有異常，但尚無法確知是內部還是外部問題，因此先關閉繳費系統，但其他如網路轉帳等功能均正常運作。中信銀表示，已盡力向客戶說明及溝通，並維護客戶權益，惟針對網友爆料有客戶電話及姓名資料等外洩，中信銀強調，均為客戶自行設定透過網銀繳交費用項目及代號，客戶姓名、帳號等資料並未外洩。」[15]

5 月 17 日另一電子媒體指出，針對此個資外洩事件，金管會限一周完成災情調查。該媒體報導：「5 月 14 日中信銀書面表示，發生異常的是網路銀行『繳費中心』的常用帳號設定功能，這是專供客戶自行設定繳費項目及代號資料，和其他網路銀行的功能無關，也沒有承認有個資外洩，僅表示將主

[15] http://www.appledaily.com.tw/appledaily/article/headline/20130514/35016413 /中信銀網銀傳外洩四千筆個資 (access date: 2016/4/12)

動通知受駭用戶，並委由鑑識團隊調查。不過，金管會銀行局副局長邱淑貞表示，中信銀通報金管會時有說明，外洩個資都是使用者自行註記在備註欄中的資料，沒有信用卡卡號。」[4]「從網路釋出的網站出錯畫面中，可以看到中信銀網路銀行繳費中心網頁外洩的個資包括姓名、室內電話、手機、身份證字號及信用卡號資料等。這些資料都被 Google 搜尋引擎擷取到暫存網頁和索引中。」[4] 媒體報導表示：「經兆法律事務所律師黃意森表示，由於這起事件情節明顯，除非中信銀可以證明已經善盡保管義務，不然受害者可以向中信銀要求法定金額範圍內的賠償。預估受害者一旦提出訴訟求償，3.3 萬名受害者，中信銀可能將面對 1,650 萬元到最高 2 億元的賠償金額。」[4]「儘管中信內部仍在調查中，但若是內部疏失，聖藍科技研發技術長王建興認為，事件可能導因於資料庫程式設計的問題，導致查詢資料條件過於寬鬆，使用者能查詢到的資料遠多於其權限所賦予的。此外，他也認為系統上線前的測試環節不夠嚴謹，案例不夠完備，導致連最容易發生的狀況都沒有檢查到。王表示，雖然漏洞是因程式設計人員設計差錯，但是系統開發流程應要確保所有差錯在上線前，都已被偵測及修正，何況這是個相當明顯的失誤，只要妥善制定好開發流程，應該不難發現這個問題。」[13]

事件發生約一個多月後，6 月 20 日，台北金融系統論壇社發文報導中信銀商業銀行 IT 組織異動 (詳見附錄 A1)。而此事件後續在網路上的討論熱度則如附錄 A2 所示。金管會並於 2013 年 8 月 22 日公佈裁罰中信銀 400 萬元，裁罰全文詳見附錄 A3。金管會網站公佈自 2012 年 1 月以來的所有裁罰案件，關於銀行局 2012/1/1~2013/9/1 的裁罰統計數字則請參考附錄 A4。而此事件發生後，除了金管會裁罰中信銀 400 萬元以外，後續並沒有關於任何客戶告中信銀民事或刑事的相關新聞報導，也沒有中信銀挽回或補償客戶行動的相關新聞報導。附錄 A5 則補充後續相關事件或改變的相關資料。

中信銀在其 2013 年 7 月出版的「2012 年企業社會責任報告」[16] 第 26 頁則以「提高網路安全機制，保護客戶資料免於外洩」為標題，簡要說明此事件及公司針對此事件後的改善措施：

一、2013 年 5 月間發生部分客戶資料疑似洩漏事件，可能洩漏之資料為客戶於網路「繳費中心」自行設定代扣繳之電話號碼、電號、監理資費等常用繳費資料，並未包含帳務交易資料，可能受影響的客戶約 1 萬名。

[16] http://www.chinatrustgroup.com.tw/2012CSR.pdf (access date: 2016/4/12)

二、本公司為保障客戶權益，於 2013 年 5 月 14 日向警方報案，警察機關已著手進行調查。為確保不再發生此類事件，進行下列改善措施：

(一)專人電話聯繫或書面專函方式主動通知此一事件受影響之客戶，並妥適溝通客戶權益補償方案，於 2013 年 5 月 24 日完成。

(二)因應此一事件，針對類似網址內容設定之流程和權限控管，納入複核範圍。每季定期委由外部資安專家執行資安審核及滲透測試。

(三)針對常用繳費功能的「繳費資訊」欄位，部分資料採隱碼顯示，並提醒客戶避免於自行設定之「暱稱」欄位輸入個人資訊。

(四)於本公司網路銀行首頁放置相關聲明警示文句，提醒外界人士勿以非法或未獲授權方式擅自重製、摘錄、擷取、轉載、散佈或改作網站之全部或部份內容。

# 伍、問題與討論

一、 試分析中信銀在此次事件中，犯了哪些錯誤？你覺得個資外洩的問題，誰該負責？

二、 如果你是中信銀資訊部門最高主管，對於個資保護的資訊安全做到的程度，在成本、安全控制、及使用者便利性三者中，你會如何權衡取捨呢？

三、 你若是中信銀資訊部門最高主管，針對此次個資外洩事件，你覺得公司內部資訊安全管理制度如何能夠改善呢？是否需增加人手進行分工呢？

四、 發生個資外洩事件這類事件，「成本」與「商譽」何者較為重要？

五、 根據本個案提供的資料，你認為中信銀高層對於資訊管理部門的定位是什麼呢？如果你是中信銀資訊部門最高主管，你會如何因應呢？

# 陸、附錄 A

附錄 A1：台北金融系統論壇社發文報導中信銀商業銀行 IT 組織異動[17]

[17] http://www.tbics.com/node/1716 (access date: 2016/4/12)


台北金融系統論壇社
Taipei Banking IT Community Service

Home

中國信託商業銀行IT組織異動-2013-6-20,台北

Wed, 2013-06-19 21:19 — 加事伯

有消息來源指出，中國信託商業銀行對該行IT組織得的調整與人事異動如下

組織調整

1.原-資訊管理處下新設-資訊安全部，專責資安架構與管理。
2.應用系統規劃部、資訊架構規劃科、資訊作業部、資訊安全管理科改為-資訊安全部。

人事異動

1.台灣區個金事業總處-作業暨資訊處代理處長改調總經理辦公室專門委員。
2.台灣區個金事業總處-財富管理產品處處長楊淑惠暫代作業暨資訊處處長。
3.資訊管理處-應用系統規劃部部長許白芳調作業暨資訊處-個金資訊部部長。
4.資訊管理處處長歐久菁另兼應用系統規劃部部長。
5.資訊安全部-資訊架構規劃科科長黃建榮升任資訊安全部部長。

消息佈告類別: 人事與組織

圖 A-1 2013 年 6 月中信銀商業銀行 IT 組織異動 [17]
資料來源：註腳17 http://www.tbics.com/node/1716

附錄 A2：Google 趨勢之主題討論熱度

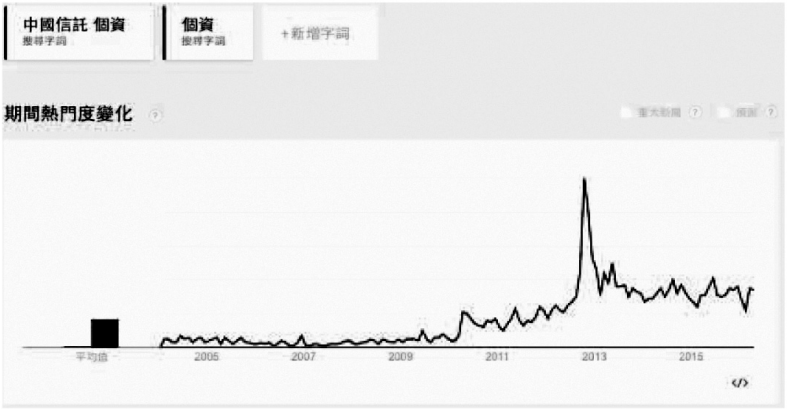


圖 A-2 中信銀個資與洩漏個資之討論熱度[18]
資料來源：註腳18 https://www.google.com.tw/trends/

[18] https://www.google.com.tw/trends/ (access date: 2016/4/23)

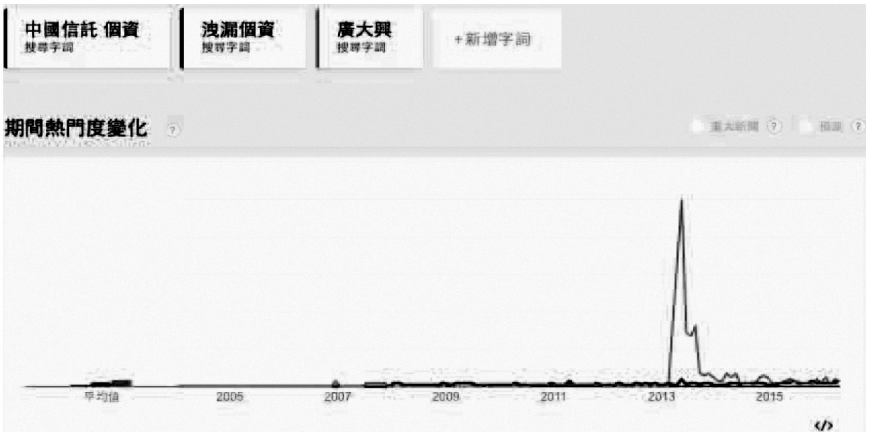


圖 A-3 中信銀個資與洩漏個資討論熱度 vs.廣大興事件討論熱度 [18]
資料來源：註腳18 https://www.google.com.tw/trends/

附錄 A3：金管會銀行局裁罰中信銀個資外洩案全文[19]

目前瀏覽位置：首頁 > 公告資訊 > 裁罰案件

裁罰案件

**中國信託商業銀行辦理網路銀行業務發生疏失，導致客戶個人資料外洩，核有未落實執行內部控制制度之缺失，違反銀行法第45條之1第1項規定，依同法第129條第7款規定，核處新臺幣400萬元罰鍰。**

受文者： 如正、副本

發文日期：中華民國102年8月22日

發文字號：金管銀控字第10200181601號

受處分人姓名或名稱：中國信託商業銀行股份有限公司

統一編號：03077208

地址：臺北市信義區松壽路3號

代表人或管理人姓名：童兆勤

身分證統一號碼：略

地址：同上

主旨：中國信託商業銀行辦理網路銀行業務發生疏失，導致客戶個人資料外洩，核有未落實執行內部控制制度之缺失，違反銀行法第45條之1第1項規定，依同法第129條第7款規定，核處新臺幣400萬元罰鍰。

[19] http://www.fsc.gov.tw/ch/home.jsp?id=131&parentpath=0,2&mcustomize=multimessages_view.jsp&dataserno=201308220001&aplistdn=ou=data,ou=penalty,ou=multisite,ou=chinese,ou=ap_root,o=fsc,c=tw&toolsflag=Y&dtable=Penalty (access date: 2016/4/12)

事實及理由：貴行於本(102)年4月13日將貴行之網站索引檔案上傳予網路搜尋引擎業者，惟貴行對網站索引檔案產出程式之設計未臻嚴謹，對相關檔案驗證方法及程序亦有欠周延，且未對貴行內部目錄網頁之讀取權限作嚴謹控管，導致一般網路使用者得進入瀏覽並取得貴行內部目錄網頁所留存之客戶資料，受影響之客戶數達33,320戶，資料筆數計57,297筆。貴行亦未能有效發現外部人士瀏覽貴行內部目錄網頁，核有未落實執行內部控制制度之缺失，違反銀行法第45條之1第1項規定。

法令依據：銀行法第129條第7款規定。

繳款方式：

一、繳款期限：自本處分送達之次日起10日內繳納。

二、請依本會銀行局檢附之繳款單注意事項辦理繳納。

三、本案聯絡人：蔡少懷，聯絡電話：（02）8968-9828，傳真電話：（02）8969-1359。

注意事項：

一、受處分人如不服本處分，應於本處分送達之次日起30日內，依訴願法第58條第1項規定，繕具訴願書經由本會（新北市板橋區縣民大道2段7號18樓）向行政院提起訴願。惟依訴願法第93條第1項規定，除法律另有規定外，訴願之提起並不停止本處分之執行，受處分人仍應繳納罰鍰。

二、受處分人如逾本處分所定繳款期限不繳納罰鍰者，即依行政執行法第4條第1項但書規定，移送法務部行政執行署所屬行政執行處辦理行政執行。

正本：中國信託商業銀行股份有限公司（代表人童兆勤）

副本：金融監督管理委員會檢查局、本會銀行局(金融控股公司組、會計室、秘書室)

附錄 A4：金管會銀行局 2012/1/1~2013/9/1 之裁罰統計數字[20]

金管會網站公佈自 2012 年 1 月以來的所有裁罰案件，銀行局於 2012/1/1~2013/9/1 總共裁罰 31 案件，其中有 5 個裁罰案是針對個人罰款 10 萬 (四件) 及 45 萬 (一件)，其他 26 件則針對銀行裁罰，相關統計數字詳見表 A-1。

表 A-1 金管會銀行局 2012/1/1~2013/9/1 針對銀行之裁罰統計表

| 處罰對象 | 處罰方式 | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 銀行 | 糾正 | 100萬 | 200萬 | 300萬 | 400萬 | 500萬 | 600萬 | 停止業務 | 停職 | 合計 |
| | 0 | 3 | 12 | 2 | 3 | 2 | 3 | 1 | 0 | 26 |
| 連帶解除銀行職員職務 | 0 | 0 | 7 | 2 | 1 | 2 | 0 | 0 | 0 | 12 |
| 連帶限制措施 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 |

資料來源：本研究整理

[20] http://www.fsc.gov.tw/ch/home.jsp?id=131&parentpath=0,2 (access date: 2016/4/12)

附錄 A5：金融機構辦理電子銀行業務安全控管作業基準[21, 22]

安控法乃銀行公會聯合各銀行討論出的自律規範，並送交銀行之主管機關－金管會銀行局核備，每家銀行一定會遵循並執行，因為金融檢查也會依據安控法來檢查。安控法的自 99 年 7 月開始陸續制定、核備、與修改，最新修訂版於 2016 年 4 月 1 日。本附錄摘錄銀行公會 102 年 3 月 28 日討論通過的安控法中，與本個案相關的部分條文如 2、網際網路應用系統之安全設計：

金融機構提供網際網路應用系統，應遵循下列必要措施：

(1) 載具密碼不應於網際路上傳送。

(2) 系統應設計連線 (Session) 控制及網頁逾時 (TimeOut) 中斷機制。

(3) 系統應辨識外部網站及其所傳送交易資料之訊息來源交易資料正確性。

(4) 系統應辨識客戶輸入與接收之非約轉交易指示一致性 。

(5) 系統應避免存在網頁程式安全漏洞(如 Injection、Cross-Site Scripting 等)

(6) 系統應偵測網頁與程式異動時， 進行紀錄與通知措施。

(7) 元件應驗證網站正確性。

下略

附錄 A6：中信銀官方網站之「內控內稽制度」[23]

- 「內規盤查」清點作業：啟動本公司內規清冊之盤點作業，要求各內規管理單位檢視內部或外部法規是否有不一致情形，以避免作業風險或違法缺失。
- 落實「內部控制」制度：為確實管理內控程序，中信銀亦要求各單位配合進行自我查核，針對管理階層監督與控制文化、風險辨識、控制活動與職務分工、資訊與溝通、監督活動與導正措施等項目進行評估，包括是否訂定適當之內部控制政策及監督其有效性及適切性、是否有效辨識可能產生之重大風險、是否設立完善之控制架構及訂定各層級內控程序、是否有適

[21] http://db.lawbank.com.tw/FLAW/FLAWDAT08.aspx?lsid=FL007892&ldate=20130614 (access date: 2016/6/6)

[22] ba.org.tw/word/安控基準修正總說明_20130603.doc (access date: 2016/6/6)

[23] http://www.ctbcholding.com/care_05_6.html (access date: 2016/6/6)

當職務分工、建立有效溝通管道等。

- 建立「內部稽核」制度：為協助董事會及管理階層查核及評估內部控制制度運作有效性，遵循「金融控股公司及銀行業內部控制及稽核制度實施辦法」建立總稽核制度，並設置隸屬董事會內部稽核單位，秉持獨立客觀的立場執行稽核業務，適時提供改進建議，以合理確保內部控制制度，包含公司內企業社會責任實務守則建立、推動等，得以持續有效實施，進而促進公司永續經營。內部稽核單位對本公司每年至少辦理一次一般業務查核，每半年至少對本公司、子公司的財務、風險管理及法令遵循辦理一次專案業務查核，主要工作項目如下：
  (1) 建立風險導向稽核，依據金控及各子公司的風險訂定稽核計劃並辦理查核
  (2) 督導各單位落實自行查核制度執行。
  (3) 持續追蹤覆查內、外部檢查意見及缺失改善情形。
  (4) 定期向董事會及審計委員會報告稽核業務執行情形及座談。
  (5) 建立內部稽核、法令遵循與風險管理雙向溝通機制，就相關法遵與風管弱點進行討論。

中信銀持續推動內部控制制度三道防線文化，由第一道防線 (自行查核)、第二道防線 (法令遵循與風險管理) 與第三道防線 (內部稽核單位)，共同確保內部控制制度之設計及運作有效執行，強化對風險管理、法令遵循、內部控制文化之意識與遵循，俾確保客戶權益，減少對企業商譽之負面影響。

<u>附錄 A7：補充資料－後續相關事件或改變</u>

本附錄補充與本個案可能相關之後續發生的事件或改變，提供給學員參考：

1. 中信銀於 2014 正式設置企業資訊安全委員會與監控中心[24]：中信銀於 2014 年正式成立企業資訊安全委員會，由總經理及各事業處執行長等高階主管擔任委員，負責企業資安議題審議、重要決策裁示、資安預算的審查等。由上而下的執行方式有利於資安政策與事務的推動。公司並辦

[24] http://www.chinatrustgroup.com.tw/2014CSR.pdf (access date: 2016/4/12)

理個資保護及資安保護教育訓練以及建立資安事件監控與應變中心 SOC (Security Of Center)。在資安控管認證及改善機制方面，則設立品質監控改善機制、致力中信銀通過 BS 10012 PIMS (Personal Information Management System) 個人資訊管理認證、以及強化資料外洩防治網。

2. 中信銀前資訊長張汝恬轉戰數位電子銀行－王道銀行[25]：2015 年，台灣工銀董事長請來有台灣「信用卡教父」之稱的羅聯福，規畫王道商銀藍圖。他當年一手打造出中信銀的信用卡龍頭市場地位，當年跟隨他的子弟兵，包括張儉生、張汝恬及張智銓等，此次都隨他轉戰「王道銀行」。台灣工銀最高顧問羅聯福說，王道銀行將以數位電子銀行業務為主，別的銀行為轉型 Bank3.0「因為包袱多」，就像打「七傷拳」一樣，每每出拳、都會內傷，但王道銀行沒有包袱，每揮一拳，拳拳都到肉。

[25] http://udn.com/news/story/7239/1225428-駱錦明拚工銀轉型-不打七傷拳 (access date: 2016/4/23)

# 個案討論

## 壹、導讀

本個案是一個真實事件的管理層級之圖書館個案，藉由本個案教學讓學生可以學習個人資料 (personal information，下文簡稱個資) 保護以及資訊安全 (下文簡稱資安) 管理等相關議題。行動數位時代，個資保護已然成為顯學，資訊安全議題不再只是管控流程的作業層級議題，而是公司政策的議題。自 1997 年以來，中信銀進行 e 化及資安建置，然而在此次由 ptt 鄉民揭露的個資外洩事件中，卻凸顯了其資安管理的問題；而在整個危機處理過程中，看似完美堪為典範的危機處理背後，卻仍有不小的隱憂存在。究其根本原因是現行制度下的成本議題－個資外洩所必須付出的代價對金控公司而言其實微不足道、資安管理的代理問題、以及銀行對資訊部門的定位與針對資訊部門節省人力成本背後的隱憂。

## 貳、教學效益與目標

本個案預期達到的教學目標與效益如下：

一、 讓資訊相關科系學生理解資安問題其實是管理議題，因為「寫出安全的程式」與「寫程式邏輯」其實是不同的思維。

二、 讓學生領悟資安管理的本質其實是代理問題，資安管理存在著資訊不對稱的事後隱藏行動的道德風險之代理問題，學生可以據此站在資訊主管角度思考因應之道。

三、 透過檢討中信銀內控流程，讓學生理解如何建立公司內部資安管理制度。

四、 透過中信銀個資外洩事件中所涉及的各類成本的權衡取捨，讓學生有機會重新思考成本的意義。

五、 啓發學生重新思考資訊部門定位與人力成本本質，以協助學生思考資訊人如何在公司做領頭羊因應制度或環境快速變遷。

# 參、個案適用之課程

資訊安全是管理議題而非僅是技術議題，所以本個案屬於管理層級而非作業層級個案。本個案適用在管理學院或商學院涉及與網路時代、數位時代、或行動通訊時代對於資訊安全管理議題相關之課程，包含「資訊管理」、「資訊安全」、「資訊安全管理」。

# 肆、教學所需之理論基礎與背景資料

## 一、個人資料保護法

新版個資法於 2012 年 10 月 1 日正式實施，本節摘錄與本個案之分析相關的個資法法條，作為回答問題與討論第 3 題及第 4 題的背景資料。

(一)個人資料保護法第 28 條：「公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。但損害因天災、事變或其他不可抗力所致者，不在此限。被害人雖非財產上之損害，亦得請求賠償相當之金額；其名譽被侵害者，並得請求為回復名譽之適當處分。依前二項情形，如被害人不易或不能證明其實際損害額時，得請求法院依侵害情節，以每人每一事件新臺幣五百元以上二萬元以下計算。對於同一原因事實造成多數當事人權利受侵害之事件，經當事人請求損害賠償者，其合計最高總額以新臺幣二億元為限。但因該原因事實所涉利益超過新臺幣二億元者，以該所涉利益為限。(下略)」

(二)個人資料保護法第 29 條：「非公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。但能證明其無故意或過失者，不在此限。依前項規定請求賠償者，適用前條第二項至第六項規定。」

(三)個人資料保護法第 41 條：「意圖為自己或第三人不法之利益或損害他人之利益，而違反第六條第一項、第十五條、第十六條、第十九條、第二十條第一項規定，或中央目的事業主管機關依第二十一條限制國際傳輸之命令或處分，足生損害於他人者，處五年以下有期徒刑，得併科新臺幣一百萬元以下罰金。」

## 二、資訊安全準則

1975 年，Saltzer 與 Schroeder 發表了建置安全的運算系統，所應遵行的準則 (Saltzer & Schroeder, 1975) 為資訊安全的經典著作，時至今日，這些標準在資訊安全領域仍是參考準則，莊友欣譯 (2004) 將其整理成電腦安全的七項設計準則，柯瓊鳳、陳專塗 (2015) 也整理相關原則，本文整理三者並簡述如下文，作為回答問題與討論第 1 題、第 2 題、及第 5 題的背景資料。

(一)最少權限 (least privilege)：每個使用者與行程都應該有必須的最小權限。給予最少的權限可以將惡意攻擊者的錯誤所造成的損失限制到最小。存取權限的提供應該是基於明確的需求，而不是根據預設值提供給使用者。此觀念是任務在分派給某人工作時，儘量給予其所需最低限度的資訊即可，以免增加資訊洩漏的可能性。

(二)簡約機制 (economy of mechanism)：系統的設計應該是小巧而簡單，以能夠被確認和正確地實作。

(三)完整檢測 (complete mediation)：每個存取動作都必須先檢驗是否有適當授權。

(四)開放性設計 (open design)：安全防護不應該倚靠攻擊者的無知。這項準則可以杜絕系統裡的後門，不讓知道有後門的使用者得以進入。

(五)權限區隔 (separation of privilege)：盡可能讓對於系統資源的存取必須滿足超過一個人以上。在組織人力許可下，應避免一項資訊系統管理業務僅授權給一位員工，以避免該員工掌握所有組織核心安全而為所欲為。

(六)最少共用機制 (least common mechanism)：使用者應被系統相互隔離。這可以避免使用者隱匿監視或互助合作，想要破壞系統的安全機制。

(七)心理上的接受程度 (psychological acceptability)：安全控管程序必須容易使用，才能讓他們發揮效用，不會有所遺漏。也就是能被所有員工了解並接受，即使再如何周岩的安全空管措施，若不能為員工所接受，則推行勢必受強大阻力，最後不免要重新修正或放棄。

(八)符合成本效益原則。

(九)可稽核性：每項安全措施在設計時，應考慮是否有稽核軌跡，以便利事後的稽核，而且這些稽核軌跡的設計，應併入安全措施的成本一併考慮。

(十)責任的分派：每項安全措施至少應有一專人負責，且將安全防衛的責任列入工作績效。

## 三、資訊安全管理之 3C 平衡取捨

此部分作為問題與討論第 2 題及第 3 題的背景資料。行動網路開放空間，資訊安全的管控已經是公司治理 (corporate governance) 不可或缺的一環，在資訊安全管理議題上，對於資訊部門主管而言，他的資源有限人力也有限，成本的分配必須在如圖 2-1 所示的 3C 權衡取捨，其中的控制即是資訊安全的考量。安全措施的執行必須在成本、控制、與便利性之間取得平衡，即所謂的 3C 原則，圖 2-1 可是為一個等邊三角形，三者對於組織隻定與安全有同等的重要性。當安全措施愈嚴密時，對員工及資料的使用等各方面所加的限制也愈多，因此可能房案組織正常的工作流程，造成員工的反彈或影響生產力，因此如何在便利性所影響的生產力與安全控管之間取得平衡，對資訊安全管理或制度的成功很重要。

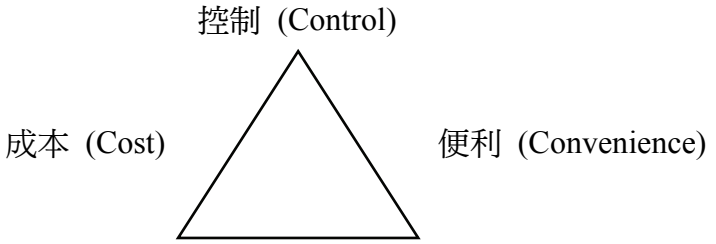


圖 2-1 建立資訊安全措施之 3C 原則

資料來源：柯瓊鳳、陳專塗 (2015)

## 四、委託－代理理論 (Principal-Agent Theory)

本理論將應用於分析第 2 題討論資安管理的代理問題。

委託－代理理論 (Principal-Agent Theory) 簡稱為代理理論 (Agency Theory)，源於 1960 年代～1970 年代初期，經濟學家如 Arrow 等討論風險分擔的議題，爾後衍申成代理問題的探討，並且廣泛應用於社會科學各領域 (Eisenhardt, 1989)。Jensen & Meckling (1976) 針對管理學的財金領域，以代理理論觀點來思考廠商的所有權結構，並從擁有者 (owner) 角度而非管理者角度提出代理成本觀念。兩位學者將代理成本區分為主理人須付出的監督成本 (monitoring expenditures)、代理人的屢約成本 (bonding expenditures)、和剩餘損失 (residual loss)。其中，監督成本是指委託人為了監督代理人的而耗費的支出；代理人為了取得委託人信任而發生的自我約束支出 (如定期向委

託人報告工作進度等)，稱為屢約成本；而委託人和代理人的利益不一致導致的其它損失，則為剩餘損失。

何謂代理問題？一個委託人想使一個代理人 (通常是擁有私人資訊的人) 按照前者的利益選擇行動，但是委託人不能直接觀測到代理人選擇了什麼行動，能觀測到的只是另一些參數，這些參數可能由代理人的行動與其他外生的隨機因素共同決定，因而充其量只是代理人行動的不完全資訊，委託人的問題是如何根據這些觀測到的資訊來獎懲代理人，以激勵其選擇對委託人最有利的行動 (張維迎，1999)。

代理問題的本質為資訊不對稱 (asymmetric information)，可以再區分為如圖 2-2 的幾個模型，其中本個案第 2 題要應用分析的為事後隱藏行動的道德風險 (Moral Hazard) 議題。道德風險是指簽約後，委託人因監督成本過高 (例如知識或時間不足) 而無法妥善監督代理人的行為，因此代理人有動機隱藏其行為資訊而做出不誠實或委託人不願意見到的行為。例如：老闆希望軟體工程師能在有限的時間內完成系統開發，但是老闆可能沒有足夠知識來判斷此工程師進行軟體開發的真正時間，也無法時時刻刻地去監督軟體工程師的作業活動 (imperfectly monitored)，因此軟體工程師有機會隱藏行動，例如他明明可以一天完成的工作，卻告訴老闆這個任務需要一週才能完成，然後真正執行此工作只有一天的時間，其他時間則是他自己的時間。

| | 隱藏行動<br>(hidden action) | 隱藏資訊<br>(hidden information) |
|---|---|---|
| 當事人簽約之前<br>(事前) | | **逆向選擇、<br>信號傳遞、資訊篩選** |
| 當事人簽約之後<br>(事後) | **隱藏行動的道德風險** | **隱藏資訊的道德風險** |

圖 2-2 委託－代理理論之分類

資料來源：張維迎 (1999)

## 五、典範移轉 (Paradigm Shift)

本理論將應用於分析第 5 題討論資訊部門定位與資安人力成本。下文前三段引述自朱元鴻、傅大為 (2001)。

典範 (Paradigm) 一詞源於 Kuhn (2012)，此書已經出版五十年了，第一版在 1962 年出版，是經典之作。按照 Kuhn 的說法，一門科學在尚未形成之前，往往學派林立，眾說紛紜，沒有大家共同接受的基本看法，這是前科學 (pre-science) 期的現象，一門科學若永遠停留在這個階段，則沒有機會發展成成熟科學 (mature science)。有些學科會慢慢脫離這個階段，研究者會逐漸形成一些共識，他們會發展出一套大家共同接受的基本觀念和研究方法。在某一特定時期，參與某一學科研究工作的科學社群 (scientific community) 所共同接受的基本觀點和研究方法，稱之為「典範」。典範一詞後來被大家廣為運用，可以泛指在一個社群 (包含社會、國家、族群等群體)所共同接受的基本觀點、方法、與行為準則 (朱元鴻、傅大為，2001)。

在某一個典範侷限之下所發展出來的學科叫做「常態科學 (normal science)」。常態科學家一方面遵循典範中的觀點與方法，另一方面也由於他們的專精研究，使得典範中原本有些模糊的觀點與方法發展得更為明確，常態科學是解謎或解決難題活動 (puzzles)。在常態科學期間，科學家的主要活動是遵照典範的規定來解決難題。有些難題是經過許多科學家的長久努力而仍然無法解決的，這種難題或謎團叫做該典範中的「異例 (anomaly)」。在常態科學期間，科學社群不會因異例的出現而放棄大家所接受的典範，他們認為問題不在於典範，而在於科學家的能力不足或努力不夠 (朱元鴻、傅大為，2001)。

異例的出現通常不會對典範構成威脅，只有在某些特別狀況下，異例才會造成危機，特別是這個異例很明顯會令人對典範的基本觀點或假設前提產生疑問時。如果異例愈來愈多，而且經過長期努裡也沒有解決的跡象，則也可能使科學社群的成員對典範的信心產生動搖。他們會開始對典範做或大或小的修改，甚至提出與當時的典範完全不同的觀點，此時不同意見的科學家之間會對許多基本觀點爭論，當心的觀點逐漸形成一個新的典範，而與原有的典範針鋒相對時，那麼科學就由危機時期開始步入革命時期。等到新典範完全取代了就典範，科學革命就完成了，也就形成新的常態科學，這就是典範移轉 (paradigm shift) (朱元鴻、傅大為，2001)。

典範移轉有不少類似的概念，例如根本性改變 (radical change)、不連續創新 (discontinue innovation)、突破性創新 (breakthrough innovation)、假說檢定統計 H1 推翻 H0 的本質……等。齊若蘭譯 (2016) 在 Kuhn 典範移轉的概念上提出第二曲線 (the second curve）的觀念，他認為第二曲線傳達的訊息

是，如果想在人生各領域跨步向前，有時候必須啟動激烈變革，開創不同的新路線，從全新的角度看待熟悉的老問題，位老問題開新路，他認為主導第一曲線的人必須對未來有截然不同的思考，或必須讓別人帶頭攀登新曲線，但這不是容易的事情。第二曲線是通往未來的轉折點，當世界改變時，我們也必須改變。

圖 2-3 以第二曲線詮釋典範移轉的觀念，幾本上不管第一曲線或第二曲線的任一個 S 曲線，可以分成三個階段，一是二次微分 f ”>0 代表前科學期，二是反曲點 f ”=0 可以代表典範已經形成，三則是 f ”<0，表示典範穩定發展期。電腦科學或資訊工程發展以來，資訊科技創新常常是觸動典範移轉的驅動力或源頭。

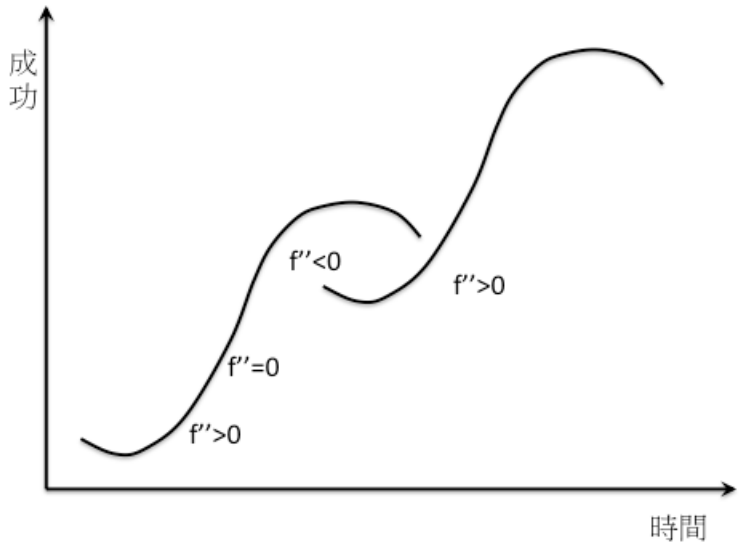


**圖 2-3 第二曲線－典範移轉**

資料來源：本研究整理

## 六、風險控制或沖抵之策略思維

本模式將應用於分析第 4 題針對資安管理議題，重新思考成本的意義。

企業主管理公司，在商言商之際，莫不將「控制並降低成本支出」視為與「獲得利潤」同等重要，若能降低經營成本同時又能增家利潤，一來一往間就可使企業獲利空間極大化。本問題與討論重點在於遵守法令維持個資安

全之成本花費會不會過鉅？企業主會不會心存僥倖，有意無意忽視成本之投入，賭一賭這不一定會發生的「資安風險」受罰及損害賠償的費用？(游士瑩，2007)

「維持個資安全所耗費的成本」可能是建置個資控管系統之花費或是聘請外部顧問/會計師/律師設計資安控管流程，所耗費之金錢/時間成本，一般來說，均比造成個資外洩事件受主管機關裁罰金額更鉅。根據上文個人資料保護法第 28 條及 29 條規定，企業對於客戶所負擔之民事損害賠償責任，每人每一事件新臺幣五百元以上二萬元以下；若為集體訴訟請求則可能求償金額高達臺幣二億元。

如圖 2-4 所示，依 Hübner et al. (2003) 風險控制或沖抵策略思維，以風險發生頻率為 X 軸，風險發生嚴重性為 Y 軸，風險產生及其處理有四種態樣：

(1) 發生頻率高，發生嚴重性高，就必須將此風險規避 (Avoid)；
(2) 發生頻率高，發生嚴重性低，就必須將此風險降低 (Reduce)；
(3) 發生頻率低，發生嚴重性高，就必須將此風險移轉/減輕 (Transfer/Mitigate)，例如：保險；
(4) 發生頻率低，發生嚴重性低，就將此風險承擔 (Assume)，這就是成本。

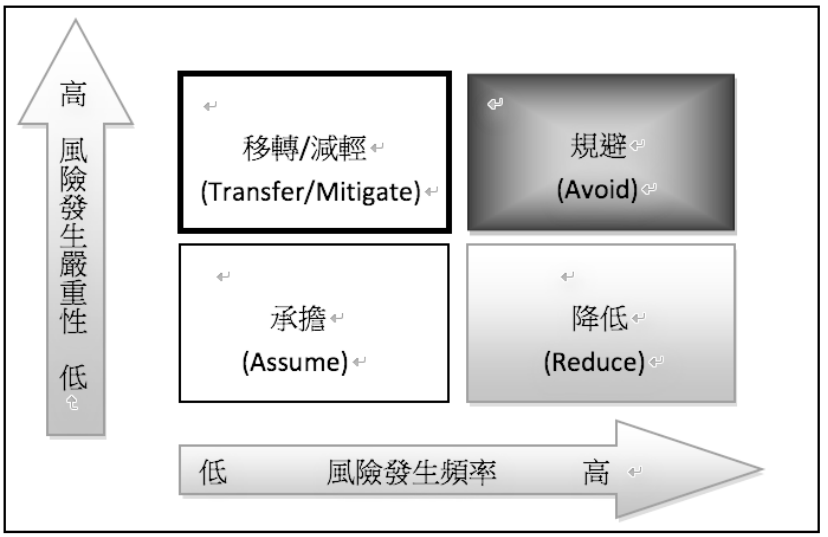


圖 2-4 風險控制或沖抵之策略思維

資料來源：Hübner et al. (2003)

綜上所述，公司高層該如何權衡取捨承擔成本？依 Hübner et al. (2003) 風險控制/沖抵之策略理論，風險之控管應集中於發生頻率高，發生嚴重性高之態樣，辨識出此風險並將此風險杜絕避免，風險發生頻率高，但發生之嚴重性較低之事件，則應努力降低發生頻率。至於風險不常發生，惟一旦發生其嚴重性很高，則應透過保險等機制，事前將此風險之影響轉嫁分散。至若風險發生頻率低，若果發生風險事件又不致於造成太嚴重之後果，則可將此風險影響列為企業必須支出之或然成本之一。如此一來，公司高層及企業主之經營管理才不會陷於為事撤肘之窘境。

# 伍、問題討論參考答案

個案本文最後提出的五個討論問題，是針對資訊安全管理議題環環相扣的分析與討論，問題 1 主要是讓學員領悟資訊安全是管理議題；問題 2 則論及資安管理的本質其實是代理問題；問題 3 則針對公司內部資安管理制度，檢討內控流程，並提出改善建議；問題 4 則讓學員針對資安管理議題，重新思考成本的意義；代理問題其實涉及一個公司資訊部門定位與資安人力成本議題，因此在問題 5 中進行討論與分析。本節下文提供這五個問題的參考答案，參考答案將個案本文的故事與本章第四節的理論連結，設法到將資料放到理論分析與討論，授課教師可以斟酌運用。

## 一、試分析中信銀在此次事件中，犯了哪些錯誤？你覺得個資外洩的問題，誰該負責？

整體而言，根據個案本文第一與第四節的事件發生過程以及附錄 A3 金管會裁罰文，可以發現中信銀在這次事件中，主要的錯誤為「貴行於本 (102) 年 4 月 13 日將貴行之網站索引檔案上傳予網路搜尋引擎業者，惟貴行對網站索引檔案產出程式之設計未臻嚴謹，對相關檔案驗證方法及程序亦有欠周延，且未對貴行內部目錄網頁之讀取權限作嚴謹控管，導致一般網路使用者得進入瀏覽並取得貴行內部目錄網頁所留存之客戶資料，受影響之客戶數達 33,320 戶，資料筆數計 57,297 筆。貴行亦未能有效發現外部人士瀏覽貴行內部目錄網頁，核有未落實執行內部控制制度之缺失。」

從附錄 A3 金管會的裁罰文中可知，4 月 13 日新網頁上線時即發生錯誤了，到 5 月 13 日被鄉民揭露前整整一個月的時間，公司人員不管資訊單位或業務單位竟無一人發現問題。此外，媒體報導、中信銀自己的說明、及金管會裁罰文三者對於事件經過的描述其實並不一致，我們可從個案本文中圖 1-2~圖 1-7 說明這些不一致之處，並進一步分析這些錯誤是如何發生的。

(一)從圖 1-3 可知此為下拉選單所呈現的資料，也就是不該出現的個人資料卻出現在下拉選單中。圖 1-6 顯示網頁原始碼 html 文件，內容是信用卡等個人資料－而且是很多人的個人資料，並不似如同第 5 頁中，金管會銀行局副局長被中信銀通報的「使用者自行註記在備註欄中的資料」。記事本的備註欄沒有這些功能，而且介面看起來跟處理事務的應用會很不一樣。科技部落客幾個截圖畫面的內容，跟備註欄也無關。

(二)金管會裁罰文內容其實與圖 1-2~圖 1-7 截圖畫面所揭露的資訊是一致的，與個案第 5 頁中 5 月 14 日中信銀的新聞稿強調的反而不一致「中信銀強調，均為客戶自行設定透過網銀繳交費用項目及代號，客戶姓名、帳號等資料並未外洩。」

(三)個案本文媒體報導，一位技術專家推測中信銀系統上線前的測試環節不夠嚴謹，提醒同學圖 1-3 截圖畫面的網址 http://consumer.chinatrust.com.tw，並不是測試環境而是正式 eTrust 登錄後的網頁。

我們進一步從網頁開發與上線的技術觀點來分析金管會裁罰文，中信銀主要的問題是「程式設計得不夠安全，而且沒有驗證妥當或沒有完整檢測」或者沒有專人來做這兩件事情。通常是測試工程師來做這件事情，測試時不能只靠人力做測試，因為通常會測試不完全且有盲點，所以還會寫測試程式來執行任務。在人力很少的公司，測試程式由資深工程師來寫可以節省時間。

值得注意的是，寫程式邏輯與寫出安全的程式屬於不同的特性，其實是不同的思維，也需要不同人力來進行，表 2-1 說明此兩者主要差別。表 2-1「寫程式邏輯 vs. 寫出安全的程式」並不是要討論程式設計者該怎麼做，而是用以凸顯資訊安全是管理議題而不僅是技術議題，授課老師可以參考個案討論的第四節中的「資訊安全準則」，例如其中的 (9) 可稽核性與 (10) 責任的分派，來進一步補充說明兩者的差異。

此外，網頁程式是在開放的環境下上線 (launch)，因此當網頁程式上線後，有經驗的資深工程師會習慣在網頁上到處點一點，安裝資安軟體是不夠

的，因為每一個軟體都有可能會被入侵。必須每天定期執行檢查出不一致的地方，或找出不合理的情況，常常必須事前防範，例如：假設資料庫若被入侵時，如何警覺到且及時找出問題所在。

表 2-1 寫程式邏輯 vs. 寫出安全的程式

| 寫程式邏輯 | 寫出安全的程式 |
|---|---|
| ● 求效率 | ● 程式寫得安全與否與效率無關 |
| ● 思考「這件事怎麼做」 | ● 此為管理議題，與「這件事怎麼做」無關，至少必須兩人簽核 (double check) |
| ● 較偏向顯性 (explicit) 知識，可以經過上課過程來學習或訓練 | ● 較偏向隱性 (tacit) 知識，無法完全經由上課學習，常常要犯過錯才能謹記在心<br>● 通常只要網頁跑得動，許多資安議題很容易被疏忽 |
| ● 不需要程式複審 (code review) | ● 需要程式複審 (code review)<br>● 有些安全議題是測試不出來的，必須經由有經驗的資深工程師看過<br>● 當公司人力不足時，code review 這些事情容易被省略 |
| ● 寫程式議題可以在系統設計階段才考慮 | ● 資安議題在系統分析初期就該納入考慮 |
| ● 事後可以測試找出問題 | ● 常常必須事先防範於未然 |

資料來源：本研究整理

資安問題是管理議題，中信銀此個資外洩事件，其所犯的錯誤，很明顯是沒有經驗的菜鳥工程師的疏忽，而且 4 月 13 日上線後整整一個月，公司內部都沒有人發現，因此若要咎責，應該由管理階層開始自我檢討起。上課老師可以進一步詢問學生「你覺得個資外洩的問題，誰該負責？」提名如 CEO、資訊主管、程式設計師、測試工程師、資安人員 (如果有的話)……等，然後投票。最透過這個投票，讓學生從了解表 2-1 的過程中，領悟並理解資安問題其實是管理議題。請注意，事發當時中信銀並無資訊長，從附錄 A1 推論當時公司內部職位最高的資訊主管，可能是資訊處長，而且是代理處長，並非一級主管，可能是三級主管。

## 二、如果你是中信銀資訊部門最高主管，對於個資保護的資訊安全做到的程度，在成本、安全控制、及使用者便利性三者中，你會如何權衡取捨呢？

根據個案本文第一節與第四節、以及附錄 A3 金管會裁罰文，中信銀在這次事件中，主要的錯誤為安全控制問題：「一個月前 (4 月 13 日) 將網站索引檔案上傳予網路搜尋引擎業者、對網站索引檔案產出程式之設計未臻嚴謹、對相關檔案驗證方法及程序亦有欠周延、且未對公司內部目錄網頁之讀取權限作嚴謹控管，導致一般網路使用者得進入瀏覽並取得貴行內部目錄網頁所留存之客戶資料」。而從附錄 A1 與附錄 A7 得知，中信銀於事後才正式設置企業資訊安全委員會與監控中心，根據上文理論基礎的圖 2-1 建立資訊安全措施之 3C 原則，可以推論在 3C 原則上，事件發生前的中信銀是取高便利性低成本而捨安全控制嚴格程度。授課老師可以據此詢問學員：請判斷中信銀在事發前對 3C 是如何取捨呢？

上文第 1 題分析重點是：資安是管理議題，雖然此次事件由工程師引起，但維護資安是全體員工的任務，而不是僅是工程師的責任。就資安層面，其實並沒有取捨問題－沒有要為求開發效率而放棄安全性這件事。安全性應該就是隨時記在心上，隨時去注意的。對工程師而言，資安不是多花時間，或多花工夫，就是隨時注意知道就可以防範。

首先，造成資安問題的是工程師，能夠釐清問題的也是工程師，也就是說，能夠真正確定問題的是什麼也還是工程師，工程師在釐清問題時有動機造假或包庇，朝向大事化小小事化無，所以個案本文中中信銀在第一時間強調沒有資料外洩的原因可能在此。人才的培育是個問題，即便是 coding 能力很強的工程師，對資訊安全都未必能夠了解得很全面。資安對於從開發出身的工程師而言，是另外一個議題，因為學習過程中只知道資訊安全的概念，如果沒有真正去演練過，並不知道她真正運作的方式。如何竊取別人網站的資料，跟如何防範這件事情，都是真正需要領悟後才能明白的。沒有當過小偷真的不知道該如何偷東西。從另一角度來說，不是很會 coding 的人也可以做資安。資訊安全控制可以用防毒軟體的概念來看，防毒軟體都是發生之後才知道如何去破解他或是去防範他。

因為中信銀是服務業，不會犧牲太多使用者特別是客戶的便利性，在此前提下，若要提高安全控制嚴格程度，勢必會增加資安成本，然而資安成本最關鍵的問題不是高額的建置成本，而是因代理問題所必須思考的代理成

本。公司內的資安議題可以分成兩個層次來思考：

(一)公司資安能力的極限：整個團隊要有一個人是最懂得資訊安全的人，在這個團隊所做出來的系統安全程度，最高就是這個人所知道的程度。但是資安問題日新月異層出不窮，這個團隊中最懂資安的人不知道的事情，他就不知道該該如何才能防範。所以團隊的安全性是有極限的是因為知識的極限，此部分與 3C 原則較沒有直接關係，實務上的做法是：通常公司會請專門的資安管理公司來做、有些公司自己做資安也找資安公司測、有些是完全自己做。以中信銀此個案而言，從 2012 年 6 月開始公司沒有 CIO，且公司內部的資訊最高主管可能是三級主管來判斷，公司資安能力的極限相較於重視資訊部門的公司是不高的。

(二)資安問題判斷所形成的代理問題 (詳見理論基礎第四節第 4 點說明)：

資安工作不管是單人執行還是多人執行，在資安知識極限內能夠做到的前提之內能不能全部做到全部的資安控制，此第二層次的問題才與 3C 原則直接相關。行動網路時代，普遍存在開放系統，而可以開放的就會有隱藏的風險，對於資訊系統開發者而言，面對資安議題，他無法保證完全沒有問題，所以他可以接受委外者請第三方的資安公司給付會請他去檢測，其檢測到的問題他都會把它處理掉。

技術上的資安工作可以透過資安程式進行，資安測試程式分黑箱與白箱，黑箱測試是從外部去檢測網站有沒有漏洞，白箱測試會掃描程式碼有沒有漏洞，可是也無法百分之百找出資安問題，甚至有時候資安測試城市提出來也不見得是真正的問題，而是它警告你那邊可能有問題，所以實際上還是要人為判斷是不是真的有問題。不安全語法的要人為檢測，人為判斷還是必要的，這就形成代理問題。

金管會裁罰文揭露的中信銀所犯的錯誤，其實就是典型的道德風險型態的代理問題。根據上文理論基礎第四節資訊安全準則中的「(10)責任的分派」，資安工作需由專人負責，假設資訊工程師已經知道要怎麼做才可以到達某個程度的安全性，但是他不見得能夠時時都能保持到這樣的安全程度。在開發工作上，程式是分工合作完成的，雖然有資安規範如上文理論基礎第四節資訊安全準則中的「(9)可稽核性」，但是工程師不一定會照規範做，必須要有額外的人力跟時間去做重複的檢查，通常此檢查會被忽略，因為這其中有很多監督成本 (主觀交易成本的其中一類)。

簡而言之，A 委託 B 來做資安工作，B 也說 ok 甚至簽約，可是事後 B 是不是真的把資安工作做好，A 可能並沒有能力去判斷，或者 A 要判斷 B 有沒有做好資安的話，A 需要花更多的時間或資源來監督 B 確認他把資安做好，但是 A 的資安知識有限，未必能找出 B 沒做到的資安工作，B 於是有動機不認真執行資安工作。如果 A 委託其他專業的資安公司做資訊安全工作，通常檢測一次就收費一次，而收費的標準是看程式碼行數，這對一個經常變動的系統來說，如果每變動一次都要檢查一次，每次檢測都是一個成本，而且系統會越來越大，委外檢測成本很高，同樣也有上述的代理問題，只是從公司內變成公司間的代理問題而已。如果以工程師的角度來看當然希望請人來做檢測最好，但是花錢的事情不是由工程師來決定的，而是管理者決定。

如何解決道德風險型態的代理問題呢？理論上是通過改變經理人激勵模型來改變員工的行為，實務上的做法可以考慮薪資結構從傳統的月薪制，改成類似職業運動員的給薪制度，如此吸引優秀資訊人員給予誘因 (incentives) 全力付出所長，惟這自然會提供高公司成本，問題則必須參考第 4 題的討論議題了。

## 三、你若是中信銀資訊部門最高主管，針對此次個資外洩事件，你覺得公司內部資訊安全管理制度如何能夠改善呢？是否需增加人手進行分工呢？

從內部資訊安全管理制度的觀點，我們再重新檢視個案本文圖 1-1～圖 1-7 以及附錄 A3、A5、與 A6。首先，授課老師可以問學生：從企業流程角度，檢視中信銀當時究竟是發生了什麼致命的問題，所以造成此次個資外洩事件呢？

(一) 程式沒有寫「檢查帳戶權限」：附錄 A3 金管會裁罰文中提及的索引檔誤置問題，在圖 1-3 的下拉選單終明顯呈現了。一般索引檔是為了方便使用者查詢或管理需要，而根據資料庫不同的欄位內容，建立不同的索引檔，以降低搜尋時間或增加查詢效率 (類似 Excel 中以不同欄位排序的概念)。如果程式有寫「檢查帳戶權限」，且假設使用者 S 在中信銀內留下兩支中華電信電話的資料，則 S 查詢時只能看到他自己的這兩筆資料；但是從圖 1-3 中顯示，S 看到了所有人的中華電信電話資料。這顯示中信銀內控的問題－程式沒寫帳戶權限檢查、寫程式的人自己沒發現

這個錯誤、公司內控沒有他人檢查的防範措施 (或馬虎行事)。

(二) 網頁上傳後，沒有進行上文第四節論及的資訊安全準則中的「完整檢測 (complete mediation)」－每個存取動作都必須先檢驗是否有適當授權。這個有問題的程式，如果根據問題 2 的參考答案，有完整的檢測－包括程式檢測與人為檢測，則這個程式的 bug 應該會被找出來，修改後才上架，但是顯然中信銀疏忽了檢測工作了。

(三) 沒有做到上文第四節論及的資訊安全準則中的權限區隔 (separation of privilege)－在組織人力許可下，應避免一項資訊系統管理業務僅授權給一位員工，以避免該員工掌握所有組織核心安全而為所欲為。如果中信銀內部的撰寫程式的人與將程式上架的人是不同的兩個人，則能增加安全檢測，這次的個資外洩事件也能避免。可是程式上架速度也會因此變慢，也就是上文圖 2-1 的 3C 取捨議題。

(四) 公開資料與個資沒有分開放置：個資如銀行內部的客戶資料、學校內的學生成績、圖書館的借閱資料等，應該放在安全管控區內，不可放在開放的網路空間，讓 Google 每天例行搜尋開放空間資料的自動程式搜尋到並收錄回 Google，並在 Google 內已經被建立索引檔了，而且從 2013/4/13~2013/5/13 整整一個月的時間，沒有任何中信銀內部員工發現這個漏洞。

附錄 A6 是中信銀根據附錄 A5 銀行公會的安控法所致動的內控制度，顯示中信銀網站自己說明的三道內部控制制度防線執行不力，也有問題，才會造成個資外洩：

1. 自我查核防線：沒訂定系統開發與維運內控流程，或沒確實執行。
2. 法令遵循與風險管理防線：忽略網路銀行資訊安全與個資管理的風險重要性。
3. 內部稽核單位防線：未確實督導查核資訊部門是否確實訂定與執行內控流程。

如果從資訊相關人員思考，下文整理資訊主管、系統設計人員、繳費業務單位 (承辦人與主管)、公司內部稽核單位等角色，在內控流程上分別犯了那些疏失：

1. 系統人員：應做單元 (與整體) 測試、資安測試。
2. 繳費業務單位：應做驗收測試。
3. 資訊主管：設計並執行系統開發與維運內控流程，降低公司資訊管

理與個資外洩風險。

4. 公司內部稽核單位：應監督並查核資訊部門有訂定並確實執行各種資安內控流程。

圖 2-5 從流程角度來彙整示意這些一連串的錯誤，其中資料庫為非開放空間。圖 2-6 則是建議的改善流程，可以避免發生同樣的錯誤，惟又回到第 2 題的 3C 取捨議題，仍是管理者必須面對的。圖 2-6 也是示意圖，增加幾個物件，其中網頁上架人可以是業務單位的資管人，而中信銀機器人是類似 Google 自動搜尋程式的功能，每天自動去公開的網路空間特別是搜尋引擎如 Google 的網頁，定時檢查公司相關個資資料是否流落在外。此處對於資料庫的動作，特別標示安全的存取/比對，是強調要執行權限區隔 (separation of privilege)。

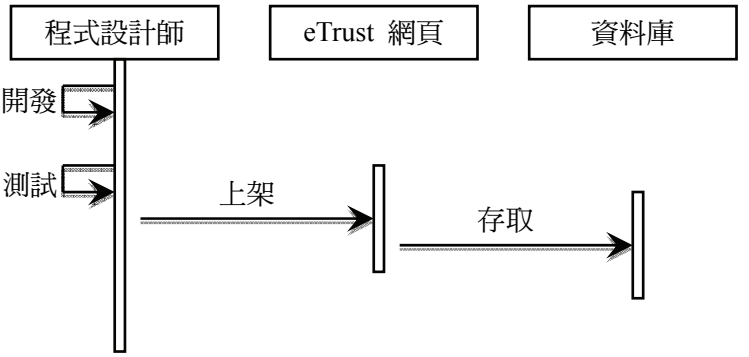


圖 2-5 個資洩漏事件的中信銀新網頁程式之可能上架流程示意圖

資料來源：本研究整理

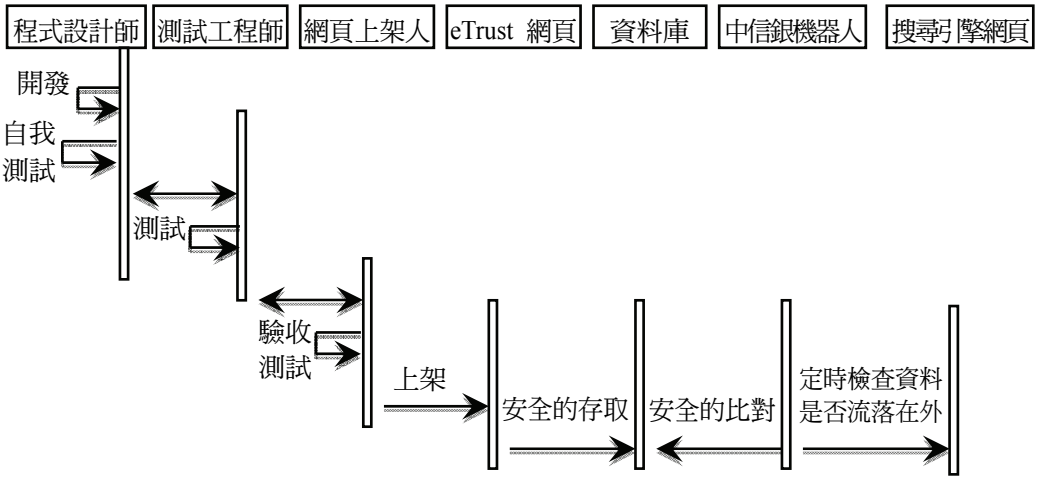


圖 2-6 本文建議改善的新網頁程式上架流程示意圖

資料來源：本研究整理

總之，進一步分析原因可能是為了成本或便利，卻犧牲了安全，反而造成客戶與商譽更重大的損失。這是組織面 (組織結構) 問題，公司必須訂定整體的系統開發與維運內控流程，但內控設計費時費力需要有高度的資源，一般都要有一級資訊單位來通盤設計規劃，但從個案本文第三節中得知，當時中信銀已無一級資訊單位，所以這種中央級的國土防災工作就沒人做，光靠分散在在各業務單位或一般行政單位的個資訊人員各自為政，當然可能出問題。

## 四、發生個資外洩事件這類事件，「成本」與「商譽」何者較為重要？

公司總想設法降低營運成本，以相對地增加獲利。換言之，假使建置個資保護系統所需之時間耗費、人力投入及金錢成本過鉅，而如果個資外洩之風險不確定，受裁罰之金額也相對於建制資保護系統成本花費少，企業主或高階經理人基於公司之獲利，會考慮乾脆遭受處罰比較划算。只是遭受處罰會涉及商譽受損，商譽乃無價，一旦受損將致公司基礎受到動搖，似乎再鉅的建置成本也要咬牙投進？但是一家公司若個資外洩事件發生率不高，是否要花費這麼多成本來預防這樣的風險？此時決策者陷入兩難之抉擇中。而在本個案中，中信銀付出的相關成本為：

(一) 維持個資安全所耗費的成本：是他投入在資安相關資源與時間的成本，若要真的落實整個資安體系，所費不貲，個案中並沒有明顯的資安成本說明，但在第三節提及 1997~2001 的 e 化工程耗資 10 億、2009 年中信銀拉高資安委員會層級。 (從附錄 A7 第 1 點得知，中信銀於 2014 才正式設置企業資訊安全委員會與監控中心）

(二) 因個資外洩所受主管機關之裁罰：從附錄 A3 得知，金管會裁罰新台幣 400 萬，元，而從附錄 A4「金管會銀行局 2012/1/1~2013/9/1 之裁罰統計數字」，可以了解，金管會裁罰 400 萬元對銀行其實已經是很重的處罰了，此為銀行界公開的資訊。然而，對於一個金控公司而言，400 萬元其實微不足道。

(三) 對客戶之民事損害賠償責任：根據上文第四節背景資料中的個資法第 28 條，在個案中曾有律師提及：「預估受害者一旦提出訴訟求償，3.3 萬名受害者，中信銀可能將面對 1,650 萬元到最高 2 億元的賠償金額。」不過，這是假設 3.3 萬名左右的客戶集體求長的前提下才會發生的金額，

實際上，台灣環境很少發生集體求償的訴訟，所以這部分中信銀付出的代價是 0。雖然個案本文第 6 頁最後提及，2013 年 5 月 24 日已經補償約一萬名受影響客戶，詳細數字不清楚，但是相較於假設集體求償訴訟賠償數字，則是微不足道。接下來先請問學員：為何此次個資外洩事件中無人提起訴訟呢？根據個案本文，此個案外洩事件因當時廣大興號(詳見附錄 A2）更大的事件而沒有造成新聞輿論發酵，加上 Google 相關暫存網頁在事發後中信銀也聯繫其刪除，事後得知此消息再於 Google 查詢自己個資，可能已經找不到相關資料佐證自己就是受害者，因此可能造成不少人不知道自己是受害者，即使知道自己是受害者，但困難點是舉證因果關係，因此沒有集體訴訟發生。此外，個案中也呈現中信銀自己在企業社會責任報告書揭露於當年 5 月 24 日之前，中信銀已經主動聯繫並補償他們認為受影響的一萬多名客戶 (金管會裁罰文卻是 33,320 客戶)，這一萬多名客戶是誰？個案本文沒有足夠的資料呈現。而台灣目前的環境對於個資保護的集體訴訟的氛圍尚未成型，加上訴訟結果也因舉證證明「損害與個資外洩有因果關係」困難無法預判絕對會獲勝，種種原因造成此事件無人提起訴訟。

(四) 關於維護商譽所必須付出的代價，建議老師可以以下列提問來討論：

1. 你認為「商譽」價值多少？辜且先不論述企業負責人或內部有企業行為人，意圖為自己或第三人不法之利益或損害他人之利益，而觸犯相關刑法 (上文第四節背景資料中的個人資料保護法第 41 條) 惡性重大這部分。另外要考量的企業成本是企業「商譽」。「商譽」是無價，難以金錢估算，嚴重者可以使一家企業因此衰敗倒閉。惟是否個資安全疑慮事件均足以造成企業「商譽嚴重受損」，與企業之危機處理能力以及民眾對於個資安全意識有關。
2. 你若是中信銀企業主會如何維護商譽呢？當然是全力維護，特別是上市公司，最怕因此影響股價，不過還是會斟酌事件嚴重程度來決定如何因應。而在此事件中，中信銀第一時間及時危機處理、快速發新聞稿、後續快速補償低調客戶。
3. 這次事件中中信銀對於「維護商譽」做了什麼努力呢？如 (b) 所述之外，個案本文提及 5 月 14 日新聞稿對外一直否認有網銀資訊外洩，由於恰巧遇到廣大興號事件，後續中信銀就以冷處理的方式來避開新聞熱議，順勢維護商譽。

4. 你認為中信銀覺得此個資外洩事件會影響他的商譽多久呢？由於台灣新聞媒體特性與台灣人健忘的特性，不少人很容易在一波波新聞事件中，很快忘記事不關己的重要議題，因此研判中信銀認為此事件只要股價不受影響或沒有太多波動，則對其商譽也不會影響太久。從後續中信銀冷處理的狀況，以及網路討論熱度被淹沒在廣大興事件熱議中 (詳見附錄 A2)，此事件對中信銀的商譽並沒有太大影響。

(五) 根據(一)~(四)所討論的上述四類成本，老師可以繼續以下列提問來總結：

1. 請問此次事件中，中信銀總共付出多少代價呢？根據個案本文與附錄內容，總計「被金管會裁罰 400 萬＋補償一萬多名客戶」，此代價相較於中信銀的獲利數字或建置資安體系所需付出動輒數千萬或數億的成本，其實微不足道，所以是屬於文第四節理論基礎第 6 點中的圖 2-4 中的(4)發生頻率低，發生嚴重性低，於是中信銀就將此風險承擔 (Assume)，這就是中信銀對於個資外洩所付出的微小成本。
2. 你認為中信銀覺得此個資外洩事件嚴重嗎？由上述分析可以推論中信銀可能認為並不嚴重，此事件並不是什麼大不了的事情。

## 五、根據本個案提供的資料，你認為中信銀高層對於資訊管理部門的定位是什麼呢？如果你是中信銀資訊部門最高主管，你會如何因應呢？

關於資訊安全議題，有三個保安威脅 (security threat) 來源：人為錯誤、惡意行為、與自然災害 (Kroenke & Boyle, 2016)，資安知識偏向屬於隱性知識，很難透過上課學習到，常常要犯過錯才能謹記在心，因此在公司內宜由資深工程師帶著新人 (老鳥帶菜鳥) 的師徒制方式進行，不必等新人犯錯後才知道教科書有提過卻無法真正領悟或沒教過的資安經驗。如果公司為了節省資訊相關部門的人力成本，造成沒有或很少資深工程師來帶領新人，則公司內的資安問題是堪慮的。

從事發當時，中信銀並沒有資訊長，從個案本文第三節得知，2012 年的 6 月中信銀就沒有資訊長了。從附錄 A1 推論當時公司內部職位最高的資訊主管，可能是資訊處長，而且是代理處長，並非一級主管，可能是三級主管。

我們無法推論此個資外洩事件是否與此有關，但是似乎可以推論可能是節省資訊部門人力成本有關。

建議授課老師可以進一步詢問學員「中信銀如何節省資訊部門的人力成本呢？背後有什麼隱憂呢？」我們推論：2012 年 6 月沒有資訊長後，最高資訊主管為資訊處長，因此資訊主管的薪資已然節省了，整個資訊部門的人力成本必然也節省了。如此一來，資深資訊人員可能會陸續離職，新招募一批新人來負責資訊部門相關事宜，而根據第 4 題的推論，資安相關知識是隱形 (tacit) 知識，無法經由上課學習到，資訊部門新人在公司缺少有經驗的資深工程師的提醒或 code review，於是犯下了其實完全可以避免的技術錯誤 (也不符合上文第四節背景資料中的資訊安全準則)，再加上資訊部門在公司是支援單位不受重視，可能對資安議題管理的疏忽而導致此次個資外洩事件。

資訊部門在台灣的本土銀行界通常是支援單位，從個案本文第三節中可知，除了支援一般性的行政事務，中信銀的資訊人員已經散落在各業務單位支援其業務。在科技根本性改變或典範移轉時 (典範移轉詳見理論基礎第 5 點之說明，授課老師可以在此處補充說明)，資訊部門在銀行才會受到重用，典型的中信銀自己的例子：1997~2001 導入 FNS 系統全面 e 化，就是因應從 1994 年開啟的 web 技術讓 Internet 於 1995 年全面商業化的趨勢。作為 CIO，必須讓企業主或主要股東明白資訊科技日新月異的快速進步，不能只將資訊部門視為支援單位，於科技典範移轉時才開始跟進，而是從策略思維或可能創造新市場的角度來看待資訊部門，現在金融界正面臨區塊鏈變革 (Blockchain revolution，金融界稱為 FinTech 或 Bank 3.0) 的衝擊 (Tapscott & Tapscott, 2016)，而附錄 A7 第 2 點提及中信銀前資訊長被王道銀行網羅，其實正是開啟企業主、CEO、CIO 重新思考資訊部門人力成本本質的契機。

## 陸、教學建議

開始上課時，建議教師可以先以暖身題詢問學生認為自己的個資是否早就已經外洩、面對自己個資外洩問題可曾採取過什麼行動、對於個資保護與資訊安全有沒有什麼想法……等問題，讓學生自由分享與發揮之後，再讓學生投票整體事件是否影響他們對於中信銀的評價。由於學生已經事先研讀過個案內容，在透過輕鬆的分享與投票之後，接下來可以直接進入分析階段，

討論內容可著重在重新思考成本的意義、寫程式邏輯與寫出安全的程式其實是不同的思維、危機處理、因應制度變遷或環境改變、以及重新思考資訊部門定位與人力成本本質等議題，過程中可讓學生角色扮演個案事件中的各種角色，思考如何決策，以因應下一波資訊科技導致的經濟體系運作典範移轉的未來。本個案教學建議規劃 90 分鐘，但可依據學生程度與討論狀況進行適度調整，建議之教學時間與主題分配如表 2-2 所示，教學板書建議如圖 2-7 所示：

表 2- 2 教學時間與主題分配

| 時間 | 主題 | 討論重點 | 說明 |
|---|---|---|---|
| 10 分鐘 | 主題一：經驗分享 | ● 你認為自己的個資是否早已外洩了？<br>● 面對自己的個資外洩可曾採取過什麼行動？<br>● 對於個資保護與資訊安全有什麼想法呢？<br>● 如果你是當時 eTrust 客戶，你會怎麼做呢？ | 暖身題，可以投票或冷點名 (cold call) 進行 |
| 20 分鐘 | 主題二：資訊安全是管理議題 | ● 中信銀在此次事件中，犯了哪些錯誤？<br>● 媒體報導、中信銀自己的說明、及金管會裁罰文三者對於事件經過的描述是否一致呢？<br>● 你覺得個資外洩的問題，誰該負責？ 提名如 CEO、資訊主管、程式設計師、測試工程師、資安人員 (如果有的話)……等，然後投票。 | 請參考問題討論參考答案 1 題討論。<br>附錄 A1<br>附錄 A2<br>附錄 A3 |
| 15 分鐘 | 主題三：資安管理的代理問題 | ● 請判斷中信銀在事發前對 3C 是如何取捨呢？<br>● 公司資安能力的極限<br>● 資安問題判斷所形成的代理問題<br>● 如何解決道德風險型態的代理問題呢？ | 請參考問題討論參考答案第 2 題討論 |
| 15 分鐘 | 主題四：公司內部資安管理制度－內控流程檢討 | ● 從企業流程角度，檢視中信銀當時究竟是發生了什麼致命的問題，所以造成此次個資外洩事件呢？<br>● 中信銀自我標榜的三道內控制度防線，如何執行不力呢？<br>● 內控流程可以如何改善，避免犯相同錯誤呢？ | 請參考問題討論參考答案第 3 題討論。<br>附錄 A5<br>附錄 A6 |
| 15 分鐘 | 主題五：針對資安管理議題，重新思考成本的意義 | ● 中信銀的「維持個資安全所耗費的成本」是什麼？<br>● 中信銀的「因個資外洩所受主管機關之裁罰」是什麼？<br>● 中信銀的「對客戶之民事損害賠償責任」是什麼？<br>● 你認為「商譽」價值多少？你若是中信銀企業主會如何維護商譽呢？<br>● 這次事件中中信銀對於「維護商譽」做了什麼努力呢？<br>● 你認為中信銀覺得此事件會影響他的商譽多久呢？ | 請參考問題討論參考答案第 4 題討論。<br>附錄 A2<br>附錄 A3。<br>附錄 A4。 |

| 時間 | 主題 | 討論重點 | 說明 |
|---|---|---|---|
| | | ● 綜合上述四類成本，請問此次事件中，中信銀總共付出多少代價呢？此代價相較於中信銀的獲利或建置資安體系，是什麼比例呢？<br>● 你認為中信銀覺得此個資外洩事件嚴重嗎？ | |
| 15 分鐘 | 主題六：資訊部門定位與資安人力成本 | ● 中信銀高層對於資管部門的定位是什麼呢？<br>● 中信銀如何節省資訊部門人力成本呢？有何隱憂呢？<br>● 如果你是 CIO，你會如何因應呢？<br>● 面對已經開始衝擊到金融業的 Blockchain revolution，你又會如何因應呢？ | 請參考問題討論參考答案第 5 題討論。<br>附錄 A1<br>附錄 A7 |

資料來源：本研究整理

**【版書一】10 分鐘**
你認為自己的個資是否早已外洩了？
面對自己的個資外洩可曾採取過什麼行動？
對於個資保護與資訊安全有什麼想法呢？
如果你是當時 eTrust 客戶，你會怎麼做呢？
……

**【版書二】20 分鐘**
中信銀在此次事件中，犯了哪些錯誤？
媒體報導、中信銀自己的說明、及金管會裁罰文三者對於事件經過的描述是否一致呢？
你覺得個資外洩的問題，誰該負責？
提名如 CEO、資訊主管、程式設計師、測試工程師、資安人員(如果有的話)……等，然後投票。
……

**【版書三】15 分鐘**
請判斷中信銀在事發前對 3C 是如何取捨呢？
公司資安能力的極限
資安問題判斷所形成的代理問題
如何解決道德風險型態的代理問題呢？
……

**【版書四】15 分鐘**
從企業流程角度，檢視中信銀當時究竟是發生了什麼致命的問題，所以造成此次事件呢？
內控流程可以如何改善，避免犯相同錯誤呢？
畫圖 2-5 與圖 2-6
……

**【版書五】15 分鐘**
中信銀的「維持個資安全所耗費的成本」？
中信銀的「因個資外洩所受主管機關之裁罰」？
中信銀的「對客戶之民事損害賠償責任」？
你認為「商譽」價值多少？
你若是中信銀企業主會如何維護商譽呢？
中信銀對於「維護商譽」做了什麼努力呢？
……

**【版書六】15 分鐘**
中信銀高層對於資管部門的定位是什麼呢？
如果你是 CIO，你會如何因應呢？
中信銀節省資訊部門的人力成本的隱憂？
Blockchain Revolution
……

圖 2-7 教學板書建議
資料來源：本研究整理

# 參考文獻

朱元鴻、傅大為，2001，孔恩：評論集，初版，台北：巨流圖書。(Chu, Y. H. and Fu, T. W., 2001, **T. S. Kuhn: Collection of Critical Essays**, 1st, Taipei, TW: Chu Liu Book Company.)

張維迎，1999，賽局理論與信息經濟學，初版，台北：茂昌圖書。(Zhang, W. Y., 1999, **Game Theory and Economics of Information**, 1st, Taipei, TW: Tuugo.)

莊友欣譯，Simson Garfinkel and Gene Spafford 著，2004，電子商務與網路安全，二版，台北：O'Reilly。(Garfinkel, S. and Spafford, G., 2002, **Web Security, Privacy & Commerce**, 2nd, Sebastopol, CA: O'Reilly Media.)

柯瓊鳳、陳專塗，2015，會計資訊系統：Cloud・IFRS・Big Data，八版，台北：新陸書局。(Ko, J. and Chen, C. T., 2015, **Accounting Information System: Cloud, IFRS, and Big Data**, 8th, Taipei, TW: Shin Lou Book Store.)

游士瑩，2007，我國銀行遵循法令制度研究，銘傳大學管理學院高階經理碩士論文。(Yu, S. Y., 2007, **Study of Compliance Function in Domestic Banks**, Master Thesis, Ming Chuan University.)

齊若蘭譯，Charles Handy著，2016，第二曲線：英國管理大師韓第的16個思索，預見社會與個人新出路，初版，台北：天下文化。(Handy, C., 2016, **The Second Curve: Thoughts on Reinventing Society**, 1st, London: Random House UK.)

Eisenhardt, K. M., 1989, "Agency Theory: An Assessment and Review," **Academy of Management Review**, Vol. 14, No. 1, 57-74.

Hübner, R., Laycock, M., and Peemöller, F., 2003, "Managing Operational Risk" in Jenkins, S. and Roberts, K. (eds.), **Advances in Operational Risk, Frimwide Issues for Financial Institutions**, Second Edition, London: Risk Books, 17-42.

Jensen, M. C. and Meckling, W. H., 1976, "Theory of the Firm: Managerial Behavior, Agency Costs, and Ownership Structure," **Journal of Financial Economics**, Vol. 3, No. 4, 305-360.

Kroenke, D. M. and Boyle, R. J., 2016, **Experiencing MIS**, 6th, New York: Pearson.

Kuhn, T. S., 2012, **The Structure of Scientific Revolutions: 50th Anniversary Edition**, 4th, Chicago: University of Chicago Press.

Saltzer, J. H. and Schroeder, M. D., 1975, "The Protection of Information in Computer Systems," **Proceedings of the IEEE**, Vol. 63, No. 9, 1278-1308.

Tapscott, D. and Tapscott, A., 2016, **Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World**, 1st, New York: Portfolio Penguin.

# 作者簡介

**游士瑩**

上海交通大學凱原法學院經濟法研究所博士候選人，現任渣打商業銀行法令遵循處助理副總裁 (AVP)，主要研究領域為金融業利害關係人授信及交易之金融監理。

E-mail: uniceu@gmail.com

**蘇雅惠**

國立台灣大學商學博士，現任國立中央大學資訊管理學系助理教授。研究興趣與專長為創業家精神、企業經營模式創新與設計、以及技術創新。

E-mail: suesu@mgt.ncu.edu.tw

**林裕得**

國立中央大學資訊管理碩士 (2008)，國立交通大學管理科學學士 (2002)，現任旭得數位有限公司創辦人兼執行長，專長為軟體工程與電子商務。

E-mail: hydelin@gmail.com

**連文雄**

國立中央大學資訊管理學系博士，現在是國立中央大學資訊管理學系助理教授，同時兼任國立中央大學圖書館資訊系統組組長。研究興趣與專長為數位圖書館、資訊系統管理。

E-mail: wslian@ncu.edu.tw