國立臺灣大學管理學院碩士在職專班商學組

碩士論文

Executive MBA Program in Business Administration

College of Management

National Taiwan University

Master Thesis

以詐騙集團攻擊國內購物平台業者個案，探討企業危機管理

──以 PayEasy 的防詐措施為例

Using a Case of Fraud Gangs Attacking Online Shopping Site to Investigate Corporate Crisis Management
- The Anti-fraud Procedures of PayEasy

林坤正

Kun Cheng Lin

指導教授：戚樹誠 博士

Advisor: Shu-Cheng Chi, Ph.D.

中華民國 98 年 7 月

July, 2009

國立臺灣大學碩士學位論文

口試委員會審定書

以詐騙集團攻擊國內購物平台業者個案，探討企業危機管理——以 PayEasy 的防詐措施為例

Using a Case of Fraud Gangs Attacking Online Shopping Site to Investigate Corporate Crisis Management
— The Anti-fraud Procedures of PayEasy

本論文係林坤正君（P95748012）在國立臺灣大學管理學院碩士在職專班商學組完成之碩士學位論文，於民國九十八年七月 14 日承下列考試委員審查通過及口試及格，特此證明

口試委員：

_____（指導教授）

_____

_____

_____

系主任、所長 _____

誌　謝

詐騙集團攻擊 PayEasy 事件發生至今近兩年，說實話當初遭逢這樣的危機事件，面對多方的龐大壓力與時間的急迫，我沒有太多的時間去思考對應策略，只能憑藉著直觀，單純的價值判斷，以及我們合作無間的團隊，成功抵禦歹徒的攻擊，保護我們的顧客免除詐騙威脅。

我決定以此案例作為畢業論文的題目，目的是藉由學術的檢核，嘗試釐清當初採行的危機處理模式能夠成功防禦詐騙集團攻擊的原因，並檢討在處理危機過程中，我們是否有改善的空間與更佳的應對策略。

在此誠摯的感謝指導教授戚樹誠博士，老師嚴謹的治學精神確實給了我不少的啟發，在老師細心指導與討論過程中，使我得以窺探賽局理論的精要以及實務運用，終得以完成論文，並感謝黃崇興教授、翁崇雄教授在口試時的指正，讓本論文更臻至完整。

最後我要感謝當年與我共同面對處理該危機事件的所有 PayEasy 同仁，由於我們的正義感與堅持不懈，保全了顧客的財產安全，證明我們是台灣最有良知與膽識的團隊。

林坤正　謹識

于台大管理學院

民國９８年７月

中文摘要

企業處於現今如此多元且遽變的社會環境中，隨時可能面臨危機的考驗及挑戰；所以，如何適時有效的面對與因應危機，實為企業當前重要課題之一。2007 年 12 月，PayEasy 第一次遭遇詐騙集團資料拼圖攻擊，IT 部門、客服部門、營運部門、公關部門和行銷部門大家並肩作戰。當時 PayEasy 與會員利用首頁保持對話，請客戶接獲詐騙電話立即回撥給客服，接著客服、行銷每天聯手更新歹徒最新話術，就掛在首頁連結上。跟同業不同的是，PayEasy 在 2007 年面對相同的資安威脅時，採衝突對峙的賽局策略「囚犯困境」中的「弱雞賽局」、「邊緣人理論」，將入侵的駭客視為競合的對象。為了使客戶提早警覺，因應詐騙集團的詐騙手法，PayEasy 正視危機的方式，短時間內成立應變小組，通知所有用戶迅速更改密碼，防止對岸 IP 登入等危機處理方式，保護客戶，避免受害人數增加。

關鍵詞： 危機管理、賽局、詐騙集團

THESIS ABSTRACT

Business Administration

COLLEGE OF MANAGEMENT

NAME： Kun Cheng Lin

MONTH/YEAR：JANUARY, 2005

ADVISER： Shu-Cheng Chi

TITLE：

The Research of Enterprise Crisis Management --While Fraud Gangs Attacking Online Shopping Site--A case study of the anti-fraud procedures of PayEasy

Every crisis caused by information security breaches presents challenges for enterprises in modern days. To cope with the increasing needs of enterprises and their clients, we have seen an emergence of complex information systems. But, in fact, the attempt of developing a perfect information system for managing varieties of threats is nearly impossible. The data merger attacks confronted by PayEasy exemplify a case that even a well-managed information system could unexpectedly being hacked. Moreover, this event pinpoints the importance of the elaboration of a crisis management procedure and a security management framework that is essential for preventing and confronting crises.

The account hacking crisis of PayEasy in December 2007 had put its clients into the risk of being fraud. In the face of a dilemma of assuring the safety of clients' properties or maintaining the credibility of the company, PayEasy adopted the strategy

of disclosing the crisis to the public. A multilevel analysis reveals two benefits of such crisis disclosure strategy. One is, honestly informing the customers who undergo the crisis regains their trust and wins back PayEasy's reputation. Second, based on the Chicken's Game theory, the best strategy to prevent continuing threat from both hackers and fraud gangs is to confront them and directly fight against them since this kind of direct confrontations achieves the best payoff in comparison with evasion (swerve).

Lastly, since there exists no information system that is perfectly designed to secure the attack. All related enterprises should work together and share the responsibility in fighting against the online gangsters. In such cases, a win-win situation can be created between customers and sellers. That is, the customersl have strong faith in the online shopping companies and the companies increase their market share in e-commerce business.

Keywords: Crisis management, game theory, fraud gangs

目　錄

圖目錄

表目錄

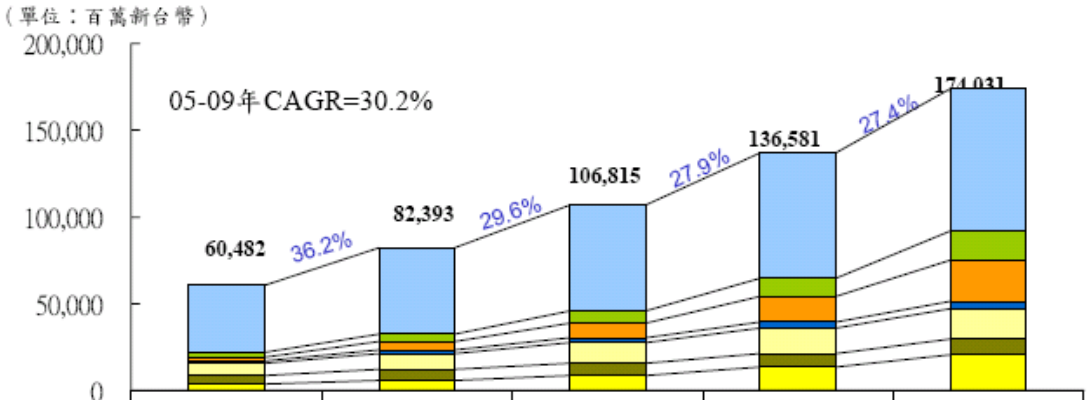
第一章 緒論

第一節、研究動機與目的

隨著全球資訊網服務(WWW)以及寬頻網路的普及，使用網路的人口與日俱增。根據資策會於 2008 年第三季對台灣上網人口的調查結果發現，截至 2008 年 9 月底止，我國有線寬頻網路用戶數達 474 萬，較去年同期增加 16 萬戶，較上一季有線寬頻用戶共增加 4 萬戶，小幅成長 1%。 龐大的上網人口也造就潛藏的網路商機。

近年來，隨著購物業者加入，販售產品種類增加，服務品質提升以及實體通路商建立網路虛擬通路，購物族群也隨之增加。2008 年台灣 B2C (Business to consumer) 的市場規模也將達到 1,365 億新台幣。於 2009 年，更可望突破 3,000 億新台幣。線上交易在台灣最近 5 年的使用人數也持續穩定成長，「轉帳或信用卡刷卡繳交帳單」使用人數，在 2003 年到 2007 年的複合成長率達 30.9%。顯示電子商務將成為未來民眾重要的消費平台之一（見圖 1.1）。

但儘管線上購物的使用人數已達 262 萬人，但如果與整體上網人口相較，可以發現線上購物的普及率仍有成長空間。據資策會 2008 年對線上購物使用者的調查中，發現網友在抉擇網路購物平台時，取貨便利性(63.9%)，資訊安全(53.9%)以及習慣使用(53.6%)是主要考量因素。而 57%的網友認為購物平台的網路安全性有待加強。資訊安全在購物交易的重要性也隨之彰顯。

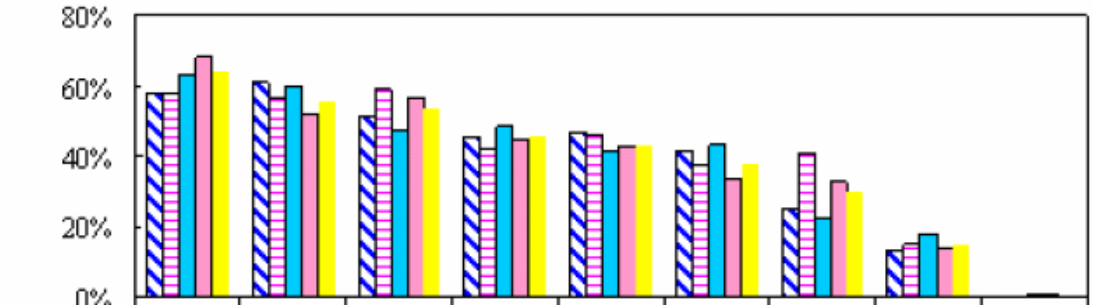


	2005	2006	2007	2008(e)	2009(f)
旅遊產品	38,397	50,300	61,436	71,776	82,044
美容保健	3,417	4,360	6,758	11,082	16,827
服飾精品	1,890	4,803	8,309	14,387	23,859
書籍雜誌	1,262	2,007	2,858	3,580	4,396
資訊電子	7,028	9,261	11,839	14,375	17,147
票務	4,773	5,728	6,874	8,180	9,627
其它	3,715	5,934	8,741	13,199	20,132

圖 1.1 2005-2009 年台灣 B2C 市場規模

近年來，日漸頻繁的網路交易平台成為許多犯罪者取得個人隱私資料的「便捷」途徑。根據刑事局 2008 年網路購物平台客戶被詐騙統計，全台灣主要購物平台 (見註一) 客戶被詐騙數高達 15,044 件，金額亦高達 4.89 億新台幣，除了顯示網路犯罪者的猖狂，亦顯示網路安全的重要性。近年來相關研究以及實際事件的發生，已經得到證實。如何增進網路安全，減少因為網路攻擊而受到傷害的機率，以及如何減少攻擊所造成的傷害，已經是資訊安全熱門的研究議題 (Alpcan 2003)。

註一: 資料來源**刑事局 165 反詐欺專線週報 2008 年統計** 購物平台遍及網購，網拍，電視購物，郵購業者；計有 PayEasy、YAHOO 拍賣、東森購物、年代購票網、DHC、PCHOME、MOMO 電視購物、博客來、興奇科技(YAHOO 購物)、金石堂、新絲路網路書店、華文網路書店、統一購物網、露天拍賣、鼎文書局、巴哈姆特電玩、LATIV 生活著、太平洋 SOGO、美商如新、VIVA、鼎茂書局、誠品書店....，有報案紀錄的平台業者超過八十家者



	取貨便利	技術安全	習慣使用	口碑	付款方式	退換方便	已建立紅利、個人資料	客服諮詢	其它
高所得男	57.7%	60.9%	51.4%	45.5%	47.0%	41.3%	25.2%	13.5%	0.4%
高所得女	57.7%	56.7%	59.0%	42.3%	45.9%	37.8%	40.8%	15.0%	0.3%
低所得男	63.1%	59.6%	47.3%	48.5%	41.5%	43.3%	22.7%	18.2%	0.5%
低所得女	68.3%	51.8%	56.8%	44.8%	42.8%	33.4%	32.8%	13.7%	1.0%
整體	63.9%	55.9%	53.6%	45.6%	43.4%	37.9%	29.9%	15.1%	0.7%

圖 1.2　2008 網友選擇購物平台因素考量

表 1.1　2008 年網友認為購物平台可改善項目

排行	2007 年	2008 年
1	介面容易找到需要的商品(63.7%)	介面容易找到需要的商品 (65.9%)
2	資料安全性(57%)	網站容易瀏覽(61%)
3	網站容易瀏覽(53.7%)	資料安全性(52.9%)
4	簡化交易流程(40.3%)	簡化交易流程(41.4%)
5	改善視覺效果(30.9%)	改善視覺效果(27%)
6	線上可與客服人員即時通訊(30.6%)	線上可與客服人員即時通訊(25.1%)
7	線上可與賣方即時通訊(28.4%)	線上可與賣方即時通訊(22%)
8	設定個人化頁面(22.6%)	增加影音展示說明(21.5%)
9	寄送年度消費清單(27.6%)	建立社群討論區或 Blog(20.5%)
10	建立社群討論區或 Blog(25.2%)	寄送年度消費清單(20.2%)

資料來源：資策會 MIC，2008 年 11 月

2007 年 12 月 11 日上午 11 點，擁有 240 萬名會員的 PayEasy 購物平台發現來自中國福建廈門地區的 IP，大量比對 5 千多個會員帳號的密碼，行逕疑似企圖竊取會員的個人資料。正在開主管會議的 PayEasy 資訊部副總經理，在接獲資訊部門回報後，立即通知總經理。這次詐騙攻擊事件是來自中國福建廈門地區的詐騙集團，該集團事前已從四面八方取得大量個人資料，包括身份證字號、電話、地址、出生日等，以及網站登入資料，例如帳號、密碼、交易紀錄等，進行「資

料拼圖」，並利用拼湊出來的帳號與密碼，比對 PayEasy 是否有使用相同帳號、密碼的會員，藉此取得購物明細以進行詐騙。他指出，中國駭客集團總共比對了 39,000 多筆會員帳號和密碼名單，大約有 14%（將近 5,500 名會員）的名單和 PayEasy 會員所使用的帳號、密碼相同。

這是許多線上購物購物平台所面臨的難題。因為一般使用者習慣在多個網路服務使用相似的帳號密碼，一旦犯罪者利用其他網站的資訊安全漏洞，竊取到帳號密碼，就會利用這份資料，藉由「資料拼圖」的駭客手法，比對各大知名網站，企圖能順利登入，堂而皇之地取得個人資料。但除了網路安全的漏洞所造成的外部威脅外，內部員工將資料外流、脆弱網路系統以及因應法律需求的事件也構成個人隱私外流的一大威脅及挑戰。以致相似事件層出不窮，防不勝防。以往各大被入侵網站，多單單只有向警局備案，或淡化處理，使受害者與日俱增。但資訊安全的威脅不只單純留在財務層面，對賴以網路為生的購物業者，更會影響到品牌形象甚至威脅企業經營 (MIC 06,2008)。

跟同業不同的是，PayEasy 在 2007 年面對相同的資安威脅時，採衝突對峙的賽局策略「囚犯困境」(prisoner's dilemma)中的「弱雞賽局」、「邊緣人理論」，將入侵的駭客視為競合的對象。為了使客戶提早警覺，因應詐騙集團的詐騙手法，PayEasy 正視危機的方式，短時間內成立應變小組，通知所有用戶迅速更改密碼，防止對岸 IP 登入等危機處理方式，保護客戶，避免受害人數增加。

因此本論文將從「衝突對峙的賽局策略」的論點切入，探討在面對駭客的外部威脅時，正面面對威脅、處理危機，可以落實「企業社會責任」，以有效嚇阻駭客更進一步的威脅，並用各種管道向大眾、媒體、會員示警，以減少會員在面對歹徒時的「資訊不對稱」，進而降低會員被詐騙得逞的機會以保護平台顧客的權益，重塑顧客忠誠，基業長青。

綜合上述研究動機，本研究目的如下：

一、探討PayEasy面對詐騙攻擊事件之防詐措施。

二、以「衝突對峙的賽局理論」分析PayEasy之因應策略。

第二節、研究流程

為使整個研究的進行程序與內涵能清楚明瞭，在此列出本研究的研究流程圖，如圖1.3所示：

依據研究動機確立所欲研究的目的，並進行國內外資安、企業危機管理與賽局理論相關文獻的蒐集及彙整，以作為解決問題的參考及依據，並藉此整理出PayEasy 危機處理之相關組織配合因素及其影響因素。歸納各學者的看法，配合研究者本身處理詐騙集團危機的經驗，據此做為其他網路購物平台危機管理策略以及刑事單位對於圍堵詐騙集團的參考。


文獻探討：
◎資訊安全威脅
・分析、歸類資安威脅手法
◎企業危機管理
・危機發生的周期
・危機處理與媒體溝通
◎衝突對峙的賽局策略
對歹徒——
・弱雞賽局
・邊緣人理論
對會員——
・使其資訊對稱
◎PayEasy 個案分析
・危機生命周期
・決策手法
・企業危機管理的應用
◎危機管理評估
・賽局應用分析
・資安問題分析與處理方式
◎檢討與結論
・改進的可能性?
・供企業及政府參考

圖 1.3 研究流程圖

第三節、研究名詞界定

1. 衝突對峙的賽局策略

衝突對峙的賽局策略 (Conflict Strategy) 指在與他人一連串動態的互動過程中，瞭解自己的目標、偏好及限制，在詳盡思考後採取對自己最有利的理性行為。

2. 囚犯困境

囚犯困境是賽局理論下的決策困境，指的是當警方逮捕甲、乙兩名共犯時，並未握有證據同時將兩人指控入獄，於是分別將兩個人隔離訊問。假設警方提供下列選項於兩名歹徒。

(1) 若一人認罪並作證指控對方，而對方保持緘默時，認罪的一方將無罪開釋，緘默的一方將有十年的牢獄之災。

(2) 若兩人都保持緘默，則同樣得有半年的牢獄之災。

(3) 如果雙方互相出庭指證對方，則雙方都得坐兩年牢。

在此賽局中，雙方都有優勢策略 (指控對方)，但均衡 (雙方都採用優勢策略) 的報酬比採取劣勢策略 (雙方都保持緘默) 的報酬要低。

3. 弱雞賽局

又稱為懦夫或膽小鬼賽局，這是因為其英文為 chicken game，(chicken 在英文中有懦弱、膽小的雙關意思)，最早的故事是兩個年輕人同時開車相撞，誰先把車子轉彎或煞車，誰就是膽小鬼，較晚轉彎者就是英雄。

4. 危機邊緣策略

危機邊緣策略 (Brinkmanship) 指將危機局勢不斷推升至發生災難的邊緣 (verge)，源自 1962 年的古巴飛彈危機，可以被廣泛應用在國際關係、外交政策上。

5. 詐騙集團

指海峽對岸的詐騙非法組織結合駭客集團、黑幫，利用名單蒐集以滲透及竊

取資料庫，以詐取金錢從事詐欺的集團。

6. B2C

Business to consumer; 企業透過網路提供消費者購物之服務。企業透過網際網路，提供客戶各種交易與服務，而客戶只要利用電腦連接該企業所架設的網站，即可取得各種線上即時服務或進行交易活動。

7. 資料拼圖

將不同來源取得的個人資料比對後，拼湊出完整的資料，再利用一般民眾喜歡用生日、電話號碼等特殊數字作為密碼的習慣，直接上網「測試」各種可能的帳號密碼組合。一旦成功，即可以合法的身份登入使用者帳號，直接觀看使用者的個人資料與各種記錄，讓資料更完整。

8. 駭客

駭客通常有兩種解釋:

1. 是指對電腦科學、程式設計方面具高度理解的人。
2. 惡意（非法）試圖破解或破壞某個程式、系統及網絡安全的人。

本篇研究的駭客指的是後者。

第二章 文獻探討

第一節、資訊安全

一、駭客與詐騙集團

根據賽門鐵克與警政署資訊室發佈的地下經濟研究報告顯示，台灣的詐騙集團與駭客組織已開始相互勾結、各取所需。此份報告是由該公司安全技術與應變中心 (Security TechnoLogy and Response，STAR)， 從 2007 年 7 月 1 日至 2008 年 6 月 30 日之間的地下經濟伺服器蒐集而來的資料。資料指出，地下經濟交易總額超過$2.76 億，其中信用卡佔了 59%、個資佔了 16%，而伺服器帳號為 10%。

其中，詐騙集團提供警政單位的名單給予駭客集團，由駭客集團竊取組織機密資料。而駭客集團可以從各大商業網站，竊取信用卡卡號已從該用戶帳號竊取金錢，或將個人資料外賣給詐騙集團。另外，駭客集團亦將各式攻擊手法包裝成套裝軟體，已供詐騙集團，竊取個人資訊，再利用各式手法欺騙被害人，以獲取更高的利益。

(一) 詐騙集團組織

隨通訊科技日漸發達及兩岸交流日進頻繁，台灣的詐騙集團也將據點轉移至對岸以降低被查緝的風險，但除了組織型態從單一在台經營模式改為跨境模式外，組織架構不變。皆分為「核心首謀」、「機手」、「車手」三部分。「業務」則依不同功能劃分為大陸及台灣兩區。大陸地區主要擔任「機手」，撥接電話以詐騙受害人。台灣地區擔任「首謀」及「車手」，其中「首謀」進行總務及洗錢作業，並負責建置機房平台，將話務從大陸轉至來台；「車手」主要負責測試人頭帳戶及負責領款 (如圖2.1所示)。

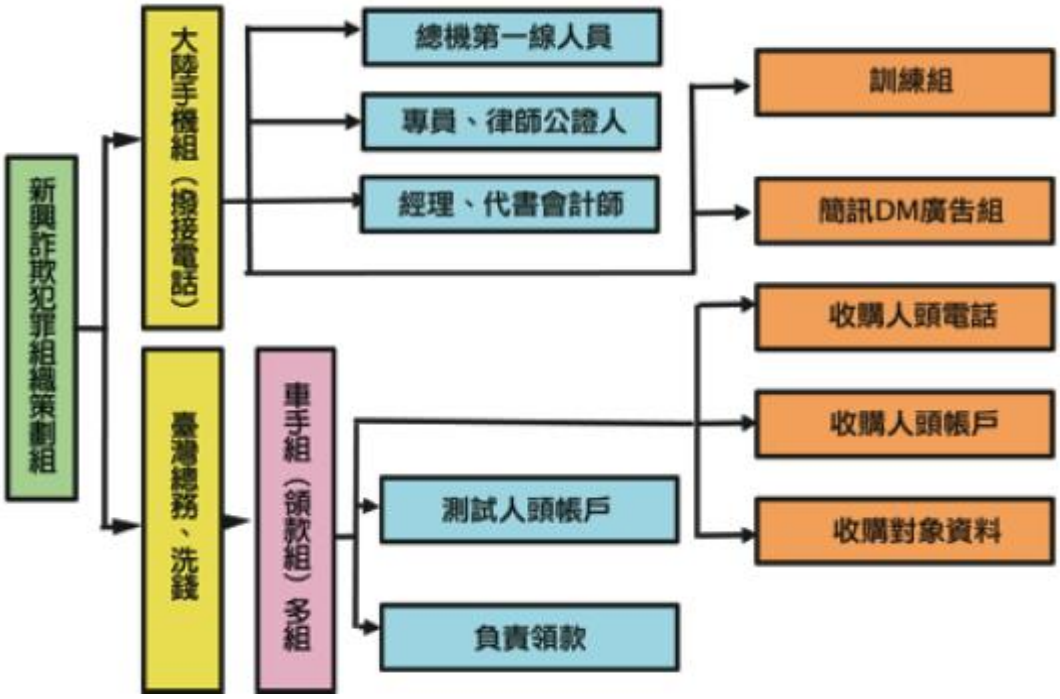


圖 2.1，詐騙集團組織圖 (陳永鎮，2008)

(二) 詐騙集團的三項特性

根據陳永鎮(2008)「新興詐欺犯罪特性及運作模式之探討」一文探討，現在的詐騙集團具有以下三種特性。

1. 具有「三低二高」特性：

「三低」成本低、風險低、量刑低

「二高」報酬高與隱匿性高。

2. 非屬智慧型犯罪：集團成員教育程度及學歷不高，社會大眾被害多，詐騙技術的改進源於經驗傳承、相互觀摩學習及編撰教戰手冊。

3. 手法多樣化：犯罪高層並未具有犯罪工具的專業知識，而是利用整合其他專業人士的技術進行詐騙。因此依業務的專業衍生出不同分工集團，如：竊取資料的駭客、收購人頭帳戶集團、電話集團、收購個人資料集團、車手及電信集團等。

(三) 詐騙集團運作模式

詐騙集團疑先勾結不肖通訊行或個人以冒名證件向電信公司申購大量人頭電話SIM卡，並將民眾名冊電話轉寄大陸「機手」。並建置電話機房平台。將話務從大陸轉接至台灣，以利大陸「機手」對一般民眾進行詐騙。另外，集團會收

購人頭帳戶，並購買「青的」(郵局）及「紅的」(其他金融銀行）等帳簿供提款車手使用。詐騙對象的名單，則可能透過網路駭客，不肖內部員工等多元方式取得，以利詐騙集團取信於民眾，以詐騙成功。成員之間為防止警方查緝，以綽號及單線方式聯繫，彼此不知對方真實身份，極為保密，所以警方往往只能逮捕車手，卻無法破獲整個詐騙組織 (張意唐、李中宇，2006)。

(四) 詐騙步驟

圖2.2跟圖2.3描述詐騙集團於詐騙時所採取的步驟，步驟通常可以分為引誘、取信、言聽計從三個階段。手法規劃也會依警局政策、民眾反應適時更新，確保集團可以持續獲利。由於網路交易日漸頻繁，買賣方之間的聯繫往往成為詐騙集團的切入點，加上詐騙集團現已跟網路駭客有合作關係，透過駭客取得個人交易及私人資料，將使得詐騙情境更能取信於當事人。

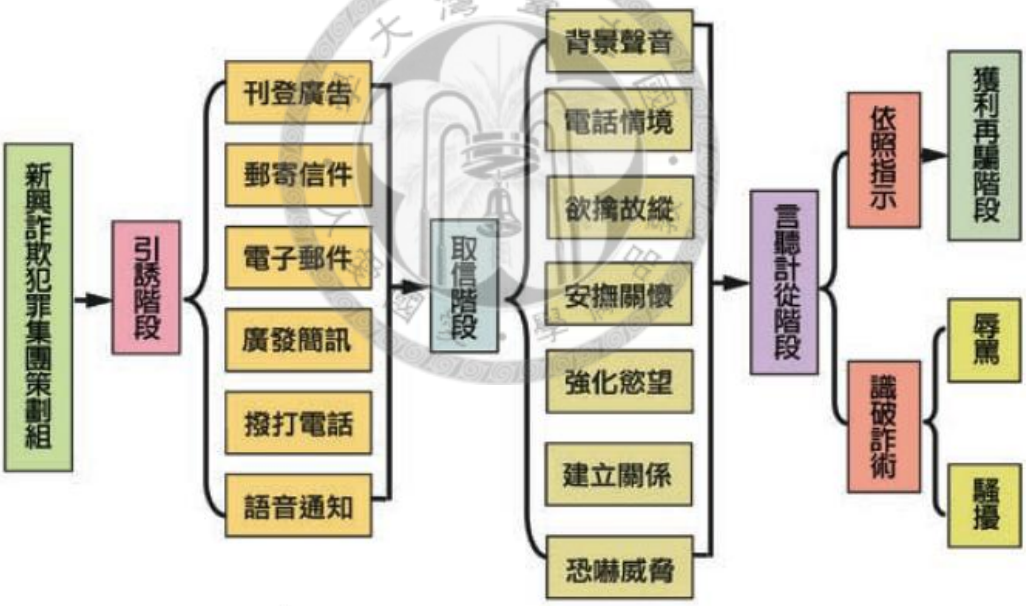


圖 2.2　詐騙互動流程圖 (陳永鎮，2008)

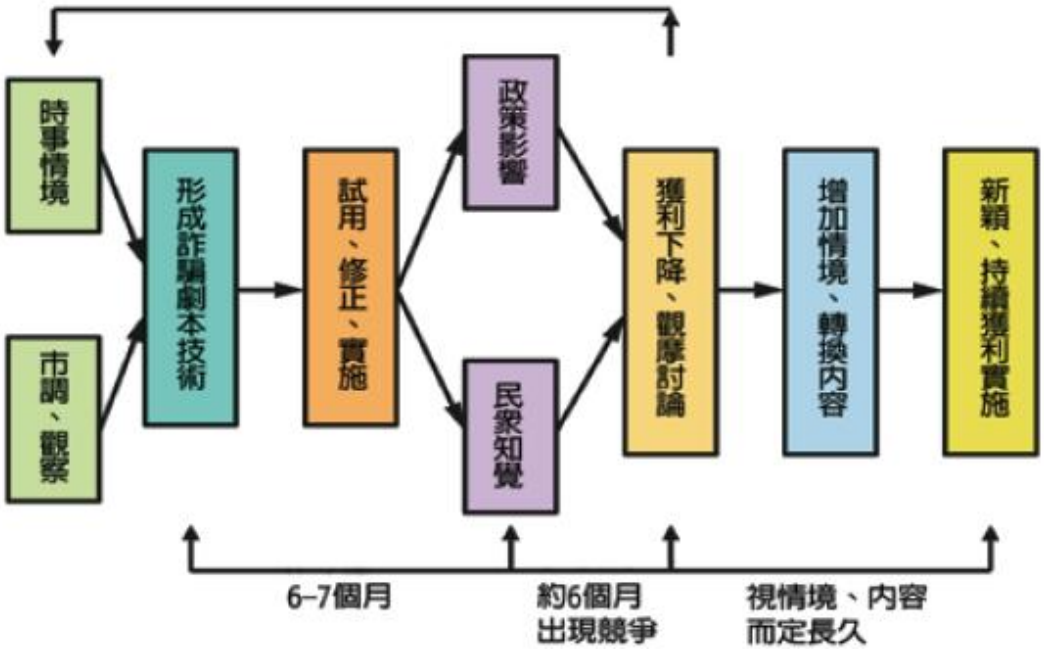


圖 2.3　精進詐騙技術流程圖 (陳永鎮，2008)

二、資訊安全的定義

根據美國安全系統協會 (CNSS) 定義，資訊安全是保護資訊以及其重要元素，其中包含使用、存取、傳送資訊的系統以及硬體。世界經濟合作開發組織 (Organization for Economics Corporation and Development, OECD) 在2001年會議中則將資訊安全的目標訂為「確保資訊系統上的各種利益，及避免機密性 (Confidential)、完整性 (Integrity) 及可用性 (Availability) 受到損害」，機密性、完整性、可用性即成為議題中所主要討論的三個目標 (見圖2.4)。

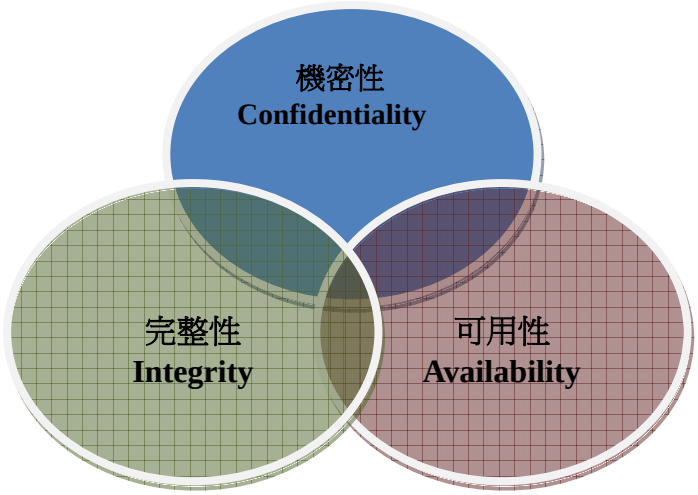


圖 2.4　資訊安全的三個目標

- 機密性：必須確保唯有擁有權限的使用者得以存取資料。
- 完整性：確保資料在傳送的過程中，保有資料原有的完整性。
- 可用性：通過認證的使用者可以隨時取得所需的資訊。

根據資訊安全規範BS7799中的論述，達成三個目標方能確保企業經營上具有競爭力、現金調度流暢，符合法律規範及維護良好的企業形象。

隨著資訊漸漸融入日常生活之中以及資訊安全漏洞對企業及個人所造成的龐大損失，管理資訊安全也成為企業經營的骨幹之一。資訊安全可以分為「技術面」跟「管理面」來探討。以往，資訊安全被狹隘定義為技術、設備漏洞的問題，但根據 CSI Computer Crime & Security Survey 2007年的報告，平均每一企業因為資安活動所造成的損失高達$350,424，其中大部分的損失都來自於內部不肖員工竊取商業機密而造成。這事件顯示單單解決技術上的漏洞不能防堵自家人所造成的損失。因此，如何管理資訊安全，已經比如何在技術上面應對安全漏洞更來的重要。而管理資訊安全的重責大任，也將從資訊人員本身，提升到管理階層。藉由建立「由上到下」的管理方針，以及制定面對資訊威脅時的應對策略，方能建立與顧客之間的信賴關係，使企業永續經營。

三、資訊安全的風險管理

在面對資訊安全的威脅時，管理階層的對策決定組織面對危機時的成敗。身為管理階層，必須具有以下三種特質 (岸田明，2004)：

1. 給予組織承諾與領導統御

企業的安全意識是企業文化的一部分，管理階層必須在資訊安全的面向中，承擔責任，並承諾授權於下屬全權處理資安威脅。

2. 參與風險分析

領導者必須實際參與風險評估規畫，並針對風險評估的內容，決策資訊設備的採購或補強。

3. 與團隊積極合作

事故發生時，不斥責執行者，以免執行者因畏懼而隱瞞資安漏洞的事實，釀成更大傷害。

管理階層必須從了解資訊安全所可能碰到的威脅、資訊漏洞以及可能的損失後，評估風險及其後的影響可以為組織提供更好的決策支援 (李順仁，2003)。資訊安全的風險管理可以利用風險矩陣來加以表示（見圖 2.5）。其中，若系統中的漏洞或是威脅越多時，所要承受的風險也會相對增加。因此具高威脅及多漏洞的第一象限具高度風險，低威脅及少漏洞的第四象限為低度風險區。

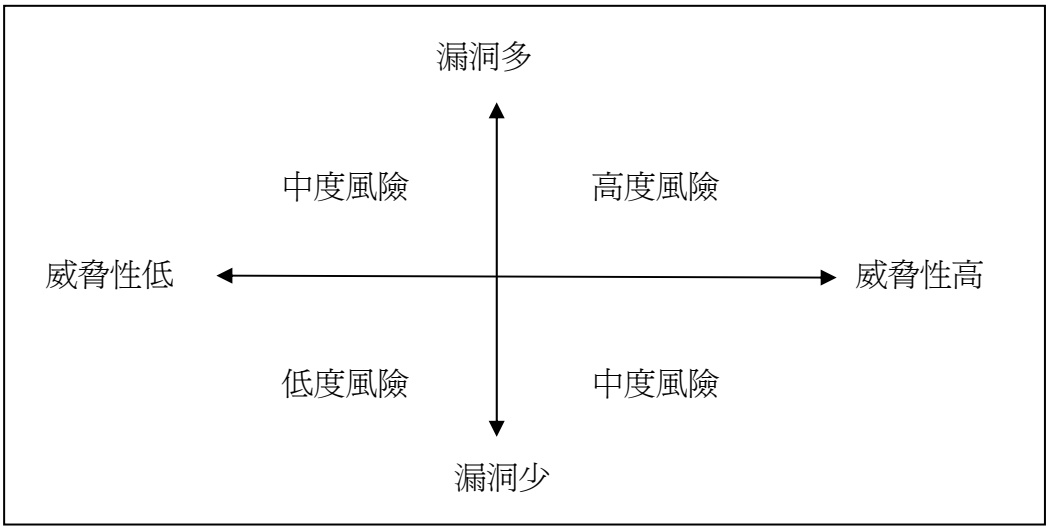


圖 2.5　風險矩陣

而進行完風險評估後，建立風險管理機制以應對不同威脅及漏洞，風險管理可以分為以下六個項目 (岸田明，2004)：

1. 實體與環境安全

   防止未經核准進出，影響或損害工作業務場所、資產及人員。

2. 人員安全

   降低人員不當行為所產生的風險。

3. 資訊安全

   確保系統的機密性、完整性及可用性不受威脅，並將傷害降到最低。

4. 緊急應變計畫

   對威脅預做準備已降低對事業的負面影響。

5. 安全稽核及事件調查

   提供企業安全狀態吉安全危害得真實資訊，給企業管理階層做為參考或採取必要行動。

6. 安全教育訓練及宣導

   提升員工對企業現存安全威脅和顧慮之了解跟關心，並支持公司的企業安全政策。

四、資訊安全管理的跨層次分析

當多數資訊安全規範 (GMIT, BS7799) 皆只規範單一公司的資訊安全管理政策時，這些規範仍難以防堵現今駭客多變的網路攻擊模式。以 PayEasy 在 2007 年受到的資安威脅為例，當時位於對岸的駭客先以各式網路攻擊手法竊取其他網站上的個人資料，再利用資料拼圖的手法，突破 PayEasy 的資安防線，竊取更多的客戶資料。從這個例子中，可以發現即使 PayEasy 建構再強大的資安系統，如果同業的資安漏洞沒有進行修補，亦難逃被攻擊的命運。此時若以圖 2.5 的風險矩陣來做評估，此時風險即來自於同業的資安漏洞，而非公司內部。上述例子說明單一公司內的資安分析已不符現實情況，因此必須利用跨層次分析 (Cross-level Inference)，根據不同層次的「單元」間不同的特質，分析不同層次間的「互動」關係。不單分析公司內部的資訊安全，更需分析公司與公司間對資

訊安全所抱持的態度以及其他公司的資訊漏洞對自身客戶權益的影響。

為探討資安風險對公司所造成的影響，可以根據不同的層次可以定義出不同的分析問題：

1. 客戶與公司方面：

自家公司的資安漏洞使得客戶資料外洩，進而可能造成客戶財物上的損失。公司也因為客戶的損失使得名譽受損，公司及品牌價值進而減損。

2. 客戶與客戶之間：

受損失的客戶因為不甘受損，進而利用網路、媒體等媒介聯合其他客戶抵制於該公司消費。

3. 自家公司與同業之間：

其他公司的資安漏洞，使得駭客得以藉由竊取其他公司客戶的資料，進而侵入自家公司的資安系統，造成資安威脅。

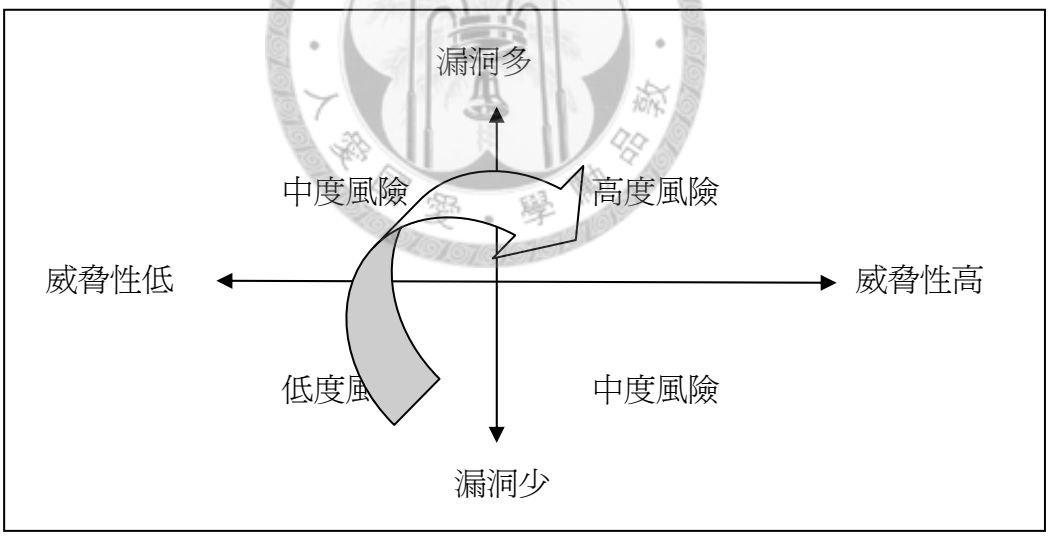


圖 2.6 跨層次的風險移轉

以單一企業來說 PayEasy 為低度風險，但是只要有一家企業出了漏洞 就會造成問題，讓詐騙集團有機可乘，因此如此的系統性風險，會使 PayEasy 成為高度風險的企業。(如圖 2.6 箭頭所示)

在本篇研究中，我們更關注自家公司與同業是否能在資安議題中取得共識。

同業間如果皆能加強自家公司的資安；分享公司近期受到的資安威脅事件；提供同業資訊能於事件發生前做進一步預防的動作；甚至同樣正視網路駭客及詐騙集團帶來的威脅。同業間即可形成一密不可分的鎖鏈 (Chain)，化解每次的危機。若同業間採取不合作的態度，公司間的關係即像一條殘缺不全的破鏈 (Broken Chain)，使得歹徒有機可乘。

第二節、危機處理

企業環境會因自然生態改變、科技進步而更加複雜，危機處理者也將面對更大的挑戰，而且時間更為緊迫。對於危機的型式、發生的原因、處理方式做深入研究，可幫助危機管理者儲備足夠能力與知識應付各種突發狀況。

本論文在探討 PayEasy 購物平台在企業危機下的安全管理做法，因此，將先定義危機處理，並界定危機的類型；探討企業危機的發生步驟，藉此定義 PayEasy 在此次事件中每一步驟的處理方式。此外，在危機發生以後，媒體的報導策略與企業媒體溝通的過程也是一件非常重要的課題。

一、危機管理的定義

任何防止危機發生的措施，都算危機管理。任何消除危機產生的風險與疑惑，使人更能主宰自身命運的辦法都是處理危機。就像小時候考試那一天被提醒帶兩支筆去，萬一有一支鉛筆筆芯壞了，還有另外一支可以繼續參加考試，絲毫不受影響，簡單來說這就是處理和應付危機的一種方法（韓應寧譯，1987）。

Coombs（1999）指出危機可以被視為「資訊缺乏」的情況，在典型的危機狀況裡需要大量的資訊，因為危機發生之初人們所了解的事實非常少，整個危機會快速變化，其變化情形沒有規則難以預料，因此能否有效率處理危機壓力，在於如何快速地、正確地取得資訊並加以處理（林文益、鄭安鳳譯，2001）。

危機處理是在危機爆發之後，企業被迫的緊急處理，如同航空公司遭遇空難事件一樣。企業危機的發生，常與缺乏危機意識與危機管理計劃有關，這種習而不察的漸進危機，待爆發之際常使企業措手不及、資訊不足、壓力極大、破壞力

極強、可反應的時間極短、危機處理的選項極有限等。危機管理屬於預防階段，有充分時間與人力，而且不像危機處理階段的龐大外在壓力及有限的時間。在此階段如果不能辨認危機因子、程度及其癥結，就無法適時順利的解決危機，更可能浪費危機決策的寶貴時間（朱延智，2003）。

危機處理是危機管理的一部分，即是組織在危機爆發期所進行的決策過程、採取的應變措施、以及溝通行動等一系列實務工作執行之動態過程，其目的在於災害控制，將組織的損失減到最小（王紫薇，2004）。危機處理，就是使危機小組及時運作，並依計畫緊急動員、傳訊聯絡、籌謀對策、尋求奧援、爭取在第一時間解決等（朱愛群，2002）。Barton（2001）即認為，危機處理的成敗是以組織能否影響利益關係人的認知及想法為指標，即強調以利益關係人立場為考量之重要性（吳宜蓁譯，2002）。

綜合上述專家對危機管理的定義，多認為是不管在危機前、危機時或危機後等各階段，針對危機所做的一切處理均稱之。也就是包含了發現、偵測、警訊、爆發、行動、控制、減少損害、善後、補救、學習或解決等許多處理階段。

二、危機的類型

Gonzalea-Harrero 與 Pratt（1995）將危機區分為風潮型（fad）、攀高型（scalable）、循環型（cyclical）。風潮型：指稍縱即逝的危機，來的快、去的也快，是威脅性最低的危機類型，也代表企業組織危機處理得宜，使危機在最短時間內得以化解，迅速終止。攀高型：危機處理不當、使危機如滾雪球般擴大，或是危機本身複雜，原本的危機強度不斷累積，甚至發展成另一種危機。循環型：通常和季節時間有關，景氣造成的經營危機，如颱風季節對農漁業的威脅（轉引自吳宜蓁，2002）。

不過吳宜蓁（2002）認為，循環性危機又意謂一波未平一波又起的波浪式危機，當一個危機即將衰退終止時，突然又形成一個新的危機。例如1994 年間麥當勞連續發生多起顧客遭熱咖啡燙傷的事件，受傷顧客怒而控告麥當勞理賠，使得麥當勞付出相當的金錢和形象的代價。

三、企業危機的生命周期

朱延智（2002）的「企業危機生命週期理論」 (如圖2.7)，闡述危機在不同階段有不同的生命特徵，並分別提出對策：

1、危機潛伏期：許多危機皆是漸變，在爆發形成嚴重危機前之問題癥結，即潛藏的危機因子。通常此時危機徵兆並不明顯，若能掌握警訊，及時處置，將危機化為無形，則小警訊將不會形成大危機。

2、危機爆發期：當危機升高、跨過危機門檻後，危機即進入爆發階段。此時可能會威脅到企業的重大利益，造成企業營收頓減、企業形象受損，甚至可能下市或未來經營嚴重受挫而瓦解。倘若不立即處理，則危機將會升高，造成損害之範圍與強度會變為更廣、更大。

3、危機擴散期：企業發生危機後，會對其他領域產生連帶影響，有時會衝擊其他領域，而造成不同程度的危機，尤其危機的破壞力愈大，形成其他領域的影響也愈大。

4、危機處理期：此時期之發展則端視危機決策者的專業智慧，企業若能找出且運用企業本身所具之優勢，掌握外部可用機會，使優勢發揮到極大化，並使外部機會擴大到極大化，進而運用此外部機會，掩蓋與化解企業本身的弱點，克服外在威脅，使威脅極小化。

5、企業危機處理結果與後遺症期：危機經過緊急處理後，問題可能獲得真正解決，或者無效的危機處理致使企業受到的威脅更為嚴重。即使針對問題、解決問題，但難免仍有危機殘餘的因子存在，甚至會重新進入危機潛伏期；倘若未徹底解決，所疏忽的危機可能會在此時期不經醞釀期而再度引爆。

Gonzalea-Harrero 與 Pratt（1995）亦將危機視為如生命週期，經歷出生、成長、成熟與衰退四個階段。Fink（1986）則是將危機的發展比喻為疾病，發生原因取決於幾種變數，是一種不穩定、會變化的狀況。過程從危機潛伏期（Prodromal crisis stage）、危機爆發期（Acute crisis stage）、危機善後期（Chronic crisis stage）和危機解決期（Crisis resolution stage），循環不斷週而復

始，當一個危機解決時，可能又是一個危機的潛伏（韓應寧譯，1987）。

1、危機潛伏期

潛伏期就是危機警告期，是危機事件轉機的關鍵時刻，這個時期會有一些徵兆提醒組織正視問題。所以潛伏期又稱作「危機發生前」的階段，這時期的危機處理不但簡單而且有效，所以若能早期發現就能抑制損害。

2、危機爆發期

警報一結束就由潛伏期進入爆發期，事件已造成損害發生，損害的輕重就要看接下來的表現。此時處理危機的關鍵在儘量能夠控制危機，如果不能控制危機的發生與否，就儘可能影響危機爆發的地點、方式和時間，比如可以選擇發佈新聞的時間和地點來減少危機的損害。

3、危機善後期

危機善後期也是恢復期。屬於自我分析自我檢討的療傷止痛期，聰明管理者應該運用這段期間做好進一步的「危機處理計劃」，分析出毛病出在什麼地方，並採取補救措施。此時期有時會是公司財務不安、人事改組、被其他公司接收和宣告破產的時期。如果有實行危機處理計劃即可以縮短這個階段的時間。

4、危機解決期

此時危機已完全解決，在現實生活裏，一場危機的解決常是另一場即將來臨的危機預兆。

雖然各學者對危機發展的階段期各有所差異，但在內容上卻都雷同。無論是 Fink（1986）的四階段論或是 Coombs（2001） 的三階段論，從中都可歸納為三大部分，也就是危機前、危機時及危機後。危機前包括了發現、偵測、警訊、預防或準備；危機時包括了爆發、行動、控制、減少損害、克服；危機後則包括了善後、補救、學習或解決。而不管是風潮型、攀高型或循環型，都會歷經這些階段，只是時間處理上的長短。但就如同 Booth（1993）所言，縱觀許多危機的發生，其實危機的發展並不必然有一定的規則。某些危機並沒有歷經警訊、偵測等的危機前階段，就直接近入危機階段而讓人措手不及。

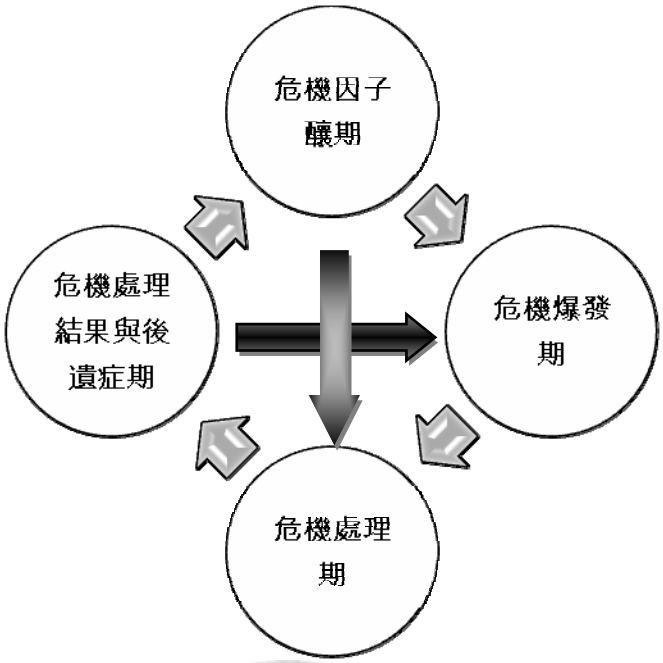


圖2.7　企業危機生命週期

四、危機處理與媒體溝通

記者與消息來源長久以來兩者間存在相當複雜的關係，雙方的互動不但影響到新聞的採訪，更涉及新聞內容的報導趨勢和結果呈現。余穎（1998）研究發現，地方政府消息來源與記者之互動關係有「同化關係」、「對立關係」與「利益合作關係」三種模式。而在新聞內容的呈現上，不管消息來源處於何種關係之記者，大都不會刻意在新聞中對消息來源做有利的報導；但是在淡化處理不利於消息來源之新聞方面，多數記者認為只要不是大弊案或有損大眾利益之事，基於彼此間的交情，大都會加以配合淡化之。

媒體為了搶新聞，往往到了新聞現場，見到相關人等就進行訪問，為了搶獨家，甚至由現場的目擊者直接描述犯罪過程，且採用許多相關未查證的消息來源，不論是匿名或相關傳聞等。此現象不但有未審先判的情況，且會對裁決者在進行裁決時產生民意或媒體上的壓力，致使裁決的正確性與公平性有所偏差（劉幼俐，1998）。賴富山（2004）的研究指出，第一線上記者與採訪對象的互動，並非侷限於兩個人或記者個人與消息來源的單純互動情境，反而會隨著整個經濟

大環境及媒體組織場域，受制市場導向的實際務實現況，並影響到新聞的內文呈現。綜合上述對消息來源的定義，視消息來源為「新聞的供應者，包括報導中所標明的事件製造者，以及由記者引述之相關言論或資料，彼此爭取成為新聞框架的核心立場。（杜玟玲，2005）

但是相對於在災難性的危機中，媒體基於截稿時間緊迫而事件又極端複雜而難以釐清肇因，為快速轉報災情，媒體與消息來源即會建立了一種合夥（partnership）關係。臧國仁和鍾蔚文（2000）指出，在災難時期媒體極需「災情資訊簡報中心（centralized location for activities）」，一方面便於掌握各項救災基本活動，同時也能藉此進一步尋找更具新聞性之其他消息來源，進行深度採訪報導；依過去研究顯示，一般災難訊息散布來源多來自企業組織發言人及專業人士（如科學家、律師、政府相關處理單位等）（臧國仁、鍾蔚文，2000）。

綜合上述專家學者針對媒體與消息來源之間互動的模式，多數都認為媒體與消息來源多在「同化關係」、「對立關係」與「利益合作關係」間變化。或許是因為隨著時間、空間、環境與事件的不同，媒體與消息來源會隨之轉變彼此間的關係。尤其現在媒體是處在戰國時代，媒體為了搶佔市場、製造獨家，與消息來源間可能存在多重複雜的關係。

因此本研究認為，當企業危機發生時，通常記者會無法了解整體事件的來龍去脈，如何長期培養與記者之間的關係是相當重要的，不但可以讓整體事件的真相公諸於世，並且可以藉此培養企業形象。

第三節、衝突對峙的賽局策略

當競爭者在進行決策時，可以利用賽局理論分析競爭者之間的衝突及理性互動行為，此一作法被廣泛用在商場、政壇、外交界和戰場上。賽局基本上包含三個元素：參與者(Players)、報酬(Paysoff)以及策略(Strategies)。同一賽局的參與者會為了獲取最大報酬，選擇對自己最有利的策略來進行賽局。

駭客跟企業資安系統的攻防，也同樣可以使用賽局理論來加以評估。其中，

駭客跟企業可以視為賽局中的競爭者，駭客希望侵入企業主的系統之中，取得關鍵資料，並加以轉售，但得必須避免被警方盯上並逮捕的風險；同樣的企業主必須防止資料外流，造成企業金額及名譽上的受損，也防止顧客權益受害。因此，近年來賽局理論也被廣泛用在於擬定應對外來侵入者的策略，以及用於評估資訊安全設備的風險。

以下介紹在面對衝突對峙情況下，可以使用的賽局策略。並說明如何利用資訊對稱，彌補資訊劣勢，並逆轉賽局中的競爭地位。

一、賽局策略

1. **懦夫賽局**

當賽局有多個均衡時，不能單用納許均衡（Nash equilibrium）來思考策略，此時懦夫賽局可以作為多均衡賽局的解。懦夫賽局起源自 1950 年，比喻自兩個美國年輕人在同一條街道上相向而駛，如果將車子偏向以避免車禍的人即是「懦夫」，而不轉向的人即為勝利者，但如果兩個人都不轉向，雙方就會互撞，發生車禍。

懦夫賽局的報酬，只有尊嚴受損或身體受傷兩種結果。如果將雙方競賽的可能結果寫成假設性的報酬表（見圖 2.8），可以發現雖然雙方都希望獲勝，卻也都不希望發生車禍。在兩種報酬權衡下，雙方都為懦夫的結果比只有自己是懦夫的結果要好。因此為了在懦夫賽局中勝出，必須讓大家認為自己是強硬的，以嚇阻對手。或是讓對方相信自己已經做了直衝的承諾。

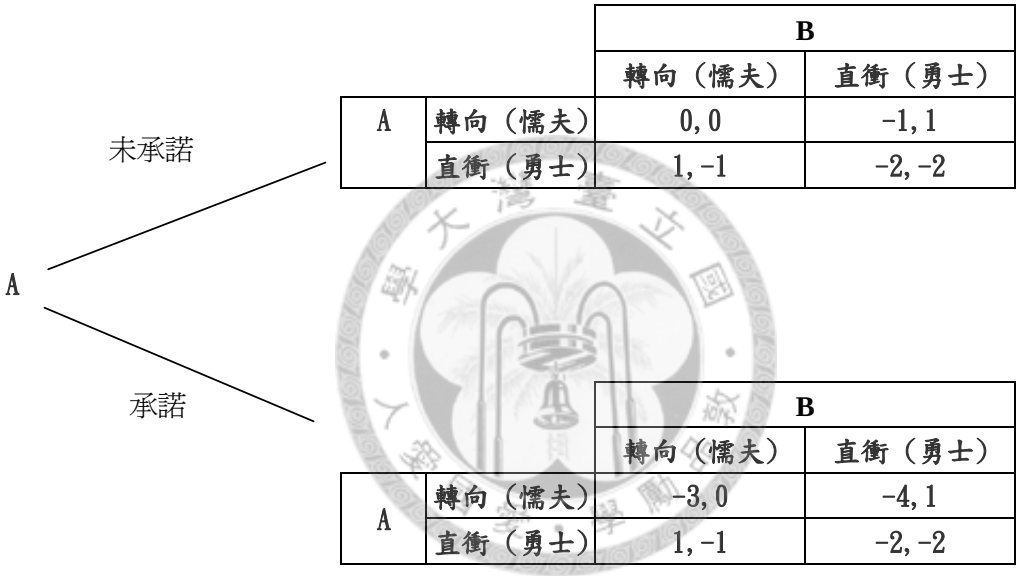
		B	
		轉向（懦夫）	**直衝（勇士）**
A	**轉向（懦夫）**	0, 0	-1, 1
	直衝（勇士）	1, -1	-2, -2

圖 2.8 賽局報酬

圖 2.8，A、B 為兩個同樣參與懦夫賽局的參賽者，若其中一方在競賽中轉向，而另一方繼續直衝，則直衝的一方將獲得勝利，並在報酬表上獲得一分；轉

向者則損失一分。若兩者皆持續直衝，則會發生車禍，產生雙輸的局面。因此，當雙方都承諾自己是懦夫時，才會雙贏。

為了讓承諾更取信於對手，這個承諾必須符合(1)堅決(2)被對手知曉。例如：參賽者中的其中一方將方向盤拿掉以讓對手相信自己是玩真的，從兩階段賽局樹中，可以發現當A作出承諾時，賽局表的報酬將會隨之改變。此時對A來說，直衝相對於轉向來說，會是比較好的選擇。而 B 此時應該選擇轉向，以避免發生車禍。



		B	
		轉向（懦夫）	直衝（勇士）
A	轉向（懦夫）	0, 0	-1, 1
	直衝（勇士）	1, -1	-2, -2

		B	
		轉向（懦夫）	直衝（勇士）
A	轉向（懦夫）	-3, 0	-4, 1
	直衝（勇士）	1, -1	-2, -2

圖 2.9　A 作出承諾以後，報酬表上的報酬將變為有利於 A 直衝，B 轉向

2.、危機邊緣策略

危機邊緣策略可視為互相傷害風險不斷提升的懦夫賽局，或是實際生活中的懦夫賽局 (chicken in real game)。懦夫賽局只考量賽局剛開始時對決策對結果的影響，但在實際生活中，決策往往是可以因為情勢而有所更改的。如果兩個參賽者在一開始都互相直衝，隨兩輛車子距離越來越近時，雙方則會考量自己能承受的風險大小以及對方可能的底限而將車子轉向。如果雙方都在車子已經相當接近時再轉向，則最終依然會相撞。

危機邊緣策略緣起於 1962 年的古巴飛彈危機。當時蘇聯在古巴境內部署飛彈，威脅到美國領土及領空的安全，當時美國總統甘迺迪以核戰作為威脅，希望迫使蘇聯屈服，並將飛彈撤離古巴。美方為了展示他們的決心，因此開始展開了封鎖行動，將蘇聯推至危機邊緣。此時的危機就如同兩個互相朝對方直衝的懦夫賽局參賽者。為了使雙方都不致於輸掉賽局或走向毀滅，雙方都得將對方逼到極限，以致情勢不致於對己不利。賽局決策情形可以以下面賽局樹(圖 2.10)來表示。

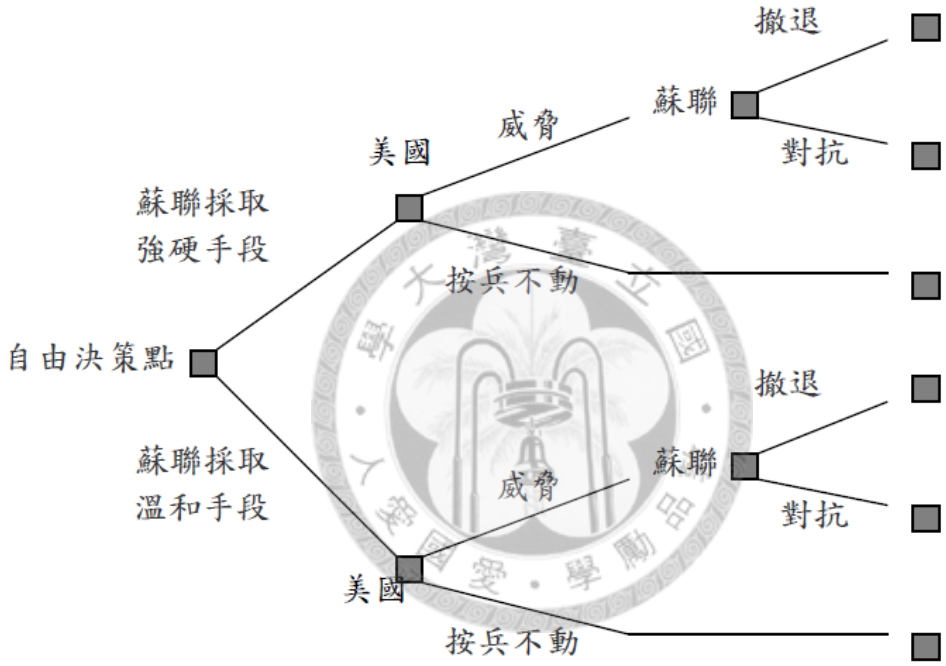


圖 2.10 危機邊緣策略的決策樹

但古巴危機並非只是美俄雙方領導人之間的兩人賽局，而可視為美俄兩方陣營之間的賽局，因為在各方之間都有包含懷有不同目的及不同調的參與者，這些參與者的反應與資訊也會間接影響雙方領導人的決策。因此該賽局可以視為兩方的多人賽局。Graham Allison 在其著作「決策的本質」 (1999) 中曾指出雙方陣營中的分歧意見將會導致領導人決策的更動。而不只對領導人，如果部屬對資訊與情勢擁有不同詮釋，亦會增加此賽局的不確定性，以致於結果變得難以預測。

面對古巴飛彈危機，美方不能單純威脅俄方將展開戰爭，因為單純威脅並未

考量到賽局中其他參賽者所可能潛藏的危險性，使得可能發生戰爭的風險將變得不可控制，並可能將雙方置於不得抽身的狀態，雙方都不會從中獲利。因此，策略目的在於能控制風險成本的情況下有效嚇阻對方，如何控制失控的可能性發生，直到對方在面臨逐漸升高的風險而屈服，才能從危機邊緣中勝出。

以圖 2.10 的模型作為基礎，將雙方的報酬以數字量化。在不知道蘇聯的態度前，假設美國發出威脅後，蘇聯撤退會得到 -8 分，反抗將得到 -4 分，蘇聯則在權衡報酬後，會偏好採取對抗的手段。而一但蘇聯採取對抗手段，雙方衝突的結果會使美國在賽局中失利，獲得負分，以致報酬降至 -10 分，假設美國不提出威脅，按兵不動，則會得到 -2 分，雖然在報酬上處於劣勢，但可以避免戰爭發生，蘇聯則在賽局中勝出。

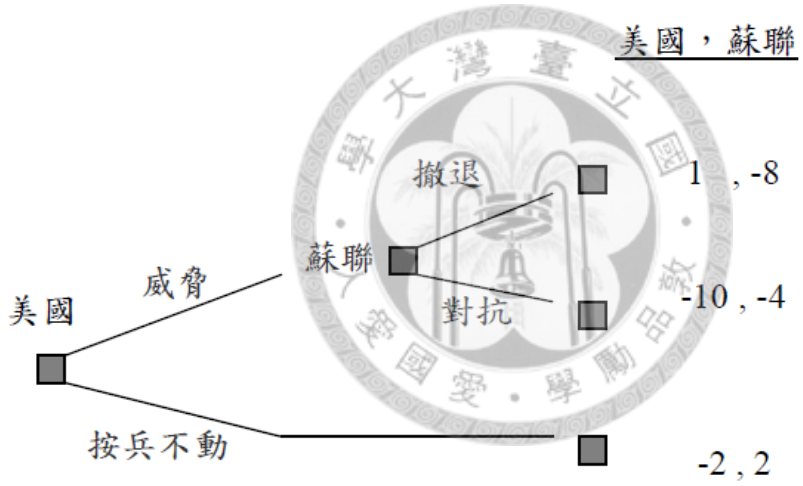


圖 2.11 蘇聯採取強硬手段的賽局

但在此例中，美國無法推斷蘇聯是採溫和還是強硬派，因此可以假設採取強硬派的機率為 P，採取溫和派的機率為 (1-P)，計算期望報酬以推知是否該發出威脅。假設蘇聯採取強硬手段，發出威脅可以得到 -10 分；在蘇聯採溫和手段下，發出威脅可得到 1 分。可推得美國的期望報酬為 -10P +(1-P)=1-11P，而美國不發出威脅時，無論如何都得到-2 分，權衡期望報酬後，當 1-11P > -2 => 11P<3 推得 P<3/11=0.27 時，美國應該發出威脅。重新得出決策樹如圖 2.12。

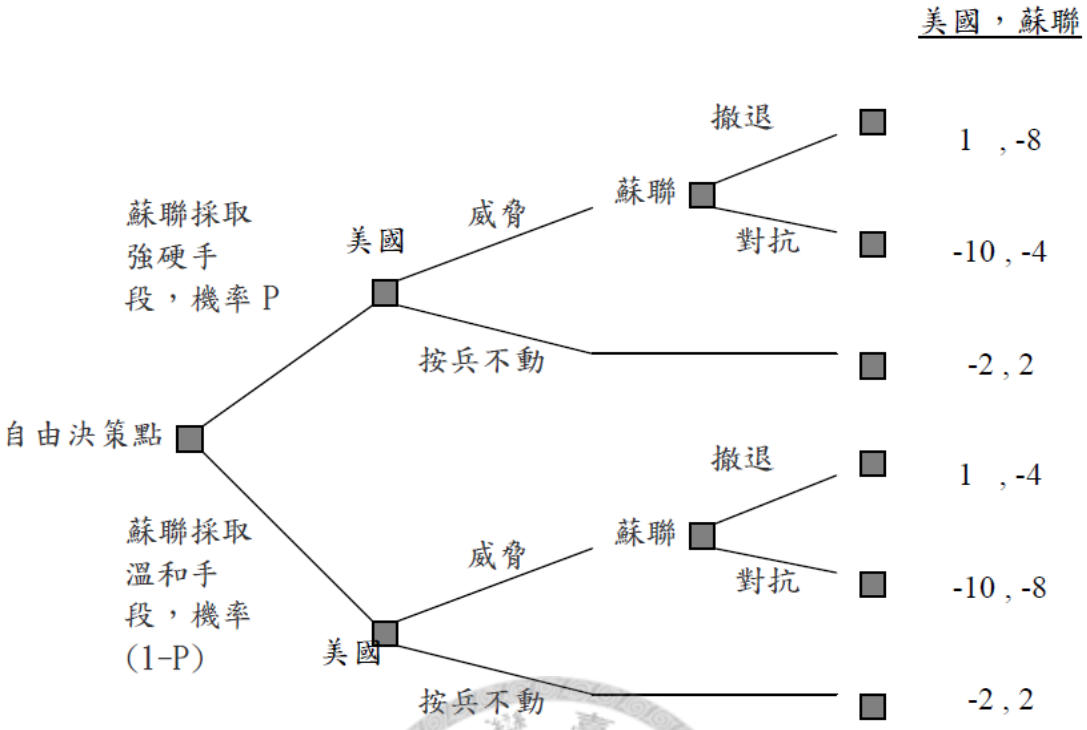


圖 2.12 蘇聯採取強硬手段的賽局機率

雖然可以計算出蘇聯採取強硬手段的機率為 0.27，但採取威脅手段可能招致核子戰爭的可能性，單純用機率來決定對策顯得相當魯莽。因此，為了保全國家利益與避免戰爭，在決策上必須再考慮蘇聯若對抗美國，戰爭發生的可能性。於是將戰爭可能發生的機率設為 q ，(1-q) 為美國讓步的機率。重新畫出決策數可得圖 2.13。

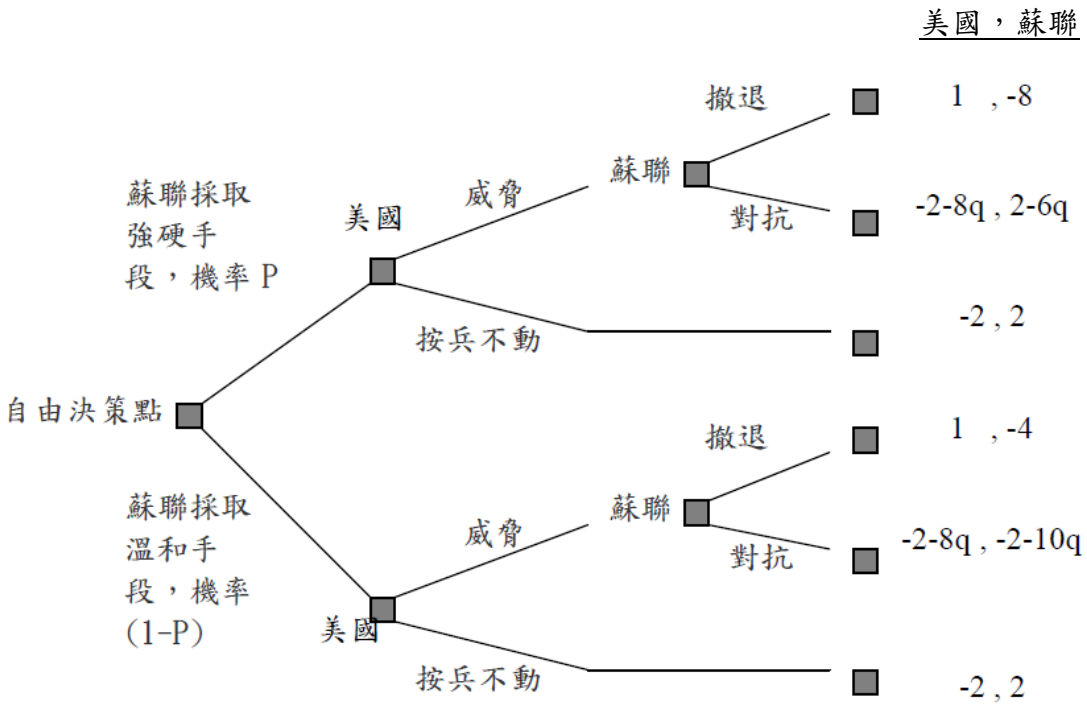


圖 2.13 危機邊緣策略模型

重新評估蘇聯可能的動作，假使蘇聯為強硬派，蘇聯會因戰爭獲得 -4 分，發生戰爭的可能性為 q，美國讓步的話，蘇聯獲得 2 分。可能性為(1-q)，蘇聯可獲得的期望報酬為 2-6q。若撤退的話，蘇聯會得到 -8 分。則不論何種情況下，採取強硬派的蘇聯當局都會反抗美國的威脅。若蘇聯為溫和派，反抗的期望報酬為 2-10q，撤退為 -4 分。所以撤退最好是 -4>2-10q，即 q>0.6，代表要有 60% 戰爭的可能性，危機邊緣策略才能嚇阻蘇聯。

最後將美國採取威脅的機率考慮進去，可能威脅的期望報酬率為 (-2-8q)*p+1*(1-p) = -8pq-3p+1，若美國不做威脅，他們可以得到-2 分，因此美國作出威脅的條件為-8pq-3q+1>-2 或 q<3/8*(1-p)/p = 0.375(1-p)/p，可以歸納出若蘇聯認為美國作出威脅的機率>=0.38，危機邊緣策略即會失效。因此美國必須讓蘇聯認為美國對他們的威脅機率約為 0.38，以達到嚇阻作用，但如果威脅機率大於 0.38，則會有戰爭風險。

二、彌補客戶的資訊劣勢

1. 訊息非對稱的賽局

所有參賽者都是針對已知的消息設計策略，期望在賽局中降低風險或甚至勝出。但在實際賽局中，訊息往往是不對稱的，此時消息多或少的人都必須操作訊息以保持在賽局中的優勢，或扭轉劣勢。

訊息多的參賽者可能會做出以下兩種反應：

(1) 隱藏訊息或顯示錯誤訊息

隱藏訊息可以使訊息較多的參賽者保持競爭優勢，同時訊息較多的參賽者可以放出錯誤訊息「干擾」其他競爭者。

(2) 選擇性的顯示正確訊息

若考量到其他競爭者在收到訊息後可以做出良性的「合作」行為以增加報酬，訊息多的人可以誘導其他競爭者相信你所傳遞的訊息是善意的。

訊息少的參賽者可能會做出以下兩種反應：

(1) 誘出訊息或篩選正確訊息

為了扭轉劣勢，訊息劣勢者則可以採取策略誘導訊息優勢者放出更多消息，然而有可能會遇到消息是錯誤的情形，因此還必須適時的篩選訊息是否正確。

(2) 保持無知

保持無知可以避免受到訊息優勢者的威脅或承諾。

2. 扭轉客戶的資訊劣勢

因為資安漏洞而外洩的客戶資料，會進而成為詐騙集團詐騙的資訊來源。在客戶並不知曉資料外洩的情況下，擁有資訊優勢的詐騙集團可以輕易的在賽局中

占上風，利用客戶資料先取信於對方(見附錄:詐騙手法)，再以錯誤訊息誤導客戶以騙取財物。爲扭轉客戶的資訊劣勢，避免客戶遭受損失，受害公司可以於受害第一時間，將受害訊息告知客戶，避免客戶受害。策略示意圖(圖 2.13)如下。

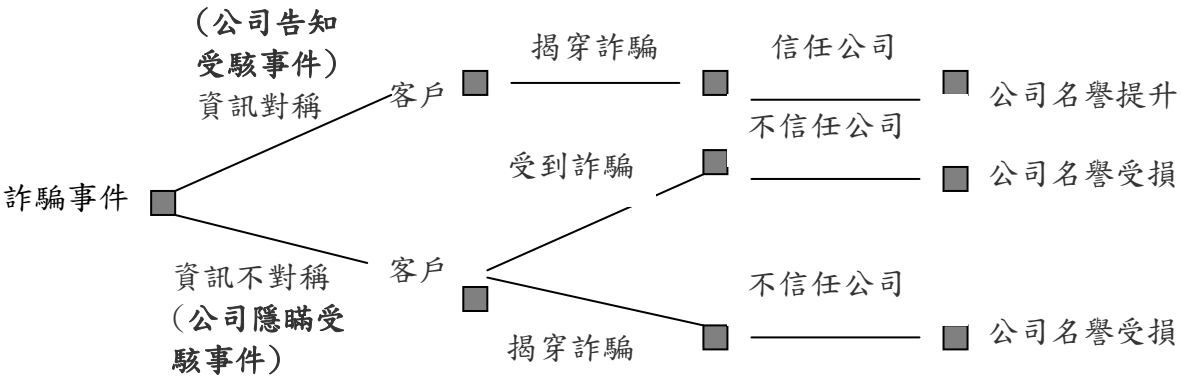


圖 2.14 不同資訊對稱性所產生的決策樹

從圖 2.14 可以發現雖然資訊不對稱不一定會造成客戶上的損失(政策宣導、曾受詐騙)，但公司很可能因為未分享受害訊息，因而使得公司不受客戶信任，名譽受損，客戶進而轉向其競爭者。

第三章 PayEasy 個案說明

以下整理出 PayEasy 公司於 2007 年所遭遇的駭客事件，並敘述在當時身為公司、客戶、詐騙集團、刑警單位不同角色在面對同一事件時，所採取的不同策略。

第一節、公司簡介

PayEasy ，全名為「康迅數位整合股份有限公司」，成立於 2000 年，為台新金控相關企業，並且是台灣目前第三大的電子商務平台，利用虛擬通路 (網際網路)將購買與銷售、產品與服務等商業活動結合在一起，以滿足顧客便捷、多樣化的購物需求。

一、核心價值

相較於其他同業所採取的資本及減價策略 (Capital and Cut price strategy)，PayEasy 模仿百貨公司的經營模式，採取創意及品牌策略(Brain and Brand strategy)，專注於會員價值的創造，更在網路購物的競爭紅海中，穩健成長。以下是PayEasy的經營理念，憑著這樣的經營理念才能創造出不同於競爭者的核心價值，並且，正因為PayEasy有如此的經營理念，在面對駭客攻擊入侵時才能以顧客為優先，維持零詐騙的紀錄。

1.堅持誠信、品質與服務

發展電子商務之初就強調客服的重要性，建置24小時0800免付費客服機制，產品凡有瑕疵故障，絕對提供退換服務，以高品質服務的精神獲取客戶認同。由以下的例子可以看的出PayEasy對於誠信、品質及服務的堅持。2002年初PayEasy在草創時期，推出一條貓眼石的幸運草項鍊，特價199元再加上吸引人的「幸運一整年」的文案，一個禮拜就熱賣9000多條，但兩週後，陸續有顧客抱怨葉片會掉落，原來是因為底部黏著面磨得太亮，導致黏著劑黏不住。

儘管當時PayEasy全部現金只剩500萬元，但公司毅然決定，不論顧客有無主動反映，一律重新補寄新項鍊給先前購買的顧客。這個決定的代價是近80萬元，對當時的PayEasy來說可謂受傷慘重。

2.以網路做公益

開創公益活動新模式，率先投入資源以協助重建區代銷商品為開端，發展出關懷台灣系列活動，並導入台新金控的資源協助重建區的產業發展。自2002年開始協助南投信義鄉銷售梅子，接下來中寮鄉柳丁認養、龍眼密，魚池鄉紅茶，國姓鄉空手道選手培訓，以及去年的稻米企業認養「我的一畝田」活動，至今，已經持續7年，並將繼續推動下去。

3.創造持續創新的環境

在網路上提供更多樣化的服務包括企業電子福委會等系統的建置。

二、 事件參與者關係圖

列出此次危機中的主要參與者，每一參與者對事件的反應都會影響到其他參與者做出不同的反應。

以下分別列出參與者的互動關係：

供應商 V.S. PayEasy：PayEasy 200 多家供應商對此事件也很重視，PayEasy在遇到危機時，有權責向供應商報告事態。

台新金控 V.S. PayEasy：台新金控為PayEasy 的關係企業暨股東，PayEasy在遇到危機時，有權責向台新金控報告事態。

PayEasy V.S. 檢警單位：遇到駭客入侵時，PayEasy向檢警報告，希冀檢警協助緝捕歹徒；檢警提供事件處理諮詢及受害民眾報案情形。

PayEasy V.S. 詐騙集團：PayEasy 正面迎擊詐騙集團，呼籲歹徒放棄作案；詐騙集團透過各式入侵手法，企圖竊取顧客資訊。

PayEasy V.S. 客戶：PayEasy 主動向客戶透露受入侵的消息，並以警示函呼籲民眾被詐騙的風險，防止受騙民眾增加；客戶告知 PayEasy 接到詐騙電話，供 PayEasy 及時反應處理危機。

客戶 V.S. 詐騙集團：詐騙集團詐騙PayEasy 客戶。

客戶　V.S. 檢警單位：受騙客戶向檢警申訴報案。

媒體　V.S 全體參與者：媒體報導的內容會影響各個參與者互動的關係。

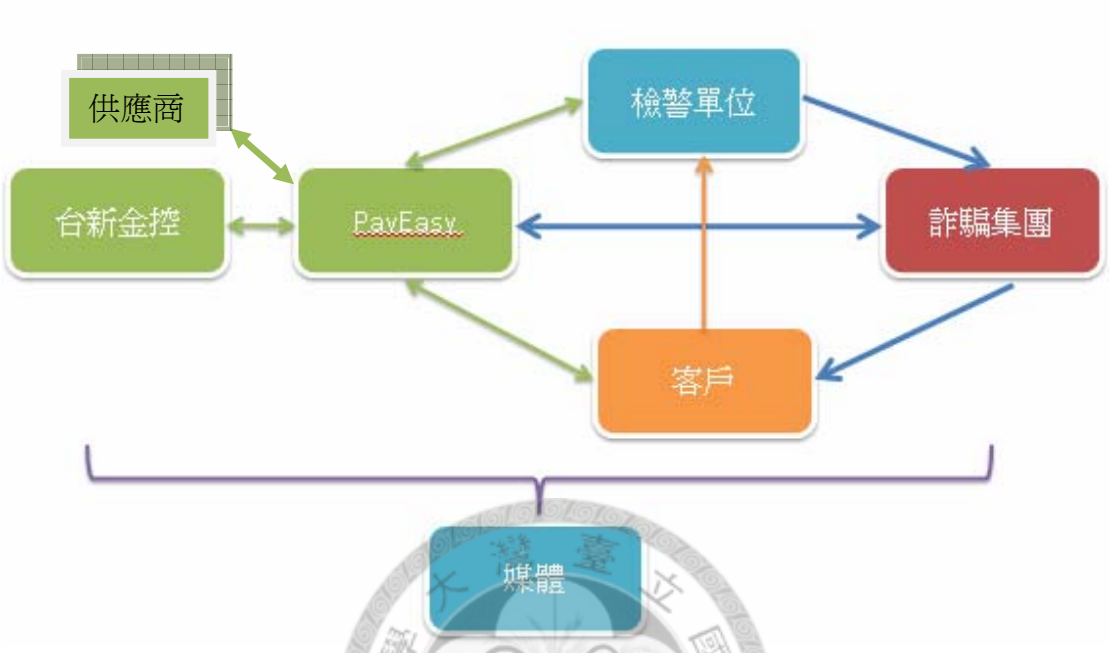


圖3.1 參與者關係圖

三、 各部門權責組織圖

事件爆發之後，PayEasy各部門根據其職責以因應危機，各部門權責組織圖如圖3.2。以總經理為危機處理核心，IT資訊部、客服、公關部、營運以及行銷等部門各司其職，由內到外，化解危機。

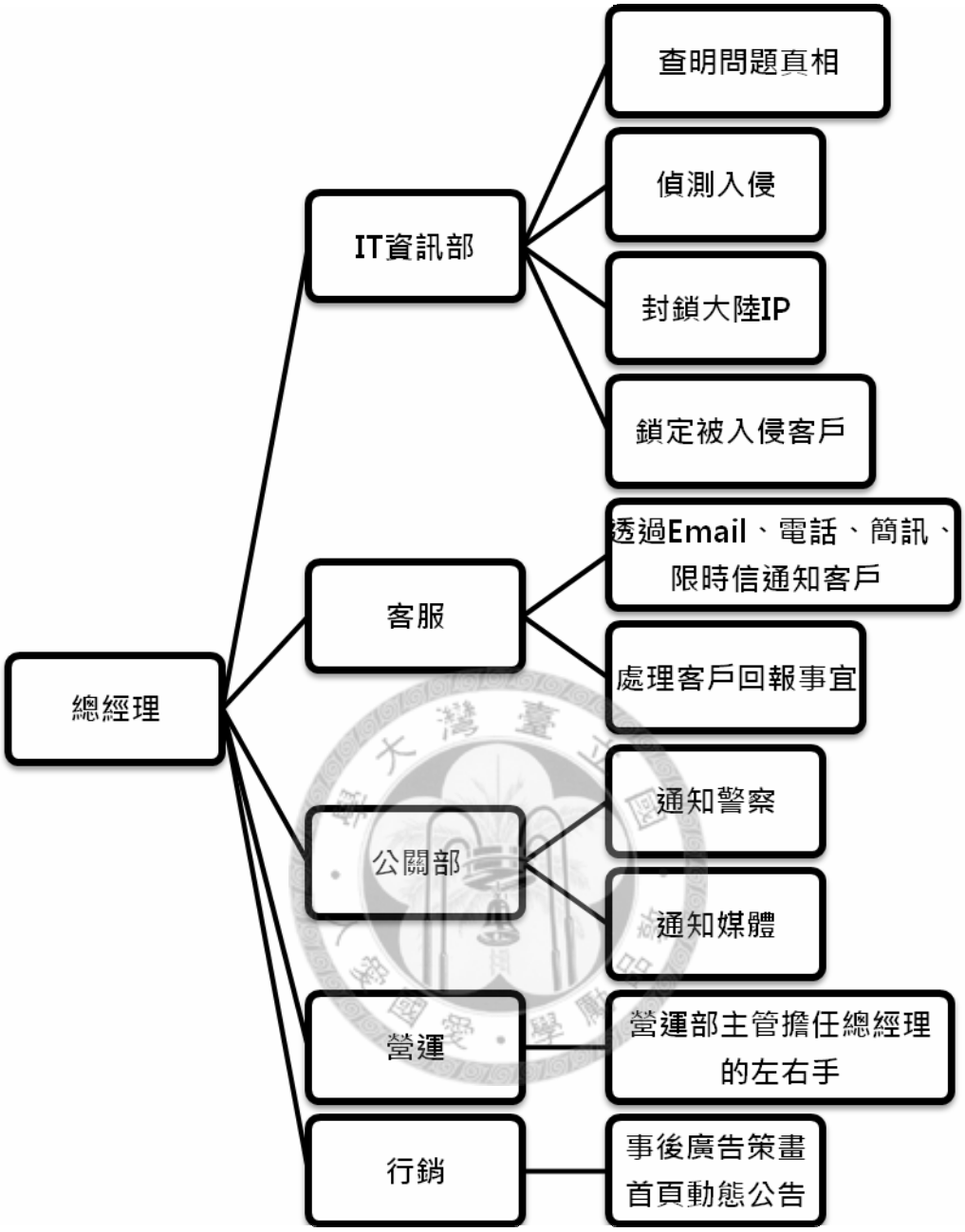


圖3.2 PayEasy 因應危機組織權責架構

第二節、危機發生始末

各個企業因為有不同的企業文化，因此在危機發生時會有的因應措施也都有所不同，PayEasy 在面對詐騙集團的攻擊危機時，又有什麼樣的因應措施？以下參考 Fink（1986）的四階段論，將 PayEasy 的危機事件發生過程區分為危機潛伏

期、危機爆發第一期、危機爆發第二期、危機善後期及危機解決期，在不同的時期都有相應的處理方式。

一、危機潛伏期

在 2007 年十二月九號之前，各大網路拍賣公司如 Yahoo 奇摩拍賣以及博客來等紛紛遭到詐騙集團攻擊。博客來一直以來都很注意資訊安全，會發生這樣的事情，對於 PayEasy 來說是一個重大警訊，詐騙集團已經將觸腳慢慢伸向各大網站，此時雖然 PayEasy 尚未受到攻擊，但是似乎已是危機四伏。

歹徒透過員工監守自盜、木馬程式或是 SQL injection 的方式等知道客戶的訂單資料，而 PayEasy 在 2007 年時，身為訂單數最多的實體店鋪平台，擁有兩百四十萬的會員數以及六百萬的訂單量，似乎很容易成為歹徒攻擊的目標。

因此此時 PayEasy 持續關切其他同業受害情形，並且透過以下方式強化網站安全：

1.強化軟體開發流程

從人員安全訓練、開發流程安全機制以及程式碼安全品管入手。而滲透測試以及原始碼檢測，是最常使用的兩種網站安全檢測方式，主要能尋找出網站有哪些漏洞或程式碼問題。多數企業受限於經費，往往從中選擇出一種測試方法，其實，兩種方式採取相反的檢測思維，搭配使用，能夠相互彌補彼此的缺點。

2.用架構來控管安全

2005 年，PayEasy 重新架構核心系統成 4 層架構，有彈性的 IT 架構，才能貫徹以保護客戶資料為核心的決定。

由資訊部所規畫的 4 層 IT 架構，最底層的核心是資料庫，上一層是 Java EJB（Enterprise Java Bean）中介層，任何應用程式的呼叫或執行，都必須透過 EJB 來執行，再上一層就是 Web 的前端應用程式，最上層則是 Web。資料庫是所有 IT 架構的核心，除了機密資料加密之外，所有的欄位都必須獨立並分割，而所有應用程式要存取相關資料庫資料時，都必須透過 EJB 執行。透過 EJB 把資料庫的資料包裝成資料物件，程式可以用物件化方式去控制資料物件，而不是直接就以 SQL 語法查詢資料庫。

現在很多線上購物平台因為資料庫容易被插入其他的資料庫控制語法，造成 SQL Injection 的資安威脅。因為程式要存取資料庫都必須透過 EJB 呼叫或執行，反而讓常見的 SQL Injection 沒有爆發的機會。

3.用資安防護產品爭取時效

資安防護產品可以第一時間發現網站漏洞，防堵惡意攻擊，爭取修補網站程式防禦碼的時間，也可以避免損失繼續擴大。防禦硬體方面，除了網路安全設備可以提供網 路環境的保護之外，針對網站的防禦，主要是網站應用程式防火牆（Web Application Firewall，WAF)，能同時保護網站與使用者。

4.用權限來控管安全

透過系統嚴格控管員工存取資料的等級，而有權存取客戶重要資料的部門，更要進一步做到網路隔離與實體隔離。之所以要這麼隔離特定員工的電腦，為的就是避免有權存取機密資料員工的電腦，遭到特定的魚叉式攻擊──先透過控制內部員工電腦，以此為跳板再進而入侵資料庫系統。像是必須存取客戶資料的客服部門，不只是採用隔離的網段，客服人員的電腦也無法使用任何 USB 裝置及外接式儲存設備。對於也能接觸到資料的 IT 部門，PayEasy 機房人員則是清一色使用精簡客戶端 (thin client) 機器。

5.將使用者納入網站安全防護圈

PayEasy 針對會員帳號、密碼、姓名等重要資料採取加密保護，若需保管原始資料或檔案，則以 AES 256 位元加密。使用者的安全是網站安全的最後一道防線，網站業者必須將使用者納入防護，才能建構完整的網站防護圈。雖然不論是安裝防護程式，或者是使用一次性密碼的方式，都會造成使用者的不便，但是，不能一味地考慮使用者的方便性，必須在安全性和方便性之間取得平衡。
這個時候雖然 PayEasy 尚未受到攻擊，但是對於可能會出現的危機，採取積極的行動，改善資訊安全加強控管記錄 IP。

二、危機爆發第一期

2007 年 12 月 9 日晚上八點到 2007 年 12 月 10 日早上十點詐騙集團登錄 PayEasy 會員中心。其中有四個 IP 來自大陸福州電信一個 IP 來自香港，共登錄

39,000 筆資料。其中有 23,000 筆(59%)非 PayEasy 會員，10,500 筆(27%) 為 PayEasy 會員但密碼不符合，5,467 筆(14%)PayEasy 會員且密碼符合。這 5,467 筆即成為詐騙集團攻擊的首要目標。

PayEasy 為了維護客戶權益，最後決定正視問題，在 12 月 10 日即採取以下的緊急應變：

- 11:00am 封鎖攻擊的 5 個 IP
- 12:00pm 凍結 5,467 個被比對成功的會員帳號，會員必須重新申請新密碼。
- 12:30pm 確認歹徒攻擊方法，清查受損害範圍。
- 13:00pm 呈報台新兩位長官。
- 13:00pm 開始發簡訊給 39,000 名被比對過的會員
- 15:00pm 至刑事局偵九隊報案，並請求偵九協助預定於 12/11 與刑事局共同召開記者會
- 16:00pm 通報台新公關，台新 IT 等相關部門。
- 18:00pm 向董事長報告，東亮董同意明日召開記者會。
- 19:00pm 發現歹徒又上來測試會員帳戶。
- 20:00pm 開始封鎖來自中國所有的 IP，並派員整夜監測

過了一天，PayEasy 決定要力求保障客戶權益，決定採取與其他同業不同的做法，積極報案，並召開記者會。

- 10:00am 至刑事局準備開記者會，但刑事局並未通知記者到場。
- 11:00am 請求警方讓我們自行開記者會。
- 12:00pm 有兩位會員回報接到詐騙電話，其中一名不在 5,467 名單中。
- 12:00pm 召集全公司同仁，說明事件發生經過，以及我決心與歹徒對抗，向媒體與會員宣告這次攻擊事件。
- 13:00pm 開始通知 200 家供應商，以及 100 家企業客戶，告知明天的報紙會報導這個消息
- 13:00pm 決定擴大範圍，發簡訊給三個月內曾經購物的 70 萬會員。
- 15:00pm 聯合報，經濟日報，蘋果日報，自由時報記者來訪。

- 18:00pm 開始在首頁，結帳頁加註警語
- 21:00pm 在 PayEasy 首頁發表公開聲明書，詳細說明 PayEasy 受攻擊的過程，並向會員宣告受損範圍

PayEasy 擔心事件擴大，利用媒體跟自家網站採坦白溝通的策略，強化客戶、供應商、員工對公司的信心。對於供應商及廠商先行對可能不利消息消毒；對客戶方面，使客戶充分獲得消息，避免在資訊不對偶的劣勢下，受到詐騙。對員工方面宣示與歹徒對抗的決心，驅使內部同仁齊力面對危機。

三、危機爆發第二期

各個報章及電子媒體在十二日播出的報導十分負面，造成 PayEasy 會員恐慌以及台新高層關切。

- 9:00am
  - 早上蘋果，自由時報見報，標題聳動，台新長官來電關切，台新公關擔心會影響到台新。
  - 新聞媒體的不正確誇大的報導，已經造成會員的恐慌
- 9:30am 電子媒體，大愛，華視，台視 (非凡) ，民視要求採訪。
- 10:00am 提供查詢介面，讓會員進入會員中心，查詢其個人資料是否被歹徒比對成功。
- 12:00pm 午間新聞報導，標題以「PayEasy 資料外洩」做主標題，台新高層與公關再度來電關切。

十二月十三日，PayEasy 沒有因為記者的負面報導而退縮，持續地向歹徒開戰─開放歹徒詐騙回報專線、每日更新歹徒詐騙最新話術，從會員回報統計，可以發現詐騙電話驟減。PayEasy 會員沒有被「詐騙得逞」，達成「零詐騙」的奇蹟。而同業對於 PayEasy 這樣的表現沒有任何正面或支持的回應。

PayEasy 腹背受敵，業績掉落三成，不僅供應商關切，母公司台新金控亦感到憂心，在大家都在質疑是否應該繼續為了客戶的權益而繼續跟歹徒奮戰到底。就如同危機邊緣策略理論所提到的，在這雙方互相傷害風險不斷提升時，雙方一開始都互相直衝，隨兩輛車子距離越來越近時，雙方則會考量自己能承受的風險

大小以及對方可能的底限而將車子轉向。歹徒不斷地在測試 PayEasy 的底線，而 PayEasy 也不斷在正面對抗歹徒，不惜毀滅自己的聲譽登報紙、開記者會，就是為了與歹徒槓上，讓歹徒知道 PayEasy 是來真的。

2007 年 12 月 17 日詐騙集團再度攻擊，接獲 3 通客戶回報的詐騙案子。發覺可能來自於某宅配業者託運的訂單，該公司在 11 月底將配送單查詢系統關閉，與某電視購物比對，發現同時間配送的訂單均收到詐騙電話。PayEasy 動員全體員工打電話給這些客戶、補發簡訊，但持續有詐騙回報。歹徒連續兩天打了 3000 通電話，有 120 人向 PayEasy 回報接到詐騙電話。PayEasy 連夜製作 3000 封警示信函，於週五早上以限時專送寄出。PayEasy 與歹徒搶時間，要比歹徒搶先一步通知到客戶，以免客戶受到傷害。

四、危機善後期

PayEasy 為了不再讓詐騙集團再攻擊，決定採取較激烈的手段。透過派中間人傳話的方式，委託台灣警政退休官員，藉由特殊管道，向對方傳達「只要你不攻擊我，我就不在媒體上反擊」的承諾。就如同危機邊緣策略理論所說的，兩個人同在懸崖邊的時候，有溝通的管道是可以讓雙方都各退一步的。

其他同業截至十二月底受傷慘重，東森受騙人數 1200 人，估計有近一億元的損失，博客來、金石堂、MOMO 仍有零星詐騙，而 PayEasy 仍然保持「零詐騙」的成績 (刑事局 2008 年詐騙統計資料)。為了彌補先前受傷的聲譽，PayEasy 刊登報紙廣告──零詐騙奇蹟。並且致力修補媒體關係，尋求立委開公聽會，讓社會大眾瞭解詐騙集團在其他同業網站已經造成傷害，並配合刑事局警官刑事局犯罪預防科警務正，宣導防詐觀念。此外還參加經濟日報座談並上公視節目，做好媒體公關，改善社會觀感。

總結 PayEasy 的危機處理關鍵即是「跟詐騙集團搶時間」，在 PayEasy 發生被中國駭客鎖定比對會員帳號密碼的事件時，選擇第一時間公布 PayEasy 受駭情況，就是要跟詐騙集團搶時間，盡可能在第一時間提醒會員，並杜絕會員受騙上當的可能性，降低會員因資訊不對稱所產生的不利。

PayEasy 通知會員的電話與詐騙電話是同時進行的。能夠越早通知有高風險的會員，就越能降低受詐騙的可能性。因為歹徒嘗試比對的會員名單持續增加，PayEasy 決定要正面面對駭客集團的攻擊，對於難以用電話聯絡上的會員，更連夜製作警示信函，以限時專送寄出。這些都是為了在第一時間讓會員知情，讓詐騙手法無法得逞。

四、危機解決期

PayEasy 的主動出擊，達成了零詐騙的艱難目標。當詐騙集團取得正確資料的難度越高，為了快速牟利，就會轉向其他更容易取得資料的地方。PayEasy 希望主動分享防堵、檢核的經驗，透過同業的經驗分享與聯防，才能在現今這樣的局面下提高電子網站客戶資料的安全性。

下表 3.1 顯示從 2008 年至今，每月累計詐騙件數，PayEasy 在 2008 年的五月和六月總共有三件詐騙件數，但是事後都證實這三件都不是真正的詐騙案件，其中一件是刑事局登錄失誤，另外兩件是客戶誤報，因此 PayEasy 在 2007 年 12 月受詐騙集團攻擊後，可以說是維持零詐騙的紀錄。

下圖是根據表 3.1 中的詐騙件數所畫出的統計圖 3.3，可以發現詐騙集團的攻擊是有波段性的，主要攻擊 YAHOO 拍賣/購物中心和東森購物，MOMO 電視購物和博客來也有零星幾個案例，其中最近六月 MOMO 被攻擊較為頻繁，這對其他網路購物平台來說可以說是一項重大的警訊。

表 3.1 各大網路購物平台 2008 年及 2009 年詐騙案件統計

	PayEasy	YAHOO 拍賣/ 購物中心	東森購物	MOMO 電視購物	博客來	DHC	PCHOME	金石堂	誠品書店	露天拍賣
Jan-08	0	88	105	45	0	**0**	**0**	**40**	**0**	**0**
Feb-08	0	175	138	2	22	0	0	8	16	0
Mar-08	0	549	741	11	108	0	2	4	4	1
Apr-08	0	1114	945	5	10	76	0	0	0	3
May-08	1	1453	868	3	30	7	14	1	0	3
Jun-08	2	909	271	0	52	4	19	0	0	4
Jul-08	0	929	174	0	44	16	16	0	0	3
Aug-08	0	636	602	0	17	11	0	4	0	6
Sep-08	0	901	541	0	0	15	6	56	0	1
Oct-08	0	659	515	0	1	3	2	25	0	2
Nov-08	0	297	117	0	0	0	0	55	0	6
Dec-08	0	759	261	0	94	0	0	20	0	9
Jan-09	0	532	104	0	79	0	2	5	0	20
Feb-09	0	747	48	0	92	19	0	0	0	20
Mar-09	0	917	94	48	73	23	0	0	0	11
Apr-09	0	547	25	60	0	0	1	58	0	58
May-09	0	482	3	112	1	0	0	9	0	34
Jun-09	0	366	6	252	0	21	0	2	0	11

資料來源：2008、2009 年刑事局詐騙數量統計

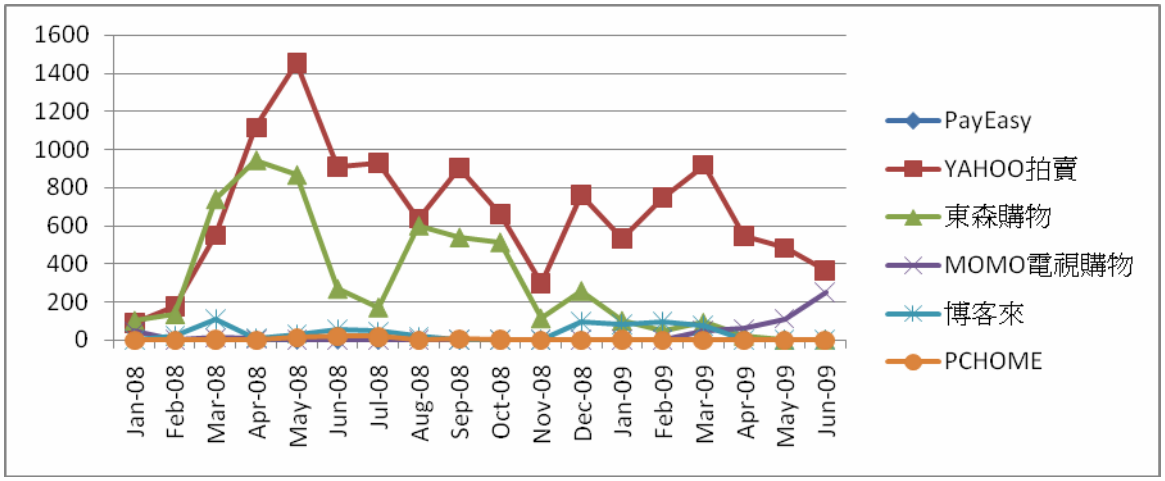


圖 3.3 各大網路購物平台詐騙案件統計圖

以下依事件發生順序，表列危機發生經過，及 PayEasy 應對策略。

表 3.2 危機潛伏期

時間	2007/12/09 之前
事件: 其他同業陸陸續續遭受詐騙集團的攻擊 YAHOO 奇摩拍賣 ● 處理帳號盜用案件比平日高出兩成 博客來網路書店 ● 詐騙集團利用木馬程式偵測使用者帳號密碼 **事件意義：** 詐騙集團開始蠢蠢欲動，同業紛紛遭受傷害，PayEasy 當時為訂單數最多的虛擬店鋪平台，因此也很有可能成為詐騙集團攻擊的目標。此階段為危機事件中的潛伏期。PayEasy 加設 Log 的機制，紀錄 IP。	

表 3.3　危機爆發第一期

<table>
<tr><td>時間</td><td>2007/12/09 20:00pm ~ 2007/12/10 10:00am</td></tr>
<tr><td colspan="2">事件: 來自大陸的 5 個可疑 IP 嘗試登入 PayEasy 網站。

登入資料共 39,000 筆,其中:
● 23,000(59%) 為非 PayEasy 會員
● 10,500(27%) 為 PayEasy 會員但密碼不符合
● 5,467(14%) 為 PayEasy 會員且密碼符合 (高風險)

事件意義：
此階段進入危機事件中的爆發期。詐騙集團攻上門來，針對這樣的情形，必須擬定一個適合的危機處理方式。</td></tr>
<tr><td>時間</td><td>2007/12/10 11:00am ~ 18:00pm</td></tr>
<tr><td colspan="2">事件: PayEasy 採取緊急應變措施。

PayEasy 應變措施:
<table>
<tr><th>對駭客</th><th>對檢警</th><th>對客戶</th><th>對上級</th></tr>
<tr><td>1. 封鎖攻擊的 5 個 IP。</td><td>1. 至刑事局偵九隊報案。</td><td>1. 凍結 5,467 個被比對成功的會員帳號，會員必須重新申請新密碼。</td><td>1. 呈報台新長官。並通報台新公關、IT 等相關部門。</td></tr>
<tr><td>2. 確認歹徒攻擊方法，清查受損害範圍。</td><td>2. 請求偵九協助預定於 12/11 與刑事局共同召開記者會。</td><td>2. 變更會員密碼並發簡訊給 39,000 名被比對過的會員。</td><td>2. 向台新董事長報告，董事長同意召開記者會。</td></tr>
</table>
事件意義：
此階段為危機爆發第一期。
PayEasy 在行動面上：
首先封鎖入侵 IP，控制受害範圍。並向檢警報案，希冀糾出幕後元兇。
PayEasy 在訊息面上：
警惕直接利益參與者發生的可能受到的損害：

● 將訊息告知上級以釐清對 PayEasy 危機處理的疑慮。
● 告知民眾以避免損害擴大至民眾的財產安全。</td></tr>
</table>

時間	2007/12/10 19:00pm

事件: 歹徒又上來測試會員帳戶。

PayEasy 應變措施:

開始封鎖來自中國所有的 IP，並派員整夜監測

事件意義：

企業已防堵在資訊安全上的威脅，避免損失持續擴大。

時間	2007/12/11

事件: PayEasy 召開記者會

事件參與者反應：

客戶：兩位會員回報接到詐騙電話，其中一名不在 5,467 名單中。

PayEasy 應變措施:

1. 對外公開訊息：	**2. 內部公開訊息：**
a. 媒體： 召開記者會，接受聯合報，經濟日報，蘋果日報，自由時報記者來訪。 **b. PayEasy 網頁:** ● 開始在首頁，結帳頁加註警語 ● 在 PayEasy 首頁發表公開聲明書，詳細說明 PayEasy 受攻擊的過程	**a. 對供應商及廠商：** 通知 200 家供應商，以及 100 家企業客戶，告知明天的報紙會報導這個消息 **b. 對客戶：** 發簡訊聲明稿給三個月內有登入 PayEasy 網站的 70 萬會員(12/12 開始發送)， 並向會員宣告受損範圍。 **c. 對員工：** 召集全公司同仁，說明事件發生經過，以及我決心與歹徒對抗

事件意義：

利用媒體跟自家網站採坦白溝通的策略，強化客戶、供應商、員工對公司的信心。

對供應商及廠商：先行對可能不利消息消毒。

對客戶：使客戶充分獲得消息，避免在資訊不對偶的劣勢下，受到詐騙。

對員工：宣示與歹徒對抗的決心，驅使內部同仁齊力面對危機。

表 3.4　危機爆發第二期

時間	2007/12/12
▪**事件:** 平面媒體以聳動標題報導這次駭客入侵事件。 **事件參與者反應：** 上級：台新上級來電關切事情發展，台新公關擔心會影響到台新。 客戶：新聞媒體的誇大報導，造成會員恐慌。 媒體: 電子媒體，大愛，華視，台視(非凡) ，民視要求採訪。 **應變措施:** ● 提供查詢介面，讓會員進入會員中心，查詢其個人資料是否被歹徒比對成功。 ● 發送第二封 PayEasy 聲明稿給全數 240 萬會員 ● 於蘋果、自由、經濟、中時刊登全版廣告「非駭客型詐騙攻擊」 **事件意義：** 此為危機爆發第二期，媒體誇張的報導等於是在 PayEasy 傷口上灑鹽，使上級跟客戶對公司的信心動搖。因此發出聲明稿及提供查詢介面，希冀客戶增進對公司的信心。	
時間	2007/12/13
事件: 悍衛會員的權益。 **應變措施:** ● 開放歹徒詐騙回報專線 ● 於網站上每日更新歹徒詐騙最新話術 **事件意義：** 建立起對稱的資訊流通管道，使直接攸關利益的參與者不會蒙受損失。	
時間	2007/12/17
事件: 詐騙死灰復燃 **事件參與者反應：** 客戶: 客戶回報收到 3 通詐騙電話 **應變措施:** **1. 調查發生原因:** ● 可能來自於某宅配業者託運的訂單 **2. 警示客戶:** ● 補發簡訊給客戶 ● 連續兩天打 3000 通電話警示客戶，其中有 120 人接到詐騙電話。 ● 連夜製作 3000 封警示信函，於週五早上以限時專送寄出。	

表 3.5　危機善後期

時間	2007/12/17~2008/1/15

事件: 委託台灣警政退休官員，藉由特殊管道向歹徒表達我們的決心、另一方面修補媒體關係

事件參與者反應：

上級：台新上級來電關切事情發展，台新公關擔心會影響到台新。

客戶：新聞媒體的誇大報導，造成會員恐慌。

媒體: 電子媒體，大愛，華視，台視(非凡) ，民視要求採訪。

應變措施:

- 向對岸詐騙集團傳達「只要你不攻擊我，我就不在媒體上反擊」
- 於四大報登全版廣告──零詐騙奇蹟
- 尋求立委開公聽會，讓社會大眾瞭解詐騙集團在其他同業網站已經造成傷害，而 PayEasy 卻沒有人遭受詐騙
- 刑事局召開記者會，公開國內八大網站均受詐騙集團攻擊，造成客戶的損失，公佈名單中沒有 PayEasy。

事件意義：

此階段步入危機善後期，爲進一步減短後遺症的發作期間，PayEasy 主動近一步的調查危機來自何處，並通知客戶以避免詐騙事件再度發生。更重要的是派中間人傳話，讓詐騙集團停止攻擊。修補與媒體之間的關係，讓公司形象更好，與媒體作互動及溝通，在發生事情時確保媒體做正確的報導。

表 3.6　危機解決期

時間	2008/1/16—迄今

事件: 詐騙事件不再發生，客戶信心也逐漸回籠

事件參與者反應：

客戶：建立信心

媒體：關係改善

- 於 2008/4/14 刊登全版報紙廣告—「廈門詐騙集團新攻勢」
- 參加經濟日報座談
- 上公視節目座談

PayEassy 內部

- 持續強化內部安控,取得 ISO27001 認證

事件意義：

PayEasy 採取開誠佈公並正面迎對歹徒的做法，使得除了少數客戶有接到詐騙電話外，達成「零詐騙」的成績。事件發生初期，雖然業績下降約三成，但此次危機處理得當，建立起客戶對 PayEasy 使得危機化為轉機。之後農曆年的業績比去年同期增長了 23%。

PayEasy 的危機生命周期可以總結於下圖

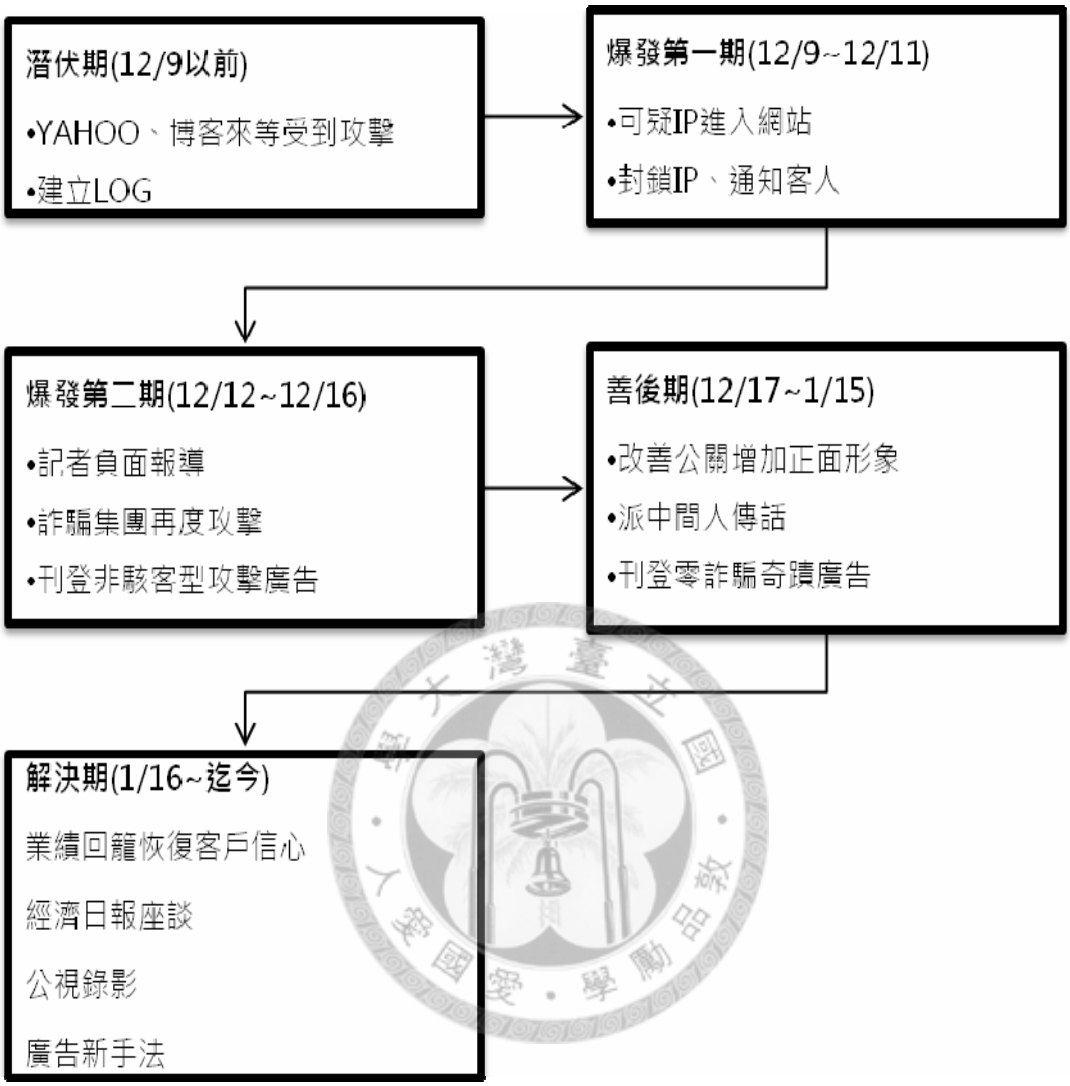


圖 3.4 PayEasy 危機生命週期

第三節、PayEasy 資安問題分析與處理方式

PayEasy 為一網路購物平台，透過網頁即可提供使用者便利的網路購物服務。但在帶給使用者便利的同時，開放的網路平台也容易成為網路犯罪的溫床。為了抵禦惡意侵入者的攻擊，必須先針對網站的資訊安全做出詳細審視，防堵可能的弱點，降低被侵害的風險。

一般網路購物平台的弱點可以依使用者分為網站經營端和用戶端，網站經營端的弱點可以包含網路危險、系統危險，內部人員危險、內部網路危險及關連網站危險。用戶端的弱點則端看各用戶的網路使用習慣與情形。為了建構安全的網路交易平台，PayEasy 於創立初期即積極做好資訊安全設施部署。

一、 實體安全

為了防止未經授權者直接接觸系統與設備，PayEasy 利用指紋辨識技術與 24 小時的錄影設備控制管理公司的 IT 監控室，並限制唯有 IT 監控室的電腦方能連接機房內的資料庫。因此當其他部門要取得客戶重要資料時，必須經過部門主管、資訊部主管及總經理的批准後，才可由資料庫管理員於 IT 監控室內存取資料。

二、資料分級

為了保護客戶資料對隱私予保密的要求，進而降低內部人員監守自盜或外部人員利用社交工程竊取資料的風險，PayEasy 對所有資料都有制定機密等級分類。為了確保資料的隱密性，所有的客戶資料都以 AES(Advanced Encryption Standard) 256 位元加密，確保未經授權的使用者無法瀏覽資料內容，進而落實權限管理。嚴密的權限控管可以避免公司不會遭受魚叉式攻擊：以員工電腦為跳板，侵入公司資料庫。

而根據每個使用者的存取權限，PayEasy 定義不同的行為規範。例如：客服人員的網段跟主要內部網路 (intranet) 有所區隔，隔離外在的可能入侵行為。另外，限制客服人員的電腦設備，使得客服人員無法以各種外接儲存媒介，將公司資料攜出公司外。而對第一手接觸 IT 設備的機房管理人員，則使用精簡客戶端機器，節省資訊安全的管理維護工作。

三、網路安全

為了確保在網路上的交易資訊會被有心人士攔截、修改，PayEasy 利用加密技術，加密網路上流通的資訊，增加資料被攔截、破解的難度。

四、系統安全

為了避免駭客於網站內植入惡意語法 (SQL injection、Script insertion)，PayEasy 將資訊系統構成四層，最底層是資料庫，上一層是 Java EJB（Enterprise Java Bean）中介層，任何應用程式的呼叫或執行，都必須透過 EJB，上一層是 Web 的前端應用程式，最上層則是 Web。透過 EJB 呼叫應用程式，使得駭客無法利用植入惡意與法的方式直接攻擊 PayEasy 的網路購物平台。

五、IP 紀錄

為了確認交易時的不可否認性(Non-repudiation)與確保不受到有心人士的攻擊，PayEasy 保存每位使用者的登入資訊，其中包含了登入時的 IP 位址。由於藏匿足跡並不容易，所以保留 IP 的紀錄 (Log) 可以有助於辨識威脅的來源。

六、PayEasy 資安弱點

雖然四個層面的安全部署使得 PayEasy 網路購物平台能抵禦大部分的威脅，但多半只能防禦小規模的攻擊與惡意探測。2007 年 12 月的攻擊事件，顯示 PayEasy 在面對集團式的攻擊時，看似堅不可破的資安系統還是存在弱點。

圖 3.5 PayEasy 網路購物流程圖

如圖 3.5，在 PayEasy 的購物流程中，第一步是使用者驗證(Authentication)，驗證過後的使用者得以自己在網路上的身分，選定欲購買商品，並完成刷卡購物等功能。在事件發生之前，如同多數的網路購物平台，PayEasy 在使用者身份驗證上，只需輸入使用者名稱跟密碼，便可以通過驗證，進行身分修改、訂單查詢、購物等動作。但是多數使用者在使用不同網路平台時，為了方便，習慣使用同一組的帳號與密碼。駭客便利用這個漏洞，在侵入其他購物平台，取得該使用者的各種資料後，透過大量嘗試或密碼拼圖法，猜出使用者帳號密碼重新將這些資料組合，於 PayEasy 平台上測試是否可以登入，並於侵入後，近一步取得客戶的資料，提供詐騙集團進行詐騙。

面對大規模的測試、侵入行為，PayEasy 既有的資安設施無法第一時間阻擋侵入。只得依靠登入的 Log 資訊，追蹤攻擊來源。因此在此波的攻擊之下，共 5,467 位客戶的資料受到入侵。

第四節 PayEasy 面對衝突對峙的賽局分析與資安對策

當發現 PayEasy 遭受駭客入侵後，PayEasy 管理階層必須決定以何種態度面對危機：

1. 迴避危機；選擇不公開購物平台被駭事件
2. 面對危機；開誠佈公向大眾說明被駭事件

由於個人隱私是購物族群最關心的事，所以平台的安全性，會影響到族群對平台的喜好。以往，多數購物平台選擇迴避危機，隱匿被駭事件，或將責任推委到其關聯廠商，以致顧客受駭時才發現購物平台擁有安全問題，引發顧客對購物平台的不信任感，反而會致使公司信譽受到更大的損害；但是如果開誠佈公向大眾說明被駭事件，沒有妥善處理危機，反而可能會引發更大的恐慌。若以賽局理論來分析一連串事件所應該做的決策，可以利用事件反應可能產生的預期報酬，來決定該採取何種策略。

我們先依不同的競賽角色區分賽局，並依賽局理論包含的三個元素：參與者、報酬以及策略；加以分析各個賽局。

一、 PayEasy 與客戶的賽局:

當 PayEasy 受到駭客攻擊時，因資安漏洞而外洩的資料會成為駭客進行詐騙時可以運用的資料，為了避免客戶因為不明個人資料外洩而受到詐騙，於是 PayEasy 必須提供顧客公司受駭的資訊，彌補顧客的資訊劣勢，避免受騙；而對於 PayEasy 而言，顧客對公司的信譽及品牌形象是公司最重要的資產，若顧客不相信 PayEasy 可以保護他們消費時的個人隱私，身處競爭激烈的購物市場中，PayEasy 即很快被淘汰。因此在此一賽局中，我們分別對三個元素做不同定義。

1. 參與者：

PayEasy、客戶

2. 報酬:

對 PayEasy 而言：公司的信譽，顧客對公司的信賴是這場賽局中的籌碼，根據 Suzanne Walters (1994)的論文，開發新顧客的成本是留住原本顧客的六倍，所以我們簡略定義失去顧客信賴所要付出的報酬為-6，贏得顧客的信賴為+1。

對客戶而言：我們將顧客被詐騙的報酬定為-1，顧客未被詐騙事件的報酬定為 0。

3. 策略：

首先將訊息傳遞跟決策反應的狀態表示成樹狀圖，從詐騙事件出發，假使公司充分警告顧客受駭事件，顧客將可以百分之百揭穿詐騙(損失為 0)，假使有 p %的人相信 PayEasy 對客戶資料的重視，因而使公司名譽上升(+1*p)，但告知消息的同時，也有可能造成顧客的恐慌，使得客戶選擇不相信公司，則公司的名譽損失為(-6* (1-p))。假設顧客因為公司未告知受駭事件而導致顧客權益受損，則顧客的損失可設為-1，公司則因名譽受損受到-6 分的罰分。

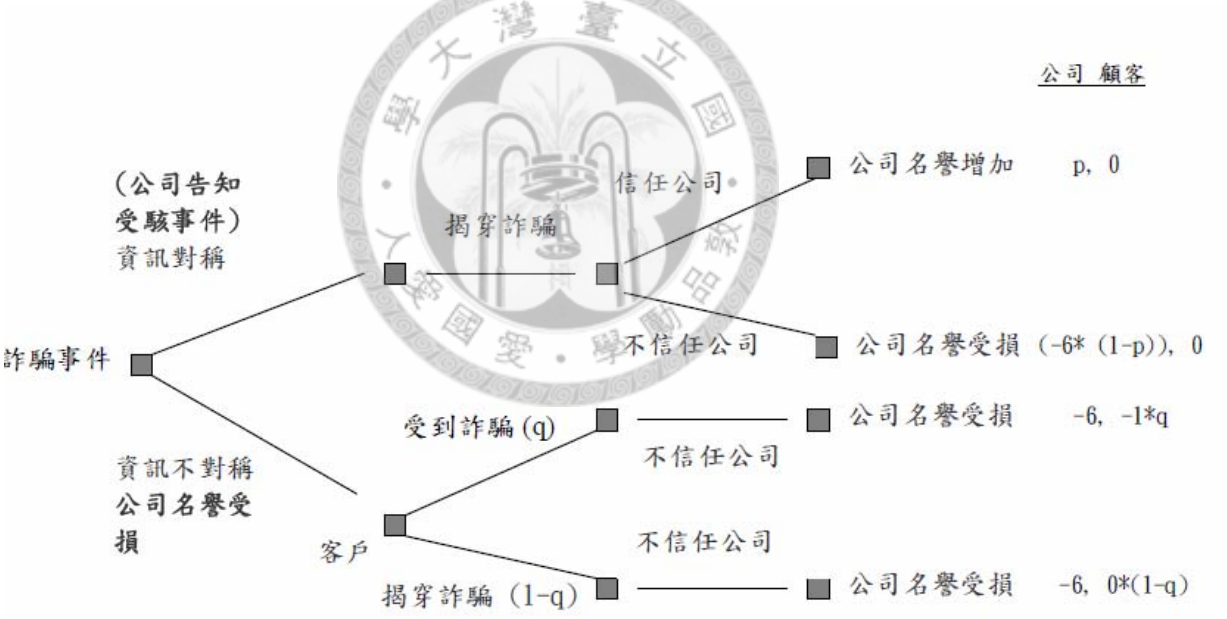


圖 3.6 是否告知顧客被駭事件的決策圖

如果 PayEasy 採取隱匿資訊，不通知客戶，PayEasy「信譽損失的期望值」為-6，顧客的損失為-q，均高於採行告知受駭事件的機率，因此採行主動告知的決策優於隱匿訊息。

當 PayEasy 採行主動告知，公司名譽提升的機率為何?

假設資訊對稱(顧客相信 PayEasy 是負責任的企業)的機率為 P，期望值大於零，則表示公司的名譽提升，因此-6*(1-p)+P>0, P>6/7=0.857。

因此 PayEasy 除了要主動告知顧客，還必須向社會大眾強力宣傳詐騙事件的猖狂以及 PayEasy 採行的措施與其他漠視消費者權益受損業者間的不同，當超過 85.7%的民眾了解事件的緣由時，PayEasy 的信譽才能因而提升。

綜合來看，雖然告知客戶跟不告知客戶都有可能使公司的信譽受損，不過選擇不告知時，會對公司信譽造成更大的損害；；因為只要 P 的機率大於零，其主動告知的期望報酬就會比不告知的報酬來的高

另外，當客戶收到公司提出的警訊後，便可以成功防治歹徒的詐騙，因而使客戶不會蒙受損失。站在保護客戶的立場來看，PayEasy 應該選擇將被駭資訊告訴客戶。

二、 PayEasy 與詐騙集團的賽局:

PayEasy 在 2007 年 12 月所面對的駭客集團，經過分析登陸檔 (Log) 檔後，研判是來自於大陸的集團，利用人工進行資料拼圖後，嘗試以該使用者名義登入購物平台。集團利用一般購物平台不敢散佈被駭訊息，以保全近利與聲譽的心態，並藉由兩岸法令限制的屏障，肆無忌憚的惡意侵入 PayEasy 平台。為了避免顧客財務有所損失，更要進一步的嚇阻駭客集團再三的攻擊。PayEasy 採用了賽局理論中的「懦夫賽局」來嚇阻駭客的侵襲。

1. 參與者：

PayEasy、駭客

2. 報酬:

對 PayEasy 而言，信譽跟營收為 PayEasy 在賽局中的籌碼。假設 PayEasy 信用破產的話，會獲得-10 分的罰分，若選擇公開受入侵的消息，則會獲得-2.5 分的罰分。而詐騙事件頻傳的話，將多給予-2.5 分的罰分。

對詐騙集團而言，詐騙成功為詐騙集團的獲利來源，當成功詐騙購物平台使用者時，獲得+10 的報酬，但如果受到阻礙，使得獲利時間拖長，報酬變成-5分。

3. 懦夫賽局策略:

假設在賽局中的 PayEasy 選擇冷處理駭客入侵事件，詐騙集團即會一而再再而三地攻擊 PayEasy 的網站，因此 PayEasy 的信譽掃地，獲得-10 分的罰分。而詐騙集團將可一直獲得利益，得到 10 分的報酬。而當 PayEasy 選擇開誠佈公，將公司被駭事件公諸於消費者時，消費者可能會因負面消息而選擇不使用 PayEasy，致使公司損失，PayEasy 獲得-2.5 分的罰分。由於詐騙集團相當注重回收報酬率(Return on investment)，當獲利時間拖長即不利詐騙團生存。而可能轉向其他購物平台使用者詐騙，因此當 PayEasy 積極應對詐騙集團時，報酬轉為負分。

		詐騙集團	
		轉向(懦夫)	直衝(勇士)
PayEasy	轉向(懦夫)	0,0	-10,10
	直衝(勇士)	-2.5,0	-5,-5

圖 3.7 PayEasy V.S. 詐騙集團報酬表

從表上所列的各種可能性來看，在不知道詐騙集團的可能動向前(假設轉向與直衝機率各為 50%)，PayEasy 正面與詐騙集團抗衡，所獲得的平均報酬率為(-5-2.5)/2 = -0.375，因為在這一個報酬表中，PayEasy 與詐騙集團都不可能轉向，所以 PayEasy 轉向的報酬率為-10 分。因此在此一賽局中，PayEasy 應該與詐騙集團正式抗衡。嚇阻詐騙集團，保護公司信譽與顧客的權益。

而 PayEasy 召開記者會，刊登報紙廣告，並積極的防堵歹徒攻擊，主動通知客戶，協助客戶抵禦詐騙集團的攻擊，採行懦夫賽局中其中一方做出絕對不讓步的承諾，逼使另一方轉向，讓詐騙集團相信，PayEasy 將採破釜沉舟的策略，絕不轉向，迫使詐騙集團轉向，避免損失。

		詐騙集團	
		轉向(懦夫)	直衝(勇士)
PayEasy	轉向(懦夫)	-5,0	-10,10
	直衝(勇士)	-2.5,0	-5,-5

圖 3.8 PayEasy V.S. 詐騙集團在加強承諾後報酬表

由於 PayEasy 與詐騙集團的賽局為一對多的賽局，當其他業者都採取轉向的策略時，詐騙集團也同樣設想 PayEasy 會採取轉向的策略，結果沒想到 PayEasy 選擇直衝，在詐騙集團可以選擇轉往攻擊其他業者時，詐騙集團便會選擇轉向。

4. 危機邊緣策略應用

懦夫賽局只考量賽局開始時候的對決，但這次的詐騙攻擊事件除了在 12/9 發動第一波攻勢，其後在 12/17 發動第二波攻擊，PayEasy 在當時是採行強硬手段決策下，應該壓迫詐騙集團的程度要超過多少程度，才能讓歹徒放棄攻擊？分析如下：

從圖 3.9 分析，如果 PayEasy 選擇轉向，詐騙集團則絕對採行直衝的策略，因此 PayEasy 必須在攻擊的第一時間，以直衝來代替防禦。

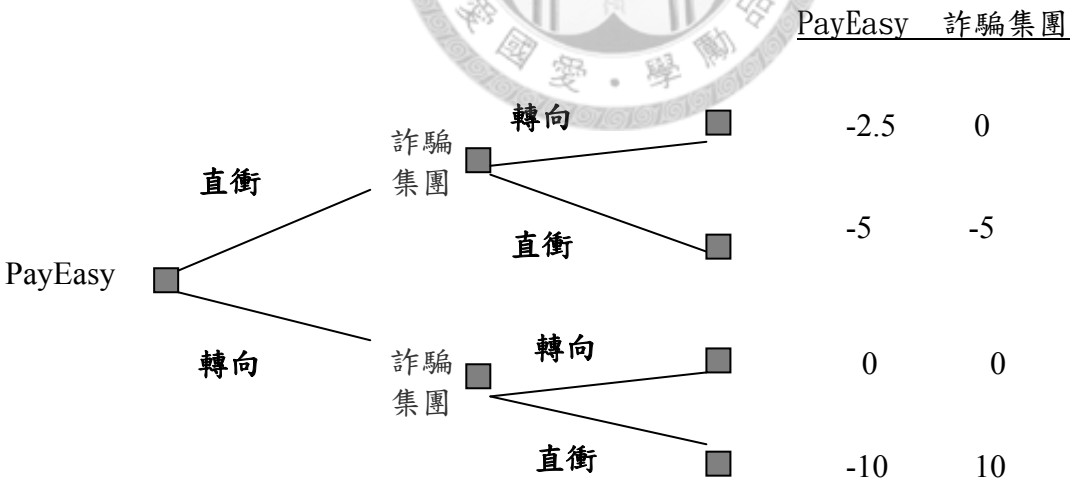


圖 3.9 PayEasy 採取強硬手段的賽局機率

當詐騙集團面臨 PayEasy 的抵禦下，接下來的策略會採行轉向或者是直衝，從詐騙集團的期望報酬來分析：

$-5q+10(1-q)>0$, $q<2/3=0.67$ ，代表 PayEasy 給詐騙集團的壓力要大於 0.67，讓詐騙集團相信 PayEasy 有 67%以上的機率會持續與他們對抗，因此傳達這個訊息必須明確且堅決，否則詐騙集團有可能持續的伺機進犯。

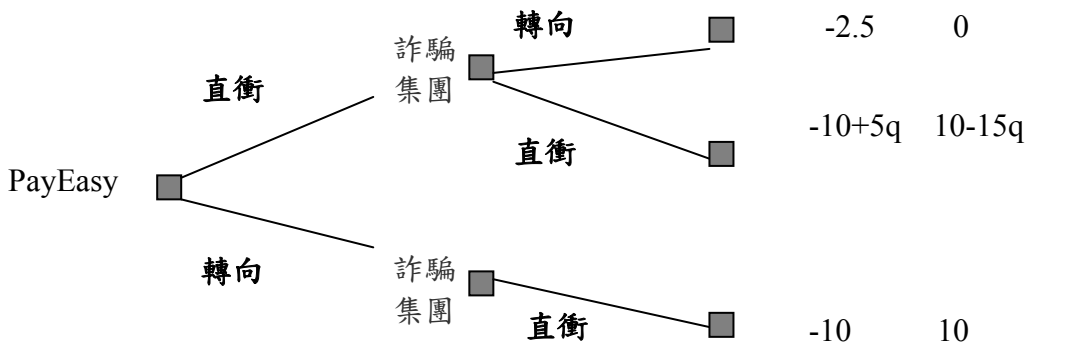


圖 3.10 PayEasy 採取強硬手段的決策樹

5. 面對危機時的資安對策:

PayEasy 在決定正面應對駭客的威脅後，公司於一個半小時內成立危機處理小組，針對威脅、弱點以及客戶權益做出第一時間的應對。公司的作法有：

1. 封鎖來自威脅來源的 IP
2. 停用被入侵的使用者帳號
3. 利用各種媒介向客戶宣告駭客入侵事件

顯示公司在危機處理時，不只是針對系統做出補救措施，更顯現 PayEasy 注重客戶權益的核心思想。

表 3.7　PayEasy 2007 年 12 月業績

日期	業績	說明
12/3—12/9	63,075,072	
12/10-12/16	57,979,081	(12/11 發生詐騙危機),相對於 12/3-12/9 衰退 8%
12/17-12/23	50,965,727	相對 12/3-12/9 衰退 19%
12/24-12/30	52,734,755	相對 12/3-12/9 衰退 16%

2007 年 12 月正值 Payeasy 週年慶，12 月的最後兩週是週年慶活動高潮，雖然相較於第一周業績只衰退 8%、19%、16%，就原先預算目標，最後兩週業績應該要比第一周高，業績可以達到 7000—7500 萬元。因此估算業績受到詐騙事件，Payeasy 採行公開手段，業績因此衰退 30%。但正面應對詐騙集團及開誠佈公的手法，創造良性循環，以致後來的營收逐漸起步回色。

為了避免相同的攻擊手法再次發生，在系統方面：PayEasy 在驗證使用者的部分加入驗證碼，避免程式自動測試登入，也增加了人工嘗試登入的時間。另外除了利用登錄檔追蹤來源，在管理連線狀態上，針對使用者連線過程的授權狀態的資訊、Cookie、網頁程式傳遞的資料進行保護，並透過限制使用者連線位置或數量，增加資安保護的強度。在管理方面，加強取得客戶資料申請的管控流程，限制可以取得客戶資料的使用者層級。

而在經歷此次攻擊後，PayEasy 為了提昇公司對資安風險的控管能力，因此開始規劃導入 ISO27001 認證，建立公司的資訊安全管理政策。為達成 ISO27001 所定義的安全管理要項：安全政策、安全組織、資產分類與控制、人員安全、實體與環境安全、電腦與網路管理、存取控制、系統開發與維護、業務持續管理、符合性。PayEasy 展開 ISM 管理審查會議，於辨認公司可資產後，分析未來可能碰到的威脅與內部的弱點。並開始運用 PDCA (Plan Do Check Act) 四個步驟循環，改進 PayEasy 的資訊安全管理，以期預防可能遭到的資安風險。

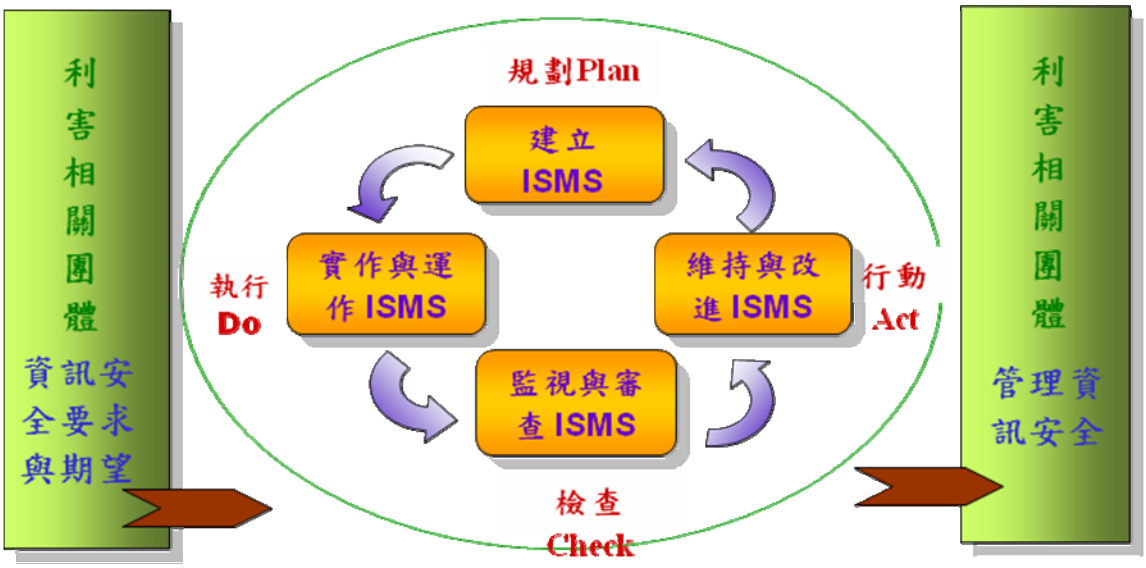


圖 3.11　PDCA 四循環流程圖

5.　PayEasy 及同業對資安的態度：

除了提昇公司的資安等級，積極管理資安可能產生的風險外，PayEasy 希冀同樣身為購物平台的同業，可以一同積極面對駭客所的威脅。在此利用合作賽局的模型說明為何購物平台為何需要聯手抵抗駭客。

二、 購物平台合作賽局

1. 參與者：

PayEasy、同業

2. 報酬:

對 PayEasy 及同業而言，信譽跟營收為在賽局中的籌碼。若公司信譽受損則獲得罰分-1 分，相對若客戶因為不相信該購物平台，而轉向其他平台時，則獲得顧客青睞的平台將獲得 1 分。

3. 策略:

假設 PayEasy 及同業皆選擇冷處理駭客入侵事件，消費者可能會不再信任該網路購物而使得兩家公司皆獲得-1 分的罰分；而當有公司正面向駭客宣戰，而其他保持漠視時，正面宣戰的平台將隨後受到廣大使用者的信賴，並使使用者轉移購物使用平台，使得正面處理危機的公司獲得+1 分，冷處理的公司獲得-1 分的罰分。但如果所有同業皆共同向駭客宣戰，使得購物平台不再成為網路

犯罪的溫床，則消費者將增加對購物平台的使用率，進而促進所有購物平台的業績皆有所增長，並可促使良性競爭，所有同業都獲得+1 分，創造共贏。

		同業	
		冷處理	積極處理危機
PayEasy	冷處理	-1,-1	-1,+1
	積極處理危機	+1,-1	+1,+1

圖 3.12　PayEasy V.S. 同業報酬表

理論上積極處理大家都可以雙贏 ，但是為何實際上大家卻不願意這樣做呢？原因有以下幾點：

1. 應該由市場佔有率前幾名的主要公司來整合才有其顯著效益，但由於它們早就已經深陷詐騙集團的苦海中，在被詐騙當時都沒有站出來，因此不可能推翻之前錯誤的決策。

2.　PayEasy 縱使有其影響力，但整合意願並不高，因為目前 PayEasy 在資安方面本身已經維持其安全性，就算有意願也會淪為強出頭，成為詐騙集團的首要目標。

3. 兩岸或許可以共同協商共同打擊犯罪，但是現階段大陸警方配合願意不高，不過隨著時間的推移，台灣民眾漸漸對詐騙集團資訊對稱，而詐騙集團也慢慢轉而向大陸人民詐騙，因此未來可能兩岸政府會積極合作，共同防治詐騙。

第四章 結論與建議

本研究採取個案分析的途徑，藉由文獻探討與公司內部人員訪談來進行資料蒐集及分析，以及刑事局統計資料分析，以達成研究目的並回答本文之研究問題：(一)深入了解個案的發展歷程與處理過程。(二)探討此個案在危機管理的「危機潛伏期」「危機爆發第一期」「危機爆發第二期」「危機善後期」「危機解決期」各個階段。(三)提供未來網路公司危機處理之建議。本章首先在第一節對研究結果作整合與歸納，第二節將說明對未來相關研究之建議，第三節則是本研究對於同業或是政府會有的貢獻。

第一節、研究結論

一、個案發展歷程

2007 年 12 月，PayEasy 第一次遭遇詐騙集團資料拼圖攻擊，IT 部門、客服部門、營運部門、公關部門和行銷部門大家並肩作戰，有人打電警告電話、有人在深夜幫忙摺信，更有人雙眼盯著 Log 資料徹夜值班。接著營運部主管林明芳帶全公司人員幫忙塞信、封口、貼地址，準備第二天一早寄出限時警告信，IT 更是震央，事發後 24 小時監視 Log，晚上也留了同仁徹夜值班。

透過經濟日報出面舉辦防詐騙座談會，總經理出席闡述理念與作法，後來成為福委會簡報時的利器。當時 PayEasy 與會員利用首頁保持對話，請客戶接獲詐騙電話立即回撥給客服，接著客服、行銷每天聯手更新歹徒最新話術，就掛在首頁連結上。

PayEasy 勇敢地站出來，小心翼翼地防範，沒有一位會員在這波詐騙狂潮中受到損失，但在民視消費高手電話行銷平台部份，卻出現 3 位客戶被詐，這部份雖然已不屬於 PayEasy 責任範圍，但 PayEasy 仍扛起責任，針對每位受詐者派員親自拜訪，並致贈慰問金。

PayEasy 還登了三波報紙廣告，告訴大家究竟發生了什麼事，也向往來廠商作過說明；在事發第一時間連夜發採訪通知，連夜做海報，初期媒體反應冷淡，但是在自由時報以聳動的標題報導刊出後，吸引各大電子媒體的追逐這則新聞，並以驚悚的誇大標題處理，PayEasy 遭到大眾的誤解與會員的不信任；這意味著 PayEasy 必須獨自扛起這整個事件，這個時候就是在考驗公司應該做什麼決定的

時候了，PayEasy 也可以「比照」其他的同業，對事件「冷處理」，但最後 PayEasy 做出一個勇敢的決定。但這樣的警告用在賽局理論中，卻是成為致勝的關鍵點，最開始是為了要提醒客戶小心防詐，但事實上也是向歹徒宣戰。

即使在詐騙新聞風聲鶴唳之際，仍有不少客人處之泰然，如常地上 PayEasy 購物，於是，當年度周年慶 PayEasy 以「你挺我、我回饋」為題，在 12 月底的最後兩週，針對在 PayEasy 購物的會員，提供購物消費金額的 3%，回饋會員 PayEasy 購物金，作為下次消費的折抵。

經歷過 2007 年底的詐騙集團攻擊事件，PayEasy 沒有因為歹徒沒有繼續在攻擊而停止改進的動力，在資訊系統上已取得 ISO27001 認證，面對這種危機也已形成一套因應流程，希望 PayEasy 的客人都能平安消費，一旦詐騙集團發動攻擊，PayEasy 將有能力對歹徒並保護所有會員的安全。

二、詐騙攻擊事件的危機處理階段

本研究參考 Fink（1986）的四階段論，將 PayEasy 的危機事件發生過程區分為危機潛伏期、危機爆發第一期、危機爆發第二期、危機善後期及危機解決期，在不同的時期都有相應的處理方式。

(一) 危機潛伏期

在危機潛伏期間，透過蒐集並偵測風吹草動，以分析並加強改善現有的系統，使預警系統更加準確，且提早警示；除了預警系統以外，透過防衛系統，提早知道事件會有的沙盤推演，使受傷的程度降低，並且在發生傷害時能快速釐清損害之處及損害的範圍。在詐騙集團開始蠢蠢欲動，同業紛紛遭受傷害的當時，PayEasy 透過強化軟體開發流程、用架構控管安全、用資安防護產品爭取時效、用權限來控管安全以及將使用者納入網站安全防護圈等方式，對於可能會出現的危機，採取積極的行動，改善資訊安全加強控管記錄 IP。

(二) 危機爆發期

當來自大陸的 5 個可疑 IP 嘗試登入 PayEasy 網站時，即進入危機爆發期，

在危機爆發的當下，當務之急就是要先採取必要措施將危機的傷害降到最低，PayEasy 對於客戶的安全維護最為重視，因此危機爆發時，PayEasy 的處理方式可以歸納為下列兩點：

1. 建立防火牆把損害限制在某個區域內，把進犯的 IP 鎖住，甚至在最後把大陸一億多的 IP 封住，目的為阻斷詐騙集團的攻勢。
2. 尋求決策的支持與正當性——與母公司台新金控溝通，支會供貨商，並且與員工討論。PayEasy 擔心事件擴大，透過與關係人溝通的方式，目的為了強化客戶、供應商、員工對公司的信心。

(二) 危機善後期

在危機善後期時，PayEasy 為了確保詐騙集團不再死灰復燃， PayEasy 管理階層決定面對危機——開誠佈公向大眾說明被駭事件。以往，多數購物平台選擇迴避危機，隱匿被駭事件，或將責任推委到其關聯廠商，如果開誠佈公向大眾說明被駭事件，沒有妥善處理危機，反而可能會引發更大的恐慌。因此本研究以賽局理論來分析一連串事件所應該做的決策。

在 PayEasy 與客戶的賽局方面，若顧客不相信 PayEasy 可以保護他們消費時的個人隱私，身處競爭激烈的購物市場中，PayEasy 即很快被淘汰，因此經由分析的結果，站在保護客戶的立場來看，PayEasy 應該選擇將被駭資訊告訴客戶。

在 PayEasy 與詐騙集團的賽局方面， PayEasy 採用了賽局理論中的「懦夫賽局」來嚇阻駭客的侵襲。在此一賽局中，PayEasy 應該與詐騙集團正式抗衡。嚇阻詐騙集團，保護公司信譽與顧客的權益。

在購物平台合作賽局中，如果所有同業皆共同向駭客宣戰，使得購物平台不再成為網路犯罪的溫床，則消費者將增加對購物平台的使用率，進而促進所有購物平台的業績皆有所增長，並可促使良性競爭，創造共贏。

(四) 危機解決期

為了避免相同的攻擊手法再次發生，PayEasy 採取以下的措施：

1. 在系統方面：PayEasy 在驗證使用者的部分加入驗證碼，避免程式自動測試登入，也增加了人工嘗試登入的時間。在管理連線狀態上，針對使用者連線過程的授權狀態的資訊、Cookie、網頁程式傳遞的資料

進行保護，並透過限制使用者連線位置或數量，增加資安保護的強度。

2. 在管理方面：加強取得客戶資料申請的管控流程，限制可以取得客戶資料的使用者層級。
3. 修補媒體關係與社會大眾觀感：尋求立委開公聽會，讓社會大眾瞭解詐騙集團在其他同業網站已經造成傷害，並配合刑事局警官刑事局犯罪預防科警務正，宣導防詐觀念。
4. 導入 ISO27001 認證：安全政策、安全組織、資產分類與控制、人員安全、實體與環境安全、電腦與網路管理、存取控制、系統開發與維護、業務持續管理、符合性。

下圖 4.1 總結出 PayEasy 危機處理的模式：

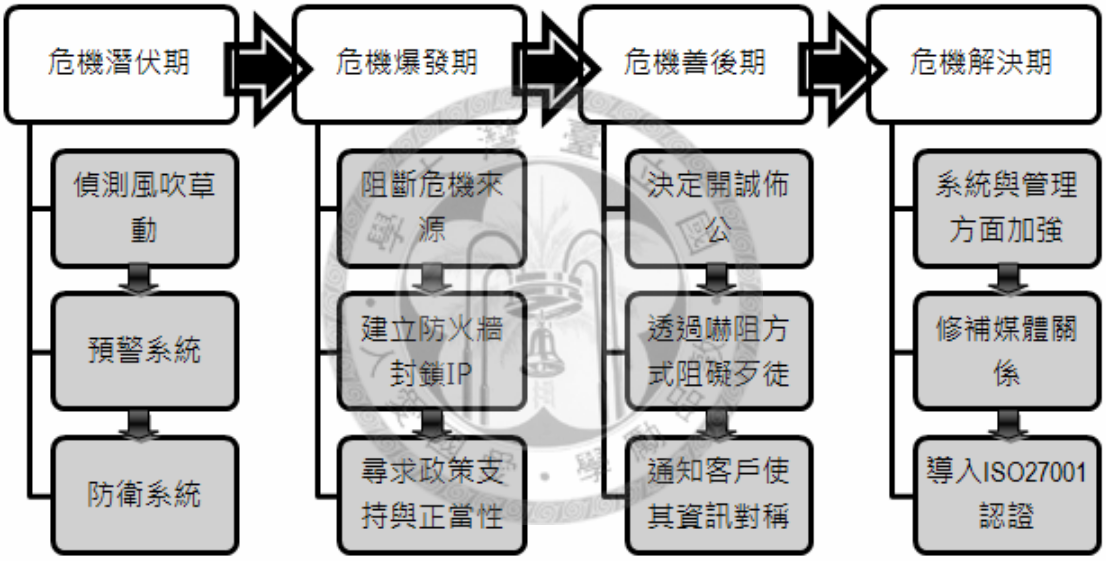


圖 4.1 PayEasy 危機處理模式

三、詐騙攻擊事件的價值判斷

在本次事件中，PayEasy 所有決策背後，其實一直都有一個信念在支持著，那就是本著顧客至上的良心。詐騙集團的猖獗，使得消費者在享受完購買商品的愉悅之後，仍得承受詐騙集團的騷擾甚至遭受詐騙，導致身心及財產受到威脅。而其他網路公司一直以來卻都採取消極的策略，導致詐騙集團更加食髓知味，因此 PayEasy 才會採取恫嚇歹徒的方式，使其退讓，並且告知社會大眾，使客戶在資訊對稱的狀態下，免除遭受詐騙的危機。

第二節、檢討與建議

本研究謹做如下之檢討與建議，提供企業界與學術界所參考運用。

(一) 雖然 PayEasy 成功有效嚇阻詐騙集團的攻擊，並確保會員的權益達到零詐騙的目標，但本事件爆發當時因媒體渲染對於 PayEasy 造成了傷害，讓母公司擔心、客戶失去信心，若是反應不要如此激烈，而改採取較溫和的方式來處理或許較不會有嚴重的形象受損。

(二) 對於企業而言，平日積極主動從事媒體關係營造，為的就是希望增加傳播媒體對企業的了解與彼此的信任關係。現代傳播科技發達，資訊流通快速，社會大眾都有知的權利，媒體總是扮演給予資訊傳遞的角色，常會影響大眾對企業形象的認知與評價，所以媒體的力量是不容忽視的。所謂「養兵千日，用在一時」，這些平時就與媒體保持良好互動關係的企業更期望：一旦企業遭遇危機事件時，媒體能夠在對於事件的報導手法與角度上，給予企業較為公正、甚至是正面的報導，而不致於發生過度渲染與偏頗的負面報導，導致社會大眾對事件的恐慌，對企業產生更多不利的影響。

(三) 企業危機管理是一種具有實用意涵的理論與架構，經過實務運用經驗的不斷驗證，才能獲取更大、更多的效益。本研究因受限於時間的因素，主要係採用質化研究途徑，期待往後有志研究本領域的學者，能再加入量化分析的方式，搭配理論推導，更能取得佐證的效果。

第三節、研究貢獻

由於許多公司對於詐騙集團的攻擊多半採用漠視態度，並沒有善盡責任告知客戶真實情形，以致於每年都有很多人遭受詐騙，而 PayEasy 透過賽局的危機處理方式，維持零詐騙的紀錄，或許這種決策過程可以作為參考，並提供給刑事局在打擊詐騙集團時的參考。本研究由於是針對危機生命周期中的「危機潛伏期」、「危機爆發第一期」、「危機爆發第二期」、「危機善後期」及「危機解決期」這五個階段中所採取的危機處理策略和對利益關係人管理，呈現出

一完整且深入的分析探討，在學術研究方面，可拓展國內對危機處理相關研究領域的深度與廣度。在企業實務方面，也可讓我們了解到購物平台危機處理的現況，更可藉由本研究的結果，提供給購物平台未來在危機處理方面之參考。

參考文獻

一、中文部分

1. 于鳳娟(譯)(2001)。Otto Lerbinger 著。危機管理。台北：五南。

2. 孔誠志等人（1998）。形象公關--實務操演手冊（初版）。台北：科技圖書。

3. 王美淑（1999）。企業危機處理個案研究。國立中山大學企業管理研究所碩士論文，全國博碩士論文摘要，088NSYS5121037。

4. 王紫薇（2004）。政府危機事件媒體溝通研究-以行政院環保署處理「阿瑪斯號貨油污事件」為例。國立政治大學新聞研究所碩士論文。全國博碩士論文摘要，092NCCU5383008。

5. 朱延智(2000)。危機處理的理論與實務。台北：幼獅。

6. 朱延智(2003)。企業危機管理。台北：五南。

7. 朱愛群(2002)。危機管理：解讀災難謎咒。台北：五南。

8. 余穎（1998）。地方政府消息來源與記者互動關係之研究－以三重市為例。世新大學教育學類研究所碩士論文，未出版，台北市。

9. 吳佩玲(譯)(2001)。Norman R.Autustine 等著。危機管理。台北：天下遠見。

10. 吳宜蓁（2002）。危機傳播－公共關係與語藝觀點的理論與實證。台北：五南。

11. 吳宜蓁、徐詠絜(譯)(1996)。Mitroff,I.I.and Pearson,C.M 著。危機管理診斷手冊。台北：五南。

12. 李順仁(2003)。資訊安全。台北：文魁。

13. 杜玟玲（2005）。災難新聞之新聞處理研究—以「南亞大海嘯」報導為例。

14. 杜秋菁 (2006)。企業危機事件與媒體報導之相關性研究。國立中山大學傳播管理研究所碩士論文。

15. 岸田明(2003) ，學資訊安全的第一本書。博碩。

16. 林文益、鄭安鳳(譯)(2003)。W.Timothy Commbs 著。危機傳播與溝通：計畫、管理與回應。台北：風雲論壇。

17. 邱毅（1999）。危機管理。台北：中華徵信所。

18. 徐漢章(譯)(1999)。瀧澤正雄著。企業危機管理：組織邁向安全經營的法則。台北：高寶國際。

19. 高大宇、王旭正、資訊密碼暨建構實驗室著（2003）。資訊安全。博碩文化。

20. 張意唐、李中宇（2006）。兩岸電訊戰－「地下基地台」詐騙案偵辦紀實。刑事雙月刊，第 12 期，頁 28-32。

21. 陳永鎮（2008） 。新興詐欺犯罪特性及運作模式之探討。刑事雙月刊，第 22 期 ，頁 50-55。

22. 喻靖媛（1994）。記者與消息來源互動關係及新聞處理方式關聯性研究。政治大學新聞研究所碩士論文。全國博碩士論文摘要，083NCCU0382011。

23. 游育蓁(1999)。危機管理不二法門。管理雜誌，301，52-73。

24. 詹中原(2004)。危機管理：理論架構。台北：聯經。

25. 劉幼俐（1998）。電視媒體報報導犯罪新聞的法律與倫理（中）。新聞鏡周刊，503， 4 6 -51。

26. 賴富山（2003）。地方記者人際傳播之研究-以台中縣黨政路線記者為例。世新大學傳播研究所碩士論文。全國博碩士論文摘要，091SHU00376035。

27. 韓應寧(譯)(1987)。Steven Fink 著。危機管理。台北：天下文化。

二、英文部分

1. Booth S.A, Crisis Management Strategy, London: J.J Press Ltd, 1993. pp86-88.
2. FBI/CIS. CSI Computer Crime & Security Survey, 2007.
3. Gonzalez-Herrero, A.,& Pratt, C. B. how to manage a crisis before—or whenever—it hits. Public Relations Quarterly, 40 (1), 1995. 25-29.
4. Graham T. Allison, Essnece of Decision: Explaining the Cuban Missile Crisis, Longman, New York, 1999.
5. ISF. The standard of good practice for information security. Technical report, Information Security Forum, 2005.
6. NIST (National Institute of Technical Standards), An introduction to computer security: the NIST handbook, Special Publication 800-12, 1995.
7. OECD,"OECD Guidelines for the Security of Information Systems ,Information Security Objective. 2001
8. Steven ,FinkCrisis Management: Planning for the Invisible, NewYork: American Management Association, 1986. P15.
9. Symantec, Symantec Report on the Underground Economy July 07–June 08 Published November 2008.

附錄

附錄 1 網路駭客攻擊

網路駭客會透過社交工程偵測大型電腦系統漏洞、網路監看、假造網址、散佈木馬等方式以大量蒐集資料。蒐集完資料後再來攻擊大型購物平台，以合法入侵，目的是為了取得 Trigger Data。

軟體開發人員並不想設計不安全的程式。舉例來說，一般作業系統通常都耗費數萬小時的時間，由數百萬行的程式碼所組成。一個簡單的小錯誤或是疏失，就可能在原本很安全的系統裡意外開出一個後門。攻擊者不停地想利用程式弱點，開發者則不停地想修補弱點，這是一場無止盡的對抗。就像鎖匠和小偷，或警報器製造商和偷車賊的關係一樣。這也就是軟體開發廠商發行更新程式修補已知弱點的原因，也是需要安裝這些更新的理由。駭客入侵攻擊事件，隨著資訊化的影響而與日俱增。每天在世界上各地，多少都會有部分系統、伺服器成為駭客的攻擊目標。而攻擊手法也日新月異，防不勝防。以下簡單介紹幾種常見的攻擊型態（王旭正、高大宇）：

1. 阻絕服務(Denial of Service):

   利用通訊網路協定的缺點，傳送大量封包使系統負荷過重，令主機提供的服務無法運作、發生錯誤，甚至癱瘓整個系統，使整個系統當機。利用多台殭屍電腦同時進行惡意阻斷式服務攻擊(DDoS)以癱瘓網站並勒索公司或企業。

2. 網址假造：

   入侵者假造錯誤、不存在或被授權的網址(使用者)，已進行攻擊作為或規避系統管理者及執法機關的查緝，並利用兩主機信賴的漏洞，送出其他電腦的特徵或網址，達到假扮另一台電腦的目的。例如有名的 paypal.com 就曾經被偽裝成 paypa1.com 變成數字的『1』，或 host 中用數字的「0」替換，如果警覺性不高或未仔細察看，則不容易發覺。也有利用 URL 網址使用上的技

巧，來矇騙受害者，例如：

http://www.hinet.net:index.cfmThfz@fake.com.tw/?sessTGTS，這樣的連結內容是合法的表示，看起來是聯結到中華電信網頁，而實際上則會連結到fake.com.tw。

3. 社交工程：

以影響力或說服力來欺騙他人以獲得有用的資訊，這是近年來造成企業或個人極大威脅和損失的駭客攻擊手法。社交工程造成極大威脅的原因，在於惡意人士不需要具備頂尖的電腦專業技術，只要企業員工對於防範詐騙沒有足夠的認知，就可以輕易地避過了企業的軟硬體安全防護，而騙取到各項帳號密碼、個人資料、財務資料或公司重要資料等資訊，對企業所造成的損害與威脅，完全不下於網路上的各種駭客攻擊。

4. 木馬程式：

一種遠端管理工具(軟體)，駭客利用電腦輾轉植入被害人電腦，被植入木馬程式的電腦會將內部資料向外傳輸，駭客也可在遠端遙控中毒電腦。

5. 系統漏洞：

電腦系統程式設計或維護時所留下的錯誤或私人秘道。

6. 緩衝區溢位：

強制寫入超過原先緩衝區大小的資料，已達成執行錯誤指令的效果。

造成指令錯誤系統當機

以往，有能力撰寫病毒或破解網路系統的人惟有少數人，但隨著論壇以及破解程式、方法充斥於網路，現今有能力駭進系統的人也隨之增加。如何鎖定犯罪對象並擬定抵禦策略也越來越困難。

為抵禦駭客及詐騙集團的聯手威脅，企業用戶必須肩負起保護使用者資料的任務，加強網路安全設備，以避免信用卡資料或個人資料外流。除保護公司本身的權益，也保護個人使用者權益。

附錄 2　事件未爆發前，2007/11/22 發現博客來遭受攻擊，要求同仁提升 IT 的防護措施，預言 PayEasy 將是下一個攻擊目標的內部 email。

RE: 今日緊急應變會議新功能上線

寄件者：[redacted]
收件者：[redacted]，主管通訊，客戶服務部　行銷部
日期：2007 年 11 月 24 日 - 0:49

[redacted]:請注意客戶的反應.

並注意是否有客戶來電表示未修改資料,但收到資料修改訊息.

[redacted].

對於客戶資料修改的動作要有 log 紀錄 IP 位址.

[redacted],資料加密的 key 是否需要變更,長度是否加長.

還有提高弱點偵測的頻率…

各位:請留意,尤其是 IT..我直覺從 Yahoo 的 email 入侵,博客來..接下來歹徒的對象轉向我們.

試想,如果博客來如真的被入侵,歹徒擁有近百萬筆的 ID, name, password, email, phone no, address, and spending records.. 接下來應該會測試其他知名網站.

Payeasy 或許會是下一個目標.提醒您如果您再各網站習慣留同樣 password…趕快去修改.

我有不祥的預感,希望不會發生.

From: [redacted]

Sent: Friday, November 23, 2007 6:25 PM

To: 主管通訊; 客戶服務部; 行銷部

Subject: 今日緊急應變會議新功能上線

Dear All,

有關今日緊急應變會議新功能已全部上線 !

包括 :

1. 會員中心新增強化防止詐騙的警語
2. AutoMail 訂單內容及取貨資訊移除
3. 會員異動密碼 or 手機 or E-mail 發簡訊提醒

Regards,

[redacted]

附錄 3 第一封新聞稿

新聞稿

網路犯罪新手法─資料拼圖　2007.12.10

敬請發佈

網路購物業者康迅數位整合股份有限公司（PayEasy.com）資管人員 12 月 10 日（一）發現，該公司網站在 9 日晚間遭中國大陸及香港等特定網段（IP）異常大量登入，經研判，極可能是網路犯罪集團的偵測行為，為保護會員權益，PayEasy 資管人員在 10 日上午 10 點，已全面封鎖相關 IP 及其所屬網段之連線，同時對於有個資外流風險之會員，已凍結其帳號及密碼，並呼籲消費者提高警覺。

除了已向警政署刑事警察局報案之外，PayEasy 決定公開這個事件，雖然這可能造成恐慌，過程也相當痛苦，但身為網路犯罪的受害者，PayEasy 認為，這已經是全產業、全社會的問題，即使可能動搖網路購物信心，我們仍必須站出來將這個經驗公開出來提醒消費者，因為 PayEasy 不希望任何一名無辜消費者因此蒙受損失。

近月以來，網路犯罪集團陸續挑戰各網路與電視購物同業，部份客戶資料被用來遂行詐騙，PayEasy 研判，上述大量登入行為，可能是犯罪集團在蒐尋可能的作案機會。

進一步分析犯罪集團的犯罪手法，是以大量資料，包括個人資料如身份證字號、電話、地址、出生年月日等，以及網站登入資料，例如帳號、密碼、交易紀錄等，就好像在進行一種「資料拼圖」，目的是拼湊成足以詐騙消費者的「有用訊息」。

詐騙成功之道在於取信被害人，網路犯罪集團事前從四面八方已取得大量個人資料，這次挑上 PayEasy 並大量登入，其實是在找出那些確實是 PayEasy 會員。

截至封鎖特定 IP 之前，這些可疑 IP 共利用 3 萬 9000 筆事前非法取得的帳號與密碼，企圖登入 PayEasy 網站，其中 59%並非 PayEasy 會員；27%會員帳號正確，但密碼錯誤；對於近 14%約 5400 筆被測試得逞的會員帳號，PayEasy 已在第一時間內，先凍結這 5400 筆帳號的交易功能，同時以簡訊、電子郵件緊急通知這 5400 筆帳號、密碼的擁有者，請其立即更改密碼，即可恢復正常交易，並提醒這些會員，後續若有任何自稱 PayEasy 客服人員要求轉帳或提供個人資

料，請提高警覺。

在確實告知消費者之後，10 日下午 4 點 PayEasy 已派員向警政署刑事警察局主動報案，並提供包括可疑 IP 位址、歹徒曾嘗試登入之帳號、密碼等必要資料，供警方調查。

研判歹徒下一步將是利用這組正確的帳號及密碼，上網查詢交易資料，然後再將這塊失落的資料「拼圖」（交易資料）填滿，使歹徒更能假扮成 PayEasy 客服人員，在詐騙電話中，成功說出能夠取信於潛在被害人的完整的詐騙話術。

舉例來說，PayEasy 曾接獲一名會員投訴，這名會員只在 PayEasy 消費過 1 次，且交貨方式是超商取貨，也就是「貨到付款」，從未在 PayEasy 使用信用卡付款，但犯罪集團卻在詐騙電話中，卻能準確說出被害人信用卡號，來核對被害人身份。

鑑於同業陸續傳出客戶個資外洩給予犯罪集團可乘之機，PayEasy 早在 10 月份已發給所有會員一封「資訊安全通知函」，請消費在接獲自稱「PayEasy 客服人員」來電時，立即回撥 0800023008 的客服電話確認」；並在 11 月直接在會員中心網頁上，加註「PayEasy 不會主動要求會員更改結帳方式或提供個人資料，若接到類似訊息，請拒絕回應並與 0800023008 客服電話查詢」。

在發現最近這件惡意登入事件後，我們更在全站掛上警語，請會員隨時更改登入密碼，並附上刑事局防詐騙 165 專線電話。

PayEasy 呼籲消費者，請立即上網更改在網站上的密碼，不要讓最後這塊「拼圖」拱手讓給犯罪集團，另一方面也請消費者認知一件事：

詐騙行為之所以發生損失，關鍵都在操作 ATM 或甚至臨櫃進行提款、轉帳，呼籲消費者在接獲自稱某網購業者客服電話，並要求提供存款餘額、要求轉帳時，請千萬先打刑事局 165 防詐騙專線，務必確認再確認。

新聞連絡人：

PayEasy 公共事務推展部　陳中興

附錄 4 開放在會員登入首頁，讓會員了解自身的風險程度

RE: 會員中心登入首頁的訊息新增

日期：2007 年 12 月 11 日 - 13:41

請 [redacted] 當記者會後,把我們的新聞稿放上網，當 [redacted] 完成查詢機制後,把連結放上去,讓客戶自己進入會員中心查詢.

陳述重點.

1.本次歹徒「資料拼圖」的犯罪過程中，截至目前我們掌握資料顯示，您的帳戶並未被遭受歹徒「資料拼圖」，但爲安全起見，強烈建議立即變更您經常使用各網站登錄密碼。

2. 本次歹徒「資料拼圖」的犯罪過程中，就我們掌握資料顯示，您的帳戶曾遭受歹徒「資料拼圖」，但密碼不正確，被我們的系統成功攔阻，請留意歹徒的詐騙電話，爲安全起見，強烈建議立即變更您經常使用各網站登錄密碼。

3. 本次歹徒「資料拼圖」的犯罪過程中，就我們掌握資料顯示，您的帳戶曾遭受歹徒「資料拼圖」，且密碼完全符合，請留意歹徒的詐騙電話，強烈建議立即變更您經常使用各網站登錄密碼，如有接獲歹徒詐騙電話，請速與我們連絡 0800023008,02-33169019 或 165 防詐騙專線連絡。

請在網站上面說明何爲「資料拼圖」以及防範的方法.

[redacted]

附錄 5　2007/12/11 晚上掛在 PayEasy 首頁的聲明稿

◎PayEasy 資訊安全聲明稿◎

各位敬愛的 PayEasy 會員：

各位敬愛的 PayEasy 會員，近月以來國內各大購物網站、電視購物業者頻傳所謂「個資外洩」事件，我們是最安全的購物網站，在 PayEasy 重重把關下，我們再次確認會員資料庫安全無虞，但請注意一種新型態網路犯罪手法—「資料拼圖」正在醞釀中，**請儘快上 PayEasy 會員中心更改密碼以策安全**。

我們很明白公告此事可能影響您的消費信心，但我們不管別人怎麼做，我們仍決定不計代價要讓您了解這個事實，甚至動用媒體力量，因爲我們正在和歹徒搶時間，要在歹徒採取進一步行動之前，讓我們的消費者有所防備。

最近一兩個月以來，疑似有新的詐騙集團利用外界四處流竄的大量個人資料，逐步拼湊成足以詐騙消費者的「有用訊息」，預作詐騙之用，目前我們所發現的犯罪手法是：

歹徒利用到處蒐集而來的會員帳號與密碼，不斷以人工登入方式，測試每一組帳號與密碼所歸屬的網站，就像拿著幾萬把「鑰匙」來開我們的門，要讓歹徒的鑰匙無效，最簡單的方法就是換一副「鎖頭」，這裡的「鎖頭」就是的您的密碼，只要經常更換密碼，您就沒有風險。

PayEasy 的資管人員 12 月 10 日（一）發現，我們的網站在 9 日晚間出現特定 IP 位址大量登入本站，經研判極可能是網路犯罪集團的偵測行爲。爲保護會員的安全與權益，PayEasy 資管人員在 10 日上午 10 點，已全面封鎖這些可疑 IP 之連線，我們同時也凍結部份有個資外流風險之會員帳號及密碼；很抱歉，爲了維護您的交易安全，我們不得不作此處置。

如果您發現鍵入正確帳號、密碼，仍無法登入本站時，請主動上 PayEasy 網站操作更改密碼手續，或來電客服電話 0800-023-008 或 02-33169019，經客服人員確認身份後，我們會補寄密碼函到您的 E-mail 信箱，再請您重新登入即可繼續購物。

如果您想了解您的帳號與密碼是否有外流風險，**請您在 12 月 12 日上午 10 點以後，上 PayEasy 網站，登入會員中心，我們將會告訴您是否有必要更改密碼。**

我們建議您在不同網站使用不同的帳號及密碼，並且強烈建議您儘速修改您

經常瀏覽的網站密碼，不要讓歹徒輕易比對出您所登錄的網站，即可避免詐騙集團的騷擾。

萬一您仍接到自稱 PayEasy 客服人員的電話，且要求您操作 ATM 或要求您透露您的存款餘額，我們提醒您，PayEasy 不會主動要求會員更改結帳方式或提供個人資料，更不會要求您去操作 ATM，若接到類似訊息，請拒絕回應並與 0800-023-008 或 02-33169019 客服電話連絡，或直接撥打**刑事局防詐騙 165 專線**電話查詢。

我們除了已向警政署刑事警察局報案之外，PayEasy 已由資管人員執行 24 小時全天侯即時監控，我們會拒絕可疑的不法登入，以保護所有 240 萬會員的安全。

最後，PayEasy 祝您天天平安喜樂

PayEasy 康迅數位整合股份有限公司
總經理 林坤正　敬上

最後提醒：**詐騙行爲之所以發生損失，關鍵都在操作 ATM 或甚至臨櫃進行提款、轉帳，呼籲消費者在接獲自稱某網購業者客服電話，並要求提供存款餘額、要求轉帳時，千萬不要照做，請撥先打刑事局 165 防詐騙專線，或直接去電網購業者，務必確認再確認。**

附錄 6　緊急發送 70 萬則簡訊通之會員

From: [redacted]

Sent: Wednesday, December 12, 2007 10:05 AM

To: [redacted]

Subject: 緊急任務， 即刻發送 - PayEasy 聲明稿_第一批

Dear [redacted],

如剛電話中說明，今日須緊急發送 70 萬通簡訊，

請協助緊急調度，希望今日(12/12) 21:00 前能全數發送完畢。

先給你第一批名單，共計: 109,882 筆

簡訊文案:

PayEasy 提醒您：絕不以任何理由要求會員至 ATM 做帳務修改，防止新型網路詐騙「資料拼圖」，請定期變更密碼，詳情請上 Payeasy.com

附錄 7 媒體的負面報導

PayEasy 個資外洩 5400 會員遭殃

分類：關乎專業新聞

PayEasy 個資外洩 5400 會員遭殃

公共電視 更新日期: 2007/12/12 22:10

最近接二連三發生個人資料外洩事件，在柏克來書店、東森購物台之後、有 200 萬會員的知名購物網站 PAYEASY、也傳出有 5400 筆會員資料外流！PAYEASY 發現狀況後、已經緊急通知會員不要受騙。法務部則打算要祭出重罰、未來如果再發生消費者資料外洩、每一筆最高要罰兩萬元！

20 多線客服人員，全都忙得不可開交，因爲 PAYEASY 傳出 5400 筆客戶個人資料外洩，擔心的客戶電話不斷打進來，就怕自己也被詐騙集團給鎖定！

PAYEASY 不斷強調，14%的客戶資料外洩，絕對不是出自網站內部，而是不肖人士從別的管道得到，而個人資料外洩，這也不是第一起，日前東森購物也傳出客戶資料外流，但到現在都沒有答案，柏克萊網路書店也傳出遭侵入，消費者的購物安全，亮起紅燈，法務部將祭出重罰，未來每筆資料，最高可罰兩萬元！

只是?法進度緩慢，在這段法律空窗期，消費者除了趕快變更密碼，保障自身權益外，接獲任何自稱「客服」或銀行的電話都不要輕易相信，更不要任意前往銀行轉帳，若要查證，可撥打 165 反詐騙專線。

2. PayEasy 5467 筆個資 詐騙集團一夜比對成功

新聞來源:

聯合晚報

電視網路購物詐騙，從今年 11 月開始，位居詐騙手法第一名，面對詐騙案件一再發生，網路交易安全性產生質疑，警方調查發現，各大購物網站資料遭駭客入侵，以「資料拼圖」方式，從中竊取民眾資料。(記者劉星君/台北報導)

警方指出，網路詐騙手法是「千騙、萬騙、不離 ATM」，各大購物網站或網路賣家，不會主動要求民眾操作 ATM，民眾應保持警覺，並常換密碼。

警方在本月 9 日接獲國內 PayEasy 購物網站報案，發現 PayEasy 購物網站在本月 9 日晚間，該公司資料庫有異常登入現象，共攔截到 3 萬 9000 多筆來自數個特定 IP 的帳號、密碼。歹徒以「資料拼圖」方式，

將搜集而來的會員帳號、密碼，不斷以人工登入方式，企圖測試每一組帳號與密碼歸屬的網站。警方發現，其 IP 位址在中國大陸福建省福州的電信局，並且以每 3.5 秒的速度，測試會員帳號、密碼。

警方估計，當天晚間 PayEasy 有 14%的會員資料遭到比對成功，預估其個人資料比對成功達 5467 人。警方表示，詐騙集可能先前就以取得會員的帳號密碼資料，現階段鎖定 PayEasy 購物網，從中再嘗試獲得其他的帳號密碼資料。

警方說，網路購物詐騙的模式，其數量不是很多，但是網路的平台增多，再從中竊取消費者資料。

警方呼籲民眾，平常在購買手機、辦保險、辦信用卡等，其個人資料都容易流出去，在登入各大入口網站時，要經常更換密碼。

3. 2007/12/12 自由時報報導

PayEasy受「駭」 5400會員個資外洩

自由時報 更新日期：2007/12/12 04:09

今開放會員查詢帳號是否被竊

〔記者王珮華／台北報導〕國內第三大購物網站PayEasy昨呼籲使用者盡快更換密碼。該網站表示，上週日晚間遭來自中國的不明人士，以身分證字號輸入會員帳號測試密碼達三萬九千多次，其中有五千四百筆資料帳號密碼正確被登入，隔天有十三位會員反應接到詐騙集團電話，PayEasy認為該事件非單一個案，極可能延燒到國內其他網站。PayEasy指出，今天上午十點起將開放會員查詢，其帳號密碼是否在此事件中被詐騙集團掌握。

已凍結遭竊帳號 寄發新密碼

針對被成功登入的五千四百個帳號，PayEasy已立即凍結帳號，無論是歹徒或使用者都無法登入，同時發出簡訊與e-mail給帳號所有人，並寄發新密碼。

附錄 8　PayEasy 遭「非駭客型」攻擊說明，於四大報全版刊登

PAYEASY 時尚 Shopping 一點子

PayEasy遭「非駭客型」攻擊說明

籲請全民立即上網更改不重複之全新密碼

非駭客型攻擊

12月9日週拜天晚間8點起，PayEasy網站遭受來自中國大陸的數個特定網址，以來路不明、且以非法手段取得的大量帳號密碼，企圖透過合法登入手段，一筆一筆登入Payeasy會員中心，這種犯案模式堪稱「非駭客型」資料比對攻擊。

很多網友為求方便好記，習慣在不同網站使用相同密碼，但是，當歹徒掌握第一批個人資料之後，他們就可以「順藤摸瓜」般拿去測試每個網站，如果您在網路上的帳號密碼都用同一組，則個資外洩的風險會提高好幾倍；對網路業者而言，彼此會員很可能重複，再加上很多會員使用同一組密碼遊走各站，則**「一家失火，殃及四鄰」就不足為奇了**。

歹徒對PayEasy的攻擊行動中，有59%登入帳號並非PayEasy會員所有，有27%登入帳號確有其人但密碼錯誤，另有14%則因帳號密碼均正確，故遭登入成功；研判歹徒此舉的目的在比對手上的帳號密碼，窺探會員訂單明細，下一步可能偽冒PayEasy客服人員，並以訂單明細取信會員，遂行其詐騙企圖。

個資未自PayEasy外洩

據PayEasy提供刑事局的電腦登入資料顯示，**歹徒只比對、未複製客戶資料，因此個資未自PayEasy外洩**，每筆登入停留時間從3.8秒到15秒不等，且每筆帳號只登入一次即換下一筆，因登入動作太慢，且停留時間參差不齊，我們研判，程式犯案的可能性不高，**我們的資料庫仍安全無虞**。

我們的處置

歹徒以合法手段進入PayEasy網站，因此極難察覺，但我們的資管人員仍在隔天9點上班後，主動查覺異狀，接著在第一時間內我們採取以下緊急處置行動：

①切斷數個來自中國大陸的特定IP

②凍結遭歹徒比對成功的PayEasy會員帳號密碼，確保這群會員個資不再外流

③同時發送簡訊通知會員提高警覺

④在PayEasy網站公告事件經過，彙整詐騙話術供會員參考，提供會員測試帳號是否安全

⑤向刑事局偵九隊報案

⑥邀集媒體記者配合報導、呼籲網民更改密碼

PayEasy唯一主動公告

在所有網路業者中，唯獨PayEasy勇敢站出來，主動告知會員，告知媒體，我們在與歹徒搶時間，目的在歹徒採取進一步詐騙行動前，搶先讓我們的會員知道風險。

保持零詐騙

經由這些斷然處置，歹徒騷擾PayEasy會員的高峰期已過，且截至目前並沒有任何PayEasy會員遭詐騙得逞，我們希望繼續保持「零詐騙」。

全民改密碼

在處理過程中，我們意識到歹徒手上所掌握的帳號密碼等個人資料數量極為龐大，而且隨著時間的累積，歹徒的「資料拼圖」愈來愈完整，他們仍在找尋下一個作案目標，每一個人都可能淪為詐騙集團的騷擾對象，因此我們在此大聲呼籲：**請立即上網更改不重複之全新密碼**，阻絕歹徒的資料比對行為；**若遇可疑電話，千萬不要配合到ATM轉帳**。

籲同業聯手防詐

自今年四月以來，各大網拍、網購、電視購物業者陸續傳出客戶個資外洩，累計近千名消費者因此遭詐騙得逞，我們研判歹徒的犯案模式可能雷同，面對這種「合法登入」、「資料拼圖」式的犯罪手法，我們認為最好的防範之道不是更換電腦系統或提升安全層級，更不是沈默以對，而是在事發的第一時間，儘速凍結帳號、通知會員、通知媒體。

在這段期間內，PayEasy感謝會員們的情義相挺，您所展現的合作精神，我們深受感動；對於各大媒體配合報導、阻斷歹徒繼續犯案，以及刑事局、調查局的指導與協助，我們在此一併表達誠摯感謝。

通報專線

若您仍接到自稱「PayEasy客服人員」的詐騙電話，請撥打0800023008免付費電話，或者市內電話(02)3316-9019回報給我們。若前兩支電話均忙線，請改撥(02)2531-9113，也籲請所有PayEasy會員，請將這支電話留給接到詐騙電話的會員，若非通報詐騙，請勿撥打。

以上全部文字歡迎您的善意轉載，並請傳給您的親朋好友，大家一起對抗詐騙。最後，PayEasy祝您天天平安喜樂。

康迅數位整合股份有限公司
PayEasy.com 敬上

附錄 9　PayEasy 遭「非駭客型」攻擊說明(置於網頁)

2007.12.12

◎PayEasy 遭「非駭客型」攻擊說明◎

感謝您的信賴與配合

自 12 月 10 日我們發現部份 PayEasy 會員可能面臨詐騙風險時，開始對會員發出一波又一波警示：我們發出警告簡訊、我們提供您測試密碼安全性、我們請您上網改密碼、甚至請接到詐騙電話的會員回報給我們…

我們站在前線把關您的安全，您把信任交在我們手上，對於我們的善意提醒，您一一機警配合，讓 PayEasy 至今保持「零詐騙」，在此向您致上十二萬分謝意與敬意。

●PayEasy 唯一主動攔截並公告

在此向您報告，PayEasy 不辱您的信賴，近半年來，國內各大網站陸續傳出「個資外洩」事件，PayEasy 獨家成功攔截詐騙集團的非法登入行爲，並在第一時間內通知會員、通知警方、通知媒體，爲的是和歹徒搶時間，要在歹徒著手詐騙前，讓會員知道風險。

位在對岸福建的詐騙集團，試圖用手上所掌握的大量來路不明的帳號密碼，一筆一筆以合法方式登入 PayEasy 網站，目的在比對手上的既有資料，確認那幾筆是 PayEasy 會員所有。

●個資未自 PayEasy 外洩

據 PayEasy 提供刑事局的詐騙集團電腦登入資料顯示，**歹徒只比對、未複製客戶資料，因此個資未自 PayEasy 外洩**，每筆登入停留時間從 3.8 秒到 15 秒不等，且每筆帳號只登入一次即換下一筆，因登入動作太慢，且停留時間參差不齊，我們研判，**程式犯案的可能性不高，應非「駭客入侵」，我們的資料庫仍安全無虞。**

●我們的處置

歹徒以合法手段進入 PayEasy 網站，因此極難察覺，但我們的資管人員仍在隔天 9 點上班後，主動查覺異狀，接著在第一時間內我們採取以下緊急處置行動：

1.切斷數個來自中國大陸的特定 IP

2.凍結遭歹徒比對成功的 PayEasy 會員帳號密碼、確保這群會員個資不再外流

3.同時發送簡訊通知會員提高警覺

4.在 PayEasy 網站公告事件緣由、彙整詐騙話術供會員參考、提供會員測試帳號是否安全

5.向刑事局偵九隊報案

6.邀集媒體記者配合報導、呼籲網民更改密碼

7.在自由、蘋果、工商、經濟等四大報刊登廣告，籲請全民改密碼

我們認爲 Payeasy 除了照顧會員權益之外，也有責任把這件事件讓全民有所警惕,共同防堵詐騙。

●保持零詐騙

經由這些斷然處置，歹徒騷擾 PayEasy 會員的高峰期已過，且截至目前並沒有任何 PayEasy 會員遭詐騙得逞，我們

希望繼續保持「零詐騙」。

●千萬別操作 ATM

您若接到任何自稱 PayEasy 客服人員的電話，**凡是要求您去操作 ATM 者，極可能是詐騙集團所打，所謂「千騙、萬騙，不離 ATM」，呼籲您千萬不要聽從**。

●全民改密碼

在處理過程中，我們意識到歹徒手上所掌握的帳號密碼等個人資料數量極爲龐大，而且隨著時間的累積，歹徒的「資料拼圖」愈來愈完整，他們仍在找尋下一個作案目標，因此每一個人都可能淪爲詐騙集團的騷擾對象，我們在此大聲呼籲：**請立即上網更改不重複之全新密碼**，阻絕歹徒的資料比對行爲；**若遇可疑電話，千萬不要配合到 ATM 轉帳**。

●籲同業聯手防詐

自今年四月以來，各大網拍、網購、電視購物業者陸續傳出客戶個資外洩，累計近千名消費者因此遭詐騙得逞，我們研判歹徒的犯案模式可能雷同，面對這種「合法登入」、「資料拼圖」式的犯罪手法，我們認爲最好的防範之道不是更（加入）換電腦系統或提升安全層級，更不是沈默以對，而是在事發的第一時間，儘速凍結帳號、通知會員、通知媒體。

在這段期間內，PayEasy 感謝會員們的情義相挺，您所展現的合作精神，我們深受感動；對於各大媒體配合報導、阻斷歹徒繼續犯案，以及刑事局、調查局的指導與協助，我們在此一併表達誠摯感謝。

●通報專線

若您仍接到自稱「PayEasy 客服人員」的詐騙電話，請撥打 0800023008 免付費電話，或者市內電話（02）33169019 回報給我們。若前兩支電話均忙線，請改撥（02）25319113，也籲請所有 PayEasy 會員，請將這支電話留給接到詐騙電話的會員，**若非通報詐騙，請勿撥打**。

以上全部文字歡迎您的善意轉載，並請傳給您的親朋好友，大家一起對抗詐騙。

最後，PayEasy 祝您天天平安喜樂

康迅數位整合股份有限公司 PayEasy.com 敬上

最後提醒：**詐騙行爲之所以發生損失，關鍵都在操作 ATM 或甚至臨櫃進行提款、轉帳，呼籲消費者在接獲自稱某網購業者客服電話，並要求提供存款餘額、要求轉帳時，千萬不要照做，請先撥打刑事局 165 防詐騙專線，或直接去電網購業者，務必確認再確認。**

附錄 10　PayEasy 資訊安全即時通報 2007.12.14

◎PayEasy 資訊安全即時通報◎

各位敬愛的 PayEasy 會員：

●詐騙威脅大幅降低

親愛的會員朋友，經過近二天來的會員簡訊、首頁公告，乃至於媒體報導，我們動用各種管道告訴您，有歹徒曾嚐試以大量來路不明且非法取得之帳號、密碼登入 PayEasy 網站找尋作案目標，經由這些努力，在此向各位報告，這個事件已獲得控制，歹徒對 PayEasy 會員的詐騙威脅已大幅降低。

就目前來電表示接到詐騙電話的統計分析,我們在 12 月 10 日傍晚到 12 月 11 日共收到 **17 通**的客戶通報曾接到詐騙電話，**12 月 12 日只有 1 通會員通報，13、14 日共只有 1 通，這代表歹徒已暫停騷擾 PayEasy 會員。**

●「PayEasy 防詐騙專線」啓用

會員萬一不幸遭歹徒詐騙成功，請立即撥打（02） 25319113 直撥專線向我們反映，我們除了加強警戒之外，將協助您對歹徒採取法律行動，但請大家配合，這支專線請留給遭詐騙的不幸會員，如果不是通報受騙，請千萬不要撥打。

●保持「零詐騙」

經由網站公告以及媒體披露，回 PayEasy 網站更密碼的會員數達到平時的 56 倍以上，歹徒已經知道詐騙 PayEasy 會員是高成本、高難度的工程，讓人欣慰的是到目前爲止**沒有會員遭詐騙得逞**，我們希望會員朋友與我們合作。

●商品查詢暫勿撥打客服電話

這幾天我們的 0800-023-008 或 02-33169019 等客服專線應接大量會員查詢，您可發覺客服電話在白天上班時間很難接通，在此向您說聲抱歉，爲節省您在電話線旁的等候時間，請您儘量上網到 PayEasy 首頁點擊「客服中心」，用線上書面方式與我們連絡，**在這個時刻，我們不在乎賺錢，我要全力保障會員的安全，若您只是查詢商品，則請利用首頁「客服中心」以書面發問。**

●感謝各界支持

在這場針對犯罪集團的戰役中，我們感謝警政署刑事警察局的協助、感謝各大媒體的配合宣導，也感謝廣大會員對 PayEasy 的愛護與支持，雖然公開此事影響消費信心，但在事件公開之後的第二天（12 月 12 日），PayEasy 網站單日業績仍突破新台幣 1000 萬元，另外有近千名愛用者在同一天新加入 PayEasy 成爲新會員。

滿載各界的關懷，PayEasy 對全體會員致上最大謝意，我們已全面提升全站資訊安全等級，不僅由資管人員 24 小時監控可疑登入，並且提供 24 小時真人客服，且會定期向各位報告最新資安狀況，我們希望不負會員所託，讓您在此安心購物。

PayEasy 康迅數位整合股份有限公司

總經理 林坤正 敬上 96.12.14

最後提醒：**詐騙行爲之所以發生損失，關鍵都在操作 ATM 或甚至臨櫃進行提款、轉帳，呼籲消費者在接獲自稱某網購業者客服電話，並要求提供存款餘額、要求轉帳時，千萬不要照做，請先撥打刑事局 165 防詐騙專線，或直接去電網購業者，務必確認再確認。**

附錄 11　2007/12/22 鄭運鵬出面說明

鄭運鵬：慎防非駭客型個資詐騙

THE CENTRAL NEWS AGENCY 中央通訊社

更新日期：2007/12/22

圖說：

民進黨籍立委鄭運鵬二十二日在立法院表示，最近數件網路個人資料洩漏事件，極可能是中國詐騙集團測試台灣民眾帳號密碼的「非駭客型個資詐騙」類型，若歹徒與中國情治單位結合，將破壞金融體系或國安系統。中央社記者王飛華攝 九十六年十二月二十二日

附錄 12　2007/12/25 刑事局召開記者會

八大購物網被駭　會員資料外洩

華視 CTS 更新日期：2007/12/25 14:39

國內八個購物網站傳出駭客入侵會員資料外洩，警方懷疑各大購物網站可能都遭殃。嫌犯可能是偷來一組帳號密碼之後，到處測試盜用，警方提醒密碼要常改，接到詐騙電話千萬不要到ATM轉帳。在網路上買東西，先逛第一家再逛第二家，貨比三家不吃虧，不過如果三家店，都是同一個帳號和

附錄 13　2008/1/15 經濟日報 報導

網購防詐騙 業者主動出擊

【台北訊】

經濟日報昨（14）日舉辦「詐騙狂潮下網路業者該做什麼？」座談會，與會人包括有消基會董事長程仁宏、警政署警務正常金蘭、康迅數位整合（PayEasy）總經理林坤正，探討消費者、業者和警方如何攜手打擊近來層出不窮的網路購物詐騙事件。

PayEasy在12月8日遭來自廈門的詐騙集團，採用來路不明、事前非法取得的大量帳號密碼，以合法方式，一筆一筆登入PayEasy網站，以便進行詐騙行動。

PayEasy在隔天上午發現異狀，隨即採取一連串反制行動，其中包括全面通知會員，甚至不惜商譽，主動向媒體發布新聞，目的在保護會員避免上當。這是自今年4月國內網購、電視購物業者陸續爆發會員遭詐騙事件以來，唯一主動公開的業者，且至今維持會員零詐騙紀錄。

座談會上，程仁宏、常金蘭都表示，所有網購與電視購物業者，凡遭遇類似事件，應以消費者權益爲先，企業不能短視利益，而犧牲長遠的商譽。（陳家詡）

【2008-01-15/經濟日報/A16版/工商活動】

附錄 14　PayEasy 感謝會員配合，創造「零詐騙奇蹟」

◎PayEasy 資訊安全聲明◎

PayEasy 感謝 240 萬會員的信任與肯定
共同創造「零詐騙」奇蹟

就在去年年底，PayEasy 熱鬧舉辦年終促銷的當口，詐騙集團悄悄盯上 PayEasy，我們認爲保護我們的會員比做生意更重要，當即決定把年終慶先放到一邊，直接面對詐騙集團的挑戰，捍衛會員的安全。

詐騙集團利用事前非法取得、且來路不明的大量帳號密碼，從對岸福建廈門一筆一筆地嘗試登入 PayEasy 網站，原本是神不知不覺，但仍被我們的資管人員識破，在這場正邪角力的戰役中，感謝您的信賴與配合，讓我們共同安渡一場詐騙風暴。

讓我們回顧一下當時的狀況：

●緊急處置

當我們發現系統異狀，第一時間內我們凍結掉 5467 筆遭測試成功的會員帳號、全面阻斷來自中國上億個 IP 的連線權，封鎖掉歹徒後續的資料竊取行動；接著，我們對會員發出近 100 萬通簡訊，警告會員不要受騙，然後我們向刑事局偵九隊、調查局資四科報案。

經過這段緊急處置，我們接著在 PayEasy 首頁的顯著版位上，說明事件原委，並詳述詐騙集團的犯案過程，提供會員檢測帳號密碼，確認是否曾遭歹徒「資料拼圖」得

逞，並呼籲會員儘速全面變更密碼。

●PayEasy 變身「反詐騙網站」

爲掌握歹徒最新動態，PayEasy 設立防詐熱線，請求會員一旦接獲詐騙電話，立即向我們回報，然後我們索性將歹徒最新詐騙話術一一登在首頁，而且天天更新；這樣一來，PayEasy 從首頁開始到產品頁、結帳頁、會員中心，乃至於出貨外包裝，統統加註警語，整個 PayEasy 活像一個「反詐騙網站」。

做到這些還不夠，我們不顧商譽可能受損，堅持在事發第一時間主動召開記者會，我們不怕媒體「拷問」，只要儘快給大眾知道 PayEasy 出了什麼事，我們甚至在網路與報紙上購買大篇幅防詐廣告…做這些事情目的只有一個：務必在歹徒對會員下手前要會員提高警覺。

●全體動員連夜 Call Out

我們曾發現歹徒正在打電話詐騙某些特定客戶，一度緊急動員全體同仁，連夜 Call Out 給客戶、甚至連夜製作數千封警告信，以限時專送寄給客戶，我們精神緊繃，凡事求快，因爲我們知道歹徒正瞄準我的客戶，我要和歹徒比速度。

據平面媒體報導指出，網路、電視購物詐欺案正以每周 350 件的速度增加中；另有報導指稱，每月因詐騙受害金額達新台幣 6000 萬元以上；若報導屬實，則以此類推全年因此上當的民眾將多達上萬人，無辜損失金額也將達數億元之譜，即使警方已加強查緝，但這畢竟是一種新型態犯罪，一時之間難以防堵。

●PayEasy 保持「零詐騙」

在這波詐騙狂潮下，大部分的同業無奈地選擇沉默，PayEasy 選擇公開；大部分同業瞻前顧後，我們選擇迎戰；大部分同業深覺委曲，我們則堅強地站起來保護會員，不讓會員成爲受害者，在這場戰役中，我們既受傷且孤獨。

但是，經由上述一系列措施，詐騙集團已停止騷擾 PayEasy 會員，且截至目前沒有任何 PayEasy 會員遭詐騙得逞，我們持續保持「零詐騙」，這是唯一足堪告慰之事。

●請會員繼續協助

歹徒詐騙手法不斷推陳出新，請會員們繼續協助我們，如果您接到冒稱 PayEasy 客服人員的電話，要求您去操作 ATM 者，一定是詐騙集團所爲，所謂「千騙、萬騙，不離 ATM」，不配合操作 ATM 是防堵各式電話詐騙不二的法門!

我們的防詐熱線會持續的運作下去，如果您接到冒名 PayEasy 客服人員的詐騙電話，請務必撥打 0800-023-008 免付費電話，或者市內電話（02）3316-9019 向 PayEasy 通報，以便我們研判歹徒的動作預作防範。

在這段期間內，PayEasy 感謝會員們的情義相挺，您所展現的合作精神，我們深受

感動；對於各大媒體配合報導、阻斷歹徒繼續犯案，以及刑事局、調查局的指導與協助，我們在此一併表達誠摯感謝。

最後，PayEasy 祝您天天平安喜樂

康迅數位整合股份有限公司 PayEasy.com 敬上
2008/1/15

最後提醒：詐騙行爲之所以發生損失，關鍵都在操作 ATM 或甚至臨櫃進行提款、轉帳，呼籲消費者在接獲自稱某網購業者客服電話，並要求提供存款餘額、要求轉帳時，千萬不要照做，請先撥打刑事局 165 防詐騙專線，或直接去電網購業者，務必確認再確認。

附錄 15　PayEasy 零詐騙奇蹟 2008.1.14 於四大報全版刊登廣告

PayEasy感謝240萬會員的信任與肯定

共同創造「零詐騙」奇蹟

就在去年年底，PayEasy熱鬧舉辦年終促銷的當口，詐騙集團悄悄盯上PayEasy，我們認為保護我們的會員比做生意更重要，當即決定把年終慶先放到一邊，直接面對詐騙集團的挑戰，捍衛會員的安全。

詐騙集團利用事前非法取得、且來路不明的大量帳號密碼，從對岸竄建廣門一筆一筆地嘗試登入PayEasy網站，原本是神不知不覺，但仍被我們的資管人員識破，在這場正邪角力的戰役中，感謝您的信賴與配合，讓我們共同安渡一場詐騙風暴。

讓我們回顧一下當時的狀況：

＊緊急處置

當我們發現系統異狀，第一時間內我們凍結掉5467筆遭測試成功的會員帳號、全面盲斷來自中國上億個IP的連線權，封鎖掉歹徒後續的資料竊取行動；接著，我們對會員發出近100萬通簡訊，警告會員不要受騙，然後我們向刑事局偵九隊、調查局資四科報案。

經過這段緊急處置，我們接著在PayEasy首頁的顯著版位上，說明事件原委，並詳述詐騙集團的犯案過程，提供會員檢測帳號密碼，確認是否曾遭歹徒「資料拼圖」得逞，並呼籲會員儘速全面變更密碼。

＊PayEasy 變身「反詐騙網站」

為掌握歹徒最新動態，PayEasy設立防詐熱線，請求會員一旦接獲詐騙電話，立即向我們回報，然後我們索性將歹徒最新詐騙話術一一登在首頁，而且天天更新；這樣一來，PayEasy從首頁開始到產品頁、結帳頁、會員中心，乃至於出貨外包裝，統統加註警語，整個PayEasy活像一個「反詐騙網站」。

做到這些還不夠，我們不顧商譽可能受損，堅持在事發第一時間主動召開記者會，我們不怕媒體「拷問」，只要儘快給大眾知道PayEasy出了什麼事，我們甚至在網路與報紙上購買大篇幅防詐廣告…做這些事情目的只有一個：務必在歹徒對會員下手前要會員提高警覺。

＊全體動員連夜Call Out

我們曾發現歹徒正在打電話詐騙某些特定客戶，一度緊急動員全體同仁，連夜Call Out給客戶、甚至連夜製作數千封警告信，以限時專送寄給客戶，我們精神緊繃，凡事求快，因為我們知道歹徒正在瞄準我的客戶，我要和歹徒比速度。

據平面媒體報導指出，網路詐欺案正以每周350件的速度增加中；另有報導指稱，每月因詐騙受害金額達新台幣6000萬元以上；若報導屬實，則以此類推全年因此上當的民眾將多達上萬人，無辜損失金額也將達數億元之譜，即使警方已加強查緝，但這畢竟是一種新型態犯罪，一時之間難以防堵。

＊PayEasy保持「零詐騙」

在這波詐騙狂潮下，大部分的同業無奈地選擇沉默，PayEasy選擇公開；大部分同業瞻前顧後，我們選擇迎戰；大部分同業深覺委曲，我們則堅強地站起來保護會員，不讓會員成為受害者，在這場戰役中，我們既受傷且孤獨。

但是，經由上述一系列措施，詐騙集團已停止騷擾PayEasy會員，且截至目前沒有任何PayEasy會員遭詐騙得逞，我們持續保持「零詐騙」，這是唯一足堪告慰之事。

＊請會員繼續協助

歹徒詐騙手法不斷推陳出新，請會員們繼續協助我們，如果您接到冒稱PayEasy客服人員的電話，要求您去操作ATM者，一定是詐騙集團所為，所謂「千騙、萬騙，不離ATM」，不配合操作ATM是防堵各式電話詐騙不二的法門!

我們的防詐熱線會持續的運作下去，如果您接到冒名PayEasy客服人員的詐騙電話，請務必撥打0800-023-008免付費電話，或者市內電話（02）3318-9019向PayEasy通報，以便我們研判歹徒的動作預作防範。

在這段期間內，PayEasy感謝會員們的情義相挺，您所展現的合作精神，我們深受感動；對於各大媒體配合報導、阻斷歹徒繼續犯案，以及刑事局、調查局的指導與協助，我們在此一併表達誠摯感謝。

最後，PayEasy祝您天天平安喜樂

康迅數位整合股份有限公司PayEasy.com 敬上

附錄 16　PayEasy 花錢買沒有用的廣告,在 Yahoo 購買廣告警示大眾—節錄某部落格的內容

今天一大早，照慣例打開yahoo首頁時，居然看到
Yahoo首頁醒目的廣告：厦門詐騙集團將對台灣民眾發動全新詐騙攻勢

原本以爲，只是一個誇張化的廣告宣傳用語
一般電子商務或購物網站偶爾也會用的手法～
但還是好奇地給它點了進去

沒想到，竟然是真真正正貨真價值的公告頁!!
http://www.payeasy.com.tw/payeasy/edm/970414.htm?sid=96960014T-bar_0415deFraud

此時，我不得不佩服payeasy這家公司
願意花大筆廣告錢做這件事

畢竟在競爭的商務市場
公司對每一個wording,每一段廣告
甚至每一個活動頁，都要看到數字及預估數據的評估
但...**payeasy卻買了這則可能沒有任何業績的公告頁廣告**

附錄 17　詐騙集團第二次攻擊--新聞媒體下標聳動

2008/04/14 09:55

700 張僞信用卡 盜刷 PAYEASY 千萬

中時電子報 www.chinatimes.com 更新日期: 2008/04/14 04:33 吳俊陵台北報導

警方提醒民眾，詐騙集團恐怕又出新招了！知名購物網站 PAYEASY 十三日向刑事局偵一隊備案指出，他們的網站在二天內，遭歹徒以多達七百多張信用卡密集盜刷了一千多萬元！警方研判這起大量盜刷事件，可能是詐騙集團「連環騙」的一環，先鬧大事情、勾起卡友的恐慌，再假冒銀行或警方的身分，打電話詐騙。

PAYEASY 的法務及公關人員昨日向警方備案指稱，從前天到昨天不到四十八小時之內，他們的監控中心發現有十二個新開戶的帳號，密集輸入七百多張信用卡號，疑似連續盜刷七百多筆交易。經查每筆交易金額從數千元到一萬九千元不等，且以三Ｃ家電爲主，累積的交易總金額達一千一百萬元。

據了解，一般購物網站會員都是一人一卡，每次一筆消費，十二個帳號使用不同的七百多張信用卡交易極不尋常，而且交易的時間都集中在半夜到凌晨之間也違反常理。購物網站驚覺事態嚴重，馬上通知國內卅多家銀行密切注意這批信用卡號的動向；其中，有數家銀行反應部分信用卡號曾爲列管盜刷警示卡，顯示幕後恐有信用卡盜刷集團或詐騙集團操縱，網站於是通知銀行立即止付，並在昨日報警。

令警方疑惑的是，歹徒密集、大量盜刷不但增加盜刷的困難度，也很容易讓犯行曝光，與信用卡盜刷集團所採取「小額、分散」的作案模式不同，顯然另有企圖。警方研判，可能是詐騙集團故意製造大規模的信用卡盜刷事件，以引起媒體報導後，再假藉銀行風險管理科或警方名義，向一般民眾以「你的信用卡已被盜刷」爲由，進行詐騙。

目前全案已由警方介入偵辦，並調閱購物網站的交易及會員資料追查，警方和銀行也呼籲，在這段調查期間，任何可能被冒名盜刷的民眾，在接獲自稱查證或要求「停卡」的電話時，能夠先打電話向「一六五」進行反向求證，以過濾來電者，到底是警察還是歹徒？

2.　PayEasy 遭盜刷千萬　恐設下連環騙圈套

卡優新聞網 cardu.com.tw　黃靜萍

國內知名購物網站 PAYEASY 傳出遭歹徒盜刷七百多張信用卡，金額超過上千萬元，而且交易時間都集中在深夜到凌晨這段時間，還好網站人員即時發現向刑事局報案。

但警方擔心這是詐騙集團「連環騙」的伎倆，目的要引起持卡人恐慌，再伺機行騙。因此警方提醒卡友，若接到銀行通知「卡片遭盜刷」訊息，切記要臨櫃辦理相關手續，千萬別聽從指示操作 ATM。

警方調查，四月十一、十二日短短兩天時間，PAYEASY 購物網出現大量異常的交易情況，有十二個最近新加入的會員帳號，連續刷卡購買高單價的 3C 商品，金額從數千元到上萬元不等，總計有七百八十多筆交易記錄，累計一千多萬的消費額度。

網站人員監控到異常交易，隨即通報國內三十多家銀行立即止付，同時清查這批信用卡的交易記錄，發現部分信用卡曾被列爲盜刷警示卡，因此網站立即終止交易，沒有將下單商品出貨，尚未造成損失。

警方表示，以往信用卡盜刷集團多半採取小額、分散刷卡，避免犯行太早曝光，但這次歹徒犯案模式卻反其道而行，只利用少數會員帳號密集刷卡，其中大有玄機。警方研判，歹徒可能想製造信用卡被嚴重盜刷的話題，引起持卡人恐慌，再假扮警察辦案、或是銀行客服人員向民眾行騙。

刑事局接獲報案後，已經著手調閱 PAYEASY 購物網站的會員及相關交易資料追查，而這段時間，銀行也會陸續通知信用卡可能遭盜刷的民眾。但警方提醒，如果接獲自稱是銀行或是警方的電話，要求辦理停卡，或是通知被盜刷訊息，一定要先向 165 反詐騙諮詢專線求證，不要隨便透露個人資料或是前往 ATM 操作匯款。

附錄 18　Payeasy 呼籲大眾防範新詐騙手法的網站聲明

2008.4.14

◎PayEasy 資訊安全聲明◎

廈門詐騙集團將對台灣民眾發動全新攻勢
—PayEasy 的急切呼籲與提醒

各位親愛的會員朋友您好：

如同「假車禍、真詐財」的翻版，網路購物市場近來也發現疑似透過非法蒐集而來的信用卡卡號，到購物網站登入會員，然後立刻刷卡僞裝購買高價商品，其實他們並非要詐騙貨品，而是「假冒刷、真詐騙」；最近若您被銀行通知信用卡被冒刷，請您注意後續有沒有人打電話要您去作轉帳行爲，如果有，請千萬小心。

歹徒所在位置爲對岸廈門

PayEasy 在 4 月 12-13 日，2 天內多了 12 名「新會員」，歹徒用虛構的地址與姓名註冊，PayEasy 彙整來自銀行、警方、以及我們內部截獲破解源自於歹徒所留下的資料與信息，我們有足夠的證據推論：這群不速之客和去年對台發動「資料拼圖」的歹徒應屬同一批來自對岸廈門的詐騙集團。

製造冒刷行爲，爲後續詐騙電話埋伏筆

在加入會員後，他們立刻在 PayEasy 網站上大肆「購物」，這群「新會員」每個人各用近百張信用卡卡號在線上瘋狂刷卡，但他們動作太過密集，馬上會被識破；再者，他們所下單的商品很多都是「冰箱」、「冷氣」等大型家電，這些東西甚至必須「到府安裝」，明顯不符詐取財物、快速變現的邏輯，我們斷定，「盜刷」不是他們的真正目的，而是在爲後續的詐騙行動鋪路。

我們在 4 月 13 日事發第二天就彙整所有資料，向刑事局報案，報案當時，共計發現 12 個可疑登入帳號，共使用 700 多張信用卡，訂購量近 1200 萬元，**訂單全都被我們封鎖，不會產生損失**，我們同時向媒體發出訊息，4 月 14 日各大媒體均見「PayEasy 遭盜刷千萬元」等新聞。

歹徒行徑囂張，無畏媒體曝光

我們原本想用新聞來嚇阻詐騙集團，但令人驚訝的是，即使在新聞披露後，他們仍持續「購物」，直到 14 日晚間 9 點左右，這群「人」累積已刷過近 1700 筆信用卡卡號，分別來自超過 32 家發卡銀行，幾乎全台所有發卡銀行統統中獎。

早在 4 月 10 日，PayEasy 就曾接獲國內某大銀行來電，要求我們對某張信用卡訂單凍結出貨，原因是：這張卡號已在其他大型購物網站上被冒刷；14 日以後，有更多銀行向我們證實，更多大型購物網站同時都遭到這類冒刷攻擊，**更有銀行告訴我們，客戶已接到詐騙電話**，這也證實了我們先前推論，而這個時候仍只有 PayEasy 對媒體與民眾發出警告。

更大一波的攻擊，全面發動在即

重點還在後頭，這類冒刷事件，既然目的不是詐取財物，則必然背後會有更大野心，爲此，我們推演歹徒可能的詐騙「劇本」：

歹徒先在購物網站上冒刷持卡人 A 先生的信用卡→歹徒僞裝警察致電 A 先生說：你的信用卡被盜刷，請趕快去電發卡銀行作確認→A 先生緊張地打電話問銀行，銀行果然回覆「確實被盜刷」→歹徒再去電 A 先生問到底有沒有？A 先生回答：的確有…

劇本寫到這裡，您將不難想像，A 先生後續將陷入極大的被詐騙風險，因爲，這件事有「銀行」作背書，怎麼可能是假的，**詐騙的基本原理就是來自於取信，銀行是大家最信任的單位，有銀行的背書，民眾如何分辨真僞**？

我們推斷，即將發動或已經發動的這波詐騙行動，將是有史以來騙術最高明、最令人真假莫辨、傷害性也會最大一次，而且發動在即。

我們在此提出四點呼籲

1.請檢警單位儘速查出信用卡外洩管道，我們已提供警方大量有效信用卡卡號，期盼警方能夠協同銀行找出洩露源頭，儘早制止禍源。

2.請各大網購/電視購物同業不要再沈默以對，儘快將您手中掌握的資料提供警方偵辦，勿錯失機會，讓無辜的民眾被詐騙得逞。

3.請各銀行在通知持卡人遭冒刷時，同步提醒持卡人後續歹徒有可能假冒警察、銀行，誘導民眾到 ATM 轉帳詐騙。

4. 過去兩岸關係冰凍，如今春暖花開，期待兩岸關改善的同時，新政府將網路詐騙列入兩岸共同打擊犯罪的重點。

PayEasy 堅持做「對的事情」，而且絕對貫徹到底

當事件發生的時候，我們可以隱匿不報，反正我們沒有損失，或者是報案後要求警方不公開，因爲披露此事會衝擊到 PayEasy 正在進行的週年慶特賣活動。

但我們仍選擇最困難的抉擇，也是最傻的決定：通報 32 家銀行、請銀行通知持卡人、向警

方報案、請媒體協助，對台灣社會發出警訊。

我們認爲有良知的企業，明知將發生且嚴重危害民眾的生命與財產安全的事件時，縱使與你無關，也絕不會選擇袖手旁觀。

近一年來，網路購物、電視購物大部分的同業對詐騙集團一再隱忍，原本各有苦衷，但這種態度卻無形中讓詐騙集團食髓知味，爲之坐大，對於上千成萬的詐騙受害者來說，高達數億元的財產損失，這無異姑息養奸，養虎貽患。

孤身迎戰詐騙集團， PayEasy 爲企業經營建立新標竿

讓我們引以爲傲的是，到目前爲止 PayEasy 沒有一位會員因爲上 PayEasy 購物而遭詐騙得逞，由於我們不計代價的維護會員權益、由於我們對於社會正義仍有一絲絲的寄望，去年年底我們挺身孤單對抗詐騙集團，保護會員，現在我們爲了守護 1700 名無辜的持卡人，再次迎戰。

儘管我們知道這 1700 名持卡人絕大部份不是 PayEasy 會員，只因他們的信用卡號莫名其妙被人竊取、只因我們的專業分析推斷他們可能淪爲下一波被詐騙對象，我們仍毅然一肩扛起。

他日如有同類型的事件發生，我們還是會做同樣選擇，因爲這是深植入 PayEasy 的企業信念，當 PayEasy 的員工面對自己，面對家人，面對同業，面對社會時，我們會驕傲的說：**PayEasy 做對的事情，堅持貫徹到底!!**

*****請您儘快將這個訊息傳給您的週遭親友，越多越好，越廣越好，期盼台灣能夠早日免除被詐騙的恐懼，這是普遍升斗小民的憐憫祈求。**

康迅數位整合股份有限公司 PayEasy.com 敬上

最後提醒：**詐騙行爲之所以發生損失，關鍵都在操作 ATM 或甚至臨櫃進行提款、轉帳，呼籲消費者在接獲自稱某網購業者客服電話，並要求提供存款餘額、要求轉帳時，千萬不要照做，請先撥打刑事局 165 防詐騙專線，或直接去電網購業者，務必確認再確認。**

附錄 19　PayEasy 2008/4/15 呼籲在三大報刊登

PAYEASY 的急切呼籲與提醒

廈門詐騙集團
將對台灣民眾發動全新攻勢

如同「假車禍、真詐財」的翻版，網路購物市場近來也發現疑似透過非法蒐集而來的信用卡卡號，到購物網站登錄會員，然後立刻刷卡偽裝購買高價商品，其實他們並非要詐騙貨品，而是「假冒刷、真詐騙」；最近若您被銀行通知信用卡被冒刷，請您注意後續有沒有人打電話要您去作轉帳行為，如果有，請千萬小心。

來自廈門

PayEasy在4月12-13(週六日)，2天內多了12名「新會員」，歹徒用虛構的地址與姓名註冊，PayEasy彙整來自銀行、警方、以及我們內部截獲破解源自於歹徒所留下的資料與信息，我們有足夠的證據推論：這群不速之客和去年對台發動「資料拼圖」的歹徒應屬同一批來自對岸廈門的詐騙集團。

製造冒刷 預備詐騙

在加入會員後，他們立刻在PayEasy網站上大肆「購物」，這群「新會員」每個人各用近百張信用卡卡號在線上瘋狂刷卡，但他們動作太過密集，馬上會被識破；再者，他們所下單的商品很多都是「冰箱」、「冷氣」等大型家電，這些東西甚至必須「到府安裝」，明顯不符詐取財物、快速變現的邏輯，我們斷定，「盜刷」不是他們的真正目的，而是在為後續的詐騙行動鋪路。

我們在4月13日事發第二天就彙整所有資料，向刑事局報案，報案當時，共計發現12個可疑登錄帳號，共使用700多張信用卡，訂購量近1200萬元，**訂單全都被我們封鎖，不會產生損失**，我們同時向媒體發出訊息，4月14日各大媒體均見「PayEasy遭盜刷千萬元」等聳動新聞。

歹徒我行我素

我們原本想用新聞披露來嚇阻詐騙集團，但令人驚訝的是，即使在新聞披露後，他們仍持續「購物」，直到14日晚間6點左右，這群「人」累積已刷過近1700筆信用卡卡號，分別來自超過32家發卡銀行，幾乎全台所有發卡銀行統統中獎。

早在4月10日，PayEasy就曾接獲國內某大銀行來電，要求我們對某張信用卡訂單凍結出貨，原因是：這張卡號已在其他大型購物網站上被冒刷；14日以後，有更多銀行向我們證實，更多大型購物網站同時都遭到這類冒刷攻擊，**更有銀行告訴我們，客戶已接到詐騙電話**，這也證實了我們先前推論，而這個時候仍只有PayEasy對媒體與民眾發出警告。

大攻擊發動在即

重點還在後頭，這類冒刷事件，既然目的不是詐取財物，則必然背後會有更大野心，為此，我們推演歹徒可能的詐騙「劇本」：

歹徒先在購物網站上冒刷持卡人A先生的信用卡→歹徒偽裝警察致電A先生說：你的信用卡被盜刷，請趕快去電發卡銀行作確認→A先生緊張地打電話問銀行，銀行果然回覆「確實被盜刷」→歹徒再去電A先生問到底有沒有？A先生回答：的確有…

劇本寫到這裡，您將不難想像，A先生後續將陷入極大的被詐騙風險，因為，這件事有「銀行」作背書，**怎麼可能是假的，詐騙的基本原理就是來自於取信，銀行是大家最信任的單位，有銀行的背書，民眾如何分辨真偽？**

我們推斷，**即將發動或已經發動的這波詐騙行動，將是有史以來騙術最高明、最令人真假莫辨、傷害性也會最大一次，而且發動在即。**

我們在此提出四點呼籲：

一、請檢警單位儘速查出信用卡外洩管道，我們已提供警方大量有效信用卡卡號，期盼警方能夠協同銀行找出洩露源頭，儘早制止禍源。

二、請各大網購/電視購物同業不要再沈默以對，儘快將您手中掌握的資料提供警方偵辦，勿錯失機會，讓無辜的民眾被詐騙得逞。

三、請各銀行在通知持卡人遭冒刷時，同步提醒持卡人後續歹徒有可能假冒警察、銀行，誘導民眾到ATM轉帳詐騙。

四、過去兩岸關係冰凍，如今春暖花開，期待兩岸關改善的同時，新政府將網路詐騙列入兩岸共同打擊犯罪的重點。

PayEasy做對的事情，堅持貫徹到底

當事件發生的時候，我們可以隱匿不報，反正我們沒有損失，或者是報案後要求警方不公開，因為披露此事會衝擊到PayEasy正在進行的週年慶特賣活動。

但我們仍選擇最困難的抉擇，也是最優的決定：通報32家銀行、請銀行通知持卡人、向警方報案、請媒體協助，對台灣社會發出警訊。

我們認為有良知的企業，明知將發生且嚴重危害民眾的生命與財產安全的事件時，縱使與你無關，也絕不會選擇袖手旁觀。

近一年來，網路購物、電視購物大部分的同業對詐騙集團一再隱忍，原本各有苦衷，但這種態度卻無形中讓詐騙集團食髓知味，為之坐大，對於上千成萬的詐騙受害者來說，高達數億元的財產損失，這無異姑息養奸，養虎貽患。

孤身迎戰詐騙集團，PayEasy建立高度

讓我們引以為傲的是，到目前為止PayEasy沒有一位會員因為上PayEasy購物而遭詐騙得逞，由於我們不計代價的維護會員權益、由於我們對於社會正義仍有一絲絲的寄望，去年年底我們挺身孤單對抗詐騙集團，保護會員，現在我們為了守護1700名無辜的持卡人，再次迎戰。

儘管我們知道這1700多名持卡人絕大部份不是PayEasy會員，只因他們的信用卡號莫名其妙被人竊取、只因我們的專業分析推斷他們可能淪為下一波被詐騙對象，我們仍毅然一肩扛起。

他日如有同類型的事件發生，我們還是會做同樣選擇，因為這是深植PayEasy的企業信念，當PayEasy的員工面對自己，面對家人，面對同業，面對社會時，我們會驕傲的說：**PayEasy做對的事情，堅持貫徹到底!!**

***請您儘快將這個訊息傳給您的週遭親友，越多越好，越廣越好，期盼台灣能夠早日免除被詐騙的恐懼，這是普遍升斗小民的卑微祈求。

康迅數位整合股份有限公司
PayEasy敬上97.4.15

附錄 20　PayEasy 2008 年 5 月資訊安全聲明，主要的目的是向歹徒示警，PayEasy 有周全防禦，勿再來犯。

◎PayEasy資訊安全聲明◎

防範詐騙大家一起來

親愛的會員朋友們您好：

日前我們接獲**刑事局防詐騙165**專線通報訊息，顯示詐騙集團在最近一個月內活動頻繁，尤其最近半個月內，國內拍賣、網路及電視購物均遭受攻擊。我們承諾，一旦詐騙集團攻擊Payeasy，絕不會怯懦、隱匿訊息，而是負責任的站起來不計代價保護您的財產安全。

過去我們因應詐騙集團的挑釁，**不僅對客戶發出簡訊、主動電話聯繫，甚至主動發佈新聞稿、斥鉅資購買全版報紙廣告，這次，如果詐騙集團膽敢來犯，我們依舊會比照辦理。**

如果您接到任何可疑詐騙電話，麻煩您立即撥打**0800-023-008客服專線**與我們聯絡，我們將隨時將您所反映的歹徒詐騙話術在首頁連結中公告周知，讓您有所提防。

期待您提高警覺，並祝您購物愉快

康迅數位整合股份有限公司PayEasy.com 敬上

最後提醒：

(1) PayEasy不會主動去電「協助」您更改付款方式，更不會要求您操作ATM，如果接獲電話卻要求您做這樣的事，必然是詐騙電話，再次提醒您：「千騙萬騙不離ATM」，切勿依歹徒指示操作ATM，他們就是要引導您轉帳。

(2) 最近歹徒都會請您打電話到匯款銀行，或信用卡發卡銀行查詢，接著您的手機就會接一通來電顯示為銀行客服中心號碼的來電，目的是要取信於您，事實上這通顯示為銀行客服號電話的來電，極可能是假的。

(3) 0800-023-008為PayEasy客服中心接聽代表號，無法外撥，若您接到此電話來電顯示，請您勿理會並儘速與我們連絡。

附錄 21 會員登入驗證


PayEasy 陪你 Shopping 一輩子
會員中心
Shopping免上街，我天天都上PayEasy!
加入PayEasy會員好處多多
◎ 數萬件商品優惠，我們只讓會員獨享！
◎ 24小時便利商店付現取貨，付款安全免擔心！
◎ 台新信用卡會員獨享無息分期服務，花小錢先享受最划算！
◎ 親切的專業客服人員為您服務，任何問題均可e-mail聯絡我們
◎ 真心邀請，PayEasy陪您Shopping一輩子！
加入會員
特別提醒!
PayEasy不會主動向會員要求提供密碼，
會員中心服務（登入後即可使用）
個人訂單資料查詢
個人資料維護
電子報訂閱/取消
快樂e點點數查詢
簡訊平台
圖鈴下載
會員登入
請輸入您的帳號及密碼
身分證字號
密碼
右下驗證碼
0 8588
確 定
加入會員
忘記密碼
●重要提醒：
・PayEasy不會主動來電要求您操作ATM或透露存款餘額，若接到可疑電話，請拒絕回應並與客服中心0800-023-008、02-33169019聯絡，或直接撥打刑事局防詐騙165專線

附錄 22　對內部同仁公開信

寄件者: [redacted] [林坤正]
寄件日期: 2008 年 4 月 14 日星期一　下午 4:31
收件者: 全體員工
主旨: PayEasy 的企業價值就從歷次的危機中萃練出來...

各位同仁:
從週六開始，許多同仁加班處理歹徒的新詐騙手法，在此表達謝意，
我們也發現，本事件早已發生再國內其他知名網站有一周，但至今卻沒有一家站出來呼籲，
我們爲何選擇跳出來，不計毀譽的去通知所有被冒刷的持卡人，這些人與我們並沒有關係，
Why……..,

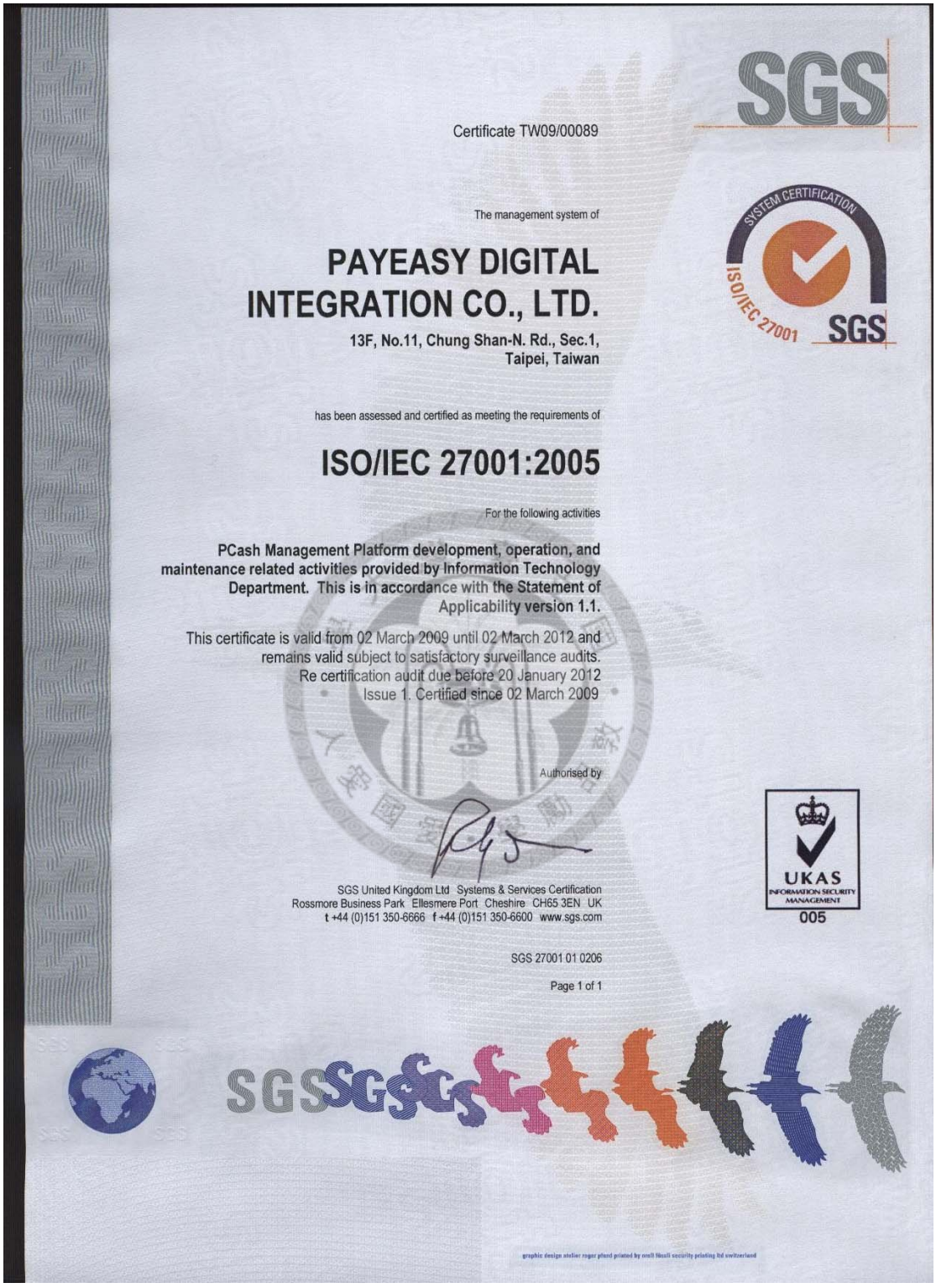
當事情發生的時候,
我們可以採取隱匿不報..反正我們沒有損失.
或者是報案,要求警方不公開..至少完成報案流程.
我們選擇最困難的方案，也是最傻的方法，通報銀行，通知警方，媒體公開

我認爲一家企業，
當你明知將有事件發生會嚴重傷害到他人的生命與財產安全的時候,縱使與您沒有相關，
一家有良知的企業絕不會選擇袖手旁觀。
這一年來，對於同業姑息，隱忍的態度造成詐騙集團食髓知味，爲之坐大，
對於爲數上千成萬的無辜受害者，
這些漠視不管的同業,儼然成爲詐騙集團的幫兇，

讓我們自豪的是，到目前爲止 Payeasy 沒有一位會員被詐騙集團詐騙得逞，
由於我們不計代價的維護會員權益，
由於我們對於社會正義仍有一絲絲的寄望，
去年年底我們挺身孤單的對抗詐騙集團,保護會員
昨天我們爲了守護 1000 多名無辜的持卡人,再次迎戰。
明日如有同類型的事件發生，我們還是會做同樣選擇,
因爲這是深植入 PayEasy 所有同仁的信念，
我相信我們同仁面對自己，面對家人，面對同業，面對社會時，我們會驕傲的說，
我以身爲 PayEasy 的一員爲榮。

[redacted]

附錄 23　ISO27001 認證



SGS

Certificate TW09/00089

SYSTEM CERTIFICATION ISO/IEC 27001 SGS

The management system of

PAYEASY DIGITAL INTEGRATION CO., LTD.

13F, No.11, Chung Shan-N. Rd., Sec.1,
Taipei, Taiwan

has been assessed and certified as meeting the requirements of

ISO/IEC 27001:2005

For the following activities

PCash Management Platform development, operation, and maintenance related activities provided by Information Technology Department. This is in accordance with the Statement of Applicability version 1.1.

This certificate is valid from 02 March 2009 until 02 March 2012 and remains valid subject to satisfactory surveillance audits.
Re certification audit due before 20 January 2012
Issue 1. Certified since 02 March 2009

Authorised by

UKAS INFORMATION SECURITY MANAGEMENT 005

SGS United Kingdom Ltd Systems & Services Certification
Rossmore Business Park Ellesmere Port Cheshire CH65 3EN UK
t +44 (0)151 350-6666 f +44 (0)151 350-6600 www.sgs.com

SGS 27001 01 0206

Page 1 of 1

graphic design atelier roger pfund printed by orell füssli security printing ltd switzerland