洪嘉慶、黃正魁、古政元（2018），『資訊安全新聞事件與企業股價異常報酬之研究』，*中華民國資訊管理學報*，第二十五卷，第三期，頁 283-306。

資訊安全新聞事件與企業股價異常報酬之研究

洪嘉慶*
國立中正大學資訊管理學系

黃正魁
國立中正大學企業管理學系

古政元
國立交通大學資訊管理研究所

摘要

隨著資訊科技與網路應用的快速發展，企業已開始利用它們來提升組織內部與外部之間的溝通效率，但這也同時產生了資訊傳遞、個人資料保護與資訊安全的相關問題，因此企業在進行資訊化的當下其實亦面臨著潛藏之風險。另外，當網路與電腦計算能力提升的同時，駭客與惡意程式攻擊的傷害衝擊也隨之增加，如果企業的重要資料被竊取或洩漏，除了會重創企業的形象之外，也可能會影響公司的營運，並造成公司財務上的損失。因此，本研究希望透過資訊安全新聞事件的蒐集以及事件研究法的分析，找出資訊安全新聞事件與企業股價的關聯性，也就是希望瞭解當企業發生資訊安全事件時，是否會產生異常報酬？接下來透過統計方法來探討其顯著性，再將蒐集到的新聞事件依產業別進行分類，研究不同產業別是否產生不同的異常報酬？對於資訊安全事件的敏感程度是否也有所差異？研究結果顯示，資訊安全事件會讓企業產生短期的異常報酬，多在事件日當天與後一天，而不同的產業對於資訊安全事件的反應也有所不同。

關鍵詞：資訊安全新聞事件、事件研究法、市場價值、異常報酬

* 本文通訊作者。電子郵件信箱：morris.hung@gmail.com
2017/09/10 投稿；2017/12/05 修訂；2018/04/01 接受

Hung, C.C., Huang, C.K. and Ku, C.Y. (2018), 'Research on abnormal return of enterprise stock price for the information security news', *Journal of Information Management*, Vol. 25, No. 3, pp. 283-306.

Research on Abnormal Return of Enterprise Stock Price for the Information Security News

Chia-Ching Hung*
Department of Information Management, National Chung Cheng University

Cheng-Kui Huang
Department of Business Administration, National Chung Cheng University

Cheng-Yuan Ku
Institute of Information Management, National Chiao Tung University

Abstract

Purpose－To investigate the impact of information security news on corporate stock price, this study analyzes the degree of influence and also the response time lag in various industries.

Design/methodology/approach－In order to find out the relevance between information security news and corporate stock price, this study adopts event study method. Real information security news and the corresponding stock prices were collected. With the statistical methods, we tried to explore whether there will be abnormal return when the information security news appeared. In addition, we examine whether there will be differences in abnormal return or sensitive level of information security news by categorizing the events in disparate industries accordingly.

Findings－The research result demonstrates that the information security news will cause short-term abnormal return of stock price in the day of incident and the next day. Furthermore, the reaction to the information security events will vary in different industry.

* Corresponding author. Email: morris.hung@gmail.com
2017/09/10 received; 2017/12/05 revised; 2018/04/01 accepted

Research limitations/implications－Recently, the transmission of information security news not only depends on news media, but also on social media. Nevertheless, the research model which is suitable for collecting and analyzing on this aspect has not been formulated. It cannot be inferred that whether it will influence the investor to have different investment decision when they acquire the information this way. In the future, the transmission methods should be included in the research for analysis.

Practical implications－With the advancement of information technology and development of network applications, it is a very important issue for enterprises to reduce operational risk which is brought about by information technology. If the information security incidents lead to user information leakage, it will cause damage to enterprise image. Through this research result, enterprises should pay more attention to maintenance of information security.

Originality/value－By analyzing the recent news, the occurrence of information security incidents causes short-term abnormal return of enterprise stock price. Moreover, in different industry, such as Consumer Discretionary, Financials and Information Technology, the level of abnormal return is very different.

Keywords: information security news, event study method, market value, abnormal return

壹、緒論

近年來，隨著網際網路及雲端建設的普及，企業開始利用資訊系統來提升企業內部與外部之間的執行效率，也因此衍生了許多的資訊科技管理的問題；當企業的營運資訊，在組織內甚至於跨組織的快速傳遞時，除了帶來高效率，如何保障這些資訊的完整性、機密性及可用性等資訊安全特性也就成為資訊化企業必須加以考慮的問題（Mohr 1996）。除此之外，隨著網路傳輸與電腦計算能力的提升，駭客與惡意程式的攻擊與危害能力也跟著逐年增加，相關資訊安全的維護也更加顯的重要。2011 年的 Sony PlayStation Network 用戶個人資料外流，2013 年 Adobe 的網站遭駭客入侵，竊走用戶的帳戶資料，這些資訊安全事件在在都嚴重影響了企業的外在形象，並降低了使用者對於企業網站和系統的使用信心，也造成了公司巨大的損失，因此益發導致愈來愈多的企業開始重視資訊安全之議題。

資訊安全之漏洞所造成公司的實際損失其實是多方面的，除了營業額的減少之外，無形損失更為巨大，例如：因為資訊安全防護未做完善，發生客戶信用卡資料外流，因而導致消費者信心與信任的喪失，這些無形資產的損失，常常遠遠超過其他營運業務上的損失。此外，也有一些研究結果顯示企業資訊系統安全跟系統開發與創新和公司股價的波動有頗為密切的關連（DeFond et al. 2010; Dos et al. 1993; O'Leary 2010）。

在資訊安全與股價波動的相關研究中，大部分都使用事件研究法（Event Study）來找出相關事件新聞的發生是否會造成公司股價的上漲或下跌。所謂事件研究法是當市場接收到新的新聞消息時，投資人是否會有連動的反應，其研究目的在探討當某一事件發生時，是否會引起企業股價的異常變動（劉書助 & 林宜學 1997）？並進一步產生異常之報酬（Abnormal Returns; AR）。這些相關事件可用來瞭解股票市場價格與特定事件是否有關聯性，也因此事件研究法經常被應用於資訊技術、財務金融、會計與管理等相關領域的實證研究（Arya & Zhang 2009; Carow et al. 2004; Chen et al. 2009; Konchitchki & O'Leary 2011; Wang et al. 2013; 葉鎮源等 2014）。除此之外，也有許多的論文以事件研究法探討大數據（Huang et al. 2016）、資訊應用（Dos Santos et al. 1993; Son et al. 2014）及企業智慧系統（Rubin & Rubin 2013）等議題。

貳、相關背景與文獻探討

一、事件研究法

在近代的商管領域之研究方法當中，事件研究法為廣泛被使用的方法之一，

其目的主要在探討當企業發生某一重大事件時，其公司的股價是否會產生變動。目前已被廣泛應用於金融和管理領域相關新聞事件的研究包括：企業購併，高級主管的人事變動以及資訊系統更新與維護……等，由相關研究的結果可以得知這些新聞或重大事件的發佈對於企業股價多有影響（Ball & Brown 1968; Chaney et al. 1991; Das et al. 1998; Konchitchki & O'Leary 2011; MacKinla 1997; McWilliams & Siegel 1997; Wang et al. 2013），此外也有一些研究探討資訊安全與企業股價的關係（Wang et al. 2013）。

雖然每個領域使用事件研究法有著不同的方式，不過基本的實施步驟大體說來是一致的，首先要先定義要研究之新聞事件的類別，例如：企業併購事件、資訊安全事件等，接下來透過相關新聞的資料庫檢索，確認新聞事件的事件日，並同時檢索是否有其他因素會交互影響，如果有，則此新聞事件需要排除，然後定義估計期、事件窗口與估算異常報酬率，之後再利用統計方法進行檢定，最後由檢定結果進行相關相關分析與討論。綜上所述，事件研究法的實施步驟可以整理如表 1。

表 1：事件研究法的步驟

步驟	說明
1. 事件定義	研究人員必須準確地選擇一個事件及一個時間段，之後對於其間的股票價格進行評估。事件的時間週期稱為事件窗口（Event Window），事件窗口長度必須充足以便涵蓋事件發生前和發生後的股價。
2. 選擇新聞的樣本和來源	研究人員開始收集符合定義的事件，同時必須確定採樣週期長度，例如：2010-2014 年。一般情況下，週期長度愈長可以收集到更多的新聞事件，而新聞來源可以由相關的新聞資料庫中進行檢索與蒐集，例如：LexisNexis 和 Factiva 等。除此之外，須留意蒐集的新聞事件期間是否有混淆效應（Confounding Effect）發生，如果有，則此事件必須被剔除。
3. 分析正常（Normal）和異常報酬（Abnormal Returns）	感興趣的新聞事件的影響，是通過測量異常報酬（Abnormal Returns）來確定的。異常報酬是指股票實際投資收益扣除正常收益後的股票收益。在（Brown & Warner 1980）的研究中列出三種衡量股票報酬的方法，分別為平均調整模式（Mean Adjusted Returns Model）、市場調整模式（Market Adjusted Returns Model）和最小平方市場模式（Ordinary Least Square Market Model）。
4. 估計程序	估計窗口（Estimation Window）被用來確定預期的正常收益。研究人員建議使用估計期之前，需確定估計窗口內不得含有事

	件，以確保正常收益的估計。
5. 測試程序	取得異常報酬率的計算結果。建立測試異常報酬的框架，其中包括虛無假設的定義以及個別公司的異常報酬。
6. 實證結果	依據實驗設計的程序產出結果，並運用表格或圖形報表等方式來呈現。
7. 結論	事件研究方法的目的是提供相關的實證結果以探索定義的事件是否會影響股票價格？

二、資訊安全事件研究法

當企業發生資訊安全事件時，往往會造成企業重大的損失，例如：2011 年 Sony Play Station Network 遭受到駭客攻擊，遭駭客竊走用戶個人資料及信用卡付款資訊，估計造成企業損失 10 億美元，諸如此類的事件一再地警示企業應該加強資訊安全的維護，以讓資訊系統可以更加安全地運作。

資訊安全事件與事件研究法的相關研究包括從：企業資訊安全策略（Siponen 2006; Straub Jr. 1990）、資訊安全投資（Gal-Or & Ghose 2005; Schecter & Smith 2003）以及高層管理團隊與資訊安全管理相關議題（Kwon et al. 2012）等面向進行探討，而在 Wang 等學者（2013）的研究中曾提到，媒體報導是一個獲取訊息的重要來源，如各大報章媒體及部落格等都是，當一個企業資訊安全漏洞的訊息在媒體上傳出時，極有可能造成短期內股票交易的數量、金額與價格異常。

在 Gordon 等學者（2010）的研究中，便說明了隨著科技演變和電子商務的發展，資訊安全變得尤其重要，而且企業也越來越願意投資許多預算在資訊安全的維護上，並且充份揭露相關訊息給投資大眾知道（Gordon et al. 2010），其研究使用了表 2 的資訊安全關鍵字以在企業年度報告中進行搜尋：

表 2：Gordon 等學者 2010 年研究使用的關鍵字

Access Control	Cyber Security	Network Security
Authentication	Cybersecurity	Security Breach
Business Continuity	Denial of Service	Security Expenditure
Computer Breach	Disaster Recovery	Security Incident
Computer Intrusion	Encryption	Security Management
Computer Security	Hacker	Security Measure
Computer System Security	Information Security	Security Monitoring
Computer Virus	Infosec	
Cyber Attack	Intrusion	

Wang 等學者（2013）的研究中，就是分析資訊安全事件對於公司股價的影響，當一個企業傳出資訊安全漏洞的訊息時，有可能會造成短期內股票交易量的異常與股價的波動，此異常便可稱之為異常報酬，因此投資者在投資前必須了解資訊安全漏洞如何影響一個公司的未來營收，讓自己能夠做出正確的投資決策。投資者能夠取得資訊來源最主要的管道便是報章媒體，例如: Wall Street Journal、USA Today、Washington Post 和 New York Times 等（Wang et al. 2013）。表 3 為 Wang 等學者（2013）檢索新聞時所使用的關鍵字：

表 3：Wang 等學者 2013 年研究使用的關鍵字

Computer attack	Hacker
Computer Break-in	Identity Theft
Computer Security	Network Intrusion
Cyber Fraud	Phishing
Cyber-attack	Security Breach
Data Theft	Virus (or Worm）
Denial of Service	

以上的研究結果多顯示企業如果沒有做好資訊安全的相關維護措施，當資訊系統發生重要資料外洩、服務中斷……等問題時，對於企業的無形商譽與實體價值都會造成莫大的傷害。表 4 為資訊安全事件股價衝擊之相關研究論文所使用的新聞年份區間、新聞筆數以及主要研究成果的摘錄整理。

表 4：資訊安全事件相關研究整理

作者	新聞年份區間	新聞數量	主要研究成果摘錄
Campbell et al. 2003	1995-2000	43	資訊安全事件對於市場股價是有負的異常報酬
Cavusoglu et al. 2004	1996-2001	66	資訊安全事件對於受影響公司是負的異常報酬，而在做資訊安全的廠商則是在事件日和事件日後一天有正的異常報酬
Hovav, A. and D'Arcy, J. 2005	1988-2002	92	市場很難懲罰有漏洞的資訊產品，不過市場對於資訊產品中含嵌入式病毒（embedded viruses）會給予懲罰

Andoh-Baidoo and Osei-Bryson, 2007	1997-2003	41	資訊安全事件對於網路公司的影響遠大於非網路公司
Liginlal, D. et al. 2009	2005-2008	151	由美國境內所發生的隱私洩漏事件，利用事件研究法分析有負的異常報酬產生。
Gatzlaff K.M. and McCullough K.A. 2010	2004-2006	77	企業如果發生資料外洩事件，對於公司股價在事件日和事件日後一天會產生負的異常報酬
Smith et al. 2011	2000-2005	10	網路犯罪的成本遠超出被盜取的資產；網路犯罪對公司股價有負的異常報酬
Chen, J. et al. 2012	2006-2007	83	當公司發生資訊安全事件時，資訊安全諮詢相關的企業會有正的異常報酬產生
Wang et al. 2013	1997-2008	89	研究證明在資訊安全事件所產生負的異常報酬時間中，存在著短期投資者有利的機會
Pirounias et al. 2014	2008-2012	105	資訊安全事件對企業在事件日當日和當天有負的異常報酬產生，而在資訊產業的損失遠大於非資訊產業的損失
Modi et al. 2015	2005-2010	146	分析因為資訊委外廠商的疏失所造成的資料外洩，對於原本企業會有負的異常報酬產生

三、假說建立

在早前相關的研究當中，已有許多的文獻在找出資訊科技應用與投資是否會影響企業的股價，例如：Acquisti 等學者（2006）的論文中，探討企業因為資訊系統漏洞，造成客戶隱私權的危害時，是否會影響公司的股價，資料搜集的年份從 2000 年到 2006 年，研究結果為事件日的前一天有異常報酬的產生。另外在 Andoh-Baidoo 等學者（2007）這篇論文中，則是探討網路資訊安全的威脅事件，資料搜集的年份是 1997 年到 2003 年，研究結果顯示事件日的前一天與後一天都有異常報酬的產生，Hinz 等學者（2015）的論文則探討資料竊取對於公司股價是否會有影響，資料搜集為 2011 年到 2012 年，他們發現如果是重要的客戶資料被竊取，則股價影響的時間相對較長，如果是一般的資料遭盜取，則影響時間較短，而事件日的後三天內都有可能有異常報酬的產生。

由以上所提及之論文都已證明了資訊安全事件會造成企業的股價波動，進而產生異常的報酬，然而這些研究的新聞來源與股價都較舊，多是 2008 年以前或在 2011 年到 2012 年之間，事實上近幾年由於行動商務和金融科技（FinTech）的快速發展與日新月異，再加上網路新聞傳播的速度更快，資訊安全事件及延伸問題衝擊企業與個人的層面更廣更大，其影響力更超乎以往的想像，所以本研究希望能蒐集較新的新聞來源（2009 年-2015 年），透過事件研究法與統計工具來找出是否仍然會有異常報酬的產生，或者觀察在創新資訊科技充斥的當前是否會有其它不一樣的結果？因此，本研究設立了第一個假說。

假說一：企業發生資訊安全事件新聞報導時，會有異常報酬的產生。

近年來資訊安全與資訊應用相關的事件研究法論文當中，產生異常報酬的時間點多在事件日前後 1-3 天之內，詳如表 5 所整理。從表 5 中可以得知資訊安全事件在短時間會造成企業一定的衝擊，進而產生異常報酬。如果企業資訊安全危機在短期之內處理得當，應該可以將傷害降至最低，並縮短事件影響的時程。近年來，隨著企業資訊系統與網路的廣泛應用，加上許多歷史經驗的教訓，大型企業越來越重視資安，並且對資安事件的處置也多已建立一套標準的處置程序，因此，本研究提出第二個假說，認為異常報酬的風險是短期的，不會長期持續影響投資人的想法。

假說二：資訊安全事件影響股價的事件期多為短期衝擊。

表 5：相關研究論文產生異常報酬的日期

論文作者	主題	異常報酬的影響日
Acquisti 等（2006）	隱私權	（-1,0）
Andoh-Baidoo 等（2007）	資訊安全威脅	（-1,1）
Wang 等（2013）	資訊安全威脅	（-1,1）
Hinz 等（2015）	資料竊取	（0,3）

另外，在之前的研究論文當中，一篇論文多半只探討一種行業，例如：Hinz 等學者（2015）這篇論文，就只研究資料竊取對於消費型電子商務企業的影響。然而，在各種行業中，因為經營模式的不同，對於資訊涉入的程度也不同，不同的產業別，對於資訊安全事件的反應強度應該會不一樣，例如：在 Andoh-Baidoo 等學者（2012）所做的研究當中，將公司類別分成網路與非網路公司，個別地進

行分析研究，研究結果顯示，不同的企業類別，對於事件的反應程度也會有不同。除此之外，如果產業類別之營運核心和資訊科技高度相關的話，發生了資訊安全事件，應該對於企業的衝擊與影響會較為明顯，因此本研究設立了第三個假說。

假說三：不同產業別，對於資訊安全事件會產生不一樣的異常報酬。

參、研究方法

一、研究流程

本研究先由蒐集資訊安全新聞事件開始，再分析新聞內容，最後以事件研究法找出關聯性，其完整研究流程如圖 1：

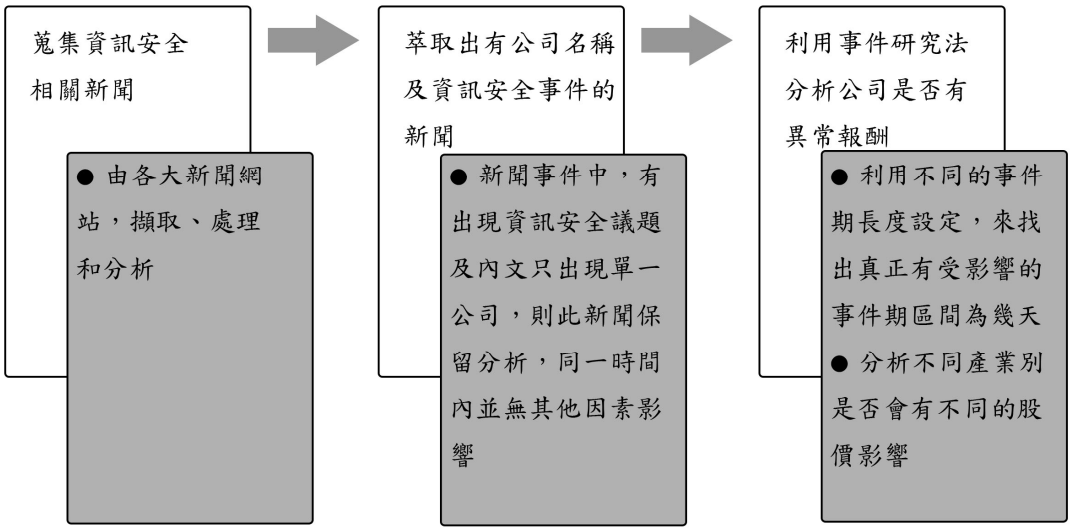

圖 1：資訊安全新聞事件分析步驟

二、資料蒐集與選擇

由於之前論文所使用的資料集範圍多在 1998 年到 2012 年這段期間裡，但隨著資訊科技的快速發展，舊有的攻擊事件與資訊安全問題可能與現今所存在的問題不符，進而引發的市場反應也會有不同，因此，對於資訊安全新聞的蒐集，我們蒐集了 2009 到 2015 年的新聞事件資料來進行研究。

資訊安全事件的蒐集是從 Factiva 資料庫中找尋有關於資訊安全的相關新

聞，從以前學者研究中所使用到的關鍵字（Campbell et al. 2003; Wang et al. 2013），加上資訊安全管理系統認證 ISO 27001 中的關鍵字，最後整理與新增出表 6 本研究使用的關鍵字：

表 6：本研究所使用搜尋資訊安全新聞的關鍵字

Computer Attack	Computer Worm	Identity Theft
Computer Breach	Cyber Fraud	Network Intrusion
Computer Break-in	Cyber-attack	Phishing
Computer Intrusion	Data Theft	Security Breach
Computer Security	Denial of Service	Security Controls
Computer Virus	Hacker	Security Incident

在事件樣本的選取標準上，我們採取了以下五個基本準則去進行樣本的篩選，茲詳述如下：

1. 檢索到的新聞事件中必須是標準普爾 500 中的企業（S&P 500）；
2. 以美國各大報新聞為主要的蒐集目標；
3. 事件發生日前需有連續 180 天以上的交易紀錄；
4. 排除混淆作用，也就是公司在資訊安全事件期間，不能有其他影響估計的事件發生，例如：公司併購，財報，高層人事異動等因素，如果有發生類似事件則此新聞不列入研究使用，避免產生異常報酬認知的混淆；
5. 資訊安全事件以第一筆報導新聞當天做為事件日。

三、事件研究法異常報酬計算與檢定

事件研究法中對於事件與股票價格影響的估計方法有很多，其中以市場模式（Market Model）最被廣泛使用。市場模式最早使用在估計企業的正常報酬率，並探討市場整體因素對於企業的影響，其方法為利用市場模式將估計期的資料，以最小平方市場模式（Ordinary Least Square; OLS）建立個別股價之迴歸模型（Sharpe 1964），公式如下：

$$R_{it} = \alpha_i + \beta_i R_{mt} + \varepsilon_{it}$$

其中 $t = t_i, ..., t_2$ 和 $i = 1, 2, ..., n$ 且 a_i 和 β_i 為估計參數，ε_{it} 為誤差項，R_{mt} 為 t 期的市場報酬率。

計算完收益率（rate of return）後，可以利用事件日 i 來估算企業的異常報酬（abnormal return），公式如下：

$$AR_{iE} = R_{iE} - (a_i + b_i R_{mE})$$

其中 AR_{iE} 為在事件期 E 中 i 公司的異常報酬率，a_i 和 b_i 為估計參數，R_{mE} 為 t 期的市場報酬率，R_{iE} 為公司在估計期之實際報酬率。

研究過程中必須計算股價預期報酬率為何，所以必須根據一段時間期來建立預期模型，此一時間區間就稱為估計期，如圖 2 中的 t_a 到 t_b，此外，事件發生日的前後也必須設定一個區間以分析事件會影響多久，這段區間則稱為事件期或事件窗口，如圖 2 中的 t_m 到 t_n，最後利用實際報酬率來減掉預期報酬率，就可以得到此一事件所產生的異常報酬率。估計期的長度，目前並無客觀的標準，太短的估計期可能會影響預期模式的預測能力，太長的估計期可能造成事件資料發生改變，產生不穩定的現象。目前相關的文獻，若以日報酬率建立估計模型時，估計期通常可設為 100 天至 300 天不等（Dobij et al. 2010; Konchitchki & O'Leary 2011; McWilliams & Siegel 1997; Wang et al. 2013; Wang et al. 2013），因此本研究取中間值，訂為 180 天。

在之前學者的研究中，常將事件發生日定義為 $t = 0$，事件發生日的前一天定義為 $t = -1$ 天，前二天定義為 $t = -2$ 天；事件發生日後則為 $t = +1$ 天，後二天為 $t = +2$ 天，以此類推（Konchitchki & O'Leary 2011）。太長的事件窗口容易造成無法確認受影響的真實事件為何，而影響檢定結果，中等長度的事件窗口可以有足夠之觀察並避免摻雜了其他的混淆事件，例如：公司財報公布或企業購併……等，因此是相對較好的設定，所以本研究將事件窗口設為（-10,+10）。

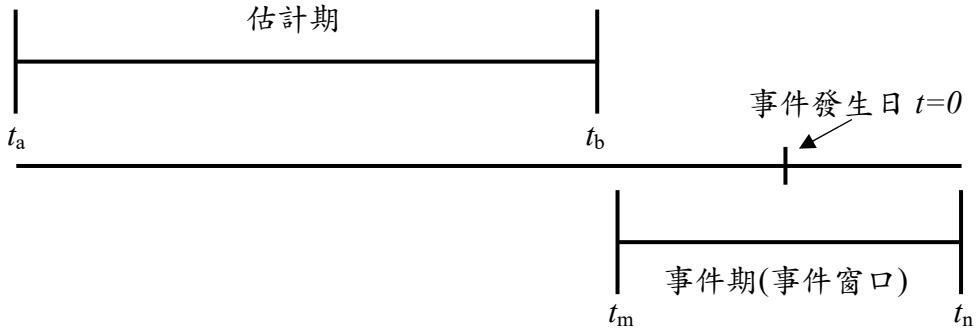

圖 2：估計期與事件期之時間圖

接下來可以由上述式子得到的相關異常報酬，計算出平均異常報酬 AR_E（average abnormal return）（McWilliams & Siegel 1997），公式如下：

$$AR_E = \frac{1}{N} \sum_{i=1}^{N} AR_{iE}$$

其中 N 為公司的數量。

除此之外也可以透過已求取的資訊，得到 T_1 到 T_2 期間的累積異常報酬 CAR（cumulative abnormal return）（McWilliams & Siegel 1997），公式如下：

$$CAR(T_1,T_2)=\sum_{E=T_1}^{T_2} AR_E$$

在計算完 AR 和 CAR 後，事件研究法中最後是需要透定檢定的方式來找到事件日與異常報酬是否有顯著的差異，傳統 t 檢定法（Brown & Warner 1985）公式如下：

$$t_{TM}^{AR}=\frac{AR_E}{\frac{1}{N}\sqrt{\sum_{i=1}^{N}\hat{s}_i^2}} \text{ 且 } \hat{S}_i^2=\sum_{t=1}^{T}(\hat{\varepsilon}_{it}-\bar{\hat{\varepsilon}})^2/(T_i-1) \text{ 和 } t_{TM}^{CAR}=\frac{\sum_{i=1}^{N}[\sum_{t=t_1}^{t_2}(\frac{AR_{iE}}{\hat{S}_i})/\sqrt{m}]}{\sqrt{N}}$$

AR_E 為 E 天裡的平均異常報酬，可以利用公式計算，例如：$AR_E=\frac{1}{N}\sum_{i=1}^{N}AR_{iE}$，$\hat{S}_i^2$ 是估計期之殘差變異數，T_i 為估計期間內的個數，m 是累積期間內的天數。

除了傳統 t 檢定法外，本研究還使用了標準化殘差法（Standardized-Residual Method）來檢定（Patell 1976），在檢定前需先將個別公司的異常報酬率標準化，讓個別公司的異常報酬率成為單一常態分配，標準化異常報酬（SAR_{iE}）的計算如下：

$$SAR_{iE}=\frac{AR_{iE}}{\hat{S}_i\sqrt{1+\frac{1}{T_i}+\frac{(R_{mE}-\bar{R}_{mi})^2}{\sum_{T=\tau_1}^{t_2}(R_{mT}-\bar{R}_{mi})^2}}}$$

接下來再由標準化殘差法的公式來檢定，公式如下：

$$t_{SRM}^{AR}=\frac{\sum_{i=1}^{N}SAR_{iE}}{\sqrt{\sum_{i=1}^{N}\frac{T_i-2}{T_i-4}}}$$

和

$$t_{SRM}^{SCAR} = \frac{\sum_{i=1}^{N}\sum_{E=T_1}^{T_2}\left(\frac{SAR_{iE}}{\sqrt{m}}\right)}{\sqrt{\sum_{i=1}^{N}\frac{T_i-2}{T_i-4}}}$$

透過這兩種檢定法，來探討資訊安全事件是否會對公司股價有影響並且產生異常報酬。

肆、資料分析

一、事件樣本篩選與分類

在新聞事件的選擇上，我們使用了之前所提到的資訊安全關鍵字在 Factiva 上搜尋，搜尋的新聞以美國主要大報為主，詳如表 7 所列：

表 7：本研究所使用之美國各大報

The New York Times	Washington Post	San Jose Mercury News
USA Today	Los Angeles Times	The Washington Post
New York Daily News	New York Post	Chicago Tribune
Chicago Sun-Times	The Denver Post	The Wall Street Journal
The Dallas Morning News	Newsday	The Orange County Register
Houston Chronicle		

總共所搜尋到的新聞事件如表 8 所示，有出現搜尋關鍵字的新聞筆數總計有 3846 筆新聞，然而必須扣除重複之新聞條目 761 筆，所以最後實際可用的新聞數量為 3085 筆。

表 8：初步篩選後的新聞筆數

關鍵字	總筆數	可用筆數	重複新聞項目
Computer Attack	26	20	6
Computer Breach	16	15	1
Computer Break-in	0	0	0
Computer Intrusion	13	10	3
Computer Security	668	529	139
Computer Virus	63	50	13

Computer Worm	30	22	8
Cyber Fraud	1	1	0
Cyber-attack	157	142	15
Data Theft	134	110	24
Denial of Service	200	156	44
Hacker	964	786	178
Identity Theft	753	591	162
Network Intrusion	1	1	0
Phishing	326	256	70
Security Breach	427	348	79
Security Controls	46	33	13
Security Incident	21	15	6
總計	3846	3085	761

接下來將搜尋到的結果依據新聞內容來判斷是否為資訊安全事件，並且在新聞中所報導的對象為 S&P 500 的公司，同時也要確認是否有其它混雜事件的影響，而混雜事件之篩選程序如下：

1. 於 Factiva 新聞資料庫中搜尋該企業在事件發生日前後一段時間內是否也有其他重大新聞事件揭露，如：公司併購，財報揭露或高層人事異動等可能會影響股價之事件，一旦發現有這些事件時，則該筆案例剔除，不列入考量。
2. 利用 Google 搜尋，再次確保當下是否有非研究事件發生。

經過這些程序篩選後總計有 162 筆新聞事件符合檢定之要求，這些事件的年份分布如表 9 所列。

表 9：由內容分析與混雜事件排除後符合檢定要求的新聞筆數

年份	數量	年份	數量
2009	15	2013	18
2010	37	2014	33
2011	22	2015	8
2012	29	合計有 162 筆新聞	

在這 162 筆新聞事件中，共影響到 45 間 S&P 500 的公司，我們再將這些公司依照行業類別統計區隔並得到圖 3，其中以資訊科技（Information Technology;

IT）、財金（Financials）與非必需性消費（Consumer Discretionary; CD）等三個產業占較大部分。

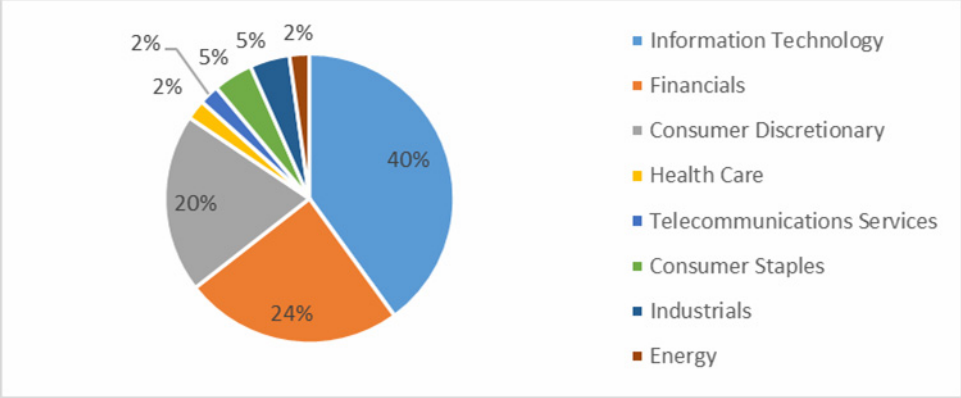

圖 3：新聞事件公司的行業類別

伍、分析結果

一、異常報酬計算與檢定

為了驗證假說一：企業發生資訊安全事件時，會有異常報酬的產生與假說二：資訊安全事件影響股價的事件期為短期。首先將蒐集到的 162 筆新聞與股價進行異常報酬與檢定計算，事件窗口設為[-10, 10]，估計期為 180 天，得到表 10 的結果，結果顯示事件日後一天的平均異常報酬為-0.00214，也就是資訊安全新聞事件讓企業產生負的異常報酬，而在傳統 t 檢定中，事件日後 1 天的 t 值為-2.51，P 值為 0.0131，標準化殘差法中 t 值為-2.97，P 值為 0.003462426，計算結果皆為顯著，在事件日後 2 天裡標準化殘差中 t 值為 2.23，為 P 值為 0.027194395 也為顯著，之後的數值在事件後第 6、8 和 9 天，雖然也有稍顯著之結果，但因為和事件日相隔較遠，且股價在事件後第二天多已回穩，所以有可能是摻雜了其他非新聞報導或隱性之混雜事件，所以不予考量。由這些實驗結果可以驗證假說一：企業發生資訊安全事件時，會有異常報酬的產生，也同時驗證了假說二：資訊安全事件影響股價的事件期多為短期影響，圖 4 則為事件期間企業股價的平均異常報酬圖。

表 10：平均異常報酬、傳統 *t* 檢定和標準化殘差法檢定結果

事件日	新聞筆數	平均異常報酬（%）	標準差	傳統 t 檢定	標準化殘差法
-10	162	0.000953	0.017391	0.7	0.68
-9	162	-0.00057	0.012463	-0.58	-0.37
-8	162	-0.00053	0.01217	-0.56	-0.39
-7	162	0.000293	0.0127	0.29	0.82
-6	162	-0.00051	0.016119	-0.4	-0.05
-5	162	-0.00167	0.01615	-1.32	-2.74***
-4	162	0.001379	0.013438	1.31	0.81
-3	162	-0.00012	0.012967	-0.12	0.31
-2	162	-0.0002	0.011417	-0.23	-0.83
-1	162	-0.00044	0.014416	-0.39	-0.55
0	162	0.0002	0.014837	0.17	0.22
1	162	-0.00214	0.010874	-2.51**	-2.97***
2	162	0.00174	0.014141	1.57	2.23*
3	162	-0.00068	0.01466	-0.59	-1.28
4	162	-0.00029	0.014945	-0.25	-0.06
5	162	-0.0017	0.013769	-1.57	-0.78
6	162	-0.00202	0.017384	-1.48	-3.09***
7	162	-0.00114	0.012772	-1.13	-1.25
8	162	0.001956	0.015479	1.61	2.48**
9	162	-0.00216	0.013369	-2.06**	-3.36***
10	162	-0.00062	0.013967	-0.56	-0.95

註：***表示 p-value 小於 0.01；**表示 p-value 小於 0.05；*表示 p-value 小於 0.1

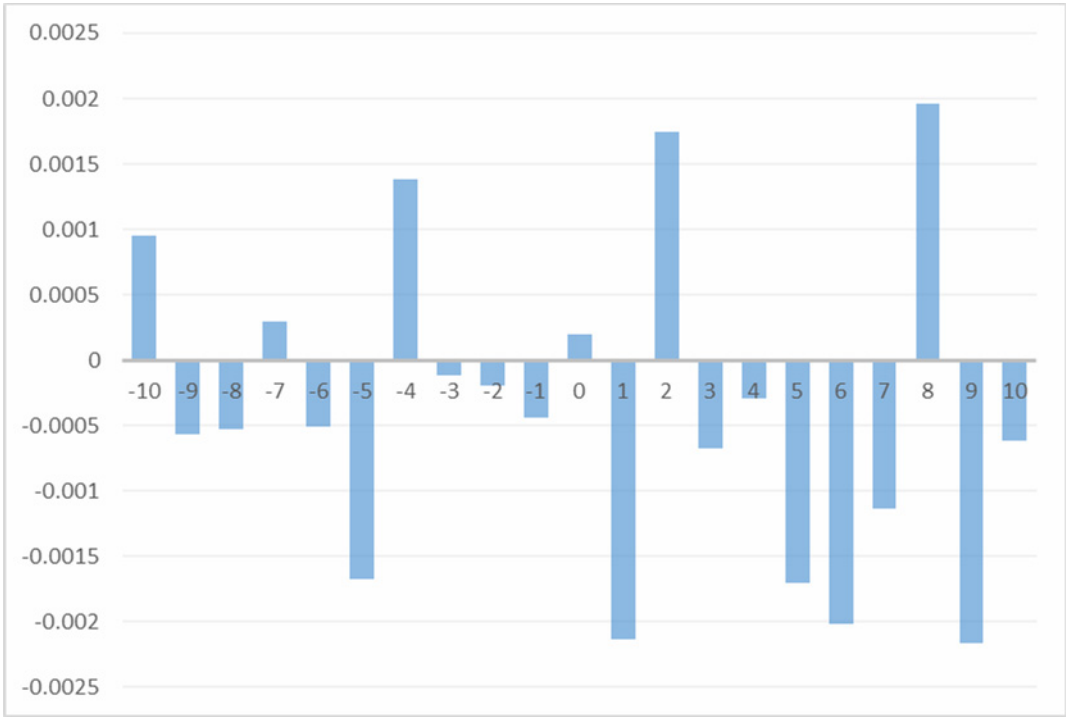

圖 4：事件期間企業股價的平均異常報酬圖

二、不同產業別的平均異常報酬計算

由上述的分析結果得知資訊安全新聞事件對於企業會產生負的異常報酬，但在不同產業間是否會有不同的市場反應呢？為了驗證假說三：不同產業別會有不同的股價影響。所以本研究將樣本數較多的 3 個產業再計算平均異常報酬，以了解是否會因產業別不同而有不同的市場反應。表 11 為非必需性消費產業的平均異常報酬計算，樣本數為 29 個，在非必需性消費產業的結果中得知市場對於新聞市場反應較快速，在事件日當天即有負的異常報酬產生。

表 11：非必需性消費產業的平均異常報酬表

事件日	平均異常報酬（%）	標準差	最小值	最大值	t-value
-5	0.0047259	0.0201315	-0.02086	0.0719	1.26
-4	-0.0010803	0.0113588	-0.02313	0.03491	-0.51
-3	0.0023693	0.0108849	-0.01765	0.03056	1.17
-2	-0.0020376	0.0099475	-0.02978	0.01187	-1.10
-1	0.000265862	0.0155724	-0.03462	0.0374	0.09
0	-0.0023828	0.0167671	-0.04246	0.03623	-0.77

1	0.000322759	0.0080086	-0.02057	0.01793	0.22
2	-0.000229655	0.0076434	-0.01977	0.01499	-0.16
3	0.0010528	0.0112644	-0.02349	0.03049	0.50
4	0.002169	0.0224386	-0.0847	0.05657	0.52
5	-0.0017017	0.0129139	-0.0388	0.02216	-0.71

表 12 為財金的平均異常報酬計算，樣本數為 36 個，在財金產業中，在事件日後一天有負的異常報酬產生。

表 12：財金產業的平均異常報酬表

事件日	平均異常報酬（%）	標準差	最小值	最大值	t-value
-5	-0.0051019	0.0113255	-0.03561	0.01615	-2.70
-4	0.000355278	0.0125281	-0.03238	0.03138	0.17
-3	-0.000942222	0.016253	-0.0503	0.04958	-0.35
-2	-0.000016667	0.0149226	-0.02907	0.05242	-0.01
-1	0.000333333	0.0104386	-0.01762	0.0277	0.19
0	0.0005275	0.0121915	-0.04384	0.01726	0.26
1	-0.0021658	0.0113493	-0.04034	0.0172	-1.15
2	0.0050286	0.017249	-0.02348	0.07041	1.75
3	-0.0012553	0.0147745	-0.05203	0.03313	-0.51
4	-0.0030481	0.0137677	-0.04264	0.03203	-1.33
5	0.000992222	0.0135711	-0.02652	0.05096	0.44

表 13 為資訊科技產業的平均異常報酬計算，樣本數為 83 個。在資訊科技產業中，在事件日後一天有負的異常報酬產生。由以上實驗結果可知，在不同的行業別中，對於資訊安全事件的反應也會有一些不同，因此也驗證了假說三：不同產業別會有不同的股價影響。

表 13：資訊科技產業的平均異常報酬表

事件日	平均異常報酬（%）	標準差	最小值	最大值	t-value
-5	-0.0032164	0.0169138	-0.08674	0.03047	-1.73
-4	0.0026898	0.014985	-0.02796	0.07661	1.64
-3	-0.00084241	0.0123015	-0.06402	0.01735	-0.62

-2	0.000587349	0.0102385	-0.03254	0.03809	0.52
-1	-0.0017889	0.0160293	-0.07934	0.0422	-1.02
0	0.0012516	0.0161014	-0.04176	0.10414	0.71
1	-0.0029529	0.0120669	-0.03979	0.01894	-2.23
2	0.0010602	0.0150116	-0.04209	0.07603	0.64
3	-0.0010947	0.0164822	-0.08708	0.03955	-0.61
4	-0.000473373	0.0125219	-0.0374	0.02991	-0.34
5	-0.0028802	0.0147208	-0.04397	0.036	-1.78

由上述的整理可以知道表 11 的結果顯示，在非必需性消費產業裡對於資訊安全事件股價的反應較為快速，事件當日即有產生負的異常報酬，我們認為可能是因為在此類別中的企業有許多是一般民眾所熟悉的非常知名企業，如：Mcdonald's Corp.、Starbucks Corp.，因此在發生資訊安全事件時，新聞媒體會給予特別高度之關注，除此之外，也有以電子商務為主的企業，如：Amazon.com Inc.，以資訊網路為主的企業對於資訊安全事件的敏感度也比較高，因此在事件日就有負的異常報酬產生。

在表 12 的財金產業和表 13 的資訊科技產業裡，資安新聞事件的敏感度雖然也高，但沒有比非必需性消費產業來的強，所以在事件發生的後一天才產生負向的異常報酬，另外，這些比較也可以驗證前述的假說三：不同產業別會有不同的股價影響速度，也就是產生異常報酬的時間會依產業別而有快慢的差異。

陸、結論

由美國各大報 2009 年 1 月 1 日至 2015 年 12 月 31 日的資訊安全相關新聞事件進行探討，本研究獲得以下結論：

1. 根據本研究實證結果，當美國企業受到資訊安全事件影響時，投資者將會接收到相關負面的訊息，而讓企業的股價波動，進而產生負的異常報酬。
2. 由於資訊安全事件為突發事件，因此對於企業股價的波動並不會持於太長的時間。以實驗結果顯示為事件日當天或事件日後一天。
3. 在不同的產業別中，對於資訊安全事件的反應程度有所不同，有些產業較為敏感，因此會有更快的市場反應，並且都會產生負的異常報酬。

透過事件研究法的分析與統計的相關檢定，驗證了資訊安全新聞事件對於企業是有顯著的影響，並且會產生負的異常報酬，透過更進一步的檢定分析也找到最有影響的是在事件發生後的一天。

本研究成果相信會讓企業更重視資訊安全的相關工作，由平常的從業人員的

資訊安全教育訓練到企業資訊系統安全的強化，從中找到預防與解決的方法，讓企業在資訊安全的維護上能夠更加健全。對於市場反應相對敏感的產業，尤其更要做好資訊安全的維護，才能降低企業的損失。

最後，在未來研究建議上，在研究過程中，雖為周詳的蒐集新聞資料，但目前資訊安全事件的訊息傳遞上，並不一定是透過新聞媒體報導，如：社群軟體之間的傳播等，然而，這方面目前仍沒有適合蒐集與分析的研究模式出現，投資者是否會由這管道獲知消息而對投資行為產生異動尚無法推測，將來勢必需將這種訊息傳遞方式列入研究與分析。

參考文獻

葉鎮源、楊維邦、柯皓仁、鄭培成（2014），『應用語句關係網路計算語句向心性之新聞事件摘要方法』，*中華民國資訊管理學報*，第二十一卷，第三期，頁271-304。

劉書助、林宜學（1997），『在股利宣告事件效應下股價預測模式之研究』，*電子商務學報*，第二卷，第一期，頁 23-47。

Acquisti, A., Friedman, A. and Telang, R. (2006), 'Is there a cost to privacy breaches? An event study', *ICIS 2006 Proceedings*, Wisconsin, USA, Dec 10-13, pp. 1563-1580.

Andoh-Baidoo, F.K. and Osei-Bryson, K.-M. (2007), 'Exploring the characteristics of Internet security breaches that impact the market value of breached firms', *Expert Systems with Applications*, Vol. 32, No.3, pp. 703-725.

Andoh-Baidoo, F.K., Osei-Bryson, K.-M. and Amoako-Gyampah, K. (2012), 'A hybrid decision tree based methodology for event studies and its application to e-commerce initiative announcements', *SIGMIS Database*, Vol. 44, No.1, pp. 78-101.

Arya, B. and Zhang, G. (2009), 'Institutional reforms and investor reactions to CSR announcements: evidence from an emerging economy', *Journal of Management Studies*, Vol. 46, No. 7, pp. 1089-1112.

Ball, R. and Brown, P. (1968), 'An empirical evaluation of accounting income numbers', *Journal of Accounting Research*, Vol. 6, No.2, pp. 159-178.

Brown, S.J. and Warner, J.B. (1980), 'Measuring security price performance', *Journal of financial economics*, Vol. 8, No. 3, pp. 205-258.

Brown, S.J. and Warner, J.B. (1985), 'Using daily stock returns: The case of event study', *Journal of Financial Economics*, Vol. 14, No. 1, pp. 3-31.

Campbell, K., Gordon, L.A., Loeb, M.P. and Zhou, L. (2003), 'The economic cost of

publicly announced information security breaches: empirical evidence from the stock market', *Journal of Computer Security*, Vol. 11, No. 3, pp. 431-448.

Carow, K., Heron, R. and Saxton, T. (2004), 'Do early birds get the returns? An empirical investigation of early-mover advantages in acquisitions', *Strategic Management Journal*, Vol. 25, No. 6, pp. 563-585.

Cavusoglu, H., Mishra, B. and Raghunathan, S. (2004), 'The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers' *International Journal of Electronic Commerce*, Vol. 9, No. 1, pp. 70-104.

Chaney, P.K., Devinney, T.M. and Winer, R.S. (1991), 'The impact of new product introductions on the market value of firms', *Journal of Business*, Vol. 64, No. 4, pp. 573-610.

Chen, J.V., Li, H.-C., Yen, D.C. and Bata, K.V. (2012), 'Did IT consulting firms gain when their clients were breached?', *Computers in Human Behavior*, Vol. 28, No.2, pp. 456-464.

Chen, Y., Ganesan, S. and Liu, Y. (2009), 'Does a firm's product-recall strategy affect its financial value? An examination of strategic alternatives during product-harm crises', *Journal of Marketing*, Vol. 73, No. 6, pp. 214-226.

Das, S., Sen, P.K. and Sengupta, S. (1998), 'Impact of strategic alliances on firm valuation', *Academy of Management Journal*, Vo. 41, No. 1, pp. 27-41.

DeFond, M.L., Konchitchki, Y., McMullin, J.L. and O'Leary, D.E. (2010), 'Does superior knowledge management increase shareholder value', *Paper presented at the American Accounting Association Annual Meeting*, San Francisco, USA.

Dos Santos, B.L., Peffers, K. and Mauer, D.C. (1993), 'The impact of information technology investment announcements on the market value of the firm', *Information Systems Research*, Vol. 4, No. 1, pp. 1-23.

Gal-Or, E. and Ghose, A. (2005), 'The economic incentives for sharing security information', *Information Systems Research*, Vol. 16, No. 2, pp. 186-208.

Gatzlaff K.M. and McCullough K.A. (2010), 'The effect of data breaches on shareholder wealth', *Risk Management and Insurance Review*, Vol.13, No.1, pp. 61-83.

Gordon, L.A., Loeb, M.P. and Sohail, T. (2010), 'Market value of voluntary disclosures concerning information security', *MIS Quarterly*, Vol. 34, No. 3, pp. 567-594.

Hinz, O., Nofer, M., Schiereck, D. and Trillig, J. (2015), 'The influence of data theft on the share prices and systematic risk of consumer electronics companies',

Information & Management, Vol. 52, No. 3, pp. 337-347.

Hovav, A. and D'Arcy, J. (2005), 'Capital market reaction to defective IT products: The case of computer viruses', *Computers & Security*, Vol. 24, No. 5, pp. 409-424.

Huang, C.K., Wang, T.T. and Tsai., Y.T. (2016), 'Market reactions to big data implementation announcements', *Paper presented at the 20th Pacific Asia Conference on Information Systems (PACIS 2016)*, Chiayi, Taiwan.

Konchitchki, Y. and O'Leary, D.E. (2011), 'Event study methodologies in information systems research', *International Journal of Accounting Information Systems*, Vol. 12, No. 2 , pp. 99-115.

Kwon, J., Ulmer, J.R. and Wang, T. (2012), 'The association between top management involvement and compensation and information security breaches', *Journal of Information Systems*, Vol. 27, No.1, pp. 219-236.

Liginlal, D., Sim, I. and Khansa, L. (2009), 'How significant is human error as a cause of privacy breaches? An empirical study and a framework for error management', *Computers & Security*, Vol. 28, No. 3, pp. 215-228.

MacKinlay, A.C. (1997), 'Event studies in economics and finance', *Journal of Economic Literature*, Vol. 35, No.1, pp. 13-39.

McWilliams, A. and Siegel, D. (1997), 'Event studies in management research: Theoretical and empirical issues', *Academy of Management Journal*, Vol. 40, No. 3, pp. 626-657.

Modi, S.B., Wiles, M.A. and Mishra, S. (2015), 'Shareholder value implications of service failures in triads: The case of customer information security breaches.', *Journal of Operations Management*, Vol. 35, pp. 21-39.

Mohr, J.J. (1996), 'The management and control of information in high-technology firms', *The Journal of High Technology Management Research*, Vol. 7, No. 2, pp. 245-268.

O'Leary, D.E. (2010), 'The impact of manager philosophy on knowledge management systems', *Intelligent Systems in Accounting, Finance and Management*, Vol. 17, No. 2, pp. 111-126.

Patell, J.M. (1976), 'Corporate forecasts of earnings per share and stock price behavior: Empirical test', *Journal of Accounting Research*, Vol. 14, No. 2, pp. 246-276.

Pirounias, S., Mermigas, D. and Patsakis, C. (2014), 'The relation between information security events and firm market value, empirical evidence on recent disclosures: An extension of the GLZ study', *Journal of Information Security and Applications*, Vol. 19, No. 4-5, pp. 257-271.

Rubin, E. and Rubin, A. (2013), 'The impact of Business Intelligence systems on stock return volatility', *Information & Management*, Vol. 50, No. 2-3, pp. 67-75.

Schechter S.E. and Smith M.D. (2003), 'How much security is enough to stop a thief?', *International Conference on Financial Cryptography (FC 2003)*, Berlin, Germany, pp. 122-137.

Sharpe, W.F. (1964), 'Capital asset prices: A theory of market equilibrium under conditions of risk', *The Journal of Finance*, Vol. 19, No. 3, pp. 425-442.

Siponen, M. (2006), 'Six design theories for IS security policies and guidelines', *Journal of the Association for Information Systems*, Vol. 7, No. 7, pp. 445-472.

Smith, K.T., Smith, M. and Smith, J.L. (2011), 'Case studies of cybercrime and its impact on marketing activity and shareholder value', *Academy of Marketing Studies Journal*, Vol. 15, No. 2, pp. 67-81.

Son, I., Lee, D., Lee, J.-N. and Chang, Y.B. (2014), 'Market perception on cloud computing initiatives in organizations: An extended resource-based view', *Information & Management*, Vol. 51, No. 6, pp. 653-669.

Straub Jr, D.W. (1990), 'Effective IS security: An Empirical Study', *Information Systems Research*, Vol. 1, No. 3, pp. 255-276.

Wang, T., Kannan, K.N. and Ulmer, J.R. (2013), 'The association between the disclosure and the realization of information security risk factors', *Information Systems Research*, Vol. 24, No. 2, pp. 201-218.

Wang, T., Ulmer, J.R. and Kannan, K. (2013), 'The textual contents of media reports of information security breaches and profitable short-term investment opportunities', *Journal of Organizational Computing and Electronic Commerce*, Vol. 23, No. 3, pp. 200-223.