The Market Value of Information System (IS) Security: An Event Study of e-Banking Service Providers

by

Linda Brock

A dissertation submitted in partial fulfillment of the requirements for the degree of
Doctor of Philosophy
in
Information Systems

Graduate School of Computer and Information Sciences
Nova Southeastern University

2012

An Abstract of a Dissertation Submitted to Nova Southeastern University in Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy

The Market Value of Information System (IS) Security: An Event study of e-Banking Service Providers

by
Linda Brock
August 2012

Understanding the financial value resulting from IS security investments is critically important to organizations focused on protecting service confidentiality, integrity, and availability in order to preserve firm revenues and reputations. Quantifying the financial effect from IS security investments is difficult to derive. This study investigated the relationship between e-banking investments in IS security and their market value impacts.

Using an event study approach, the author captured e-banking firm specific data and isolated the IS security effect through the measured change in market values. The author hypothesized that announcements of IS security investments would result in statistically significant changes in market values. The author also hypothesized two sub-segments of the selected security investment data, technology and people, would support statistically significant changes in the market values of e-banking service providers. The hypotheses were tested by measuring stock market reactions to the IS security announcements selected from an eight-year period (2003-2010).

Study findings indicated statistically significant market reactions for e-banking firms making IS security investment announcements and suggested that investors rewarded IS security technology investments more highly than e-banking firms making IS security people-focused investment announcements. The author concluded that because investors understand that mandatory regulatory compliance represents an e-banking firm's commitment to creating a secure computing environment, e-banking information systems are perceived as secure therefore, disclosing IS security investments results in weak changes to market values. Ultimately effective management of IS security requires acceptance of the idea that it is not technically feasible or financially viable to implement protections for all identified IS security risks therefore IS security investments must be effectively measured and risk levels consciously selected in order to implement the right technical and operational protections to support a firm's selected risk posture. The study contributes to the event study literature as well as the literature examining the economic effects of information systems security.

Acknowledgments

I wish to thank my committee chairperson, Dr. Marlyn Littman. Her unwavering support and guidance throughout the dissertation process has been exceptional and were sincerely appreciated. I also wish to thank my committee members, Dr Ling Wang and Dr Yair Levy, for their invaluable comments on earlier drafts of this dissertation. I greatly enjoyed the coursework offered by all three of these education professionals and am thankful for the opportunity to have worked with each of them.

In addition, I am indebted to Meleisa Holek for supporting my doctoral education goal and obtaining IBM executive approvals to fund my degree. I also wish to thank Klaus Julisch for his early belief in my perspective and value as a security professional. Finally I wish to acknowledge the on-going support I received from the IBM team of security and compliance professionals I am lucky enough to work with everyday.

Table of Contents

List of Tables

Tables

List of Figures

Figures

Chapter 1

Introduction

Background

In today's business environment, information systems (ISs) are an absolute necessity in order for companies to attain strategic goals and improve operational performance (Jeong & Stylianou, 2010). The United States (U.S.) Department of Commerce, National Institute of Standards and Technology (NIST) defines an information system (IS) as a set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of information (U.S. Department of Commerce NIST, 2011). There are costs associated with managing IS including security, storage, and retrieval therefore ongoing IS investments are required (Kendall & Kendall, 2008). Investments refer to an expenditure to acquire property, equipment or other capital assets intended to produce revenue or to an investment of effort and time on the part of an individual who wants to reap profits from the success of his labor (Siegel & Shim, 2010).

IS investments have dramatically affected the United States (U.S.) banking industry (Howell & Wei, 2010). The U.S. banking industry was one of the first to adopt Internet technologies and innovate with online brokerage, banking, and mortgage lending (Zhu, Kraemer, Xu, & Dedrick, 2004). At the time of their introduction online banking services, commonly referred to as electronic or e-banking services, were primarily

developed and implemented by banks to integrate older IS banking operations with newer information technologies such as the Internet in order to deliver innovative online banking services to customers (Liao & Wong, 2008). Over time information systems and technologies have transformed the structure of banking transactions and fundamentally altered the way banks conduct business since less physical money is used on a daily basis and instead, financial transactions are increasingly conducted virtually through a combination of devices ranging from e-banking servers and public and private networks to personal computers (PCs) and smartphones (Howell & Wei, 2010).

Financial institutions around the globe know they must proactively work to protect customer data and transactions as well as their own IS assets (Ifinedo, 2008). To ensure a secure e-banking environment, rigorous measures must be implemented including the restriction of unauthorized access, the control of allowable transactions, and the protection of online data which are all required (Liao & Wong, 2008). Implementing protective measures creates new costs for IS resources intended to detect and prevent security breaches, guard against vulnerabilities, and manage online attacks (Anderson & Choobineh, 2008).

Regulatory Demands

IS security is no longer just good business practice, it is also a legal obligation (Smedinghoff, 2007). The commercial banking industry is one of the highest regulated industries in the U.S. (Howell & Wei, 2010). Approximately 4,000 U.S. federal, state, and local laws and regulations must be followed by commercial banks in governing the management of electronic records (e-records) (Burns & Peterson, 2010). Laws and regulations impose requirements on IS business practices, products, and services to

achieve goals such as privacy, safety, and accessibility (Breaux, Anton, Boucher, & Dorfman, 2009). According to Gant (2009), firms that comply with regulatory requirements generally experience improvements in IS security and thereby reduce their risk posture. NIST defines IS security as the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability (CIA) (U.S. Department of Commerce NIST, 2011). Further, IS security is a dynamic process that must be proactively managed for an organization to effectively identify and respond to new system threats and vulnerabilities (U.S. Department of Commerce NIST, 2011).

Mandated regulatory requirements for U.S. banks processing financial transactions are driven by security and privacy provisions that exist in U.S. common law, federal and state constitutions, and a variety of legal statutes (Cassini, Medlin, & Romaniello, 2008). Regulatory legislation such as the Gramm-Leach-Bliley Act (GLBA) and Sarbanes-Oxley Act (SOX) require organizations to implement safeguards to ensure confidential information is safely maintained (Khansa & Liginlal, 2009). Specifically the GLBA empowers the U.S. Federal Deposit Insurance Corporation (FDIC), the Office of the Controller of the Currency (OCC), the Federal Savings and Loan Insurance Corporation (FSLIC), and other bank regulatory agencies to control and direct the security of bank data (Gatzlaff & McCullough, 2010). For example, according to GLBA financial institutions must maintain reasonable data security and also develop a formal response plan in the event of a data breach (Gatzlaff & McCullough, 2010).

Another regulatory example is the Sarbanes-Oxley (SOX) Act of 2002, intended to protect investors by improving the accuracy and reliability of corporate financial

disclosures (Burns & Peterson, 2010). SOX compliance is focused on the integrity objective of IS security by requiring firms to implement internal controls that effectively protect financial information from computer crimes, employee mistakes, and other security threats and vulnerabilities that could lead to inaccurate financial statements (Spears & Barki, 2010). SOX also requires annual external audits of a firm's internal security controls and company executives are held personally accountable for audit findings (Spears & Barki, 2010). According to Islam, Mouratidis, and Jurgens (2011), financial organizations spend approximately $5.8 billion annually to ensure compliance with regulations such as SOX.

Another financial regulatory requirement established by the Bank for International Settlements is the Basel II Agreement that enables banks to decrease their financial reserves in exchange for documenting and sharing IS vulnerability information (Pfleeger & Rue, 2008). The Basel II Agreement is intended to ensure effective risk management is in place for individual financial institutions and requires banks to perform regular IS risk detection, assessment, and measurement (Shih, 2010). In addition, Section 215 of the U.S. PATRIOT (Providing Appropriate Tools Required to Intercept and Obstruct Terrorism) Act of 2001 mandated that financial entities provide account information to government agencies when suspicious activities, such as money laundering, are identified (Cassini et al., 2008). The aforementioned laws are modified with amendments when old legislation is repealed or new legislation is introduced. Islam et al. (2011) observed that these legal modifications or amendments to existing laws most frequently occur in the information security legislative domain.

As a consequence of the financial crisis and global economic recession of 2008-2009, banks must also support a host of new compliance requirements pertaining to risk management (Yurcan, 2012). The Dodd-Frank Wall Street Reform and Consumer Protection Act, drafted as a direct response to the financial crisis, contain hundreds of new rules and provisions U.S. banks must support (Yurcan, 2012). The U.S. Department of the Treasure now requires e-filing by banks of suspicious activity reporting (SAR) to the Financial Crimes Enforcement Network (Yurcan, 2012). Moreover, the Federal Financial Institutions Examination Council (FFIEC) requires financial institutions to implement multiple types of online security, such as device authentication in addition to standard username and passwords, to support online authentication and fraud prevention requirements (Yurcan, 2012). The FFIEC also monitors the participation of a financial entity's executive management team and their board of directors involvement in IS planning by examining their decision-making processes around IS security measures should any breaches occur (Fisher, 2010).

As a consequence of the aforementioned regulations and on-going changes to existing regulations as well as the expanding number of laws that now exist in the U.S., perhaps no other industry is as overtly focused on IS security as the banking industry (Cassini et al., 2008). Banks are expressly committed by regulatory authorities to ensure the confidentiality, availability, and integrity of financial data (Podebrad & Drotleff, 2009). Recent research conducted by the Bank Systems and Technology group indicated that the top 2012 bank priority areas for IS investment are regulatory compliance and risk management (Burger, 2012).

Bank compliance with various laws and regulations results in a lower risk of liability and increased investor confidence in banking firms (Burns & Peterson, 2010). Announcement of an IS security investment is intended to communicate a bank's commitment to supporting regulatory requirements and are typically conveyed in corporate published documentation such as annual reports or press release announcements generated to describe company operating decisions expected to contribute to improved market values (Gordon, Loeb, & Sohail, 2010). Regulatory compliance authorities enforce regulatory controls by issuing penalties and imposing legal consequences for noncompliance (Dlamini, Eloff, & Eloff, 2009).

For those firms that do comply with mandated regulations, certificates are awarded in recognition of their compliance (Dlamini et al., 2009). Failure to comply with regulations could result in brand damages, negative impacts to stock prices and credit ratings, and ultimately the loss of consumer trust in banks that fail to adhere to current laws (Tashi, 2009). The ability to demonstrate security and privacy regulatory compliance is one of the most important drivers of IS security spending by e-banking service providers (Tashi, 2009). Investments in IS security however, are constrained by available company resources typically expressed in terms of time and money which, according to Pfleeger and Rue (2008), tends to drive the use of an economic argument to successfully justify spending on IS security.

IS Security in the Banking Sector

As businesses depend more on networked computing systems, they become more vulnerable to security attacks (Vijayaraghavan, Paul, & Rajarathnam, 2010). Organizations commonly suffer from security threats to corporate data, information

technology infrastructures, and personal computing (Johnston & Warkentin, 2010). Determining how best to achieve a secure IS environment however, is not straightforward due to multiple uncertainties about security threats and vulnerabilities, the consequences of a successful attack, and the effectiveness of selected mitigation measures (Rue, Pfleeger, & Ortiz, 2007).

Companies depending heavily on maintaining an online presence must address inadequate IS security or experience the costs of service disruption and the resulting negative revenue impacts (Smith & McKeen, 2009). Typically firms relying on the use of the Internet for service delivery recognize that security issues can hinder their ability to provide a desired level of service as well as cause economic losses in the form of lawsuits, adversely impact reputations, or negatively impact overall market values (Andoh-Baidoo, Amoako-Gyampah, & Osei-Bryson, 2010). Additionally, IS security issues can expose weaknesses in company management teams that can also negatively impact market values (Smith & McKeen, 2009).

In sectors such as banking, where sensitive data are commonplace, the need for additional IS security controls, capabilities and specifically customer data protections appears obvious (Podebrad & Drotleff, 2009). E-banking service providers are required to protect their informational assets against cyber crime, denial-of-service attacks, web hackers, data breaches, identity and credit card theft, and fraud (Smith, Winchester, & Bunker, 2010). Strong security measures must be implemented and continuously updated and monitored to ensure protection against present and future security issues (Vijayaraghavan et al., 2010). Assessing the value of IS security technologies is essential to the effective management of security (Cavusoglu, Mishra, & Raghunathan, 2004b).

IS dependent firms must also have strong security policies and practices in place to protect system resources and ensure negative publicity, consumer backlash, or government intervention does not occur (Storey, Kane, & Schwaig, 2009). Effective IS security involves a continuous process of identifying and prioritizing IS security risks, implementing safeguards or countermeasures, and constantly monitoring those controls to ensure risks are mitigated (Spears & Barki, 2010). Perceived security has a significant and positive impact on e-banking customer interactions (Liao & Wong, 2008). In fact, security is one of the biggest customer concerns when considering e-banking adoption (Howell & Wei, 2010). As a result, creating a secure e-banking environment has become a primary focus of commercial banks offering e-banking services (Bo & Congwei, 2009).

Problem Statement

According to Ho and Mallick (2010), IS investments such as security are commonly believed to have a positive effect on a firm's profitability however, quantifying the positive effect has proven to be difficult to determine. Measuring investment in IS security is a challenge because firms are typically unwilling to publicly disclose this kind of strategic information (Khansa & Liginlal, 2009). Moreover, the difficulty in measuring the financial benefits associated with IS security are compounded by the assumption that IS security only involves technical measures such as the use of approved firewalls, better tools for detecting intrusions and malicious code, or proof of cryptographic protocol usage (Magnusson, 2011), none of which considers the security professionals responsible for selecting and deploying IS security tools. According to Pfleeger (2009), typically attempts to develop effective information system security measurements are unsuccessful due to the inability to either identify all security expenditures within an organization or

due to a lack of available expenditure data. Currently a specific market value cannot be isolated and allocated to IS security and, as a consequence, assigning a financial value to IS security is difficult to derive (Neubauer & Hartl, 2009).

The root cause of the problem is economics since we do not know the costs of either getting security or of not having it (Lampson, 2009). IS investments span functional and organizational boundaries including departmental, interdepartmental, enterprise, and interorganizational (Xue, Liang, & Boulton, 2008). Additionally IS security expenditures are distributed over tools, policies, technology, procedures and personnel (Anderson & Choobineh, 2008). IS investments are found embedded throughout organizations to enable business strategies, process improvements, or new capabilities making it very difficult for researchers to pinpoint and measure the IS security contribution separate from the new strategy or capability (Mittal & Nault, 2009).

Yao, Sutton, and Chan (2009) found that firms are unlikely to make IS investments of any kind in the absence of some type of measured beneficial return resulting from these investments. Pfleeger and Rue (2008) concluded that organizations are limited in making informed investment decisions about financially effective IS security expenditures. Questions such as how much to invest in IS security, which security investments will have the most impact, and what financial metrics enable the effective measurement of IS security investments prove difficult to answer (Carin, Cybenko, & Hughes, 2008). Since the precise financial value of technology investments such as IS security are difficult to quantify, an understanding of the full financial values gained as well as confidence in the value of future technology investments is reduced (Wilkin & Chenhall, 2010).

Fundamentally, IS security is a business decision (Maguire & Miller, 2010). Security is the most important variable to the success of e-banking (Ochuko, Cullen, & Neagu, 2009). However, conclusive evidence documenting the relationship between investments in IS security and their associated market value impacts is unknown (Ho & Mallick, 2010). IS decision-makers must be able to quantify the positive effects resulting from IS security in order to gain managerial and financial support for current and future investments in IS security (Kauffman, Lee, & Sougstad, 2009).

Dissertation Goal

This investigation encompassed a unique large-scale examination of the market value impacts resulting from investments made in IS security by e-banking service providers. By using an event study approach, the study captured e-banking firm specific data and isolated the IS security effect through the measured change in market values. The findings were expected to illustrate the relative financial benefits associated with IS security investments designed to safeguard the integrity of e-banking operations (Kauffman et al., 2009). Based on the work conducted by Morris and Strickland (2008/2009), the author created a figure to explain the study scope (Figure 1):

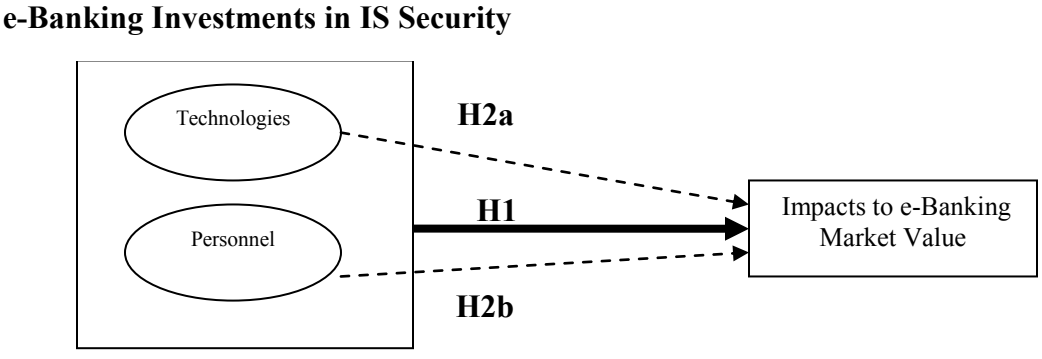

Figure 1. E-banking investments in IS security and their impacts on market value.

Research Hypotheses

According to Andoh-Baidoo et al. (2010), investors lost confidence in firms involved in announced IS security breaches, which directly resulted in a loss of market value. Gatzlaff and McCullough (2010) also found that announcements of IS security breaches resulted in negative impacts to firm market values. When firms publish announcements about the IS security investments made to eliminate or reduce IS security issues, which includes both technology and personnel investments, consumer confidence increases and investors are assured firms are working to secure their business systems (Andoh-Baidoo et al., 2010). Additionally, voluntary disclosure of IS security investments signals to the marketplace that the announcing firm is actively engaged in preventing, detecting, and correcting possible IS security issues (Gordon et al., 2010). Banks must frequently and consistently inform customers of the e-banking security measures implemented to protect financial transactions in order to promote the use of their e-banking services (Liao & Wong, 2008). Public announcement of investments in IS security technologies and personnel reflect the commitment of e-banking service providers to build stronger IS security capabilities and more effective IS security resources that can assimilate new technology innovations and capitalize on new business practices (Jeong & Lu, 2008). IS security announcements represent an important part of the image of a bank, therefore banks must carefully consider the security measures adopted and disclosed to the public so as to gain their confidence and, thereby, increase the market value of the firm (Yuen, Yeow, Lim, & Saylani, 2010). The market value impacts resulting from IS security investment announcements are intended to benefit e-banking service providers and thus the following general hypothesis was proposed for the study:

H_1: Investments in IS security will have a statistically significant impact on e-banking market values.

A significant portion of security decision-making and system management relies on the end user, resulting in a significantly increased vulnerability profile for decentralized IS governance environments such as e-banking (Johnston and Warkentin, 2010). Internet-based service providers such as e-bankers must work to continuously inform stakeholders that IS security issues are being addressed with a combination of technologies and personnel (Sanayei & Noroozi, 2009). For e-banking service providers in particular, supporting an IS security investment focus is critical since new technologies continue to become more and more integral to the long-term success of each service provider (Arduini & Morabito, 2010). An example of a technology-related IS security investment might include the announcement of a bank implementing a security mechanism to ensure authenticity of a given e-banking website (Oppliger, Rytz, & Holderegger, 2009). Jeong and Lu (2008) found that specific IS technology investments, such as Radio Frequency Identification (RFID), can produce significant positive increases in market reactions to the announcing firm and thus create considerable market value. While security technology investments do not guarantee market value increases, those investments undoubtedly put organizations in a better position to obtain their IS security goals (Howell & Wei, 2010). The market value impacts resulting from announcements of investments in IS security technologies will likely benefit e-banking service providers and thus the second study hypothesis proposed was:

H_2a: Investments in IS security technologies will have a statistically significant impact on e-banking market values.

IS security incidents not only damage corporate reputations but also expose weaknesses in company management teams (Smith & McKeen, 2009). An IS security incident is defined by the U.S. Department of Commerce NIST (2011) as an occurrence that jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores or transmits. IS security professionals must weigh the integration of IS security demands against the firm's business goals and objectives (Whitten, 2008). IS security professionals strive to align IS resources and the actions of users with the desired security posture of the management team (Johnston & Warkentin, 2010). Critical staff members with deep specialist knowledge in their area of responsibility, such as IS security, can represent big financial value for a company since it is assumed by their hiring that IS security problems and their affiliated negative market value impacts will not occur (Podebrad & Drotleff, 2009). Such leadership is frequently cited as a critical component of successful IS security programs (Johnston & Hale, 2008) and therefore the market value impacts resulting from announcements of investments in IS security people will likely benefit e-banking service providers. Thus the third study hypothesis proposed was:

H_2b: Investments in IS security people will have a statistically significant impact on e-banking market values.

Relevance and Significance

In conducting this research, the author used the event study methodology to assess the market value of investments in IS security in the e-banking sector. Eugene Fama is an American economist, known for his work on the efficient market hypothesis and publication of the first event study that sought to analyze how stock prices responded to

an event (Corrado, 2011). According to the classic Fama (1970) publication, the event study methodology enables a financial assessment of announced investments and their impacts to a given firm's stock price. The event study methodology is well accepted for studying the market value implications of public announcements and their associated impacts on market values (Telang & Wattal, 2007). By applying the event study methodology to examine the market value impacts of e-banking IS security investments, the author will contribute to the existing body of event study research literature (Jeong & Lu, 2008).

In addition to being an accepted research approach, event studies are of practical importance to business executives as stock performance is an important proxy for firm performance (Roztocki & Weistroffer, 2009b). A better understanding of the market value impacts associated with any type of IS investment is of interest to both industry and academic professionals given that technology investment expenditures continue to increase along with the need to justify those expenditures (Nagm & Kautz, 2008). By using the event study methodology, e-banking IS security decision-makers and company executives are able to determine the full financial value of their technology and personnel investments in order to be able to rationalize both current and future IS security investments (Kauffman et al., 2009). As further research focused on the economic impacts of investments in IS security is conducted, capital allocations assigned to IS security efforts can be financially quantified and their market value impacts more readily understood by both financial and IS managers (Gordon, Loeb, Sohail, Tseng, & Zhou, 2008).

Barriers and Issues

As noted by Tian, Haleblian, and Rajogopalan (2011), conclusions drawn from an event study are valid only if all confounding events are removed from the study scope. Multiple company announcements can occur on the same day that might contain any number of topics including earnings announcements, notice of executive turnovers, launches of new product lines, large investment decisions, recalls of defective products, merger and acquisition announcements, or legal actions (Duan, Grover, & Balakrishnan, 2009). Using an event study to assign individual market value impacts across multiple company announcements made on a single day is not possible and instead, all of the announcements made on that given day would be considered confounding events and thus removed from the study scope (Hovav & D'Arcy, 2005). If confounding events are not removed from the study scope, researchers may incorrectly assign market impacts to the scope of the study and incorrectly conclude greater market value impacts than actually occurred as a result of the given announcement (Hovav & D'Arcy, 2005). Any firm that was found to have confounding events occurring on the same day it made public an investment in IS security technologies or people was eliminated from the data sample (Dardan, Stylianou, & Kumar, 2006/2007).

A firm's shareholders have a significant effect on the firm's technology investments (Ravichandran, Han, & Hansan, 2009). All existing event studies assume that investors revised their expectations of a given firm's market value based on new information provided in press announcements (Jeong & Lu, 2008). Sometimes however, new company information is leaked or anticipated in advance of public announcements (Cavusoglu, Mishra, & Raghunathan, 2004a). As an example, regulatory changes are

often debated in the political arena over time and as a result, any accompanying market value effects are gradually incorporated into the financial value of a firm as the probability of the change being adopted increases (Campbell, Lo, & MacKinlay, 1997). Event studies are far less useful if the event was anticipated (Fama, 1998). Only events with confirmed announcement dates were selected for the study scope.

Regarding issues, outlying observations can significantly influence the findings of an event study (Dardan et al., 2006/2007). Outlying observations, also known as outliers, are data points that fall outside the normal distribution of event study results (Campbell, Cowan, & Salotti, 2010). Since outliers can appear to cause either a significant or lack of a significant market value impact, the event study methodology requires the removal of outliers from the core of consideration (Corrado, 2011). To ensure that the research results correctly reflect all market impacts, outlying events that fell outside the range of the mean plus and minus three standard deviations were removed from the study scope (Cavusoglu et al., 2004a).

Limitations and Delimitations

Roztocki and Weistroffer (2009b) achieved a higher validity of their event study results by maintaining a narrow study focus, concentrated only on IS investments related to EAI technologies. Also the suitability of the event study method applied to multi-country non-U.S. markets has not been established in the literature due to the many different dimensions of each stock market (Campbell et al., 2010). For example, size, trading volumes, accounting standards, regulation and corporate governance are just some of the many differences between the U.S. stock market and others (Campbell et al., 2010). This study scope focused only on publicly traded U.S. e-banking service providers

making IS security related investments as opposed to e-banking service providers outside of the U.S. or an examination of IS investments in general.

In the classic study conducted by Cavusoglu et al. (2004), the researchers explained that firm size and type may limit the results of an event study. Large firms can typically withstand negative economic and financial downturns more easily compared to smaller firms (Telang & Wattal, 2007). As a result, the assumption that an IS security-related investment announcement can have a similar effect across all firm sizes is not a reasonable conclusion (Cavusoglu et al., 2004). The study sample consisted of only large firms therefore the study results are not applicable to small companies or not-for-profit organizations (Hovav & D'Arcy, 2005).

Definition of Terms

Abnormal Return (AR) - Abnormal returns are the excess stock market returns compared to normal, expected returns in the event's absence (Andoh-Baidoo et al., 2010).

Availability – timely and reliable access to information (U.S. Department of Commerce NIST, 2011).

Bank – a corporation authorized by law to issue bills, notes, or other evidences of debt for circulation as money, to receive deposits of money and commercial paper, and to make loans (Bienvenu, 2012).

Confidentiality – preserving authorized restrictions on information access and disclosure (U.S. Department of Commerce NIST, 2011).

Information System (IS) - a set of information resources organized for the collection, processing, maintenance, use, dissemination or disposition of information (U.S. Department of Commerce NIST, 2011).

Information System Security - the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability (U.S. Department of Commerce NIST, 2011).

Information Security Incident - an occurrence that jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores or transmits (U.S. Department of Commerce NIST, 2011).

Integrity – guarding against improper information modification or destruction (U.S. Department of Commerce NIST, 2011).

Investment(s) – expenditure to acquire property, equipment or other capital asset that is intended to produce revenue (Siegel & Shim, 2010).

National Association of Securities Dealers Automated Quotations (NASDAQ) - computerized stock trading system that allows brokers to access price quotations for stocks being traded electronically or sold on the floor of a stock exchange (Siegel & Shim, 2010).

Net Present Value (NPV) - a well-established economic process used for budgeting capital investments which consists of calculating the difference between the present value of cash inflows generated by the project or asset and the amount of the initial investment (Siegel & Shim, 2010).

New York Stock Exchange (NYSE) - also known as the Big Board or The Exhange, the NYSE was founded in 1792 and is located on Wall Street in New York City. Securities are bought and sold in an auction market by brokers acting as agents for the buyer and seller. It is the oldest and largest stock exchange in the U.S. (Siegel & Shim, 2010).

Return on Assets (ROA) - indicator of efficiency based on the amount earned on each dollar of assets invested, typically stated as a percentage (Siegel & Shim, 2010).

Return on Equity (ROE) - an indicator of profitability and typically stated as a percentage, represents the amount earned on a common stock investment for a given period (Siegel & Shim, 2010).

Return on Investment (ROI) - a set of formulas to calculate how much value a firm derives from its assets to determine the firm's profitability on its business operations and thus serves to measure management's effectiveness (Siegel & Shim, 2010).

Return on Sales (ROS) – the amount of income recognized for sales made during the year, ROS can be a useful measure of overall operational efficiency when compared with prior periods or with other companies in the same industry (Ferraino, 2010).

Securities – financial instrument that shows ownership (e.g., stock), debt instrument (e.g., bond), or right (e.g., option) (Siegel & Shim, 2010).

Standard Industrial Classification (SIC) - is a federally designed standard numbering system established by the Office of Management and Budget that identifies companies by industry and provides other information. It is typically used to compare economic statistics from various facets of the U.S. economy (Downes & Goodman, 1998).

Stock – evidence of ownership in a company (Siegel & Shim, 2010).

Summary

The continued demand for IS investments such as security, require careful consideration of the delivered financial value (Wilkin & Chenhall, 2010). Investments in IS security reflect the technology and policy landscape of a given firm, as well as organizational priorities, culture, and investment practices (Pfleeger & Ciszek, 2008). E-

banking investments in IS security technology and people necessary to comply with U.S. laws and regulations can be measured using the event study method in order to understand their impacts on the firm's stock price performance (Morris & Strickland, 2008/2009). Understanding the financial value resulting from IS security investments is critically important to successful organizations since poor IS investment decisions adversely impact a firm's market performance (Adomavicius, Bockstedt, & Gupta, 2008). This study investigated the relationship between e-banking investments in IS security technology and people and their market value impacts for selected e-banking firms.

Chapter 2

Review of the Literature

Introduction

A longstanding theme in IS research focuses on establishment of the relationship between technology investments and financial values (Wilkin & Chenhall, 2010). Much of the literature has focused on IS financial investment values based on case studies, anecdotes, and conceptual frameworks with little empirical data that could accurately characterize market value or gauge the impact on firm financial performance (Zhu, 2004). Previous empirical studies examined the link between IS and firm performance by using accounting-based measures that reported mixed results (Stoel & Muhanna, 2009). Accounting-based measures, such as Return on Investment (ROI), Net Present Value (NPV) or some combination of these and other accounting-based measures, resulted in limited empirical data that could accurately characterize market value or gauge the impact on firm financial performance (Bojanc & Jerman-Blazic, 2008). The following literature review examined empirical research studies conducted over the last 12 years. The literature review included studies using accounting-based measures and market-based measures of IS investments covering general IS investments as well as outsourcing, ERP/EAI, e-Commerce, industry-specific, personnel, and security-related IS investments.

Accounting-based Measures of IS Investments

In the classic study by Gordon and Loeb (2006), the researchers identified a trend of accounting-based financial analysis used to evaluate the return on investments (ROIs) made in IS security. ROI is a set of formulas used to calculate how much financial value a company delivers from its assets and investments (Yao et al., 2009). According to Yao et al. (2009) calculating a return on investments in IS can provide firms with a benchmark for measuring the financial value of IS systems at the asset (ROA), equity (ROE), or sales (ROS) levels. According to Yao et al. (2009) there is no universal calculation for determining ROI and therefore it is an approach that cannot be uniformly applied.

In the classic study by Purser (2004), guidelines for improving the ROI of IS security investments were provided since calculating quantitative ROI values is very difficult when applied to IS security. The problem with an ROI approach is that risk mitigations are not reflected as a part of the ROI values (Purser, 2004). Since a reduced risk profile is one intended financial value the investing firm is seeking, the impacts from mitigations should also be reflected as part of the return on the IS security investments that made them possible (Purser, 2004). Purser (2004) concluded that current accounting-based measures such as ROI do not consider the affect of the change in risk associated with IS security-related business initiatives and therefore provides only a partial image of the true return on IS security investments. Sobol and Klein (2009) found that only IS application support is highly correlated with a performance measure such as ROI because application support is a well defined set of services commonly needed by all firm employees and therefore results in a more uniformly spread and readily defined set of costs.

In their classic study, Gordon and Loeb (2006) maintained that information security expenditures should be examined using more traditional accounting-based approaches. These researchers conducted an empirical study to examine the cost-benefit analysis approaches many corporations used to make decisions regarding investments in IS security. For example, a well-established economic process used for budgeting capital investments applies cost-benefit analysis using the net present value (NPV) model. NPV consists of estimating and comparing the risk-adjusted discounted present financial value of expected benefits with expected costs (Gordon & Loeb, 2006). The researchers found that senior information security managers typically use some form of NPV analysis in budgeting for information security investments. The researchers also found that it is rarely possible to use completely rational economic models like NPV for cost-benefit analysis of IS security investments since estimating the expected benefits requires information on the probability and potential losses resulting from security breaches which most firms do not regularly create or collect.

Yao et al. (2009) examined the relationship between IS spending and four traditional accounting performance measures, namely Return on Investment (ROI), Return on Equity (ROE), Return on Sales (ROS), and Return on Assets (ROA) which attempt to capture a firm's economic impacts resulting from IS investments, equity, sales or assets. According to Yao et al. (2009), the use of the aforementioned measures resulted in erratic and weak correlations between investments in IS and these traditional accounting performance measures. Investments in IS have some unique characteristics such as rapid depreciation, short useful life, and unpredictable operational aspects, making them unlike

other organizational assets successfully rationalized using traditional accounting measures such as ROI, ROE, ROS, and ROA (Kibiloski, 2007).

Market-based Measures of IS Investments

In the classic study by Thatcher and Pingry (2007), the researchers found that IS investments did not result in measurable improvements using traditional accounting-based measures of financial value, and as a result, recommend the need to consider other effective measures of financial value. For over a decade, IS researchers have studied firm performance impacts resulting from various types of investments in IS using the event study methodology (Yao et al., 2009). Event studies reflect a market-based measure that expresses the stock market reaction to a specific event and the resulting changes in a firm's market value and therefore can demonstrate the measurable effects of investments in IS on firm performance (Roztocki & Weistroffer, 2009b). Duan et al. (2009) found this method superior to the majority of other available accounting-based measures of value since it represents an assessment by an efficient and rational third party, namely the stock market, rather than an assessment completed by financial managers from within a given company who are likely bias. Simply stated, an event study enables researchers to examine the impact of an event on the financial value of the firm (Corrado, 2011). Since its introduction, the methodology has been recognized as a powerful research tool for evaluating all types of firm announcements (McWilliams & Siegel, 1997). In this segment of the literature review, precedent is established for using an event study methodology in the investigation of IS security investments and their impacts on e-banking service providers.

General IS Event Studies

Classic event studies addressing a broad range of general information systems issues include Chatterjee, Pacini, and Sambamurthy's (2002) widely cited event study focused on technology infrastructure investments. These researchers found that technology infrastructure investments were perceived as a platform for growth and revenue generation opportunities, which generated positive returns for the announcing firms (Chatterjee et al., 2002). Dehning, Richardson, and Zmud's (2003) classic event study examined transformational IS investments and found market values increased in conjunction with announcements of those investments. Roztocki and Weistroffer (2006) conducted a now classic event study that investigated the effect of cost management systems and their related technology investments and found that investors did not automatically associate positive market value impacts with a company's adoption of an activity-based costing approach and their associated IS investments. The classic event study conducted by Dardan et al. (2006/2007) found that customer-related IS investments improved customer satisfaction levels and therefore provided positive market value impacts to investing firms. Another classic event study conducted by Sabherwal and Sabherwal (2007) demonstrated that knowledge management investments also resulted in positive market value impacts for the investing firms.

More recent event studies addressing a broad range of general information system investments include Nagm and Kautz's (2008) study examining the impacts of technology investments on publicly traded Australian firms which generated positive market value impacts. Png, Wang and Wang (2008) used an event study to examine the market value impacts of government enforcement used to deter online attacks. The

researchers found limited evidence that government enforcement deterred attacks within the given country. Morris and Strickland (2008/2009) examined IS process improvements using an event study approach and found that capability maturity model (CMM) transitions demonstrating improved IS-related processes resulted in positive market value impacts. Bharadwaj, Keil, and Mahring (2009) used an event study to understand financial impacts resulting from unforeseen operating or implementation-related information technology (IT) failures and measured a 2% average drop in market values for those firms reported. Also in 2009a, Roztocki and Weistroffer applied the event study method to examine the market value of investments in IS to support activity based costing and found those investments do not lead to either positive or negative market value impacts for announcing firms. Finally, Choi and Jong (2010) were able to measure the positive market value impacts resulting from knowledge management investments by using an event study approach.

IS Outsourcing Event Studies

The classic event study conducted by Hayes, Hunton, and Reck (2000) examined the market value impacts of IS outsourcing announcements and found positive market value reactions for announcing firms. In the classic event study conducted by Agrawal, Kishore, and Rao's (2006) market reactions to e-business outsourcing announcements also resulted in positive market value reactions for announcing firms. More recently, an event study of business process outsourcing announcements was conducted by Duan et al. (2009). The researchers found positive market value reactions for both primary and supportive business process outsourcing announcements. Similarly, Jeong and Stylianou

(2010) conducted an event study of application service provider (ASP) adoption and found positive increases in the market value of the announcing firms.

IS ERP/EAI Event Studies

Roztocki and Weistroffer (2008) used an event study to compare the market value reactions of enterprise resource planning (ERP) investments to enterprise application integration (EAI) investments and found insignificant financial value changes for both types of investments. Further, Roztocki and Weistroffer's 2009b event study of EAI investments clarified that the announcement of EAI investments are not always treated as good news from investors and, as a consequence, did not generally result in positive market reactions. Hayes et al. (2001) also studied the market reaction to ERP system investments. In this classic study, positive market reactions were found for ERP investments (Hayes et al., 2001), as did Ranganathan and Brown in their 2006 classic study of ERP investments.

IS e-Commerce Event Studies

Event studies have also been used to understand market value impacts resulting from IS e-commerce investments, including the now classic Subramani and Walden (2001) examination of e-commerce announcements and the related changes in the value of announcing firms. The researchers found positive market value impacts resulting from e-commerce investments. These findings were also supported in the Dehning, Richardson, Urbaczewski, and Wells (2004) classic event study that also found similar positive market value impacts from e-commerce initiatives. A few years later, Dewan and Ren (2007) examined e-commerce announcements and their market value impacts but found no significant market value changes resulting from the selected IS investments. Baek,

Lee, and Lim's (2008) event study of e-commerce service failures announced by Korean firms resulted in negative stock value reactions. Finally, another related classic event study performed by Benbunan-Fich and Fich (2004) examined the financial value effects of web traffic announcements which resulted in increased market values. By contrast their classic 2005 event study, which was focused on measuring the market value impacts resulting from refining a firm's web presence, resulted in no significant firm valuation adjustments.

Industry-specific IS Event Studies

Event studies have also been used to measure industry-specific impacts resulting from various types of IS investments. The classic Im, Dow, and Grover 2001 event study was a follow-up to the now classic Dos Santos, Peffers, and Mauer (1993) event study which found that financial firms improved market values when innovative IS investments were announced. In contrast, Hunter's (2003) classic event study of the retail industry's IS investment announcements indicated that on average, IS investments were more likely to destroy market value than increase it. More recently, Raghu, Woo, Mohan, and Rao (2008) studied the market reaction to patent infringement litigation in the information systems industry and reported that news of patent infringement litigation was unfavorably viewed by the market thereby resulting in negative market value impacts to firms within the study scope. Finally, Jeong and Lu (2008) examined the impacts of Radio Frequency Identification (RFID) investment announcements in the manufacturing and service sectors and found improved market values for vendors making RFID investment announcements. The researchers found the IS industry segment garnered a much larger

market return for their RFID investment announcements compared to the manufacturing and services industry sectors.

Personnel-specific IS Event Studies

The event study method has also been used to measure market value impacts resulting from firm investments in IS people. Due to the significant role of executive leadership in championing or facilitating IS investments, in their classic event study Chatterjee, Richardson, and Zmud (2001) examined the effects of new Chief Information Officer (CIO) announcements on firm values. Positive market value reactions for all firms in the study, especially those competing in industries undergoing IS-driven transformation, were found by the researchers. In 2006, Guan, Sutton, Chang, and Arnold also examined market reactions to announcements of newly created CIO positions. This classic event study found increased market values for the announcing firm, confirming that CIO positions represent an important value to announcing firms. In 2007, Khallaf and Skantz conducted a classic event study examining the market reaction to new and existing CIO appointments and found that capital markets displayed no significant difference in the reaction to the two types of IS personnel announcements. More recently Tian et al. (2011) examined new CEO selection announcements and their impacts on the market values of the announcing firm and found the market reacted favorably to the appointments made by boards where the CEO industry experience and ties to other corporate boards were both deep and high.

Security-specific IS Event Studies

The event study method has also been used to measure the market value impacts resulting from IS security breaches, attacks, and defects or vulnerabilities. Campbell,

Gordon, Loeb and Zhou (2003) conducted a now classic event study that examined the market value effects of information security breaches and found limited evidence of negative market responses however, highly significant negative market reactions to announcements of security breaches involving unauthorized access to confidential data were found. In 2004a, Cavusoglu et al. conducted a classic event study in order to determine the market value impacts of Internet security breach announcements. Findings from the Cavusoglu et al. (2004a) investigation demonstrated that announcing an Internet security breach negatively impacted the firm's stock price and resulting market value. In 2006, Andoh-Baidoo and Osei-Bryson performed a classic event study to explore breach characteristics and their impacts on market values. Andoh-Baidoo and Osei-Bryson (2006) found that Internet-based businesses experienced more negative market value impacts compared to non Internet-based firms. Goel and Shawky (2009) also found that the announcement of a security breach had a significantly negative market value impact equating to about 1% of the market value of the firm. A 2010 follow-up study by Andoh-Baidoo et al. confirmed the previous 2006 study findings that announcing an Internet security breach results in a loss of confidence in a firm and therefore results in lower market values. Gatzlaff and McCullough (2010), also using the event study methodology, found evidence that the market responds negatively to announcements of security breaches of customer and/or employee data at publicly traded firms.

Ettredge and Richardson's (2003) classic event study focused on the market reaction to denial-of-service (DoS) attacks and found Internet firms experienced negative market reactions resulting from DoS announcements. The classic 2003 event study conducted by Hovav and D'Arcy also examined DoS attacks and found that in general the market does

not penalize firms that experience such attacks. Internet-based firms however, were penalized by known DoS attacks (Hovav and D'Arcy, 2003). More recently, Wang, Xiao, and Rao (2010) conducted an event study to understand the impact of computer viruses and their related public vulnerability disclosures and found there was limited reaction from ordinary users and therefore limited market value impacts on firms.

Event studies have also been used to measure the market reaction to announcements of IS security-related defects and vulnerabilities. Hovav and D'Arcy (2005) conducted a classic event study focused on defective IS products resulting from computer viruses and found no change in firm market values resulting from defect announcements. Telang and Wattal (2007) used the event study methodology to examine the impact of software vulnerability announcements on market values and found software vulnerability announcements resulted in significantly negative changes to a firm's market value.

Strengths and Weaknesses of Existing Studies

According to Rue and Pfleeger (2009), industry and academic researchers have generated many different types of economic models to rationalize investments in IS security technologies and personnel. Thomas (2009) characterized the benefits derived from investments in IS security as the avoidance of uncertain losses. As a consequence, Thomas (2009) maintained that applying traditional cash flow return on investment (ROI) techniques was inappropriate, as well as confusing or misleading in terms of clarifying the value of IS security investments. Traditional economic measures such as ROI have not proven to be useful for assessing the financial value of IS security since simple questions, such as how much more security an extra dollar buys, typically go unanswered (Pfleeger & Rue, 2008).

According to Mitra (2005), utilization of accounting-based measures such as ROI are a weak approach for measuring the market value of investing in IS security since these measures are typically limited to capturing and reflecting only historical financial information. Also Thatcher and Pingry (2004) found accounting-based measures typically assumed only one cost parameter was affected at one time but in fact, any single IS investment impacts a company's costs and resulting value in multiple ways including increased productivity and improved quality. Further Thatcher and Pingry (2004) found that by using traditional accounting approaches, the difficulty of isolating a financial value actually increased. Accounting-based measures are inadequate indicators of the true impact of information and technology investments on market values (McWilliams & Siegel, 1997).

In contrast to accounting-based measures that have been examined, event studies are distinguished by a history of proven success in measuring market value impacts resulting from IS investments and over the last few decades, the adoption of the method has broadened and the level of sophistication of event studies has increased with usage (Campbell et al., 1997). As evidenced by the literature review, one of the greatest strengths of an event study is that it allows researchers to consistently and comparatively examine the market value impacts of a wide variety of IS investments on a large scale using multiple factors and firm types (Corrado, 2011). An event study is a robust and proven way to study the relationship between various types of IS investments, such as IS security, in order to understand the potential negative and positive economic impacts on firm performance (Nagm & Kautz, 2008).

Gaps in the Literature

According to Corrado (2011), no one knows exactly how many event studies have been published since the methodology was introduced. What is clear is that event studies have been used by IS researchers since the early 1990's and continue to be used as a viable research approach today. In particular, of the 44 IS event studies conducted over the last 12 years and as surveyed in the previous literature review discussion (see Appendix A for complete summary list), 11 security-specific IS event studies examined the market value impacts resulting from IS security breaches, attacks, or vulnerabilities. Specifically, based on the findings from the event studies conducted by Campbell et al. (2003), Cavusoglu et al. (2004a), Andoh-Baidoo et al. (2006), Goel and Shawky (2009), Andoh-Baidoo et al. (2010), and Gatzlaff and McCullough (2010), the negative market value impacts that can result from security breaches has been quantified. Additionally, the event studies conducted by Ettredge and Richardson (2003), and Hovav and D'Arcy (2003) provided a measure of the market value impacts resulting from various types of IS attacks. Finally, the Wang et al. (2010), Hovav and D'Arcy (2005), and Telang and Wattal (2007) study results provided a measure of the market value impacts resulting from various types of IS security vulnerabilities. A summary of these event studies examining the market value impacts resulting from IS security-related announcements are reflected in table 1 as follows:

Table 1. Security-specific IS Event Studies Surveyed in the Literature Review

Study Authors (Year)	Security Issue Type
Campbell, Gordon, Loeb, & Zhou (2003)	Breaches
Cavusoglu, Mishra, & Raghunathan (2004)	Breaches
Andoh-Baidoo & Osei-Bryson (2006)	Breaches

Goel & Shawky (2009)	Breaches
Andoh-Baidoo, Amoako-Gyampah, & Osei-Bryson (2010)	Breaches
Gatzlaff & McCullough (2010)	Breaches
Hovav & D'Arcy (2005)	Viruses
Wang, Xiao, & Rao (2010)	Viruses
Ettredge & Richardson (2003)	Hacker attacks
Hovav & D'Arcy (2003)	Denial-of-Service
Telang & Wattal (2007)	Software Vulnerabilities

While the results of the aforementioned IS security-specific event studies facilitated an understanding of the negative market value impacts associated with security breaches, attacks, and vulnerabilities, an understanding of the positive market value impacts resulting from investments in IS security is still needed to fully understand the cost/benefit ratio of the investment (Geer, 2007). The author conducted a comprehensive search of the ACM Digital Library, IEEE Computer Society Digital Library, ProQuest Computing, Wiley Online Library, and Computers and Applied Sciences Complete to examine previous research on the market value impacts resulting from investments in IS security. No event study was found that examined the market value impacts of IS security investments for e-banking service providers. The results of this event study are intended to address this gap in the literature.

Summary

As summarized in the literature review, even after many years of research studying the impacts of IS investments of all types, identification and measurement of the financial impacts resulting from technology investments is difficult to determine (Wilkin & Chenhall, 2010). Poor IS investments can destroy corporate wealth while savvy IS investments can also create corporate wealth (Parent & Reich, 2009). For the last decade, researchers have realized that security and privacy are not just a technical problem; there is a major economic component as supported by the rapid increase of investments in IS

security (Bojanc & Jerman-Blazic, 2008). An event study is a robust and proven way to study the relationship between IS security investments and the impacts to firm market values (Nagm & Kautz, 2008).

Chapter 3

Methodology

Introduction

As noted and explained in chapters 1 and 2, the event study methodology was adopted for this study. This chapter briefly reviews the theoretical basis of event studies, which is followed by a detailed discussion of the event study methodology. Data collection and analysis are also discussed, followed by an explanation of the study hypothesis testing and a summary of the chapter.

Theoretical Basis

The event study methodology assumes new information about a corporate event, such as an announced investment in IS security, is financially assessed by investors and reflected in the changes to a firm's stock price (Ranganathan & Brown, 2006). In his classic 1970 research study, Fama explains this assumption is based on the theory that the market is efficient. The efficient markets theory is based on the concept of rational expectations which assumes that stock market prices always immediately reflect all available information and every stock's price reflects all information regarding the prospects of that stock (Jang & Chen, 2009). A capital market is said to be efficient if it fully and correctly reflects all relevant information in determining stock prices (Fama, 1970).

In event studies, when financial markets learn of unanticipated news that will likely affect a firm's performance, a reaction expressed in stock price adjustment is measured to indicate the market value placed on that news (Duan et al., 2009). This valuation is possible because of market efficiencies which enable information to be absorbed immediately by the capital market and then quickly reflected in the change of the announcing firm's stock price (Fama, 1998). The event study methodology implicitly assumes that the revision in the market value of the firm is caused by the event (Campbell et al., 1997).

Event Study Methodology

Since the late 1960's, event studies have been widely used in many disciplines including finance, accounting, and economics (Campbell et al., 1997). Much more recently the event study methodology has emerged as a viable approach to investigating many different types of IS events and their impacts on firm values (Andoh-Baidoo et al., 2010). As summarized in the literature review, event studies have examined the market value impacts of many different types of company announcements including IS infrastructure, out-sourcing, e-commerce services, CIO selections, and specific technologies such as RFID. Table 1 summarized the security-specific IS event studies identified as part of the literature review, half of which focused on security breaches while the remainder focused on specific forms of IS security attacks.

Consistent with the precedent set by Campbell et al. (2003), Cavusoglu et al. (2004a), Andoh-Baidoo and Osei-Bryson (2006), Goel and Shawky (2009), Andoh-Baidoo et al. (2010), Gatzlaff and McCullough (2010), Wang et al. (2010), Hovav and D'Arcy (2005), Ettredge and Richardson (2003), Hovav and D'Arcy (2003), and Telang and Wattal

(2007) for using an event study methodology to measure IS security-related market value impacts, in this dissertation investigation a traditional event study methodology was used to estimate the cumulative abnormal return (CAR) associated with investments in IS security made by U.S. e-banking service providers. Abnormal returns are the excess stock market returns compared to normal expected returns in the event's absence (Andoh-Baidoo et al., 2010). CAR served as the main dependent variable for the study scope (Duan et al., 2009). The key independent variable was the type of technology investment announcement (Chatterjee et al., 2001).

Overview of Event Study

Aside from Fama's event study publications from the 1970's, one of the most widely referenced event study sources is the Campbell et al.(1997) book titled *The Econometrics of Financial Markets*. As explained by these authors, the execution of an event study consists of seven standard steps. The first step involves defining the event of interest and identifying the period over which the stock prices of the firms involved in the study will be examined. The events of interest selected for the study included IS security technology and people investments announced by e-banking service providers. In accordance with the U.S. Department of Commerce NIST (2011) definition of information system security, every announcement was evaluated by the author for inclusion in the study on the basis of compliance with this definition.

The period of time over which the stock prices of the firms involved in the study were examined is known as the event window. The event window is defined as the period of interest for which we observe the event was first determined (Jeong & Lu, 2008). The

day of a firm's announcement is defined as day 0 in event studies (Roztocki & Weistroffer, 2009b).

According to McWilliams and Siegel (1997), the longer the event window, the more difficult it is to control for confounding events. A short event window will, on average, capture the significant effects of an event (Dardan et al., 2006/2007). The use of a short event window can ensure capturing an abnormal return resulting from the event of interest being studied instead of due to some other effect (Jeong & Lu, 2008). A one-day event window, most commonly the day of the announcement, is usually preferred (Cavusoglu et al., 2004a). According to Telang and Wattal (2007), using a one-day event window reduces the possibility of confounding factors influencing the announcement and it also increases the power of the statistical tests. If the timing of an event is known precisely then the ability to statistically identify the effect of the event will be higher for a shorter sampling interval (Campbell et al., 1997). For these reasons, the event window selected for the study contained only one day, specifically, the day of the announcement or day 0.

After defining the event of interest and the event window, the second step of an event study involves defining the selection criteria for including an announcement in the study scope (Campbell et al., 1997). Specific to this study, the announcement publication type was restricted to newswires and press releases available from Lexis/Nexis. Lexis/Nexis search terms for the study scope included (a) security, (b) secure, (c) safety, (d) safe, (e) protect, and (f) protection. The Lexis/Nexis data search was also restricted to include only those financial service provider firms located in the United States. Also only announcements involving firms publicly traded on either the New York Stock Exchange

(NYSE) or the National Association of Securities Dealers Automated Quotations (NASDAQ) stock exchange were selected. In addition the search was limited to cover only the eight years selected for the study scope (2003-2010).

The number of usable events found in the event studies summarized in the literature review ranged from 23 (Hovav & D'Arcy, 2003) up to 640 (Dewan & Ren, 2007). Much of this variance was driven by the differences in the sample period durations ranging from three days to 15 years. More specifically, over a five year sample period security-specific IS event studies averaged a total of 40 events (Campbell et al., 2003; Cavusoglu et al., 2004a; Hovav & D'Arcy, 2003, 2005; & Andoh-Baidoo et al., 2010) while the personnel-specific IS event studies averaged a total of 110 events (Chatterjee et al., 2001; Guan et al., 2006; Khallaf & Skantz, 2007; & Tian et al., 2011). Event studies with fewer than 100 events however are not uncommon in the literature (Benbunan-Fich & Fich, 2004). This study scope included 112 events occurring over an eight year sample period.

In the third step of an event study, in order to determine the market value impacts resulting from announcements, a measure of the abnormal return is necessary (Campbell et al., 1997). The abnormal return is the return of the stock over the event window minus the normal return for the stock over the event window (Campbell et al., 1997). In order to determine whether the selected IS security announcement affected a firm's stock price, an estimate of what the firm's stock price would have been had there been no announcement must be created (Hovav & D'Arcy, 2005). Therefore the standard event study methodology requires estimating a market model for each firm contained in the study scope (Telang & Wattal, 2007).

Economic-based models such as market-models help to establish links between financial reporting and the economic consequences of that activity (Verrecchia, 2001). The market model is a statistical model that relates the return of any given stock price to the return of a market portfolio of stocks (Campbell et al., 1997). It acts as a proxy for what the stock's value would have been in the absence of the event or selected announcement (Bodie, Kane, & Marcus, 2008). The market model used for estimating expected returns was a one-factor model that assumed a linear relationship between the return of the market portfolio and the return of the individual stock examined (Goel & Shawky, 2009).

In the fourth step of an event study, market model estimation parameters were defined (Campbell et al., 1997). Estimation parameters were used to calculate the market model results. Estimation durations or windows can vary, for example, Ettredge and Richardson (2003) used 255 days while Andoh-Baidoo et al. (2010) used 120 days. The shortest of the commonly accepted estimation periods for creating a market model is 120 days (Campbell et al., 2003). Some event studies use 250 days to correspond approximately to the number of trading days in a calendar year (Corrado, 2011).

Data from a 209 trading day estimation period that ended 46 trading days before the event date was used for the study (Cowan, 2007). According to Campbell et al. (1997), when possible the period prior to the event window should be used for the estimation window and the announcement period should not be included in the estimation window selected in order to prevent the announcement from influencing the normal performance model parameters. As depicted in Figure 2, a normal stock return was computed for each firm in the study scope using this same set of assumptions.

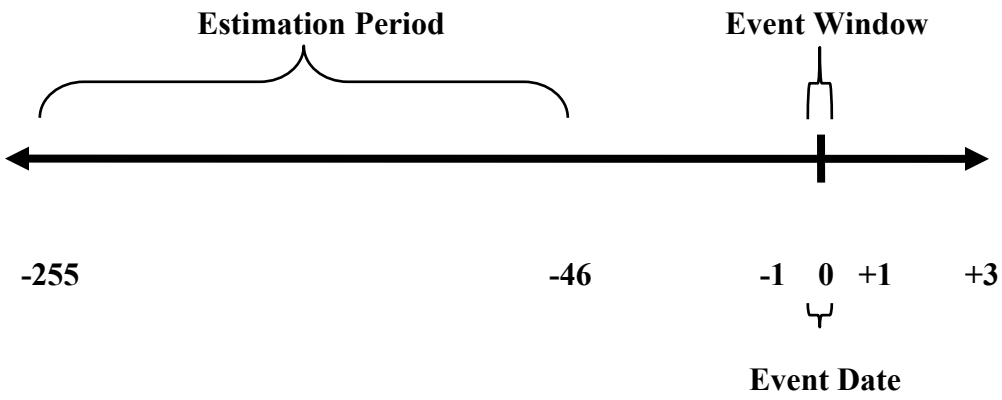

Figure 2. Estimation Period, Event Window, and Event Date

Best practice for event studies mandates use of a regression-based market model (Cable & Holland, 1999) to compute abnormal returns. The market model was used to compute the abnormal returns for all firms in the study scope (Jeong & Stylianou, 2010). The market model used regression analysis against the market return as measured by the model constructed of stocks listed in the New York Stock Exchange (Corrado, 2011). Abnormal returns were compared to the market model of normal returns (Cavusoglu et al., 2004a). The resulting cumulative abnormal returns were assumed to measure the effect of the event on the market value of the selected firm (McWilliams & Siegel, 1997).

In the fifth step, the testing procedure was defined (Campbell et al., 1997). Event studies typically report one parametric and one nonparametric statistic (Cowan, 1992) in order to examine the robustness of the test results (Chatterjee et al., 2001). The Patell Z parametric test statistic and the generalized sign nonparametric test statistic were used as the study test procedures (Cowan, 2007). Statistical significance for abnormal returns was measured at the 0.10, 0.05, 0.01, and 0.001 levels respectively using the Eventus® software tool (Cowan, 2007).

The sixth step was focused on presentation of the empirical results while the seventh and final step of an event study involves interpretation of those results (Campbell et al., 1997). The empirical results determine if the study's hypotheses can be supported. Study conclusions were based on stock price impacts resulting from the selected events and their effects on the market values of e-banking service provider firms as compared to the study hypotheses.

Event studies based on firm-level analysis can be aggregated and extrapolated into industry-level analysis (Hayes et al., 2001; Ranganathan et al., 2006). The author aggregated and extrapolated the banking industry results of the study in order to derive the study conclusions about e-banking service providers. More specifically, hypothesis testing in event studies typically entails aggregating individual CARs assuming all individual events are independent of each other and observe the same normal distribution (Duan et al., 2009). According to Cavusoglu et al. (2004a), CAR results for the selected sample can be aggregated across all events in order to draw an overall inference about their market value impacts.

The results of the study were intended to prove H_1, which is that investments in IS security will have a statistically significant impact on e-banking market values. The data sample was partitioned into two groups based on the type of IS security investment announced (technology or people) in order to compute CAR results for each of the sub-samples and determine if the second study hypothesis was supported or rejected (Campbell et al., 2003). Specifically H_2 questioned whether investments in IS security technologies or IS security people had a statistically significant impact on e-banking market values.

Abnormal returns of zero would mean there was no impact on market value. By contrast, positive abnormal returns would imply the announcement was expected to create positive market value impacts whereas a negative market value would indicate the announcement would destroy market value. According to Campbell et al. (1997), generally if the abnormal returns are large one will have little difficulty rejecting the null hypothesis of no abnormal return.

Resources

The Lexis/Nexis Academic University database contains one of the most comprehensive, accurate, and reliable collections of news announcements, public records, and legal and business data available (Dardan et al., 2006/2007). Lexis/Nexis enabled the search of newswires and press releases using the selected key word search terms for all financial institutions in the U.S. over the eight year period. Events were selected from the search results based on verification of the firm's public stock trading status using the Lexis/Nexis Company Profile database.

The stock market data needed for each individual firm within the scope of the study was obtained by using the University of Chicago's Center for Research on Security Prices (CRSP) common stock returns database (Corrado, 2011). The database provides share prices for all firms on any previous day as published by various exchanges (Fama, 1991). CRSP contains historical descriptive information and market data on more than 27,000 inactive and active companies. This information is posted by the New York Stock Exchange (NYSE) or National Association of Securities Dealers Automated Quotations (NASDAQ) market exchanges and then consolidated into the CRSP database (Cowan, 2007).

The Wharton Research Data Services (WRDS) provided access to the CRSP data. WRDS is a web-based business data research service that is available from the Wharton School at the University of Pennsylvania. WRDS is the de facto standard for business data, providing researchers worldwide with access to financial, economic, and marketing data (Cowan, 2007). WRDS also offered a web interface for access to the Eventus® Software. Eventus® software was explicitly designed to execute event studies using the CRSP stock database. Eventus® is licensed to an organization or individual by Cowan Research (2007). Access and usage of the Eventus® software tool was enabled by the existing Nova Southeastern University software license agreement.

Eventus® (Cowen, 2007) computed the returns for each company's stock based on estimations using a market model, which can be simply stated as the rate of return on common stock share price of firm *i* on day *t*, expressed as:

$$Rit = Xi + BiRmt + Eit$$

where

Rit = the rate of return on the share price of firm *i* on day *t*

Rmt = the rate of return of a market index on day *t*

Xi = the market model intercept term

Bi = the parameter that measures the sensitivity of Rit to the market index

Eit = the zero mean disturbance term

Using the Eventus® (Cowan, 2007) software, abnormal returns were calculated for each firm as

$$ARit = Rit - (Xi + BiRmt)$$

where the coefficients X*i* and B*i* are the ordinary least squares (OLS) parameter estimates obtained by regressing R*it* over Rmt over the 209 day estimation period prior to the event (Hovav & D'Arcy, 2003). OLS is a popular technique used to analyze how some independent variables like market return can affect a dependent variable like actual return (Telang & Wattal, 2007). According to Campbell et al. (2003), OLS assumes that the error terms from regressions are independent and identically distributed, have a mean of zero and are homoskedastic (the variance of the errors over the sample are similar).

Abnormal returns and test statistics were executed using the Eventus® software package licensed by Cowan Research (2007). Eventus® interfaces between SAS and the CRSP database which computed the abnormal returns for the specified event window (Cowan, 2007). The index that was used as the basis of the market model was the S&P500 composite index obtained from the CRSP database. Eventus® (Cowan, 2007) computed abnormal returns using the market model previously described and as depicted in Figure 2. To test H_1 and H_2, the cumulative abnormal return (CAR) was calculated for each firm using a one day interval and aggregated across all events by the Eventus® software to draw an overall inference (Cowan, 2007).

Hypothesis Testing

Event studies typically report both a parametric and nonparametric test statistic (Cowan, 1992). The Patell Z parametric test is a standardized abnormal return test approach for event studies, which estimates a separate standard error for each announcement and assumes cross-sectional independence (Cowan, 2007). As McWilliams and Siegel (1997) pointed out, parametric tests are also important to control for the effects of outliers on the significance of results because most event study statistics

are sensitive to outliers. Parametric tests control for outliers so that there can be a higher level of confidence that the study results are not driven by outliers (Cavusoglu et al., 2004a). To ensure the study results were not driven by outliers and following precedent set in other event studies (Cavusoglu et al., 2004a), events that were outside the rate of the mean market value, plus and minus three standard deviations were removed from the study scope.

The generalized sign test enabled a check of the robustness of study conclusions (Campbell et al., 1997). Cowan's (1992) generalized sign test compared the proportion of positive CARs around an event to the proportion from a period unaffected by the event which accounted for a possible asymmetric return distribution under the null hypothesis. The null hypothesis for the generalized sign test is that the fraction of positive returns is the same as in the estimation period. The sign test uses the normal approximation to the binominal distribution (Cowen, 2007). The generalized sign test was used to validate the study results.

Summary

In summary, the research approach involved using a traditional event study methodology to estimate the abnormal returns associated with investments in IS security technology and people by e-banking service providers. No experimental adjustments or changes to the traditional event study were included as part of the study scope since a standard or traditional event study was sufficient to derive study conclusions. The author also used the Eventus® software, which was explicitly designed to execute traditional event studies (Cowan, 2007). As described, the event study methodology uses model-based statistical inference as the primary method of deduction (Campbell et al., 1997).

Therefore a market model was used to compute the abnormal returns for all firms in the study scope. Abnormal returns were compared to the market model and the resulting cumulative abnormal returns were assumed to measure the effect of the event on the market values of the selected firms. As is true with every event study summarized in the literature review, statistical testing was also used to validate event study findings.

Chapter 4

Results

Introduction

This chapter reports on the data analysis, findings, and results of the event study on market value impacts to e-banking service providers announcing security technology and people investments. An explanation of the data collection process and a discussion of the analysis of the data selected for the study sample are presented. The findings based on the event study methodology are then presented and their statistical significance examined in detail. A summary of the study results concludes the chapter.

Data Collection

As explained in chapter 3, Lexis/Nexis enabled the search of newswires and press releases made from 2003-2010. Based on conventions established in the event studies summarized in chapter 2, announcements excluded from the study data set included those published in periodicals or magazines. It was necessary to exclude this type of publication because of the difficulty in determining the exact date of the given announcement as well as the likelihood of repeat announcements of the same event occurring in a different publication at a later date (Telang & Wattal, 2007).

Additionally only e-banking service provider firms were included in the search using Lexis/Nexis. Only those firms classified within the Banking and Finance industry

segment of the service were selected. The resulting list of e-banking service providers were verified by checking the Lexis/Nexis assigned industry classification against the banking Standard Industrial Classification (SIC) codes. Specifically, only firms assigned the SIC Division H, Major Groups 60, 61, and 67 codes established by the U.S. Securities and Exchange Commission (SEC) were selected for the study scope. Any responses involving non-baking firms were removed from the data sample.

Further, only announcements involving firms publicly traded in the U.S. on either the New York Stock Exchange (NYSE) or the National Association of Securities Dealers Automated Quotations (NASDAQ) stock exchange were included in the study scope (Hovav & D'Arcy, 2005). Lexis/Nexis search results were screened to ensure that private or foreign e-banking service providers were removed from the study scope. Events were selected from the search results based on verification of the firm's public stock trading status using the Lexis/Nexis Company Profile database. The stock market data needed for each individual firm within the scope of the study was obtained by using the University of Chicago's Center for Research on Security Prices (CRSP) common stock returns database (Corrado, 2011). Additionally, each firm was also screened to ensure that they offered an e-banking website for online banking services. If an e-banking website was not found for the firm or the website contained only general service information and did not offer e-banking service capabilities, then the firm was removed from the study scope.

The Lexis/Nexis key word search terms included (a) security, (b) secure, (c) safety, (d) safe, (e) protect, and (f) protection. The initial Lexis/Nexis search results included 651 announcements that were further narrowed to 516 announcements after duplicate announcements were removed. Announcements containing the word security but that

were not, in fact, information systems security related were also removed from the study scope. Usage of the key word security within the banking and finance industry resulted in the selection of numerous announcements that were not related to IS security since company stocks are also commonly referred to as securities. Also as a common practice, many companies include a Safe Harbor statement at the end of their announcements that also contained the word security and therefore resulted in many false selections.

The author selected announcements for inclusion when the content was focused on IS security. Using the NIST (2011) definition, IS security is the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability (CIA) of a computer system and its information. The content of the 516 announcements were carefully reviewed and on the basis of their content, the author initially determined 135 announcements were valid for the study scope. The author used Lexis/Nexis to search for confounding events occurring the same day as each of the 135 selected events and following standard event-study practice, 16 announcements subsequently were removed due to the identification of confounding events. Additionally the author used the University of Chicago's Center for Research on Security Prices (CRSP) common stock returns database to validate the firms contained within the 135 events had detailed stock information available on the event date and another seven announcements were removed from scope due to insufficient CRSP data. The final data sample size of the study included 112 announcements as summarized in Table 2.

Table 2. Breakdown of Final Data Sample

Announcements	Quantity
Total initial announcements in Lexis/Nexis	651
Less: non-related and duplicate announcements	516
Number of valid announcements	135
Less: confounding affects	16
Less: firms with insufficient CRSP data	7
Final sample size	112

Table 3 presents descriptive statistics of the final data sample by year. All 112 announcements were made between 2003 and 2010.

Table 3. Final Data Sample Selection by Year

Year	Number of Announcements	% of Total
2003	8	7.2%
2004	21	18.6%
2005	26	23.2%
2006	24	21.4%
2007	8	7.2%
2008	9	8.0%
2009	8	7.2%
2010	8	7.2%

Finally, 34 different e-banking service providers are represented in the 112 study sample. The 34 e-banking firms included 18 firms listed on the NASDAQ stock exchange and 16 listed on the NYSE stock exchange. A complete listing of all 34 firms included in the study scope, as well as their stock symbol or ticker, their corresponding exchange, and their e-banking website location that qualified them as part of the study scope are reflected in Table 4.

Table 4. Service Provider Name, Ticker, Stock Exchange, and Website

Name (Ticker)	Exchange	e-banking website
Associated Banc Corp (ASBC)	NASDAQ	www.associatedbank.com
BB&T Corp (BBT)	NYSE	www.bbt.com
BOK Financial Corp (BOKF)	NASDAQ	www.bokf.com
Bank of America (BAC)	NYSE	www.bankofamerica.com
Bank of Hawaii (BOH)	NYSE	www.boh.com
CVB Financial Corp (CVBF)	NASDAQ	www.cbbank.com
Capital One Financial (COF)	NYSE	www.capitalone.com
Cascade Financial Corp (CASB)	NASDAQ	www.cascadebank.com
Citigroup Inc (C)	NYSE	www.citibank.com
Cobiz Financial (COBZ)	NASDAQ	www.cobizbank.com
Comerica Inc (CMA)	NYSE	www.comeria.com
Community Bank System Inc (CBU)	NYSE	www.communitybankna.com
Fifth Third Bancorp (FITB)	NASDAQ	www.53.com
Hancock Holding Co (HBHC)	NASDAQ	www.hancockbank.com
Heartland Financial USA (HTLF)	NASDAQ	www.htlf.com
JPMorgan Chase & Co (JPM)	NYSE	www.jpmorganchase.com
Key Corp (KEY)	NYSE	www.key.com
M&T Bank Corp (MTB)	NYSE	www.mtb.com
Northrim Bancorp Inc (NRIM)	NASDAQ	www.northrim.com
Peoples United Financial (PBCT)	NASDAQ	www.peoples.com
PNC Financial Service Group (PNC)	NYSE	www.pnc.com
Provident Bank (PBKS)	NASDAQ	www.provbank.com
Regions Financial Corp (RF)	NYSE	www.regions.com
Suffolk Bancorp (SUBK)	NASDAQ	www.scnb.com
Sun Bancorp Inc (SNBC)	NASDAQ	www.sunnbni.com
SunTrust Banks (STI)	NYSE	www.suntrust.com
Susquehanna Bancshares (SUSQ)	NASDAQ	www.susquehanna.net
Trico Bancshares (TCBK)	NASDAQ	www.tricountiesbank.com
US Bancorp (USB)	NYSE	www.usbancorp.com
Umpqua Holdings Corp (UMBQ)	NASDAQ	www.umpquabank.com
Unionbancal Corp (UB)	NYSE	www.unionbank.com
Unity Bancorp Inc (UNTY)	NASDAQ	www.unitybank.com
Washington Trust Bancorp (WASH)	NASDAQ	www.washtrust.com
Wells Fargo & Co (WFC)	NYSE	www.wellsfargo.com

Data Analysis

The final data sample was partitioned by the author based on announcement content and grouped into either the technology-focused or people-focused announcement

segments. This partitioning was needed in order to be able to test H_2 hypotheses. Almost 94% of the total data sample focused on IS technology announcements while only 6% of the total data sample focused on IS security people-focused announcements as provided in Table 5.

Table 5. Final Data Sample Selection by Announcement Type

Data Sample Partitions	% of total
Technology	105 (93.7%)
People	7 (6.3%)

The Eventus® software tool was used for calculating and reporting the advanced statistics necessary to complete this event study (Cowan, 2007). The statistical outcomes used to derive the study conclusions have been summarized in Table 6 below. Specifically the mean CARs observed for the 112 e-banking IS security announcements contained in the total data sample, the tests for significance of the effect including the Patell Z and Generalized Sign test results, and the number of positive and negative market reactions are presented. As discussed in chapter three, the Patell Z test is a standardized abnormal return test approach for event studies, which tests for the effects of outliers on the significance of results since event studies are sensitive to outliers (Cavusoglu et al., 2004a). The Generalized Sign test enabled a check of the robustness of study conclusions by comparing the proportion of positive CARs around an event to the proportion from a period unaffected by the event (Cowan, 2007). Both the Patell Z and Generalized Sign test was used to validate the study results.

Table 6. Eventus® Output: CAR Results for One Day Event Window (0, 0)

	N	Mean CAR	Patell Z	*p*-value	Generalized Sign	*p*-value	Market Reaction positive	negative
Full Sample:	112	0.10%	0.489	0.312	-0.117	0.453	54	58
Sample Partitions:								
- Technology only	105	0.15%	0.725	0.234	0.358	0.360	53	52
- People only	7	-0.64%	-0.852	0.197	-1.853	0.031	1	6

Findings

As discussed, the H_1 general study hypothesis proposed was that investments in IS security will have a statistically significant impact on e-banking market values. For the full data sample the mean cumulative abnormal return is different from zero, indicating that the events did impact market values. More specifically, the results of the test of H_1 using the standard event study methodology revealed that the mean CAR was 0.10% which is statistically significant at conventional levels. The CAR value of 0.10% however indicates a weak relationship (see Appendix B for Correlation index) between the changes in market values relative to the selected announcements. As explained, the testing procedure for event studies typically reports one parametric and one nonparametric test statistic in order to examine the robustness of study results (Cowan, 1992). The results of the H_1 parametric and nonparametric tests further revealed that the CAR value of 0.10% is likely the result of random errors since the *p*-values of the Patell Z test were 0.312 and for the Generalized Sign test were 0.453 indicating there is limited statistical evidence to support a direct market value impact resulting from the selected IS security investment announcements. On this basis, the H_1 hypothesis that investments made in IS security will result in a statistically significant impact on e-banking market values is supported however the impact appears to not be significant.

In order to further understand the impacts of the selected IS security investment announcements and the resulting market reactions, as previously described the study sample of events was partitioned into two groups reflecting the type of investment announced: technology or people. As discussed, the H_2a study hypothesis proposed was investments in IS security technologies will have a statistically significant impact on e-banking market values. For the technology partition of the data sample, the mean cumulative abnormal return is different from zero, indicating that the events did impact market values. More specifically, for investments in IS security technologies, the mean CAR was 0.15% which is statistically significant at conventional levels. The *p*-value of the Patell Z test was 0.234 and the *p*-value for the Generalized Sign test was 0.360 however, indicating a weak relationship with limited statistical evidence to support a direct relationship between market value impacts and the selected IS security technology investment announcements. Further confirmation of this outcome was reflected in the Eventus® output that indicated there were 53 positive market reactions and 52 negative market reactions across the 105 events measuring IS security technology investments and therefore the impact did not appear to be significant.

Finally, as discussed the H_2b study hypothesis proposed was investments in IS security people will have a statistically significant impact on e-banking market values. For the people partition of the data sample, the mean cumulative abnormal return is different from zero, indicating that investments in IS security people did have a statistically significant impact on e-banking market values. More specifically, for investments in IS security people, the mean CAR was -0.64% which appeared to indicate a partially significant or moderate relationship to market value impacts. As previously

described, positive abnormal returns would imply announcements created positive market value impacts whereas negative abnormal returns would indicate the announcements actually destroyed market values. The negative CAR was further explained by the Eventus® output that indicated there was only one positive market reaction to announcements concerning IS security people as compared to six negative market reactions to the same type of announcements. The *p*-value of the Patell Z test was 0.197 and the *p*-value of the Generalized Sign test was 0.031 indicating there is some statistical evidence to support a direct relationship between market value impacts and IS security people investment announcements.

It is important to note however, the people partition of the data sample included only seven announcements out of the total 112 announcements contained in the full study data set. As previously discussed, the number of usable events found in the event studies summarized in the literature review ranged from 23 (Hovav & D'Arcy, 2003) up to 640 (Dewan & Ren, 2007). More specifically, security-specific IS event studies averaged a total of 40 events (Campbell et al., 2003; Cavusoglu et al., 2004a; Hovav & D'Arcy, 2003, 2005; & Andoh-Baidoo et al., 2010) while the personnel-specific IS event studies averaged a total of 110 events (Chatterjee et al., 2001; Guan et al., 2006; Khallaf & Skantz, 2007; & Tian et al., 2011). To minimize the effect of this small sample size, following precedent established by Hovav and D'Arcy (2003), the event day was re-validated for each of the seven announcements included in the study results. Any conclusions based on a sample size of seven announcements however, must be considered preliminary and require further validation from other researchers using a

larger sample population to validate this study finding. A summary of the study hypotheses testing results are provided in table 7.

Table 7. Summary of Hypotheses Testing Results

Hypothesis	Result
H_1: Investments in IS security will have a statistically significant impact on e-banking market values.	Not significant
H_2a: Investments in IS security technologies will have a statistically significant impact on e-banking market values.	Not significant
H_2b: Investments in IS security people will have a statistically significant impact on e-banking market values.	Partially significant

Summary of Results

The overall objective of this study was to examine the market value impacts of IS security investment announcements made by e-banking service providers. It was hypothesized that announcements of IS security investments would result in statistically significant changes in market values. It was also hypothesized that two sub-segments of the selected security investment announcements would support statistically significant changes in the market values of e-banking service providers. These hypotheses were tested by measuring stock market reactions to the IS security announcements selected from an eight-year period (2003-2010). The H_1 and H_2 study hypotheses were supported as study findings did indicate statistically significant market reactions to e-banking firms making IS security investment announcements. Based on further examination of the two sub-segments of the study data sample, IS security people investment announcements resulted in moderate market value impacts whereas IS security technology investments

resulted in relatively weak or modest impacts to the market values of announcing e-banking firms.

Chapter 5

Conclusions, Implications, Recommendations, and Summary

Introduction

This research study investigated the economic impacts of IS security investment announcements for e-banking service providers. The author used the event study methodology to measure the market value changes resulting from IS security investment announcements across 34 different e-banking service providers. Within the data sample, the market value impacts resulting from IS security technology and people investments were examined.

Conclusions

The findings from this research provided evidence of market value reactions occurring when IS security investment announcements are made by e-banking service providers. Based on the study sample, market reactions to IS security people investments were moderate as compared to weak reactions to IS security technology investment announcements. On this basis it would appear that stock market participants are somewhat discriminating when assessing the market value impacts resulting from different types of IS security investment announcements.

While the study results were statistically significant, the weak relationship between IS security investment announcements and market value impacts indicated as a result of the

study could be explained in several ways. Considering the overall event-study results, it is likely investors do not perceive IS security investment announcements made by e-banking service providers as new information since it is to be expected that all e-banking providers are concerned with regulatory compliance and therefore are investing in IS security. In addition, as previously mentioned regulatory changes are often debated in the public arena so it is not unreasonable to expect that any accompanying market value effects are gradually reflected in the market values of impacted firms (Campbell, Lo, & MacKinlay, 1997).

Additionally, Gordon et al. (2010) found that firms in the Banking and Finance industries who disclosed IS security investments in their mandatory SEC reporting experienced no significant market value impacts. These study results support the Gordon et al. (2010) study conclusions. As discussed, given the many regulations the banking industry must support, regulatory compliance is likely perceived by investors as a form of IS security assurance. In other words, IS security investment announcements made by e-banking service providers resulted in weak market value impacts because investors understand that mandatory regulatory compliance represents a firm's commitment to creating a secure computing environment. As a result, e-banking information systems are perceived as secure therefore, disclosing IS security investments results in weak or no significant changes to market values.

The study results also indicated a weak market reaction to announcements of IS security technology investments. It is very probable that investors expect e-banking service providers to frequently change and leverage new security technologies or strategies in order to accommodate new regulatory changes, end-user demands (e.g.,

Mobile banking), or to mitigate new IS security threats and vulnerabilities. Therefore due to the very nature of technology and its frequent changes, the announcement of new IS security technology investments do not result in sizable market value impacts for announcing firms. This finding is consistent with Cha, Pingry, and Thatcher's 2009 survey of business leaders regarding technology spending priorities and the position that IS security investments are typically not considered strategic and therefore do little to improve firm values.

Finally, the study results indicated a moderate and negative market reaction to announcements of IS security people investments. Khallaf and Skantz (2007) found that much of the research that explores the economic value of technology investments bypasses the role of personnel expertise therefore it is possible that stockholders are not fully aware of the value IS security experts provide to firms. More specifically, Burkett (2012) found that IS security people are many times viewed as inhibiting operations since they tend to identify problems with the protection of IS assets after they have been designed and deployed. If investors do not perceive that IS security personnel expertise offers value to firms then apparently by highlighting IS security people investments, investors can only perceive negative impacts as expressed through the moderately negative market reactions found with this study. This finding is consistent with the Khallaf and Skantz (2007) study findings.

Study Limitations

This study shares the limitations common to all event studies and therefore must be interpreted with caution for several reasons. First, the event study methodology captures only the stock market's initial reaction to the event. Over time reactions to events may

change but these changes are not observable or testable using this methodology (Campbell et al., 1997). Second, the results of event studies may be sensitive to confounding events and researcher decisions regarding event windows, estimation periods, significance levels selected for hypotheses testing and validation and sample selection. All firms with selected events were checked for confounding events and removed from the study scope if found. The study event window was contained to the single day of the announcement in order to reduce the possibility of confounding factors influencing the results and to increase the power of the statistical tests. The estimation period selected for the study was the standard Eventus® estimation period that used data from a 255 trading day estimation period that ended 46 trading days before the event date (Cowan, 2007). Even after these cautionary measures however, it is possible the study was impacted by confounding events not reported in the press or found by the author as part of the data collection phase of the study.

Also the study sample selection represents only publicly disclosed information concerning IS security investments. Many IS security investments made by e-banking service providers are not reported to the media and therefore the study sample may not be representative of the overall population of IS security investments being made by e-banking service providers. Additionally the nature of the IS security investment announcements reported to the press may be quite different from those not reported. As a consequence, the study results are likely not generalizable to IS security investments that are not publicly disclosed. Also while the overall study sample was large enough to conduct statistical analysis, it is relatively small in absolute terms and therefore a larger sample size would be more desirable. Finally, by using different sources, queries and

search methods it is possible that other researchers may identify a different sample of IS security investment announcements made by e-banking service providers and consequently obtain different study results.

Implications

The results of this study have both academic research and practical implications.

Research Implications

The study contributes to the academic event study literature as well as the literature examining the economic effects of information systems security. Using a standard event study methodology, the overall study results showed that investors had weak reactions to announcements made by e-banking service providers of IS security investments. The results of the study expand the list of known influential factors regarding stock market reactions to include technology and people-focused IS security investments. Other scholars may build on these study results and possibly validate these findings through further event studies focused on IS security investments. Future research may look for other influential factors including industry and firm characteristics such as size or diversification level to clarify IS security investment market impacts.

The objective of IS security is to minimize a firm's informational risks through controls that are selected in support of the firm's risk thresholds (Ghernaouti-Helie, 2009). IS security requires proactive risk management and mitigation. Risk management requires an understanding of security costs as well as security benefits placed on a common scale so that executive management can determine when to incur or avoid IS security costs. No single index or accounting measure however, can answer the basic questions about the optimal investment levels required for the prevention of all security

risks (Bojanc & Jerman-Blazic, 2008). Balancing the costs of implementing selected security measures against the losses anticipated from security incidents will continue to be difficult until both the positive and negative financial impacts of such decisions can be measured. Future research that can articulate both the cost and the value or benefit of IS security investments and the resulting impacts to a firm's risk profile would be beneficial to both the academic and professional communities.

Practical Implications

The author concluded that investors do not perceive IS security investment announcements as a critical factor in assessing the value of e-banking firms. However value perceptions can change over time (Garbajose & Perez, 2010). It is possible that a steady campaign of publicly disclosed IS security investments can convey a firm's strength in IS security and, thereby, increase stock price values over time. Perhaps more targeted announcements that help investors see and understand the differences between high-profile/low-probability events such as attacks by cyberterrorists and low-profile/high-probability events such as installation of malware on end-user machines may be a more useful message to convey to the marketplace in order to influence the market values of firms making IS security-related e-banking investment announcements.

As discussed in Chapter 2, Cavusoglu et al. (2004a) showed that publicly disclosed IS security breaches resulted in investors questioning the financial health of the firms since it suggested a lack of adequate technology controls, failure to observe policy or processes, or a lack of management oversight or security awareness which consequently resulted in lower stock price values. If a company is perceived as having a risk-filled environment due to known breaches or attacks, announcements of investments in IS

security technologies intended to specifically address those concerns could potentially be used to restore investor confidence. Managers however should not view IS security investments in technologies or people as a means of compensating for organizational problems or issues. Ultimately effective management of IS security requires acceptance of the idea that it is not technically feasible or financially viable to implement protections for all identified IS security risks therefore IS security investments must be effectively measured and risk levels consciously selected in order to implement the right technical and operational protections to support a firm's selected risk posture.

Recommendations

Linking IS security investments to firm performance is difficult since so many factors affect firm performance and separating out the impact of just the IS security investment from other effects is not an easy task. IS investments are found embedded throughout organizations to enable business strategies, process improvements, or new capabilities making it very difficult for researchers to pinpoint and measure the IS security contribution separate from the new strategy or capability (Mittal & Nault, 2009). While far from perfect, the event-study method is widely accepted as a useful tool for performing this type of analysis and therefore might be applied to other IS security issues that have unclear value impacts.

Very little has been done to legislate IS security beyond the financial and health care industries (Hoffman, 2011). A study of IS security investments made in industries that do not have a heavy regulatory component could result in a revealing industry-level impact assessment of IS security investments. Also an event study focused on the market value effects of state legislation could also be helpful in potentially clarifying the effect of

various types or levels of legislation on investor responses to such announcements (Gatzlaff & McCullough, 2010). Future research that studies the market value impacts resulting from different laws and regulations would be helpful in clarifying the value impacts resulting from different pieces of legislation.

Additionally, the market value impacts of IS security investments grouped by Confidentiality, Integrity, and Availability (CIA) could help researchers and practioners to better understand value impacts across the spectrum of IS security investment types. The results of such research could provide additional insights to firms in balancing the costs of IS security controls with the benefits of increased security levels based on credible and quantifiable market value impacts observed for various IS security investment types (Goel & Shawky, 2009). Through such academic inquiry, IS researchers as well as accounting and business managers could gain deeper insights into why and how the market responds to IS security investments and their related impacts to firm values.

Summary

The continued demand for IS investments such as security, require careful consideration of the delivered financial value (Wilkin & Chenhall, 2010). Investments in IS security reflect the technology and policy landscape of a given firm, as well as organizational priorities, culture, and investment practices (Pfleeger & Ciszek, 2008). E-banking investments in IS security technology and people necessary to comply with U.S. laws and regulations can be measured using the event study method in order to understand their impacts on the firm's stock price performance (Morris & Strickland, 2008/2009). Understanding the financial value resulting from IS security investments is

critically important to successful organizations since poor IS investment decisions adversely impact a firm's market performance (Adomavicius, Bockstedt, & Gupta, 2008). This study investigated the relationship between e-banking investments in IS security technology and people and their market value impacts for selected e-banking firms.

As summarized in the literature review, even after many years of research studying the impacts of IS investments of all types, identification and measurement of the financial impacts resulting from technology investments is difficult to determine (Wilkin & Chenhall, 2010). Poor IS investments can destroy corporate wealth while savvy IS investments can also create corporate wealth (Parent & Reich, 2009). For the last decade, researchers have realized that security and privacy are not just a technical problem; there is a major economic component as supported by the rapid increase of investments in IS security (Bojanc & Jerman-Blazic, 2008). An event study is a robust and proven way to study the relationship between IS security investments and the impacts to firm market values (Nagm & Kautz, 2008).

Event studies have been used by IS researchers since the early 1990's and continue to be used as a viable research approach today. In particular, of the 44 IS event studies conducted over the last 12 years and as surveyed in the previous literature review discussion (see Appendix A for complete summary list), 11 security-specific IS event studies examined the market value impacts resulting from IS security breaches, attacks, or vulnerabilities. Specifically, based on the findings from the event studies conducted by Campbell et al. (2003), Cavusoglu et al. (2004a), Andoh-Baidoo et al. (2006), Goel and Shawky (2009), Andoh-Baidoo et al. (2010), and Gatzlaff and McCullough (2010), the negative market value impacts that can result from security breaches has been

quantified. Additionally, the event studies conducted by Ettredge and Richardson (2003), and Hovav and D'Arcy (2003) provided a measure of the market value impacts resulting from various types of IS attacks. Finally, the Wang et al. (2010), Hovav and D'Arcy (2005), and Telang and Wattal (2007) study results provided a measure of the market value impacts resulting from various types of IS security vulnerabilities. While the results of the aforementioned IS security-specific event studies facilitated an understanding of the negative market value impacts associated with security breaches, attacks, and vulnerabilities, an understanding of the positive market value impacts resulting from investments in IS security was still needed to fully understand the cost/benefit ratio of the investment (Geer, 2007). The author conducted a comprehensive search of the ACM Digital Library, IEEE Computer Society Digital Library, ProQuest Computing, Wiley Online Library, and Computers and Applied Sciences Complete to examine previous research on the market value impacts resulting from investments in IS security. No event study was found that examined the market value impacts of IS security investments for e-banking service providers. The results of this event study are intended to address this gap in the literature.

The overall objective of this study was to examine the market value impacts of IS security investment announcements made by e-banking service providers. It was hypothesized that announcements of IS security investments would result in statistically significant changes in market values. It was also hypothesized that two sub-segments of the selected security investment announcements would support statistically significant changes in the market values of e-banking service providers. These hypotheses were tested by measuring stock market reactions to the IS security announcements selected

from an eight-year period (2003-2010). The H_1 and H_2 study hypotheses were supported as study findings did indicate statistically significant market reactions to e-banking firms making IS security investment announcements. Based on further examination of the two sub-segments of the study data sample, IS security people investment announcements resulted in partially significant but negative market value impacts whereas IS security technology investments resulted in relatively weak or non-significant but positive impacts to the market values of announcing e-banking firms.

No experimental adjustments or changes to the traditional event study were included as part of the study scope since a standard or traditional event study was sufficient to derive study conclusions. The author also used the Eventus® software, which was explicitly designed to execute traditional event studies (Cowan, 2007). As described, the event study methodology uses model-based statistical inference as the primary method of deduction (Campbell et al., 1997). Therefore a market model was used to compute the abnormal returns for all firms in the study scope. Abnormal returns were compared to the market model and the resulting cumulative abnormal returns were assumed to measure the effect of the event on the market values of the selected firms. As is true with every event study summarized in the literature review, statistical testing was also used to validate event study findings.

The findings from this research provided evidence of market value reactions occurring when IS security investment announcements are made by e-banking service providers. Based on the study sample, market reactions to IS security people investments were moderate as compared to weak reactions to IS security technology investment announcements. On this basis it would appear that stock market participants are

somewhat discriminating when assessing the market value impacts resulting from different types of IS security investment announcements.

While the study results were statistically significant, the weak relationship between IS security investment announcements and market value impacts indicated as a result of the study could be explained in several ways. Considering the overall event-study results, it is likely investors do not perceive IS security investment announcements made by e-banking service providers as new information since it is to be expected that all e-banking providers are concerned with regulatory compliance and therefore are investing in IS security. In addition, as previously mentioned regulatory changes are often debated in the public arena so it is not unreasonable to expect that any accompanying market value effects are gradually reflected in the market values of impacted firms (Campbell, Lo, & MacKinlay, 1997).

Additionally, Gordon et al. (2010) found that firms in the Banking and Finance industries who disclosed IS security investments in their mandatory SEC reporting experienced no significant market value impacts. These study results support the Gordon et al. (2010) study conclusions. As discussed, given the many regulations the banking industry must support, regulatory compliance is likely perceived by investors as a form of IS security assurance. In other words, IS security investment announcements made by e-banking service providers resulted in weak market value impacts because investors understand that mandatory regulatory compliance represents a firm's commitment to creating a secure computing environment. As a result, e-banking information systems are perceived as secure therefore, disclosing IS security investments results in weak or no significant changes to market values.

The study results also indicated a weak market reaction to announcements of IS security technology investments. It is very probable that investors expect e-banking service providers to frequently change and leverage new security technologies or strategies in order to accommodate new regulatory changes, end-user demands (e.g., Mobile banking), or to mitigate new IS security threats and vulnerabilities. Therefore due to the very nature of technology and its frequent changes, the announcement of new IS security technology investments do not result in sizable market value impacts for announcing firms. This finding is consistent with Cha, Pingry, and Thatcher's 2009 survey of business leaders regarding technology spending priorities and the position that IS security investments are typically not considered strategic and therefore do little to improve firm values.

Finally, the study results indicated a moderate and negative market reaction to announcements of IS security people investments. Khallaf and Skantz (2007) found that much of the research that explores the economic value of technology investments bypasses the role of personnel expertise therefore it is possible that stockholders are not fully aware of the value IS security experts provide to firms. More specifically, Burkett (2012) found that IS security people are many times viewed as inhibiting operations since they tend to identify problems with the protection of IS assets after they have been designed and deployed. If investors do not perceive that IS security personnel expertise offers value to firms then apparently by highlighting IS security people investments, investors can only perceive negative impacts as expressed through the moderately negative market reactions found with this study. This finding is consistent with the Khallaf and Skantz (2007) study findings.

The results of this study have both academic research and practical implications. The study contributes to the academic event study literature as well as the literature examining the economic effects of information systems security. Using a standard event study methodology, the overall study results showed that investors had weak reactions to announcements made by e-banking service providers of IS security investments. The results of the study expand the list of known influential factors regarding stock market reactions to include technology and people-focused IS security investments. Other scholars may build on these study results and possibly validate these findings through further event studies focused on IS security investments. Future research may look for other influential factors including industry and firm characteristics such as size or diversification level to clarify IS security investment market impacts.

Appendix A: List of IS Event Studies Summarized in Literature Review

General IS event studies	Focus of Announcements
Chatterjee, Pacini, and Sambamurthy (2002)	IS infrastructure investments
Dehning, Richardson, and Zmud (2003)	Transformational IS investments
Roztocki and Weistroffer (2006)	Cost management and IS investments
Darden, Stylianou, and Kumar (2006/2007)	Customer satisfaction and investments
Sabherwal and Sabherwal (2007)	Knowledge Management investments
Nagm and Kautz (2008)	IS investments by Australian firms
Png, Wang, and Wang (2008)	IS government enforcement impacts
Morris and Strickland (2008/2009)	IS process improvement investments
Roztocki and Weistroffer (2009)	Activity-based costing and investments
Bharadwaj, Keil, and Mahring (2009)	IT failure impacts
Choi & Jong (2010)	Knowledge Management investments
IS Outsourcing event studies	
Hayes, Hunton, and Reck (2000)	IS outsourcing
Agrawal, Kishore, and Rao (2006)	E-business outsourcing
Duan, Grover, and Balakrishnan (2009)	Business process outsourcing
Jeong and Stylianou (2010)	ASP outsourcing
IS ERP/EAI event studies	
Hayes, Hunton, and Reck (2001)	ERP investments
Ranganathan and Brown (2006)	ERP investments
Roztocki and Weistroffer (2008)	EAI and ERP investments
Roztocki and Weistroffer (2009)	EAI investments
IS e-Commerce event studies	
Subramani and Walden (2001)	e-Commerce investments
Dehning, Richardson, Urbaczewski, and Wells (2004)	e-Commerce initiatives investments

Dewan and Ren (2007)	e-Commerce IS investments
Baek, Lee, and Lim (2008)	e-Commerce IS service failures
Benbunan-Fich and Fich (2004)	Effects of web traffic announcements
Benbunan-Fich and Fich (2005)	Effects of refining a web presence
Industry-specific IS event studies	**Focus of Announcements**
Im, Dow, and Grover (2001)	IS investments in finance and manufacturing sectors
Hunter (2003)	IS investments in retail sector
Raghu, Woo, Mohan, and Rao (2008)	IS patent infringement in the IS sector
Jeong and Lu (2008)	RFID investments in manufacturing and service sectors
Personnel-specific IS event studies	
Chatterjee, Richardson, and Zmud (2001)	New CIO positions
Guan, Sutton, Chang, and Arnold (2006)	New CIO positions
Khallaf and Skantz (2007)	New CIO positions
Tian, Haleblian, and Rajagopalan (2011)	New CEO selections
Security-specific IS event studies	
Campbell, Gordon, Loeb, and Zhou (2003)	Security breaches
Cavusoglu, Mishra, and Raghunathan (2004)	Security breaches
Andoh-Baidoo and Osei-Bryson (2006)	Security breaches
Goel and Shawky (2009)	Security breaches
Andoh-Baidoo, Amoako-Gyampah, and Osei-Bryson (2010)	Security breaches
Gatzlaff and McCullough (2010)	Security breaches
Ettredge and Richardson (2003)	Hacker attacks
Hovav and D'Arcy (2003)	Denial-of-Service attacks
Wang, Xiao, and Rao (2010)	Viruses
Hovav and D'Arcy (2005)	Viruses
Telang and Wattal (2007)	Software vulnerabilities

Appendix B: Correlation Index

Correlations between	Are said to be
.8 and 1.0	Very strong
.6 and .8	Strong
.4 and .6	Moderate
.2 and .4	Weak
.0 and .2	Very weak

References

Adomavicius, G., Bockstedt, J., & Gupta, A. (2008). Making sense of technology trends in the information technology landscape: A design science approach. *MIS Quarterly*, *32*(4), 779-809.

Agrawal, M., Kishore, R., & Rao, H. (2006). Market reactions to e-business outsourcing announcements: An event study. *Information & Management*, *43*(7), 861-873.

Anderson, E., & Choobineh, J. (2008). Enterprise information security strategies. *Computers & Security, 27*, 22-29.

Andoh-Baidoo, F., Amoako-Gyampah, K., & Osei-Bryson, K. (2010). How internet security breaches harm market value. *IEEE Security & Privacy*, January/ February, 36-42.

Andoh-Baidoo, F., & Osei-Bryson, K. (2006). Exploring the characteristics of internet security breaches that impact the market value of breached firms. *Expert Systems with Applications, 32*, 703-725.

Arduini, F., & Morabito, V. (2010). Business continuity and the banking industry. *Communications of the ACM*, *53*(3), 121-125.

Baek, S., Lee, S., & Lim, G. (2008). Exploring impacts of IS service failure on firm's market value. *Proceedings of the IEEE Fourth International Conference on Networked Computing and Advanced Information Management, Korea,* 450-454.

Benbunan-Fich, R., & Fich, E. (2004). Effects of web traffic announcements on firm value. *International Journal of Electronic Commerce, 8*(4), 161-181.

Benbunan-Fich, R., & Fich, E. (2005). Measuring the value of refining a web presence. *Journal of Electronic Commerce in Organizations, 3*(1), 35-52.

Bharadwaj, A., Keil, M., & Mahring, M. (2009). Effects of information technology failures on the market value of firms. *Journal of Strategic Information Systems, 18*, 66-79.

Bienvenu, E. (2012). *Accounting and Business Dictionary*. Memphis, U.S.A.: General Books LLC.

Bo, L., & Congwei, X. (2009). E-commerce security risk analysis and management strategies of commercial banks. *Proceedings of the IEEE International Forum on Information Technology and Applications, China,* 423-425.

Bodie, Z., Kane, A., & Marcus, A. (2008). *Investments.* New York, U.S.A.: McGraw-Hill Companies, Inc.

Bojanc, R. & Jerman-Blazic, B. (2008). Towards a standard approach for quantifying an ICT security investment. *Computer Standards & Interfaces, 30*(3), 216-222.

Breaux, T., Anton, A., Boucher, K., & Dorfman, M. (2009). IT compliance: aligning legal and product requirements. *IEEE IT Pro*, September/October, 54-58.

Burger, K. (2012). Battle of the Budgets. *Bank Systems & Technology, 49*(1), 1.

Burkett, J. (2012). Business security architecture: weaving information security into your organization's enterprise architecture through SABSA. Information Security Journal, 21, 47-54.

Burns, R., & Peterson, Z. (2010). Security constructs for regulatory-compliant storage. *Communications of the ACM, 53*(1), 126-130.

Cable, J., & Holland, K. (1999). Regression vs. non-regression models of normal returns: Implications for event studies. *Economic Letters, 64*, 81-85.

Campbell, C., Cowan, A., & Salotti, V. (2010). Multi-country event study methods. *Journal of Banking & Finance*, *34*, 3078-3090.

Campbell, J., Lo, A., & MacKinlay, A. (1997). *The Econometrics of Financial Markets.* Princeton, New Jersey: Princeton University Press.

Campbell, K., Gordon, L., Loeb, M., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: Empirical evidence from the stock market. *Journal of Computer Security*, *11*(3), 431-448.

Carin, L., Cybenko, G., & Hughes, J. (2008). Cybersecurity strategies: The QuERIES methodology. *IEEE Computer Magazine, 41*(8), 20-26.

Cassini, J., Medlin, B., & Romaniello, A. (2008). Laws and regulations dealing with information security and privacy: An investigative study. *International Journal of Information Security & Privacy, 2*(2), 70-82.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004a). The effect of Internet security breach announcements on market value: Capital market reactions for breached firms and Internet security developers. *The International Journal of Electronic Commerce, 9*(1), 69-104.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004b). A model for evaluating IS security investments. *Communications of the ACM, 47*(7), 87-92.

Center for Research on Security Prices (CRSP) definition. Retrieved June 10, 2012 from http://www.crsp.com/crsp/about/index.html.

Cha, H., Pingry, D., & Thatcher, M. (2009). What determines IS spending priorities? *Communications of the ACM, 52*(8), 105-110.

Chatterjee, D., Pacini, C., & Sambamurthy, V. (2002). The shareholder-wealth and trading-volume effects of information-technology infrastructure investments. *Journal of Management Information Systems*, *19*(2), 7-42.

Chatterjee, D., Richardson, V., & Zmud, R. (2001). Examining the shareholder wealth effects of announcements of newly created CIO positions. *MIS Quarterly, 25*(1), 43-70.

Choi, B., & Jong, A. (2010). Assessing the impact of knowledge management strategies announcements on the market value of firms. *Information & Management, 47*, 42-52.

Corrado, C. (2011). Event studies: A methodology review. *Accounting and Finance, 51*, 207-234.

Cowan, A. (1992). Nonparametric event study tests. *Review of Quantitative Finance & Accounting, 2*, 343-358.

Cowan, A. (2007). *Eventus® 8.0 User's Guide, Standard Edition 2.1.* Cowan Research LC, Ames, Iowa.

Dardan, S., Stylianou, A., & Kumar, R. (2006/2007). The impact of customer-related IS investments on customer satisfaction and shareholder returns. *The Journal of Computer Information Systems*, *47*(2), 100-111.

Dehning, B., Richardson, V., Urbaczewski, A., & Wells, J. (2004). Reexamining the value relevance of e-commerce initiatives. *Journal of Management Information Systems, 21*(1), 55-82.

Dehning, B., Richardson, V., & Zmud, R. (2003). The value relevance of announcements of transformational information technology investments. *MIS Quarterly*, *27*(4), 637-656.

Dewan, S., & Ren, F. (2007). Risk and return of information technology initiatives: Evidence from electronic commerce announcements. *Information Systems Research 18*(4), 370-394.

Dlamini, M., Eloff, J., & Eloff, M. (2009). Information security: the moving target. *Computers & Security, 28*, 189-198.

Dos Santos, B., Peffers, K., & Mauer, D. (1993). The impact of information technology investment announcements on the market value of the firm. *Information Systems Research, 4*(1), 1-23.

Downes, J., & Goodman, J. (1998). *Dictionary of Finance and Investment Terms*. Hauppauge, NY: Barron's Educational Series, Inc.

Duan, C., Grover, V., & Balakrishnan, N. (2009). Business process outsourcing: An event study on the nature of processes and firm valuation. *European Journal of Information Systems*, *18*, 442-457.

Ettredge, M., & Richardson, V. (2003). Information transfer among internet firms: The case of hacker attacks. *Journal of Information Systems, 17*(2), 71-82.

Fama, E.F. (1970). Efficient capital markets: A review of theory and empirical work. *The Journal of Finance*, *25*(2), 383-417.

Fama, E.F. (1991). Efficient capital markets: II. *The Journal of Finance*, *46*(5), 1575-1617.

Fama, E.F. (1998). Market efficiency, long-term returns, and behavioral finance. *Journal of Financial Economics, 49*, 283-306.

Ferraino, C. (2010). The *Complete Dictionary of Accounting and Bookkeeping Terms.* Ocala, Florida: Atlantic Publishing Group, Inc.

Fisher, D. (2010). The exam tide is changing. *ABA Banking Journal*, *102*(6), 22-24.

Gant, D. (2009). Obligation vs. opportunity. *Risk Management, 56*(7), 58-60.

Gatzlaff, K. & McCullough, K. (2010). The effect of data breaches on shareholder wealth. *Risk Management and Insurance Review, 13*(1), 61-83.

Geer, D. (2007). The evolution of security. *ACM Queue*, 5(3), 30-33.

Ghernaouti-Helie, S. (2009). An inclusive information society needs a global approach for information security. *Proceedings of the IEEE International conference on Availability, Reliability, and Security*, *Japan,* 658-662.

Goel, S., & Shawky, H. (2009). Estimating the market impact of security breach announcements on firm values. *Information & Management, 46*, 404-410.

Gordon, L., & Loeb, M. (2006). Budgeting process for information security expenditures. *Communications of the ACM*, *49*(1), 121-125.

Gordon, L., Loeb, M., Sohail, T. (2010). Market value of voluntary disclosures concerning information security. *MIS Quarterly, 34*(3), 567-594.

Gordon, L., Loeb, M., Sohail, T., Tseng, C., & Zhou, L. (2008). Cybersecurity, capital allocations, and management control systems. *European Accounting Review*, *17*(2), 215-241.

Guan, L., Sutton, S., Chang, C., & Arnold, V. (2006). Further evidence on shareholder wealth effects of announcements for newly created CIO positions. *The Database for Advances in Information Systems*, *37*(2), 176-187.

Hayes, D., Hunton, J., & Reck, J. (2000). Information systems outsourcing announcements: Investigating the impact on the market value of contract-granting firms. *Journal of Information Systems, 14*(2), 109-125.

Hayes, D., Hunton, J., & Reck, J. (2001). Market reaction to ERP implementation announcements. *Journal of Information Systems, 15*(1), 3-18.

Ho, S., & Mallick, S. (2010). The impact of information technology on the banking industry. *Journal of the Operational Research Society, 61*(2), 211-221.

Hoffmann, L. (2011). Risky Business. *Communications of the ACM, 54*(11), 20.

Hovav, A., & D'Arcy, J. (2003). The impact of denial-of-service attack announcements on the market value of firms. *Risk Management and Insurance Review, 6*(2), 97-121.

Hovav, A., & D'Arcy, J. (2005). Capital market reaction to defective IS products: The case of computer viruses. *Computers & Security*, *24*(5), 409-424.

Howell, J., & Wei, J. (2010). Value increasing model in commercial e-banking. *The Journal of Computer Information Systems, 51*(1), 72-81.

Hunter, S. (2003). Information technology, organizational learning, and the market value of the firm. *Journal of Information Technology Theory and Application, 5*(1), 1-28.

Ifinedo, P. (2008). IS security and privacy issues in global financial services institutions: Do socio-economic and cultural factors matter? *Proceedings of the IEEE Sixth Annual Conference on Privacy, Security, and Trust, Canada,* 75-84.

Im, K., Dow, K., & Grover, V. (2001). Research Report: A reexamination of IS investment and the market value of the firm – an event study methodology. *Information Systems Research*, *12*(1), 103-117.

Islam, S., Mouratidis, H., & Jurjens, J. (2011). A framework to support alignment of secure software engineering with legal regulations. *Software and Systems Modeling, 10*(3), 369-394.

Jang, W., & Chen, C. (2009). Defendant firms and response to legal crises: Effect on shareholder value. *Journal of Contingencies and Crisis Management, 17*(2), 108-117.

Jeong, B., & Lu, Y. (2008). The impact of radio frequency identification (RFID) investment announcements on the market value of the firm. *Journal of Theoretical and Applied Electronic Commerce Research*, *3*(1), 41-54.

Jeong, B., & Stylianou, A. (2010). Market reaction to application service provider (ASP) adoption: An empirical investigation. *Information & Management, 47*(3), 176-187.

Johnston, A. & Hale, R. (2008). Improved security through information security governance. *Communications of the ACM, 52*(1), 126-128.

Johnston, A. & Warkentin, M. (2010). Fear appeals and information security behaviors: an empirical study. *MIS Quarterly, 34*(3), 549-566.

Kauffman, R.J., Lee, Y.J., & Sougstad, R. (2009). Cost-effective firm investments in customer information privacy. *IEEE Proceedings of the 42nd Hawaii International Conference on System Sciences, USA,* 1-10.

Kendall, K. & Kendall, J. (2008). *Systems Analysis and Design.* Upper Saddle River, New Jersey: Pearson Education, Inc.

Khallaf, A., & Skantz, T. (2007). The effects of information technology expertise on the market value of a firm. *Journal of Information Systems*, *21*(1), 83-105.

Khansa, L. & Liginlal, D. (2009). Quantifying the benefits of investing in information security. *Communications of the ACM, 52*(11), 113-117.

Kibiloski, M., (2007). How to finance IS and handle change. *Financial Executive, 23*(2), 58-60.

Lampson, B. (2009). Usable security: How to get it. *Communications of the ACM*, *52*(11), 25-27).

Liao, Z., & Wong, W. (2008). The determinants of customer interactions with internet-enabled e-banking services. *Journal of the Operational Research Society*, *59*(9), 1201-1210.

Magnusson, C. (2011). ICT pollution and liability. *ACM SIGCAS Computers and Society, 41*(1), 48-53.

Maguire, J., & Miller, G. (2010). Web-application security: From reactive to proactive. *IEEE IT Professional, 12*(4), 7-9.

McWilliams, A., & Siegel, D. (1997). Event studies in management research: Theoretical and empirical issues. *Academy of Management Journal*, *40*(3), 626-657.

Mittal, N., & Nault, B. (2009). Investments in information technology: Indirect effects and information technology intensity. *Information Systems Research, 20*(1), 140-154.

Morris, S., & Strickland, T. (2008/2009). Exploration of information system process improvements and firm performance. *The Journal of Computer Information Systems*, *49*(2), 86-91.

Nagm, F., & Kautz, K. (2008). The market value impact of IT investment announcements – an event study. *Journal of Information Technology Theory and Application*, *9*(3), 61-79.

Neubauer, T., & Hartl, C. (2009). On the singularity of valuating IS security investments. *Proceedings of the 2009 IEEE/ACIS International Conference on Computer and Information Science, China,* 549-556.

Ochuko, R., Cullen, A., & Neagu, D. (2009). Overview of factors for internet banking adoption. *Proceedings of the IEEE International Conference on CyberWorlds*, *UK,* 163-170.

Oppliger, R., Rytz, R., & Holderegger, T. (2009). Internet banking: Client-side attacks and protection mechanisms. *IEEE Computer Magazine, 42*(6), 27-33.

Parent, M., & Reich, B. (2009). Governing information technology risk. *California Management Review*, *51*(3), 134-152.

Pfleeger, S. L. (2009). Useful cybersecurity metrics. *IEEE IS Professional, 11*(3), 38-45.

Pfleeger, S. L., & Ciszek, T. (2008). Choosing a security option: The InfoSecure methodology. *IEEE IS Professional, 10*(5), 46-52.

Pfleeger, S. L., & Rue, R. (2008). Cybersecurity economic issues: Clearing the path to good practice. *IEEE Software*, January/February, 35-42.

Png, I., Wang, C., & Wang, Q. (2008). The deterrent and displacement effects of information security enforcement: International evidence. *Journal of Management Information Systems, 25*(2), 125-144.

Podebrad, I., & Drotleff, M. (2009). IS security in banking: Processes, practical experiences, and lessons learned. *Proceedings of the IEEE Fourth International Conference on Internet Monitoring and Protection*, *Italy,* 78-83.

Purser, S. (2004). Improving the ROI of the security management process. *Computers & Security, 23*(7), 542-546.

Raghu, T., Woo, W., Mohan, S., & Rao, H. (2008). Market reaction to patent infringement litigations in the information technology industry. *Information Systems Frontier, 10*, 61-75.

Ranganathan, C., & Brown, C. (2006). ERP investments and the market value of firms: Toward an understanding of influential ERP project variables. *Information Systems Research*, *17*(2), 145-161.

Ravichandran, T., Han, S., & Hasan, I. (2009). Effects of institutional pressures on information technology investments: An empirical investigation. *IEEE Transactions on Engineering Management, 56*(4), 677-691.

Roztocki, N., & Weistroffer, H. (2006). Stock price reaction to investments in information technology: The relevance of cost management systems. *The Electronic Journal Information Systems Evaluation, 9*(1), 27-30.

Roztocki, N., & Weistroffer, H. (2008). Stock price reactions to investments in EAI and ERP: A comparative event study. *Proceedings of the IEEE 41st Hawaii International Conference on System Sciences, U.S.A*.

Roztocki, N., & Weistroffer, H. (2009a). Information technology investments: Does activity based costing matter? *The Journal of Computer Information Systems, 50*(2), 31-41.

Roztocki, N., & Weistroffer, H. (2009b). The impact of enterprise application integration on stock prices. *Journal of Enterprise Information Management, 22*(6), 709-721.

Rue, R., & Pfleeger, S. (2009). Making the best use of cybersecurity economic models. *IEEE Security & Privacy, 7*(4), 52-60.

Rue, R., Pfleeger, S., & Ortiz, D. (2007). A framework for classifying and comparing models of cyber security investment to support policy and decision-making. *Proceedings of the IEEE 2007 Workshop on the Economics of Information Security*, *U.S.A.,* 1-23.

Sabherwal, R., & Sabherwal, S. (2007). How do knowledge management announcements affect firm value? *IEEE Transactions on Engineering Management, 54*(3), 409-422.

Sanayei, A., & Noroozi, A. (2009). Security of internet banking services and its linkage with users' trust. *Proceedings of the IEEE International Conference on Information Management and Engineering, Malaysia,* 3-7.

Shih, K. (2010). Risk indicators for computer systems assisted financial examination. *The Journal of Computer Information Systems, 50*(4), 97-105.

Siegel, J., & Shim, J. (2010). Accounting Handbook. New York: Barron's Educational Series, Inc.

Smedinghoff, T. (2007). Where we're headed: New developments and trends in the law of information security. *Privacy & Data Security Law Journal*, *2*(2), 103-138.

Smith, H., & McKeen, J. (2009). Developments in Practice XXXIII: A holistic approach to managing IT-based risk. *Communications of the Association for Information Systems, 25*(41), 519-530.

Smith, S., Winchester, D., & Bunker, D. (2010). Circuits of power: a study of mandated compliance to an information systems security de jure standard in a government organization. *MIS Quarterly, 34*(3), 463-486.

Sobol, M. & Klein, G. (2009). Relation of CIO background, IT infrastructure, and economic performance. Information & Management, 46, 271-278.

Spears, J. & Barki, H. (2010). User participation in information systems security risk management. *MIS Quarterly, 34*(3), 503-522.

Storey, V., Kane, G., & Schwaig, K. (2009). The qualify of online privacy policies: A resource-dependency perspective. *Journal of Database Management, 20*(2), 19-37.

Stoel, M. & Muhanna, W. (2009). IT capabilities and firm performance: a contingency analysis of the role of industry and IT capability type. *Information & Management, 46*, 181-189.

Subramani, M., & Walden, E. (2001). The impact of e-commerce announcements on the market value of firms. *Information Systems Research, 12*(2), 135-154.

Tashi, I. (2009). Regulatory compliance and information security assurance. *Proceedings of the IEEE International Conference on Availability, Reliability, and Security*, *Japan,* 670-674.

Telang, R., & Wattal, S. (2007). An empirical analysis of the impact of software vulnerability announcements on firm stock price. *IEEE Transactions on Software Engineering, 33*(8), 544-557.

Thatcher, M., & Pingry, D. (2004). Understanding the business value of information technology investments: Theoretical evidence from alternative market and cost structures. *Journal of Management Information Systems, 21*(2), 61-85.

Thatcher, M., & Pingry, D. (2007). Modeling the IS value paradox. *Communications of the ACM, 50*(8), 41-45.

Thomas, R. (2009). Total cost of security – a method for managing risks and incentives across the extended enterprise. *Proceedings of the ACM Cyber Security and Information Intelligence Research Workshop, U.S.A*.

Tian, J., Haleblian, J., & Rajagopalan, N. (2011). The effects of board human and social capital on investor reactions to new CEO selection. *Strategic Management Journal, 32*, 731-747.

Trcek, D. (2010). Security metrics foundations for computer security. The Computer Journal, 53(7), 1-22.

Trope, R., Power, E., Polley, V., & Morley, B. (2007). A coherent strategy for data security through data governance. *IEEE Security & Privacy, 5*(3), 32-39.

U.S. Department of Commerce, National Institute of Standards and Technology, (2011). *Information Security* (NIST Special Report No. 800-137). Retrieved from http://csrc. nist.gov/publications.

Verrecchia, R. (2001). Essays on disclosure. *Journal of Accounting and Economics*, *32*(1-3), 87-180.

Vijayaraghavan, V., Paul, S., & Rajarathnam, N., 2010. iMeasure security (iMS): a framework for quantitative assessment of security measures and its impacts. *Information Security Journal, 19*, 213-225.

Wang, J., Xiao, N., & Rao, R. (2010). Drivers of information security search behavior: An investigation of network attacks and vulnerability disclosures. *ACM Transactions on Management Information Systems, 1*(1), 1-23.

Whitten, D. (2008). The chief information security officer: An analysis of the skills required for success. *The Journal of Computer Information Systems, 48*(3), 15-19.

Wilkin, C., & Chenhall, R. (2010). A review of IT governance: A taxonomy to inform accounting information systems. *Journal of Information Systems*, *24*(2), 107-146.

Xue, Y., Liang, H., & Boulton, W. (2008). Information technology governance in information technology investment decision processes: The impact of investment characteristics, external environment, and internal context. *MIS Quarterly, 32*(1), 67-96.

Yao, L., Sutton, S., & Chan, S. (2009). Wealth creation from information technology investments using the EVA. *The Journal of Computer Information Systems*, *50*(2), 42-48.

Yuen, Y., Yeow, P., Lim, N., & Saylani, N. (2010). Internet banking adoption: Comparing developed and developing countries. *The Journal of Computer Information Systems, 51*(1), 52-61.

Yurcan, B. (2012). The value of compliance. Bank Systems & Technology, 49(1).

Zhu, K. (2004). The complementarity of information technology infrastructure and e-commerce capability: A resource-based assessment of their business value. *Journal of Management Information Systems, 21*(1), 167-202.

Zhu, K., Kraemer, K., Xu, S., & Dedrick, J. (2004). Information technology payoff in e-business environments: An international perspective on value creation of e-business in the financial services industry. *Journal of Management Information Systems, 21*(1), 17-54.