Online Journal of Applied Knowledge Management
A Publication of the International Institute for Applied Knowledge Management

Volume 1, Issue 1, 2013

The market value of information system (IS) security for e-banking

Linda Brock, IBM Corporation, brock1@us.ibm.com

Yair Levy, Nova Southeastern University, levyy@nova.edu

Abstract

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. 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.

Keywords: Event study, market value, information security, value of information security investments, information systems investments, e-banking.

Introduction

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 IS as a set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of information. There are costs associated with managing IS including security, storage, and retrieval therefore ongoing IS investments are required (Kendall & Kendall, 2008). Investments refer to expenditures 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 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 intended to detect and prevent security breaches, guard against vulnerabilities, and manage online attacks create new costs items in IS budgets (Anderson & Choobineh, 2008).

Regulatory Demands

IS security is no longer just good business practice, it is also a legal obligation (Smedinghoff, 2007). The banking industry is one of the most highly regulated industries in the U.S. with approximately 4,000 federal, state, and local laws as well as regulations that must be followed when managing electronic records (Burns & Peterson, 2010). Laws and regulations impose requirements on IS business practices, products, as well as 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). 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.

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, as well as 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). 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). In addition, Section 215 of the U.S. Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (PATRIOT) 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). As a result, according to Islam, Mouratidis, and Jurgens (2011), financial organizations spend approximately $5.8 billion annually to ensure compliance with regulations such as SOX.

Due to 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 regulation 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. 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 is 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). Further, 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. 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 and e-Banking

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, and negatively impact overall market values (Andoh-Baidoo, Amoako-Gyampah, & Osei-Bryson, 2010). Also, IS security issues can expose weaknesses in company management teams that can 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 threats (Vijayaraghavan et al., 2010).

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) believe 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, investments in IS security are 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. 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).

Theoretical Background

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 has resulted in limited empirical data that can accurately characterize market value or gauge the impact on firm financial performance (Bojanc & Jerman-Blazic, 2008).

Accounting-based Measures of Investments

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. Additionally Yao et al. (2009) found there is no universal calculation for determining ROI and therefore it is an approach that cannot be uniformly applied. 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).

Purser (2004) found that 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) 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.

Gordon and Loeb (2006) conducted an empirical study to examine the cost-benefit analysis approaches many corporations use 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 must 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, collect, or attempt to measure.

Market-based Measures of IS Investments

For over a decade, IS researchers have studied firm performance impacts resulting from various types of investments in IS using the event study methodology. 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).
The event study method has been used by researchers to measure the market value impacts resulting from IS security breaches, attacks, and defects or vulnerabilities. Campbell, Gordon, Loeb and Zhou (2003) conducted an 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 2004, Cavusoglu et al. conducted an event study in order to determine the market value impacts of Internet security breach announcements. Findings from the Cavusoglu et al. (2004) 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 an 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) 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 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 an 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. A summary of these event studies examining the market value impacts resulting from IS security-related announcements are reflected in Table 1.

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 market value impacts associated with negative events such as security breaches, attacks, and vulnerabilities, an understanding of the market value impacts resulting from investments in IS security is still needed to fully understand the cost/benefit ratio of the investments (Geer, 2007). 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.

Methodology

Since the late 1960's, event studies have been widely used in many disciplines including finance, accounting, and economics (Campbell et al., 1997). 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 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).

The event window selected for the study contained only one day, specifically, the day of the announcement or day 0. A market model was used to compute the abnormal returns for all firms in the study scope (Jeong & Stylianou, 2010). Abnormal returns were compared to the market model of normal returns (Cavusoglu et al., 2004). 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). The Patell Z parametric test statistic and the generalized sign nonparametric test statistic were used as the study test procedures. Statistical significance for abnormal returns was measured at the 0.10, 0.05, 0.01, and 0.001 levels respectively. The

Eventus® software tool was used for calculating and reporting the advanced statistics necessary to complete this event study (Cowan, 2007).

Data Collection

Lexis/Nexis enabled the search of newswires and press releases from 2003-2010. Lexis/Nexis search terms included (a) security, (b) secure, (c) safety, (d) safe, (e) protect, and (f) protection. The announcement publication type was restricted to newswires and press releases available from Lexis/Nexis. Based on conventions established in previously published event studies, announcements excluded from the study data set included those published in periodicals or magazines. The Lexis/Nexis data search was restricted to include only e-banking service providers assigned the SIC Division H, Major Groups 60, 61, and 67 codes established by the U.S. Securities and Exchange Commission (SEC). 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. Finally, 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 initial Lexis/Nexis search results included 651 announcements that were narrowed to 516 announcements after duplicate announcements were removed. Using the NIST 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 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

The final data sample included 34 different e-banking service firms with 18 firms listed on the NASDAQ stock exchange and 16 listed on the NYSE stock exchange. The data sample was partitioned by the author based on announcement content and grouped into either a technology-focused or people-focused announcement segment. 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.

Empirical Results

For the full data sample the mean cumulative abnormal return (CAR) was different from zero, indicating that the events did impact market values. More specifically, the mean CAR was 0.10% which is statistically significant at conventional levels. The CAR value of 0.10% however indicates a weak relationship between the changes in market values relative to the selected announcements. The results of the 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, announced investments in IS security resulted in statistically significant impacts on e-banking market values however the impact was not significant.

In order to further understand the impacts of the selected IS security investment announcements and the resulting market reactions, the study sample of events was partitioned into two groups reflecting the type of investment announced: technology or people. For the technology partition of the data sample, the CAR was 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.

For the people partition of the data sample, the CAR was 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 moderate relationship to market value impacts. 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. Any conclusions based on a sample size of seven announcements must be considered preliminary and will require further validation from other researchers using a larger sample population to validate this study finding.

Discussion and Conclusions

The findings from this research provided evidence of market value reactions occurring when IS security investment announcements were 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.

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 if found removed from the study scope. 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, by using different sources, queries and search methods it is possible that other researchers may identify a different sample of IS security investment announcements from e-banking service providers and consequently obtain different results.

References

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*, 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.

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 Professionals, 11*(5), 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.

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. (2004). 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.

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

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

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.

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

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

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.

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

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

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.

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, pp. 75-84.

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.

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

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.

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

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

Pfleeger, S. L., & Rue, R. (2008). Cybersecurity economic issues: Clearing the path to good practice. *IEEE Software, 25*(1), 35-42.

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, pp. 78-83.

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

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.

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

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*, USA, pp. 1-23.

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.

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.

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

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.

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.

Yurcan, B. (2012). The value of compliance. *Bank Systems & Technology, 49*(1), 1-4.

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.

Acknowledgments

We would like to thank the anonymous referees for their careful review and valuable suggestions. We also would like to thank the accepting editor, Dr. Alex Koohang, for his recommendations and constructive comments.

Biographies

Linda Brock obtained her PhD in Information Systems & Security from Nova Southeastern University in 2012. She is currently an IBM employee working in the Global Technology Services division as a Security & Compliance specialist. Linda is an accomplished IT professional who has been working in the IT industry for over 25 years. She also holds a MS in the Management of Information Technology from the University of Virginia.

Yair Levy a Professor at the Graduate School of Computer and Information Sciences at Nova Southeastern University and the director of the Center for e-Learning Security Research (CeLSR). During the mid to late 1990s, he assisted NASA to develop e-learning systems. He earned his Bachelor's degree in Aerospace Engineering from the Technion (Israel Institute of Technology). He received his MBA with MIS concentration and Ph.D. in Management Information Systems from Florida International University. His current research interests include security issues with e-learning systems, cyber-security skills, and cognitive value of information systems. Dr. Levy is the author of 'Assessing the Value of e-Learning Systems' (2006). His research publications appear in numerous peer-reviewed journals and conference proceedings. Also, Dr. Levy has been serving as a member of conference proceedings committee for numerous scholarly conferences. Moreover, Dr. Levy has been serving as a referee research reviewer for hundreds of national and international scientific outlets. He is a frequent invited keynote speaker at national and international meetings on IS, Information Security, and online learning topics. Dr. Levy's teaching interests in the masters level include MIS, system analysis and design, information systems security, e-commerce, and Web development. His teaching interests in the doctoral level include Information Systems Development (ISD) and Advanced Multivariate Research Methods and Statistics. To find out more about Dr. Levy, please visit his site: http://scis.nova.edu/~levyy/