Examination of Corporate Investments in Privacy: An Event Study

by

Joseph Michael Squillace

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

College of Computing and Engineering
Nova Southeastern University

2021

We hereby certify that this dissertation, submitted by Joseph Squillace conforms to acceptable standards and is fully adequate in scope and quality to fulfill the dissertation requirements for the degree of Doctor of Philosophy.

Gurvirender Tejay, Ph.D
Chairperson of Dissertation Committee

03/15/21
Date

Ling Wang, Ph.D.
Dissertation Committee Member

03/15/21
Date

Steven Terrell, Ph.D.
Dissertation Committee Member

3/15/21
Date

Approved:

Meline Kevorkian, Ed.D.
Dean, College of Computing and Engineering

3/15/21
Date

College of Computing and Engineering
Nova Southeastern University

2021

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

Examination of Corporate Investments in Privacy: An Event Study

by
Joseph Michael Squillace
March 2021

The primary objective of any corporate entity is generating as much wealth as possible. Investing financially in technology domains has historically been a successful strategy for generating increased corporate and shareholder wealth. However, investments in Information Technology (IT), Information Systems (IS) and Information Security (InfoSec) to specifically generate increased wealth must be implemented carefully.

Shareholders reacting to corporate investments perceive financial value from individual investments. The investment's perceived value is then reflected in the corporation's updated stock market value. IS, IT, and InfoSec investments perceived to possess positive financial value, indicating strong potential for increased wealth, are rewarded by shareholders through increased stock market value; conversely, investments perceived to possess negative financial value, likely to decrease corporate wealth, are punished by shareholders through decreased stock market value.

Previous research utilizing *Event Study Methodology* (ESM) determined financial impact that investments had on corporate stock market value after press release announcements identifying the investment. Based on early success across various domains, additional *Event Study Research* (ESR) was further conducted within IS, IT, and InfoSec. Most studies aligned into one of three categories: 1) Investments in IT, 2) Information Security Breaches, and 3) IT Outsourcing, and similarly measured changes in market value from corporate investments in related IS, IT, and InfoSec products and services.

Examination of the extant body of literature identified a gap within Privacy domain; minimal ESR examining privacy and the financial impact from corporate investments in privacy. While financial loss associated with a breach incident is identified as the motivating force driving increased corporate investments in defensive measures, "*privacy*" is identified as a singular construct with little concern for the associated invasion of privacy. As such, little is known about privacy, potential financial risks associated with a privacy breach, nor an understanding of *why* corporations *are not* investing in privacy.

This research extends the body of literature and makes an academic contribution by: 1) using ESM to identify the financial and overall stock market implications from corporate investments in privacy, 2) identifying the economic incentives motivating corporate investments in privacy, and 3) gaining a better overall understating of corporate investments in privacy, and *why* corporations are *not investing* in privacy.

Acknowledgements

Successful completion of my PhD has been one of the most rewarding, yet arduous and challenging endeavors I have pursued. While dissertation publication provides finality on my PhD, it begins a new chapter in my commitment to excellence in academia and research. It is impossible to adequately express the gratitude I feel towards those who helped me along the way. Specifically, completion of my PhD would not have been possible without the uncompromising support of my partner Miss. She has supported me without question from the very beginning while making countless sacrifices for me, often at great personal expense. Navigating school, cluster sessions with late-night research meetings, and completion of my dissertation brought about a multitude of challenges, physically, mentally, and financially, that were only overcome by working together as a team. Absent this unwavering support from her, completing my PhD would not have been possible. I want to further give special thanks to my family. The continuous level of support, encouragement, and motivation you have provided cannot be overstated. You have been steadfast in believing in me and did whatever you could to help, often at great personal and financial sacrifice. Without you all, I simply would not be where I am today. I cannot truly express how grateful I am. And to my friends, Warren and Daryl, your support did not go unnoticed. While often unsaid, I always appreciated everything.

To my committee chair, Dr. Gurvirender Tejay, it is hard to put into words how great you were during my time at NSU. The positive impact you had on my life is incalculable: as my friend, mentor, and advisor. The first class I had with you I knew you were different. It is a testament how much you care for your students and how much time, effort, and energy you are willing to commit to like-minded students. It was no surprise that your impromptu, after-hour research gatherings were all the rage at NSU. I was extremely lucky to have you as my advisor and am grateful for all you have done. I also take away a newfound love for Cricket, exhilarating global competitions known as IPL T20 and World T20 (if you know, you know), and a resonating message that in life, "there's no such thing as perfect, there's only the relentless pursuit of perfection."

I would also like to thank my dissertation committee team members Dr. Ling Wang and Dr. Steven Terrell. I was lucky to have your support and valuable subject-matter expertise. Dr. Wang, you make quantitative analysis understandable and usable. Dr. Terrell, your unique ability to intertwine real-life, anecdotal stories and personal research experience into education lessons is a gift that allows students to learn challenging subject matter without difficulty. I did not realize just know how much I learned from you both until it was necessary to apply the required skillset in my dissertation.

To Dr. Zareef Mohammed and Dr. Abdul Rahim Charif; it is impossible to describe how much you both helped me. You challenged me mentally, pushed me academically, and supported my research through critical discussion. I will never forget our time at NSU.

Finally, I dedicate this PhD to my best friend Steely who sadly passed earlier this year. You were steadfast by my side, every day, without fail, and without hesitation. I miss you buddy but know that you are in a better place without pain and suffering.

"Ad Astra Per Aspera"

Table of Contents

APPENDICES:

List of Tables

List of Figures

Chapter 1

Introduction

1.1 Background

Corporations recognize the strategic importance of integrating *Information Systems* (IS) and *Information Technology* (IT) into the workplace environment. Proper selection and implementation of IS/IT can provide a corporation a variety of benefits when correctly deployed, for example increased competitive advantage and streamlined efficiency. Research has also shown, however, the most advantageous deployment of an IS/IT investment within a corporate environment is driven by the potential for increased corporate wealth (Culnan & Williams, 2009; Dardan et al., 2005).

Event Study (ES) research utilizing *Event Study Methodology* (ESM) is a powerful tool that can help Information System (IS) / Information Technology (IT) researchers assess the business performance of corporate investment options using such market-based measures as stock price or trading volume (Im et al., 2001). In addition, Event Study Methodology (ESM) can identify potential financial implications from corporate investments and help identify any existing financial correlation between potential positive/negative financial impact to overall corporate stock market value and specific corporate investments in technology, based on specified investment category.

Historical Event Study (ES) research utilizing Event Study Methodology (ESM) has been conducted throughout a variety of technology domains (Dos Santos et al., 1993) and highlights the ability for increased wealth through improved overall stock market value; both in *United States* (U.S.) (Chatterjee et al., 2002; Hayes et al., 2001; Im et al.,

2001; Ranganathan & Brown, 2006; Sabherwal & Sabherwal, 2007), and abroad (Cheng et al., 2007) (Appendix B). Investments perceived by shareholders to provide increased corporate wealth are positively rewarded (increased stock market value), while investments perceived by shareholders to provide negative corporate wealth are admonished (decreased stock market value) (Hinz et al., 2014; Khansa et al., 2012; Malhotra & Malhotra, 2010). As corporate shareholders dictate overall stock market value, investment decisions should be made such that it will be received favorably by shareholders, leading to increased stock market value.

To better address this corporate investment phenomenon, the research community has adopted Event Study (ES) research utilizing Event Study Methodology (ESM) to investigate potential financial impact that different investments in Information System (IS), Information Technology (IT), *Information Security* (InfoSec), and related technology domains have on overall corporate stock market value, and how the financial impact from different corporate investments varies across different industry segments. Event Study Methodology (ESM) is a "… powerful tool that can help researchers assess the business performance of IT investments using such market-based measures as stock price or trading volume" (Im et al., 2001).

Event Study (ES) research using Event Study Methodology (ESM) can also be used in examining potential financial impact to overall corporate stock market value from any identifiable, non-investment announcement event, made available to the general public and shareholders (i.e. newspaper press release announcing a breach event on a corporations internal network servers); however, most often the specified corporate event is a corporate press release announcement identifying a specific corporate investment).

Previously conducted IS, IT, InfoSec, and related event study research successfully highlighted how financial impact to overall corporate stock market value can be determined for both positive corporate announcement events relating to corporate investments (technology, services), as well as negative announcement events relating to a lack of corporate investments (data breach, intellectual property theft).

Prior to the successful applicability of Event Study (ES) research utilizing Event Study Methodology (ESM) within technology and related domains, researchers were unable to accurately identify true financial cost from a breach incident that involved both tangible and intangible costs. Hovav & D'Arcy (2003) notes that "…potential intangible losses such as "loss of competitive advantage" (result of the breach) and "loss of reputation" (D'Amico, 2000) are not included because intangible costs are not directly measurable." This realization drove the research community to develop an improved methodology to better ascertain true financial costs from breach incidents. A new, updated method was needed using a "…different approach to assess the risk of security breaches" (Hovav & D'Arcy, 2003).

Once Event Study (ES) research using Event Study Methodology (ESM) was identified as a successful research tool available for corporate use, capable of identifying true financial cost implications from specific corporate announcement events (i.e., corporate investments, breach incidents), areas of research interest began to shift. New areas of research focus became primarily interested in examining corporate investment options most likely to generate profit and increased stock market value, across varying technology and data protection (Privacy, Security) domains.

Accurately estimating potential financial implications from specific investment options is an extremely important responsibility for corporations. To assist in this task, corporations perform an *Investment Assessment* (IA) that includes analyzing applicable Event Study (ES) research (special focus on research analysis, results, findings, assertions, and recommendations), reviewing relevant corporate-funded research studies associated with the specific investment of interest, analyzing corporate financial data and related stock market information, and reviewing available government information relating to the investment of interest. The Investment Assessment (IA) process concludes with the completion of additional, independent Event Study (ES) research (utilizing Event Study Methodology (ESM) examining potential financial implications to overall corporate stock market value from available investment options being considered. The totality of this assessment process provides corporations with the most accurate, reliable, and true financial implications for an investment option based on science, research, and finance; necessary to make strategic investment decisions.

When conducting Event Study (ES) research utilizing Event Study Methodology (ESM), potential financial implications to overall corporate stock market value from corporate investments can be categorized in three (3) ways, based on *i*) perceived financial value obtained by the corporation directly from investment, *ii*) perceived financial value added to the corporation directly from investment (based on 1 – direct value from investment, or 2 – potential reduction in corporate losses), and *iii*) assessed financial value added or lost from enforced governmental/industry compliancy initiatives (allows corporation to not lose revenue through forced government regulations that must be followed under threat of financial penalty (Nicholas-Donald et al., 2011).

Resulting directly from the success of previously conducted Event Study (ES) research using Event Study Methodology (ESM) and its broad domain utilitarianism, its applicability and implementation reach grew exponentially across research domains, including for example: Administrative (Accounting, Finance, Healthcare) (Case & King, 2015; Huang & Behara, 2013; Khansa et al., 2012; MacKinlay, 1997; Schwaig et al., 2006); Technology (and Related) (Dos Santos et al., 1993; Hayes et al., 2001), and Data Protection (i.e., Privacy, Security, Breach) (Andoh-Baidoo & Osei-Bryson, 2013; Bose & Leung, 2014; Campbell, 2003; Chen et al., 2011; Garg et al., 2003; Goel & Shawky, 2009; Hovav & D'Arcy, 2003, 2005). Yet minimal Event Study (ES) research has been completed examining *Privacy*, even less examining *Corporate Investments in Privacy*.

The extant body of Event Study (ES) literature illustrates its universal success, general applicability, and broad domain reach. When performed in a traditional role, Event Study (ES) research uses Event Study Methodology (ESM) to examine potential financial impact to overall corporate stock market value from a designated event (i.e., corporate press release announcement identifying a data breach incident causing massive exploitation of users' personal information; corporate press release announcement announcing a new training initiative for all employees); however, most often corporate announcement events identify a specific investment.

Successful use of Event Study (ES) research spans a wide array of research domains and has highlighted the potential for increased corporate stock market value through proactive/reactive corporate investments, forced corporate investments imposed through government compliance initiatives, and even plays a major role in dictating future corporate investments/corporate investment strategy. Research results indicating a

potential for increased corporate wealth are accepted by corporations as the "… main motivating factor driving investments in technology (Dardan et al., 2005; Subramani & Walden, 2001). However, despite the rampant success of Event Study (ES) research, only minimal research interest has been committed.

From the Event Study (ES) extant literature, minimal privacy research has been conducted (Acquisti et al., 2006; Aytes et al., 2006; Hinz et al., 2014; Khansa et al., 2012; Khansa & Liginlal, 2009; Malhotra & Malhotra, 2010). Even less Event Study (ES) research has been conducted to better understand corporate investments in privacy and financial impact on overall corporate stock market value from corporate investments in privacy (Aytes et al., 2006; Cullnan & Williams, 2009; Nicholas-Donald et al., 2011). While data protection and associated research domains have received an abundance of Event Study (ES) research interest, it has been to the detriment of other research domains, most notably *Privacy* research as the privacy domain has seen reduced research interest.

Furthermore, In lieu of financial information and limited stock market analysis available from event study privacy research previously conducted, there exists almost no additional data available exploring financial implications for corporate exposure to privacy breach events, or potential financial loss from exploitation of client *Personal Identifiable Information* (PII) stolen during a privacy breach.

This phenomenon of lacking research interest in corporate investments in privacy drives the need for further examination to better understand why corporations are *not investing* in privacy. Research has provided supplemental data analysis identifying financial benefit from corporate investments in privacy (Acquisti et al., 2006; Culnan & Williams, 2009; Dinev & Hart, 2006; Malhotra & Malhotra, 2010; Nicholas-Donald et

al., 2011), so *why* are these financial incentives not encouraging corporate investments in privacy, and does there exist other motivating factors that may provide alternative encouragement for corporate investments in privacy?

The goal of this dissertation was to examine corporate investments in privacy by conducting an event study. The research objective of an event study is to examine stock market response to announcement events often related to the release of [corporate investment] information to the stock market (Im et al., 2001). Since new information will be incorporated directly into the corporate share price, changes in stock market price can be attributed to the identified corporate [investment] announcement event (Dos Santos et al., 1993). In completing this research, this event study and supporting analysis provides a better understanding of corporate investments in privacy by identifying financial implications to overall corporate stock market value from corporate investments in privacy and discovering a lack of motivating incentives encouraging corporate investments in privacy. Equally important, this examination of corporate investments in privacy provides a better understanding of *why corporations are not investing in privacy*.

Moreover, this research fills a gap in the extant research literature identified by a lack of interest in examining corporate investments in privacy. Supplementing the extant body of privacy literature in this domain, this research provides a better understanding of why corporations are not as financially vested in privacy when compared to other technology investments; specifically, when evaluated against corporate investments in Information System (IS), Information Technology (IT), Information Security (InfoSec), and related technology domains.

1.2 Problem Statement

The research objective of this dissertation was to provide a better understanding of *why corporations are not investing in privacy*. Literature review of this phenomenon highlights an identifiable gap within the extant body of Privacy, Information System (IS), Information Technology (IT), Information Security (InfoSec), and related event study research literature indicated by the presence of minimal academic studies committed to investigating privacy, corporate investments in privacy (Hinz et al., 2014; Huang & Behara, 2013; Khansa et al., 2012), nor financial implications from corporate investments in privacy (Malhotra & Malhotra, 2010; Nicholas-Donald et al., 2011).

To help bridge this research gap and add to the academic body of privacy literature, this research examination provides a better understanding of both corporate investments in privacy and potential economic/financial implications (stock market) from corporate investments in privacy. In addition, as fewer academic studies still have investigated whether there exists a correlation between increased overall corporate stock market value and announcement events identifying corporate investments in privacy (Hinz et al., 2014; Huang & Behara, 2013; Khansa et al., 2012), this study provides data identifying increased financial advantage (increased overall corporate stock market value) from corporate investments in privacy, based on specified corporate industry classification. Successful completion of this research examination adds to the body of privacy literature by providing a better understanding of corporate investments in privacy while providing additional insight into *why corporations are not investing in privacy*.

Examination of Information System (IS), Information Technology (IT), Information Security (InfoSec), and related event study research highlights one factor that

may be leading to reduced interest in, and contributing to, reduced corporate investments in privacy; corporate shareholders perceive minimal financial value from corporate investments in privacy (Acquisti et al., 2006; Culnan & Williams, 2009; Dinev & Hart, 2006). The important question to ask however is "How accurate are the perceived financial values assigned to corporate investments in privacy?" by shareholders. Data analysis by Acquisti et al. (2006) "…provides evidence to suggest a disconnect exists between actualized value and perceived value in corporate investments in privacy" (Acquisti et al., 2006). Accurate financial assessment of corporate investment in privacy options by corporate shareholders is extremely important as it is the impetus driving corporate investment decisions, yet it could be being made *incorrectly*, and a contributing factor in *why corporations are not investing in privacy*.

In attempting to decide whether or not to use available corporate resources on a specific Information System (IS), Information Technology (IT), Information Security (InfoSec), or related investment, it is of paramount importance for the corporation to properly evaluate and assign correct financial value to the available investment resource. Event study research can be used to help corporations minimize financial value assessment errors when dealing with available investment options. More specifically, event study research can be utilized as a tool providing corporations the ability to identify potential financial implications corporate investments in privacy may have on overall corporate stock market value, as well as determining true financial value for corporate investments in privacy.

Corporate responsibility exists in maximizing profit and economic standing by maintaining a strategy of focusing investment resources heavily into areas of technology

identified through research as most likely to generate increased corporate wealth (Dardan et al., 2005; Subramani & Walden, 2001); the main motivating factor driving corporate investments. However, ensuring corporate and client data privacy protection is equally important for maintaining corporate wealth as irresponsible corporate practices / policies leading to information breach and data theft incidents have caused corporations massive financial losses (Culnan & Williams, 2009; Hovav et al., 2017; Malhotra & Malhotra, 2010). Corporate decision making to invest in technology rather than improving protective privacy defenses is a balanced assessment of "risk versus reward." As noted by Hovav & D'Arcy (2003), "risk assessment is a process of choosing controls based on probabilities of loss. In IS/IT, risk assessment addresses the questions of what is the impact … and how much will it cost the organization" (Kelly, 1999).

Compounding the issue is that with only minimal research examining corporate investments in privacy, there is no universal consensus on determining financial implications caused by privacy breach incidents. At present, there is only scattered evidence about the price companies pay for their privacy debacles (Acquisti et al., 2006). Additional research examining financial implications from corporate investments in privacy will add to the body of knowledge and provide additional support for continued corporate investments in privacy to improver data privacy and protection.

From the Information System (IS), Information Technology (IT), Information Security (InfoSec), and related extant literature, a combined total of one hundred and twenty-three [123] Event Study (ES) research and Event Study (ES) literature papers have been identified for inclusion within this research proposal (Appendix B). Every event study completed using Event Study Methodology (ESM) in IS, IT, InfoSec, and

related research literature domains was read, categorized, and classified within this research proposal (Appendix B). The categorical classification process was a necessary precautionary in ensuring the research objectives of this research could successfully be accomplished (based on prior event study using ESM as the basis for research design, data collection, and analysis), in addition to validating the intended research goals would make an academic contribution to the extant body of ESM privacy and privacy literature.

Literature review examining Information System (IS), Information Technology (IT), Information Security (InfoSec), and related event study extant literature domains identified an observable gap in the research requiring additional research support; event study privacy literature. Only minimal Event Study (ES) privacy research, using Event Study Methodology (ESM), has been conducted, including work by Acquisti et al. (2006); Aytes et al. (2006); Chai et al. (2010); Hinz et al. (2014); Huang & Behara (2013); Khansa et al. (2012); Khansa & Liginlal (2009); Malhotra & Malhotra (2010); Nicholas-Donald et al. (2011); Schwaig et al. (2006). However, event study research interest *Examining Corporate Investments in Privacy* is extraordinarily low compared to event study research interest in IS, IT, InfoSec, and related domains.

Further examination of Information System (IS), Information Technology (IT), Information Security (InfoSec), and related event study extant literature domains reaffirmed the identified research gap (limited event study research examining corporate investments in privacy). Compared with minimal research interest examining privacy in event study literature, examination of IS, IT, InfoSec, and related extant literature identified the massive extent which event study research has been conducted using Event Study Methodology (ESM) across IS, IT, InfoSec, and related research domains in

determining overall stock market impact from corporate investment announcements. Examples of research domains having been investigated using event study research include: Administrative (Accounting, Finance, Healthcare) (Case & King, 2015; Huang & Behara, 2013; Khansa et al., 2012; MacKinlay, 1997; Schwaig et al., 2006); Technology (and Related) (Dos Santos et al., 1993; Hayes et al., 2001), and Data Protection (i.e., Privacy, Security, Breach) (Andoh-Baidoo & Osei-Bryson, 2013; Bose & Leung, 2014; Campbell, 2003; Chen et al., 2011; Garg et al., 2003; Goel & Shawky, 2009; Hovav & D'Arcy, 2003, 2005).

Event study research has provided evidentiary support indicating corporate investments possess the ability to increase overall corporate stock market value, across multiple IS, IT, InfoSec, and related research domains, leading to continued corporate investments in those technology domains. Yet, inexplicably, this research interest has not continued to *Privacy*; only minimal event study research exists examining privacy, leading to reduced levels of corporate concern regarding privacy. Additional event study research examining this paradox will provide more details regarding corporate investments in privacy while simultaneously providing in parallel a better understanding of *why corporations are not investing in privacy*.

According to *Efficient Market Hypothesis* (EMH) theory, used in Event Study (ES) research implementing Event Study Methodology (ESM), if there is perceived value in corporate investments in privacy, then any significant corporate investments in privacy will be positively rewarded by corporate shareholders; including positive stock market gains and increased overall corporate stock market value for the corporation making the privacy investment. Using available data (press release announcement events identifying

corporate investments in privacy), this research conducted an event study to examine corporate investments in privacy. Examining corporate investments in privacy, this research used Event Study Methodology (ESM) to identify financial implications to overall corporate stock market value from corporate investments in privacy, while also identifying a lack of financial incentives encouraging corporate investments in privacy.

1.3 Dissertation Goal

The goal of this dissertation was to examine corporate investments in privacy. In doing so, this research examination provides a better understanding of corporate investments in privacy, identifies financial implications to overall corporate stock market value from corporate investments in privacy, and discovered a lack of economic incentives encouraging corporate investments in privacy. Equally important, this research examination of corporate investments in privacy also provides a better understanding of *why corporations are not investing in privacy*. As such, this research makes the argument(s) that limited financial value exists from corporate investments in privacy, and by extension, limited economic incentives exist encouraging corporate investments in privacy. Corporations are often not even held accountable for their role in privacy breach incidents. To add, "… only scattered evidence exists about the price companies actually pay for their privacy debacles" (Acquisti et al., 2006).

Individual expectations regarding personal privacy have been continually weakened since the terror attacks of September 11th, 2001 due to concerns for improved National Security defense. At the request of the "9/11 Commission," the *Director of National Intelligence* (DNI) created a variety of new agencies that would each focus on electronic intelligence, information gathering, digital surveillance, online communication,

media, etc., and any additional related activities, in an effort to electronically track identified / potential threats against the United Stated (U.S.). All newly created agencies are accessible under a singular umbrella entity identified as an *Information Sharing Environment* (ISE). Under ISE, agencies (i.e. *National Counterterrorism Center* (NCTC), and policies (i.e. "Patriot Act" – *Department of Justice* (DOJ) and "Homeland Security Act" (2002) – *Department of Homeland Security* (DHS) are fused together with federal/local law enforcement and federal/local intelligence agencies to improve national defense efforts against individuals posing electronic and information threats.

In a manner not dissimilar to the "Privacy Paradox," identified by Dinev & Hart (2006) as the value position accepted by consumers at which time they become willing to give away their Personal Identifiable Information (PII), individuals have reached a position in which they are comfortable with exchanging individual expectations of personal privacy for improved National Security. As a collective, universal invasions of individual privacy by NCTC, *Department of Homeland Security* (DHS), *National Security Agency* (NSA), and *Federal Bureau of Investigation* (FBI) are "acceptable breaches of privacy" – provided in exchange for strengthened National Security; necessary for protecting the U.S and its citizens against threats (foreign and domestic) and terrorist attacks. This has reduced overall financial cost implications associated with corporations ensuring privacy as more individuals remove their individual expectations of privacy. In addition, data breach incidents leading to privacy violations will have no financial impact on the corporation, from reduced user expectations of privacy. Absent a scenario where corporations are repeatedly held financially responsible by users and shareholders, leading to massive financial losses in corporate wealth and overall

stock market value, corporate investments in privacy will continue to be implemented only when necessary, through forced compliance (government mandate), for example Healthcare – *Health Insurance Portability and Accountability Act* (HIPAA), and Finance – *Sarbanes-Oxley Act* (SOX) of 2012 and *Gramm-Leach-Bliley Act* (GLBA), and reactionary in nature to combat an announced, identifiable threat posing grave financial risk. Furthermore, Financial evaluation of corporate investments in privacy involves balancing "financial cost" versus "financial penalty" to determine the most economically viable decision: the "financial cost" associated with implementing corporate investments in privacy is far greater when compared to the "financial penalty" imposed by shareholders and users from a *lack of corporate investments in privacy*.

Within academia, Event study methodology (ESM) has historically been used by research scientists to identify potential financial implications from corporate investment announcement events. Events are identified as press-release (news) announcements by a corporation announcing new, previously undisclosed information, to shareholders and the general public. Financial impact the public announcement has on overall corporate stock market value of the corporation making the press release announcement is the "event" being investigated. Previous event study research representing interest from both academics and practitioners has been completed in varying domains, including: *Accounting and Finance* (MacKinlay, 1997); *Information Systems* (IS) (Dehning et al., 2003); *Information Technology* (IT) (Dos Santos et al., 1993); *Information Security* (InfoSec) (Hovav et al., 2014, 2017); *Computer Security* (ComSec) (Garg, 2003); and *Internet Security* (IntSec) (Cavusoglu et al., 2004).

Event Study literature review papers have also been completed by Dehning et al., (2003), Hovav et al., (2007), Roztocki & Weistroffer (2008, 2009, 2011), and Spanos & Angelis (2016). This body of event study literature reviews serves as a valuable source of reference within event study literature and includes identification of varying domains explored within IS/IT using Event Study Methodology (ESM), based on *Event Study Approach* (ESA). However, minimal *privacy* research has been conducted within the extant body of event study literature committed to understanding corporate investments in privacy, nor examining financial implications resulting from corporate investments in privacy (as its own independent, singular construct). Outside of inclusionary attention as a security byproduct during research exploring an Information Security (InfoSec) breach incident, minimal research has been completed to gain a better understanding of potential financial implications of corporate investments in privacy (Acquisti et al., 2006).

To help bridge this gap, this investigation adds to the extant body of knowledge by examining an area of event study research not yet fully explored. Examining corporate investments in privacy using Event Study Methodology (ESM) provided a better understanding of the financial implications associated with corporate investments in privacy. In addition, the research conducted presents corporations with an additional tool to reference when making investment decisions regarding privacy needs within corporate environments as well as when deciding on corporate investments in privacy. Furthermore, results and analysis identified within this research can be extrapolated for use across other IS, IT, InfoSec, and related domains. Results highlight existing relationships between corporate investments in privacy and the financial impact they have on overall stock market value for the associated corporation, as well as identify the

statistical significance of the relationship between the overall stock market impact and the corporate announcement event.

1.4 Research Questions and Hypotheses

This research dissertation conducted an event study to examine corporate investments in privacy. Using available public data, this research implemented Event Study Methodology (ESM) to identify potential financial implications to overall corporate stock market value from corporate investments in privacy, identified financial incentives relating to corporate investments in privacy, and gained a better understanding of why there has been so little interest in corporate investments in privacy.

1.4.1 Research Questions

Privacy as a construct has the same pervasive meaning regardless of industry; safeguarding Personal Identifiable Information (PII) while ensuring *Confidentiality, Integrity, and Availability* (CIA) of corporate and client data. Corporations utilizing Information Systems (IS), Information Technology (IT), Information Security (InfoSec), and related technology within their corporate environment have not only the moral responsibility for ensuring data privacy, they also have the more important task of ensuring organizational privacy is implemented to ensure safeguarding of data they import, employ, and export, based on financial value and importance of the data.

Ensuring corporate and client data privacy is an extremely important corporate responsibility, yet inconceivably, corporate shareholders perceive only relative financial value from corporate investments in privacy; investments in privacy designed, deployed, and implemented *specifically* to ensure privacy protection of data they possess, as well as maintaining compliance with any forced governmental imposed industry regulations.

Event study research provides the capability for corporations to identify potential financial impact investments can have on overall stock market value.

(*i*) *Research Questions*

In examining corporate investments in privacy, this research addressed the following research questions in greater detail while providing a better understanding of corporate investments in privacy and identified the financial implications related to corporate investments in privacy:

RQ 1. Why are corporations not investing in privacy?

Previously conducted *Event Study* research (various technology domains) provides literary support indicating positive potential for corporations to financially benefit from increased overall stock market value, yet minimal research interest has been shown examining the financial benefits from corporate investments in privacy; why?

While previous event study privacy research has identified one possible reason behind minimal research interest by corporations, a lack in perceived value from corporate investments in privacy, additional research data gathered from this proposed research examination provides a better understanding of *why corporations are not investing in privacy*.

RQ 2. Do financial incentives exist motivating corporate investment in privacy?

Minimal event study research has been conducted examining corporate investments in privacy, but there has not been enough resultant data produced from examining corporate investments in privacy to discern the presence of any financial incentives motivating corporate investments in privacy.

This research examination provides additional data points and analysis from a deeper investigation of corporate investments in privacy; however, it is posited that limited financial value exists from corporate investments in privacy, and, by extension, limited economic incentives exist encouraging corporations to make proactive, continued, or repeated investments in privacy.

RQ. 3 What industry benefits most from corporate investments in privacy?

This research conducted an event study to examine corporate investments in privacy. Results from this research provide insight into which industry benefits the most, and identified which industry is most positively affected overall from

> corporate investments in privacy. Evaluation of which industry "benefits the most" is based on largest financial impact to overall corporate stock market value from corporate investments in privacy; across different industry groups. This information may contribute to future proactive corporate investments in privacy.
>
> Fama et al., (1993) expressed a similar observation, "…corporate investments may have different effects on firm value in the financial services industry then in the manufacturing industry."

Privacy is an important component to ensuring the continued successful operation of any corporation. However, little is known about the financial underpinnings behind corporate investments in privacy. This research makes a contribution to the extant body of literature by presenting an empirical research investigation examining the potential financial stock market impact associated with corporate investments in privacy (along with their related public announcement announcing the specific corporate investment in privacy). In addition, this research identified financial incentives associated with corporate investments in privacy. Identification of positive financial incentives (for example an increase in overall corporate stock market value) may be a motivating factor encouraging proactive corporate investments in privacy.

1.4.2 Research Hypotheses

Successful deployment of Event Study Methodology (ESM) in multiple domains encouraged the rapid escalation and expansion of ESM into Information System (IS) / Information Technology (IT), Information Security (InfoSec) and related event study research fields for both academics and corporations. Historical ESM research identified both positive and negative financial stock market impact is possible when evaluating corporate investment announcement events. Corporate investment announcement events identified as generating *increased corporate wealth* were rewarded with *positive* (+) feedback and increased corporate stock market value. Conversely, corporate investment

announcement events identified as causing a *loss of corporate wealth* were punished by shareholders with negative feedback (–) leading to decreased stock market value.

From the literature review, for example: *IS/IT Outsourcing Investments* (Agrawal et al., 2006; Gewald & Gellrich, 2007); *Enterprise Resource Planning* (ERP) (Benco & Prather, 2008); *Supply Chain* (Mitra & Singhal, 2008); and *E-Commerce* (Walden & Browne, 2008) have all been associated with *positive* (+) shareholder feedback and increased corporate wealth. In direct comparison, *Information Security* (InfoSec) breach incident events causing information loss, data corruptions and theft, and violations to privacy and data integrity, including *Hacker Attacks* (Ettredge & Richardson, 2003; Chen et al., 2011), *Viruses* (Hovav & D'Arcy, 2005), *Phishing Scams* (Hinz et al., 2014), and *Data Loss / Theft* (Culnan & Williams, 2009; Gatzlaff & McCullough; 2010) have all been linked with *negative* (–) shareholder feedback and reduced stock market value.

(*ii*) *Research Hypotheses*

The null hypothesis that corporate *Abnormal Returns* (AR) are not significantly different from zero (0) is *rejected* in this research. It is expected that observable corporate AR's will be significantly different from zero (0). In this research, the z-test statistic will be used to assess whether or not the Average Cumulative Abnormal Return (ACAR), or Mean CAR, was significantly different (statistically) from zero, its expected value (McWilliams & Siegel, 1997). Furthermore, according to Im et al. (2001), the significance of the abnormal return based on the z-statistic test allows the researcher to infer that the privacy investment announcement events had a significant impact on the market value of the firm (Loderer & Mauer, 1992; McWilliams & Siegel, 1997). This was necessary to test the null hypothesis, as well as to test all hypotheses posited within

this research regarding corporate investments in privacy. In addition, the z-statistic will be deployed (Hovav & D'Arcy, 2005) to test the statistical significance of all AR's from corporate investment announcement events within the sample data set, and to assess whether or not *Average Cumulative Abnormal Return* (ACAR) (Mean CAR) is significantly different from zero, its expected value (McWilliams & Siegel, 1997). The appropriate Z-test statistics will be calculated based on *Expected Normal Return* (ENR), and use *Generalized Sign Test* (GST) for comparing positive (+) versus negative (-) returns (Filbeck et al., 2005).

In this research, an Event Study (ES) will be conducted to better understand corporate investments in privacy, as well as identify financial impact that corporate investments in *Privacy* had on the associated corporation's overall stock market value. After reading and analyzing previously identified Information System (IS) / Information Technology (IT), Information Security (InfoSec) and related Event Study (ES), Event Study Methodology (ESM), and Event Study (ES) data analysis and research results, it is expected there *will be* minimal financial impact to overall corporate stock market value associated with a corporate investment in privacy (rejecting the null hypothesis). Furthermore, this research posits that while there *will be* an observable financial impact to overall corporate stock market values associated with corporations investing in privacy that will be of minimal economic consequence, and *will not* be seen as a financial incentive encouraging corporate investments in privacy, nor as a motivating factor driving corporate investment in privacy as method of proactive measure intended to reduce the potential for future privacy breach incidents from occurring.

H1: ***There is positive capital markets' reaction to proactive corporate announcement events indicating privacy investments to enhance corporate privacy***

It is posited that there will be *an observable financial impact on overall corporate stock market value* for corporations associated with proactive investments in privacy made to enhance corporate privacy.

H2: ***Positive stock market reaction to corporate investments in privacy will be significantly greater in years 2013-2015 when compared to years 2016-2018***

As noted by Dinev & Hart (2006), end users are becoming more tolerable from bad corporate privacy protection methods, leading to exposure of individual "Personal Identifiable Information" (PII) in exchange for discounts in goods and services. As end user data exploitation acceptance levels grow, the less end users will expect corporations to do in order to securely protect their individual information privacy and PII.

Protecting CIA of users PII was a major information privacy concern years ago, research has unfortunately shown this is no longer the case. As Cate noted, the unfortunate reality is that data breaches are becoming the norm, and as "…news of privacy invasions and data breaches become more and more common" (Cate, 2005), loss of privacy protection and individual PII abuse becomes more rampant and acceptable.

H3: ***Stock market reaction from privacy incident events will be accepted as financially insignificant based on minimal corporate stock market loss***

This testing will help identify *why* corporations are not investing in privacy. Prior research indicates that similar to the "Privacy Paradox," privacy protection and individual end user privacy concerns have been replaced by incentives for discounts and free consumer goods, services, and discounts (Dinev & Hart, 2006). Since users today have become accustomed to less privacy, corporations will continue to "*not invest in privacy*" nor change privacy investment practices as there is no financial incentive encouraging them to do so from shareholders, nor financial loss implications from privacy breach incidents. Any expected stock market loss from announcement events indicating privacy incidents will be dismissed due to the overall minimal financial impact on corporations' stock market value.

Any observable increases in overall corporate stock market value in previous event study research examining financial impact from corporate investments in privacy has been identified as an outlier event leading to minimal economic improvement, and not indicative of sustainable, long term increased corporate wealth.

As a business unto itself, corporations have a singular responsibility to their shareholders; generate financial profit through increased growth of corporate wealth. If there is no financial incentive to encourage corporate investments in privacy, the investing corporation will be punished by shareholders for making a bad investment decision; leading to a loss of corporate wealth through a reduction of stock market value. Until financial incentives exist to encourage corporate investments in privacy, corporations are not going to modify current investment strategy or investment behavior.

To date, financial stock market reward for corporations investing in privacy has been less than the cost to implement the privacy protection mechanism, resulting in a net loss of revenue. Furthermore, despite end users demanding better privacy protection from corporations in possession of their PII, corporation will not be financially encouraged to actively invest in privacy until corporate incursion of financial losses direct resulting from a privacy breach incident are seen as equal to financial loss levels experienced during an InfoSec breach incident. Seemingly against the wishes of end users to prevent future breach incidents from occurring, corporations will continue to avoid investments in privacy as the cost for investment is privacy is higher than potential financial losses obtained from not investing.

1.5 Relevance and Significance

This research helps bridge the research gap in the extant privacy literature; limited event study research available examining financial impact from corporate investments in privacy. Supplementing the extant body of research literature in this domain, this research provides an additional examination of corporate investments in privacy, as well as supporting research helping identify potential financial incentives related to corporate

investments in privacy. This research also provides a better understanding of *why* corporations are not as financially vested in privacy investments when compared to Information System (IS), Information Technology (IT), Information Security (InfoSec), and related technology investments; specifically, when evaluated against corporate investments in InfoSec and government compliance.

Since stock market impact from corporate investments in privacy may be different across industry segments, it was important to identify where corporate investment in privacy offer the highest economic *Return on Investment* (ROI) (Hinz et al., 2014; Huang & Behara, 2013). While conducting research examining how investment announcements affected stock market value for different industry groups, Fama et al., (1993) expressed a similar observation, "…corporate investments may have different effects on firm value in the financial services industry then in the manufacturing industry." Using Event Study Methodology (ESM) in this event study, the resultant data analysis discovered helped to identify how corporate investment in privacy had varying economic impact to overall corporate stock market value across different industry segments, as well as identifying specific industry domains that benefitted the most from corporate investments in privacy.

The totality of Event Study (ES) research conducted, using Event Study Methodology (ESM) to explore the financial impact that corporate investments in privacy had on corporate stock market value, has been completed by Acquisti et al. (2006), Aytes et al. (2006), Hinz et al. (2014); Khansa et al. (2012); Khansa & Liginlal (2009), Malhotra & Malhotra (2010), and Nicholas-Donald et al. (2011). Due to a mixed result in findings and analysis extracted from their research, plus the minimal number of event study privacy research conducted in the literature, additional research investigation will

help bridge the research gap in event study literature while providing a better understanding of corporate investments in privacy, and potential financial implications to overall corporate stock market value from corporate investments in privacy.

With minimal identifiable research within the extant body of literature examining *voluntary* corporate investment in privacy, healthcare and finance provide a valuable source of reference highlighting the need for additional examination of corporate investments in privacy. Through forced government action, corporate investments in privacy have been mandatory to remain compliant yet serve as evidence supporting additional research examination of corporate investments in privacy. Personal information being handled and shared in healthcare and finance is of such importance that the federal government felt necessary to intercede on the individual user's behalf.

To ensure healthcare and finance corporations take privacy protection and security of users Personal Identifiable Information (PII) seriously, the government introduced congressional protection acts in Healthcare (*Health Insurance Portability and Accountability Act* (HIPAA) and in Finance (*Sarbanes-Oxley Act* (SOX) of 2012 and *Gramm-Leach-Bliley Act* (GLBA). HIPAA, SOX, and GLBA are examples of "*Forced Policy Compliance*" (FPC); specific governmental privacy enforcement initiatives mandating implementation of privacy controls to protect, preserve, and ensure client PII is safeguarded. While negative financial incentives do not generate any direct wealth for the corporation, they do offer the potential for reduced financial loss from governmental noncompliance fines and penalties. However, failure to comply with HIPAA, SOX, or GLBA in any manner results in corporate financial fines and penalties in an escalating

manner for each identified non-compliance offense (Chai et al., 2010; Huang & Behara, 2013; Khansa et al., 2012; Khansa & Liginlal, 2009; Schwaig et al., 2006).

Forced Policy Compliance (FPC) are industry-specific behavioral protocols imposed by government regulators enforcing specified guidelines designed to force corporate compliance of designated standards under threat of noncompliance fines and financial penalty (Chai et al., 2010; Huang & Behara, 2013; Khansa et al., 2012; Khansa & Liginlal, 2009; Schwaig et al., 2006). An example in healthcare is *Health Insurance Portability and Accountability Act* (HIPAA). Introduced in 1996, HIPAA provides privacy and security protection guidelines to all corporate entities and workplace personnel handling, storing, or accessing medical data or information (Khansa et al., 2012). Finance examples include *Sarbanes-Oxley Act* (SOX) of 2012 and *Gramm-Leach-Bliley Act* (GLBA). Introduced in 2012, SOX (Schwaig et al., 2006), protects shareholders and general public from corporate fraud and financial misconduct; introduced in 1999, GLBA (Case & King, 2015; Huang & Behara, 2013) (aka *Financial Modernization Act* (FMA99), federally regulates the manner in which corporate workplace personnel handle, store, or access Personal Identifiable Information (PII) of individuals they are working with in a financial environment.

Growing individual privacy concerns have also led to improved data protection laws to protect users from threats. Due to the importance of protecting consumer PII, continued identify theft breach event incidents have "…led to the creation of public disclosure laws requiring corporations to report incidents where customers' personal information is unlawfully or accidentally revealed" (Goel & Shawky, 2009). An illustration of this is a type of privacy threat known as "identity theft." In addition,

federal laws now ensure corporate entities disclose to consumers how the corporation will be sharing their private, financial information, and what rights they have as an individual consumer regarding corporate data collection and sharing processes.

In addition to forced government compliance in healthcare and banking, privacy as an independent component of corporate data protection has been another area providing evidentiary support for additional research examination of corporate investments in privacy. Prior event study research conducted has provided corporations with requisite evidentiary data justifying specified corporate investments in Information System (IS), Information Technology (IT), Information Security (InfoSec), Computer Security (ComSec), Internet Security (IntSec), and related technology domains. As a byproduct of the information age that transformed the manner which corporation's conduct business, and partially discovered through strategic investments in technology domains, the concept of data protection as a service morphed into a separate corporate commodity; an independent security resource possessing its own ability to cause financial wealth generation, or financial loss, if not recognized and managed correctly (Culnan & Williams, 2009; Hovav et al., 2017; Malhotra & Malhotra, 2010). Academics interested in privacy as an independent construct have conducted event study research exploring whether there exists an *actual cost* to corporation's when encountering an internal privacy breach, as there is only scattered evidence about the price companies even pay for their privacy debacles (Acquisti et al., 2006).

Data protection as a monetizable commodity includes software and hardware to ensure privacy and security protection for user and corporate information. Indirectly, digital information and client data have also become an extremely valuable corporate

asset worth protecting. Corporate implementation of data protection services include providing: 1) data Confidentiality, Integrity, Availability (CIA) for all user, employee, and corporate data the corporation possesses, 2) data protection for all digital information and electronic records, and 3) privacy protection for user for all user Personal Identifiable Information (PII) and sensitive data. Though the implementation of corporate data protection has encompassed primarily InfoSec measures (Andoh-Baidoo & Osei-Bryson, 2013; Bose & Leung, 2014; Chen et al., 2011; Garg et al., 2003; Hovav & D'Arcy, 2003, 2005; Hovav et al., 2017; Morse et al., 2011; Telang & Wattal, 2007), corporate investments in privacy were also implemented with success within corporate environments (Acquisti et al., 2006; Culnan & Williams, 2009; Dinev & Hart, 2006; Malhotra & Malhotra, 2010; Nicholas-Donald et al., 2011).

Corporations not engaged in promoting strong data protection can be susceptible to lost revenue and consumer trust (Bose & Leung, 2014), network exploitation, and aggressive attack vectors (Hovav & D'Arcy, 2005); directly resulting in the potential for massive financial losses, penalties, and fines (Culnan & Williams, 2009; Hinz et al., 2014; Hovav et al., 2017; Huang & Behara, 2013; Malhotra & Malhotra, 2010; Nicholas-Donald et al., 2011). Exposure of client Personal Identifiable Information (PII) through a privacy breach, occurring during an Information Security (InfoSec) attack, is undesirable situation for a corporation. However, research has shown a stronger financial incentive motivating the securing of corporate data (security) against an InfoSec attack (Hovav & D'Arcy, 2005; Telang & Wattal, 2007) then there is ensuring the Confidentiality, Integrity, and Availability (CIA) of client data (privacy) against a privacy breach.

Furthermore, there is little evidence supporting a consensus about the price companies even pay for their privacy debacles (Acquisti et al., 2006).

While this data practice may run counterintuitive to what clients' desire regarding PII corporations are in possession of, there must exist a positive financial incentive encouraging corporations to change their data policy guidelines regarding privacy, and consequently, their position on investments in privacy (Aytes et al., 2006; Chai et al., 2010; Hinz et al., 2014; Huang & Behara, 2013). Research portends that corporations suffering small, minimal financial loses in revenue from privacy breach incidents will not be financially motivated to ensure the prevention of additional privacy incursions in the future. For example, while being a victim of a massive data breach, exposing millions of consumers' Personal Identifiable Information (PII), both Equifax/Experian (Malhotra & Malhotra, 2010; Nicholas-Donald et al., 2011), and ChoicePoint (Acquisti et al., 2006) have shown an arcane ability to not just fully recover financially (pre-breach stock market trading levels) but have profited from the privacy breach. (Acquisti et al., 2006; Amerding, 2018; Aytes et al., 2006; Kiesnoski, 2019).

Previous event study research identified positive financial impact to overall corporate stock market value from corporate investment in IS/IT as a motivating factor for increased corporate investment (Dardan et al., 2005; Subramani & Walden, 2001). However, this creates a concerning paradox when applied unilaterally to corporate investments in privacy. Using the excuse of minimal research identifying positive financial implications from corporate investments in privacy, which is dismissed due to low volume of additional supporting research, corporations choose to not invest in privacy. With no corporate investments in privacy to examine, additional research cannot

be done to provide the "missing research identifying positive financial implications from corporate investments in privacy" and the cycle continues. This paradoxical phenomenon of a complete lack of corporate investments in privacy needs further examination to better understand why corporations are not investing in privacy.

With complete integration of security and privacy fused with software and hardware technology in every corporate environment, a research opportunity exists in better understanding corporate investments in and the financial implications from corporate investments in privacy. Dedicated research conducted in this manner will help in discerning whether or not corporate investments in privacy have an economic impact on the corporation's overall stock market value, and whether or not financial incentives exist encouraging corporate investment in privacy. Minimal event study research has been conducted that provides data analysis support identifying financial implications from corporate investments in privacy (Acquisti et al., 2006; Culnan & Williams, 2009; Dinev & Hart, 2006; Malhotra & Malhotra, 2010; Nicholas-Donald et al., 2011). So why are there not more corporate investments in privacy?

This research examination makes an academic contribution to the extant body of event study and privacy literature by completing its research objective examining corporate investments in privacy. In doing so, this research examination provides a better understanding of corporate investments in privacy, identified financial implications to overall corporate stock market value from corporate investments in privacy, and discovered economic incentives relating to corporate investments in privacy. Equally important, this research examination of corporate investments in privacy also provides a better understanding of *why corporations are not investing in privacy*?

1.6 Barriers and Issues

Based on examination of previous event study literature, strategic investments in technology have shown an ability to provide increased corporate wealth, with correlated gains in corporate stock market values, when the right IS/IT investment is deployed, at the correct time, within the best corporate environment. However, a major problem surrounding corporate investments in IS/IT is understanding how to accurately evaluate financial impact of corporate investments on stock market value, especially when evaluating corporate investments in privacy (Cate, 2005; Gellman, 2002).

To better understand the financial impact an "unexpected event" has on corporate stock market value, analysis of financial information was conducted using Event Study Methodology (ESM) (based on the *Efficient Market Hypothesis* (EMH) *theory* developed mainly by (Fama et al., 1969, 1970). In event study research, the unexpected event being investigated for potential financial impact is identifiable as a public announcement made by the corporation. The research goal of a general event study is determining if public disclosure of the identified corporate announcement event had any financial impact on the corporation's overall stock market value. Likewise, the research goal of an Information System (IS) / Information Technology (IT) event study is determining if public disclosure of the identified IS/IT corporate announcement event had any financial impact on the corporation's overall stock market value.

1.6.1 Barriers

While there has been extensive event study research conducted within IS, IT, and related domains, examining overall stock market impact from corporate investments in IS/IT (hardware, software, policy), minimal event study research has been conducted

examining corporate investments in privacy, potential financial ramifications from corporate investments in privacy, and financial implications from corporate investments in privacy "…implemented to better protect the PII and CIA of client, employee, and corporate data" (Acquisti et al., 2006).

With responsibility in generating as much increased corporate wealth as possible, investment decisions are guided by the ability of the investment option to generate the largest increase in overall stock market value, based on IS/IT research previously identified by academics. This practice, however, has led to a reduced volume of privacy research as attempts to better understand how better security for PII and CIA of personal and user data, implemented through corporate investments in privacy, have not been seen as a motivating factor driving increases in overall corporate stock market value.

Literary evidence exists to support the realization that not only are corporations not interested in proactively investing in better privacy protection measures, corporations are even less concerned about addressing privacy concerns reactively after a privacy breach incident has occurred (Acquisti et al., 2004, 2006; Culnan & Williams, 2009; Dinev & Hart, 2006). Moreover, few corporations appear to even be worried about potential financial fallout from a privacy breach incident, nor do corporations seem to be worried about possible information theft, loss, or abuse of corporate, client, and consumer PII they are directly charged with protecting (Acquisti et al., 2006; Chai et al., 2010; Hinz et al., 2014; Huang & Behara, 2013; Nicholas-Donald et al., 2011). Limited research conducted to date using Event Study Methodology (ESM) in examining stock market impact from corporate investments in privacy leaves a gap in the extant literature that this

investigation will address by examining corporate investments in privacy and identifying financial implications from corporate investments in privacy.

The global climate regarding personal concern for individual privacy has caused an increased shift towards a renewed research focus within Information System (IS), Information Technology (IT), and associated event study research towards *Privacy*. As a result, this research investigation offers a focused examination of corporate investments in privacy, while providing a better understanding of potential financial implications to overall corporate stock market value from corporate investments in privacy. Successful completion of this research contributes to the extant body of knowledge by 1) providing empirical evidence identifying the financial implications associated with corporate investments in privacy, 2) quantifying the financial impact that corporate investments in privacy had on overall corporate stock market value, and 3) offering a better understanding of financial incentives relating to corporate investments in privacy.

1.6.2 Issues

There are inherent challenges conducting an Event Study using Event Study Methodology (ESM). After examining previous Information System (IS), Information Technology (IT), and associated event study research and literature in the extant body of event study literature, with special attention on *Privacy and Information Privacy*, one major issue is the lack of consensus on a specific research design construction for data analysis in an event study. A multitude of different theories on research design construction have been presented by respected authors in their research field, with each investigation achieving comparable levels of research success using the various theories.

In addition, Information System (IS), Information Technology (IT), and associated event study research studies conducted within multiple domains have been successfully completed, with each author and study deploying a varying calculation methodology for identifying stock market impact. While all event study research utilized Event Study Methodology (ESM) in realizing their stated research objectives, many different financial calculation models were deployed to determine exact stock market impact. As noted, while "…there is no consensus on even the best method to use, and none of the available methods includes the costs of preventing a privacy incident: with the net effect of a privacy breach remaining an open question" (Svensson, 2003), there is also inconsistency on types of information theft causing financial harm; Garg et al. (2003) showed that breach of credit card information had a large negative effect on stock price, while theft of consumer information had a negligible impact (Acquisti et al., 2006).

Moreover, there is varying consensus on research design among previously conducted Information System (IS), Information Technology (IT), and associated event study research. Many different authors of event study research have utilized varying measuring techniques for assessment of corporate announcement events within their research, including different: event windows, estimation windows, analysis methodologies (Acquisti et al., 2006; Hendricks & Singhal, 1996, 1997), and even the effects of the privacy loss (Cate, 2005; Gellman, 2002). Despite the lack of standard practices for research model design in event study research, deployment of Event Study Methodology (ESM) remains the best tool to use when assessing potential financial impact of an unexpected event on corporate stock market value.

1.7 Assumptions, Limitations, and Delimitations

This research explored corporate investments in privacy through an economic lens to better understand the financial impact that privacy investments have on the stock market value of the corporation making the privacy investment. To identify stock market impact that corporate investments in privacy have on the associated corporation, an event study was conducted using Event Study Methodology (ESM) to evaluate financial affect from corporate press release announcements events relevant to privacy investments. Specifically, the theory of Efficient Market Hypothesis (EMH) was utilized to determine potential financial impact from each corporate press release announcement event identifying a corporate investment in privacy.

1.7.1 Assumptions

Utilization of Event Study Methodology (ESM) using the theory of Efficient Market Hypothesis (EMH) requires the acceptance of several assumptions regarding the stock market. First, the main assumption when implementing EMH is that stock market values for all publicly traded corporations are based on an *efficient market*. EMH asserts that financial markets are informationally efficient, and that stock prices reflect all publicly available information (Goel & Shawky, 2003). Based on the accepted industry and academic definition by Fama et al. (1969), in an *efficient market* all publicly available information for a corporation being traded on the stock market is incorporated into the corporation's stock market price.

In an *efficient market*, any newly available information will be quickly absorbed by the corporate shareholders then immediately figured into any change in stock market price. Any "adjusted" stock market price will be based on the perceived value of the new

information. In this research, new information is the corporate privacy investment announcement, and any changes in overall stock market value will be based on the perceived value of the privacy investment by the corporation's shareholders. The theory of EMH asserts that "as investors strive to earn profit from market trading, they exploit every useful piece of data, thereby causing market prices to reflect all of the relevant information at any given moment" (Kliger & Gurevich, 2014). One accepted assumption in this research is any announcement event identifying a corporate investment in privacy will be associated with some perceived financial value by the corporation's shareholders then reflected in the new overall stock market value for the corporation.

1.7.2 Limitations

In this research, several methodology limitations exist regarding use of Event Study Methodology (ESM). Within this event study, all data collected and analyzed will come from publicly traded corporations. In addition, all publicly traded corporations must be traded on one (1) of three (3) US-based stock market indexes: NYSE, AMEX, or NASDAQ. Furthermore, all included announcement event data identified for event study sample inclusion must be from corporation's that are publicly traded on one of three (3) identified stock indexes. In addition, corporations with data identified as acceptable for being publicly traded *must also* have been actively trading during accepted estimation (195-Days) and event windows (t = -1, t = 0, t = 1).

Additional limitations may constrain overall generalizability of the results in some capacity. Since all information is gathered *only* from publicly traded and actively traded corporations, any possible relevant information relating to corporate investments in privacy from entities not publicly traded will be omitted from the data sample

(i.e., private corporations, government, education, etc.). Moreover, corporations not traded in the US on one (1) of three (3) US-based indexes will also be excluded from sample data. Lastly, corporations with trading inactivity surrounding the corporate privacy investment announcement date (event window) will be excluded from sample. The inclusion/exclusion of data from these corporations may impact data analysis results as they may potentially limit the scope of the data sample available for analysis.

1.7.3 Delimitations

Delimitations will be implemented to control the scope of research investigated. Event Study Methodology (ESM) has been employed as an academic resource for over six decades, beginning with initial deployment within an Information System (IS) / Information Technology (IT) domain by Dos Santos et al., 1993. To focus the applicability of the data analysis, data collection for corporate investments in privacy will be constrained to only IS / IT and related research domains and be subject to an imposed to a 5-Year time period (01/01/2013 – 12/31/2018). During those 5 years designated for data collection, all identified corporate press release announcement events indicating a corporate investment in privacy will be analyzed for study inclusion using identified data collection processes. Implementation of identified delimitations will allow the scope of the proposed data collection to be manageable while remaining focused directly on the research goals and stated study objectives.

Limitations within this research may potentially impact internal validity of this research, while any delimitations introduced to constrain research date scope may impact the generalizability of data analysis results. While both limitations and delimitations are present within this investigation, testing will be conducted to protect the validity of all

data results obtained. Internal validity testing will be employed to ensure the integrity of the data. Furthermore, the research design and methodology applied within this investigation will follow implementation guidelines espoused in previous event study literature, including event studies using ESM in: *Accounting and Finance*, *IS*, *IT*, and *InfoSec* to evaluate the stock market impact from corporate press release announcements.

1.8 Definition on Terms

Definitions of Key Terms provided are accepted for use within this research:

1) *Privacy* –

Margulis (1977a, 1977b) identified *privacy* as a cognate-based control that extends to information privacy implemented and executed by individuals when controlling the flow of data related to themselves. Privacy as a control can be used to "… represent the control of transactions between person(s) and other(s), … and to enhance autonomy and/or to minimize vulnerability."

> The presented definition of *Privacy* as a control (Margulis, 1977a, 1977b), is accepted for use in this research. The definition is similar to Westin (1967) who referred to privacy as the ability of the individual to control the terms under which personal information is acquired and used. In this, individual concern for privacy (data control) are often in conflict with corporate use, storage, and management of client data and individual PII.
>
> *Privacy* as a control allows individuals to be in control; controlling their own PII and individual digital data until it becomes the possession of a corporate entity. At that time, intersection of *privacy* (as a control) and *Information Privacy* occurs beyond the limited control of the individual.

2) *Information Privacy* –

Despite limited control of information once collected from corporations, client's express concerns over *how* their data is being used. Smith et al. (1996) proposed collection, unauthorized secondary use (using data for purposes other than those

originally collected for), improper access, and errors as multiple dimensions of information privacy. In addition, Solove (2006) recognized expanded dimensions of information privacy to include information collection, processing, invasion, and dissemination as client concerns for data use of personal information.

> With digital data in its infancy, an accepted use definition was presented by Bélanger et al. (2002) and Stone et al. (1983); based on Westin's (1967) original definition. The updated definition presented by Bélanger et al. (2002) and Stone et al. (1983) identified *Information Privacy* as one's ability to control information about oneself. However, as the digital age has grown exponentially, customers no longer possess the ability to control *how* their individual data and PII is used once corporate controlled.
>
> In this research, *Information Privacy* relates to individual client concerns regarding *i*) manner corporations collect their PII, *ii*) nature in which corporations use individual PII under corporate control, and *iii*) potential for corporate misuse and abuse of PII in their possessions through third party sources; similar to Westin (1967). In his research, Westin referred to the definition of *Information Privacy* as individual control over collection, use, and dissemination of their own personal data and information.

3) *Information Security* –

As defined by Cherdantseva & Hilton (2013), *Information Security* is … concerned with development and implementation of security countermeasures of all available types (technical, organizational, human-oriented and legal) in order to keep information in all its locations (within and outside the organization's perimeter) and, consequently, information systems, where information is created, processed, stored, transmitted and destructed, free from threats.

> Definition of *Information Security* presented by Cherdantseva & Hilton (2013) is accepted for use within this research. *Information Security* is identified as an all-encompassing defensive posture composed of security layers including: physical security, personnel, hardware, software, and training/education. A multi-layered posture is necessary for ensuring real-time CIA for all PII (corporate and individual) in an efficient and reliable manner, across a variety of computing devices (desktop, laptop, mobile),

and spanning multiple geographic locations around the world where data is accessed.

1.9 List of Acronyms

Full Text Term	Acronym	Page #
Information System	IS	1
Information Technology	IT	1
Event Study	ES	1
Event Study Methodology	ESM	1
United States	US	1
Information Security	InfoSec	2
Investment Assessment	IA	4
Personal Identifiable Information	PII	6
Efficient Market Hypothesis	EMH	12
Director of National Intelligence	DNI	13
Information Sharing Environment	ISE	14
National Counterterrorism Center	NCTC	14
Department of Justice	DOJ	14
Department of Homeland Security	DHS	14
National Security Agency	NSA	14
Federal Bureau of Investigation	FBI	14
Health Insurance Portability and Accountability Act	HIPAA	15
Sarbanes-Oxley Act	SOX	15
Gramm-Leach Bliley Act	GLBA	15
Computer Security	COMSEC	15
Internet Security	INTSEC	15
Event Study Approach	ESA	16
Confidentiality, Integrity, and Availability	CIA	17
Enterprise Resource Planning	ERP	20
Abnormal Return	AR	21
Average Cumulative Abnormal Return	ACAR	21
Standardized Abnormal Return	SAR	21
Generalized Sign Test	GST	22
Return on Investment	ROI	24
Forced Policy Compliance	FPC	26
Financial Modernization Act of 1999	FMA99	26
Concern for Information Privacy	CFIPs	47
Fair Information Practices	FIPs	47
Social Contract Theory	SCT	51
Control Theory	CT	51
Control/Restricted Access Theory	C/RAT	51
Organization for Co-Operation and Development	OECD	52
United Kingdom	UK	53
Platform for Privacy Preferences	P3P	56
Privacy Calculus Model	PCM	58

Internet Users' Information Privacy Concerns	IUIPC	61
Federal Trade Commission	FTC	62
Dow Jones	DOW	62
Deterrence Theory	DT	64
Denial of Service	DOS	66
Distributed Denial of Service	DDOS	66
Knowledge Management Initiative	KMI	70
Mergers & Acquisitions	M&A	70
Supply Chain Management	SCM	73
Markowitz Model	MM	75
Random Walk Theory	RWT	76
Market Model	MM	82
Center for Research in Security Prices	CRSP	82
New York Stock Exchange	NYSE	83
American Stock Exchange	AMEX	83
National Association of Securities Dealers Automated Quotations	NASDAQ	83
Ordinary Least Squares	OLS	83
Cumulative Abnormal Return	CAR	87
Capital Asses Pricing Model	CAPM	87
Expected Normal Return	ENR	88
Hybrid Process Model	HPM	94
Blended Method Approach	BMA	95
Securities and Exchange Commission	SEC	96
Standard Industrial Classification (Code)	SIC	96
ProQuest	PQ	97
Business Source Premier	BSP	97
Generalized Autoregressive Conditional Heteroskedasticity	GARCH	107
Exponential Generalized Autoregressive Conditional Heteroskedasticity	EGARCH	107
Generalized Sign Z-test	GST-Z	109
Average Abnormal Returns	AAR	109
Crude Dependence Adjustment	CDA	110
Statistical Analysis System	SAS	111
University of Pennsylvania	UPENN	113
Wharton Research Data Services	WRDS	113

1.10 Summary

This research investigation explored an identified gap in the extant body of literature by expanding the limited set of privacy event study research previously completed (Hinz et al., 2014; Huang & Behara, 2013; Khansa et al., 2012) and

conducting an event study to examine corporate investments in privacy. In taking a deeper exploration of corporate investments in privacy, this research investigation helps to better understand the financial implications associated with corporate investments in privacy. In addition, this research helped extend the extant body of privacy literature by identifying the financial implications that corporate investments in privacy had on overall stock market value for the associated corporation.

Research data provides evidence suggesting an existing disconnect between actualized value and perceived value in corporate investments in privacy (Acquisti et al., 2006). Corporations with an obligation to shareholders in generating as much corporate value as possible make financial investment decisions in accordance with this goal. This action has limited corporate investment opportunities to only those investments with supporting data indicating the likelihood for increased corporate wealth. This corporate investment strategy appears to be a contributing factor contributing to reduced levels of research interest examining corporate investments in privacy. With limited research and mixed results from prior research examining corporate investments in privacy, corporations are undecided on whether or not potential financial rewards from corporate investments in privacy (increased overall stock market value) outweigh the required financial investment necessary for the proposed privacy investment.

This research examined corporate investments in privacy and identified the financial implications to overall corporate stock market value associated with corporate investments in privacy. Financial implications resulting from corporate investments in privacy were observable by fluctuating (positive (POS +) and negative (NEG -) increased overall corporate stock market values. By examining corporate investments in privacy,

this research helped to bridge the research gap identified during review of the extant body of event study literature; minimal event study research examining privacy, corporate investments in privacy, or potential financial implications associated with corporate investments in privacy. Furthermore, this research provides additional evidentiary support to previous event study privacy literature research highlighting the potential for financial changes in overall corporate stock market value from investments in privacy.

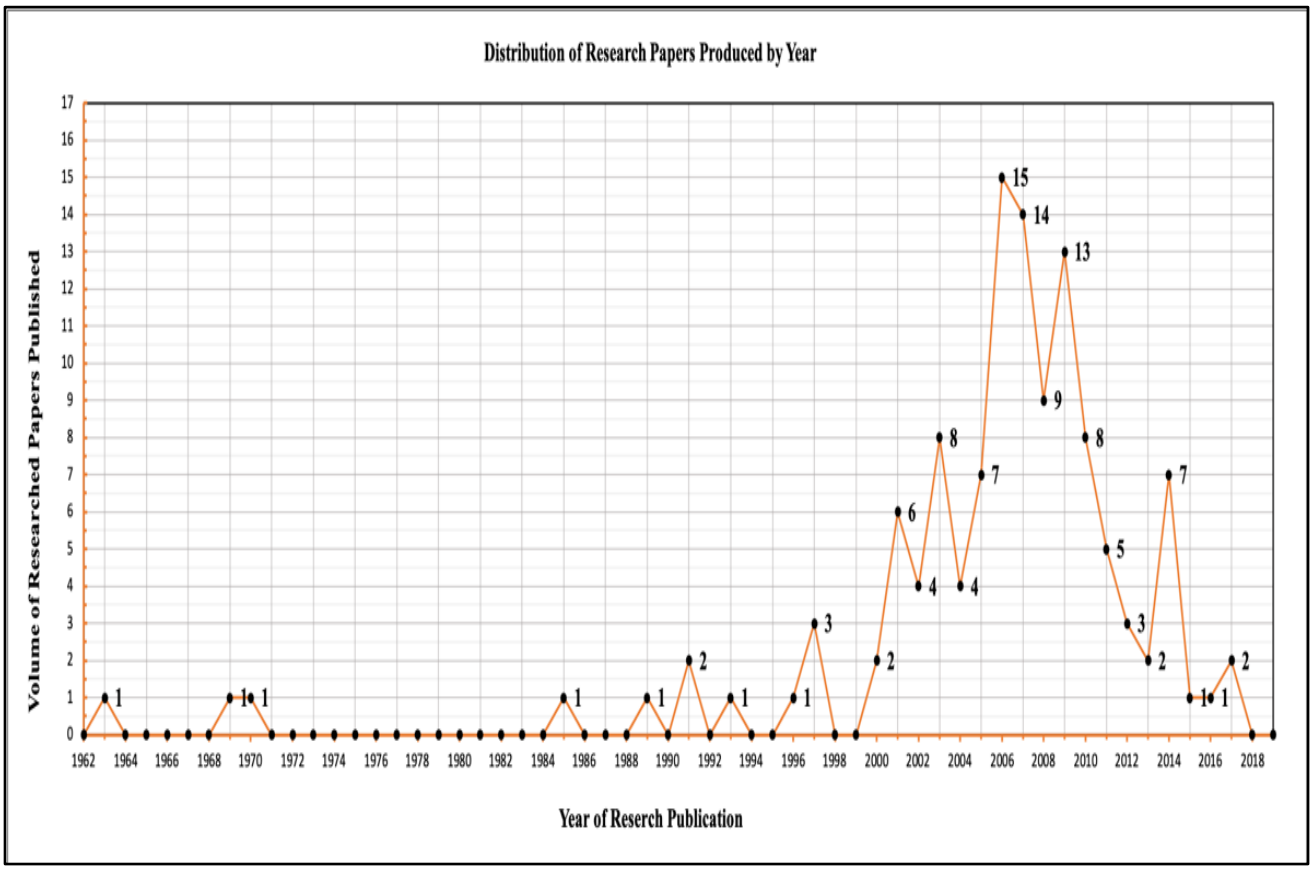


Figure 1 – Distribution and Volume of Event Study Research Papers (by Year)

Chapter 2

Review of the Literature

2.1 Introduction

The purpose of this chapter was to conduct a literature review of relevant research related to the dissertation topic: examining corporate investments in privacy. Understanding findings and academic contributions from previous research is key to identifying any research gaps within the extant information privacy literature, as well as ensuring the research objective of this dissertation is both attainable and makes an academic contribution to the extant body of information privacy literature. This literature review is separated into three (3) main sections beginning with *Information Privacy*, followed by *Privacy*, and lastly *Corporate Privacy*. The last section will provide a concise literature review summation of all *Event Study* research conducted within Information System (IS) / Information Technology (IT) and related domains, as well as "other," additional IS/IT-related event study literature (Appendix A provides full details for all event study and related research literature referenced in this research).

2.2 Information Privacy

In his 1967 seminal research work, Westin defined *Information Privacy* in simple terms as "… the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" (Westin, 1967). This definition of information privacy has since become universally accepted as the most widely accepted understanding as to the meaning and intent behind what information is defined as, and to what information privacy actually refers to in

contextual meaning. Awad & Krishnan (2006) agreed with Westin, referring to information privacy as the "… ability of the individual to personally control information about one's self" (Stone et al., 1983). Despite the simplistic definition, and basic fundamental application, implementation of information privacy is vast in meaning and complexity while encompassing multiple meanings in varying scenarios. As Malhotra et al. (2004) notes, "…although the notion of information privacy itself may sound straightforward, the practical boundary of information privacy in real life varies with numerous factors including industry sectors, cultures, and regulatory laws" (Andrews, 2002; Culnan & Bies, 2003; Milberg et al., 1995).

Applicability of information privacy in this investigation will be derived from its contextual meaning, while using a theoretical lens providing the information privacy viewpoint in context. In 1993, Culnan investigated information privacy concerns to understand differences between consumers who object to certain uses of Personal Identifiable Information (PII) from those consumers with no objection. When examining the practice of using collected PII for secondary use, the act of using PII that has been collected for one purpose but then used for a different, secondary purpose, Culnan (1993) discovered control as the identifying theme differentiating those individuals with positive outlooks towards secondary use (less concerned about privacy) of data from those individuals with a negative outlook (more concerned about privacy) towards the use of secondary data for non-specified and unknown (to the individual consumer) purposes.

With increased access to consumer PII, increased public concern began to focus directly on organizations in possession of that identified and collected consumer PII. In shared agreement with Culnan (1993), Smith et al. (1996) also focused their research

attention towards measuring individual concerns regarding organizational information privacy collection and usage practices. In this research, Smith et al. (1996) developed a 15-item instrument with four sub-scales (Collection, Errors, Unauthorized Secondary Use, and Improper Access), known as the *Concern for Information Privacy* (CFIP) measurement instrument (used as a tool during research investigations). Following the introduction of the CFIP privacy measurement tool by Smith et al. (1996), Stewart & Segars (2002) investigated the factor structure of the CFIP measurement tool to evaluate the effectiveness of CFIP within a continually changing business environment. Research by Stewart & Segars (2002) further validated the CFIP tool developed by Smith et al. (1996) as best suited for use when modeled as a second-order factor.

Introduction of *Fair Information Practices* (FIPs), and principles guiding FIPs, have also been widely recognized as methods of governmental intervention attempting to manage corporate collection, use, and accountability for business entities engaged in the process of consumer information exchange. Schwaig et al. (2005) states that while "…governments have participated in the development of Principles of FIP," it is their contention that these "Principles of FIPs" are able to "… control the use of personal information by limiting data collection and imposing accountability on data collectors (Schwaig et al., 2005). The premise is that through self-regulation, "… industries will develop rules and regulations as well as enforcement mechanisms" (Swire, 1997) that will satisfy end users concerned with corporate information privacy practices. End user concerns relating to the safeguarding PII and data are not overblown, however, as practices implemented "… carelessly can lead to abuse… and an invasion of information privacy" (Culnan, 2000; Laufer & Wolfe, 1977).

Due to the extreme necessitation for secure information, industry specific policy mandates have been introduced through legislation, by forced governmental compliance, and implemented in several domains, including healthcare and finance / banking. The most specific use case policy in healthcare is the "Health Insurance Portability and Accountability Act" (*HIPAA) – and the "Gramm–Leach–Bliley Act" (GLBA). Although well-intentioned, legislation can have negative consequences; e.g., the Gramm–Leach–Bliley Act, which requires financial institutions to notify consumers annually about their information practices, has been criticized for its implementation cost (Schwaig et al., 2005). To maintain both consumer trust and industry compliant, at a minimum, firms should develop information practices based upon acceptable standards and communicate the practices via privacy policies to the consumer (Swire, 1997).

* HIPAA was developed as a series of regulations to protect the privacy and security of certain health information using HIPAA Privacy Rule (aka. *Standards for Privacy of Individually Identifiable Health Information* – established national standards for the protection of certain health information) and HIPAA Security Rule (aka. *Security Standards for the Protection of Electronic Protected Health Information* – established national set of security standards for protecting certain health information held or transferred in electronic form)

Foxman & Kilcoyne (1993) argued that information privacy concerns are an active form of (personal) privacy control that can be overcome only "… when a person is (1) given control over personal information, and (2) informed about data collection and other issues" by the corporation in possession of user data. Caudill & Murphy (2000) extended this position of privacy concern as an active form of personal privacy control and proposed that "… an individual's concerns for information privacy center on whether the individual has control over personal information as manifested by the existence of voice (i.e., approval, modification) or exit (i.e., opt-out). This sentiment of privacy concern as a form of (personal) active privacy control is further supported in research by

Malhotra et al. (2004) who note that "… control is an active component of information privacy and it is often exercised through approval, modification, and opportunity to opt-in or opt-out." In contrast, awareness is a passive dimension of information privacy, and it refers to the degree to which a consumer is concerned about his/her awareness of organizational information privacy practices (Foxman & Kilcoyne, 1993; Culnan, 1995).

Information privacy concerns relate to personal information, electronic data, and individual PII that is now ingrained into every facet of daily existence (home, work, school), while integrating with virtually all of society through portable devices (cellular telephones, mobile payment, wireless Internet). In addition, corporations possessing this information maintain the ability to unilaterally decide how to use the personal information they have collected, and whether or not to sell any user information they have collected to third-party vendors (without user consent or knowledge and causing unintended user exploitation). "The general progression from information collection to processing to dissemination is the data moving further and further away from the control of the individual" (Solove, 2005).

Control over secondary use of information relates to the consumer's concern that once the information is freely submitted… there is diminished or nonexistent control of the further sharing of that information with third parties (Belanger et al., 2002). Personal information in a digital format can be easily copied, transmitted, and integrated, … and poses a serious threat to information privacy" (Malhotra et al., 2004) if the data is not secured and properly protected against exploitation.

Information privacy concerns relating to data control issues are often an issue of morality. For corporations, minimal legal compliance mandates exist enforcing

compliance of protection measures safeguarding user's information privacy concerns. Pavlou et al. (2007) note that this tension "… between organizational use of personal information and a person's information privacy concerns has been touted as one of the most important ethical issues of the information age (Mason, 1986). Information ethics and corporate morality become further muddied when questioning the intended use of user PII and private information corporations are in possession of, based on the global accessibility of digital information and the financial value PII and user data possesses.

Advances in Information Technology (IT) have produced efficiencies that have increased the value of personal information as a commodity for exchange, while globalization has increased the need for cross-border protection mechanisms … and information privacy safeguards (Henderson & Snyder, 1999). One of the major challenges preventing information privacy across continents, however, is the inability to implement globally accepted and enforceable international laws governing user's information privacy. Ease of collecting and accessing information over global networks has made information privacy concerns an international issue, complicated by variability in the way it is defined and protected by laws and policies across countries (Rose, 2005).

Another difficulty corporations face when addressing information privacy concerns is balancing equitable treatment of user data with financial interests of the corporation, and the subjective nature of both. Notably, information privacy concerns "… refer to an individual's subjective views of fairness within the context of information privacy" (Campbell, 1997). Corporate trust is an accepted belief associated with "fairness of information use" and applies to overall information privacy concerns users have regarding PII and data corporations possess. "Trusting beliefs are defined as the

degree to which people believe a firm is dependable in protecting consumers' personal information (Gefen et al., 2003; Grazioli & Jarvenpaa, 2000). On the other hand, "… risk beliefs refer to the expectation that a high potential for loss is associated with the release of personal information to the firm" (Dowling & Staelin, 1994).

Consumer beliefs in "corporate trust" and "fairness of information use" as information privacy concerns are concepts that align with *Social Contract Theory* (SCT); particularly in that SCT is unilaterally applicable to information privacy concerns. Malhotra et al., (2004) posits that "when applied to information privacy, Social Contract Theory (SCT) suggests a firm's collection of personally identifiable data is perceived to be fair only when the consumer is granted control over the information, and the consumer is informed about the firm's intended use of the information" (Malhotra et al., 2004). It can be argued, however, that it is "… impossible in today's world to have total control over personal information once it has been collected and dispersed (Tavani, 1999).

In addition to SCT, Westin's *Control Theory* (CT), and Moor's *Control / Restricted Access Theory* (C/R AT) can also be used when discussing information privacy and privacy concerns. Rose (2005) posits that Westin's *Control Theory* has been criticized as confusing privacy with autonomy (Westin, 1967). To help in this regard, Rose (2005) illustrates how Moor's *Control / Restricted Access Theory* "… separates the concept of privacy from the concept of control, stating that it is possible to have privacy without control and control without privacy; thus, concept of privacy, justification for it, and its management are distinct but interrelated concepts" (Moor, 1997).

2.3 Privacy

The honorable Judge Cooley emphatically declared in 1890 that "privacy was the right 'to be let alone'" (Brandeis & Warren, 1890). The simple proclamation made by Judge Cooley almost one hundred and thirty (130) years ago established the basic tenet identifying what it meant to have privacy that still resonates today. That idealistic definition of privacy has been slightly modified in time, most notably by Westin (1967). In his seminal privacy literature, Westin defined *Privacy* as the "… ability of the individual to control the terms under which personal information is acquired and used" (Westin, 1967). This definition of privacy posed by Westin has been universally accepted and forms the basis for all research relating to privacy.

The premise of Westin's definition of privacy is reliant upon a belief that while individual end users are concerned about their ability to enforce their personal privacy concerns regarding the terms under which their personal information is acquired and used, end users are most often worried about potential corporate abuse and misuse of their Personal Identifiable Information (PII). "Privacy concerns and practices, especially those dealing with the acquisition and use of consumer personal information, are at the forefront of global business and social issues associated with the information age" (Schwaig et al., 2005). While the phenomena of privacy, privacy concerns, and privacy concerns of end users have begun to gain more traction within the corporate and academic research arenas, privacy has been recognized as a significant issue in international electronic commerce as early as 1980 by the *Organization for Economic Co-operation and Development* (OECD) (Peslak, 2006).

In the United States (U.S.), while the Honorable Judge Cooley famously declared that "privacy was the right 'to be let alone'" (Brandeis & Warren, 1890), privacy "is not recognized" as a protected U.S. Constitutional right. Schwaig et al., (2005) notes that while "… not explicitly protected by the United States (U.S.) constitution, privacy is often termed a consumer right" (Goodwin, 1991). While privacy is necessary to an individual's personal autonomy and dignity in a modern democratic state (Cullen, 2009); however, at the same time, privacy is not regarded as an absolute right (Swartz, 2003). In the *United Kingdom* (U.K.), the Calcutt Committee has defined privacy as the ''right of the individual to be protected against intrusion into his personal life or affairs, or those of his family, by direct physical means or by publication of information" (Calcutt, 1990). In a manner similar to the U.S., privacy is also "not recognized" as a protected right under U.K. law. In most contexts, privacy is not viewed as an absolute right, but must be balanced against the needs of society (Calcutt, 1990).

As privacy as an individual right has not been guaranteed by protection of law, any expectation of privacy must be balanced against societal needs. Not surprisingly, this unresolved debate rages on while attempting to identify an appropriate mechanism that can successfully promote "acceptable" solutions when evaluating *individual privacy v. societal needs*. Westin (1967) and Nemati et al. (2003) argue that acceptable "trade-offs must be made to promote a balance between these seemingly competing interests (individual privacy v. societal needs)" (Nemati et al., 2003; Westin, 1967). Whereas in his research, Cullen (2009) notes that "… while scholars have claimed that privacy is a necessary requirement for life in modern democratic states…" in certain situations "… an

individual's right to privacy may be outweighed by the public interest in the disclosure of personal information" (Dempsey et al., 2003; Westin, 1967).

In their research, Cullen & Williams (2006) note that the "… decentralized technology environment today contributes to a different organizational privacy problem: data breaches" (Culnan et al., 2008). The decentralized technology environment relates to the global "… ease of collecting and accessing information over global networks, and has made both privacy and information privacy concerns an international issue; complicated more so by the variability in the way it is defined and protected by laws and policies across countries" (Rose, 2005). The global reach of electronic information combined with near instantaneous access across global borders without universal governing laws helps to ensure that *privacy* and *information privacy* "suffer from definitional ambiguity" (Solove, 2006).

As highlighted, varying nations around the world each imposing a different meaning for the accepted definition of privacy based on national law makes reducing threats to privacy a challenge. As the use of computers and network technologies expand globally, so to do privacy concerns about the collection and sharing of personal information (Caudill & Murphy, 2000). The global reach of instantaneous information access creates a massive threat to privacy and user privacy concerns due to differing laws, policies, and industry-specific guidelines in different countries around the globe governing privacy and electronic information.

Westin (1991) found that a portion of the consumer population can be classified as privacy fundamentalists. These privacy fundamentalists are extremely concerned about any use of their data and generally unwilling to provide their data to Web sites, even

when privacy protection measures were in place (Awad & Krishman, 2006). However, not all end user's express the same level of privacy concern. Cullen (2009) researched online users' privacy concerns and found a "… possible relationship between an individual's level of concern and their perception of their vulnerability in the online environment (Dinev & Hart, 2004). Support this finding, Cullen (2009) presented research by Hu & Dinev (2005) suggesting that "…people do not understand the real implications of privacy and security in the Internet age, and since they are oblivious to the issues, they are currently unable to address the problem" (Hu & Dinev, 2005).

Complicating matters, corporations constantly introduce unknown user privacy threats by deploying tools trying to streamline efficiency and data collection, along with practices attempting to capture enhanced data analysis resulting in user data exploitation and abuse. The development of "… data analysis techniques have created powerful tools for handling consumer information, but such practices present a possible threat to consumer's privacy" (Schwaig et al., 2005). Since there are no governmental regulations enforcing corporate (organization) privacy protection measures safeguarding user PII and securing the exchange of electronic information, users are hesitant about releasing private information online when interacting with corporations. In their research, Smith et al. (1996) examined individual concerns about the privacy practices of organizations and identified four (4) major areas of concern among individuals about their private information: *i*) improper access, (*ii*) unauthorized secondary use, (*iii*) errors, and (*iv*) collection (Smith et al., 1996).

In attempting to reaffirm a commitment to protecting user privacy, variations of software tools have been developed to help protect user's privacy and reduce data

integrity violations. These software tools include items such as website seals indicating valid security credentials, lock icons assuring a secure connection, and installation of secure protocols. Schwaig et al. (2005) noted another way of addressing privacy concerns involving the use of Information Technology (e.g., using the *Platform for Privacy Preferences* (P3P), where consumers submit their privacy preferences to their browser, which checks the privacy practices of the site to determine whether or not they are consistent with the consumer's preferences.

Research conducted to better understand the existence of financial relationships between privacy and stock market value has been minimal. Security threats attract more media attention and as a result draws more research funding and academic interest. As a byproduct, when compared to Information Security (InfoSec) research, privacy research overall has suffered. More specifically, from a total volume of one hundred and twenty-three (123) Information System (IS), Information Technology (IT), Information Security (InfoSec), and related event study research literature conducted, forty-seven (47) event studies focused on security breach incidents, while only eight (8) event studies focused on privacy (Appendix C provides detailed information for all event studies referenced).

Research analysis of the extant event study body of literature discovered during the literature review provided both expected research findings (i.e. corporations losing money when they expose user PII), as well as unexpected research findings. Specifically, more effort needs to be made educating consumers on the importance of preserving their individual privacy, as well as demanding privacy protection from corporations in possession of their PII. It would also be beneficial in teaching consumers how 1) they are contributing to the erosion of individual privacy, 2) their actions are having a *minimal*

impact encouraging corporate investments in privacy, and 3) how the manner in which they (as individuals) can combat eroding privacy protections by changing their perspective on their individual privacy and PII. For example, Yayla & Hu (2010) noted that "…while breach announcements did have a stock market impact for corporate announcements in the early years of their examination, the overall stock market impact was the *greatest*, however, when the results from the early years … were compared to the later years also investigated during the same research study." This indicates that consumers are becoming more accustomed and amenable to the continual data breach incidents causing losses and exposure risk to PII. Protecting CIA of users PII was a major information privacy concern years ago, research has unfortunately shown this is no longer the case. As Cate noted, the unfortunate reality is that data breaches are becoming the norm, and as "…news of privacy invasions and data breaches become more and more common" (Cate, 2005), loss of privacy protection and individual PII abuse becomes more rampant and acceptable.

The frequency, duration, and users affected from data breach incidents has increased over the past two decades. Successfully deployed data breach events impact the corporation both monetarily and through loss of consumer / employee confidence. Additionally, depending on the manner of the breach and the data exposed during the breach, some incidents possess the potential to garner governmental attention (i.e., as is occurring now with Facebook due to their repeated lack of privacy protection for member data they possess) or introduce forced compliance initiatives (i.e., HIPAA, SOX, GLBA).

As consumers continue to exercise frugality during execution of their daily personal conduct, corporation's need to design more intricate and creative ways to give

"free services" to users while still maintaining profitability for shareholders, without the price being the exchange of consumer PII. Data breach and privacy violation incidents abusing consumer PII are now forced into acceptance by unhappy users due to the frequency and nature of the incidents continuing to occur with an ever-increasing veracity (Berghel, 2017; Culnan & Williams, 2009). As the acceptance of these data breach incidents becomes more palatable to end users, and the breach events are seen as less and less a threat by end users, corporations offer to exchange *some* PII for an identified financial incentive; usually the user is able to get a discount or get the item for a sale price in exchange for access to their PII. This is perceived as an "acceptable" trade off by both the consumers and the corporation (Dinev & Hart, 2006); the user gets a better deal financially and the corporation gets the user's PII for use, advertising, future sale, etc. As stated, this phenomenon, known as the "privacy paradox," indicates the point in time at which a consumer is willing to exchange their PII, and identifies at what cost is the minimal exchange point the consumer is willing to offer their individual PII; known as the *Privacy Calculus Model* (PCM) (Dinev & Hart, 2006; Mohammed et al., 2017).

Acquisti et al. (2006) conducted an event study to ascertain whether there was any financial cost to privacy breaches using Event Study Methodology (ESM). Their research examined corporate press release news announcement presenting details regarding a privacy breach incident and discovered a negative stock market impact on the corporation's stock market value. Nicholas-Donald et al. (2011) conducted an empirical investigation of privacy breach announcements on the stock market value of exploited corporations. Not shockingly, corporations that had a privacy breach incident were penalized by shareholders and experienced a loss in stock market value. Similar to

research conducted by Nicholas-Donald et al. (2011), Hinz et al. (2014) explored stock market impact from privacy and security breach violations. Results obtained by Hinz et al. (2014) identified corporations were penalized for both privacy and security breach incidents while receiving a negative loss in stock market value.

2.4 Corporate Privacy

Looking into the role that organizational control has through employee actions with relevancy to individual consumer privacy concerns, Culnan & Armstrong (1999) investigated how organizations can collect information they need to create consumer marketing profiles for advertising to clients but doing so without jeopardizing existing relationships with clients. Research found consumers less likely to be off put by the necessary data collection practices when organization explicitly told consumers what fairness procedures, in the form of Fair Information Practices (FIPs), are observed by the company during the data collection process. This observation extended to corporate employees as well. While Smith et al. (1996) and Stewart & Segars (2002) investigated privacy concerns from individual consumers' perspective, analysis and "…perceptions of organizational privacy policies and practices may be related to levels of employee concern" (Smith et al., 1995).

Culnan & Armstrong (1999) was the first (1st) empirical study to demonstrate that observing FIPs is in the best interest of the organization for building trust with clients through fairness. Wishing to explore further the work of Culnan & Armstrong (1999) that showcased the accepted exchange of information by consumers with organizations when obtaining equitable incentive, Awad & Krishnan (2006) investigated the

willingness of consumers to share PII with an organization in exchange for online personalization or advertising services.

Research findings discovered by Awad & Krishnan (2006) presented a paradox. Individual consumers who value information transparency features are also less likely to participate in personalized online offerings (Awad & Krishnan, 2006), indicating the presence of "privacy fundamentalists" (Westin, 1991) who are unwilling to participate in online personalization regardless of the robustness of privacy protection measures implemented by the organization. On the other hand, consumers willing to participate in online personalization displayed an accepted personal agreement with themselves that the benefit value they received, in the form of personalized online services provided to them, outweighed the potential risk of a privacy invasion (Awad & Krishnan, 2006).

2.4.1 Corporate Threats to Privacy – Information System (IS) / Information Technology Data Breaches, Threats, Intrusions, and Financial Consequences

(i) Individual User Privacy Concerns and Corporate Behavior

Extending the viewpoint that organizations need individuals' Personal Identifiable Information (PII) to individualize user experience and provide targeted marketing, Chen & Rea (2004) investigated organizations employing this data collection tactic, and the control measures employed by users to protect their data. User concerns evolve from unauthorized collection of their PII by organizations that leads to consumer mistrust of the organization and drives individual behavior to be executed to prevent the unauthorized data collection from occurring. The research revealed that individual users are heavily concerned with an ability to control their private information and with its relationship with the two types of privacy concerns: unauthorized secondary use and concerns about giving out private information (Chen & Rea, 2004). Extending research

relating to consumers lack-of confidence in information privacy measures enacted by organizations when conducting e-commerce transactions to protect their data, Malhorta et al. (2004) investigated three distinct issues leading to privacy concerns among individuals within e-commerce. Malhotra et al. (2004) propose a theoretical framework on the dimensionality of *Internet Users' Information Privacy Concerns* (IUIPC).

Research by Dinev & Hart (2006), Lee et al. (2011), and Pavlou et al. (2007) examined concerns that individual consumers have regarding how their PII is accessed, used, stored, managed, granted access too, allowed third part use of, and permitted access to in an online manner. While research by Cullen (2009), Culnan & Williams (2009), Lin & Wu (2008), Liu & Arnett (2002), Milberg et al. (2000),), Schwaig et al. (2006), and Smith et al. (1996) investigated the manner in which government entities (federal, state, local), state and locally owned service companies, corporations, businesses, and foreign nations access, use, store, manage, grant access too, allow third part use of, and permit access to individual consumers PII. Lastly, Hsu (2006) and Moores (2005) investigated consumer concerns regarding how their PIA is accessed, used, stored, managed, granted access too, allowed third part use of, and permitted access to during interaction with e-commerce business entities online.

(*ii*) *Corporate Compliance – Government and Industrial Mandate*

Due to a lack of governmental / industry privacy compliance mandates forcing the public announcement of all privacy exposure incidents, the only time this news reaches end user clients and the general public is when research into the matter is conducted. Culnan & Williams (2009) examined the ChoicePoint privacy breach incident involving TJX, from an ethics perspective, in order to provide better corporate privacy compliance

initiatives moving forward in the future. Despite the massive privacy breach, results from their research examining the incident found no corporate financial impact observed.

Research by Schwaig et al. (2006) identified no stock market impact while they investigated the manner in which Fortune 500 companies were complying with *Federal Trade Commission* (FTC) Fair Information Practices (FIPs) regarding privacy breach incidents and privacy disclosures. Li et al. (2012) also explored FTC FIPs, as well as online privacy policies for thirty *Dow Jones* (DOW) corporations to determine individual level of compliance and financial recourse for non-compliance. A cursory investigation of policies, practices, and initiatives found no identifiable financial compliance incentives. Similar to research by Schwaig et al. (2006), Case & King (2015) conducted an empirical examination of online privacy and security practices for Fortune 500 companies and found no observable corporate stock market impact based on analyzed policies / practices. Khansa et al. (2012) explored corporate stock market impact that non-compliance HIPAA violations had on the guilty corporations within the healthcare industry, as well as financial effect of HIPAA violations in non-healthcare corporations. Research results indicated negative stock market impact from HIPAA non-compliance.

(*iii*) *Corporate Credibility and Information Privacy Threats*

Information threat prevention (data protection) and corporate credibility have been broad areas of interest studied by many researchers due to the potential for enormous corporate financial loss resulting from exposed vulnerabilities (Culnan & Williams, 2009). Potentially more problematic for corporation's impacted by a security breach or privacy intrusion attack is reduced consumer confidence and trust (Bose & Leung, 2014); leading to a loss in revenue and overall consumer satisfaction.

While there are limited avenues of recourse available for consumers who have become disenfranchised by the lackluster protection of their PII by corporations they engage with, competing services offering an alternative may result in the consumer leaving the corporation altogether. An example of this would be a corporation that causes multitude of users to leave the service platform in mass due to a history of repeated data breach events, privacy violations, and continued unauthorized access to user PII. While on the surface this type of passive user reaction may appear as a minor inconvenience, a continued loss of users will equate to loss in advertising revenue and the ability to resell user data to third party data clearing house services.

(*iv*) *Corporate Vulnerability*

Campbell et al. (2003) found negative stock market reaction after corporate Information Security (InfoSec) breaches announcements, while Cavusoglu et al. (2004) identified negative stock market reaction to corporate announcements of Internet security breaches. Cavusoglu et al. (2004) also noted a more severe, negative stock market for larger-sized corporations when compared to smaller-sized corporations, with the most severe, harshest financial impact reserved for Internet-based firms. Aytes et al. (2006) found negative shareholder reaction from corporations exposed to InfoSec breaches when examining intra-industry InfoSec breach incidents. Andoh-Baidoo & Osei-Bryson (2007) examined stock market reaction to corporate announcements of Internet security breach incidents. In their research, a negative reaction in overall corporate stock market value was identified immediately after corporate announcement of the Internet security breach. Goel & Shawky (2009), Kannan et al. (2007), and Yayla & Hu (2010) all found negative stock market reaction from corporate announcements identifying InfoSec breaches.

Addressing a rise in overall security concerns, Chai et al. (2010) and Huang & Behara (2013) utilized an event study to determine potential stock market impact from corporations proactively investing in enhanced security protection mechanisms. In their research, shareholders positively rewarded stock market values for corporations proactively investing in data protection enhancements to better secure internal network infrastructure (Chai et al., 2010; Huang & Behara, 2013).

Malhotra & Malhotra (2010) investigated stock market impact from security breach incidents and found a negative stock market impact for the affected corporation. Gatzlaff & McCullough (2010) investigated data breach incidents as well. However, in their research, Gatzlaff & McCullough (2010) assessed stock market value impact when the breached data incident included both customer *and* employee data. Results indicated a corporate loss in stock market value as soon as the breach incident was identified. Morse et al. (2011) identified a negative stock market reaction for data breach events involving compromised computer security, while both Cardenas et al. (2012) and Hovav et al. (2014) discovered a loss of corporate stock market value when examining security breach incidents. Conversely, while also examining security breach events, Gwebu et al. (2014) did not find any discernible impact to corporate stock market value of the affected corporation. Andoh-Baidoh & Osei-Bryson (2013) examined the financial impact from Internet security breaches using *Deterrence Theory* (DT) and identified a financial loss in corporate stock market value for corporations experiencing a data breach incident.

Hinz et al. (2014) discovered that corporations victimized by a data theft event were financially punished by shareholders through corporate loss in their stock market value. Arcuri et al. (2014) examined InfoSec breach incidents, cyber-crime, and cyber-

attacks and discovered that corporations affected by a breach event causing illegal or unauthorized access to private data (or PII) received a loss corporate stock market value and an overall negative financial impact on the corporation. Hovav et al. (2017) explored financial implications of a cyber-attack, security breach, or privacy violation for potential stock market impact but in South Korea. Like in the United States (U.S.), Hovav et al. (2017) identified both a negative shareholder reaction and reduced corporate stock market value penalization from shareholders.

Berghel (2017) examined the Equifax and Experian credit reporting agency data breach events and surprisingly discovered no overall, long-term financial impact delivered to either corporation, despite initial negative shareholder reaction and imposed government fines. Even more incredulous, however, there often exists the possibility that affected corporations will actually be better off financially (long-term) as a direct result of the security breach incident endured (Amerding, 2018; Aytes et al., 2006; Chai et al., 2010; Culnan & Williams, 2009; Goel & Shawky, 2009; Huang & Behara, 2013).

Based on the potential magnitude of loss from a successful hacker attack, research academics investigated incidents of this nature independently to determine any financial impact to affected corporations. In their research, Ettredge & Richardson (2003) identified positive stock market reaction when they investigated corporate stock market impact from the announcement of the corporation being hacked; specifically, Internet Security-based corporations. Patel (2010) found no stock market impact for corporations when making a press release announcing themselves as the victim of a hacking incident. In an interesting study, Chen et al. (2011) found positive stock market impact for IT consulting firms whose clients were victimized by a security breach incident. It was

posited that corporation should theoretically be penalized for bad service; however, breached corporation's will need upgraded services while corporations not breached will need to preemptively enhance their security so as to *not* become a breach victim.

One area of continual exposure for corporation's is software threats. Illegal access to corporate networks via software vulnerability is an example of an invasion of privacy and can lead to compromised data or information theft. This threat vector can be exploited by attackers in a variety of ways, with the end result being exposed unauthorized access to protected data, breach of consumer PII, potential theft of corporate trade secrets and confidential documents, and ultimately a loss of consumer and shareholder trust. Researchers have investigated software threats to corporations using event study methodology in areas including software vulnerabilities, virus attacks, etc., to determine if corporations are financially impacted from information breach incidents.

Hovav & D'Arcy (2003) found no stock market reaction from announcements detailing *Denial of Service* (DOS) and *Distributed Denial of Service* (DDOS) attacks against the corporation. Garg et al. (2003) found negative corporate stock market reaction when investigating non-virus InfoSec breaches. In their research, Garg et al. (2003) identified that shareholders punished the corporation as a result of the InfoSec breach, leading to a loss in corporate stock market value. Research by Telang & Wattal (2007) also found negative stock market reaction from announcement events identifying software vulnerabilities within the corporation.

Virus attack announcements have been investigated by researchers as an independent form of Information Security (InfoSec) and Security breach incident. Virus attacks are unique in their execution and typically designed to initiate an action rather

than focusing on data theft or Personal Identifiable Information (PII) exploitation. In their research, Hovav & D'Arcy (2004) investigated 224 press release announcements identifying a corporate virus attack or intrusion event within a corporate network environment, but were not able to identify any discernible difference in corporate stock market price, nor identify any financial impact stemming from the corporate press release announcement announcing the virus incident or intrusion event. In later research, Hovav & D'Arcy (2005) investigated stock market impact from corporate announcements identifying defective IT products based on software issues. Their results identified negative corporate stock market reaction, but only when the defective product announced contained a computer virus.

Anthony et al. (2006) found negative stock market reaction from announcements identifying website outages from software vulnerabilities for corporations associated with online sales and business. Bose & Leung (2014) explored financial implications of phishing alerts and discovered that shareholders perceive phishing alerts as a corporate threat penalized all corporations impacted through a loss in stock market value.

2.5 Event Study Literature Review

Researchers conducting event studies using Event Study Methodology (ESM) are able to examine potential financial impact that an unexpected event has on the financial performance of a corporation's stock market value. From the literature review, event study research was originally conducted in non-technological domains (i.e. *Accounting and Finance* (MacKinlay, 1997), *Healthcare and Hospitality* (Kim et al., 2009), *Airline Industry* (Song et al., 2007) etc., using Event Study Methodology (ESM), to evaluate financial impact to corporate stock market value based on shareholder reaction to press

release announcement events identifying corporate investments. The success of this event study research enabled ESM to quickly gain traction within the IS/IT research communities as an effective tool to measure financial stock market impact based on corporate investments in IS/IT; beginning with Dos Santos et al. (1993).

MacKinlay (1997) investigated the fields of economics and finance to determine if the use of ESM was a proper tool that could be trusted for accuracy. Dehning et al. (2003) reviewed event studies in MIS that were conducted using the EMS to better understand the applicability of firm value as a valid statistical measure for changes in corporate financial wealth. Hovav et al. (2007) examined stock market breach incidents and research papers using the ESM and developed a classification scheme based on the financial impact to the corporation's overall stock market value. Roztocki & Weistroffer (2008) created an initial literature review of event study literature; Roztocki & Weistroffer (2009) then updated the original list in their 2009 updated literature review that included additional event study research that had been conducted since 2008. Zhang & Huang (2009) also conducted a literature review of ESM papers that identified changes in corporate stock market value from corporate press release announcement events.

Roztocki & Weistroffer (2011) used their previous literature review research works from 2008, and 2009 to present a new, more cohesive and inclusive event study literature review. Their 2011 research showcased past ESM research conducted, then extrapolated present-day event study research to indicate likely research avenues in the future when using ESM. Like the other literature reviews, Spanos & Angelos (2016) also conducted their own literature review of event study literature but focused on InfoSec breach incidents and the stock market impact they cause to affected corporations.

2.5.1 General and Specific IS/IT Investments

While there has been minimal information privacy or privacy event studies conducted using *Event Study Methodology* (ESM) investigating the economic impact of corporate investment in privacy, there have been extensive event studies conducted relating to corporate investments in IS/IT, including research areas in: **General IS/IT Investments (within the United States)** (Chatterjee et al., 2001; Dehning et al., 2003; Dos Santos et al., 1993; Hunter, 2003; Im et al., 2001; Oh et al., 2006; Roztocki & Weistroffer, 2006, 2007, 2009, 2009a); **General IS/IT Investments (outside of the United States)** (Kim et al., 2009; Meng & Lee, 2007; Nagm & Kautz, 2008).

Successful results from event studies in other domains, and an increase in usability of the ESM across industry domains led to expanded use into more focused areas of research interest, including specific corporate IS/IT investments and corporate investments in IS/IT-related domains. Event studies have been conducted using Event Study Methodology (ESM) in investigating economic impact of **Specific IS/IT Investments**, including: **E-Commerce** (Chen & Siems, 2001; Cheng et al., 2007; Dardan et al., 2005; Dehning et al., 2004; Dewan & Ren, 2007; Ferguson et al., 2006; Jeong & Lu, 2008; Jeong & Stylianou, 2010; Khansa & Liginlal, 2009; Lee et al., 2002; Misra & Rao, 2009; Subramani & Walden, 2001; Walden & Browne, 2008).

2.5.2 Other IS/IT and IS/IT Related Investments

Event studies have also been conducted using ESM investigating financial impact from corporate investments in IS/IT-related domains (not hardware or software based) including: **Knowledge Management Initiatives (KMI)** (Chavez & Lorenzo, 2006; Choi & Jong, 2010; Dardan et al., 2006; Filbeck et al., 2005; Mitra & Singhal, 2008;

Sabherwal & Sabherwal, 2005; Yang & Klassen, 2008); **Enterprise Resource Planning (ERP) Initiatives** (Benco & Prather, 2008; Hayes et al., 2001; Ranganathan & Brown, 2006; Roztocki & Weistroffer, 2007, 2008, 2009); **IS/IT Outsourcing Initiatives** (Agrawal et al., 2006; Daniel et al., 2009; Duan et al., 2009; Florin et al., 2005; Gewald & Gellrich, 2007; Hayes et al., 2000; Oh et al., 2006; Peak et al., 2002); **Human Capitol (IS/IT-Related Hiring)** (Chatterjee et al., 2001; Guan et al., 2006; Khallaf & Skantz, 2007; Lubatkin et al., 1989); **Legal** (Goel et al., 2010; Raghu et al., 2008); **Mergers & Acquisitions (M&A)** (Canace & Mann, 2014; Koh & Venkatraman, 1991; Lee & Lin, 2006; Uhlenbruck et al., 2006); **Website / Internet** (Benbunan-Fich & Fich, 2004; Geyskens et al., 2002); **IS/IT Other Corporate Investment Announcements** (Hendricks & Singhal, 1996, 1997; Pardue et al., 2000; Song et al., 2007).

2.6 Summary

Evidence exists in the extant body of event study literature indicating the potential for increased corporate wealth, through increased overall corporate stock market value, from strategic corporate investments. Successful Event Study (ES) research implementing Event Study Methodology (ESM) has been conducted throughout a variety of research domains. Indications of a successful event study include the presence of positive financial rewards by corporate shareholders reacting to press release announcement events showcasing specified corporate investments; positive financial rewards by shareholders lead to increased stock market value.

Event Study (ES) success has been demonstrated in Administrative (Accounting, Finance, Business, Healthcare) – (Case & King, 2015; Huang & Behara, 2013; Khansa et al., 2012MacKinlay, 1997; Schwaig et al., 2006), Technology (and Related) –

(Dos Santos et al., 1993; Hayes et al., 2001), and Data Protection (i.e., Privacy, Security, Breach) – (Campbell, 2003; Goel & Shawky, 2009) research domains. However only minimal event study research interest has been shown towards "*Privacy*."

In direct contrast to other domains where Event Study (ES) research has been repeatedly used with reoccurring success, there has been only minimal event study research interest in: 1) better understanding corporate investments in privacy, 2) exploring potential financial implications associated with corporate investments in privacy, and 3) identifying potential financial incentives encouraging corporate investments in privacy.

The objective of this research was examining corporate investments in privacy to better understand the potential financial implications associated with corporate investments in privacy, and to determine potential financial implications to overall corporate stock market value from corporate investments in privacy. Based on an extensive review of relevant extant event study research literature, a better understanding of this phenomenon is needed to both empirically quantify the potential financial impact from corporate investments in privacy, as well as help corporations identify financial incentives encouraging corporate investments in privacy.

Executing in this manner, this research examination makes an academic contribution to the extant body of event study and privacy literature by providing a better understanding of corporate investments in privacy, identifying financial implications to overall corporate stock market value from corporate investments in privacy, presenting economic incentives associated with corporate investments in privacy, and providing a better understanding of *why corporations are not investing in privacy*.

Chapter 3

Methodology

3.1 Introduction

Academics within Information System (IS), Information Technology (IT), Information Security (InfoSec), and related research domains have been interested in better understanding financial implications from specific corporate investments. For example, corporate investments in *IT Outsourcing* (Agrawal et al., 2006), *Enterprise Resource Planning* (ERP) (Roztocki & Weistroffer, 2009), *Supply Chain Management* (SCM) (Mitra & Singhal, 2008), and *e-Commerce* (Walden & Browne, 2008) have all provided increased corporate wealth through increased overall stock market value. Identification of technology and services possessing the ability to provide enhanced positive wealth through increased overall stock market value is the impetus driving corporate investment research and the potential financial implications from these corporate investments. Alarmingly, however, minimal research interest has been shown regarding financial implications from corporate investments in *privacy* (Acquisti et al., 2006; Khansa et al., 2012; Malhotra & Malhotra, 2010; Nicholas-Donald et al., 2011), nor ways to measure resultant financial loss from inadequate corporate investments in privacy safeguarding against exploitation of user privacy (Acquisti et al., 2006; Culnan & Williams, 2009; Dinev & Hart, 2006).

Nevertheless, the veracity of recent attacks focused directly on *Privacy*, targeting both the "Confidentiality, Integrity, and Availability" (CIA) of corporate data and individual client "Personal Identifiable Information" (PII), has demanded a more refined

analysis tool be created to better determine the financial impact resulting from privacy breach incidents. Based on the minimal amount of identifiable research examining corporate investments in privacy, additional data is needed. A better understanding of corporate investments in privacy will provide corporations an additional reference when deciding on future corporate investments in privacy by presenting a more accurate representation of the financial implications associated with corporate investments in privacy, as well as identifying the financial impact to overall corporate stock market value from corporate investments in privacy. This will allow corporate decision makers to extrapolate potential financial ramifications when making investment decisions and assist in identifying the best course of action for investment asset dispersion.

3.2 Research Design

Through various research domains, event study research using Event Study Methodology (ESM) has been identified as a useful instrument when determining financial impact of an identified event announcement; for example: Information System (IS), Information Technology (IT), Information Security (InfoSec), and Computer Security (ComSec). As "McWilliams and Siegel have pointed out… the event study methodology has the advantage of capturing the relationship between event and market reactions" (Khansa et al., 2012). Furthermore, use of ESM is the most applicable tool available for academics and practitioners attempting to ascertain the totality of financial devastation caused by a breach incident, including both tangible and intangible affects typically not able to be measured when not using event study methodology.

In this event study research, Event Study Methodology (ESM) was used during data testing and analysis. In addition to the extant body of event study literature and

associated prior research, academic contributions, research results, and findings from previous event study literature provided a valuable source of reference for this study. In addition, using event study as the research method facilitated the deployment of ESM in examining corporate investments in *P*rivacy, while in parallel identifying financial impact to overall corporate stock market value from corporate investments in *Privacy*.

3.2.1 Efficient Market Hypothesis (EMH)

In his research, Sharpe (1963) introduced and discussed application of the "*Markowitz Model*" (MM) for use in financial portfolio analysis. He also lays down the basis for the future development of Efficient Market Hypothesis (EMH). Fama et al. (1969) explores how corporate stock market prices stay in a variable stay of movement when introduced to any new information; effectively identifying the EMH. This helped pave the way for the accepted assumptions that are built into the EMH. Fama (1970) presents an extensive review of "Efficient Capital Markets" and further introduces the theory and empirical work that supports the EMH. His seminal work is the foundation for all future use of Event Study Methodology (ESM). Brown & Warner (1985) examined the usability of ESM while investigating and computing daily stock returns for researched corporations. McWilliams & Siegel (1997) also explored the manner in which academics using the ESM in management research were paying attention to the theoretical and research design issues and addressed any identifiable concerns when using ESM and EMH in future research endeavors.

Fama (1991) explored in great detail capital markets to determine an effective manner that ESM could be deployed to analyze financial market data. Malkiel (2003) is credited with the creation of "*Random Walk Theory*" (RWT) and discusses the utility of

using RWT when working with financial markets and financial data. RWT was used in part as the basis for ESM. In this literature, he reviews the EMH and addresses critics of the EMH. Sewell (2011) explores in great detail the history of the EMH and provides an exhaustive timeline of the development, creation, and relevant literature relating to EMH.

3.3 Research Method and Research Design

3.3.1 Event Study Methodology – History and Background

Event Study Methodology (ESM) has been utilized in the past by researchers when attempting to observe financial impact from an identified announcement event. In an event study, the objective is to examine the stock market's response to events that are often related to the release of information to the stock market (Im et al., 2001). Historical Event Study (ES) research has been conducted throughout a variety of domains and highlights the ability for corporations to increase corporate wealth through gains in stock market value, both in the United States (U.S.) (Chatterjee et al., 2002; Hayes et al., 2001; Im et al., 2001; Ranganathan & Brown, 2006; Sabherwal & Sabherwal, 2007), and abroad (Cheng et al., 2007; Hovav et al., 2017).

It was necessary during the literature review to identify, understand, and catalog all previously conducted Information System (IS) / Information Technology (IT) and related event study research. This process allowed the identification of an existing gap in the extant body of information privacy event study research literature, while simultaneously ensuring that the proposed goal of this research, examining corporate investments in privacy, would make an academic contribution. Identifying and classifying previous IS/IT event study literature highlighted the observable research gap in event study literature; minimal amount of research interest in examining financial

impact from corporate investments in privacy. Moreover, visualizing the volume and varying domain distribution of previous event study literature into identifiable categories proved evident that additional event study research was necessary. This research helps to better understand the financial impact of privacy as an individual construct, as well as provides corporations with information relating to the financial impact from that corporate investments in privacy have on overall corporate stock market value.

Categorical classification of previous event study literature was important in this research. Analysis of the literature highlighted an increase in overall corporate stock market value associated with corporate investments across a multitude of research domains, while providing supporting data indicating positive financial incentives encouraging additional corporate investments in hardware, software, and services. However, the literature also indicated a reluctance of research interest examining corporate investments in privacy. Furthermore, little evidentiary data exists supporting a position of reduced research interest in better understanding corporate investments in privacy, the financial impact from corporate investments in privacy, or potential financial ramifications to overall stock market value from corporate investments in privacy.

During the literature review, approximately one hundred and twenty-three (123) papers were identified and categorized: Privacy (Information Privacy), Information System (IS), Information Technology (IT), Information Security (InfoSec), and Event Study-Related. Literature was categorized in one of six (6) areas: *IS/IT Investments* (47); *IS/IT Privacy – Breaches, Corporate Initiatives, Compliance, and Violations* (8); *IS/IT Security Breach and Corporate Trustworthiness* (28); *IS/IT Outsourcing Initiatives* (8);

IS/IT Announcement Events (Other) (16); *Event Study History and Background* (16).

(Appendix A provides full details for all event study research and literature referenced).

* During literature review, sixteen (16) papers identified as relevant to the history, background, or initial development and use of "Event Study" research and "Event Study Methodology" (ESM) were categorized as "Event Study History and Background." These research findings are historical in context to Event Study research and ESM and helped expand the applicability and use of ESM to mainstream research use seen today. Literature presented in this category are universally accepted as seminal research in Event Study research domains and designated as requisite reading for any Event Study research. In addition, event study literature review papers completed identifying Information System (IS) / Information Technology (IT) and associated event study research have been a valuable resource to both the extant body of event study literature and in completion of this research proposal. The applicability of Event Study and ESM for replication across a variety of research domains highlights both the power of ESM as a research tool, and the practicality of using ESM when examining corporate investments in privacy.

3.3.2 Event Study – Research Design and Implementation

Event Study Methodology (ESM) is based on the Efficient Market Hypothesis (EMH) developed by Fama at el. (1969) and has been successfully used in a multitude of research domains highlighting the financial impact of the designated event being investigated. "According to this hypothesis, financial markets process publicly available information to assess current firm performance and to adjust expectations of future achievements" (Benbunan-Fich & Fich, 2004).

To achieve the stated objective of this research, examining corporate investments in privacy to determine potential financial impact to overall corporate stock market value based on the corporate investments in privacy, the research design implemented was based on Event Study Methodology (ESM). The research design and model used in this research were utilized in a similar manner as researchers in prior event studies; identified in the extant literature during literature review. Using ESM allows "researchers to

determine the nature of the stock market's reaction to strategic moves" (Chatterjee et al., 2002) made by the corporation.

Throughout multiple research domains, including business, finance, and economics, ESM has been utilized to measure potential financial impact that a designated event had on a corporation's overall stock market value. The event study "…examines the stock market reaction to the public announcement of a particular event" (Hovav & D'Arcy, 2014). Furthermore, according to Khansa et al. (2012), "…an event is said to have an impact on the financial performance of a firm if it produces a significant abnormal movement in the price of the firm's stock (Polinsky & Shavell, 2007; Teoh et al., 1999)." When employing the semi-strong form of the efficient market hypothesis (EMH), the market price of a firm fully reflects all publicly available information (Fama et al., 1969). In addition, ESM as a research instrument has "a strong theoretical foundation and it is widely used in the accounting, finance, and management research disciplines" (McWilliams & Siegel, 1997). Recently, IS, IT, ComSec, and InfoSec have begun using ESM in examining financial impact from corporate investments in IS and IT.

Dos Santos et al. (1993) first used an event study in examining stock market impact of IT investments. The success of this seminal event study research by Dos Santos et al. (1993) influenced the expansion of ESM into a variety of additional IS and IT research streams. Following Dos Santos et al. (1993), event study research explored financial impact on stock market value from corporate investment events in varying areas of IS and IT interest, including: InfoSec Breach (Ettredge & Richardson, 2003; Hovav & D'Arcy, 2003), IT Outsourcing (Hayes et al., 2000; Oh et al., 2006), and E-Commerce Investments (Dehning et al., 2004; Subramani & Walden, 2001). Utilizing an event study

to examine potential financial impact on a corporation's stock market price from corporate investment announcement events has historically been the traditional implementation within prior event study research, both within and outside IS / IT.

ESM is the research framework used to empirically quantify an identifiable and observable change in a corporation's stock market value when an unknown variable is introduced (corporate investment announcement) to shareholders. Using ESM, corporate stock market price is the dependent variable when determining stock market impact from an announcement event on corporate stock market value due to: 1) (*i*) all publicly available information is incorporated into the corporation's stock market price, (*ii*) stock market price is set by the corporation's shareholder's, assuming an efficient market model, and (*iii*) based on the EMH theory developed by Fama et al. (1969), and 2) specific event and estimation windows sizes surrounding the event of interest can be used during research design based on specific research goals.

ESM assumes the stock market is an efficient market, and as such, any newly announced events will have an observable impact on stock market value of the associated corporation; identifiable positive or negative market impact will be based on perceived value assigned to the announcement event by the corporation's shareholders. As noted by Fama et al. (1993) "we can measure the market's assessment of the expected impact of IT investments on total firm value by examining stock price reactions around announcements of IT investments." Utilization of ESM provides the best mechanism to complete identified research objectives; exploring corporate investments in privacy to identify financial impact to stock market value from corporate investments in privacy.

Completion of event study analysis "… consists of four stages: pre-defining the event and announcement day(s); measuring the actual stock's return during the announcement period; estimating expected return of the stock during announcement period in the absence of the event… and computing abnormal return while measuring its statistical significance" (Khansa et al., 2012). Successful data analysis was achieved upon completion of the five (5) main steps identified in Figure 2. The five (5) steps identified have been adopted from research conducted by Campbell et al. (2003), and together make up essential guidelines required for any successful ESM research.

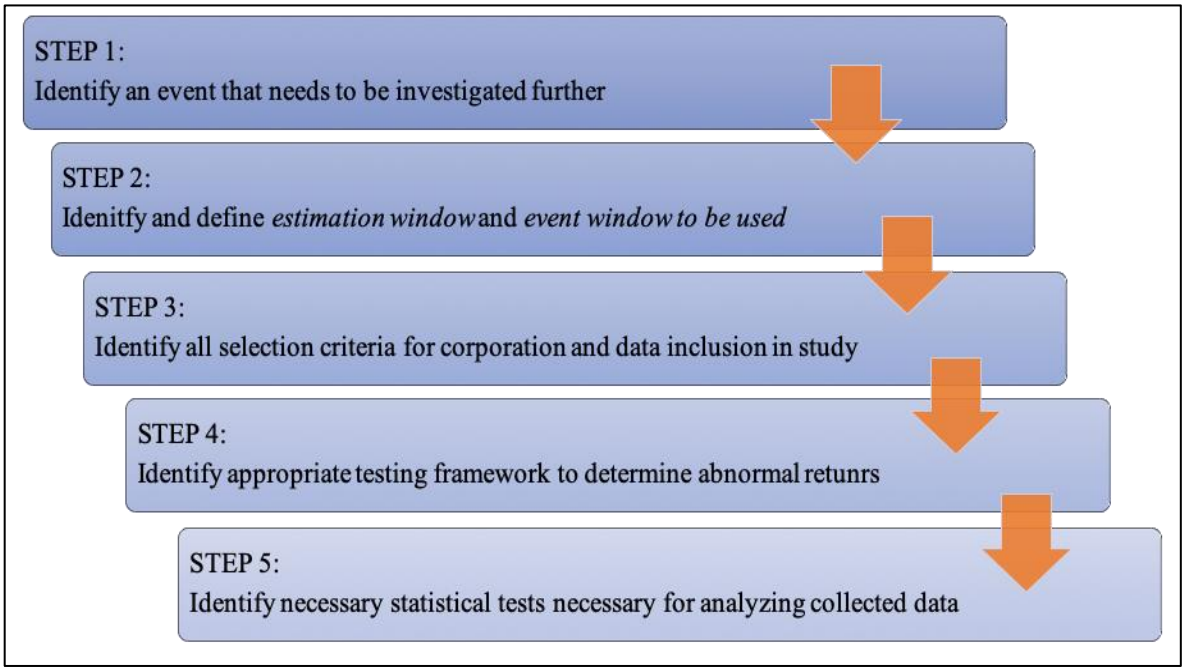


Figure 2 – Hierarchical Steps of Event Study Methodology Research Analysis

Event study research requires the calculation of the expected return for each identified corporation's stock market value; absent the event being investigated. Based on ESM literature review, there exist three (3) different return methods available to compute a corporation's *AR*s when conducting an event study using ESM: 1) *Mean Adjusted*, 2) *Market Adjusted*, and 3) *Market Model* (MM). The most commonly used

procedure for calculating abnormal returns is the market model, which controls for the historical relationship between the abnormal returns of a firm with the abnormal returns to an index (Agrawal et al., 2006). As noted, the MM "…assumes a stable linear relation between the market return and the return on the stock" (Acquisti et al., 2006).

When using MM, coefficients of the linear model are derived using calculations and sample data extracted from the determined estimation window used. When using the MM, estimations for the *alpha* (MM intercept), *beta* (MM slope), and *residual standard deviation* (MM root mean squared error) coefficients are all estimated based on the selected estimation window. A firm's expected return and the market model parameters are estimated from common stock returns (Benbunan-Fich & Fich, 2004) and will be identified through the University of Chicago's "*Center for Research in Security Prices"* (CRSP) and COMPUSTAT. The CRSP provides detailed daily data on stock prices of all publicly traded firms in the US (Agrawal et al., 2006), known as the "Daily Combined Return File," for each identified corporation. All corporations identified with qualified privacy investment announcement events and possessing all requisite corporate data necessary for inclusion within this research had all requisite financial calculations completed using information from CRSP, COMPUSTAT, and associated MM data.

An initial estimation window must first be determined when beginning an ESM. The *estimation window* is the "…length of time prior to the event over which the market model will be estimated" (Benbunan-Fich & Fich, 2004). In addition, an *event window* is also needed. The event window identifies the days *before* and *after* the investment announcement event being investigated. It is advised against using longer event windows as the potential for confounding events increases. As noted by McWilliams & Siegel

(1997), the longer the window, the greater the likelihood that other news items in addition to the event under study may affect the returns.

Corporate stock return values computed from the MM used the appropriate equally weighted *New York Stock Exchange* (NYSE), *American Stock Exchange* (AMEX), and or the *National Association of Securities Dealers Automated Quotations* (NASDAQ) stock market indexes. Coefficients for the linear regression market model, "intercept" ($\boldsymbol{\alpha_i}$) and "slope" ($\boldsymbol{\beta_i}$), were based on a sample of data taken from the estimation window used. In this research study, the estimation window used, relative to the press release announcement date, $t = 0$, was 195-Days, beginning at t = - 200-Days and ending at t = -5-Days *before* the announcement event date ($t = 0$). Literature review indicated a two hundred 200-Day (t = -200 Day) estimation window as popular in previous IS/IT ESM studies, including research by Dos Santos et al. (1993) and Im et al. (2001), who both used 200-Day estimation windows. In alignment with previous event study research, MM parameters were estimated from -200-Days to -5-Days *before* the announcement event using linear regression (*Ordinary Least Squares* (OLS).

Stock return data was calculated for each corporate event using formula:

$$R_{it} = \alpha_i + \beta_i R_{mt} + \varepsilon_{it} \qquad \text{(Formula 1)}$$

Formula (1) where:

$\boldsymbol{R_{it}}$	stock market return price for each corporation
$\boldsymbol{i^{th}}$	corporation on day $\boldsymbol{t}$
$\boldsymbol{R_{mt}}$	total market return on day $\boldsymbol{t}$
$\boldsymbol{\alpha_i}$	OLS intercept parameter estimate (based on estimation window)
$\boldsymbol{\beta_i}$	OLS slope parameter estimate of the Market Model for corporation $\boldsymbol{i}$ being investigated within this research (based on estimation window)
$\boldsymbol{\varepsilon_{it}}$	variable used to account for disturbance

Note: $\boldsymbol{\varepsilon_{it}}$ will account for disturbance; random errors for stock i on day t
$\boldsymbol{\alpha_i}$ and $\boldsymbol{\beta_i}$ are firm-dependent coefficients to be estimated in the MM

Applicable usage of EMH theory in an ESM research investigation is based on making and accepting multiple assumptions, including: 1) all publicly available information about a corporation at that precise moment is known to all corporate shareholders, 2) all known public information regarding the corporation is already incorporated / factored into the corporation's real-time, changing, overall stock market price, and 3) any new corporate information released to the general public will be instantaneously analyzed by shareholders to determine the perceived financial value of the newly released information, then immediately reflected into the corporations new, adjusted, overall stock market price. Prior ESM research conducted has indicated that the stock market will react in some capacity with the introduction or public release of any new, unexpected corporate information. As noted by McWilliams & Siegel (1997), "…since the stock price of a firm is supposed to reflect the true value of that firm determined by all relevant public information about the firm at the time, the changes in the stock price due to a specific incident should measure the financial impact of that incident more effectively than measures based on accounting numbers which are subject to manipulation." Depending on the perceived shareholder value of the information announcement, corporate shareholder's actions will dictate the actual realized value of the new information and affect a positive or negative corporate stock market movement.

Prior research has shown new information perceived by corporate shareholders to bring positive (+) value to the corporation will provide an identifiable rise in corporate market price after the information is released. Conversely, previous research has also shown the opposite to be true; corporate shareholders that perceive newly released corporate information as negative (-), or associate the information with the corporation

losing financial value based on the specified new information released, shareholders will intrinsically react negatively while punishing the corporation with an overall lower stock market value position. Using EMH theory, this research investigated the financial impact from corporate investments in privacy. Based on perceived value of the corporate privacy investment by corporate shareholders, the corporation was either be rewarded through positive increase (+) in stock market value, or penalized through negative (-) loss of stock market value, dependent upon specific shareholder reaction.

By analyzing identifiable changes in an associated corporation's financial stock market value, caused by positive (+) or negative (-) shareholder reaction to the corporate privacy investment announcement events, this research provides empirical evidence identifying corporate investments in privacy as either a positive (+) or negative (-) source of increased corporate wealth for the associated corporation. In addition, this research provides corporations an additional tool to use when evaluating the best resource allocation of investment assets relating to privacy and privacy protection.

To evaluate stock market change, daily stock return information is required for each corporation associated with a privacy investment announcement event. Using the EMH, corporate daily stock market returns "… reflect the value of a particular firm more accurately since stock prices are relatively free of insider manipulation and reflect all of the relevant information known about the firm under the EMH" (Fama, 1970). Unlike InfoSec breaches that cause corporations immediate, identifiable, and direct financial losses resulting from the attack, measuring privacy is inherently more complicated.

Literature evidence exists indicating corporations have a financial responsibility to invest in protection mechanisms to prevent InfoSec attacks. Corporations have a

fiduciary responsibility to shareholders in preventing InfoSec breach events from occurring as affected corporations suffering from a breach incident have experienced massive financial losses and lowered corporate stock market value. However, little research has explored the financial implications relating to corporate investments in privacy, privacy protection mechanism, potential financial loss from privacy breach attacks, or any financial incentives existing to motivate corporations to proactively invest in privacy, within the IS / IT domain, or across multiple industry segments. Using the EMH as the theoretical basis for this research investigation, ESM was employed to compute financial data necessary for identifying and better understanding the financial implications from corporate investments in privacy.

Expected Normal Returns (ENR) are stock market returns that a corporation will exhibit in the absence of the corporate investment announcement event being examined. To calculate the impact an event announcement had on a corporation's stock market value, a corporation's stock market *Abnormal Return* (AR) needs to be calculated. As noted, "the abnormal returns, *AR*, represent the extent to which realized returns on the event day deviate from the returns that would be expected…" (Campbell et al., 2003). Calculated *AR*'s are then subtracted from normal, expected returns to realize the empirical, financial impact the identified corporate investment announcement event had on the corporation's stock market value.

In addition to the *AR*, corporation's *Cumulative Abnormal Return* (CAR) was also calculated for each corporation to represent their individual *AR* over the total event window investigated. In this research investigation, corporate *Average Cumulative Abnormal Return* (ACAR), or Mean CAR, was further calculated for each identified

corporation associated with a privacy announcement event. Calculation of *ENR*, *AR*, *CAR*, and *ACAR* was necessary for each corporation being investigated within this research in order to ascertain true financial impact, as well as evaluate the resultant changes to overall corporate stock market value from corporate investments in privacy.

Corporate Stock Market Price

In an ESM, the first step when implementing *EMH* theory was using the relative *Capital Asset Pricing Model* (CAPM)-*based MM* to calculate corporate stock market pricing using one of the three stock market indexes identified for use within this research (NYSE, AMEX, or NASDAQ). Calculation of corporate stock market value was computed for each of the identified corporations at the specific time (date) the corporate investment announcement event was released to the public. Additional corporate data necessary for calculations was obtained from the University of Chicago's CRSP, and COMPUSTAT. This information includes data such as corporate financial information, corporate size, revenue, employee count, etc. In determining corporate daily returns using the MM, the MM is "…estimated for each firm in the sample using 195 daily returns…[using estimation window -200, -5 days] the estimation period starts -200 days before the announcement date and ends -5 days before the announcement date" (Hovav & D'Arcy, 2005). Based on a review of previously conducted event study literature, the formula used to calculate corporations' daily returns was:

$$R_{i,t} = \alpha_i + \beta_i R_{m,t} + \varepsilon_{I,t} \qquad \text{(Formula 1)}$$

Formula (1) where:

$\boldsymbol{R_{it}}$	stock market return price for each corporation
$\boldsymbol{i^{th}}$	corporation on day $\boldsymbol{t}$
$\boldsymbol{R_{mt}}$	total market return on day $\boldsymbol{t}$
$\boldsymbol{\alpha_i}$	OLS intercept parameter estimate (based on estimation window)

$\boldsymbol{\beta_i}$	OLS slope parameter estimate of the Market Model for corporation ***i*** being investigated within this research (based on estimation window)
$\boldsymbol{\varepsilon_{it}}$	variable used to account for disturbance

Note: $\boldsymbol{\varepsilon_{it}}$ will account for disturbance; random errors for stock *i* on day *t*
$\boldsymbol{\alpha_i}$ and $\boldsymbol{\beta_i}$ are firm-dependent coefficients to be estimated in the MM

Expected Normal Return (ENR)

Using the appropriate stock market index provided corporate financial information necessary to determine the overall corporate stock market impact from the investment announcement event. To identify if the corporate privacy event had any financial impact on the market value of the corporation, it was necessary to calculate what the *Expected Normal Return* (ENR) would have been for the corporation absent the press release announcement event being investigated in this research. To calculate corporate ENR, an acceptable *estimation window* must be created, designated, then used.

Abnormal Return (AR)

Once the average daily market price had been determined for each of the identified corporations, the *AR* needed to then be calculated for each corporation as well (using the identified CAPM-based MM). Corporate stock market *AR* is the difference between expected daily stock return price and actualized returned stock market price after the corporate investment announcement event was disclosed. The accepted assumption, according to Hovav & D'Arcy (2005), is that when using ESM, any identifiable and observable AR are the result of the announcement event being investigated (in this research announcement, events indicating corporate investments in privacy), and *not* the result of a random event occurring on the same day (Subramani & Walden, 2001).

Determining *AR* for each corporation during the event window ($t = -1$, $t = 0$, $t = 1$) was computed using formula:

$$AR_{it} = R_{it} - (\alpha_i + \beta_i R_{mt}) \qquad \text{(Formula 2)}$$

Formula (2) where:

$\boldsymbol{AR_{it}}$	abnormal stock market returns (AR) for each corporation ***i*** on day ***t***
$\boldsymbol{\alpha_i}$ and $\boldsymbol{\beta_i}$	estimated OLS intercept parameters (based on estimation window) obtained by regressing R_{it} over R_{mt} over the designated estimation window (-200, -5) prior to the announcement event date (t = 0)

Note: $\boldsymbol{\alpha_i}$ and $\boldsymbol{\beta_i}$ are firm-dependent coefficients to be estimated in the MM

Once stock market prices were estimated for what the corporate stock market price would have been, absent the identified press release announcement event, *AR* was then calculated. Abnormal stock returns were computed by subtracting raw returns around the event date from the market model expected returns (Benbunan-Fich & Fich, 2004). In this manner, if there is a significant, observable difference between the expected stock market return and the actualized stock market return calculated then it can be surmised that the announcement event had an effect on the corporation's stock market value; the "…magnitude of difference provides a quantifiable measure of the impact of the announcement event on firm value" (Benbunan-Fich & Fich, 2004).

Cumulative Abnormal Return (CAR)

After computing *AR* for each identified corporation (*i*) at the time of the investment announcement event date (t = 0), and computing *AR* for each identified corporation (*i*) over the designated event window (t = -1, t = 0, t = 1), the *Cumulative Abnormal Return* (CAR) was then be calculated for each corporation over the designated event window (t = -1, t = 0, t = 1) as well. Using a three (3)–Day event window in this investigation (t = -1, t = 0, t = 1), *CARs* were calculated over days -1, 0, and 1. In this calculation, t = -1 is the day *before* the investment announcement event date; t = 0 is the *actual* investment announcement event date, and t = 1 is the day *after* the investment

announcement event. To compute *CAR*s for each corporation associated with an investment announcement event, during each day of the designated 3-Day event window (t = -1, t = 0, t = 1), the following formula was used:

$$CAR_i = \sum_{t=0}^{-1,1} AR_{it} \qquad \text{(Formula 3)}$$

Formula (3) where:

$\boldsymbol{AR_{it}}$	abnormal stock market returns (AR) for each corporation ***i*** on day ***t***
t (= 0)	identified date of investment announcement event
-1, 1	beginning (t = *-1* ; 1 day *before* identified investment announcement event date) and end date (t = 1; 1 day *after* identified investment announcement event date) during which time ***ARs*** are calculated for each corporation during the investigation

Average Cumulative Abnormal Returns (ACAR)

The *Average Cumulative Abnormal Return* (ACAR), or Mean CAR, was determined for each identified corporation as well. To calculate the *ACAR* for each corporation, the following formula was used:

$$CAR = \frac{1}{N}\sum_{i=1}^{N} CAR_i \qquad \text{(Formula 4)}$$

Formula (4) where:

CARi	determined from *Formula 3* and necessary to calculate ACAR
N	number of corporations identified and being investigated

Estimation Window

The estimation window is identified as the period of time in which average daily market price is calculated for each identified corporation. The estimation window is used to calculate daily stock market pricing using the Market Model (MM) over a specified period of time, *before* the investment announcement event date (-200, -5). This provides estimated daily stock market return prices for each corporation being investigated in this study. Previous event studies have successfully utilized varying estimation windows,

each based on their specific investment announcement event investigated. Following event study research by Dos Santos et al. (1993) and Im et al. (2001), the estimation window used in this research, relative to the announcement event date, $t = 0$, is 195-Days; beginning at $t = -$ 200-Days and ending at $t =$ -5-Days. This estimation window size is consistent with the extant literature of previously conducted using ESM in IS / IT research domains. Using the formula presented, daily average stock market return pricing and MM parameters were calculated for each corporation over the designated estimation window (-200, -5); a period of time *before* the announcement event date, spanning a total timeframe of -200-Days to -5-Days (-200, -5). As noted by Hovav & D'Arcy (2005), a 195-Day estimation period starts -200 days before the announcement date and ends -5 days before the announcement date.

Event Window

The *event window* is identified as the period of time surrounding the investment announcement event date that is used to capture any identifiable stock market reaction to the corporate investment announcement event. The varying of event window sizes used throughout previous event study research has been based on the specific nature of the investment announcement event being examined, as well as specified results desired from the research investigation. For example, some InfoSec breach studies have used a longer event window to evaluate approximately how long a corporation witnessed a financial impact to their stock market value from the InfoSec breach.

Based on a review of previously conducted event study literature, a three (3) day event window was chosen for use as the most appropriate time period for the desired results in this research study. The three-day (3-Day) event window used was identified as

t = -1 (1 day *before* the announcement event date); *t* = 0 (exact, specific announcement event date); and *t* = 1 (1 day *after* the announcement event date). Consistent with the recommended preference of McWilliams & Siegel (1997), a short, three-day (3) event window (-1,0,1) was chosen for use as it provides the avenue necessary to notice an immediate corporate stock market impact based on the investment announcement event while limiting potential data degradation from potential corporate data leak (before event date) and / or confounding data events (after event date). As noted, and in agreeance with, previous IS / IT ESM literature research, examining stock market data the day *before* the announcement date will collect any internally leaked information insiders had access to; while examining stock market data the day *after* the announcement date will capture any stock market impact occurring after-market closure the day the investment announcement event was received by the public.

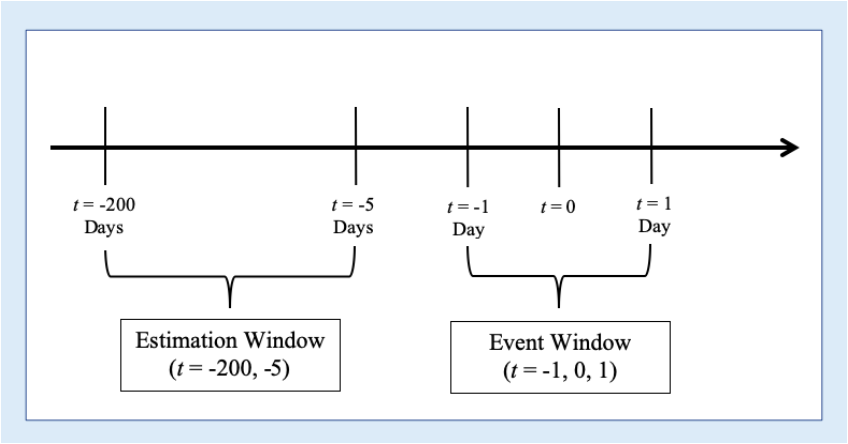


Figure 3: Designated *Estimation* and *Event Window* Sizes

3.3.3 Data Collection – Steps and Procedure

In alignment with previously conducted IS, IT, and InfoSec event study literature, this research investigation followed precedent set within the ESM extant literature. This research utilized the corporation's stock market price as the dependent variable when determining the overall financial impact to the corporation's stock market value resulting

from the introduction of an announcement event (press release announcement identifying a corporate investment in privacy). The unexpected event(s) chosen for investigation are identified as corporate privacy investment announcement events. Data collection for all identified corporate press release announcement investment events was collected over a period of five (5) years from January 1st, 2013 – December 31st, 2018.

The data collection process employed in this research was implemented using an internally designed new hybrid model known as the *Hybrid Process Model* (HPM). The HPM was designed internally and developed specifically for use in this event study. Component construction of the custom HPM included using a combination of the most successful data collection strategies and procedures identified throughout previous Information System (IS), Information Technology (IT), Information Security (InfoSec), and related event study research (Bharadwaj et al., 2009; Dehning et al., 2004; Guan et al., 2006; Hinz et al., 2014; Im et al., 2001; Nicholas-Donald et al., 2011). Utilization of the HPM also deployed the most effective and efficient data collection methodologies identified from previous event study research to ensure both internal and external validity was maintained (Acquisti et al., 2006; Chatterjee et al., 2001; Culnan & Williams, 2009; Dewan & Ren, 2007; Goel et al., 2010; Hovav et al., 2017; Malhotra & Malhotra, 2010).

To alleviate concern regarding accuracy, reliability, or effectiveness of the custom HPM, the HPM did not deviate or change any internal components or parts implemented from existing data collection methodologies used in previous event study literature (Chatterjee et al., 2002; Khallaf & Skantz, 2007; Khansa et al., 2012; Mirsa & Rao, 2009). The HPM is a new research model comprised of the most effective, useful, and

relevant data collection components from previous event study literature consolidated into a single model.

Deployment of the HPM ensured the most appropriate data collection effort was deployed during each stage of the data collection process. Total "Data Collection and Data Filtering Steps" (Figure 4) includes seven (7) individual stages including: 1) data identification, 2) data collection, 3) data filtering, 4) identify corporate industry codes, 5) identify confounding corporate event(s), 6) identify duplicate corporate events, and 7) identify necessary corporate / financial data (Appendix G). Systematical progression through each individual stage of data collection using the HPM ensured the achievement of a high level of certainty confirming all relevant events had been identified for inclusion in the study sample. Deployment of the HPM was further implemented during each individual stage spanning the entire seven stage data collection process.

In addition, similarly to the custom designed HPM implemented during data collection, a custom *Blended Method Approach* (BMA) model was designed for use during the data filtering process once initial data collection was completed. The BMA model was deployed during all steps of data collection. In a similar fashion to the HPM, the BMA is a custom developed model that was used once initial data collection was completed to filter out invalid data during data filtering steps. The BMA is also composed of each of the most efficient, effective, and accurate individual steps and processes identified in previous event study literature (Acquisti et al., 2006; Chatterjee et al., 2001; Culnan & Williams, 2009; Dewan & Ren, 2007; Goel et al., 2010; Hovav et al., 2017; Malhotra & Malhotra, 2010; Nagm & Kautz, 2008), and combined into a singular model for ease of use. For example, in identifying/qualifying corporations based on

requisite U.S. *Securities Exchange Commission* (SEC) *Standard Industrial Classification* (SIC) codes, use of the BMA ensured only relevant data was obtained for analysis by using 1) multiple procedures, 2) different data sources, and 3) varying strategies instead of a singular method. Utilizing a blended approach combining the HPM and BMA during the data collection process provided the broadest range potential for data event identification and collection, while ensuring sample validity and completeness; without contaminating data collected with bias. For accuracy and reliability, no deviations, changes, or omissions have been made to individual components of the BMA; comprised of successful data filtering methods identified in previous event study research.

Figure 4 identifies the seven (7) "Data Collection and Data Filtering" steps that were applied to all collected data for potential inclusion and use within this research.

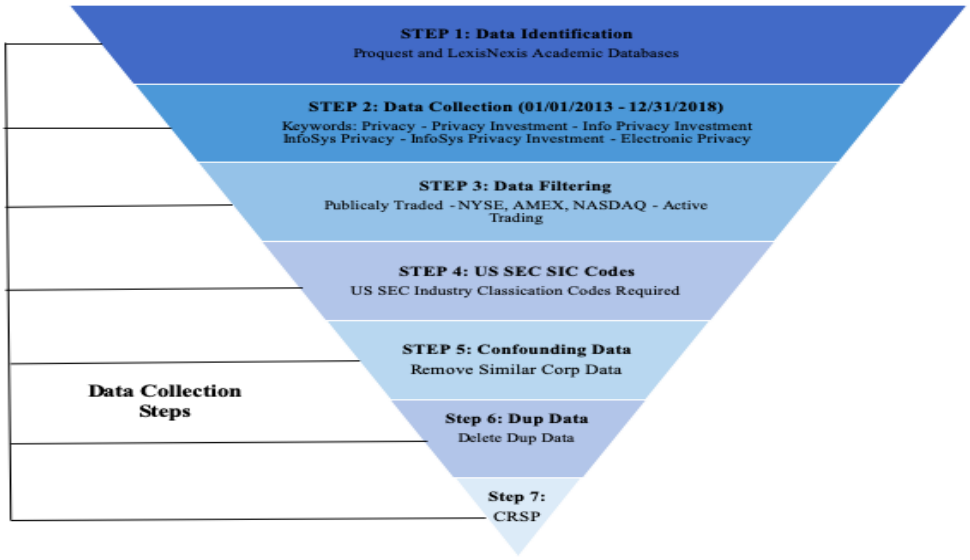


Figure 4: Data Collection and Data Filtering Steps

Step 1) Data Identification –

For duplicability, data identification followed guidelines espoused in previous Information System (IS), Information Technology (IT), Information Security (InfoSec), and related event study literature (Acquisti et al., 2006; Aytes et al., 2006; Campbell et

al., 2003; Cardenas et al., 2008; Cavusoglu et al., 2004; Chai et al., 2010; Hovav et al., 2017; Khansa et al., 2011; Malhotra & Malhotra, 2011; Subramani & Walden, 2001).

Identifying eligible corporate announcement event data began with determining eligible event data for potential inclusion in sample data. Event data came directly from two (2) online data(base) repositories: a) *ProQuest* (PQ) and b) *Business Sources Premier* (BSP). In continuing with the extant literature, each search criterion used only newspapers and news as sources for announcement event identification (newspaper, newswire, press release, news). In addition, based on previous ESM literature, only identified events on news platforms were isolated for announcement event identification and study inclusion (i.e., newspapers, online news sites, digital news).

Data Sources	
Pro Quest (PQ)	Business Source Premier (BSP)

Figure 5– Data Collection (Resources Used)

Step 2) Data Collection –

Following the procedures identified in previous Information System (IS), Information Technology (IT), Information Security (InfoSec), and related event study literature (Acquisti et al., 2006; Aytes et al., 2006; Campbell et al., 2003; Cardenas et al., 2008; Cavusoglu et al., 2004; Chai et al., 2010; Hovav et al., 2017; Khansa et al., 2011; Malhotra & Malhotra, 2011; Nicholas-Donald et al., 2011; Subramani & Walden, 2001), specific key words have been identified for search inclusion in chosen databases.

Data collection in this manner ensured only relevant corporate event data were returned. For this research investigation, six (6) key words were chosen for data identification of all relevant and applicable corporate investment event data: 1) privacy,

2) privacy investment, 3) information privacy investment, 4) information system privacy, 5) information system privacy investment, and 6) electronic privacy. In addition, the plus (+) identifier was appended to each key word search with "announcement" using an "and / or selection" designation to identify additional relevant event data results that may have been originally omitted from initial search results returned during data collection process.

ProQuest (SEARCH)

- Advanced Search
  - Source Type (Newspapers, Wire Feeds)
  - Document Type (News, Reports, Website)
  - Language (English)
  - Search Date (January 1st, 2013 – December 31st, 2018)
  - Search Word (Abstract – AB)
    - + And / Or (Abstract – AB)

Figure 6 – ProQuest (Search Parameters)

Business Source Premier Online (SEARCH)

- Advanced Search
  - Search Mode (Find all my search terms)
  - Document Type (Article)
  - Publication Type (Newspaper)
  - Language (English)
  - Search Date (January 1st, 2013 – December 31st, 2018)
  - Search Word (Abstract – AB)
    + And / Or (Abstract – AB)

Figure 7 – Business Source Premier (Search Parameters)

Step 3) Date Filtering –

Data filtering was necessary for ensuring only eligible and usable corporate announcement event data remained within the sample data set used. For this reason, and following successful procedures used in previous Information System (IS), Information Technology (IT), Information Security (InfoSec), and related event study literature

(Acquisti et al., 2006; Campbell et al., 2003; Cardenas et al., 2008; Cavusoglu et al., 2004; Chai et al., 2010; Hovav et al., 2017; Khansa et al., 2011; Malhotra & Malhotra, 2011; Nicholas-Donald et al., 2011; Subramani & Walden, 2001), only corporate announcement event data relating to *Publicly Traded* corporations were eligible for inclusion within the sample data set. In addition, corporations identified as publicly traded must also be traded on one of the three (3) identified US stock exchanges used within this research study: NYSE, AMEX, or NASDAQ.

To ensure the identified data is accurate and current, all corporations publicly trading on one of the three (3) identified US stock market exchanges must have also been actively traded on the exchange during the identified estimation window and event windows being examined within the research investigation. Identified corporations not publicly traded, or not actively trading during the estimation / event windows, were eliminated from the sample data set.

Step 4) Identify Corporate Standard Industrial Classification (SIC) *Codes* –

Having been utilized successfully in previous Information System (IS), Information Technology (IT), Information Security (InfoSec), and related event study literature (Aytes et al., 2006; Campbell et al., 2003), all corporations associated with a corporate announcement event must have been classified with a valid COMPUSTAT *Standard Industrial Classification* (SIC) code created by the US *Securities and Exchange Commission* (SEC). Corporations identified but not classified with a US SEC SIC code were eliminated from the data set and excluded from the research study.

Step 5) Identify and Remove Confounding Data (Announcement Events) –

One of the challenges when conducting an event study is knowing for certain that all observable results identified during data analysis were achieved directly from the isolated event being examined (privacy investment announcement event). Confounding events are defined as corporate announcement events that occur during, or around, the same time period as that of the event window insomuch that the confounding event may be impacting the corporation's stock market value instead of the isolated privacy investment event being investigated. The underlying presumption is that observable changes in corporate stock market price could have been caused by either the event being investigated or the identified confounding event. This research employed the same method for dealing with confounding data events as has been successfully utilized in previous Information System (IS), Information Technology (IT), Information Security (InfoSec), and related event study literature (Acquisti et al., 2006; Cardenas et al., 2008; Cavusoglu et al., 2004; Chai et al., 2010; Hovav et al., 2017; Khansa et al., 2011; Malhotra & Malhotra, 2011; Subramani & Walden, 2001).

As noted in previous event study research, confounding events are "…significant public announcements that could undermine the results of the study" (Cavusoglu et al., 2004). Confounding events include press release announcement events relating to, but not limited to 1) dividends, 2) mergers, 3) acquisitions, 4) positional hiring (i.e., CIO), 5) earnings and 6) corporate financial disclosures. As has historically been done in event study research, potential confounding events were controlled for through the use of a buffer; a time period -1-Day *before* event announcement (t = -1), and 1-Day *after* event announcement (t = 1). Identified corporate events with confounding data within the designated time period were eliminated from the data set and excluded from the research.

Step 6) Identify and Remove Duplicate Corporate Data (Announcement Events) –

Utilizing multiple data resources during the data collection process produced instances of multiple corporate event data, from the same corporation, announcing the same corporate news, but from different news outlet sources. As has been done in previous Information System (IS), Information Technology (IT), Information Security (InfoSec), and related event study literature (Campbell et al., 2003; Cardenas et al., 2008; Cavusoglu et al., 2004; Chai et al., 2010; Hovav et al., 2017; Malhotra & Malhotra, 2011; Subramani & Walden, 2001), all identifiable instances of duplicate announcement event data were eliminated. In instances presenting duplicate corporate announcement event data, earliest reported announcement events were kept and used in the sample data.

Step 7) Identify Corporate and Financial Data –

The University of Chicago's Center for Research in Security Prices (CRSP) database is a financial repository providing corporate data for all active publicly traded corporations active on one of the three (3) US stock market indexes identified for use (NYSE, AMEX, and NASDAQ). Corporate data provided in the CRSP database is necessary for determining financial impact of corporate investment announcement events. In accordance with previous Information System (IS), Information Technology (IT), Information Security (InfoSec), and related event study literature (Aytes et al., 2006; Campbell et al., 2003; Cardenas et al., 2008; Cavusoglu et al., 2004; Khansa et al., 2011; Malhotra & Malhotra, 2011), any identified corporation that did not have associated financial information within CRSP was eliminated and excluded from this research.

In addition to identification and collection of requisite corporate data within the CRSP database, corporations must have also been recognizable in COMPUSTAT. The

COMPUSTAT database provided relevant corporate information and Standard Industry Classification (SIC) codes pertaining to revenue, employee count, sales, revenue, etc. Corporate information gathered from COMPUSTAT was necessary in determining whether the presence of a financial impact relating to the investment announcement event was affected in any manner by the corporation's specific industry, type, size, revenue, etc., for each corporation investigated in this research exploration.

Accumulating requisite data in this manner required implementing variable control methods during data collection and filtering processes to ensure the remaining *sample data set* was uncontaminated. Figure 8 illustrates potential data corruption points along with applicable control method(s) employed to combat any potential negative effects untoward the data causing internal / external validity (generalizability) concerns.

Step		**Potential Problem**	**Control Method Employed**
1	Manageability	Too many data sources	Data was collected from two (2) database data repository resources (ProQuest and Business Source Premier) to ensure the scope of the research is manageable
2	Feasibility	Too much data (volume)	Targeted data for research investigation was identified by limiting results to only those specifically matching six (6) designated keywords chosen
3	Applicability (US)	Ensuring company information is publicly available for access	In order to use the data identified, all relevant company's must be publicly traded on one of the identified exchanges (NYSE, AMEX, or NASDAQ), and have all company data publicly accessible for study inclusion
4	Usability	Must be able to be identified	All companies included in the study must have a government SIC code
5	Accuracy	Data corruption or skewed results	Confounding events have the potential to give a false sense of market value or provide incorrect market analysis based on non-relevant events. All confounding events were eliminated to ensure confounding event did not provide false market movement for the investment announcement being investigated
6	Duplicity	Duplicate events	Identified duplicate announcement events were removed from the study with the earliest announced event date from the corporate event being used
7	Accessibility	Not having financial information available	All companies included for inclusion within the data investigation must have their financial information published and accessible via CRSP & COMPUSTAT

Figure 8 – Potential Data Collection Problems and Applicable Controls Deployed

Progressing through each of the seven steps ensured that only relevant data was collected and available for requisite data analysis. In this manner, the volume of potential data for study inclusion was reduced, while simultaneously eliminating non-relevant data, and all data identified as a potential source of data corruption. As the totality of data was funneled downward from Step 1 through Step 7, the data became more accurate, valid, and manageable. Following Step 7, the remaining data encompassed the final set of events identified for analysis within this research. Figure 9 (*Data Filtering Process*) illustrates the methodology that was deployed during each of the seven steps.

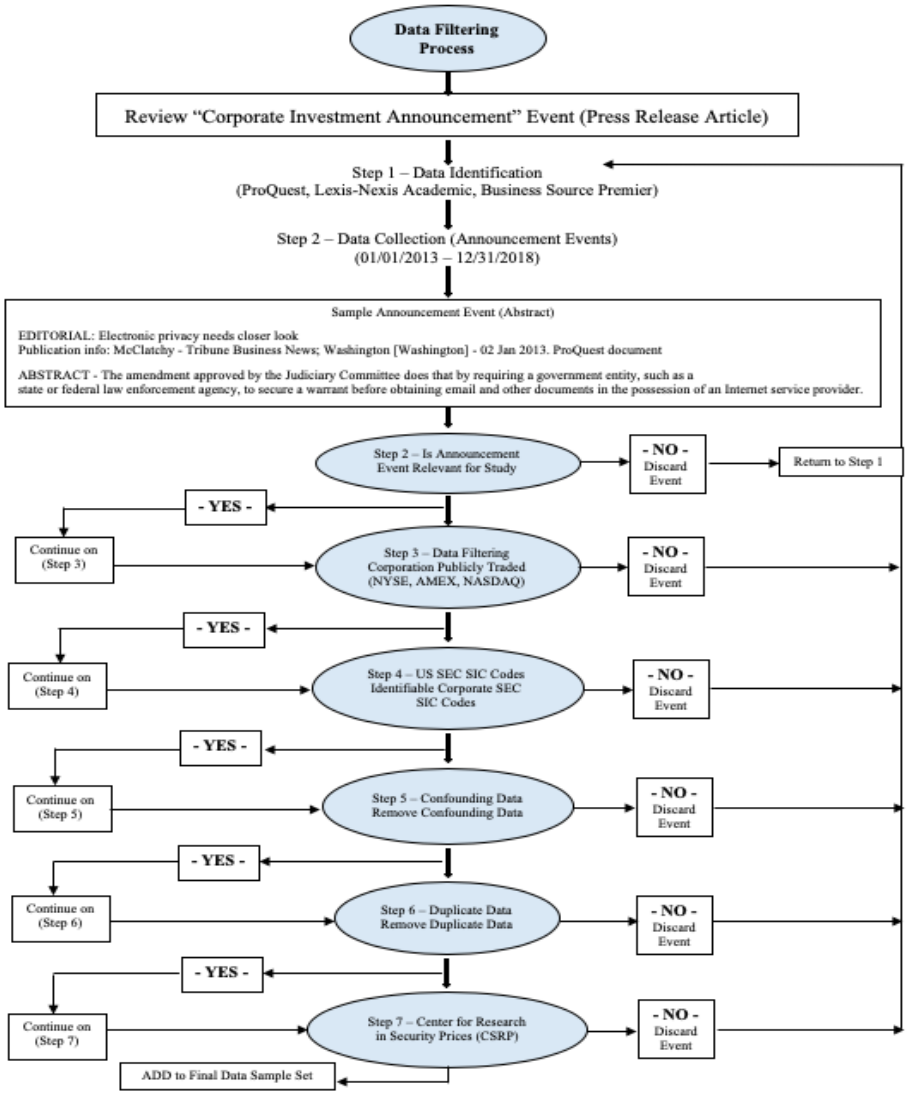


Figure 9 – Complete Data Filtering Process

3.3.4 Data Analysis

The main objective of an event study is to analyze the impact that an unexpected event has on stock market value of the associated firm. Utilizing an event study in this research, the specific event being investigated is the financial impact that a corporate privacy investment announcement (event) had on the corporation's stock market value. Determining whether or not a corporate privacy event has any financial impact on the stock market value of the associated corporation requires using Event Study Methodology (ESM) to calculate the overall stock market effect from the privacy announcement event. Using ESM requires specific stock market assumptions to be made based on the theory of Efficient Market Hypothesis (EMH). Under the EMH theory, all publicly available corporate information is built into the corporation's stock market price. Accordingly, any new corporate information released to the public will be quickly incorporated into the stock market price based on the perceived value of the new information by the corporation's shareholders.

Using financial information provided in the University of Chicago's Center for Research in Security Prices (CRSP), and COMPUSTAT, corporations normal expected average stock market value was calculated for each corporation at the time of the corporate privacy announcement (event). Following this, daily average stock market price for each corporation being investigated within this research study was computed over the designated 195-Day estimation window (t = -200, -5 Days). Average daily stock market prices were computed using the *equally weighted* stock market indices associated with the public trading of the corporation (NYSE, AMEX, or NASDAQ).

EMH theory, using the CAPM-based MM, is appropriate for executing financial calculations necessary in determining potential financial impact made by corporate announcement events identifying corporate investments in privacy. The CAPM-based MM was used in determining average corporate stock market value over the 195-Day estimation window (t = -200-Days, t = -5-Days). Calculations to compute average corporate stock market value were based on computing daily stock returns for each day in the 195-Day estimation window (-200, -5 Days). Identified Expected Normal Return (ENR) values identified corporate stock market price, absent the corporate privacy investment announcement event being investigated in this research.

Once *ENR*s were calculated for each included corporation, the next step was computing Abnormal Return (*AR*) for each corporation. *AR* is the difference between expected normal return over the estimation window and realized stock market return after the corporate privacy investment announcement (event). The *AR* for each corporation was calculated over the three-day (3-Day) event window (t = -1; t = 0; t = 1). Subtracting expected normal return from realized normal return provided empirical evidence identifying financial changes in corporate stock market value. *CAR* was determined by calculating the *AR* for each corporation over the entire event window (t = -1, t = 0, t = 1). *ACAR* for corporations was also calculated and used. The CAPM-based MM was used to estimate the linear regression parameters using OLS for each identified corporation. Once *AR*, *CAR*, and *ACAR* were calculated for each identified corporation associated with a corporate investment announcement event, data analysis was conducted to determine the significance and meaning of all obtained results.

Test Statistics

In this research, the CAPM-based MM was used to estimate coefficient parameters necessary for all mathematical computations. However, because the "…homoskedasticity assumption of the traditional market model approach may be violated" (Benco & Prather, 2008), use of both *Generalized Autoregressive Conditional Heteroskedasticity* (GARCH) and *Exponential Generalized Autoregressive Conditional Heteroskedasticity* (EGARCH) models were made available as needed to ensure study robustness was maintained, however neither was used. The GARCH estimation model, introduced by (Bollerslev, 1986), allows conditional variance to change as a function of past-realized residuals and past variances, while the EGARCH estimation model, introduced by (Nelson, 1990), does not impose non-negativity constraints on the coefficient estimators of the market model parameters and allows past residuals of different signs to have a differential impact on future volatility compared to the standard GARCH model (Benco & Prather, 2008).

The null hypothesis that corporate Abnormal Returns (*ARs*) are not significantly different from zero (0) is rejected in this research. Under the null hypothesis, *AR*s are independent, identically distributed, and normal with a mean of zero (0); the variance given by the variance of abnormal returns over the identified estimation period (Acquisti et al., 2006). In addition, a *Z*-statistic, similar to the one developed in research by Loderer & Mauer (1992), was deployed to test the statistical significance of abnormal returns from corporate investment announcement events identified within the sample data (Hovav & D'Arcy, 2005). Under the null hypothesis (of zero expected abnormal returns), *Z* is approximately unit normally distributed (Hovav & D'Arcy, 2003), as

illustrated in research presented by Loderer & Mauer (1992). The *t* statistic presented by Brown & Warner (1985) and designed specifically to work with excess returns, was available if needed to examine the significance of *AR* results due to its ability to both take into consideration event day clustering in the form of multiple, identical events, and cross-sectional dependence when investigating abnormal or excess stock market returns.

The Z-test statistic was used to assess whether or not the Average Cumulative Abnormal Return (ACAR), or Mean CAR, was significantly different (statistically) from zero, its expected value (McWilliams & Siegel, 1997). Furthermore, according to Im et al. (2001), the significance of the abnormal return based on the Z-statistic test allows the researcher to infer that the privacy investment announcement events had a significant impact on the market value of the firm (Loderer & Mauer, 1992; McWilliams & Siegel, 1997). This was necessary to test the null hypothesis, as well as to test all hypotheses posited within this research regarding corporate investments in privacy.

The Z-statistic was calculated using the formula:

$$Z = ACAR_t \times n^{0.5} \qquad \text{(Formula 5)}$$

Formula 5 where:

Z	test statistic to identify statistical significance of ACAR for each Corporation being investigated within the research
ACAR	Average Cumulative Abnormal Return for each corporation identified

Both *parametric* tests and *nonparametric* tests were used to ascertain the significance of the data results obtained within this research, as well as ensure the robustness of the research investigation. In addition to the parametric *Patell Test* (Pattel, 1976) and previously noted Z-statistic, outlier data discovered during research analysis were controlled for using non-parametric binomial Z-statistic testing. This tested

whether the "… proportion of positive to negative returns exceeds the number expected from the market model" (McWilliams & Siegel, 1997). Moreover, the *Generalized Sign Z-test* (Z-statistic) was used to examine the number of securities with positive (+) and negative (-) *Average Abnormal Returns* (AAR) during the designated estimation window (195-Days) and event window (3-Day) under the null hypothesis that the fraction of positive (+) returns during the event window is the same as the fraction of positive (+) returns during the estimation window (Benco & Prather, 2008).

The original intention during research design and methodology was to use the Patell test due to is being a stalwart testing method within the event study literature, and the gold standard testing methodology within the event study research community. However, additional event study research into the most successful manner of deployment when using the Eventus® software suite for event study testing identified a more robust testing method available known as the *Standardized Cross-Sectional Test* (StdCsect) (aka BMP test) (Boehmer et al.,1991). As a more suitable test, the BMP test was used for all statistical testing and in substitute for the Patell testing method.

Under the original Patell test (1976), the "…standardized abnormal return test of the null hypothesis that the mean abnormal return is zero, derived by Patell (1976)" (Cowan, 2020). The Patell test has important strengths that allow its use extensively within event study research. The original form Patell test (1976) has subsequently been improved and updated by various researchers and academics; most notably Brown & Warner (1980; 1985). In their updated version of the Patell test, known as the BW test, researchers Brown & Warner (1980, 1985) report "… simulation evidence that the test is well specified in random samples of actual security returns. Further, they show that the

Patell test greatly improves power to detect an abnormal return (artificially induced for the simulations) by making use of firm-specific variance estimates" (Cowan, 2020). However, Cowan notes that their research also reports that a "… variance increase on the event date can seriously bias the Patell test" (Cowan, 2020). Issues relating to the potential harm to results caused by the increased return variances around announcement events of interest have been reported as early as Beaver (1968). The most recent version of the upgraded Patel test by Brown & Warner is recognized in academia as the BW test.

Using the StdCsect (BMP) method in place of the standard Patell test option automatically includes the SERIAL option for all results. In a simplistic nature, the BMP method is an enhanced version of the original Patell (1976) test. One of the benefits of using the BMP test is increased study robustness over the traditional BW test. The BMP test is an "…extension of the Patell test, the standardized cross-sectional test, which brings in cross-sectional variance information to correct for variance increases. BMP provides Patell-type simulation evidence that the standardized cross-sectional test is robust to event-date variance increases. (Cowan, 2020). This sentiment was echoed in research by Higgins & Peterson (1998) who conducted simulations while using empirical distribution functions to equalize power under the null hypothesis across tests. In direct comparison to the BW test, research results support the overall sense of superiority of using the BMP standardized cross-sectional test.

Harrington & Shrider (2007) also provide a more rigorous analytical foundation for the BMP standardized cross-sectional test. The authors report "… additional simulation evidence of heteroskedasticity-related biases of the Patell test that the standardized cross-sectional test avoids" (Cowan, 2020). Furthermore, the author and

creators of the BMP test, Marks & Musumeci, support Harrington and Shrider's 2007 research and recommend that researchers always use the BMP standardized cross-sectional BMP test in direct preference to the Patell test (Cowan, 2020). In addition to full use support from the creator of the Eventus® software suite, Arnold Cowan, the BMP testing methodology as a superior testing option when compared to the Patell test (1967) has been directly supported with research evidence by Beaver (1968), Boehmer et al. (1991), Campbell et al. (2010), Cowan (1993), Dodd & Warner (1983), Graham et al. (1996), Harrington & Shrider (2007), Harvey (2017), Higgins & Peterson (1998), Karolyi (2011), Kolari & Pynnönen (2010), Leamer (1983), and Mikkelson & Partch (1988).

Both *parametric* tests and *nonparametric* tests were to ascertain the significance of the data results obtained within this research, as well as to ensure the robustness of the research investigation. Parametric tests used include *Standardized Cross-Sectional* (StdCsect) (aka BMP test) (Boehmer et al.,1991), in place of the traditional Patell test (1976), and standardized StdCsect Z-statistic tests. The StdCsect Z-test statistic was used to assess whether or not the Average Cumulative Abnormal Return (ACAR), Mean CAR, is significantly different from zero, its expected value (McWilliams & Siegel, 1997). Furthermore, according to Im et al. (2001), the significance of the abnormal return based on the Z-statistic test allows the researcher to infer that the privacy investment announcement events have a significant impact on the market value of the associated firm (Loderer & Mauer, 1992; McWilliams & Siegel, 1997). This is necessary to test the null hypothesis, as well as to test all hypotheses posited within this research regarding corporate investments in privacy.

Both StdCsect Z and Generalized Sign tests were used together in tandem within this research investigation to validate all identified study results. As Cavusoglu (2004) noted, the StdCsect Z test (Patell 1976 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 (Brock, 2012). Use of 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).

A multiplicity of testing was conducted using both parametric and nonparametric methods as the Information System (IS), Information Technology (IT), Information Security (InfoSec) and related event study literature does not provide consensus for a singular test for use when conducting event study research using Event Study Methodology (ESM). Furthermore, different tests provide different functional use so the ability to implement specific tests to achieve specified research objectives is a benefit; as noted Benco & Parather (2008), "…no single test appears to dominate the others in terms of power and Type I and Type II errors (e.g., Cowan, 1992)."

The Eventus® software suite assisted in the task of calculating mathematical computations necessary using their dedicated data platform and available research tools. Access to these resources was vital to the successful completion of this research investigation as they provided the opportunity to deploy a variety of specified parametric and nonparametric tests needed to achieve the stated research goals. All identified corporations with an identified investment announcement event had their abnormal returns (*AR*s) and test statistics collected using Eventus®, a software package that

interfaces between SAS (*Statistical Analysis System*) and the CRSP database and computes the abnormal returns (*AR*s) for "…specified event windows using specified models (Agrawal et al., 2006). The main usage benefit from this analysis software is that Eventus® was designed specifically to collect stock return information and test statistics, as well as assist in data analysis, in event study research using ESM.

Once completion of the sample data set was achieved through successfully executing all data collection procedures, relevant corporate information was needed for each associated corporation investigated within the research investigation. Eventus® requires both corporate CRSP and COMPUSTAT financial information, as well as associated US SEC corporate SIC codes. Once the identified information was provided, the software performed the designated calculations (Formulas 1 – 5) for corporate *AR*, *CAR*, *ACAR* and obtained all information necessary for CAPM-based MM computations.

All relevant corporate investment announcement event data was identified, collected, filtered, then prepared for data analysis using Event Study Methodology (ESM). The research methodology presented indicates the nature and manner in which all associated corporate investment announcement event data collected were analyzed. Data analysis was conducted for all corporate data included within the sample data set with results presented to highlight all relevant corporate stock market details, including associated *Ar*s, *CAR*s, *ACAR*s, etc. This information was supported by additional results presented identifying the statistical significance of identified *AR*s for each associated corporation, based on a multiple of parametric and nonparametric tests.

Data analysis is presented to showcase the financial impact identified from corporate investments in privacy, based on the resultant change in stock market from the

corporate privacy investment announcement event. The analysis illustrates the severity of the financial impact for corporations based on specific corporate industry (SIC codes), size of corporation, financial outlook (corporate sales, revenue, value), etc. Furthermore, the analysis also indicates identifiable, observable, and quantifiable financial implications to encourage and incentivize increased corporate investments in privacy.

3.4 Resource Requirements

This research study utilized Event Study Methodology (ESM) while examining the financial impact that an unexpected event, identified in this research as a corporate investment in privacy announcement, had on corporate stock market value. As an event study, only publicly available data was required in this research. All event data was identified from ProQuest and Business Source Premier online database repositories, with requisite access to both database repositories successfully secured. These academic database repositories yielded all requisite corporate event data required for further examination in this research.

All relevant corporate data and financial information for identified corporate investment announcement events required for data analysis in this research came from the University of Chicago's CSRP database and COMPUSTAT through the Eventus® software suite. Special access was required for software access necessary in this event study. Similar to the academic database repositories listed, special access was requested and granted for all requisite software, including the University of Chicago's CSRP database, COMPUSTAT, and Eventus® software suite. In examining potential financial impact that corporate privacy investment announcement event(s) had on corporate stock market values, access was needed to the three (3) identified US-based stock market

indexes: NYSE, AMEX, and NASDAQ. Data required from the three (3) stock market indexes is freely accessible to the general public. In addition, included corporate event data must be identified with appropriate US SIC codes; designated and assigned from US SEC classification system. Access to the US SEC SIC classification code database is a free service with access secured.

Data calculations required access to Eventus® financial analysis software suite. In accordance with previous event study research successfully utilizing the Eventus® platform, this research also relied upon the Eventus® platform to assist in conducting stock market calculations necessary for identifying potential financial impact from corporate investments in privacy. Full access rights (special individual user) to the Eventus® platform were granted in partnership with *University of Pennsylvania* (UPENN) Wharton School of Business "Wharton Research Data Services" (WRDS).

3.5 Summary

Corporation's operate with a fiduciary responsibility to shareholders in maximizing profits. Sales, services, subscriptions, contracts, and customer retention have been traditional methods in which corporations are able to increase financial revenue; however, in a non-traditional sense, strategic corporate investments have also proven to be an equal source of wealth generation when the correct investment is identified and deployed within the correct environment. Academics originally identified the financial impact of a corporate investment announcement event in finance, economics, and accounting. Due to the generalizability of event study research using Event Study Methodology (ESM), however, academics quickly extended the thought process to identify the financial impact of corporate investment announcement events in other

research domains, including Information Systems (IS), Information Technology (IT), Information Security (InfoSec), Computer Security (ComSec), etc. An extensive literature review of the extant event study literature identified corporate investments in IS/IT as a potential source of corporate wealth through an increased stock market value when the IS/IT was implemented successfully, within the correct industry.

Corporations that originally identified the potential for positive increased stock market value from strategic investments in IS/IT further expanded their research efforts to identify any financial impact from corporate investments in InfoSec when security became a corporate concern, as well as hardware, software, and policy initiatives. According to the literature review, corporations used event study research extensively to help identify investment areas that could generate increased corporate wealth; except one, privacy. This limited focus of research interest was the impetus driving this research dissertation. Research examining corporate investments in privacy helps bridge this research gap and provides a better understanding of the potential financial implications associated with corporate investments in privacy.

Previous Information System (IS), Information Technology (IT), Information Security (InfoSec), and related event study literature (Aytes et al., 2006; Campbell et al., 2003; Cardenas et al., 2008; Cavusoglu et al., 2004; Khansa et al., 2011; Malhorta and Malhorta, 2011), have successfully used ESM identifying financial impact of corporate investment announcement events. In accordance with previous research success, this study used ESM in identifying potential financial implications when examining corporate investments in privacy. This literary analysis enhances the extant body of literature by filling an existing research gap relating to corporate investments in privacy.

As corporations are required to generate increased corporate wealth, this research posits that there is simply not enough financial incentive to motivate increased corporate investments in privacy, nor has any financial incentive been yet identified encouraging additional / continued corporate investments in privacy. Identifiable results proving the existence of a financial incentive promoting corporate investments in privacy may be the impetus necessary to change corporate investment behavior. Absent that, it is unlikely that change to corporate privacy investment practices will occur.

The research objective of this investigation is examining corporate investments in privacy. This research is necessary to provide corporations and research academics data and analysis requisite for better understanding corporate investments in privacy. To encourage any financial policy change, relevant to corporate investment strategy, data must exist providing support to showcase the likelihood of increased, sustainable corporate wealth directly resulting from a specified investment decision. Previous Information System (IS), Information Technology (IT), Information Security (InfoSec), and related event study literature have provided this data to corporations, which has led to increased IS/IT investments. However, evident in the extant literature, only minimal event study research interest has been shown examining corporate investments in privacy, nor the financial implications associated with corporate investments in privacy. To help bridge this research gap, this study provides an examination of corporate investments in privacy, presents financial implications from corporate investments in privacy, identifies industry segments benefitting the most from corporate investments in privacy, and provides relevant information to help better understand *"Why are Corporations Are Not Investing in Privacy?*

Chapter 4

Results

4.1 Introduction

Strategic investment options present corporations with an opportunity to gain corporate wealth through increased stock market value when implemented correctly within a corporate environment. A major challenge, however, is accurately estimating the financial value of the proposed investment option to be sure the increased financial growth outweighs the requisite upfront investment capital necessary to implement the proposed investment option. In this research investigation, corporate investments in privacy were examined to determine whether there exists any potential financial impact to overall corporate stock market value from corporate investments in privacy.

In this chapter, data analysis, research findings, and results are presented. The resultant data produced from this research examination is intended to supplement the extant body of event study literature. This research presents quantitative support identifying how corporate investments in privacy affect overall corporate stock market value, as well as highlighting both financial incentives relating to corporate investments in privacy, and financial penalties for corporations *not* to investing in privacy.

4.2 Data Sample

The goal of this research investigation was to examine the financial implications associated with corporate investments in privacy, as well as isolate any financial implications for corporations *not investing* in privacy. To achieve this research objective, an event study was conducted to ascertain any financial implications associated with

corporate investments in privacy. In this event study research, a final data sample set was used for testing and analysis that included a total of 323 individual corporate press release announcement events relating to "corporate investments in privacy," from 75 different corporations, spanning five years: January 1st, 2013 – December 31st, 2018.

4.2.1 Data Identification

In this research investigation, literature review included an examination of Privacy, *Information Privacy* (IP), Information Systems (IS), Information Technology (IT), Security, Information Security (InfoSec), and related technology domains, as well as analysis of event study literature across multiple research domains. Covering a time period of almost sixty years (1962 – Present), 123 event study and related literature research encompasses the (estimated) totality of the event study extant body of literature.

Table 1

Final Sample Set – Event Study Research and Literature Breakdown (by Research Category)

Literature Category	Number of Research Papers	Percentage (%) Total Research Literature Completed
IS/IT Investments	47	38.21%
IS/IT Privacy	8	6.50%
IS/IT Security	28	22.77%
IS/IT Outsourcing	8	6.50%
IS/IT (Other)	16	13.01%
Event Study (History / Background)	16	13.01%
Total	123	100%

4.3 Data Collection

In this research investigation, research data was identified using the ProQuest (PQ) and Business Source Premier (BSP) online academic database repositories.

Financial and corporate stock market data was identified using the *New York Stock Exchange* (NYSE), *American Stock Exchange* (AMEX), and/or the *National Association of Securities Dealers Automated Quotations* (NASDAQ) stock market indexes, with related corporate data provided from the University of Chicago's *Center for Research in Security Pricing* (CRSP) and Eventus® software platform.

Both data identification and data collection processes were implemented within this research using an internally designed new model known as the *Hybrid Process Model* (HPM). Component construction of the new HPM included combining together the most successful data identification and collection strategies identified throughout previous Information System (IS), Information Technology (IT), Information Security (InfoSec), and related event study research (Bharadwaj et al., 2009; Dehning et al., 2004; Guan et al., 2006; Hinz et al., 2014; Im et al., 2001; Nicholas-Donald et al., 2011) into a single, more robust model. Utilization of the new HPM also ensured requisite internal and external validity was successfully maintained (Acquisti et al., 2006; Chatterjee et al., 2001; Culnan & Williams, 2009; Dewan & Ren, 2007; Goel et al., 2010; Hovav et al., 2017; Malhotra & Malhotra, 2010; Nagm & Kautz, 2008). Once initial data identification and data collection was complete, data filtering began.

The data filtering process followed a similar approach to the data identification and data collection processes. In addition to the aforementioned newly created *Hybrid Process Model* (HPM), a customized model specific for event study use was also created and designed for the data filtering process once initial data identification and data collection was completed, known as the *Blended Method Approach* (BMA) model. The BMA model was deployed during each of the identified data collection and data filtering

steps (Table 2); necessary when completing an event study to eliminate and filter out invalid data from potential inclusion in the study.

Table 2

Data Collection and Data Filtering Steps

Step	Action
Step 1	Data Identification
Step 2	Data Collection
Step 3	Data Filtering (7-Step process)
Step 4	US SIC Code (identification)
Step 5	Confounding Data (eliminate)
Step 6	Duplicate Data (eliminate)
Step 7	CRSP Data (identification)

The new BMA model is a singular, easy to use model combining the most efficient, effective, and accurate individual steps, processes, and procedural guidelines identified as most successful throughout previously event study research and literature (Acquisti et al., 2006; Chatterjee et al., 2001; Culnan & Williams, 2009; Dewan & Ren, 2007; Goel et al., 2010; Hovav et al., 2017; Malhotra & Malhotra, 2010; Nagm & Kautz, 2008). Deployed use of the BMA ensured only relevant data was obtained for analysis by using 1) multiple procedures, 2) different data sources, and 3) varying strategies instead of a singular method. Utilizing a blended model approach combining both HPM and BMA during data collection provided the broadest range potential for data event identification and collection, while ensuring sample validity, thoroughness, and completeness; without contaminating data collected with bias. The hybrid model combined the most successfully used practices identified throughout previously conducted event study research within the Information Technology domain and beyond, identified in Chapter 2 (Acquisti et al., 2006; Aytes et al., 2006; Campbell et al., 2003;

Cardenas et al., 2008; Cavusoglu et al., 2004; Chai et al., 2010; Subramani & Walden, 2001). The practice of combining established procedural guidelines and recommendations into the newly introduced hybrid models allowed successful data identification, collection, and filtering within this research investigation.

During each step of the event study process, corporate announcement event (data) identified as not aligning with the study's predefined sample parameters were eliminated from inclusion. In *Step 1 – Data Identification*, initial data identification and data collection was limited in scope to only data from ProQuest (PQ) and Business Source Premier (BSP) online academic database repositories. Following traditional event study guidelines, a 5-Year timeframe was chosen for research exploration: January 1st, 2013 – December 31st, 2018.

In *Step 2 – Data Collection*, following historic Information System (IS) and Information Security (InfoSec) event study literature guidelines (Dos Santos et al., 1993; Hovav et al., 2017; Khansa et al., 2011; Malhotra & Malhotra, 2011; Nicholas-Donald et al., 2011), a set of six defined keywords were chosen as search parameters that helped narrow the focus of study to only announcement events identifying corporate investments in privacy within this research. The six (6) key words chosen for data identification included: 1) Privacy, 2) Privacy Investment, 3) Information Privacy Investment, 4) Information System Privacy, 5) Information System Privacy Investment, and 6) Electronic Privacy. In addition, the plus (+) identifier was appended to each key word search with "announcement" using "and / or selection" designation to identify additional relevant event data results that may have originally been omitted from initial data

collection results. In addition, only corporate announcement events identified as originating from newspaper, news feeds, wire feeds, or news media were included.

During *Step 3 – Data Filtering*, corporate announcement events were cross checked with financial and corporate trading information. In alignment with previous event studies conducted, only announcement events made by corporation's publicly traded within the United States (U.S.) on one of the identified stock market indices accepted for use in this research (NYSE, AMEX, NASDAQ) were considered for inclusion in the sample data set. In addition, corporations were then cross referenced with active trading data to ensure they were actively traded on one of the three accepted stock market exchanges during both the selected estimation window (-200, -5) and event window (-1, 0, 1) being examined within the research investigation. Corporations not actively traded on one other three chosen indexes, or not actively traded during the estimation and event windows were eliminated from the sample data set.

In *Step 4 – US SEC SIC Code* (*identification*), each corporation corresponding to an announcement event was examined to identify their US Securities and Exchange (SEC) Standard Industrial Classification (SIC) code. A SIC code was necessary for financial data aggregation, so all corporations identified without an active US SEC SIC code were eliminated from the sample data set.

During *Step 5 – Confounding Data* (*eliminate*), resultant data from both ProQuest (PQ) and Business Source Premier (BSP) database searches were first combined into a singular final sample set for ease of use, then searched for confounding and duplicate data. By definition, *Confounding Data* are identified as corporate announcement events occurring during, or around, the same time period as the event window (-1, 0, 1), that

may have an influence on the privacy investment announcement event being studied in this research. Confounding data include, but are not limited to, corporate press release announcement events relating to: 1) dividends, 2) mergers, 3) acquisitions, 4) positional hiring (i.e., CIO), 5) earnings and 6) corporate financial disclosures. As "…significant public announcements that could undermine the results of the study" (Cavusoglu et al., 2004), confounding events must be accounted for. To be certain that all observable results identified during data analysis were achieved directly from the isolated privacy investment announcement event being examined, and not from the potential conflicting confounding event, all corporate events with confounding data identified were eliminated from the data set and excluded from the study.

In *Step 6 – Duplicate Data* (*eliminate*), after the resultant data from both ProQuest (PQ) and Business Source Premier (BSP) database searches were combined into a single data set, all duplicate corporate announcement events were eliminated from the final data sample. In instances of duplicate data from multiple news sources, announcement events with the earliest publication date were kept, with later published announcement events removed from the final data sample.

In *Step 7 – CRSP* (*identification*), corporations with associated privacy announcement event data were checked to ensure all necessary financial data needed for completing the event study was available. In accordance with previous IS, IT, InfoSec, and related event study research (Aytes et al., 2006; Campbell et al., 2003; Cardenas et al., 2008; Cavusoglu et al., 2004; Khansa et al., 2011; Malhotra & Malhotra, 2011), any identified corporations without financial information within CRSP were eliminated.

Progressing through data collection and data filtering steps allowed only relevant corporate privacy announcement events to remain within the final sample set while removing all invalid and unusable data events. From the list of 2,371 initially identified data announcement events relating to "corporate investments in privacy," 2,048 events were eliminated during data collection and data filtering. The remaining 323 data events were included in the study sample.

Table 3 identifies descriptive statistics observed during progression through each step of the data collection / data filtering process. The final data sample indicated presents the complete list of corporate announcement events from both ProQuest (PQ) and Business Source Premier (BSP) included in the final data set, for each of the 323 identified corporate announcement events spanning the timeframe investigated in this research: January 1st, 2013 – December 31st, 2018.

Table 3

Final Data Sample – Announcement Event Breakdown by Step (1-7)

Corporate Announcement Event(s)	ProQuest (PQ)	Business Source Premiere (BSP)
Step 1 – Data Identification (Initial Search Results)	2,052	319
Step 2 – Data Collection	617	215
Step 3 – Data Filtering	367	200
Step 4 – US SEC SIC Code (Identification)	349	194
Step 5 – Confounding Data (Eliminate)	323	137
Step 6 – Duplicate Data (Eliminate)	316	123
Step 7 – CRSP Data (Identification)	311	116
PQ (311) + BSP (116) Totals combined with confounding and duplicate announcement events removed		
Final Sample Set	**323 Announcement Events**	

Table 4 identifies descriptive statistics for corporations included in the final data set, including yearly breakdown and percentage distribution for each of the 323 identified

corporate announcement events spanning the timeframe investigated in this research: January 1st, 2013 – December 31st, 2018.

Table 4

Final Data Sample – Announcement Events (by Year)

Year	Number of Announcement Events	% of Total (Announcement Events)
2013	59	18.27%
2014	54	16.72%
2015	47	14.55%
2016	36	11.15%
2017	83	25.70%
2018	44	13.62%
Total	323	100%

The final data sample set included 323 individual press release announcement events relating to corporate investments in privacy, from 75 different corporations, spanning the time period January 1st, 2013 – December 31st, 2018. Based on individual assigned corporate US SEC SIC code designators, the final sample set of 323 corporate investment in privacy announcement events included individual announcement event data from 6 different US SEC SIC Code *Divisions*, (J – *Public Administration*, I – *Services*, D – *Manufacturing*, E – *Transportation, Communications, Electric, Gas, and Sanitary Services*, G – *Retail Trade*, and H – *Finance, Insurance, and Real Estate*).

Table 5 identifies descriptive statistics for each corporation included in the final data set of 323 individual corporate announcement events, broken down by corporate classification according US SEC SIC Code – Division Classification.

Table 5

Final Data Sample – SIC Code Breakdown (by Division)

SIC Code – Division	SIC Code – Division Name	Number of Privacy Announcement Events
J	Public Administration	75
I	Services	160
D	Manufacturing	54
E	Transportation, Communications, Electric, Gas, and Sanitary Services	28
G	Retail Trade	2
H	Finance, Insurance, and Real Estate	4
Total Announcement Events		323

Table 6 presents descriptive statistics for each corporation associated with an individual press release announcement event identifying a corporate investment in privacy, discovered during the data identification and data collection processes, along with the number of announcement events associated with each identified corporation included in the final data sample.

Table 6

Final Sample Set – Announcement Event Breakdown (by Corporation)

#	Corporation	# of Events	#	Corporation	# of Events
1	Google Inc.	69	**39**	Harris Corp.	2
2	Microsoft Corp.	19	**40**	Xerox Corp.	1
3	Ebay Inc.	2	**41**	Apple Inc.	31
4	Comcast Corp.	5	**42**	Equifax Inc.	2
5	AT&T Inc.	6	**43**	SalesForce Inc.	3
6	IBM Inc.	5	**44**	Oracle Inc.	1
7	Facebook Inc.	67	**45**	Delta Air Lines	3
8	Verizon Comm.	6	**46**	Blackrock Income Growth Inv	1
9	AOL	1	**47**	Virtru Inc.	1
10	Regeneron Pharmaceuticals	1	**48**	Gartner Inc.	1
11	Target Inc.	2	**49**	Twitter Inc.	8
12	CHE Trinity Health	1	**50**	LifeLock Inc.	1

13	Boeing Co.	1	**51**	Mattel Inc.	2
14	Netflix Inc.	2	**52**	Box Inc.	1
15	Accenture Inc.	1	**53**	VeriSign Inc.	1
16	Cerner Innovation Inc.	2	**54**	Tata Consultancy Serv Inc.	1
17	Taser International	1	**55**	PayPal Inc.	2
18	8x8 Inc.	1	**56**	Hewlett Packard (HP)	2
19	PHT Corporation	1	**57**	WhatsAp (Facebook)	5
20	Instagram (Facebook)	1	**58**	Yahoo! Inc.	9
21	Varonis	1	**59**	Adobe Systems Inc.	2
22	GE Healthcare	2	**60**	Amazon Inc.	13
23	NextGen Healthcare	1	**61**	Honeywell Inc.	1
24	Brocade	1	**62**	Ooma Inc.	1
25	Aon Plc.	1	**63**	Research In Motion (RIM)	1
26	CapSpeciality	1	**64**	Dish Network	1
27	Navigant Consulting	1	**65**	Constellation Research	1
28	Synchronoss Tech Inc.	1	**66**	Commvault (Data Platform)	1
29	Bell Mobility	1	**67**	Intuit Inc.	1
30	Sony Corp.	2	**68**	Mercury Inc.	1
31	FireEye	1	**69**	CenturyLink Inc.	1
32	Hanover	1	**70**	Charter Comm.	1
33	Liquidity Services Inc.	1	**71**	Sprint/Nextel	1
34	AVG Inc.	2	**72**	Spectrum (Time Warner)	1
35	3M	1	**73**	Marriott Inc.	1
36	Quest Diagnostics Inc.	1	**74**	Visa Intl. Inc.	1
37	Bottomline Technologies	1	**75**	JetBlue Inc.	1
38	Pure Storage	1			

4.4 Data Analysis

The objective of this research investigation was to examine the potential financial implication that corporate investments in privacy had on the overall stock market value of the associated corporation. Furthermore, it was of additional research interest to also determine if any industry benefitted the most from investing in privacy, whether or not corporations were penalized financially for *not investing* in privacy, and lastly if there existed any financial incentives for corporations associated with *proactively* investing in

privacy when compared to *reactively* investing in privacy, or to negative privacy news. To achieve these research goals, it was necessary to break the final sample data set into several data set groupings. Each individual data set required an independent event study test, with both parametric (StdCsect-Z) and non-parametric (Generalized Sign-Z) testing performed using the Eventus® software suite over the designated 3-Day event window.

As discussed in Chapter 3, the Eventus® software suite (Cowan, 2007) was used to calculate results for all the advanced mathematical formulas necessary within this research investigation, as well as the University of Chicago's CRSP database for determining all parameter estimates needed for calculating required variable input. Using the designated input variables, Mean Cumulative Abnormal Return (Mean CAR) results were presented for the total data set on the announcement event date ($t = 0$), the day *before* the event date ($t = -1$), and the day *after* the event date ($t = +1$) for each corporation with a press release announcement event identifying a corporate investment in privacy. Mean CAR was determined by adding all of the individual CAR results then dividing by the number of corporations in the sample (323). The number of announcement events identifying a positive or negative financial impact are presented, along with p-value (probability) and z-value (standard deviation: < 0 = less than Mean CAR; > 0 = greater than Mean CAR) results indicate significance of the results obtained.

Once average daily market price was determined for each identified corporation, *Abnormal Returns* (*AR*) were calculated using the CAPM-based MM. Corporate stock market *AR* is the difference between expected daily stock return price and actualized returned stock market price after the announcement event was disclosed. Abnormal stock returns were computed by subtracting raw returns around the event date from the MM

expected returns… with the magnitude of difference providing a quantifiable measure of the impact of the announcement event on firm value (Benbunan-Fich & Fich, 2004). After computing *AR* for each corporation on the event date, *AR, Cumulative Abnormal Return* (CAR) and *Average Cumulative Abnormal Return* (ACAR) were then calculated for each corporation over the 3-Day event window (t = -1, t = 0, t = 1).

The original intention during research design and methodology was to use the Patell-Z test due to it being a stalwart and gold standard testing methodology within the event study literature and research community. However, additional event study research into ensuring the most accurate results were obtained when using the Eventus® software suite for event study testing highlighted a more robust testing method available within Eventus®, known as the *Standardized Cross-Sectional Test* (StdCsect) (aka BMP test) (Boehmer et al.,1991). As a more suitable test, the BMP test was used for all statistical testing and in substitute for the Patell-Z testing method.

Under the original Patell-Z test (Pattell, 1976), the "…standardized abnormal return test of the null hypothesis that the mean abnormal return is zero" (Cowan, 2020). While the Patell-Z test has important strengths that allow its use extensively within event study research, the original form Patell-Z test (1976) has subsequently been improved and updated by various researchers and academics. The most notable, and most recent version of the upgraded Patel test by Brown & Warner (1980; 1985), is recognized in academia as the BW test. In their updated version of the Patell-Z test, known colloquially as the BW test, researchers Brown & Warner (1980, 1985) report "… simulation evidence that the test is well specified in random samples of actual security returns. Further, they show that the Patell test greatly improves power to detect an

abnormal return (artificially induced for the simulations) by making use of firm-specific variance estimates" (Cowan, 2020). It is noted, however, that their research also reports a "… variance increase on the event date can seriously bias the Patell test" (Cowan, 2020). Issues relating to the potential harm to results caused by the increased return variances around announcement events of interest have been reported as early as Beaver (1968).

Using the StdCsect (BMP) method in place of the standard Patell-Z test option automatically includes the SERIAL option for all results. In a simplistic nature, the BMP method is an enhanced version of the original Patell-Z (1976) test. One of the benefits of using the BMP test is increased study robustness over the traditional BW test. The BMP test is an "…extension of the Patell-Z test, the standardized cross-sectional test, which brings in cross-sectional variance information to correct for variance increases. BMP provides Patell-type simulation evidence that the standardized cross-sectional test is robust to event-date variance increases. (Cowan, 2020). This sentiment was echoed in research by Higgins and Peterson (1998) who conducted simulations while using empirical distribution functions to equalize power under the null hypothesis across tests. In direct comparison to the BW test, reseach results support the overall sense of superiority of using the BMP standardized cross-sectional test.

Harrington & Shrider (2007) also provide a more rigorous analytical foundation for the BMP standardized cross-sectional test. The authors report "… additional simulation evidence of heteroskedasticity-related biases of the Patell-Z test that the standardized cross-sectional test avoids" (Cowan, 2020). Furthermore, the author and creators of the BMP test, Marks & Musumeci, support Harrington and Shrider's 2007 research and recommend that researchers always use the BMP standardized cross-

sectional BMP test in direct preference to the Patell-Z test (Cowan, 2020). In addition to full use support from the creator of the Eventus® software suite, Arnold Cowan, the BMP testing methodology as a superior testing option when compared to the Patell test (1967) has been directly supported with research evidence by Beaver (1968), Boehmer et al. (1991), Campbell et al. (2010), Cowan (1993), Dodd & Warner (1983), Graham et al. (1996), Harrington & Shrider (2007), Harvey (2017), Higgins & Peterson (1998), Karolyi (2011), Kolari & Pynnönen (2010), Leamer (1983), and Mikkelson & Partch (1988).

Following traditional event study and Event Study Methodology (ESM) testing criterion, both *parametric* tests and *nonparametric* tests were used ascertain the significance of the data results obtained within this research, as well as ensure the robustness of the research investigation. The parametric test used was the *Standardized Cross-Sectional* (StdCsect-Z Test) (aka BMP test) (Boehmer et al.,1991), in place of the more traditional Patell-Z test (1976); the nonparametric test used was the *Generalized Sign Test* (GST). The StdCsect Z-test statistic was used to assess whether or not the Average Cumulative Abnormal Return (ACAR), Mean CAR, was significantly different from zero, its expected value (McWilliams & Siegel, 1997). Furthermore, according to Im et al. (2001), the significance of the abnormal return based on the Z-statistic test allows the researcher to infer that the privacy investment announcement events have a significant impact on the market value of the associated firm (Loderer & Mauer, 1992; McWilliams & Siegel, 1997). This was necessary to test the null hypothesis, as well as to test all hypotheses posited within this research using the final data sample of 323 identified press release announcement events relating to corporate investments in privacy.

4.5 Findings

The final sample set is comprised of 323 individual press release announcement events relating to a corporate investment in privacy. Table 7 presents individual test results from the event date ($t = 0$) and the entire 3-Day event window ($t = -1$, $t = 0$, $t = 1$).

Table 7

Complete Data Sample Set – Eventus®
CAR Results: 3-Day Event Window (t = -1 through t =1)

		Market Reaction						
	n	Mean CAR	POS (+)	*NEG* (-)	StdCsect-z	*p*-value	Generalized Sign-z	*p*-value
Privacy Events - Full Sample (*t* = 0)	323	-0.20%	162	161	-1.282	0.0999	0.724	0.2346
Day (*t* = -1)	323	-0.04%	153	170	-0.581	0.2805	-0.278	0.3904
Day (*t* = 0)	323	-0.16%	146	177	-1.479	0.0696	-1.058	0.1451
Day (*t* = +1)	323	0.01%	163	160	0.429	0.3341	0.835	0.2018

Note: Symbols (, <, <<, <<< or), >, >>, >>> indicate direction and significance of a generic one-tail generalized sign test at 0.10, 0.05, 0.01 and 0.001 levels

The final data sample set of 323 individual corporate announcement events was examined to determine potential financial implications that a press release announcement event identifying a corporate investment in privacy might have on the overall stock market value of the associated corporation. Analysis of the final data sample revealed Mean Cumulative Abnormal Return (Mean CAR) to be different from zero and negative -0.20% (rejecting the null hypothesis ($CAR \neq 0$). CAR results indicate a negative financial impact to overall stock market value; however, the financial impact is not statistically significant. In addition, the overall sample is statistically significant based on an observed StdCsect *p*-value of 0.09 ($p < 0.10$) at traditional statistical significance testing levels (Appendix L – Table 25).

Results indicate a negative financial impact to overall corporate stock market value from the corporate announcement events relating to corporate investments in privacy. In addition, an observed parametric (StdCsect) *p*-value of 0.09 ($p < 0.10$) indicates a weak relationship existing between announcement events related to corporate investments in privacy and the overall reduction in corporate stock market value for associated corporations (Appendix M – Table 26). Further evidence supporting this position is identifiable in the manner in which the economic impact to overall corporate stock market value was nearly equally distributed between POS (+) financial impact - 162 (50.15%), and NEG (–) financial impact - 161 (49.85%), from the final data set of 323 announcement events.

The final data set included 323 individual corporate announcement events from 75 different corporations. Individual statistics with resultant data for each announcement event associated with a corporate investment in privacy is listed in Table 8.

Table 8

Individual Corporate Announcement Events – Eventus®
CAR Results: 3-Day Event Window (t = -1 through t =1)

		Market Reaction						
	n	Mean CAR	POS (+)	*NEG* (-)	StdCsect-z	*p*-value	Generalized Sign-z	*p*-value
Google	69	0.06%	36	33	0.497	0.3097	0.804	0.2107
Microsoft	19	0.40%	13	6 >	1.660	0.0485	1.724	0.0424
Ebay	2	1.06%	1	1	0.452	0.3255	0.157	0.4378
Comcast	5	-.031%	2	3	-0.546	0.2924	-0.229	0.4094
AT&T	6	-0.08%	3	3	-0.262	0.3965	-0.082	0.4674
IBM	5	-0.27%	3	2	-0.770	0.2207	0.385	0.3502
Facebook	67	-0.34%	28	39	-1.084	0.1393	-1.140	0.1271
Verizon	5*	0.32%	3	2	0.336	0.3685	0.385	0.3502
AOL	1	0.96%	1	0	0.784	0.2165	1.094	0.1369
Regeneron	1	-1.69%	0	1	-0.480	0.3158	-0.869	0.1926

Target	2	-0.49%	0	2 (	-3.952	< .0001	-1.428	0.0766
CHE Trinity	1	0.63%	1	0	0.276	0.3913	1.000	0.1587
Boeing	1	-1.84%	0	1	-1.077	0.1408	-0.990	0.1611
Netflix	2	-5.46%	0	2	-1.246	0.1065	-1.273	0.1016
Accenture	1	0.14%	1	0	0.102	0.4593	1.140	0.1272
Cerner	2	1.10%	2	0)	1.638	0.0508	1.525	0.0637
Taser Intl	1	2.50%	1	0	0.534	0.2967	1.151	0.1248
8x8	1	-0.77%	0	1	-0.220	0.4130	-0.932	0.1756
PHT Corp	1	0.46%	1	0	0.384	0.3507	0.895	0.1853
Instagram	1	1.30%	1	0	0.436	0.3313	1.020	0.1538
Varonis	1	2.58%	1	0	0.412	0.3403	1.151	0.1248
GE Health	2	-0.22%	1	1	-0.225	0.4110	0.114	0.4548
NextGen	1	2.10%	1	0	0.905	0.1828	1.083	0.1393
Brocade	1	-0.74%	0	1	-0.364	0.3578	-0.923	0.1780
AON Plc	1	-1.79%	0	1	-1.402	0.0805	-0.980	0.1635
CapSpecialty	1	-1.40%	0	1	-1.082	0.1396	-0.961	0.1683
Navigant	1	0.42%	1	0	0.222	0.4120	0.980	0.1635
Synchronoss	1	1.52%	1	0	0.450	0.3265	1.051	0.1466
Bell Mobility	1	-0.78%	0	1	-0.612	0.2702	-0.980	0.1635
Sony Corp	2	-1.28%	1	1	-0.543	0.2935	0.078	0.4690
FireEye	1	-4.99%	0	1	-1.104	0.1348	-1.000	0.1587
Hanover	1	1.75%	1	0	1.249	0.1058	1.117	0.1320
Liquidity	1	0.63%	1	0	0.127	0.4496	0.970	0.1659
AVG Inc	2	1.82%	2	0)	1.582	0.0569	1.414	0.0787
3M	1	-1.12%	0	1	-0.971	0.1657	-1.020	0.1538
Quest Diag	1	0.18%	1	0	0.109	0.4568	1.010	0.1562
Bottomline	1	0.47%	1	0	0.255	0.3995	1.083	0.1393
Pure Storage	1	-0.89%	0	1	-0.236	0.4067	-0.905	0.1829
Harris Corp	2	-0.43%	1	1	-0.210	0.4168	-0.021	0.4915
Xerox Corp	1	-1.13%	0	1	-0.607	0.2721	-0.860	0.1950
Apple Inc	31	-0.16%	11	20 (	-0.624	0.2663	-1.429	0.0766
Equifax Inc	2	-12.11%	0	2 (	-1.083	0.1393	-1.414	0.0787
SalesForce	3	-0.91%	2	1	-0.280	0.3898	0.694	0.2437
Oracle Inc	1	-8.98%	0	1	-5.306	< .0001	-1.000	0.1587
Delta Air	3	-0.62%	0	3)	-1.908	0.0282	-1.620	0.0526
Blackrock	1	-0.34%	0	1	-0.239	0.4057	-0.961	0.1683
Virtru	1	0.48%	1	0	0.095	0.4620	1.051	0.1466
Gartner Inc	1	-0.28%	0	1	-0.153	0.4392	-1.000	0.1587
Twitter Inc	8	-1.37%	2	6)	-2.043	0.0205	-1.285	0.0994

LifeLock Inc	1	1.73%	1	0	0.235	0.4070	1.020	0.1538
Mattel Inc	2	1.11%	2	0)	2.867	0.0021	1.479	0.0695
Box Inc	1	0.41%	1	0	0.096	0.4618	1.041	0.1490
VeriSign Inc	1	-1.13%	0	1	-0.629	0.2648	-1.041	0.1490
Tata Consult	1	1.76%	1	0	0.249	0.4019	0.990	0.1611
PayPal Inc	2	1.79%	1	1	0.789	0.2152	-0.021	0.4915
HP	2	-1.38%	1	1	-0.909	0.1818	-0.007	0.4972
WhatsApp	5	-0.98%	2	3	-0.822	0.2057	-0.225	0.4111
Yahoo! Inc	9	0.02%	6	3	-0.010	0.4960	1.199	0.1152
Adobe Sys	2	0.83%	1	1	0.577	0.2819	-0.064	0.4746
Amazon Inc	13	0.62%	9	4)	2.723	0.0032	1.612	0.0535
Honeywell	1	0.60%	1	0	0.483	0.3146	0.961	0.1683
Ooma Inc	1	0.45%	1	0	0.152	0.4395	1.020	0.1538
RIM	1	0.75%	1	0	0.120	0.4523	1.062	0.1441
DishNetwork	1	-2.43%	0	1	-1.063	0.1438	-0.951	0.1708
Constellation	1	-1.86%	0	1	-0.396	0.3459	-0.860	0.1950
Commvault	1	0.38%	1	0	0.194	0.4230	0.942	0.1732
Intuit Inc	1	0.28%	1	0	0.213	0.4156	1.073	0.1417
Mercury Inc	1	0.55%	1	0	0.316	0.3759	0.961	0.1683
CenturyLink	1	2.59%	1	0	1.108	0.1339	1.062	0.1441
Charter	1	-0.45%	0	1	-0.209	0.4173	-0.970	0.1659
Sprint/Nextel	1	0.23%	1	0	0.111	0.4559	1.073	0.1417
Spectrum	1	0.79%	1	0	0.395	0.3465	1.030	0.1514
Marriott Inc	1	1.13%	1	0	0.646	0.2592	0.932	0.1756
Visa Intl	1	-1.17%	0	1	-0.980	0.1635	-1.041	0.1490
JetBlue Inc	1	-1.02%	0	1	-0.466	0.3206	-0.886	0.1877

Note: Symbols (, <, <<, <<< or), >, >>, >>> indicate direction and significance of a generic one-tail generalized sign test at 0.10, 0.05, 0.01 and 0.001 levels

In Table 9, from the 75 corporations associated with the 323 corporate events, 11corporations were observed with either statistically significant parametric or nonparametric test results. Eight corporations were observed with statistically significant results from *both* parametric and nonparametric testing; three corporations were observed with statistically significant results from *either* parametric or nonparametric testing.

Table 9

Eventus® – CAR Results: Significant at p < 0.10, 0.05, 0.01, or 0.001
3-Day Event Window (t = -1 through t =1)

	n	Market Reaction			StdCsect-z	*p*-value	Generalized Sign-z	*p*-value
		Mean CAR	POS (+)	*NEG* (-)				
Microsoft	19	0.40%	13	6 >	1.660	0.0485	1.724	0.0424
Target	2	-0.49%	0	2 (	-3.952	< .0001	-1.428	0.0766
Cerner	2	1.10%	2	0)	1.638	0.0508	1.525	0.0637
AVG Inc	2	1.82%	2	0)	1.582	0.0569	1.414	0.0787
Apple Inc	31	-0.16%	11	20 (	-0.624	0.2663	-1.429	0.0766
Equifax Inc	2	-12.11%	0	2 (	-1.083	0.1393	-1.414	0.0787
Oracle Inc	1	-8.98%	0	1	-5.306	< .0001	-1.000	0.1587
Delta Air	3	-0.62%	0	3)	-1.908	0.0282	-1.620	0.0526
Twitter Inc	8	-1.37%	2	6)	-2.043	0.0205	-1.285	0.0994
Mattel Inc	2	1.11%	2	0)	2.867	0.0021	1.479	0.0695
Amazon Inc	13	0.62%	9	4)	2.723	0.0032	1.612	0.0535

Note: Symbols (, <, <<, <<< or), >, >>, >>> indicate direction and significance of a generic one-tail generalized sign test at 0.10, 0.05, 0.01 and 0.001 levels, respectively

In a manner similar to the *Privacy Paradox* phenomenon discovered by researchers Dinev & Hart (2006), in which consumers express a voluntary willingness to exchange personal privacy for goods / services, separate data sets were created to determine whether or not privacy as an individual right (construct) has gained or lost support over the 5-Year time period investigated within this research, using separate time period data subsets: (2013-2015) and (2016-2018).

Table 10 presents descriptive statistics for each corporation associated with an individual press release announcement event identified from 2013-2015.

Table 10

Privacy Events (2013-2015) – Eventus®
CAR Results: 3-Day Event Window (t = -1 through t =1)

	n	Market Reaction			StdCsect-z	*p*-value	Generalized Sign-z	*p*-value
		Mean CAR	POS (+)	*NEG* (-)				
Privacy Events (2013-2015)	160	-0.13	75	85	-0.098	0.4608	-0.032	0.4871

Note: Symbols (, <, <<, <<< or), >, >>, >>> indicate direction and significance of a generic one-tail generalized sign test at 0.10, 0.05, 0.01 and 0.001 levels

The data statistics presented in Table 10 represent the analysis of the sample subset of 160 individual announcement events from 2013-2015. Mean CAR was different from zero and negative -0.13% (rejecting the null hypothesis (CAR ≠ 0). Results indicated a negative financial impact to overall stock market value that was not statistically significant. In addition, no statistical significance is evident based on the observed StdCsect *p*-value of 0.4608 and GST *p*-value of 0.4871. These results indicated that while there was a negative financial impact to overall stock market value from the corporate privacy announcement event, the results are not statistically significant and indicate no relationship existing between the corporate announcement event and the overall reduction in corporate stock market value for the associated corporations.

Table 11 presents descriptive statistics for each corporation associated with an individual press release announcement event identified from 2016-2018.

Table 11

Privacy Events (2016-2018) – Eventus® – CAR Results:
3-Day Event Window (t = -1 through t =1)

	n	Market Reaction			StdCsect-z	*p*-value	Generalized Sign-z	*p*-value
		Mean CAR	POS (+)	*NEG* (-)				
Privacy Events (2016-2018)	163	-0.27%	87	76	-1.389	0.0824	1.050	0.1468

Note: Symbols (, <, <<, <<< or), >, >>, >>> indicate direction and significance of a generic one-tail generalized sign test at 0.10, 0.05, 0.01 and 0.001 levels

The data statistics presented in Table 11 represent the analysis of the sample subset of 163 individual announcement events from 2016-2018. Mean CAR was different from zero and negative -0.27% (rejecting the null hypothesis (CAR ≠ 0). Results indicated a negative financial impact to overall stock market value that was not statistically significant. In addition, there is some statistical significance observable in results as denoted by a StdCsect *p*-value of 0.0824 and GST *p*-value of 0.1468. In years 2016-2018, while the overall results indicated that while there was a negative financial impact to overall stock market value from the corporate privacy announcement event, the results are not statistically significant but do indicate some relationship existing between the corporate announcement event and the overall reduction in corporate stock market value for the associated corporations.

Strategic investments maintain the propensity to provide positive or negative financial impact to the associated corporation's stock market value. One important factor to consider when evaluating a potential corporate investment in privacy is the specific industry in which the privacy investment will be made as financial impact from corporate investments in privacy can vary extensively from one industry to another. To determine

if it was more advantageous for any one specific industry to invest in privacy for likely increased corporate stock market value, corporate announcement events were separated into data sets based on US SEC Standard Industrial Classification (SIC) Code Divisions.

Table 12 presents descriptive statistics for each corporation and its associated alignment within its designated US SEC SIC Code Division.

Table 12

SIC Code (by Division) – Eventus®
CAR Results: 3-Day Event Window (t = -1 through t =1)

		Market Reaction						
	n	Mean CAR	POS (+)	*NEG* (-)	StdCsect-z	*p*-value	Generalized Sign-z	*p*-value
Division J - Public Admin	75	-0.40%	32	43	-1.181	0.1188	-1.023	0.1531
Division I - Services	160	-0.10%	93	67 >>	-0.455	0.3247	2.620	0.0044
Division D - Manufacturing	54	-0.24%	23	31	-1.433	0.0759	-0.836	0.2016
Division E - Trans., Comm.	28	-0.14%	12	16	-0.566	0.2859	-0.613	0.2701
Division G - Retail Trade	2	-0.49%	0	2 (	-3.952	< .0001	-1.428	0.0766
Division H - Finance, Ins.	4	-0.01%	2	2	-0.019	0.4926	0.030	0.4880

Note: Symbols (, <, <<, <<< or), >, >>, >>> indicate direction and significance of a generic one-tail generalized sign test at 0.10, 0.05, 0.01 and 0.001 levels

The data statistics presented in Table 12 represent the analysis of the data sample set of 323 individual announcement events after being broken into separate data sets based on US SEC SIC classification code divisions. Each individual division was then analyzed separately to determine if any particular industry benefitted more financially from corporate investments in privacy.

Mean CAR for "Division J" (N = 75) is different from zero and negative -0.40% (rejecting the null hypothesis (CAR ≠ 0). CAR results indicate a negative financial impact to overall stock market value that is not statistically significant ($p < 0.05$). No statistical significance observable in results, denoted by an StdCsect p-value of 0.1188 and a GST p-value of 0.1531, indicating no existing relationship between corporate privacy investment announcement events and the overall reduction in corporate stock market value for associated corporations assigned to US SEC SIC Division J.

Mean CAR for "Division I" (N = 160) is different from zero and negative -0.10% (rejecting the null hypothesis (CAR ≠ 0). CAR results indicate a negative financial impact to overall stock market value that is statistically significant ($p < 0.10$). A strong statistical significance is observable, denoted by a GST p-value of 0.0044, indicating a strong relationship existing between corporate privacy investment announcement events and the overall reduction in corporate stock market value for associated corporations assigned to US SEC SIC Division I.

Mean CAR for "Division D" (N = 54) is different from zero and negative -0.24% (rejecting the null hypothesis (CAR ≠ 0). CAR results indicate a negative financial impact to overall stock market value that is not statistically significant ($p < 0.10$). There is statistical significance observable in the results, denoted by StdCsect p-value of 0.0759 ($p < 0.10$), indicating some relationship existing between corporate privacy investment announcement events and the overall reduction in corporate stock market value for associated corporations assigned to US SEC SIC Division D.

Mean CAR for "Division E" (N = 28) is different from zero and negative -0.14% (rejecting the null hypothesis (CAR ≠ 0). CAR results indicate a negative financial

impact to overall stock market value that is not statistically significant ($p < 0.10$). No statistical significance observable in results, denoted by an StdCsect *p*-value of 0.2859 and a GST *p*-value of 0.2701, indicating no relationship existing between corporate privacy investment announcement events and the overall reduction in corporate stock market value for associated corporations assigned to US SEC SIC Division E.

Mean CAR for "Division G" ($N = 2$) is different from zero and negative -0.49% (rejecting the null hypothesis (CAR $\neq 0$). CAR results indicate a negative financial impact to overall stock market value that is not statistically significant ($p < 0.10$). Strong statistical significance is observable in results, denoted by StdCsect *p*-value of 0.001 ($p < 0.001$) and a GST *p*-value of 0.0766 ($p < 0.10$), indicating a strong relationship existing between corporate privacy investment announcement events and the overall reduction in stock market value for corporations assigned to US SEC SIC Division G.

Mean CAR for "Division H" ($N = 4$) is different from zero and negative -0.01% (rejecting the null hypothesis (CAR $\neq 0$). CAR results indicate a negative financial impact to overall stock market value that is statistically significant ($p < 0.05$). No statistical significance observable in results, denoted by an StdCsect *p*-value of 0.4926 and a GST *p*-value of 0.4880, indicating no relationship existing between corporate privacy investment announcement events and the overall reduction in corporate stock market value for associated corporation assigned to US SEC SIC Division G.

Based on overall results for each US SEC SIC Division within the data set, Division I (Services) had the most statistically significant results ($p = 0.01$) and largest volume of announcement events associated with a positive financial impact (58.13%). Division E (Transportation, Communications, Electric, Gas, and Sanitary Services)

followed with 42.86% events indicating a positive financial impact, however, results were not statistically significant.

This research also explored whether there existed any financial incentives motivating corporations to *proactively* invest in privacy, compared to corporations *reactively* investing in privacy *after* a privacy incident. Corporations identified as having taken a proactive approach to investing in privacy, as well as corporations reacting negatively to privacy incidents, were each separated into their own data set and examined to determine if either were rewarded by shareholders for their investment strategy.

Event study research identified within the extant literature indicated minimal financial interest in corporate investments in privacy. To help address this issue, separate testing and analysis was conducted to determine whether or not corporations were motivated by economic incentives, POS + (reward), or NEG – (penalized), based on the nature and timing of the corporate investment in privacy.

Table 13 presents descriptive statistics for each press release announcement event identified as a corporate investment in privacy made *proactively*, in an effort to *increase* their privacy position, or to harden their privacy footprint; POS (+) Privacy Events.

Table 13

POS (+) Privacy Announcement Events – Eventus®
CAR Results: 3-Day Event Window (t = -1 through t =1)

		Market Reaction						
	n	Mean CAR	POS (+)	*NEG* (-)	StdCsect-z	*p*-value	Generalized Sign-z	*p*-value
POS (+) Privacy Events	51	0.01%	28	23	-0.345	0.3651	0.867	0.1930

Note: Symbols (, <, <<, <<< or), >, >>, >>> indicate direction and significance of a generic one-tail generalized sign test at 0.10, 0.05, 0.01 and 0.001 levels

The data statistics presented in Table 13 represent the analysis of the data sample set of 51 individual "proactive" announcement events. Mean CAR was different from zero and positive 0.01% (rejecting the null hypothesis (CAR ≠ 0). CAR results indicated a positive (neutral) financial impact to overall stock market value that was statistically significant (p = < 0.01). In addition, there was no statistical significance observable in results as denoted by a StdCsect p-value of 0.3651 and GST p-value of 0.1930. Overall, results for corporations making proactive investments in privacy indicated their action was positively received by shareholders (positive increase in overall stock market value) and statistically significant. However, results further indicated no relationship existing between corporate announcement events and the overall reduction in corporate stock market value for the associated corporations.

Corporate press release announcement events identifying corporate investments in privacy made *reactively,* after a privacy (security) breach or incident, negative in nature, or relating to a negative privacy situation made public through a negative press event, were grouped as NEG (-) Privacy Events. Table 14 presents announcement events identified as NEG (-) Privacy Events along with descriptive statistics and testing results.

Table 14

NEG(-) Privacy Announcement Events – Eventus®
CAR Results: 3-Day Event Window (t = -1 through t =1)

		Market Reaction						
	n	Mean CAR	POS (+)	*NEG* (-)	StdCsect-z	*p*-value	Generalized Sign-z	*p*-value
NEG (-) Privacy Events	46	-0.51	19	27	-0.957	0.1692	-0.924	0.1778

Note: Symbols (, <, <<, <<< or), >, >>, >>> indicate direction and significance of a generic one-tail generalized sign test at 0.10, 0.05, 0.01 and 0.001 levels

The data statistics presented in Table 14 represent the analysis of the data sample set of 46 individual "reactive" announcement events. Mean CAR was different from zero and negative -0.51% (rejecting the null hypothesis (CAR ≠ 0). CAR results indicated a negative financial impact to overall stock market value that was not statistically significant. In addition, no statistical significance was observable in results as denoted by a StdCsect *p*-value of 0.1692 and GST *p*-value of 0.1778. Overall, for corporations making *reactive* investments in privacy, after a privacy breach has occurred, or after a negative privacy-related incident, results indicated their action was negatively received by shareholders (decrease in overall stock market value) but not statistically significant.

These results indicated that while average financial impact to overall stock market value was negative, there was no observable relationship existing between corporate privacy announcement events and the overall reduction in corporate stock market value for the associated corporations when reacting to privacy issues "after the fact" or for "failing to invest in privacy."

4.5.1 Hypotheses Testing – Results and Analysis

Under the null hypothesis, abnormal returns are independent, identically distributed, and normal with a mean of zero (0); the variance given by the variance of abnormal returns over the identified estimation period (Acquisti et al., 2006). Under the null hypothesis of zero expected abnormal returns, *Z* is approximately unit normally distributed (Hovav & D'Arcy, 2003), as illustrated in research presented by Loderer & Mauer (1992). The null hypothesis that corporate Abnormal Returns (*ARs*) are not significantly different from zero (0) was rejected in this research (CAR ≠ 0). It was expected that observable corporate AR's will be significantly different from zero (0).

Table 15 presents the hypotheses posited within this research investigation, along with results obtained based on the statistical testing and analysis.

Table 15

Hypotheses Results

		Result
Hypothesis: H_0	*Null Hypothesis*	*Rejected*
Hypothesis: H_1 *There is positive capital markets' reaction to proactive corporate announcement events indicating privacy investments to enhance corporate privacy*		*Accepted*
Hypothesis: H_2 *Positive stock market reaction to corporate investments in privacy will be significantly greater in years 2013-2015 when compared to years 2016-2018*		** Partially Rejected*
Hypothesis: H_3 *Stock market reaction from negative privacy incident events will be accepted as financially insignificant based on minimal corporate stock market loss*		*Accepted*

4.6 Summary of Results

The main research objective of this research investigation was to determine the potential financial implication from corporate investments in privacy. Conducting an event study to examinate corporate investments in privacy allowed the author to better understand *why* corporations are not investing in privacy, as well as identify the existence of financial ramifications from corporate investments in privacy.

In this investigation, it was hypothesized that *there is positive capital markets' reaction to proactive corporate announcement events indicating privacy investments to enhance corporate privacy* (H_1). To test this hypothesis, two different data subsets were created and tested separately, then compared to one another to discern the differences. One data subset was comprised of corporations identified as having introduced privacy investments "proactively," and the second data subset was comprised of corporations identified as having introduced privacy investments "reactively," or corporations

associated with a negative privacy incident (breach). Results indicated that corporations associated with *proactive* corporate investments in privacy achieved an overall positive financial stock market reaction; 54.90% of individual announcement events within the "proactive" data subset had a direct, positive financial impact to overall corporate stock market value. Conversely, corporations associated with *reactive* corporate investments in privacy, or announcement events caused by a negative privacy incident (breach), achieved an overall negative financial stock market reaction; only 41.30% of the individual announcement events within the "reactive" data subset had a direct, positive financial impact to overall corporate stock market value.

It was also hypothesized that p*ositive stock market reaction to corporate investments in privacy will be significantly greater in years 2013-2015 when compared to years 2016-2018* (*H_2*). This hypothesis was partially rejected as it was unable to be accepted or rejected completely. This hypothesis was evaluated by independently assessing two separate data subsets, announcement events from 2013-2015 and announcement events from 2016-2018, to determine the presence of any observable differences in the resultant data. The data revealed a negative financial impact to the corporations' overall stock market value from the corporate investment in privacy. However, where the results from 2013-2015 were not statistically significant, the results from 2016-2018 were statistically significant as denoted by a StdCsect *p*-value of 0.0824 ($p < 0.10$). In years 2016-2018, however, while there was a negative financial impact to overall corporate stock market, the results were statistically significant. This indicated some relationship existing between corporate privacy announcement events and the overall reduction in corporate stock market value for the associated corporations.

The research further hypothesized that *stock market reaction from negative privacy incident events will be accepted as financially insignificant based on minimal corporate stock market loss* (*H_3*). This hypothesis was accepted. To test this hypothesis, a data subset was created and comprised of corporations identified as having introduced privacy investments "reactively," or those corporations whose announcement events were associated with a negative privacy incident (ex. lawsuit, breach). Results indicated that corporations introducing investments in privacy reactively, or due to a negative privacy incident, saw an overall negative financial stock market impact, with only 41.30% announcement events directly having a positive financial impact.

Overall, corporations making proactive investments in privacy were positively rewarded by shareholders through increased overall stock market value with results that were statistically significant. However, results also indicated there was no observable relationship existing between corporate privacy announcement events and the overall increase in corporate stock market value for the associated corporations.

Corporations making reactive investments in privacy were negatively punished by shareholders through decreased overall stock market value. Similarly, results indicated there was no observable relationship existing between corporate privacy announcement events and the overall reduction in corporate stock market value for the associated corporations when reacting to privacy issues "after the fact" or for "failing to invest in privacy."

Chapter 5

Conclusions, Implications, Recommendations, and Summary

5.1 Introduction

Corporations recognizing the importance of maintaining profitability long-term are forced to invest strategically based on financial implications. Accordingly, corporations implement investment opportunities based on expected Return on Investment (ROI). Since stock market impact from corporate investments in privacy may be different across industry segments, it is important to identify where corporate investment in privacy offer the highest economic *Return on Investment* (ROI) (Hinz et al., 2014; Huang & Behara, 2013). Furthermore, when evaluating non-tangible goods and services, such as privacy, traditional tools available to decision-makers when attempting to ascertain potential ROI are unable to be used. Traditional event study literature highlights this fact as corporations and research academics have been unable to accurately identify true financial implications involving both tangible and intangible costs. Hovav & D'Arcy (2003) notes that "…potential intangible losses such as "loss of competitive advantage" and "loss of reputation" (D'Amico, 2000) are not included because intangible costs are not directly measurable." This has had a noticeably negative affect on corporate investments in privacy. Review of the extant body of privacy and event study literature revealed an observable gap relating to reduced research interest by academics in parallel with minimal investment interest by corporations. This event study investigation helps bridge this research gap and makes an academic contribution by

presenting quantitative evidence identifying the financial impact to overall corporate stock market value from corporate investments in privacy.

Through the use of Event Study Methodology (ESM), the author was able to: 1) evaluate the financial impact that corporate investments had on overall corporate stock market value of the associated corporation, 2) identify whether any specified industry is more likely to benefit from corporate investments in privacy, 3) discover why corporations are *not investing in privacy*, and 4) identify economic implications associated with financial incentives motivating corporate investments in privacy.

5.2 Conclusions

The sample data set, containing 323 individual press release announcement events from 75 different corporations, was initially tested as a whole (*Final Sample Set* - FSS). Following that, each individual corporation making up the FSS was then tested within unique data subsets to identify results based on different data criterion. This was necessary to address both the research questions and the posited hypotheses within.

Analysis performed on the resultant data in this research confirmed there is negative financial impact to overall stock market value (Mean CAR -0.20%) associated with press release announcement events identifying corporate investments in privacy, but results were not statistically significant. However, while Mean CAR results were negative and not statistically significant, the associated StdCsect *p*-value 0.0999 was statistically significant ($p < 0.01$), indicating an existing relationship between corporate privacy announcement events and the overall reduction in corporate stock market value for the associated corporation.

Data subset testing was necessary in order to answer a major research question within this investigation; *why* are corporations are *not investing in privacy*? Addressing this question required supplementary analysis to discern *i*) whether or not stock market reaction observed from negative privacy incident events was accepted as financially insignificant based on minimal corporate stock market loss, *ii*) whether or not there exists financial motives encouraging "proactive" corporate investments in privacy, *iib*) whether or not there exists "negative" financial motives encouraging corporate investments in privacy, and *iii*) whether or not any specific industry is more likely to benefit from corporate investments in privacy when evaluated against competing industry interests.

As noted, overall results for the FSS indicated announcement events associated with corporate investments in privacy had a negative (NEG -) Mean CAR (-0.20%) and were not statistically significant. An associated StdCsect *p*-value of 0.0999 indicated statistical significance ($p < 0.01$) and suggested an existing relationship between corporate privacy investment announcement events and the reduction in overall corporate stock market value for the associated corporation. Additional breakdown of the data yielded a total of 75 individual corporations comprising the FSS (323 separate press release announcement events). From those 323 announcement events, 97 events (30.03%) were explicitly identified as being either "proactive" or "reactive" (or having a negative connotation based on nature of and/or title of announcement event). Of those 97 events, 51 events (52.58%) from 39 corporations (52%) were identified as "proactive" and had a positive (POS +) financial impact on overall stock market value, while 46 events (47.42%) from 36 corporations (48%) were identified as "reactive" (or having a

negative connotation based on nature of and/or title of announcement event) and had a negative (NEG -) financial impact on overall stock market value.

These results highlight an important conclusion reached in this investigation that helps to better understand *why* corporations are *not investing in privacy*. One important discovery was the minimal presence of financial incentives existing to *motivate* corporate investments in privacy: positive or negative. Corporations not enticed by economic motivation will see no incentive to invest financially into a product or service likely to generate a negative (NEG -) ROI. Moreover, corporations have been hesitant to invest in privacy as limited research conducted to date has all indicated minimal to no financial stock market benefit from corporate investments in privacy.

From the Final Sample Set (FSS) of 323 announcement events, only 51 (15.79%) events were corporate investments in privacy made proactively. This data subset was identified as the most likely category of events to produce the greatest positive financial impact to the associated corporation's overall stock market value. Mean CAR of the 51 individual events in this subset was slightly positive (0.01%) and statistically significant. However, based on both the StdCsect *p*-value of 0.3651 and GST *p*-value of 0.1930 being statistically insignificant, there was no identifiable relationship existing between the corporate privacy announcement events and the overall positive increase in overall corporate stock market value for the associated corporations.

This showcased that while corporations who proactively invested in privacy were economically rewarded by shareholders with a positive increase in overall corporate stock market value, with results identified as statistically significant, there was no identifiable relationship existing between the corporate privacy announcement events and

the overall positive increase in overall corporate stock market value for the associated corporations. It is therefore posited by the author that announcement events relating to proactive corporate investments in privacy were seen accepted by shareholders as inconsequential overall, offering the corporation limited to no long-term financial value.

Another important discovery was made regarding whether or not stock market reaction from negative privacy incident events was accepted as financially insignificant, based on minimal corporate stock market loss. From the Final Sample Set (FSS) of 323 announcement events, 46 (15.79%) events were corporate investments in privacy made "reactively," or having a negative connotation based on nature of and/or title of announcement event. This data subset was identified as the most likely category of events to produce the greatest *negative* financial impact to the associated corporation's overall stock market value. Mean CAR of the 46 individual events in this subset was negative overall (-0.51%), indicating a negative financial impact to overall corporate stock market value, but not statistically significant. In addition, based on both the StdCsect *p*-value of 0.1692 and GST *p*-value of 0.1778 being statistically insignificant, there was no identifiable relationship existing between the corporate privacy announcement events and the overall positive increase in overall corporate stock market value for the associated corporations.

This revealed that corporations reacting to negative privacy incidents, or having negative announcement events associated with investments in privacy, were penalized economically by shareholders with reduced overall corporate stock market value, with results that were identified as not statistically significant, and presented no identifiable relationship existing between the corporate privacy announcement events and the overall

negative reduction in overall corporate stock market value for the associated corporations. It is therefore posited by the author that announcement events relating to reactive corporate investments in privacy, or negative announcement events associated with investments in privacy, were seen accepted by shareholders as inconsequential overall, offering the corporation limited or no long-term financial value.

This research was also interested in discerning whether or not any specific industry is more likely to benefit from corporate investments in privacy when evaluated against competing industry interests. From the Final Sample Set (FSS) of 323 announcement events, each of the different industry divisions were grouped into one of six data subsets (Division J, I, D, E, G, and H). Interestingly, each of the six individual data subset divisions returned a negative Mean CAR value: Division J (-0.40%), Division I (-0.10), Division D (-0.24), Division E (-0.14%), Division G (-0.49%), and Division H (-0.01%), indicating that there was a negative financial impact to overall corporate stock market value for each industry division examined. Of the six Division subset data groups tested, only Division I and Division G identified results that were statistically significant.

Corporations trading in Division I ($N = 160$) had a negative financial impact to their overall stock market value (Mean CAR (-0.10%) that was statistically significant. Results observed with a GST p-value of 0.0044 ($p < 0.05$) were also statistically significant and indicated a relationship existing between the announcement event and the reduced overall corporate stock market value. Corporations trading in Division G had a negative financial impact to their overall stock market value (Mean CAR (-0.49%), and the most statistically significant results with a StdCsect p-value of < 0.0001 and GST p-value of 0.0766 ($p < 0.10$), but Division G contained only 2 corporations ($N = 2$).

Corporations trading in Division H had the least financial impact to their overall stock market value based on having the lowest Mean CAR (-0.01%), but there were only 4 corporations (N = 4) in Division H and the results were not statistically significant. Corporations trading in Division J (N = 75) had a Mean CAR (-0.40%), corporations trading in Division D (N = 54) had a Mean CAR (-0.24%), and Corporations trading in Division E (N = 28) had a Mean CAR (-0.14%). Based on their respective Mean CAR, announcement events in Divisions H, D, and E had negative financial impact to overall corporate stock market values associated with their negative Mean CAR results, but all observed results for both StdCsect and GST p-values were not statistically significant. From the data collected and observed, results were most statistically significant for corporations in Division J. In addition, Division J also presented the highest percentage of announcement events (58.13%) having a positive (POS +) financial impact to overall corporate stock market value than any other Division investigated.

This research also investigated time specific data subsets of corporate privacy announcement events to discern the presence of increased, or decreased, consumer concern for corporate investments in privacy and privacy-related matters over the time period being investigated 2013-2018. From the Final Sample Set (FSS) of 323 announcement events, the data subset group from 2013-2015 contained 160 announcement events with negative (NEG -) Mean CAR (-0.13%). Resultant values related to StdCsect p-value (0.4608) and GST p-value (0.4871) indicated results were not statistically significant and presented no identifiable relationship existing between the corporate announcement events and the associated negative financial impact to overall corporate stock market value. The data subset group from 2016-2018 contained 163

announcement events with negative (NEG -) Mean CAR (-0.27%). Resultant values related to StdCsect *p*-value (0.0824) were statistically significant ($p = <0.10$), with GST *p*-values (0.1468) not statistically significant, indicating that results presented an observable, weak relationship existing between the corporate announcement events and the associated negative financial impact to overall corporate stock market value.

It was also necessary to present statistical information identified within the data sample to make accurate inferences from the observed results. From the total list of 75 corporations responsible for the 323 separate announcement events examined in this investigation, 39 corporations (52%) had positive (POS +) Mean CAR results that identified a positive financial impact to overall corporate stock market value. Conversely, 36 corporations (48%) had negative (NEG -) Mean CAR results that identified a negative financial impact to overall corporate stock market value. Overall results indicated that despite slightly more announcement events having a positive financial impact on overall corporate stock market value (52% v. 48%). However, the negative announcement events were more financially damaging to those affected corporations as evident in negative Mean CAR (-0.20%) for the entire FSS containing all 323 announcement events. In addition, observed results for the entire data sample related to StdCsect *p*-value (0.0999) were statistically significant ($p = <0.10$), but the GST *p*-values (0.2346) were not statistically significant, indicating that results presented an observable, but weak relationship existing between the entire sample of corporate announcement events and the associated negative financial impact to overall corporate stock market value.

Lastly, identification of all statistically significant resultant data observed within the final sample data set allowed the author to further extrapolate additional inferences from the observed results. The FSS was comprised 75 different corporations responsible for the totality of the 323 separate press release announcement events associated with a corporate investment in privacy or a related privacy incident. From the FSS of 323 announcement events, 11 corporations (14.67%) were identified as having 85 announcement events (26.32%) with statistically significant results using either parametric or nonparametric tests implemented. Of those 11 corporations, eight (8) corporations (five positive (POS +) Mean CAR and three negative (NEG -) Mean CAR) were identified as having announcement events (49) with statistically significant results from *both* parametric and nonparametric tests implemented. Only 3 corporations (zero positive (POS +) Mean CAR and three negative (NEG -) Mean CAR) were identified as having announcement events (36) with statistically significant results from either parametric or nonparametric tests implemented.

These results helped illustrate *why* there has been little interest in corporate investments in privacy as there was almost no identifiable relationship existing between the privacy announcement event and the related financial impact to overall corporate stock market value; positive (POS +) or negative (NEG -). Of the 75 total corporations included in this research, eight corporations (10.67%) returned results that were statistically significant for *both* parametric and nonparametric testing criterion for their 49 announcement events (15.17%), and only 3 corporations (4.00%) returned results that were statistically significant for either the parametric or nonparametric testing criterion used for their 36 announcement events (11.15%).

It was extrapolated from these results that regardless of the financial impact to the associated corporations overall stock market value, results were statistically significant for only eleven 11 of the 75 total corporations (14.67%). In addition, only 49 of the 323 total announcement events (15.17%) indicated the presence of a strong relationship, with just 36 of the 323 announcement events (11.15%) indicating the presence of any relationship at all. The existence and strength of the observable relationship represents the statistical significance existing between the corporate announcement event and the financial impact to the corporation's overall stock market value.

Based on the resultant data, announcement events from CenturyLink (*N* = 1) (2.59%), Varonis (*N* = 1) (2.58%), TaserIntl (*N* = 1) (2.50%), NextGen (*N* = 1) (2.10%), and AVG Inc (*N* = 2) (1.82%) had the *largest positive financial impact* to overall corporate stock market value, while announcement events from Equifax (*N* = 2) (-12.11%), Oracle Inc (*N* = 1) (-8.98%), Netflix (*N* = 1) (-5.46%), FireEye (*N* = 1) (-4.99%), and Dish Network (*N* = 1) (-2.43%) had the *most negative financial impact* to overall corporate stock market value (based on Mean CAR calculations performed to determine the financial impact that the corporate announcement event had on the associated corporations overall stock market value; higher Mean CAR = positive (POS +) financial impact, lower (or negative) Mean CAR = negative (NEG -) financial impact).

While these corporations and associated announcement events represented the highest and lowest overall stock market impact, actualized financial implications experienced by the associated corporation may be less dramatic. Only 3 announcement events from 3 corporations in the list of "most impactful" were observed as being

statistically significant. The announcement event from AVG Inc (N = 1) was statistically significant at both StdCsect p-value 0.0569 (p = < 0.10) and GST p-values 0.0787 (p = < 0.10) and indicated a strong relationship existing between the corporate announcement event and positive (POS +) financial impact the event had on overall corporate stock market value. Conversely, while Equifax (N = 1) (GST p-value 0.0787 (p = < 0.10), and Oracle Inc. (N = 1) (StdCsect p-value 0.0001 (p = < 0.0001) announcement events were also both statistically significant, their statistical significance was relegated to only one of the two tests implemented and represented a weak relationship existing between the announcement events and the associated negative financial impact to overall corporate stock market value.

5.2.1. Study Limitations

In this research investigation, an event study was conducted using Event Study Methodology (ESM) to determine the potential financial impact from corporate investments in privacy. As an event study, there are a series of built-in assumptions that must be accepted as study limitations when examining a research problem using this type of methodology. Implementing an event study methodology based on the Efficient Market Hypothesis (EMH) required the author to accept certain stock market assumptions and introduce specified market assertions. First, stock market values for all publicly traded corporations are based on an *efficient market.* EMH asserts that financial markets are informationally efficient, and that stock prices reflect all publicly available information (Goel & Shawky, 2003). Second, based on accepted industry and academic definition (Fama et al., 1969), in an *efficient market* all publicly available information for a corporation being traded on the stock market is incorporated into the corporation's

stock market price. In an *efficient market*, any newly available information will be quickly absorbed by the corporate shareholders then immediately figured into any change in stock market price. Any "adjusted" stock market price will be based on the perceived value of the new information.

In this research, the new information is the corporate privacy investment announcement, with observed changes in overall stock market value being attributed to the perceived value of the privacy investment by the corporation's shareholders. The theory of EMH asserts that "as investors strive to earn profit from market trading, they exploit every useful piece of data, thereby causing market prices to reflect all of the relevant information at any given moment" (Kliger & Gurevich, 2014). Third, any announcement event reflecting a corporate investment in privacy will be associated with some perceived financial value by the corporation's shareholders and reflected in the new overall stock market value for the corporation.

There are also general limitations present within this research based solely on the nature in which an event study investigation is conducted. The limitations identified within this research investigation are similar to imitations identified and accepted in previous event study research conducted by academics across multiple research domains, including: Administrative (Accounting, Finance, Healthcare) (Case & King, 2015; Huang & Behara, 2013; Khansa et al., 2012; MacKinlay, 1997; Schwaig et al., 2006); Technology (and Related) (Dos Santos et al., 1993; Hayes et al., 2001), and Data Protection (i.e., Privacy, Security, Breach) (Andoh-Baidoo & Osei-Bryson, 2013; Bose & Leung, 2014; Campbell, 2003; Chen et al., 2011; Garg et al., 2003; Goel & Shawky, 2009; Hovav & D'Arcy, 2003, 2005). While identified limitations are specific to this

research exploration, the limitations discussed are "… shared limitations common to all event studies and therefore must be interpreted with caution" (Brock, 2012).

Data Collection Limitations

The data collection process employed in this research investigation was thorough and exhaustive yet presented potential imitations, mainly as all data identified for potential sample inclusion were artificially constrained by being limited to only corporate press release announcement events publicly disclosed to the general public.

Data collection was implemented using a newly developed data model known as the *Hybrid Process Model* (HPM); internally designed specifically for use in this event study during data collection. Component construction of the custom HPM included combining the most successful data collection strategies and procedures identified throughout a variety of design models used during previous Information System (IS), Information Technology (IT), Information Security (InfoSec), and related event study research, into a single model (Bharadwaj et al., 2009; Dehning et al., 2004; Guan et al., 2006; Hinz et al., 2014; Im et al., 200; Nicholas-Donald et al., 2011;). Utilization of the HPM allowed successful deployment of effective and efficient data collection methodologies using a single model that ensured both internal and external validity was maintained (Acquisti et al., 2006; Chatterjee et al., 2001; Culnan & Williams, 2009; Dewan & Ren, 2007; Goel et al., 2010; Hovav et al., 2017; Malhotra & Malhotra, 2010).

Similar to the custom Hybrid Process Model (HPM) implemented during data collection, a newly created *Blended Method Approach* (BMA) model was used during data filtering. The BMA model is a simple, easy to use model composed of the most efficient, effective, and accurate individually identified data filtering steps and processes

used in previous event study research (Acquisti et al., 2006; Chatterjee et al., 2001; Culnan & Williams, 2009; Dewan & Ren, 2007; Goel et al., 2010; Hovav et al., 2017; Malhotra & Malhotra, 2010; Nagm & Kautz, 2008). Internally designed and developed for specific use within this event study research, the BMA model was deployed once initial data collection was completed and applied unilaterally during each step of the total data filtering process to filter out invalid and incompatible data.

Deployment of the HPM and BMA models by the author ensured the data sample was thoroughly validated and complete, however, specific criterion used to identify individual corporate data contained within the data sample created potential limitations relative to the manner in which data was identified, and how data was validated for acceptable use within the research. Methodical progression through each of the individual stages included within the data collection / data filtering processes facilitated the identification of theoretical issues that could potentially be construed as a limitation.

Furthermore, event data included within this research investigation was restricted to only corporations actively trading on one of the three permitted United States (U.S.) stock market indexes (NYSE, AMEX, NASDAQ), with historic trading activity available during specified time periods (195-Day estimation window and 3-Day event window).

Depending on an individual's literal interpretation, these "limitations" could be seen as artificially introduced restrictions potentially possessing the ability to limit the applicability of the research results. However, this event study followed traditional design and methodological guidelines espoused in historical event study research literature. Identified limitations were implemented by the author to reduce the overall

scope of the data while simultaneously minimizing the overall volume of potential corporate event data identified for potential inclusion within the final sample data set.

Data Limitations (*Corporate Announcement Events*)

First, all data identified for inclusion during *Data Identification* was discovered only within the ProQuest (PQ) or Business Source Premier (BSP) online database repositories. In addition, all corporate press release announcement events identified must have come directly from a news source; newspaper, news wire, press release, or other news-related medium. Second, *Data Collection* was limited to a 5-Year time period (2013 – 2018) and confined to only search results relating directly to one of six specified keywords used (+ appended (and/or) keywords) – *i*) Privacy, *ii*) Privacy Investment, *iii*) Information Privacy Investment, *iv*) Information System Privacy, *v*) Information System Privacy Investment, and *vi*) Electronic Privacy.

Third, *Data Filtering* reduced the data set to only publicly traded corporations actively trading on one of three accepted United States (U.S.) stock market indices used (NYSE, AMEX, NASDAQ). In addition, only corporations actively traded on one of the three accepted stock market indexes during both the estimation window (195-Day), and event window (3-Day), were included in the data set. Fourth, corporations identified with event data must have an active Standard Industrial Classification (SIC) code, issued by the U.S. Securities and Exchanger (SEC) commission. Fifth, corporations with relevant event data must have historical stock market and corporate financial data available in the University of Chicago's Center for Research in Security Prices (CRSP) database.

Event Study Research Limitations

In addition to previously mentioned potential data identification and data collection limitations, there are also theoretical limitations inherent within the general manner in which event study research investigations are conducted, including research design, methodology, analysis, and testing. While specific limitations discussed by the author within this research are unique to the individual event study investigation presented, all potential limitations discussed are inherent and identifiable within all event study research conducted; past, present, future.

Event study research identified within the extant body of literature revealed no specific set of applicable guidelines having been universally accepted for use when conducting an event study investigation. For example, among event study literature exists varying opinions regarding the specific length of time that should be used for estimation and event window sizes, analysis, testing methodology (Acquisti et al., 2006; Hendricks & Singhal, 1996, 1997), significance levels for hypothesis testing, analysis, and validation, minimum number of individual corporate events, how to account for duplicate data, inclusion of (identifiable) confounding events, etc. As such, individualized results discovered by the author in this research investigation were based on these specific choices made relative to study design, methodology, model, and parameter selection for use in this particular event study research. Different results would have been achieved if different selection choices were made by the author.

The estimation window used in this research, relative to the corporate announcement event date ($t = 0$) was 195-Days (beginning at $t = -200$-Days and ending at $t = -5$-Days *before* announcement event date ($t = 0$) and used *Ordinary Least Squares*

(OLS) linear regression to estimate requisite MM parameters. Literature review of previous IS/IT ESM studies (Dos Santos et al. (1993) and Im et al. (2001), indicated use of a 200-Day (t = -200 Day) estimation window as the most popular when conducting an event study, as indicated in research by Dos Santos et al. (1993) and Im et al. (2001), who both used 200-Day estimation windows.

Based on historical event study literature, a 3-Day event window (-1, 0, 1) was chosen for use as the most appropriate time period to achieve the desired research objectives (t = -1) (1 day *before* event date); t = 0 (event date); and t = 1 (1 day *after* event date). A 3-Day event window (-1, 0, 1) is also the recommended preference of McWilliams & Siegel (1997) as a short event window provides the avenue necessary to notice an immediate corporate stock market impact based on the investment announcement event while limiting potential data degradation from potential corporate data leaks before and after the event date. In alignment with previous IS / IT ESM event study literature, examining stock market data the day *before* the announcement date provided any internally leaked information insiders had access to; while examining stock market data the day *after* the announcement date captured any stock market impact occurring after-market closure the day the investment announcement event was received by the public. In addition, steps were taken by the author to identify and remove both confounding data and duplicate announcement event data surrounding the announcement event date to ensure data accuracy, validity, and to help reduce overall sample clutter.

While both the 195-Day estimation window, and 3-Day event window chosen for use by the author were based on historical event study precedent, the specified lengths of time chosen had an impact on research results. Furthermore, although proactive steps

were taken to limit their impact, the possibility exists that leaked or confounding corporate data events not identified and eliminated were mistakenly included within announcement event sample data that may have impacted study results.

In addition, while all precautions were made by the author to ensure the accuracy of the data, necessary in order to confirm the validity of the resultant analysis, there exists the possibility that not all announcement event data were identified for sample inclusion, or that some of the data included within the sample data set was done so erroneously. In addition, conclusions presented within this research from data analysis were based on the sample examined. The sample size of 323 announcement events (from 75 corporations) is large enough to capture data, conduct statistical testing and analysis, and present reliable results, however 63 of the 75 corporations included were responsible for less than 5 announcement events apiece; 12 corporations were responsible for ≥ 5 announcement events. It was also noted that all observable announcement event results having the most financial impact to overall corporate stock market value (positive and negative) were from corporations associated with less than 5 announcement events; indicating these specific results were extremely limited in nature and could be considered outlier events.

5.3 Implications

Results of this event study have both research and academic implications, across multiple research domains. Results from this research also have implications for the extant body of privacy and event study literature as well. In addition, this research contains implications for corporations interested in better understanding corporate investments in privacy and their associated financial implications to overall corporate stock market value.

5.3.1 Research Implications

The desired goal of event study research is to ascertain the financial impact that an observable, identifiable, and unexpected event had on the associated corporations overall stock market value. Under the accepted assumptions when using an event study, the visible change in stock market value can be attributed to the (unexpected) event of interest being examined. The "observable, identifiable, and unexpected event" in this event study investigation were corporate press release announcement events associated with a corporate investment in privacy. This event study research was designed and conducted to examine the financial impact these announcement events had to overall corporate stock market value for associate corporations.

Event Study Methodology (ESM) has been deployed throughout a variety of research domains, including *Accounting and Finance* (MacKinlay, 1997); *Information Systems* (IS) (Dehning et al., 2003); *Information Technology* (IT) (Dos Santos et al., 1993); *Information Security* (InfoSec) (Hovav et al., 2014, 2017); *Computer Security* (ComSec) (Garg, 2003); and *Internet Security* (IntSec) (Cavusoglu et al., 2004). However, event study research has only been minimally implemented within the privacy and privacy investment domain (Acquisti et al., 2006; Aytes et al., 2006; Hinz et al., 2014; Khansa et al., 2012; Khansa & Liginlal, 2009; Malhotra & Malhotra, 2010; Nicholas-Donald et al., 2011). This event study investigation contributes to the extant body of privacy and event study literature by adding a source of resource reference that addressed an observable gap in research currently receiving little academic interest.

Event Study Methodology (ESM) as a practical research tool within the technology arena gained traction and widespread acceptance after successful research by

Dos Santos et al. (1993). Following their success, researchers subsequently extended the use of ESM across additional technology domains, including Information Systems (IS) (Dehning et al., 2003), Information Technology (IT) (Dos Santos et al., 1993), Information Security (InfoSec) (Hovav et al., 2014,2017), and related domains. While research interest using ESM has grown across the technology spectrum, minimal event study privacy research, using Event Study Methodology (ESM), has been conducted (Acquisti et al., 2006; Aytes et al., 2006; Chai et al., 2010; Khansa & Liginlal, 2009; Malhotra & Malhotra, 2010; Nicholas-Donald et al., 2011; Schwaig et al., 2006). Even less research interest has been expressed in examining the potential financial impact associated with corporate investments in privacy. Moreover, fewer academic studies still have investigated whether there exists a correlation between increased overall corporate stock market value and announcement events identifying corporate investments in privacy (Hinz et al., 2014; Huang & Behara, 2013; Khansa et al., 2012).

The goal of this research objective was to make an academic contribution to the extant body of privacy and event study literature by examining corporate events in privacy. This research conducted an event study to identify the financial implications associated with corporate investments in privacy, as well as determined whether corporate investments in privacy had a financial impact to the associated corporation's overall stock market value. In addition, results of this research helped discern the presence of financial incentives existing motivating corporate investments in privacy, identified whether any specific industry benefitted more from corporate investments in privacy, and helped to better understand *why* corporations *are not* investing in privacy.

Estimation of the financial impact that corporate investments in privacy had on the corporation's overall stock market value was achieved using Event Study Methodology (ESM). ESM was chosen, and successfully implemented, within this research based on its historical use throughout event study literature as the most accurate, robust, and appropriate tool to use when evaluating financial impact that an unexpected, observable event (announcement event) had on a corporation's stock market value.

As a source of research reference, this event study investigation adds to extant body of privacy and event study literature by extending the results identified in previous event study research (Chen et al., 2011; Culnan & Williams, 2009; Ettredge & Richardson, 2003; Gatzlaff & McCullough; 2010; Hinz et al., 2014; Hovav & D'Arcy, 2005). Furthermore, this research simultaneously offers supporting data validation to the power of event study and ESM as a successful tool when measuring financial impact to overall corporate stock market value caused by the introduction of an unexpected, but observable, event (in this research the "event" was the public press release announcement identifying a corporate investment in privacy).

The results and analysis extracted from this research can also be extrapolated, applied, and implemented in whole, or partially, within other academic domains. Furthermore, for generalizability purposes, duplication of the research design, methodology, and data testing methods presented and conducted within this research, using the same data used in the final sample data set, will produce the same results achieved within this research investigation. Lastly, using event study and Event Study Methodology (ESM) allowed the author to successfully complete all stated objectives of this research investigation while addressing research hypotheses and research questions.

5.3.2 Practical Implications

Corporations are forced to maintain a fiduciary responsibility to shareholders requiring a steadfast commitment towards maximized corporate wealth and overall financial standing through increased stock market value. This mandate ensures that all decision making related to potential investment opportunities is codified solely towards increased corporate profits; increased corporate wealth is accepted by corporations as the "… main motivating factor driving investments" (Dardan et al., 2005; Subramani & Walden, 2001). As such, evidentiary support must exist indicating a likely probability of financial success prior to installation and implementation of any investment opportunity within a corporate environment.

It was discovered in the literature review that lack of perceived financial value by corporations is a significant factor contributing to minimal corporate investments in privacy, and reduced event study interest in privacy and privacy investments. As noted, corporate shareholders perceive minimal financial value from corporate investments in privacy (Acquisti et al., 2006; Culnan & Williams, 2009; Dinev & Hart, 2006). This notion was promulgated further by a universal corporate consensus decreeing that stopping the onslaught of continual breach incidents causing corporations huge financial losses from exposed security vulnerabilities was their number one priority. This shift in focus usurped almost the entirety of most corporation's financial investment resource allocation from technology investments towards investments in threat prevention.

Simultaneously, as breach incidents continued to occur, privacy violations were being committed in parallel and also causing corporations huge financial losses (Acquisti et al., 2006; Amerding, 2018; Aytes et al., 2006; Kiesnoski, 2019; Malhotra & Malhotra,

2010; Nicholas-Donald et al., 2011). This realization encouraged corporate acceptance of the concept separating privacy exposure as a secondary concern (identified during security breach incidents) into privacy as a primary, singular, and independent risk construct on its own. Risk assessment is a process of choosing controls based on probabilities of loss (Hovav & D'Arcy, 2003).

Privacy as a separate area of concern necessitated separate consideration for its own dedicated investment resource allocation, requiring the immediate need for an investment-estimate apparatus to help identify the potential financial implications from corporate investments in privacy. However, a major problem facing corporations was understanding how to accurately evaluate the financial impact of corporate investments on stock market value, especially when evaluating corporate investments in privacy (Cate, 2005; Gellman, 2002). Dos Sanots et al. (1993) was the first to recognize this need and subsequently updated EMH into a workable event study model using ESM.

Following the precedent set by Dos Santos et al. (1993) and other research academics, across varying domains, event study research implemented ESM to determine the financial impact of corporate investments in privacy (Acquisti et al., 2006; Culnan & Williams, 2009; Dinev & Hart, 2006; Malhotra & Malhotra, 2010; Nicholas-Donald et al., 2011). To extend this body of event study privacy research, the results of this investigation provide an additional resource for academics and corporations to reference when deliberating potential financial expenditures on corporate investment in privacy. In alignment with previous event study research conducted, results identified within this study presented a negative financial impact to overall corporate stock market value that

was statistically significant with an observable, but weak, relationship existing between corporate privacy announcement events and negative overall stock market impact.

The complete data sample (323 announcement events) of press release announcement events associated with corporate investments in privacy was discovered to have a negative (NEG -) financial impact to overall corporate stock market value that was statistically significant with a StdCsect *p*-value 0.0999 ($p = <0.10$). However, the GST *p*-value (0.2346) was not statistically significant and indicated that while results showed a negative financial impact to overall corporate stock market value, the results presented an observable, weak relationship existing between corporate announcement events and associated negative financial impact to overall corporate stock market value.

In addition, only 11 corporations were identified as having results that were statistically significant. It was inferred from this revelation that the majority of corporate shareholders did not place much credence into announcement events associated with corporate privacy announcement events as they had minimal financial impact with statistical significance (weak relationship). This indicated that random error or fluctuations in the stock market were mostly likely to have caused the decrease in overall corporate stock market value, not the associated privacy announcement events.

Data was extracted individually for each corporation and then analyzed again to glean additional statistical value from testing. Based on US SEC SIC Divisions, while each of the 6 separate divisions tested together as a single entity had a negative (NEG -) financial impact to overall corporate stock market value, Division I (Services) had the least financial impact and most statically significant results when compared to the other US SEC SIC Divisions examined in this investigation. Statically significant results

implied an existing relationship between the corporate announcement events and the associated negative financial impact to overall corporate stock value, as well as indicated the announcement events were likely to have caused the decrease in overall corporate stock market value, not random error or fluctuation in the stock market.

Announcement events were separated from 2013-2015 and 2016-2018, tested as independent data subgroups, then compared with one another to discern potential patterns of users' privacy concerns over time. In analysis of these results, it was determined that both time periods exhibited a negative (NEG -) financial impact to overall corporate stock market value. Time period 2013-2015 was not statistically significant and indicated no relationship existing between the corporate announcement events and the associated negative financial impact to overall corporate stock market value. Time period 2016-2018, however, was statistically significant with an StdCsect *p*-value of 0.0824 ($p = < 0.10$) that indicated an observable but weak relationship existing between the corporate announcement events and the associated negative financial impact to overall corporate stock market value. It was inferred from these results that while the impact to overall corporate stock market value was negative, announcement events from more recent points in time were statistically significant; indicating that the actual announcement events from 2016-2018 could have caused the decrease in overall corporate stock market value, not likely random error or stock market fluctuation.

Corporate announcement events were also separated into subset groups based on being a proactive investment in privacy, or a reactive investment in privacy (or negative announcement events based on connotation or announcement title), then tested separately to determine if corporations were rewarded (positive (POS +) financial inventive) or

penalized (negative (NEG -) financial incentive) by shareholders or consumers for their privacy investment decision making. Corporations identified as having proactive investments in privacy had a positive (POS +) financial impact on overall corporate stock market value, but results were not statistically significant and indicated that random error or fluctuation in the stock market was likely to have caused the increase in overall corporate stock market value, not the actual announcement events.

Corporations identified as having reactive investments in privacy (or negative announcement events based on connotation or announcement title), had a negative (NEG -) financial impact on overall corporate stock market value, but results were also not statistically significant and indicated that random error or fluctuation in the stock market was likely to have caused the decrease in overall corporate stock market value, not the actual announcement events. It was inferred from these results that while the data set containing proactive investments in privacy observed a slight positive (POS +) impact to overall corporate stock market value, when compared to the data set containing reactive investments in privacy (negative (NEG -) impact to overall stock market value), corporate shareholders most likely dismissed the results as insignificant and not reflective of any actual financial change in long-term overall corporate stock market value.

These results established that not only did corporations who proactively invested in privacy not see any financial benefit from the privacy investment, corporations were also not rewarded by shareholders for proactively investing in privacy. More concerning, however, is that corporations who reactively invested in privacy, or corporations that were identified as having negative announcement events based on connotation or

announcement title, while they did report a decrease in stock market value, these corporations were also not penalized by shareholders for weak privacy.

Furthermore, despite announcement events identified as proactive in nature seeing a positive (POS +) financial impact to overall corporate stock market value, when compared to announcement events identified as reactive (or negative in nature) that received negative (NEG -) financial impact to overall stock market value, corporate shareholders most likely dismissed both results as insignificant and not reflective of any actual financial change in long-term overall corporate stock market value. This indicated that corporations trying to stay ahead of privacy issues through preemptive investments in privacy received no positive (POS +) financial incentive for doing so, nor did corporations exposed by weak privacy protection receive a negative (NEG -) penalty for their lack of concern. Ultimately, it was discovered that no financial incentives exist to motivate corporate investments in privacy; positive (reward) or negative (penalized).

As both groups (proactive and reactive) results were statistically insignificant, shareholders for the associated corporations dismissed both positive (POS +) and negative (NEG -) impacts to stock market value as likely caused by random error or fluctuation in the stock market. This lends support to the idea that no financial incentives exist motivating corporate investments in privacy; positive (reward) or negative (penalized). Results were similar to those identified in previous IS/IT event studies.

Corporations will ultimately determine their individual privacy risk exposure and compare it against the estimated financial expenditure required to ensure they are insulated against liability from a potential privacy breach incident when considering corporate investments in privacy. Corporations constantly strive for internal alignment to

achieve a "… well-informed sense of assurance that information risks and controls are in balance" (Anderson, 2003). Achieving this balance ensures extra financial costs required to implement protection mechanisms are not wasted on investment options without the likelihood of high ROI, as witnessed in this research. Data from this event study research investigation, and other event study research, have indicated that while privacy protection is a major concern to end users, the potential financial cost of penalization resulting from a privacy breach incident has been of minimal financial concern or motivation encouraging corporate investments in privacy.

5.4 Recommendations

This research investigation conducted adds to the body of privacy and event study literature and will help bridge the identified research gap. Event study research examining the economic impact, and financial impact to overall corporate stock market value associated with corporate investments in privacy, has not been conducted with nearly the same vigor, intensity, or fervor as other research domains, as evident in domain breakdown within the totality of event study research discovered during the literature review. Through this event study, implications were presented, based on data observations and testing analysis, to serve as an additional resource reference made available for academics and corporate entities interested in better understanding corporate investments in privacy, and the economic implications associated with corporate investments in privacy relating to overall corporate stock market value.

In an effort to be as useful as possible, this research investigated several areas where corporate investments in privacy were evaluated to determine whether the privacy investment made a positive (POS +), or negative (NEG -), financial impact to the

associated corporations overall stock market value. Individual data sets were also targeted for independent examination and testing and included multiple time periods (2013-2015 and 2016-2018) within the entire investigation window (2013-2018), separate US SIC Divisions, and both proactive and reactive (negative) announcement events. This was an effort to provide as much generalizability and cross-domain applicability as possible. It is recommended, however, that additional event study testing be conducted to further the research agenda presented.

Future research opportunities exist that could extend this event study. Separate data could be collected based on different criteria to further isolate potential financial benefits from corporate investments in privacy. Additionally, testing could be conducted using varying estimation window and event window sizes, in addition to shorter and longer periods of time identifying confounding and conflicting corporate data. Different statistical significance tests could also be completed to compare results using more than one parametric and nonparametric test (using then the Eventus® software suite).

Additional parametric and nonparametric tests available for data testing within future research could include: *Generalized Rank Test* (Generalized Ranked *T*, Generalized Ranked *Z*), *Corrado Rank Z-test* (Z-statistic) (Corrado, 1989) – combines estimation window and event window into a single set of ranked, stock return data; then ranks the daily estimation window and event window *AR*s event by event; *Rank* test – the nonparametric statistic that appears with non-standardized parametric tests instead of the generalized sign test, the *Jackknife* test – will accompany non-standardized method parametric tests instead of the generalized sign test as the nonparametric test; *Wilcoxon Signed Rank test* – considers both sign and magnitude of *AR*s and applies the signed rank

test cross-sectionally; test assumes that none of the absolute values are equal and that none of the absolute values are equal to zero (0), *Time-Series Standard Deviation Method* (also known as the *Crude Dependence Adjustment* (CDA) – developed by Brown & Warner (1980) where unlike the standardized abnormal return method, calculates a single variance estimate for the entire portfolio, with *** *Bootstrapping* to select nonparametric bootstrapped versions of certain parametric tests available for use.

Changes in research design, methodology, and statistical testing methodology could help identify discernable financial differences to overall corporate stock market value, as well as potential short-term and long-term financial implications, from corporate investments in privacy identified in this study. Due to limited privacy event study research existing within the extant body of literature, any and all future research examinations further investigating corporate investments in privacy will provide valuable academic and practical implications.

*** Note: According to Eventus®, when using the *Bootstrap* option, by default, *Bootstrap* will only test for the designated event windows, not each individual day *within* the event window. However, *Bootstrap* tests for an individual day or month can be obtained by specifying an event window with the same beginning and ending date. In addition, only Patell-Z, standardized cross-sectional, time-series standard deviation, skewness-corrected transformed normal, and cross-sectional tests are eligible for the bootstrap. Only tests which are selected by the appropriate option specifications (or the Patell-Z test if no parametric test is explicitly specified) are bootstrapped. If the Patell-Z test is used, the SERIAL option is implied by the BOOT option. That is, when the bootstrap is selected, the Patell-Z test is adjusted for serial dependence in both parametric and bootstrap results.

By default, the resampling ratio is 0.25 and the bootstrap significance level is one- or two-tailed according to the TAIL option. You can, however, override these defaults using the RESAMPLE=ratio and BTAIL=1|2 options.

5.5 Summary

The main objective of this research investigation was to examine corporate investments in privacy by focusing directly on privacy investments as an independent construct to better understand their financial impact. By accomplishing this goal, the author was able to add to the extant body of literature by better understanding the

economic relationship between corporate privacy announcement events and their financial impact on the associated corporation's overall stock market value. Results obtained during this event study investigation answered all hypotheses and research questions posited within this research while also providing evidentiary data relating to the financial implications associated with corporate investments in privacy, and the financial stock market impact analysis relating to corporate investments in privacy.

Lastly, in completing this research, the author was able to better understand *why* corporations are *not investing* in privacy, addressed the idea of financial incentives existing to motivate corporate investments in privacy, and discovered specific industry segments that are more likely to benefit financially from corporate investments in privacy, when directly compared to corporations within competing industry segments. This event study uncovered research implications that serve as a resource reference to academics, corporations, and future advocates extending event study research.

Review of the extant body of literature identified a gap in the privacy and event study literature: event study research completed within the privacy domain has been almost nonexistent when directly compared to the volume of event study research having been conducted within the Privacy, Information System (IS), Information Technology, Information Security (InfoSec), and related domains (Appendix B – Table 16). Even more disparity exists when evaluating historic event study research associated with the financial impact of corporate investments in privacy (Appendix B – Table 16).

Accurate financial assessment of investment options by shareholders is the main impetus driving decision-making relating to corporate investment in privacy (Dardan et al., 2005; Subramani & Walden, 2001). However, little evidence exists to suggest that

shareholders are accurately evaluating perceived financial value from corporate investments in privacy. A disconnect exists between actualized value and perceived value in corporate investments in privacy (Acquisti et al., 2006; Culnan & Williams, 2009; Dinev & Hart, 2006). Corporations unable to ensure a positive (POS +) financial *Return on Investment* (ROI) from corporate investments in privacy are reluctant to make financial expenditures on risk averse investment options, including privacy investments.

The issue is further compounded by the realization that within the limited body of event study privacy research, there has been no universally accepted consensus when determining financial implications caused by privacy breach incidents. At present, there is only scattered evidence about the price companies pay for privacy debacles (Acquisti et al., 2006) due to inaccurate methodology in measuring true financial cost of beach incidents. Hovav & D'Arcy (2003) note "…potential intangible losses such as "loss of competitive advantage" (breach) and "loss of reputation" (D'Amico, 2000) are not included as intangible costs are not directly measurable."

To determine if corporate investments in privacy had any financial impact on overall stock market value of the associated corporation, it was necessary to obtain a testable data set. This included the following steps to identify and collect valid data for testing: 1) Data Identification, 2) Data Collection, 3) Data Filtering, 4) US SEC SIC Codes, 5) Confounding Data, 6) Duplicate Data, and 7) CRSP Data (Table 2).

Data identified for examination were press release announcement events associated with corporate investments in privacy. Data identification and data collection of announcement event data needed to originate from a news source and match one of six specified keywords used: 1) Privacy, 2) Privacy Investment, 3) Information Privacy

Investment, 4) Information System Privacy, 5) Information System Privacy Investment, and 6) Electronic Privacy. Further, all announcement data must have been published between January 1st, 2013 – December 31st, 2018 (Table 4) and originate from either ProQuest (PQ) or Business Source Premier (BSP) online database repositories.

To manage the scope of the Final Sample Set (FSS), data was filtered through several mechanisms to ensure only accurate and valid data remained within the sample. Only corporations publicly traded on one of three United States (U.S.) stock market indices (NYSE, AMEX, NASDAQ) were eligible for study inclusion. In addition, corporations must have also been actively trading during both the designated 195-Day estimation window and 3-Day event window and possess an active U.S. Securities and Exchange Commission (SEC) Standard Industrial Classification (SIC) Code (Table 3).

All data was then checked for potential confounding and duplicate data. Confounding data are defined as events that may influence observable changes in overall stock market value. Removing confounding data events is vital to ensuring observable changes in stock market value were caused by the announcement event being investigated and not the confounding event. All confounding events were eliminated within 3-Days of announcement event date (-1, +1). Duplicate data events were also identified and eliminated with the earliest event date kept. Lastly, all corporate data was cross-referenced for available data in the University of Chicago's Center for Research in Security Prices (CRSP) database and COMPUSTAT.

The original data set identified 2,371 press release announcement events relating to corporate investments in privacy (Table 3). After data collection and data filtering steps (Table 2), the Final Sample Set (FSS) was reduced to 323 announcement events

(Appendix F – Table 19). The FSS set of 323 events represented 75 corporations (Appendix K – Table 24) and was used to test all posited research hypotheses and answer all research questions advanced within this event study. Once data composition of the FSS was complete, the author then determined requisite corporate stock market values.

Corporate stock market pricing and stock market value were first calculated, using the appropriate market index (NYSE, AMEX, or NASDAQ), for each corporation on the date the investment announcement event was released to the public. With accurate stock market pricing, *Expected Normal Return* (ENR) values, expected corporate stock market value absent the press release announcement event being investigated, were then calculated for each corporation using the designated 195-Day estimation window, followed by the calculation of corporate Abnormal Return (AR) values. Corporate stock market AR is the difference between expected ENR (daily stock return price), and actualized returned stock market price, after the corporate investment announcement event was publicly disclosed. In this research, "the abnormal returns represent the extent to which realized returns on the event day deviate from the returns that would be expected…" (Campbell et al., 2003).

Using historical event study literature for reference, this research used the CAPM-based Market Model (MM) for identification and collection of financial records and stock market returns. The CAPM-MM is the most commonly used procedure for calculating Abnormal Returns (AR) and "…controls for the historical relationship between the abnormal returns of a firm with the abnormal returns to an index" (Agrawal et al., 2006). The Eventus® software suite was used for mathematical calculations and statistical testing. After computing AR for each corporation, *Cumulative Abnormal Return* (CAR)

and *Average Cumulative Abnormal Return* (ACAR) was determined for each corporation over the designated 3-Day event window (t = -1, t = 0, t = 1).

Once requisite numerical values were determined for each corporation (ENR, AR, CAR, ACAR), announcement event data was tested. Using appropriate statistical significance testing, data was analyzed to determine financial impact that corporate investments in privacy had on overall corporate stock market value. In this research, the null hypothesis, corporate Abnormal Returns (ARs) are not significantly different from zero (0), was rejected (Acquisti et al., 2006). Following traditional event study guidelines, both *parametric* tests and *nonparametric* tests were used. Statistical significance testing using multiple metrics was necessary to test the null hypothesis, as well as identify corroborating evidentiary data to either *accept or reject* hypotheses posited within this research regarding privacy investments. Furthermore, *parametric* and *nonparametric* testing ensured statistical validity and robustness of this research, while helping ascertain the significance of the data results (Appendix L – Table 25).

Parametric tests used were *Standardized Cross-Sectional* (StdCsect) (aka BMP test) (Boehmer et al.,1991), in place of the traditional Patell-Z test (1976), and standardized StdCsect Z-statistic tests. The StdCsect Z-test statistic was used to assess whether or not the Average Cumulative Abnormal Return (ACAR), Mean CAR, was statistically significantly and different from zero (reject null hypothesis), its expected value (McWilliams & Siegel, 1997). According to Im et al. (2001), significance of the AR based on the Z-statistic test allows the researcher to infer that the privacy investment announcement events have a significant impact on the market value of the associated firm (Loderer & Mauer, 1992; McWilliams & Siegel, 1997) (Appendix M – Table 26).

The nonparametric *Generalized Sign Z-test* (Z-statistic) was used to examine the number of securities with positive (+) and negative (-) *Average Abnormal Returns* (AAR) during the designated 195-Day estimation window and 3-Day event window under the null hypothesis that the fraction of positive (+) returns during the event window is the same as the fraction of positive (+) (Benco & Prather, 2008). Both the StdCsect-Z and Generalized Sign Test (GST) were used together to validate results.

The Final Sample Set (FSS), containing 323 press release announcement events (Appendix F – Table 19) from 75 different corporations (Appendix K – Table 24), was initially tested as a single data set. Following that, each corporation making up the FSS was then tested individually, and collectively within unique data subsets, to identify results based on different data criterion. Analysis of the FSS (323 announcement events) confirmed a negative financial impact to overall corporate stock market value (Mean CAR -0.20%) from press release announcement events identifying corporate investments in privacy; however, results were not statistically significant, indicating some relationship existing between corporate privacy announcement events and the overall reduction in corporate stock market value (Appendix M – Table 26).

To better understand *why* corporations are *not investing in privacy*, additional data subset testing was needed. Breakdown of the Final Sample Set (FSS) yielded 75 individual corporations comprising the FSS (323 separate announcement events). From the 323 announcement events, 97 events (30.03%) were explicitly identified as being either “proactive” or “reactive” (negative connotation). Of those 97 events, 51 events (15.79%) from 39 corporations (52%) were identified as “proactive” and had a positive (POS +) financial impact, while 46 events (14.24%) from 36 corporations (48%) were

identified as “reactive” (negative connotation) and had a negative (NEG -) financial impact. These results help better understand *why* corporations are *not investing in privacy*; minimal financial incentives existing to *motivate* corporate investments in privacy (POS or NEG). Corporations not enticed by economic motivation see no financial incentive to make an investment likely to generate negative (NEG -) ROI.

Ultimately, it was concluded that no financial incentives exist motivating corporate investments in privacy; positive (reward) or negative (penalized). As both groups (proactive and reactive) results were statistically insignificant, shareholders for the associated corporations dismissed both positive (POS +) and negative (NEG -) impacts to stock market value as likely caused by random error or fluctuation in the stock market. Results achieved were similar to results identified in previous IS/IT event studies. It was inferred from these results that while the data set containing proactive investments in privacy observed a slight positive (POS +) financial impact to overall corporate stock market value, corporate shareholders most likely dismissed the results as insignificant and not reflective of any changes to long-term stock market value.

These results established that not only did corporations who proactively invested in privacy not see any financial benefit from the privacy investment, corporations were also not rewarded by shareholders for proactively investing in privacy. More concerning, however, was that corporations who reactively invested in privacy, or corporations that were identified as having negative announcement events based on connotation or announcement title, while they did report a decrease in stock market value, these corporations were also not penalized by shareholders for weak privacy.

This research also determined whether any specific industry was more likely to benefit from corporate investments in privacy. From the Final Sample Set (FSS) of 323 announcement events, each industry division was grouped into one of six data subsets (Division J, I, D, E, G, and H). It was concluded that while no corporation benefitted from privacy investments, corporations assigned to U.S. SEC SIC Code classification designator "Division I" (Services) received the least *negative* financial impact to overall corporate stock market value from corporate investments in privacy and had identifiable results that were the most statistically significant. While there were no observable economic incentives existing for any specific "Division" motivating investments in privacy, corporations in "Division I" were penalized less overall for privacy investments.

Time specific data subsets were tested to discern the presence of increased, or decreased, consumer concern for privacy over the time period investigated 2013-2018. It was noted that the separate time periods examined did not present any indication as being likely to motivate corporate investments in privacy. Results from time period 2013-2015 had a *negative* financial impact to overall corporate stock market value from corporate investments in privacy that was not statistically significant. Conversely, while the data subset from 2016-2018 contained 163 announcement events that were also *negative* (NEG -), Mean CAR (-0.27%), results *were* statistically significant ($p = <0.10$) and indicated an observable, but weak, relationship existing between the corporate announcement events and the associated negative overall financial stock market impact.

Additionally, separate identification and analysis of announcement events identified as statistically significant within the Final Sample Set (FSS) allowed further extrapolation of additional inferences. The FSS was comprised 75 different corporations

responsible for the totality of the 323 separate announcement events associated with a corporate investment in privacy. From the 323 announcement events, 11 corporations (14.67%) were identified as having 85 announcement events (26.32%) with statistically significant results using either parametric or nonparametric tests implemented. Of those 11 corporations, eight (8) corporations (five positive (POS +) Mean CAR and three negative (NEG -) Mean CAR) were identified as having announcement events (49) with statistically significant results from *both* parametric and nonparametric tests implemented, while three (3) corporations (zero positive (POS +) Mean CAR and three negative (NEG -) Mean CAR) were identified as having announcement events (36) with statistically significant parametric or nonparametric test results.

It was extrapolated that regardless of the financial impact to the associated corporations overall stock market value, results were statistically significant for only 11 of the 75 total corporations (14.67%). In addition, only 49 of the 323 total announcement events (15.17%) indicated the presence of a strong relationship, with just 36 of the 323 announcement events (11.15%) indicating the presence of any relationship at all. The existence and strength of the observable relationship represents the statistical significance existing between the corporate announcement event and the financial impact to the corporation's overall stock market value. It was inferred from this discovery that the majority of corporate shareholders did not place much credence into observed financial changes in stock market value associated with corporate privacy announcement events due to the weak financial impact and minimal statistical significance (weak relationship). This indicated that random error or stock market fluctuations mostly likely caused the decrease in corporate stock market value, not the privacy investment announcement.

Results of this research indicated that minimal financial benefits exist to corporations when investing in privacy, and minor positive financial implications to overall corporate stock market value associated with corporate investments in privacy. Corporations were not rewarded for proactively investing in privacy, nor were they penalized for failing to invest in privacy or resulting from privacy breach incidents. There were also no economic incentives, nor industry specific (Division) financial benefits, discovered encouraging corporate investments in privacy. While results will not assist in helping to encourage corporate investments in privacy, the resultant event study makes an academic contribution to the extant body of privacy and event study literature. Future research extending this event study will provide additional data supporting continued corporate investments in privacy.

Completing this event study research, the author was able to successfully answer the research questions and hypotheses posited, while addressing the underlying question motivating an: “Examination of Corporate Investments in Privacy: an Event Study!”

Appendix A

Event Study (ES) Research and Literature

IS / IT Investments

Year	Author (s)	Publication Name	Research Area (s)
1989	Lubatkin et al.	*Academy of Management Journal*	Stockholder Reaction to CEO Changes in Large Corporations
1993	Dos Santos et al.	*Information Systems Research*	Impact based on *Industry* and *General IS/IT Investment*
2001	Chatterjee et al.	*MIS Quarterly*	CIO Positions (timing, industry, external vs. internal hire)
2001	Hayes et al.	*Journal of Information Systems*	ERP Implementation (company size, financial health, vendor characteristics)
2001	Im et al.	*Information Systems Research*	Impact comparisons based on Industry, company size, timing
2001	Chen & Siems	*Journal of Economic & Financial Review*	B2B integration; vertical vs. horizontal, e-commerce initiatives, acquisitions, etc.
2001	Subramani & Walden	*Information Systems Research*	E-Commerce (company type, B2B vs. B2C, type of goods)
2002	Chatterjee et al.	*Journal of Management Information Systems*	Impact from general IS/IT infrastructure investment
2002	Lee et al.	*Journal of Electronic Commerce Research & Application*	E-Business Initiatives
2003	Dehning et al.	*MIS Quarterly*	Impact from transformative IS/IT investments
2003	Hunter	*Journal of Information Theory & Application*	Compared impact of exploitive vs exploratory IS/IT investments
2004	Dehning et al.	*Journal of Management Information Systems*	E-Commerce
2005	Dardan et al.	*Journal of Electronic Commerce Research & Application*	Examined E-Commerce investments
2005	Ferguson et al.	*International Journal of Accounting Information Systems*	Examined impact from E-Commerce investments
2005	Filibeck et al.	*Journal of Business Logistics*	Supplier-Chain Related IT
2005	Sabherwal & Sabherwal	*Decision Sciences*	IT-Based Knowledge Management Initiatives
2006	Chavez & Lorenzo	*Supply Chain Forum*	Supply Chain Applications
2006	Dardan et al.	*Journal of Computer Information Systems*	Customer-related IT
2006	Guan et al.	*Database for Advances in Information Systems*	CIO Positions
2006	Oh et al.	*Journal of Information Systems*	Compared impact based on company type, type of IT, and size of company
2006	Ranganathan & Brown	*Information Systems Research*	ERP Implementation

Year	Author (s)	Publication Name	Research Area (s)
2006	Roztocki & Weistroffer	*Electronic Journal of Information Systems Evaluation*	Company type, type of IT, and cost management
2007	Cheng et al.	*Industrial Marketing Management*	E-Commerce (Taiwan)
2007	Dewan & Ren	*Information Systems Research*	Risk and IT Investments
2007	Khallaf & Skantz	*Journal of Information Systems*	CIO Appointments
2007	Lin et al.	*International Journal of Service Industry Management*	E-Service Initiatives (Taiwan)
2007	Meng & Lee	*Decision Support Systems*	Company Location
2007	Sabherwal & Sabherwal	*IEEE Transactions on Engineering Management*	IT-Based Knowledge Management Initiatives
2007	Roztocki & Weistroffer	*Hawaii International Conference on System Services*	Examined whether enterprise application has an impact on corporate stock market values
2007	Roztocki & Weistroffer	*European Conference on Information Systems*	Attempted to identify success factors investing in IT using activity-based costing (ABC)
2008	Roztocki & Weistroffer	*Hawaii International Conference on System Services*	Stock Price Reaction to Investments in EAI and ERP: A Comparative Event Study
2008	Benco & Prather	*Quarterly Journal of Finance & Accounting*	ERP Systems
2008	Mitra & Singhal	*Journal of Operations Management*	Supply Chain Integration
2008	Nagm & Kautz	*Journal of Information Technology – Theory & Application*	IN Investments (Australia)
2008	Jeong & Lu	*Journal of Theoretical and Applied Electronic Commerce Research*	RFID
2008	Walden & Browne	*Journal of Electronic Commerce Research & Application*	E-Commerce (explanation of Internet Bubble)
2008	Yang & Klassen	*Journal of Enterprise Information Management*	Self-Service Technologies
2009	Kim et al.	*Tourism Economics*	IT Investments (in Hospitality Firms)
2009	Khansa & Liginlal	*European Journal of Operational Research*	Evaluated the financial flexibility of investing in security process innovations
2009	Misra & Rao	*Journal of Organizational Computing & Electronic Commerce*	Transactional web sites
2009	Roztocki & Weistroffer	*Journal of Enterprise Information Management*	Enterprise Application Integration (EAI) – evaluated the change in timing, company characteristics, market conditions, etc. had on the financial stock market impact
2009	Roztocki & Wesitroffer	*Journal of Computer Information Systems*	ABC system, risk factor, market condition compared to general IS/IT investments
2009	Roztocki & Weistroffer	*European Conference on Information Systems*	Examined stock market reactions to investments in IT using a newly developed explanatory model
2010	Choi & Jong	*Information & Management*	IT-Based Knowledge Management Initiatives

Year	Author (s)	Publication Name	Research Area (s)
2010	Jeong & Stylianou	*Information & Management*	Impact of / market reaction to, adoption of Application Service Provider (ASP)
2010	Chai et al.	*Decision Support Systems*	Examined value of investments in IT security on corporate stock market value
2013	Huang & Behara	*International Journal of Production Economics*	Economic impact from security prevention investments
47 Papers			

IS / IT Privacy – Breaches, Compliance, Violations, and Trustworthiness

Year	Author (s)	Publication Name	Research Area (s)
2006	Acquisti et al.	*Economics of Information Security*	Impact to corporation after a privacy breach
2006	Schwaig et al.	*Information & Management*	Investigated compliance of fair information practices (FIPs) of Fortune 500 when handling online privacy disclosures
2009	Culnan and Williams	*MIS Quarterly*	Organizational Privacy behaviors and ethical responsibilities
2011	Nicholas-Donald et al.	*Americas Conference on Information Systems*	Economic effect of privacy breach announcements on corp stock market price
2012	Li et al.	*Communications of the International Information Management Association*	Online privacy policies for 30 Dow Jones corporations
2012	Khansa et al.	*Computers & Security*	Impact of HIPAA compliance on corporate stock market value (healthcare, IS/IT, etc.)
2014	Hinz et al.	*Business & Information Systems Engineering*	Investigated the economic impact of privacy violations and security breach incidents (Research Paper)
2015	Case and King	*American Society of Business and Behavioral Sciences*	Study of "Fair Information Practices" (Privacy Policy) of *Fortune 500* corporation's
8 Papers			

IS / IT Security – Breaches, Threats, Intrusions, and Financial Consequences

Year	Author (s)	Publication Name	Research Area (s)
2003	Cambell et al.	*Journal of Computer Security*	Security Breaches
2003	Ettredge & Richardson	*Journal of Information Systems*	Hacker Attacks
2003	Hovav & D'Arcy	*Risk Management and Insurance Review*	Denial of Service (DOS) Attacks
2003	Garg et al.	*Information Management & Computer Security*	Non-Virus Security Breaches
2004	Cavusoglu et al.	*International Journal of Electronic Commerce*	Internet Security Breaches
2004	Hovav & D'Arcy	*Information Systems Security*	Virus Attack Announcements
2005	Hovav & D'Arcy	*Computers & Security*	Defective IT Products
2006	Anthony et al.	*International Journal of Accounting Information Systems*	Outages of Commercial Websites

Year	Author (s)	Publication Name	Research Area (s)
2006	Aytes et al.	*Americas Conference on Information Systems*	Examining stock market impact from security breaches; funding to prevent breaches
2007	Andoh-Baidoo & Osei-Bryson	*Expert Systems with Applications*	Internet Security Breaches
2007	Kannan et al.	*International Journal of Electronic Commerce*	IT Security Breaches
2007	Telang & Wattal	*IEEE Transactions on Software Engineering*	Defective IT Products
2009	Goel & Shawky	*Information & Management*	Estimated market impact from security breach announcements
2010	Yayla & Hu	*Journal of Information Technology – Advance Online Publication*	Information Security Breaches – Effect of Contingency Factors
2010	Malhotra & Malhotra	*Journal of Service Research*	Examining corporate stock market impact from security breaches and privacy exposure
2010	Gatzlaff & McCullough	*Management & Insurance Review*	Examining corporate stock market impact from data breach events (loss of both customer and employee data)
2010	Patel	*Working Paper (Duke University)*	Determining the effects of IT hacker announcements on corporate stock market value
2011	Chen et al.	*Computers in Human Behavior*	Identifying changes in stock market value for companies providing info security products/services to the identified corporation's that had their data hacked
2011	Morse et al.	*Information Security Journal – A Global Perspective*	Examining corporate stock market impact from breaches in computer security (ComSec)
2012	Cardenas et al.	*Americas Conference on Information Systems*	Investigated corporate stock market impact from publicly announced security breaches
2013	Andoh-Baidoo & Osei-Bryson	*International Journal of Electronic Finance*	Investigated corporate investors' reaction to Internet Security Breach events using Deterrence Theory
2014	Gwebu et al.	*Pacific Asia Conference on Information Systems*	Examination of the stock market impact from an identified breach incident
2014	Hinz et al.	*Information & Management*	Examined long term financial consequences to corporate stock market value from data theft events / privacy violations
2014	Arcuri et al.	*Working Paper (University of Sicily di Roma)*	Stock market impact from InfoSec breaches and cyber-attacks and crime (1995 to 2012)
2014	Hovav et al.	*ACM Advances in Information Systems*	Investigated the stock market impact from security breach events
2014	Bose & Leung	*Decision Support Systems*	Investigated if phishing alerts impact firm market value
2017	Hovav et al.	*ACM Advances in Information Systems*	Stock market reaction to cyber incidents / breach announcements in South Korea
2017	Berghel	*IEEE Computer Society*	Examined Equifax and Experian data breaches
28 Papers			

IS / IT Outsourcing Initiatives

Year	Author (s)	Publication Name	Research Area (s)
2000	Hayes et al.	*Journal of Information Systems*	Outsourcing impact based on firm size and industry
2002	Peak et al.	*Journal of Information Technology – Cases and Applications*	Company Size, Effect on Risk from Outsourcing

Year	Author (s)	Publication Name	Research Area (s)
2005	Florin et al.	*Journal of High Technology Management Research*	IT Outsourcing
2006	Agrawal et al.	*Information & Management*	Outsourcing E-Commerce
2006	Oh et al.	*Journal of Management Information Systems*	Contract Size, Vendor Characteristics from outsourcing
2007	Gewald & Gellrich	*Information Technology & Management*	Outsourcing
2009	Daniel et al.	*Journal of Enterprise Information Management*	Outsourcing
2009	Duan et al.	*European Journal of Information Systems*	Business Process Outsourcing
8 Papers			

Event Study History and Background

Year	Author (s)		Research Area (s)
1963	Sharpe	*The Journal of Finance*	Application of the Markowitz model for financial portfolio analysis
1969	Fama et al.	*International Economic Review*	Explored the varying of corporate stock prices when exposed to new information
1970	Fama	*The Journal of Finance*	Efficient Capital Markets: A Review of Theory and Empirical Work
1985	Brown & Warner	*Journal of Financial Economics*	Examined using Event Study methodology while investigating Daily Stock Returns
1991	Fama	*The Journal of Finance*	Explored in greater depth capital markets
1997	McWilliams and Siegel	*Academy of Management Journal*	Examination of the attention paid towards theoretical and research design issues when using the event study methodology in management research
1997	MacKinlay	*Journal of Economic Literature*	Examined event studies in economics and finance
2003	Malkiel	*Journal of Economic Perspectives*	Review of "Efficient Markey Hypothesis" and critics; (*Random Walk Theory*)
2003	Dehning et al.	*Hawaii International Conference on System Services*	Reviewed applicability of firm value framework using Event Studies in MIS
2007	Hovav et al.	*Annual Security Conference*	Classification of security breach events based on their corporate stock market impact
2008	Roztocki & Weistroffer	*Americas Conference on Information Systems*	Event study literature review
2009	Roztocki & Weistroffer	*Americas Conference on Information Systems*	Updated event study literature review
2009	Zhang & Huang	*International Journal of Business and Management*	Review of empirical research examining market value impact from information security breach event announcement
2011	Sewell	*Research Notes (UCL Department of Computer Science)*	Background and history of "Efficient Market Hypothesis" (EMH) using a research note that gives a chronological review of the notable literature relating to EMH
2011	Roztocki & Weistroffer	*European Journal of Information Systems*	Event study review of past, present, and future outlook

Year	Author (s)	Publication Name	Research Area (s)
2016	Spanos & Angelis	*Computers & Security*	Literature review of corporate stock market impact from information security breach events
16 Papers			

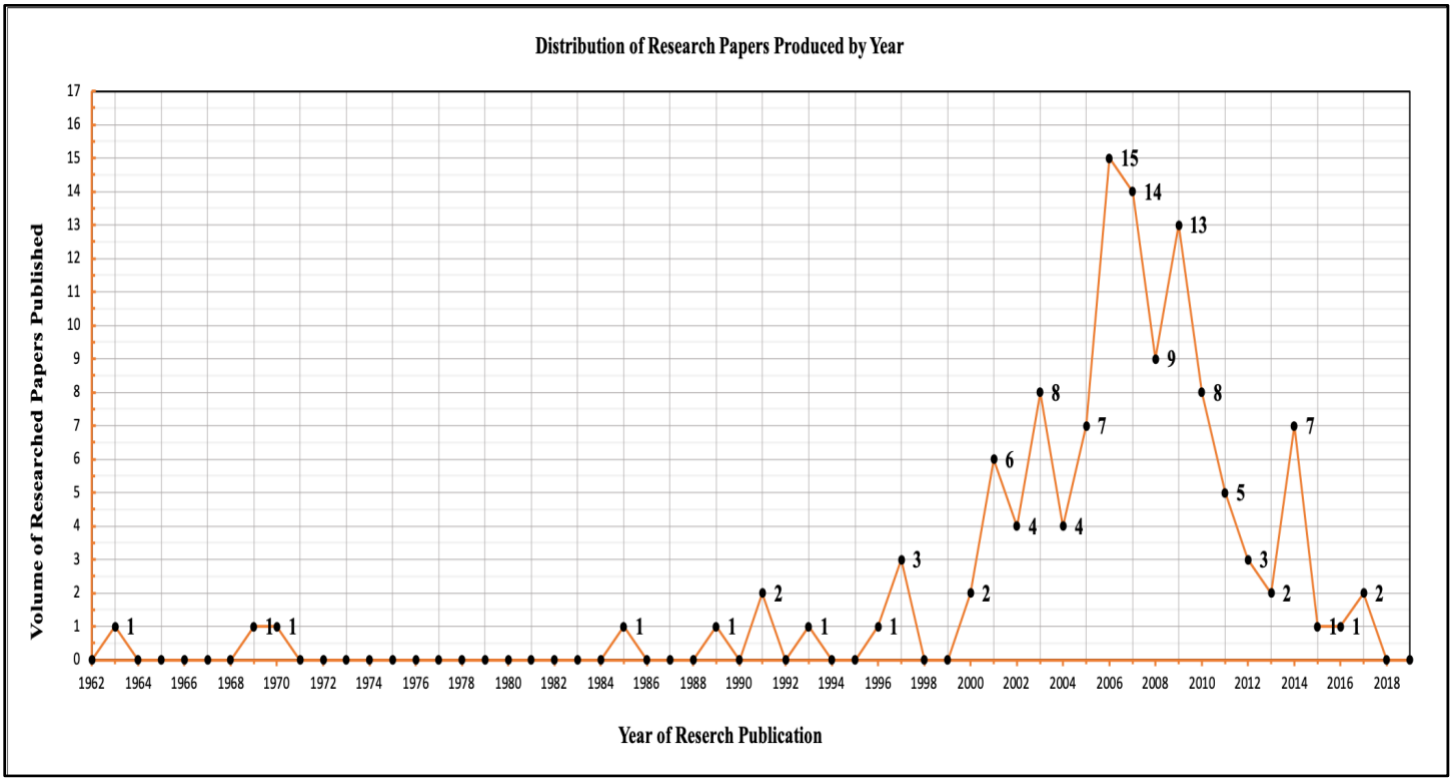
IS / IT Announcement Events (Other)

Year	Author (s)	Publication Name	Research Area (s)
1991	Koh & Venkatraman	*Academy of Management Journal*	Joint Venture Formation
1996	Hendricks & Singhal	*Management Science*	Investigated the financial impact that receiving an award has on a corporation's market value
1997	Hendricks & Singhal	*Management Science*	Investigated the financial impact that new product delays have on a corporation's market value
2000	Pardue et al.	*Engineering Economist*	New Product Announcement
2001	Bharadwaj & Keil	*Working Paper (Emory University)*	Effects of IT failure on market value of effected corporation
2002	Geyskens et al.	*Journal of Marketing*	Establishing an Internet Delivery Outlet
2004	Benbunan-Fich & Fich	*International Journal of Electronic Commerce*	Web Traffic
2005	Benbunan-Fich & Fich	*Journal of Electronic Commerce in Organizations*	Website Redesign
2006	Aggarwal et al.	*International Journal of Electronic Commerce*	XML Standardization
2006	Lee & Lin	*Review of Quantitative Finance and Accounting*	Merger and Joint Ventures of IT Firms
2006	Uhlenbruck et al.	*Strategic Management Journal*	Acquisitions Involving Internet Firms
2007	Song et al.	*Information Systems Frontiers*	Code-sharing Agreements in the Airline Industry
2008	Raghu et al.	*Information Systems Frontiers*	IT-Related Patent Infringements
2009	Bharadwaj et al.	*The Journal of Strategic Information Systems*	Market impact from IT Project Failures
2010	Goel et al.	*California Management Review*	Examined impact that illegal Peer-to-Peer file sharing has on the media industry via stock market value
2014	Canace & Mann	*Review of Quantitative Finance & Accounting*	Extend Lee and Lim (2006) and examined market impact of M&A's and Joint Ventures
16 Papers			

Appendix B

Table 16

Event Study (ES) Research and Literature – Publication Distribution



Distribution and Volume of Event Study Research and Literature (by Year)

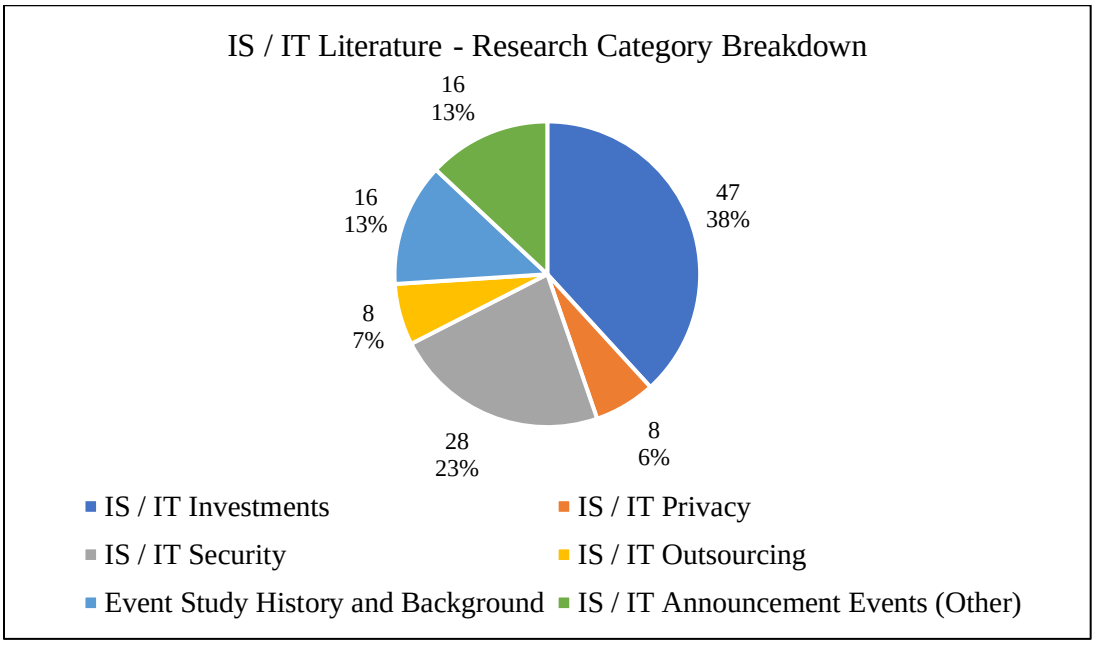
Appendix C

Table 17

Event Study (ES) Research and Literature Breakdown (by Category)

Total Event Study Literature Completed – 123 Research Papers			
Color Code	Literature Category	Number of Research Papers	Percentage of Total Literature Completed
Bright Blue	IS/IT Investments	47	47 Papers is 38% of 123 Total Papers
Orange	IS/IT Privacy	8	8 Papers is 6% of 123 Total Papers
Gray	IS/IT Security	28	28 Papers is 23% of 123 Total Papers
Yellow	IS/IT Outsourcing	8	8 Papers is 7% of 123 Total Papers
Green	IS/IT (Other)	16	16 Papers is 13% of 123 Total Papers
Light Blue	Event Study History / Background	16	16 Papers is 13% of 123 Total Papers

Observing the distribution of research interest in the data below, it is noteworthy that from a total volume of 123 papers conducted, the two largest areas of commitment (when *excluding from the total* the literature identified as "Event Study History and Background") were Information System (IS) / Information Technology (IT) investment (designed to *generate* revenue) and Information Security (InfoSec) (designed to *not loose* revenue). The data also identifies *Privacy* as having been shown the *least amount* of research interest from the academic community or corporations.



Appendix D

Table 18

Event Window Size(s) Used in Event Study (ES) Research

* Event Study History and Background papers have been excluded as there were no event windows identified since data collection was completed (sixteen (16) research papers total)

Note regarding the "Event Window" sizes used and identified below:

t = announcement event date and is directly specified as included in event window (example: event window sized (-1,0) identifies one day *before* announcement date (-1), and the announcement date (0), for a total event window of 2 days. Some event windows use days *before* and *after* the announcement date (example (-1,1) identifies a total event window used of 3 days that includes a time period that begins collecting data one day *before* the announcement date (-1), and continues collecting data until one day *after* the announcement date (1), while including the announcement date.

IS / IT Investments (47 Total Research Papers)			
General IS / IT Investments (13)			
Year	**Author (s)**	**Research Area (s)**	**Event Window (Size Used)**
1993	Dos Santos et al.	Impact based on Industry and General IS/IT Investment	(-1,0)
2001	Im et al.	Industry, company size, timing	(-1,0)
2002	Chatterjee et al.	Impact from General IS/IT Infrastructure Investment	(-1,0) (0,1) (-1,1) (-2,2)
2003	Dehning et al.	Impact from transformative IS/IT investments	(-1,1)
2003	Hunter	Compared impact of exploitive vs exploratory IS/IT investments	(-1,1) (-2,2) (-5,5) (-10,10)
2006	Oh et al.	Compared impact based on company type, type of IT, and size of company	(-2,-1) (0,1) (2,3)
2006	Roztocki & Weistroffer	Company type, type of IT, and cost management	(-1,0)
2007	Roztocki & Weistroffer	Attempted to identify success factors investing in IT with activity-based costing (ABC)	(-1,0) (-1,1)
2007	Meng & Lee	Company Location (US vs China)	(0,2)
2008	Nagm & Kautz	IT Investments (Australia)	(-1,1) (-5,5)
2009	Kim et al.	IT Investments (in Hospitality Firms)	(-1,0) (0,1) (-1,1)
2009	Roztocki & Wesitroffer	ABC system, risk factor, market condition compared to general IS/IT investments	(-1,0) (-1,1)
2009	Roztocki & Weistroffer	Examined stock market reactions to investments in IT using a newly developed explanatory model	(-1,0) (-1,1)
Specific IS / IT Investments (14)			
2001	Subramani & Walden	E-Commerce (company type, B2B vs. B2C, type of goods)	(-5,5) (-10,10)
2001	Chen & Siems	B2B integration; vertical vs. horizontal, e-commerce initiatives, acquisitions, etc.	(-1,1)
2002	Lee et al.	E-Business Initiatives	(-1,1)
2004	Dehning et al.	E-Commerce	(-1,1) (-5,5) (-10,10)

2005	Dardan et al.	E-Commerce	(-1,1)
2005	Ferguson et al.	E-Commerce	(-1,1) (-5,5) (-10,10)
2007	Dewan & Ren	Risk and IT Investments	(-1,1) (-10,10)
2007	Cheng et al.	E-Commerce (Taiwan)	(-5,5)
2007	Lin et al.	E-Service Initiatives (Taiwan)	(-1,2)
2008	Walden & Browne	E-Commerce (explanation of Internet Bubble)	(-1,1)
2008	Jeong & Lu	Financial impact from RFID investment	(-1,1)
2009	Misra & Rao	Transactional web sites	(-5,5) (0,1) (2,5) (-5,-1)
2009	Khansa & Liginlal	Evaluated the financial flexibility of investing in security process innovations	N/A
2010	Jeong & Stylianou	Impact of / market reaction to, adoption of Application Service Provider (ASP)	(-1) (0) (1)
Knowledge Management Initiatives (KMI) (8)			
2005	Filibeck et al.	Supplier-Chain Related IT	(-10,-6) (-5,-2) (-1,1) (2,5) (-6, 10)
2005	Sabherwal & Sabherwal	IT-Based Knowledge Management Initiatives	(-2,2)
2006	Dardan et al.	Customer-related IT	(-1,1)
2006	Chavez & Lorenzo	Supply Chain Applications	(0) (-2,2) (-4,4) (-6,6) (-8,8) (-10,10)
2007	Sabherwal & Sabherwal	IT-Based Knowledge Management Initiatives	(0,1) (-1,1) (-2,2)
2008	Yang & Klassen	Self-Service Technologies	(0) (1) (2) (3) (4)
2008	Mitra & Singhal	Supply Chain Integration	(-1,0)
2010	Choi & Jong	IT-Based Knowledge Management Initiatives	(-2,2)
Enterprise Integration Technology (6)			
2001	Hayes et al.	ERP Implementation (company size, financial health, vendor characteristics)	(0,1)
2006	Ranganathan & Brown	ERP Implementation	(-2,2) (-1,1) (-1,0) (0,1) (0,2)
2007	Roztocki & Weistroffer	Examined whether enterprise application has an impact on corporate stock market values	(-1,0)
2008	Benco & Prather	ERP Systems	(-1,1)
2008	Roztocki & Weistroffer	Stock Price Reaction to Investments in EAI and ERP: A Comparative Event Study	(-1,0) (-1,1)
2009	Roztocki & Weistroffer	Enterprise Application Integration (EAI) – evaluated the change in timing, company characteristics, market conditions, etc. had on the financial stock market impact	(-1,0) (-1,1)
Human Capitol (IS/IR-Related Hiring Positions) (4)			
1989	Lubatkin et al.	CEO Changes in Large Corporations	(-1,0) (-50,0) (1,50) (-50,50) (100,300)
2001	Chatterjee et al.	CIO Positions (timing, industry, external vs. internal hire)	(-1,0) (-1,1)
2006	Guan et al.	CIO Positions	(-5,-1) (-30,-1) (-20,-1) (-10,-1)
2007	Khallaf & Skantz	CIO Appointments	(-1,1)
Security Protection (2)			

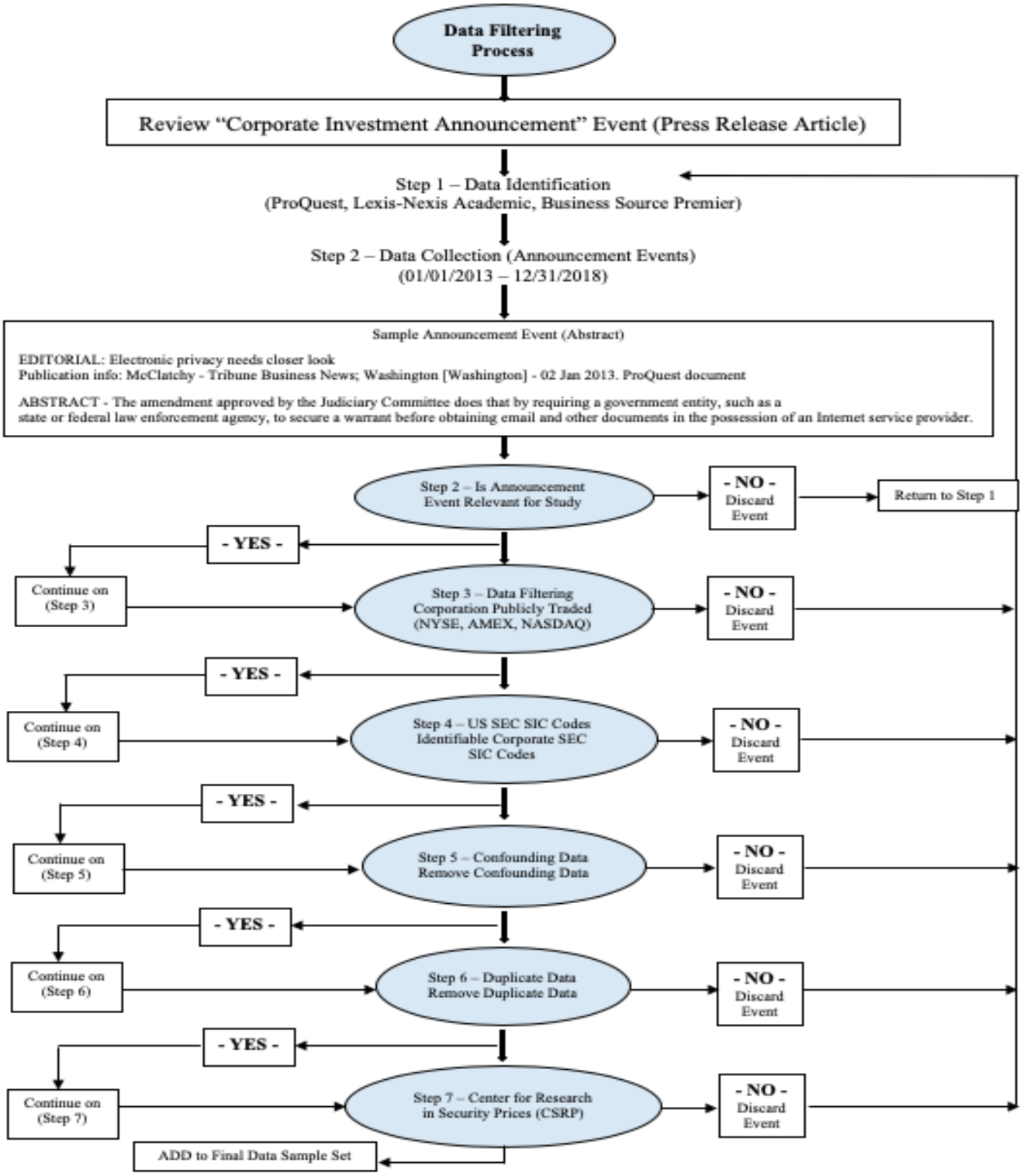
2010	Chai et al.	Examined value of investments in IT security on corporate stock market value	(-1,1) (-2,2) (-1,0) (0,1)
2013	Huang & Behara	Economic impact from security prevention investments	(0)
IS / IT Privacy – Breaches, Compliance, Violations, and Trustworthiness (8 Total Research Papers)			
Privacy Breach (3)			
2006	Acquisti et al.	Impact to corporation after a privacy breach	(0)
2011	Nicholas-Donald et al.	Economic effect of privacy breach announcements on corp. stock market price	(-1,0,1)
2014	Hinz et al.	Investigated the economic impact of privacy violations and security breach / data theft incidents	(-10,10)
Corporate Compliance (3)			
2006	Schwaig et al.	Investigated the manner of compliance of fair information practices (FIPs) for Fortune 500 when handling online privacy disclosures	N/A
2012	Khansa et al.	Impact of HIPAA compliance on corporate stock market value (healthcare, IS/IT, etc.)	(-10,0,10)
2015	Case & King	Study of "Fair Information Practices" (Privacy Policy) of *Fortune 500* corporation's	N/A
Corporate Behavior (2)			
2009	Culnan & Williams	Organizational Privacy behaviors and ethical responsibilities	N/A
2012	Li et al.	Online privacy policies for 30 Dow Jones corporations	N/A
IS / IT Security – Breaches, Threats, Intrusions, and Financial Consequences (28 Total Research Papers)			
Security Breach (18)			
2003	Campbell et al.	Security Breaches	(-1,1)
2004	Cavusoglu et al.	Internet Security Breaches	(0,1)
2006	Aytes et al.	Examining stock market impact from security breaches; funding to prevent breaches	(-2,2)
2007	Andoh-Baidoo & Osei-Bryson	Internet Security Breaches	(-1,1)
2007	Kannan et al.	IT Security Breaches	(-1,2) (-1,7) (-1,29)
2009	Goel & Shawky	Estimated market impact from security breach announcements	(-119,10)
2010	Yayla & Hu	Information Security Breaches – Effect of Contingency Factors	(-1,1) (-1,5) (-1,10)
2010	Malhotra & Malhotra	Examining corporate stock market impact from security breaches and privacy exposure	(-1,1) (2,30)
2010	Gatzlaff & McCullough	Examining corporate stock market impact from data breach events (loss of both customer and employee data)	(-5,0) (-2,-1) (-1,0) (0) (6,10,20,30,35, 39) (0,40,60,180)
2011	Morse et al.	Examining corporate stock market impact from breaches in computer security (ComSec)	(0) (0,1) (1,220) (1,240) (1,440) (1,480) (0) (0,1) (1,5) (1,10)
2012	Cardenas et al.	Investigated corporate stock market impact from publicly announced security breaches	(-1,0,1)
2013	Andoh-Baidoo & Osei-Bryson	Investors Reaction to Internet Security Breach (using Deterrence Theory)	(-1,1)
2014	Hovav et al.	Investigated the stock market impact from security breach events	(0,270)

2014	Gwebu et al.	Examination of the stock market impact from an identified breach incident	(-90,0,90)
2014	Hinz et al.	Examined financial consequences to corporate stock market value from data theft events	(-10,10)
2014	Arcuri et al.	Stock market impact from InfoSec breaches and cyber-attacks and crime (1995 to 2012)	(-20,20) (-10,10) (-5,5) (-3,3) (-1,1)
2017	Hovav et al.	Stock market reaction to cyber incidents / breach announcements in South Korea	(-1,0) (-1,1) (-1,5) (-1,10) (-1,25)
2017	Berghel	Examined Equifax and Experian data breaches	N/A
Hacker Attack (3)			
2003	Ettredge & Richardson	Hacker Attacks	(1,3)
2010	Patel	Determining the effects of IT hacker announcements on corporate stock market value	(0,3) (0,8) (0,30)
2011	Chen et al.	Identifying changes in stock market value for companies providing info security products/services to the identified corporation's that had their data hacked	(0,1)
Defective IS / IT Product (s) (2)			
2005	Hovav & D'Arcy	Defective IT Products	(0,1) (0,5) (0,10) (0,25)
2007	Telang & Wattal	Defective IT Products	(0,1) (0,2) (0,5) (0,10)
Software Vulnerability (2)			
2003	Hovav & D'Arcy	Denial of Service (DOS) Attacks	(-1,0) (-1,1) (-1,5) (-1,10) (-1,25)
2003	Garg et al.	Non-Virus Security Breaches	(0) (0,1) (0,2)
Virus Attacks (1)			
2004	Hovav & D'Arcy	Virus Attack Announcements	(0) (0,1) (0,5) (0,10) (0,25)
Other IS / IT Security Threats (2)			
2006	Anthony et al.	Outages of Commercial Websites	(-1,2)
2014	Bose & Leung	Investigated if phishing alerts impact firm market value	(-1,0,1)
IS / IT Outsourcing Initiatives (8 Total Research Papers)			
2000	Hayes et al.	Outsourcing impact based on firm size and industry	(0,1)
2002	Peak et al.	Company Size, Effect on Risk from Outsourcing	(-45,-1) (-1,1) (2,45) (1,0) (-45,45)
2005	Florin et al.	IT Outsourcing	(-30,-1) (0,1) (2,250)
2006	Agrawal et al.	Outsourcing E-Commerce	(-1,1)
2006	Oh et al.	Contract Size, Vendor Characteristics from outsourcing	(-5,-1) (-1,0) (-1,1) (0,1) (0,2) (-2,2) (2,5) (-5,5)
2007	Gewald & Gellrich	Outsourcing	(0) (-1,1) (-3,3) (-10,10) (-20,20)
2009	Daniel et al.	Outsourcing	(0) (-1,0) (0,1) (-1,1)
2009	Duan et al.	Business Process Outsourcing	(-1,1)

IS / IT Announcement Events (Other) (16 Total Research Papers)			
IS / IT Other Announcements (7)			
1996	Hendricks & Singhal	Investigated the impact that receiving an award has on a corporation's market value	(-1,0,1)
1997	Hendricks & Singhal	Investigated the impact that new product delays have on a corporation's market value	(-1,0) (-5,5)
2000	Pardue et al.	New Product Announcement	(-1,0)
2001	Bharadwaj & Keil	Effects of IT failure on market value of effected corporation	(-1,0)
2006	Aggarwal et al.	XML Standardization	(-1,0)
2007	Song et al.	Code-sharing Agreements in the Airline Industry	(-1,0), (-20,2), (1,20)
2009	Bharadwaj et al.	Stock market impact from IT Project Failures	(-1,0)
Mergers & Acquisitions (4)			
1991	Koh & Venkatraman	Joint Venture Formation	(-1,0)
2006	Lee & Lim	Merger and Joint Ventures of IT Firms	(0,2)
2006	Uhlenbruck et al.	Acquisitions Involving Internet Firms	(0)
2014	Canace & Mann	Extend Lee and Lim (2006) and examined market impact of M&A's and Joint Ventures	(-1,1)
Website / Internet (3)			
2002	Geyskens et al.	Establishing an Internet Delivery Outlet	(-5,5)
2004	Benbunan-Fich & Fich	Web Traffic	(-1,1)
2005	Benbunan-Fich & Fich	Website Redesign	(-1,1), (-3,3), (-5,5)
Legal (2)			
2008	Raghu et al.	IT-Related Patent Infringements	(-1,0)
2010	Goel et al.	Legal Initiatives to Protect Digital Intellectual Capital (Peer-to-Peer File Sharing)	(-5,-1), (0), (1,5)

Appendix E

Data Filtering Process to Identify Data Sample Set



Appendix F

Table 19

Final Data Sample – Corporate Privacy Announcement Events

FINAL DISSERTATION DATA SAMPLE SET (PROQUEST (PQ) and BUSINESS SOURCE PREMIER (BSP) DATABASES:
CORPORATE PRESS RELEASE ANNOUNCEMENT EVENTS IN STUDY SAMPLE - 323 EVENTS

	ORIGINAL NUMBER (Previous Data Set)								STOCK MARKET SYMBOL			RESEARCH ARTICLE TITLE		
	ORIGINAL PQ NUMBER	ORIGINAL BSP NUMBER	UPDATED NUMBER	CORPORATION	PERMNO	DATE	SIC		NYSE	AMEX	NASDAQ	PROACTIVE (POS +) (GREEN)	REACTIVE (NEG -) (RED)	Keywords in Article Title Identifying "Proactive" (POS +) / "Reactive" (NEG -) Corporate Investment in Privacy (Privacy (data), Breach, Hack(ed), Security (breach), Violation)
	170		1	Google Inc.	90319	2013-01-23	7375				GOOG			
	172		2	eBay Inc.	86356	2013-01-24	7389				EBAY			
	173		3	Amazon Inc.	84788	2013-01-24	7374				AMZN			
		1	4	Google Inc.	90319	2013-02-19	7375				GOOG			EU Nations Weigh Action Against Google Privacy Practices
		2	5	Facebook Inc.	13407	2013-03-11	9999				FB			
	3		6	Google Inc.	90319	2013-03-13	7375				GOOG			Google reaches settlement with Ohio, 37 other states over data collection
	270		7	Facebook Inc.	13407	2013-04-01	9999				FB			
	4		8	Google Inc.	90319	2013-04-22	7375				GOOG			
		3	9	Google Inc.	90319	2013-05-17	7375				GOOG			Google Glass Privacy Worries Lawmakers
	5		10	Google Inc.	90319	2013-05-22	7375				GOOG			
	141		11	GE Healthcare	12060	2013-05-28	3511				GE			GE Healthcare achieves Infoway Certification for second Diagnostic Imaging product: Centricity ™ PACS
	6		12	Google Inc.	90319	2013-05-31	7375				GOOG			
	7		13	Verizon Comm.	65875	2013-06-06	4813		VZ					
	8		14	Google Inc.	90319	2013-06-10	7375				GOOG			
	9		15	Facebook Inc.	13407	2013-06-10	9999				FB			
NO TRADING DATA (WEEKEND): ADDED +2 DAYS	178		16	Yahoo! Inc.	83435	2013-06-10	7375				YHOO			
NO TRADING DATA (WEEKEND): ADDED +2 DAYS	179		17	Microsoft Corp.	10107	2013-06-10	7389				MSFT			
NO TRADING DATA (WEEKEND): ADDED +2 DAYS	180		18	Apple Inc.	14593	2013-06-10	3571				AAPL			
	10		19	Verizon Comm.	65875	2013-06-12	4813		VZ					
	11		20	Google Inc.	90319	2013-06-12	7375				GOOG			
	12		21	Research In Motion	86745	2013-06-18	3663		BB					
	13		22	Google Inc.	90319	2013-06-18	7375				GOOG			
	14		23	Apple Inc.	14593	2013-06-18	3571				AAPL			
	15		24	Microsoft Corp.	10107	2013-06-18	7389				MSFT			
	16		25	Dish Network	81696	2013-06-18	4841				DISH			
	17		26	Comcast Corp.	89525	2013-06-18	4841				CMCSA			
	181		27	Facebook Inc.	13407	2013-06-20	9999				FB			
	182		28	Google Inc.	90319	2013-06-20	7375				GOOG			
	183		29	Yahoo! Inc.	83435	2013-06-20	7375				YHOO			
	184		30	Constellation Research	64899	2013-06-20	8732		STZ					
	185		31	Microsoft Corp.	10107	2013-06-20	7389				MSFT			
		4	32	Google Inc.	90319	2013-06-21	7375				GOOG			
	18		33	Google Inc.	90319	2013-07-02	7375				GOOG			
	19		34	Google Inc.	90319	2013-07-31	7375				GOOG			
	20		35	Google Inc.	90319	2013-08-14	7375				GOOG			Google's email users should not expect privacy
NO TRADING DATA (WEEKEND): ADDED +1 DAY	21		36	Google Inc.	90319	2013-08-19	7375				GOOG			
	22		37	Facebook Inc.	13407	2013-08-28	9999				FB			
		6	38	Google Inc.	90319	2013-09-05	7375				GOOG			Google Is Sued in European-Privacy Test Case
		7	39	Facebook Inc.	13407	2013-09-09	9999				FB			Facebook Probed On Privacy Issues
	271		40	Google Inc.	90319	2013-09-10	7375				GOOG			Google DID break the law by harvesting data from people's homes with Street View cars, appeals court rules in landmark decision

FINAL DISSERTATION DATA SAMPLE SET (PROQUEST (PQ) and BUSINESS SOURCE PREMIER (BSP) DATABASES:
CORPORATE PRESS RELEASE ANNOUNCEMENT EVENTS IN STUDY SAMPLE - 323 EVENTS

	ORIGINAL NUMBER (Previous Data Set)								STOCK MARKET SYMBOL					RESEARCH ARTICLE TITLE
	23		41	Yahoo! Inc.	83435	2013-09-12	7375				YHOO			
NO TRADING DATA (WEEKEND): ADDED +2 DAYS	24		42	Apple Inc.	14593	2013-09-23	3571				AAPL			
	25		43	Google Inc.	90319	2013-09-27	7375				GOOG			Gmail wiretap lawsuit can move forward; Users object to reading of emails to target ads
		66	44	Google Inc.	90319	2013-10-11	7375				GOOG			Google's about to start selling your image to advertisers
		67	45	Facebook Inc.	13407	2013-10-11	9999				FB			
NO TRADING DATA (WEEKEND): ADDED +2 DAYS		8	46	Google Inc.	90319	2013-10-14	7375				GOOG			Privacy/Profits; Google, Facebook aim for balance in using data its users produce
	137		47	Facebook Inc.	13407	2013-10-15	9999				FB			
	26		48	Facebook Inc.	13407	2013-11-01	9999				FB			
	27		49	Google Inc.	90319	2013-11-01	7375				GOOG			
	28		50	Apple Inc.	14593	2013-11-01	3571				AAPL			
	29		51	Yahoo! Inc.	83435	2013-11-01	7375				YHOO			
	30		52	Microsoft Corp.	10107	2013-11-01	7389				MSFT			
	31		53	AOL	77418	2013-11-01	7812				AOL			
	32		54	Facebook Inc.	13407	2013-11-04	9999				FB			
	33		55	Google Inc.	90319	2013-11-19	7375				GOOG			Google to pay $500k to state in privacy case
	34		56	Google Inc.	90319	2013-11-22	7375				GOOG			Google pays $17 million compensation over privacy breach
		95	57	Amazon Inc.	84788	2013-12-02	7374				AMZN			
	272		58	Amazon Inc.	84788	2013-12-06	7374				AMZN			
	273		59	Google Inc.	90319	2013-12-06	7375				GOOG			
	35		60	Facebook Inc.	13407	2014-01-03	9999				FB			Facebook sued over alleged abuse of privacy
	190		61	Regeneron Pharmaceuticals	76614	2014-01-03	2834				REGN			
NO TRADING DATA (WEEKEND): ADDED +2 DAYS	36		62	IBM Inc.	12490	2014-01-06	3571		IBM					
	37		63	Google Inc.	90319	2014-01-09	7375				GOOG			
	38		64	Facebook Inc.	13407	2014-01-09	9999				FB			
		69	65	Target Inc.	49154	2014-01-10	5331		TGT					Target data breach highlights state privacy role
	275		66	CHE Trinity Health	55001	2014-01-16	8062		TRN					CHE Trinity Health Demonstrates Commitment to Protecting Patient Privacy
	41		67	Verizon Comm.	65875	2014-01-30	4813		VZ					Verizon Teams With PRIVO to Enable Identity Pilot to Protect Online Activities of Millions of Children
		61	68	Boeing Co.	19561	2014-03-05	3721		BA					
	43		69	Google Inc.	90319	2014-03-10	7375				GOOG			
	44		70	Apple Inc.	14593	2014-03-10	3571				AAPL			
	45		71	Microsoft Corp.	10107	2014-03-10	7389				MSFT			
	46		72	Salesforce Inc.	90125	2014-03-10	7372		CRM					
	47		73	Amazon Inc.	84788	2014-03-10	7374				AMZN			
	142		74	Microsoft Corp.	10107	2014-03-12	7389				MSFT			Microsoft takes a stand on student privacy with best-in-class education solutions
		9	75	WhatsApp (Facebook)	13407	2014-03-14	9999				FB			WhatsApp Faces Privacy Challenge
	276		76	WhatsApp (Facebook)	13407	2014-03-18	9999				FB			WhatsApp CEO reassures users on privacy, says won't collect new data; denies Facebook acquisition compromises user privacy
	279		77	Microsoft Corp.	10107	2014-03-21	7389				MSFT			Microsoft Software Leak Inquiry Raises Privacy Issues
	143		78	Facebook Inc.	13407	2014-03-24	9999				FB			
	144		79	Google Inc.	90319	2014-03-24	7375				GOOG			
	145		80	Netflix Inc.	89393	2014-03-24	7841				NFLX			
	281		81	Facebook Inc.	13407	2014-03-26	9999				FB			
	50		82	AVG Inc.	13255	2014-03-31	7372		AVG					
NO TRADING DATA (WEEKEND): ADDED +3 DAYS	51		83	Google Inc.	90319	2014-04-21	7375				GOOG			
	195		84	Accenture Inc	89071	2014-05-06	7389		ACN					
		72	85	Facebook Inc.	13407	2014-05-22	9999				FB			
		73	86	Google Inc.	90319	2014-05-22	7375				GOOG			
NO TRADING DATA (WEEKEND): ADDED +3 DAYS		99	87	Facebook Inc.	13407	2014-05-27	9999				FB			
	301		88	Apple Inc.	14593	2014-06-12	3571				AAPL			
		74	89	Facebook Inc.	13407	2014-06-13	9999				FB			Facebook will mine your Web searches to target ads; Not everyone is happy about it
		75	90	Google Inc.	90319	2014-06-13	7375				GOOG			

FINAL DISSERTATION DATA SAMPLE SET (PROQUEST (PQ) and BUSINESS SOURCE PREMIER (BSP) DATABASES:
CORPORATE PRESS RELEASE ANNOUNCEMENT EVENTS IN STUDY SAMPLE - 323 EVENTS

	ORIGINAL NUMBER (Previous Data Set)								STOCK MARKET SYMBOL					RESEARCH ARTICLE TITLE
		62	91	Google Inc.	90319	2014-06-25	7375				GOOG			
		10	92	Google Inc.	90319	2014-06-27	7375				GOOG			
NO TRADING DATA (WEEKEND): ADDED +1 DAY	283		93	Facebook Inc.	13407	2014-06-30	9999				FB			Facebook Changes Tracking Practices: Social Networking Giant Now Watching What Users Do on Phones, Other Websites
NO TRADING DATA (WEEKEND): ADDED +3 DAYS	284		94	Facebook Inc.	13407	2014-07-07	9999				FB			Facebook faces U.S. privacy complaint: Canadian privacy commission gives muted response to controversial research
NO TRADING DATA (WEEKEND): ADDED +3 DAYS	285		95	Cerner Innovation Inc.	10909	2014-07-07	7373				CERN			Cerner Innovation, Inc.; Patent Issued for HIPAA-Compliant Third Party Access to Electronic Medical Records
	52		96	Facebook Inc.	13407	2014-08-01	9999				FB			Facebook sued by law student Max Schrems for privacy violations
		11	97	Google Inc.	90319	2014-09-10	7375				GOOG			
	53		98	Taser International	89031	2014-09-11	3489				AAXN			
	55		99	Apple Inc.	14593	2014-09-16	3571				AAPL			
	302		100	Cerner Innovation Inc.	10909	2014-09-18	7373				CERN			Cerner Innovation, Inc.; Patent Application Titled "HIPAA-Compliant Third Party Access to Electronic Medical Records" Published Online
		12	101	Apple Inc.	14593	2014-09-24	3571				AAPL			Apple's Latest Marketing Pitch: More Privacy
		63	102	Google Inc.	90319	2014-09-24	7375				GOOG			
	196		103	8x8 Inc.	85177	2014-09-30	4813		EGHT					
	303		104	Microsoft Corp.	10107	2014-10-08	7389				MSFT			Tech firms pledge to protect data about pupils: Microsoft and 13 others won't sell details of those in high school or below
	159		105	PHT Corporation	89372	2014-10-09	6726		PHT					PHT Corporation Completes Safe Harbor Privacy Framework Compliance Certification
		13	106	Instagram (Facebook)	13407	2014-10-10	9999				FB			
		14	107	Apple Inc.	14593	2014-10-22	3571				AAPL			Apple's China iCloud Hacked
	56		108	Facebook Inc.	13407	2014-11-18	9999				FB			
		15	109	AT&T Inc.	66093	2014-11-19	4813		T					AT&T Joins Fray On Location Data
	287		110	Apple Inc.	14593	2014-12-05	3571				AAPL			
	288		111	Microsoft Corp.	10107	2014-12-05	7389				MSFT			
	289		112	Sony Corp.	51131	2014-12-05	3651		SNE					
NO TRADING DATA (WEEKEND): ADDED +1 DAY	57		113	Facebook Inc.	13407	2014-12-26	9999				FB			Facebook to face lawsuit on scanning of messages
	146		114	Varonis	14472	2015-01-07	7372				VRNS			Varonis Keeps Client and Company Data Protected and Private at Campbell Global, Timber Management and Investment Leader
	58		115	GE Healthcare	12060	2015-01-20	3511		GE					GE Healthcare and NextGen Healthcare First to Achieve EHNAC's Practice Management System Accreditation
	59		116	NextGen Healthcare	64961	2015-01-20	7372				NXGN			
	60		117	Google Inc.	90319	2015-01-20	7375				GOOG			
	61		118	Microsoft Corp.	10107	2015-01-20	7389				MSFT			
	62		119	Brocade	86881	2015-01-28	3572				BRCD			Brocade Enables Pervasive Data Privacy Across Public and Private Cloud
	63		120	Aon Plc.	61735	2015-01-29	6411		AON					Aon continues as Data Privacy Day Champion
	291		121	CapSpeciality	71271	2015-01-30	8049		Y					CapSpecialty rolls out new E&O product to protect from cyber attack
	64		122	Google Inc.	90319	2015-01-30	7375				GOOG			
	65		123	Microsoft Corp.	10107	2015-01-30	7389				MSFT			
	198		124	Navigant Consulting	84103	2015-02-11	8742		NCI					Navigant Expands Legal Technology Solutions Expertise with the Addition of Four Senior Professionals
NO TRADING DATA (WEEKEND): ADDED +3 DAYS	66		125	Apple Inc.	14593	2015-02-17	3571				AAPL			Tim Cook: Cyber privacy is a 'life and death' issue
		16	126	Synchronoss Technologies	91366	2015-03-30	7371				SNCR			
	67		127	Mattel Inc.	39538	2015-03-31	3942				MAT			New Barbie faces backlash; Group seeks to stop release of web-connected doll over privacy fears
	68		128	Facebook Inc.	13407	2015-04-10	9999				FB			Facebook seeks to stop court battle over 'privacy breach'
	292		129	Bell Mobility	29647	2015-04-16	4813		BCE					$750 Million Bell Mobility Privacy Breach Class Action Launched
	304		130	Sony Corp.	51131	2015-05-06	3651		SNE					
	305		131	FireEye	14159	2015-05-06	9999				FEYE			
	153		132	Google Inc.	90319	2015-06-02	7375				GOOG			
		101	133	Apple Inc.	14593	2015-06-10	3571				AAPL			
	70		134	eBay Inc.	86356	2015-06-11	7389				EBAY			
		17	135	Facebook Inc.	13407	2015-06-16	9999				FB			Facebook Faces Privacy Suit in Europe as Scrutiny Increases
	72		136	Facebook Inc.	13407	2015-06-19	9999				FB			
	73		137	Google Inc.	90319	2015-07-23	7375				GOOG			
	294		138	Hanover	82292	2015-07-27	6411		THG					Hanover Launches New Suite of Cyber Coverages: Innovative insurance program provides enhanced data breach protection for businesses
	199		139	Amazon Inc.	84788	2015-07-31	7374				AMZN			
	200		140	Microsoft Corp.	10107	2015-07-31	7389				MSFT			
	201		141	Google Inc.	90319	2015-07-31	7375				GOOG			

FINAL DISSERTATION DATA SAMPLE SET (PROQUEST (PQ) and BUSINESS SOURCE PREMIER (BSP) DATABASES:
CORPORATE PRESS RELEASE ANNOUNCEMENT EVENTS IN STUDY SAMPLE - 323 EVENTS

	ORIGINAL NUMBER (Previous Data Set)								STOCK MARKET SYMBOL					RESEARCH ARTICLE TITLE
	203		142	IBM Inc.	12490	2015-08-13	3571		IBM					IBM Assigned Patent for Enhanced Privacy and Control Features for Electronic Message
	202		143	AT&T Inc.	66093	2015-08-17	4813		T					
	74		144	Google Inc.	90319	2015-08-18	7375				GOOG			
		18	145	Microsoft Corp.	10107	2015-09-08	7389				MSFT			
	204		146	Liquidity Services Inc.	91095	2015-09-15	7389		LQDT					
	154		147	AVG Inc.	13255	2015-09-15	7372		AVG					AVG Releases One-page Privacy Policy And Challenges Industry To Follow
		19	148	Apple Inc.	14593	2015-09-16	3571				AAPL			
NO TRADING DATA (WEEKEND): ADDED +2 DAYS	76		149	Salesforce Inc.	90125	2015-09-28	7372		CRM					
NO TRADING DATA (WEEKEND): ADDED +2 DAYS	77		150	Facebook Inc.	13407	2015-09-28	9999				FB			
NO TRADING DATA (WEEKEND): ADDED +2 DAYS	78		151	Google Inc.	90319	2015-09-28	7375				GOOG			
		20	152	Apple Inc.	14593	2015-10-09	3571				AAPL			Apple Deletes Ad-Blocking Apps Amid Security Concerns
	79		153	Hewlett Packard (HP)	27828	2015-10-15	3571		HPQ					HP and 3M Team To Combat Visual Hacking With Innovative Integrated Screen Privacy Solution for PCs
	80		154	3M	22592	2015-10-15	3841		MMM					
	81		155	Quest Diagnostics Inc.	84373	2015-10-15	8071		DGX					
	295		156	Bottomline Technologies	86717	2015-11-11	7373				EPAY			Bottomline Technologies Healthcare Privacy and Data Security Solution Receives Meaningful Use Certification
	138		157	Microsoft Corp.	10107	2015-11-18	7389				MSFT			US Patent Issued to Microsoft Technology Licensing for "Information privacy system and method"
	139		158	Gartner Inc.	12570	2015-11-18	7361		IT					
	82		159	Twitter Inc.	14295	2015-12-22	7375		TWTR					
		21	160	Facebook Inc.	13407	2015-12-31	9999				FB			
	83		161	LifeLock Inc.	13616	2016-01-13	7382		LOCK					Online Trust Alliance Recognizes LifeLock Security and Privacy Practices
		76	162	Google Inc.	90319	2016-02-01	7375				GOOG			Berkley students sue Google for privacy breach
		23	163	Apple Inc.	14593	2016-02-18	3571				AAPL			U.S. and Apple Dig In for Court Fight Over Encryption
		24	164	Apple Inc.	14593	2016-02-22	3571				AAPL			Apple CEO Calls For Government Panel On Encryption Issues
		25	165	Apple Inc.	14593	2016-02-26	3571				AAPL			Apple Shareholders Show Support For Company's Privacy Stance
NO TRADING DATA (WEEKEND): ADDED +3 DAYS		26	166	Apple Inc.	14593	2016-03-28	3571				AAPL			Apple Says It May Not Need To Unlock iPhone In NY Case, Citing FBI
		77	167	Apple Inc.	14593	2016-03-30	3571				AAPL			End of Apple-FBI Dispute Could Intensify Larger Fight Over Data Privacy
		28	168	Mattel Inc.	39538	2016-04-12	3942				MAT			
	206		169	Microsoft Corp.	10107	2016-04-15	7389				MSFT			Microsoft sues US govt over data disclosures
NO TRADING DATA (WEEKEND): ADDED +2 DAYS	85		170	Facebook Inc.	13407	2016-05-09	9999				FB			
	208		171	Twitter Inc.	14295	2016-05-10	7375		TWTR					
	87		172	Box Inc.	15145	2016-05-17	7375		BOX					
	161		173	VeriSign Inc.	85753	2016-05-18	7372				VRSN			
	162		174	Tata Consultancy Services	14274	2016-06-01	7379		TCS					
	306		175	Apple Inc.	14593	2016-06-20	3571				AAPL			
	88		176	Microsoft Corp.	10107	2016-07-14	7389				MSFT			Microsoft ruling limits government access to data stored overseas
	210		177	Google Inc.	90319	2016-07-14	7375				GOOG			
	211		178	Facebook Inc.	13407	2016-07-14	9999				FB			
	212		179	PayPal Inc.	86356	2016-07-14	7389				PYPL (EBAY)			
		78	180	WhatsApp (Facebook)	13407	2016-08-16	9999				FB			
	89		181	WhatsApp (Facebook)	13407	2016-08-25	9999				FB			WhatsApp to Share User Data With Facebook
	91		182	Hewlett Packard (HP)	27828	2016-08-26	3571		HPQ					HP Introduces World's Only Notebooks With Integrated Privacy Screens
NO TRADING DATA (WEEKEND): ADDED +2 DAYS	296		183	WhatsApp (Facebook)	13407	2016-08-29	9999				FB			WhatsApp to share data with Facebook: Change disturbs users who counted on privacy of messaging service
	213		184	Yahoo! Inc.	83435	2016-10-04	7375				YHOO			Report: Yahoo searched customer emails for NSA
	93		185	Yahoo! Inc.	83435	2016-10-13	7375				YHOO			Digital privacy campaign urges users to 'Dump Yahoo'
NO TRADING DATA (WEEKEND): ADDED +1 DAY	94		186	Facebook Inc.	13407	2017-10-16	9999				FB			Facebook stokes privacy row with new data pact
		30	187	Facebook Inc.	13407	2016-10-27	9999				FB			Facebook defends use of clients' biometric data; Facial recognition technology could be abused, privacy advocates say
		31	188	Google Inc.	90319	2016-10-27	7375				GOOG			
		32	189	AT&T Inc.	66093	2016-10-27	4813		T					
NO TRADING DATA (WEEKEND): ADDED +2 DAYS	96		190	Facebook Inc.	13407	2016-10-31	9999				FB			
	307		191	Google Inc.	90319	2016-11-03	7375				GOOGL			
NO TRADING DATA (WEEKEND): ADDED +2 DAYS	97		192	Facebook Inc.	13407	2016-11-14	9999				FB			

FINAL DISSERTATION DATA SAMPLE SET (PROQUEST (PQ) and BUSINESS SOURCE PREMIER (BSP) DATABASES:
CORPORATE PRESS RELEASE ANNOUNCEMENT EVENTS IN STUDY SAMPLE - 323 EVENTS

	ORIGINAL NUMBER (Previous Data Set)								STOCK MARKET SYMBOL				RESEARCH ARTICLE TITLE
	98		193	Yahoo! Inc.	83435	2016-11-15	7375				YHOO		
	214		194	Adobe Systems Inc.	75510	2016-12-13	7374				ADBE		US Patent Issued to Adobe Systems for "Privacy preserving electronic document signature service"
NO TRADING DATA (WEEKEND): ADDED +1 DAY	308		195	Adobe Systems Inc.	75510	2016-12-27	7374				ADBE		Adobe Systems Inc.; Patent Issued for Privacy Preserving Electronic Document Signature Service
	215		196	Amazon Inc.	84788	2016-12-29	7374				AMZN		
		33	197	Google Inc.	90319	2017-01-10	7375				GOOG		
		34	198	Facebook Inc.	13407	2017-01-10	9999				FB		
	99		199	Facebook Inc.	13407	2017-01-31	9999				FB		Facebook Fights for User Privacy – WSJ
NO TRADING DATA (WEEKEND): ADDED +2 DAYS	216		200	Google Inc.	90319	2017-02-06	7375				GOOG		
	219		201	Yahoo! Inc.	83435	2017-02-06	7375				YHOO		
	220		202	Facebook Inc.	13407	2017-02-06	9999				FB		
	100		203	Facebook Inc.	13407	2017-02-08	9999				FB		
	101		204	Amazon Inc.	84788	2017-02-08	7374				AMZN		
	102		205	Honeywell Inc.	10145	2017-02-08	3714		HON				
	103		206	Google Inc.	90319	2017-02-08	7375				GOOG		
	104		207	Microsoft Corp.	10107	2017-02-08	7389				MSFT		
	163		208	Ooma Inc.	15582	2017-02-13	7374		OOMA				Ooma, Inc.; Patent Issued for Identifying and Filtering Incoming Telephone Calls to Enhance Privacy
NO TRADING DATA (WEEKEND): ADDED +2 DAYS	221		209	Facebook Inc.	13407	2017-02-21	9999				FB		
	309		210	Commvault Data Platform	91463	2017-02-21	7372				CVLT		Commvault Sees Growing Healthcare Industry Demand for Powerful Holistic Data Management: Growing security threats, industry consolidation, and use of the cloud are driving healthcare organizations to adopt the Commvault Data Platform –
	106		211	Microsoft Corp.	10107	2017-02-23	7389				MSFT		Microsoft commits to GDPR compliance in the cloud by 2018 deadline
	164		212	IBM Inc.	12490	2017-02-27	3571		IBM				
	165		213	Harris Corp.	85419	2017-03-03	8051		CSU				
	222		214	Amazon Inc.	84788	2017-03-06	7374				AMZN		
	223		215	Apple Inc.	14593	2017-03-07	3571				AAPL		
	225		216	Google Inc.	90319	2017-03-07	7375				GOOG		
	226		217	IBM Inc.	12490	2017-03-08	3571		IBM				
	227		218	Amazon Inc.	84788	2017-03-08	7374				AMZN		
	230		219	Intuit Inc.	78975	2017-03-08	7373				INTU		
	231		220	PayPal Inc.	86356	2017-03-08	7389				PYPL (EBAY)		
	232		221	Google Inc.	90319	2017-03-09	7375				GOOG		
	233		222	Apple Inc.	14593	2017-03-09	3571				AAPL		
	234		223	Mercury Inc.	52936	2017-03-09	3679				MRCY		
NO TRADING DATA (WEEKEND): ADDED +2 DAYS	235		224	Apple Inc.	14593	2017-03-13	3571				AAPL		
NO TRADING DATA (WEEKEND): ADDED +2 DAYS	236		225	Google Inc.	90319	2017-03-13	7375				GOOG		
NO TRADING DATA (WEEKEND): ADDED +2 DAYS	237		226	AT&T Inc.	66093	2017-03-13	4813		T				
NO TRADING DATA (WEEKEND): ADDED +2 DAYS	238		227	Verizon Comm.	65875	2017-03-13	4813		VZ				
NO TRADING DATA (WEEKEND): ADDED +2 DAYS	239		228	CenturyLink Inc.	60599	2017-03-13	4813		CTL				
NO TRADING DATA (WEEKEND): ADDED +2 DAYS	242		229	Facebook Inc.	13407	2017-03-13	9999				FB		
NO TRADING DATA (WEEKEND): ADDED +2 DAYS	243		230	Comcast Corp.	89525	2017-03-13	4841				CMCSA		
NO TRADING DATA (WEEKEND): ADDED +2 DAYS	244		231	Charter Comm.	12308	2017-03-13	4841				CHTR		
NO TRADING DATA (WEEKEND): ADDED +2 DAYS	245		232	Yahoo! Inc.	83435	2017-03-13	7375				YHOO		
	107		233	Facebook Inc.	13407	2017-03-15	9999				FB		Facebook bars developers from using data for surveillance
	246		234	Comcast Corp.	89525	2017-04-04	4841				CMCSA		
	247		235	Verizon Comm.	65875	2017-04-04	4813		VZ				
	248		236	Netflix Inc.	89393	2017-04-04	7841				NFLX		
	249		237	Google Inc.	90319	2017-04-04	7375				GOOG		
		36	238	AT&T Inc.	66093	2017-04-05	4813		T				
		100	239	Microsoft Corp.	10107	2017-04-18	7389				MSFT		
	250		240	Sprint/Nextel	91937	2017-04-19	4812				TMUS		
NO TRADING DATA (WEEKEND): ADDED +1 DAY	251		241	Google Inc.	90319	2017-04-24	7375				GOOG		
NO TRADING DATA (WEEKEND): ADDED +1 DAY	252		242	Facebook Inc.	13407	2017-04-24	9999				FB		
NO TRADING DATA (WEEKEND): ADDED +1 DAY	253		243	Comcast Corp.	89525	2017-04-24	4841				CMCSA		

FINAL DISSERTATION DATA SAMPLE SET (PROQUEST (PQ) and BUSINESS SOURCE PREMIER (BSP) DATABASES:
CORPORATE PRESS RELEASE ANNOUNCEMENT EVENTS IN STUDY SAMPLE - 323 EVENTS

	ORIGINAL NUMBER (Previous Data Set)								STOCK MARKET SYMBOL					RESEARCH ARTICLE TITLE
NO TRADING DATA (WEEKEND): ADDED +1 DAY	254		244	Spectrum (Time Warner Cable)	12308	2017-04-24	4841				CHTR			
NO TRADING DATA (WEEKEND): ADDED +1 DAY	255		245	Verizon Comm.	65875	2017-04-24	4813		VZ					
NO TRADING DATA (WEEKEND): ADDED +1 DAY		79	246	Apple Inc.	14593	2017-04-24	3571				AAPL			
	256		247	Visa Intl. Inc.	92611	2017-05-08	7389		V					
NO TRADING DATA (WEEKEND): ADDED +2 DAYS		82	248	Twitter Inc.	14295	2017-05-22	7375		TWTR					
NO TRADING DATA (WEEKEND): ADDED +2 DAYS		83	249	Facebook Inc.	13407	2017-05-22	9999				FB			
NO TRADING DATA (WEEKEND): ADDED +2 DAYS		84	250	Google Inc.	90319	2017-05-22	7375				GOOG			
NO TRADING DATA (WEEKEND): ADDED +1 DAY	299		251	Twitter Inc.	14295	2017-05-22	7375		TWTR					
		85	252	Google Inc.	90319	2017-05-24	7375				GOOG			Google data mine digs into credit card privacy
NO TRADING DATA (WEEKEND): ADDED +2 DAYS		86	253	Google Inc.	90319	2017-05-30	7375				GOOG			Google's data mine grows deeper; To prove its ads work, the company has begun connecting digital trails and offline purchases
		102	254	Delta Air Inc.	91926	2017-06-01	4512		DAL					
		103	255	JetBlue Inc.	89353	2017-06-01	4512				JBLU			
		38	256	Apple Inc.	14593	2017-06-07	3571				AAPL			
		39	257	Facebook Inc.	13407	2017-06-07	9999				FB			
		40	258	Amazon Inc.	84788	2017-06-07	7374				AMZN			
		104	259	Delta Air Inc.	91926	2017-06-20	4512		DAL					
	257		260	Comcast Corp.	89525	2017-06-20	4841				CMCSA			
	258		261	AT&T Inc.	66093	2017-06-20	4813		T					
	108		262	Google Inc.	90319	2017-06-23	7375				GOOG			Google Will Stop Reading Your Emails for Gmail Ads
NO TRADING DATA (WEEKEND): ADDED +1 DAY	259		263	IBM Inc.	12490	2017-06-26	3571		IBM					
NO TRADING DATA (WEEKEND): ADDED +1 DAY	260		264	Pure Storage	15729	2017-06-26	3572		PSTG					
	109		265	Google Inc.	90319	2017-06-27	7375				GOOG			Gmail will no longer scan your emails for advertising purposes
	167		266	Harris Corp.	85419	2017-06-27	8051		CSU					
NO TRADING DATA (WEEKEND): ADDED +1 DAY	261		267	Xerox Corp.	27983	2017-07-05	3577		XRX					Xerox Corporation; Patent Issues for Methods and Systems of Securely Storing Documents on a Mobile Device (USPTO 9686074)
NO TRADING DATA (WEEKEND): ADDED +1 DAY	262		268	Google Inc.	90319	2017-07-05	7375				GOOG			
NO TRADING DATA (WEEKEND): ADDED +1 DAY	263		269	Apple Inc.	14593	2017-07-05	3571				AAPL			
NO TRADING DATA (WEEKEND): ADDED +1 DAY	264		270	Facebook Inc.	13407	2017-07-05	9999				FB			
	110		271	Facebook Inc.	13407	2017-07-10	9999				FB			
NO TRADING DATA (WEEKEND): ADDED +2 DAYS		87	272	Equifax Inc.	52476	2017-09-11	7323		EFX					The Equifax Breach Exposes America's Identity Crisis
NO TRADING DATA (WEEKEND): ADDED +2 DAYS		88	273	Google Inc.	90319	2017-09-11	7375				GOOG			
	111		274	Apple Inc.	14593	2017-09-27	3571				AAPL			
	112		275	Twitter Inc.	14295	2017-11-03	7375		TWTR					
		89	276	Google Inc.	90319	2017-11-14	7375				GOOG			
		90	277	Facebook Inc.	13407	2017-11-14	9999				FB			
	168		278	Google Inc.	90319	2017-11-22	7375				GOOG			
		41	279	Apple Inc.	14593	2017-12-14	3571				AAPL			Apple's Consumer Privacy Push Smacks Targeted Ad Firm Criteo
NO TRADING DATA (WEEKEND): ADDED +1 DAY	300		280	Facebook Inc.	13407	2018-01-22	9999				FB			
NO TRADING DATA (WEEKEND): ADDED +1 DAY	267		281	Salesforce Inc.	90125	2018-01-22	7372		CRM					
		91	282	Facebook Inc.	13407	2018-03-20	9999				FB			
	149		283	Oracle Inc.	10104	2018-03-20	7372		ORCL					
		96	284	Facebook Inc.	13407	2018-03-22	9999				FB			Advocates Ask Facebook Why It's Opposing Privacy Act
	140		285	Twitter Inc.	14295	2018-03-22	7375		TWTR					
		42	286	Facebook Inc.	13407	2018-03-26	9999				FB			Facebook Data Scandal Worsens As FTC Announces Investigation
		43	287	Facebook Inc.	13407	2018-03-28	9999				FB			Facebook to Limit Use of Data Brokers for Ad Targeting
	116		288	Facebook Inc.	13407	2018-04-02	9999				FB			Facebook leak shows need for regulation of social media
		45	289	Facebook Inc.	13407	2018-04-04	9999				FB			CalSTRS Will Engage Facebook Amid Scandal on Privacy Issues
		46	290	Facebook Inc.	13407	2018-04-09	9999				FB			
NO TRADING DATA (WEEKEND): ADDED +1 DAY	311		291	Delta Air Inc.	91926	2018-04-09	4512		DAL					Delta Air Lines: Airports adopt high-tech security: Passengers find use of fingerprints, facial scans is on the rise
	119		292	Apple Inc.	14593	2018-04-10	3571				AAPL			The Latest: Apple co-founder bashes Facebook over privacy
	122		293	Facebook Inc.	13407	2018-04-11	9999				FB			Zuckerberg Says Facebook Collects Internet Data on Non-Users
		47	294	Facebook Inc.	13407	2018-04-23	9999				FB			

FINAL DISSERTATION DATA SAMPLE SET (PROQUEST (PQ) and BUSINESS SOURCE PREMIER (BSP) DATABASES:
CORPORATE PRESS RELEASE ANNOUNCEMENT EVENTS IN STUDY SAMPLE - 323 EVENTS

	ORIGINAL NUMBER (Previous Data Set)									STOCK MARKET SYMBOL					RESEARCH ARTICLE TITLE
	123			295	Google Inc.	90319	2018-04-24	7375				GOOG			
	124			296	Google Inc.	90319	2018-05-17	7375				GOOG			Google LLC Files Patent Application for Systems and Methods for Detecting Sensitive Information Leakage While Preserving Privacy
	125			297	Amazon Inc.	84788	2018-05-23	7374				AMZN			Amazon urged not to sell facial recognition tool
	127			298	BlackRock Income Growth Investment	87267	2018-05-25	6282		BLK					
	151			299	Virtru Inc.	15302	2018-05-31	9999				VIRT			Virtru Revolutionizing Data Privacy; Closes $37.5 Million Series B Investment
	152			300	Facebook Inc.	13407	2018-05-31	9999				FB			
	169			301	Apple Inc.	14593	2018-06-05	3571				AAPL			Apple Ups Privacy Controls in Growing Spat With Facebook
	130			302	Facebook Inc.	13407	2018-06-05	9999				FB			
		48		303	Facebook Inc.	13407	2018-06-29	9999				FB			
		49		304	Google Inc.	90319	2018-06-29	7375				GOOG			
		50		305	Amazon Inc.	84788	2018-06-29	7374				AMZN			
		51		306	Facebook Inc.	13407	2018-07-06	9999				FB			Facebook Stock Near Record High, Despite Data-Privacy Scandal Woes
	131			307	Facebook Inc.	13407	2018-08-07	9999				FB			
		52		308	Facebook Inc.	13407	2018-09-04	9999				FB			
		53		309	Twitter Inc.	14295	2018-09-04	7375		TWTR					
NO TRADING DATA (WEEKEND): ADDED +2 DAYS	132			310	Apple Inc.	14593	2018-09-17	3571				AAPL			Safari, Firefox browsers aim to thwart tracking ads
		54		311	Google Inc.	90319	2018-09-28	7375				GOOG			
		55		312	Facebook Inc.	13407	2018-09-28	9999				FB			
		56		313	Amazon Inc.	84788	2018-09-28	7374				AMZN			
		57		314	Facebook Inc.	13407	2018-10-18	9999				FB			
		58		315	Twitter Inc.	14295	2018-10-18	7375		TWTR					
		59		316	Google Inc.	90319	2018-10-18	7375				GOOG			
		92		317	Marriott Inc.	85913	2018-12-04	7011				MAR			Even If Your Personal Data Wasn't Stolen in the Latest Equifax Breaches, You're Probably Compromised
		93		318	Equifax Inc.	52476	2018-12-04	7323		EFX					
		94		319	Target Inc.	49154	2018-12-04	5331		TGT					
		60		320	Facebook Inc.	13407	2018-12-12	9999				FB			Facebook Denies Providing Tech Firms Unauthorized Access To User Data
NO TRADING DATA (WEEKEND): ADDED +1 DAY	133			321	Facebook Inc.	13407	2018-12-17	9999				FB			
NO TRADING DATA (WEEKEND): ADDED +1 DAY	134			322	Google Inc.	90319	2018-12-17	7375				GOOG			
	135			323	Facebook Inc.	13407	2018-12-19	9999				FB			D.C. sues Facebook over Cambridge Analytics data scandal

Appendix G

Table 20

Corporations Associated with *Proactive* (POS +) Investments in Privacy

FINAL DISSERTATION DATA SAMPLE SET (PROQUEST (PQ) and BUSINESS SOURCE PREMIER (BSP) DATABASES:
CORPORATE PRESS RELEASE ANNOUNCEMENT EVENTS IN STUDY SAMPLE - 323 EVENTS

POSITIVE (+) Corporate Investments in Privacy (51 of 323 - 15.79 % of Total Announcement Events)

CORPORATION	PERMNO	DATE	SIC CODE		PROACTIVE (POS +) (GREEN)		RESEARCH ARTICLE TITLE Keywords in Article Title Identifying "PROACTIVE" (POS +) / "REACTIVE" (NEG -) Corporate Investment in Privacy - (Privacy (data), Breach, Hack(ed), Security, Violation)
GE Healthcare	12060	2013-05-28	3511	1			GE Healthcare achieves Infoway Certification for second Diagnostic Imaging product: Centricity ™ PACS
CHE Trinity Health	55001	2014-01-16	8062	2			CHE Trinity Health Demonstrates Commitment to Protecting Patient Privacy
Verizon Comm.	65875	2014-01-30	4813	3			Verizon Teams With PRIVO to Enable Identity Pilot to Protect Online Activities of Millions of Children
Microsoft Corp.	10107	2014-03-12	7389	4			Microsoft takes a stand on student privacy with best-in-class education solutions
Facebook Inc.	13407	2014-06-30	9999	5			Facebook Changes Tracking Practices: Social Networking Giant Now Watching What Users Do on Phones, Other Websites
Cerner Innovation Inc.	10909	2014-07-07	7373	6			Cerner Innovation, Inc.: Patent Issued for HIPAA-Compliant Third Party Access to Electronic Medical Records
Cerner Innovation Inc.	10909	2014-09-18	7373	7			Cerner Innovation, Inc.: Patent Application Titled "HIPAA-Compliant Third Party Access to Electronic Medical Records" Published Online
Apple Inc.	14593	2014-09-24	3571	8			Apple's Latest Marketing Pitch: More Privacy
Microsoft Corp.	10107	2014-10-08	7389	9			Tech firms pledge to protect data about pupils: Microsoft and 13 others won't sell details of those in high school or below
PHT Corporation	89372	2014-10-09	6726	10			PHT Corporation Completes Safe Harbor Privacy Framework Compliance Certification
Varonis	14472	2015-01-07	7372	11			Varonis Keeps Client and Company Data Protected and Private at Campbell Global, Timber Management and Investment Leader
GE Healthcare	12060	2015-01-20	3511	12			GE Healthcare and NextGen Healthcare First to Achieve EHNAC's Practice Management System Accreditation
Brocade	86881	2015-01-28	3572	13			Brocade Enables Pervasive Data Privacy Across Public and Private Cloud
Aon Plc.	61735	2015-01-29	6411	14			Aon continues as Data Privacy Day Champion
CapSpeciality	71271	2015-01-30	8049	15			CapSpecialty rolls out new E&O product to protect from cyber attack
Navigant Consulting	84103	2015-02-11	8742	16			Navigant Expands Legal Technology Solutions Expertise with the Addition of Four Senior Professionals
Apple Inc.	14593	2015-02-17	3571	17			Tim Cook: Cyber privacy is a 'life and death' issue
Hanover	82292	2015-07-27	6411	18			Hanover Launches New Suite of Cyber Coverages: Innovative insurance program provides enhanced data breach protection for businesses
IBM Inc.	12490	2015-08-13	3571	19			IBM Assigned Patent for Enhanced Privacy and Control Features for Electronic Message
AVG Inc.	13255	2015-09-15	7372	20			AVG Releases One-page Privacy Policy And Challenges Industry To Follow
Apple Inc.	14593	2015-10-09	3571	21			Apple Deletes Ad-Blocking Apps Amid Security Concerns
Hewlett Packard (HP)	27828	2015-10-15	3571	22			HP and 3M Team To Combat Visual Hacking With Innovative Integrated Screen Privacy Solution for PCs
Bottomline Technologies	86717	2015-11-11	7373	23			Bottomline Technologies Healthcare Privacy and Data Security Solution Receives Meaningful Use Certification
Microsoft Corp.	10107	2015-11-18	7389	24			US Patent Issued to Microsoft Technology Licensing for "Information privacy system and method"
LifeLock Inc.	13616	2016-01-13	7382	25			Online Trust Alliance Recognizes LifeLock Security and Privacy Practices

POSITIVE (+) Corporate Investments in Privacy (51 of 323 - 15.79 % of Total Announcement Events)							
CORPORATION	**PERMNO**	**DATE**	**SIC CODE**		**PROACTIVE (POS +) (GREEN)**		**RESEARCH ARTICLE TITLE Keywords in Article Title Identifying "PROACTIVE" (POS +) / "REACTIVE" (NEG -) Corporate Investment in Privacy - (Privacy (data), Breach, Hack(ed), Security, Violation)**
Apple Inc.	14593	2016-02-18	3571	26			U.S. and Apple Dig In for Court Fight Over Encryption
Apple Inc.	14593	2016-02-22	3571	27			Apple CEO Calls For Government Panel On Encryption Issues
Apple Inc.	14593	2016-02-26	3571	28			Apple Shareholders Show Support For Company's Privacy Stance
Apple Inc.	14593	2016-03-28	3571	29			Apple Says It May Not Need To Unlock iPhone In NY Case, Citing FBI
Apple Inc.	14593	2016-03-30	3571	30			End of Apple-FBI Dispute Could Intensify Larger Fight Over Data Privacy
Microsoft Corp.	10107	2016-04-15	7389	31			Microsoft sues US govt over data disclosures
Microsoft Corp.	10107	2016-07-14	7389	32			Microsoft ruling limits government access to data stored overseas
Hewlett Packard (HP)	27828	2016-08-26	3571	33			HP Introduces World's Only Notebooks With Integrated Privacy Screens
Adobe Systems Inc.	75510	2016-12-13	7374	34			US Patent Issued to Adobe Systems for "Privacy preserving electronic document signature service"
Adobe Systems Inc.	75510	2016-12-27	7374	35			Adobe Systems Inc.; Patent Issued for Privacy Preserving Electronic Document Signature Service
Facebook Inc.	13407	2017-01-31	9999	36			Facebook Fights for User Privacy – WSJ
Ooma Inc.	15582	2017-02-13	7374	37			Ooma, Inc.; Patent Issued for Identifying and Filtering Incoming Telephone Calls to Enhance Privacy
Commvault Data Platform	91463	2017-02-21	7372	38			Commvault Sees Growing Healthcare Industry Demand for Powerful Holistic Data Management: Growing security threats, industry consolidation, and use of the cloud are driving healthcare organizations to adopt the Commvault Data Platform –
Microsoft Corp.	10107	2017-02-23	7389	39			Microsoft commits to GDPR compliance in the cloud by 2018 deadline
Facebook Inc.	13407	2017-03-15	9999	40			Facebook bars developers from using data for surveillance
Google Inc.	90319	2017-06-23	7375	41			Google Will Stop Reading Your Emails for Gmail Ads
Google Inc.	90319	2017-06-27	7375	42			Gmail will no longer scan your emails for advertising purposes
Xerox Corp.	27983	2017-07-05	3577	43			Xerox Corporation; Patent Issues for Methods and Systems of Securely Storing Documents on a Mobile Device (USPTO 9686074)
Apple Inc.	14593	2017-12-14	3571	44			Apple's Consumer Privacy Push Smacks Targeted Ad Firm Criteo
Facebook Inc.	13407	2018-03-28	9999	45			Facebook to Limit Use of Data Brokers for Ad Targeting
Delta Air Inc.	91926	2018-04-09	4512	46			Delta Air Lines: Airports adopt high-tech security: Passengers find use of fingerprints, facial scans is on the rise
Apple Inc.	14593	2018-04-10	3571	47			The Latest: Apple co-founder bashes Facebook over privacy
Virtru Inc.	15302	2018-05-31	9999	48			Virtru Revolutionizing Data Privacy; Closes $37.5 Million Series B Investment
Apple Inc.	14593	2018-06-05	3571	49			Apple Ups Privacy Controls in Growing Spat With Facebook
Apple Inc.	14593	2018-09-17	3571	50			Safari, Firefox browsers aim to thwart tracking ads
Marriott Inc.	85913	2018-12-04	7011	51			Even If Your Personal Data Wasn't Stolen in the Latest Equifax Breaches, You're Probably Compromised

Appendix H

Table 21

Corporations Associated with *Reactive* (NEG -) Investments in Privacy

FINAL DISSERTATION DATA SAMPLE SET (PROQUEST (PQ) and BUSINESS SOURCE PREMIER (BSP) DATABASES:
CORPORATE PRESS RELEASE ANNOUNCEMENT EVENTS IN STUDY SAMPLE - 323 EVENTS

NEGATIVE (-) Corporate Investments in Privacy (46 of 323 - 14.24 % of Total Announcement Events)

CORPORATION	PERMNO	DATE	SIC CODE			REACTIVE (NEG -) (RED)	RESEARCH ARTICLE TITLE Keywords in Article Title Identifying "PROACTIVE" (POS +) / "REACTIVE" (NEG -) Corporate Investment in Privacy - (Privacy (data), Breach, Hack(ed), Security, Violation)
Google Inc.	90319	2013-02-19	7375	1			EU Nations Weigh Action Against Google Privacy Practices
Google Inc.	90319	2013-03-13	7375	2			Google reaches settlement with Ohio, 37 other states over data collection
Google Inc.	90319	2013-05-17	7375	3			Google Glass Privacy Worries Lawmakers
Google Inc.	90319	2013-08-14	7375	4			Google: email users should not expect privacy
Google Inc.	90319	2013-09-05	7375	5			Google Is Sued in European-Privacy Test Case
Facebook Inc.	13407	2013-09-09	9999	6			Facebook Probed On Privacy Issues
Google Inc.	90319	2013-09-10	7375	7			Google DID break the law by harvesting data from people's homes with Street View cars, appeals court rules in landmark decision
Google Inc.	90319	2013-09-27	7375	8			Gmail wiretap lawsuit can move forward; Users object to reading of emails to target ads
Google Inc.	90319	2013-10-11	7375	9			Google's about to start selling your image to advertisers
Google Inc.	90319	2013-10-14	7375	10			Privacy/Profits; Google, Facebook aim for balance in using data its users produce
Google Inc.	90319	2013-11-19	7375	11			Google to pay $500k to state in privacy case
Google Inc.	90319	2013-11-22	7375	12			Google pays $17 million compensation over privacy breach
Facebook Inc.	13407	2014-01-03	9999	13			Facebook sued over alleged abuse of privacy
Target Inc.	49154	2014-01-10	5331	14			Target data breach highlights state privacy role
WhatsApp (Facebook)	13407	2014-03-14	9999	15			WhatsApp Faces Privacy Challenge
WhatsApp (Facebook)	13407	2014-03-18	9999	16			WhatsApp CEO reassures users on privacy, says won't collect new data; denies Facebook acquisition compromises user privacy
Microsoft Corp.	10107	2014-03-21	7389	17			Microsoft Software Leak Inquiry Raises Privacy Issues
Facebook Inc.	13407	2014-06-13	9999	18			Facebook will mine your Web searches to target ads; Not everyone is happy about it
Facebook Inc.	13407	2014-07-07	9999	19			Facebook faces U.S. privacy complaint: Canadian privacy commission gives muted response to controversial research
Facebook Inc.	13407	2014-08-01	9999	20			Facebook sued by law student Max Schrems for privacy violations
Apple Inc.	14593	2014-10-22	3571	21			Apple's China iCloud Hacked
AT&T Inc.	66093	2014-11-19	4813	22			AT&T Joins Fray On Location Data
Facebook Inc.	13407	2014-12-26	9999	23			Facebook to face lawsuit on scanning of messages
Mattel Inc.	39538	2015-03-31	3942	24			New Barbie faces backlash; Group seeks to stop release of web-connected doll over privacy fears
Facebook Inc.	13407	2015-04-10	9999	25			Facebook seeks to stop court battle over 'privacy breach'

NEGATIVE (-) Corporate Investments in Privacy (46 of 323 - 14.24 % of Total Announcement Events)							
CORPORATION	**PERMNO**	**DATE**	**SIC CODE**			**REACTIVE (NEG -) (RED)**	**RESEARCH ARTICLE TITLE Keywords in Article Title Identifying "PROACTIVE" (POS +) / "REACTIVE" (NEG -) Corporate Investment in Privacy - (Privacy (data), Breach, Hack(ed), Security, Violation)**
Bell Mobility	29647	2015-04-16	4813	26			$750 Million Bell Mobility Privacy Breach Class Action Launched
Facebook Inc.	13407	2015-06-16	9999	27			Facebook Faces Privacy Suit in Europe as Scrutiny Increases
Google Inc.	90319	2016-02-01	7375	28			Berkley students sue Google for privacy breach
WhatsApp (Facebook)	13407	2016-08-25	9999	29			WhatsApp to Share User Data With Facebook
WhatsApp (Facebook)	13407	2016-08-29	9999	30			WhatsApp to share data with Facebook: Change disturbs users who counted on privacy of messaging service
Yahoo! Inc.	83435	2016-10-04	7375	31			Report: Yahoo searched customer emails for NSA
Yahoo! Inc.	83435	2016-10-13	7375	32			Digital privacy campaign urges users to 'Dump Yahoo'
Facebook Inc.	13407	2017-10-16	9999	33			Facebook stokes privacy row with new data pact
Facebook Inc.	13407	2016-10-27	9999	34			Facebook defends use of clients' biometric data; Facial recognition technology could be abused, privacy advocates say
Google Inc.	90319	2017-05-24	7375	35			Google data mine digs into credit card privacy
Google Inc.	90319	2017-05-30	7375	36			Google's data mine grows deeper; To prove its ads work, the company has begun connecting digital trails and offline purchases
Equifax Inc.	52476	2017-09-11	7323	37			The Equifax Breach Exposes America's Identity Crisis
Facebook Inc.	13407	2018-03-22	9999	38			Advocates Ask Facebook Why It's Opposing Privacy Act
Facebook Inc.	13407	2018-03-26	9999	39			Facebook Data Scandal Worsens As FTC Announces Investigation
Facebook Inc.	13407	2018-04-02	9999	40			Facebook leak shows need for regulation of social media
Facebook Inc.	13407	2018-04-04	9999	41			CalSTRS Will Engage Facebook Amid Scandal on Privacy Issues
Facebook Inc.	13407	2018-04-11	9999	42			Zuckerberg Says Facebook Collects Internet Data on Non-Users
Amazon Inc.	84788	2018-05-23	7374	43			Amazon urged not to sell facial recognition tool
Facebook Inc.	13407	2018-07-06	9999	44			Facebook Stock Near Record High, Despite Data-Privacy Scandal Woes
Facebook Inc.	13407	2018-12-12	9999	45			Facebook Denies Providing Tech Firms Unauthorized Access To User Data
Facebook Inc.	13407	2018-12-19	9999	46			D.C. sues Facebook over Cambridge Analytics data scandal

Appendix I

Table 22

US SEC SIC Codes – Filtered by Corporate Assignment Designator

DIVISION	DIVISION NAME	SIC CODE	SIC CODE (DESCRIPTION)	NUMBER
J	**Public Administration**			**[75]**
		9999	Nonclassifiable Establishments	75
I	**Services**			**[160]**
		7375	Information Retrieval Services	87
		7389	Business Services, Not Elsewhere Classified	26
		7374	Computer Processing and Data Preparation and Processing Services	16
		8732	Commercial Economic, Sociological, and Educational Research	1
		7812	Motion Picture and Video Tape Production	1
		8062	General Medical and Surgical Hospitals	1
		7372	Prepackaged Software	10
		7841	Video Tape Rental	2
		7373	Computer Integrated Systems Design	4
		8049	Offices and Clinics of Health Practitioners, Not Elsewhere Classified	1
		8742	Management Consulting Services	1
		7371	Computer Programming Services	1
		8071	Medical Laboratories	1
		7361	Employment Agencies	1
		7382	Security Systems Services	1
		7379	Computer Related Services, Not Elsewhere Classified	1
		7011	Hotels aand Motels	1
		8051	Skilled Nursing Care Facilities	2
		7323	Credit Reporting Services	2

DIVISION	DIVISION NAME	SIC CODE	SIC CODE (DESCRIPTION)	NUMBER
D	**Manufacturing**			**[54]**
		3511	Steam, Gas, and Hydraulic Turbines, and Turbine Generator Set Units	2
		3571	Electronic Computers	38
		3663	Radio and Television Broadcasting and Communications Equipment	1
		2834	Pharmaceutical Preparations	1
		3721	Aircraft	1
		3489	Ordnance and Accessories, Not Elsewhere Classified	1
		3651	Household Audio and Video Equipment	2
		3572	Computer Storage Devices	2
		3942	Dolls and Stuffed Toys	2
		3841	Surgical and Medical Instruments and Apparatus	1
		3714	Motor Vehicle Parts and Accessories	1
		3679	Electronic Components, Not Elsewhere Classified	1
		3577	Computer Peripheral Equipment, Not Elsewhere Classified	1
E	**Transportation, Communications, Electric, Gas, And Sanitary Services**			**[28]**
		4813	Telephone Communications, Except Radiotelephone	15
		4841	Cable and Other Pay Television Services	8
		4812	Radiotelephone Communications	1
		4512	Air Transportation, Scheduled	4
G	**Retail Trade**			**[2]**
		5331	Variety Stores	2
H	**Finance, Insurance, And Real Estate**			**[4]**
		6726	Unit Investment Trusts, Face-Amount Certificate Offices, and Closed-End Mar	1
		6411	Insurance Agents, Brokers, and Service	2
		6282	Investment Advice	1

Appendix J

Table 23

US SEC SIC Codes – Corporate Breakdown by Division and Subdivision

DIVISION			DESCRIPTION	Number	Sample Data Set
J	**Public Administration**				
	SIC CODE	**9999**	**Nonclassifiable Establishments**	75	5, 7, 15, 27, 37, 39, 45, 47, 48, 54, 60, 64, 75, 76, 78, 81, 85, 87, 89, 93, 94, 96, 106, 108, 113, 128, 131, 135, 136, 150, 160, 170, 178, 180, 181, 183, 186, 187, 190, 192, 198, 199, 202, 203, 209, 229, 233, 242, 249, 257, 270, 271, 277, 280, 282, 284, 286, 287, 288, 289, 290, 293, 294, 299, 300, 302, 303, 306, 307, 308, 312, 314, 320, 321, 323
	Major Group:	99	Nonclassifiable Establishments		
	Industry Group:	999	Nonclassifiable Establishments		
I	**Services**				
	SIC CODE	**7375**	**Information Retrieval Services**	87	1, 4, 6, 8, 9, 10, 12, 14, 16, 20, 22, 28, 29, 32, 33, 34, 35, 36, 38, 40, 41, 43, 44, 46, 49, 51, 55, 56, 59, 63, 69, 79, 83, 86, 90, 91, 92, 97, 102, 117, 122, 132, 137, 141, 144, 151, 159, 162, 171, 172, 177, 184, 185, 188, 191, 193, 197, 200, 201, 206, 216, 221, 225, 232, 237, 241, 248, 250, 251, 252, 253, 262, 265, 268, 273, 275, 276, 278, 285, 295, 296, 304, 309, 311, 315, 316, 322
	Major Group:	73	Business Services		
	Industry Group:	737	Computer Programming, Data Processing, and other Computer Related Services		
	SIC CODE	**7389**	**Business Services, Not Elsewhere Classified**	26	3, 20, 27, 34, 55, 75, 78, 81, 88, 109, 116, 123, 128, 139, 145, 150, 151, 162, 175, 182, 185, 213, 217, 226, 245, 253
	Major Group:	73	Business Services		
	Industry Group:	738	Miscellaneous Business Services		
	SIC CODE	**7374**	**Computer Processing and Data Preparation and Processing Services**	16	4, 60, 61, 77, 144, 200, 201, 202, 210, 214, 220, 224, 264, 303, 311, 319
	Major Group:	73	Business Services		
	Industry Group:	737	Computer Programming, Data Processing, And Other Computer Related Services		
	SIC CODE	**8732**	**Commercial Economic, Sociological, and Educational Research**	1	33
	Major Group:	87	Engineering, Accounting, Research, Management, And Related Services		
	Industry Group:	873	Research, Development, And Testing Services		

DIVISION			DESCRIPTION	Number	Sample Data Set
I	Services				
	SIC CODE	**7812**	**Motion Picture and Video Tape Production**	1	56
	Major Group:	78	Motion Pictures		
	Industry Group:	781	Motion Picture Production And Allied Services		
	SIC CODE	**8062**	**General Medical and Surgical Hospitals**	1	69
	Major Group:	80	Health Services		
	Industry Group:	806	Hospitals		
	SIC CODE	**7372**	**Prepackaged Software**	10	76, 86, 119, 121, 152, 154, 179, 216, 287, 289
	Major Group:	73	Business Services		
	Industry Group:	737	Computer Programming, Data Processing, And Other Computer Related Services		
	SIC CODE	**7841**	**Video Tape Rental**	2	84, 242
	Major Group:	78	Motion Pictures		
	Industry Group:	784	Video Tape Rental		
	SIC CODE	**7373**	**Computer Integrated Systems Design**	4	99, 105, 161, 225
	Major Group:	73	Business Services		
	Industry Group:	737	Computer Programming, Data Processing, And Other Computer Related Services		
	SIC CODE	**8049**	**Offices and Clinics of Health Practitioners, Not Elsewhere Classified**	1	126
	Major Group:	80	Health Services		
	Industry Group:	804	Offices And Clinics Of Other Health Practitioners		
	SIC CODE	**8742**	**Management Consulting Services**	1	129
	Major Group:	87	Engineering, Accounting, Research, Management, And Related Services		
	Industry Group:	874	Management And Public Relations Services		
	SIC CODE	**7371**	**Computer Programming Services**	1	131
	Major Group:	73	Business Services		
	Industry Group:	737	Computer Programming, Data Processing, And Other Computer Related Services		
	SIC CODE	**8071**	**Medical Laboratories**	1	160
	Major Group:	80	Health Services		
	Industry Group:	807	Medical And Dental Laboratories		
	SIC CODE	**7361**	**Employment Agencies**	1	163
	Major Group:	73	Business Services		
	Industry Group:	736	Personnel Supply Services		
	SIC CODE	**7382**	**Security Systems Services**	1	167
	Major Group:	73	Business Services		
	Industry Group:	738	Miscellaneous Business Services		

DIVISION			DESCRIPTION	Number	Sample Data Set
I	**Services**				
	SIC CODE	**7379**	**Computer Related Services, Not Elsewhere Classified**	1	180
	Major Group:	73	Business Services		
	Industry Group:	737	Computer Programming, Data Processing, And Other Computer Related Services		
	SIC CODE	**7011**	**Hotels aand Motels**	1	323
	Major Group:	70	Hotels, Rooming Houses, Camps, And Other Lodging Places		
	Industry Group:	701	Hotelss and Motels		
	SIC CODE	**8051**	**Skilled Nursing Care Facilities**	2	219, 272
	Major Group:	80	Health Services		
	Industry Group:	805	Nursing And Personal Care Facilities		
	SIC CODE	**7323**	**Credit Reporting Services**	2	278, 324
	Major Group:	73	Business Services		
	Industry Group:	732	Consumer Credit Reporting Agencies, Mercantile		
D	**Manufacturing**				
	SIC CODE	**3511**	**Steam, Gas, and Hydraulic Turbines, and Turbine Generator Set Units**	2	14, 120
	Major Group:	35	Industrial And Commercial Machinery And Computer Equipment		
	Industry Group:	351	Engines And Turbines		
	SIC CODE	**3571**	**Electronic Computers**	38	21, 26, 45, 53, 65, 74, 92, 104, 106, 112, 115, 130, 138, 147, 153, 157, 158, 169, 170, 171, 172, 173, 181, 188, 218, 221, 223, 228, 230, 252, 262, 269, 275, 280, 285, 298, 307, 316
	Major Group:	35	Industrial and Commercial Machinery and Computer Equipment		
	Industry Group:	357	Computer aand Office Equipment		
	SIC CODE	**3663**	**Radio and Television Broadcasting and Communications Equipment**	1	24, 71
	Major Group:	36	Electronic And Other Electrical Equipment And Components, Except Computer Equipment		
	Industry Group:	366	Communications Equipment		
	SIC CODE	**2834**	**Pharmaceutical Preparations**	1	64
	Major Group:	28	Chemicals And Allied Products		
	Industry Group:	283	Drugs		
	SIC CODE	**3721**	**Aircraft**	1	72
	Major Group:	37	Transportation Equipment		
	Industry Group:	372	Aircraft and Parts		
	SIC CODE	**3489**	**Ordnance and Accessories, Not Elsewhere Classified**	1	103
	Major Group:	34	Fabricated Metal Products, Except Machinery And Transportation Equipment		
	Industry Group:	348	Ordnance And Accessories, Except Vehicles And Guided Missiles		

DIVISION			DESCRIPTION	Number	Sample Data Set
D	Manufacturing				
	SIC CODE	3651	Household Audio and Video Equipment	2	117, 135
	Major Group:	36	Electronic And Other Electrical Equipment And Components, Except Computer Equipment		
	Industry Group:	365	Household Audio And Video Equipment, And Audio		
	SIC CODE	3572	Computer Storage Devices	2	124, 270
	Major Group:	35	Industrial And Commercial Machinery And Computer Equipment		
	Industry Group:	357	Computer And Office Equipment		
	SIC CODE	3942	Dolls and Stuffed Toys	2	132, 174
	Major Group:	39	Miscellaneous Manufacturing Industries		
	Industry Group:	394	Dolls, Toys, Games And Sporting And Athletic		
	SIC CODE	3841	Surgical and Medical Instruments and Apparatus	1	159
	Major Group:	38	Measuring, Analyzing, And Controlling Instruments; Photographic, Medical And Optical Goods; Watches And Clocks		
	Industry Group:	384	Surgical, Medical, And Dental Instruments And Supplies		
	SIC CODE	3714	Motor Vehicle Parts and Accessories	1	211
	Major Group:	37	Transportation Equipment		
	Industry Group:	371	Motor Vehicles And Motor Vehicle Equipment		
	SIC CODE	3679	Electronic Components, Not Elsewhere Classified	1	229
	Major Group:	36	Electronic And Other Electrical Equipment And Components, Except Computer Equipment		
	Industry Group:	367	Electronic Components And Accessories		
	SIC CODE	3577	Computer Peripheral Equipment, Not Elsewhere Classified	1	273
	Major Group:	35	Industrial And Commercial Machinery And Computer Equipment		
	Industry Group:	357	Computer And Office Equipment		
E	Transportation, Communications, Electric, Gas, And Sanitary Services				
	SIC CODE	4813	Telephone Communications, Except Radiotelephone	15	16, 22, 70, 108, 114, 134, 148, 195, 232, 233, 234, 241, 244, 251, 267
	Major Group:	48	Communications		
	Industry Group:	481	Telephone Communications		
	SIC CODE	4841	Cable and Other Pay Television Services	8	28, 29, 236, 237, 240, 249, 250, 266,
	Major Group:	48	Communications		
	Industry Group:	484	Cable And Other Pay Television Services		
	SIC CODE	4812	Radiotelephone Communications	1	246
	Major Group:	48	Communications		
	Industry Group:	481	Telephone Communications		
	SIC CODE	4512	Air Transportation, Scheduled	4	260, 261, 265, 297
	Major Group:	45	Transportation By Air		
	Industry Group:	451	Air Transportation, Scheduled, And Air Courier		

DIVISION			DESCRIPTION	Number	Sample Data Set
G	**Retail Trade**				
	SIC CODE	**5331**	**Variety Stores**	2	68, 325
	Major Group:	53	General Merchandise Stores		
	Industry Group:	533	Variety Stores		
H	**Finance, Insurance, And Real Estate**				
	SIC CODE	**6726**	**Unit Investment Trusts, Face-Amount Certificate Offices, and Closed-End Management Investment Offices**	1	110
	Major Group:	67	Holding And Other Investment Offices		
	Industry Group:	672	Investment Offices		
	SIC CODE	**6411**	**Insurance Agents, Brokers, and Service**	2	125, 143
	Major Group:	64	Insurance Agents, Brokers, And Service		
	Industry Group:	641	Insurance Agents, Brokers, And Service		
	SIC CODE	**6282**	**Investment Advice**	1	304
	Major Group:	62	Security And Commodity Brokers, Dealers, Exchanges, And Services		
	Industry Group:	628	Services Allied With The Exchange Of Securities		

Appendix K

Table 24

Privacy Investment Announcement Event Breakdown (by Corporation)

	COMPANY	TOTAL NUMBER of Separate Announcement Events (January 1st 2013 - December 31st 2018)
1	Google Inc.	69
2	Microsoft Corp.	19
3	Ebay Inc.	2
4	Comcast Corp.	5
5	AT&T Inc.	6
6	IBM Inc.	5
7	Facebook Inc.	67
8	Verizon Comm.	6
9	AOL	1
10	Regeneron Pharmaceuticals	1
11	Target Inc.	2
12	CHE Trinity Health	1
13	Boeing Co.	1
14	Netflix Inc.	2
15	Accenture Inc.	1
16	Cerner Innovation Inc.	2
17	Taser International	1
18	8x8 Inc.	1
19	PHT Corporation	1
20	Instagram (Facebook)	1
21	Varonis	1
22	GE Healthcare	2
23	NextGen Healthcare	1
24	Brocade	1
25	Aon Plc.	1
26	CapSpeciality	1
27	Navigant Consulting	1
28	Synchronoss Technologies Inc.	1
29	Bell Mobility	1
30	Sony Corp.	2
31	FireEye	1
32	Hanover	1
33	Liquidity Services Inc.	1
34	AVG Inc.	2
35	3M	1
36	Quest Diagnostics Inc.	1
37	Bottomline Technologies	1
38	Pure Storage	1
39	Harris Corp.	2
40	Xerox Corp.	1
41	Apple Inc.	31
42	Equifax Inc.	2
43	SalesForce Inc.	3
44	Oracle Inc.	1
45	Delta Air Lines	3
46	Blackrock Income Growth Investment	1
47	Virtru Inc.	1
48	Gartner Inc.	1
49	Twitter Inc.	8
50	LifeLock Inc.	1
51	Mattel Inc.	2
52	Box Inc.	1
53	VeriSign Inc.	1
54	Tata Consultancy Services Inc.	1
55	PayPal Inc.	2
56	Hewlett Packard (HP)	2
57	WhatsAp (Facebook)	5
58	Yahoo! Inc.	9
59	Adobe Systems Inc.	2
60	Amazon Inc.	13
61	Honeywell Inc.	1
62	Ooma Inc.	1
63	Research In Motion (RIM)	1
64	Dish Network	1
65	Constellation Research	1
66	Commvault (Data Platform)	1
67	Intuit Inc.	1
68	Mercury Inc.	1
69	CenturyLink Inc.	1
70	Charter Comm.	1
71	Sprint/Nextel	1
72	Spectrum (Time Warner Cable)	1
73	Mariott Inc.	1
74	Visa Intl. Inc.	1
75	JetBlue Inc.	1
		323 Total Announcement Events

Appendix L

Table 25

Statistical Significance Testing (Levels)

Statistical Significance Levels – Based on **StdCsect *p* -value and General Sign Test (GST) *p* –value**			
Probability Level (%) (Accuracy)	Error Probability (%) (Accident)	Confidence Level (%)	Statistically Significant *p* levels
90%	10%	0.10 %	$p < 0.10$
95%	5%	0.05 %	$p < 0.05$ **
99%	1%	0.01 %	$p < 0.01$
99.9%	0.001%	0.001 %	$p < 0.001$
** *p* levels < 0.05 were accepted as "Statistically Significant" in this research in accordance with event study guidelines			

Statistical testing for significance was important in this research to identify any relationships existing between observable increased (+) / decreased (-) financial impact to overall corporate stock market value associated with corporate investments in privacy.

Observed (*p* values) that fell within recognized "Statistically Significant" ranges were accepted in this research as indicating a relationship existing between the observed financial impact to overall corporate stock market value (Mean CAR) and the associated corporate investment in privacy. The type and strength of the identified relationship was indicated by the level of the statistical significance.

Appendix M

Table 26

Relationship Correlation from Overall Stock Market Impact

(Based on Observed *p* Values)

Statistical Significance Levels – Based on **StdCsect *p* -value and General Sign Test (GST) *p* –value**				
Probability Level (%) (Accuracy)	Error Probability (%) (Accident)	Confidence Level (%)	Statistically Significant *p* levels	Identified Relationship
90%	10%	0.10 %	$p < 0.10$	Weak
95%	5%	0.05 %	$p < 0.05$ **	Statistically Significant
99%	1%	0.01 %	$p < 0.01$	Strong
99.9%	.001%	0.001 %	$p < 0.001$	Very Strong
** *p* levels < 0.05 were accepted as "Statistically Significant" in this research in accordance with event study guidelines				

Observed (*p* values) that fell within recognized "Statistically Significant" ranges were accepted in this research as indicating a relationship existing between the observed financial impact to overall corporate stock market value (Mean CAR) and the associated corporate investment in privacy. The type and strength of the identified relationship was indicated by the level of the statistical significance.

Appendix N

Table 27

Largest Data Breach Events Leading to Information Loss and Exploitation of User Personal Identifiable Information (PII)

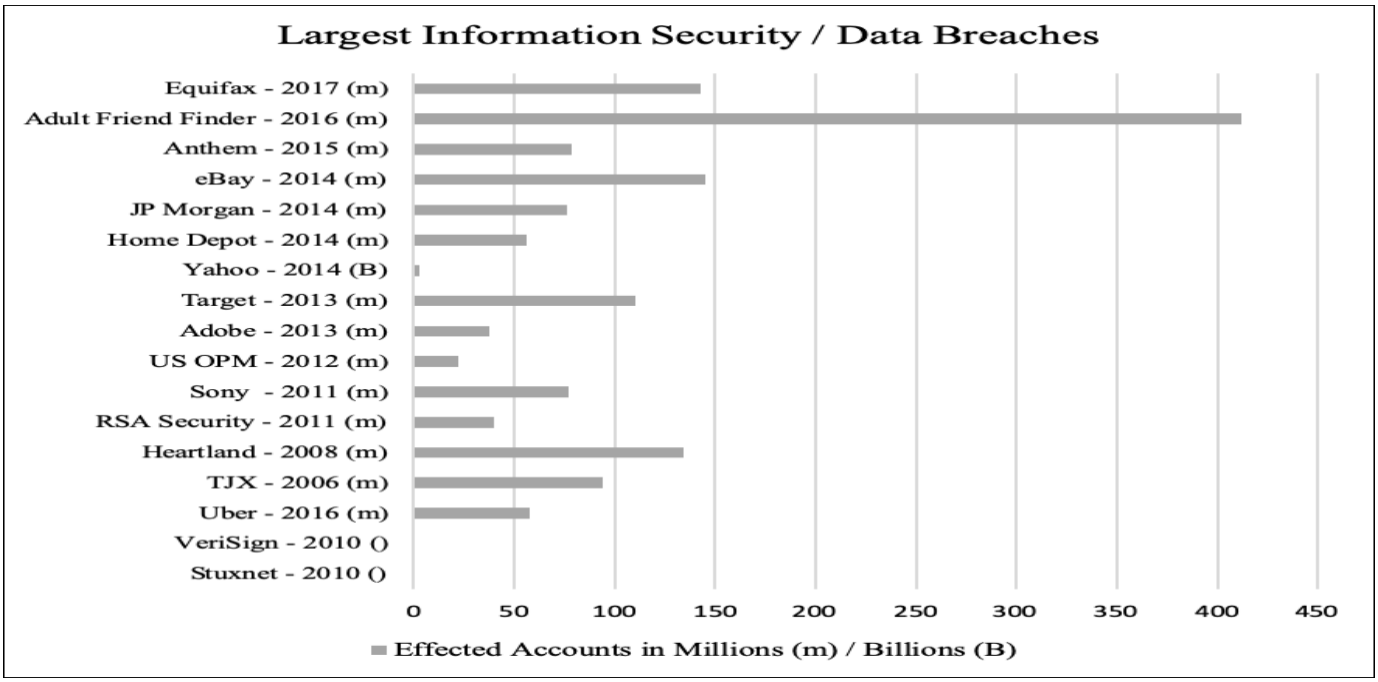


Table 5 – Largest US InfoSec Attacks Leading to Privacy / Data Breach

Data is illustrated by name of company, year of InfoSec breach incident leading to Privacy / Data breach, and volume of affected users in Millions / Billions of accounts

* *n* = designates volume of affected users in *Millions* of accounts
* *B* = designates volume of affected users in *Billions* of accounts

Note:
While not admitting to the exact extent / severity of the security breach incident, *VeriSign* (Greene, 2012) in 2010, and *Heartland Payment Systems* (Messmer, 2009) also experienced data breach events. The *Heartland* breach incident is believed to have exposed nearly 150 million (m) user records, the alleged breach results cannot be taken as a certainty without corporate confirmation to the exact disclosure damage.

Furthermore, due to potential political fallout and geopolitics, there is near uncertainty surrounding exact levels of success and deployment execution of the *Stuxnet* threat. Due to near total secrecy surrounding *Stuxnet*, information relating to parties / nation states affected, damage estimates, and devastation potential have never been realized to the general public but instead relegated to those with permissible legal, authoritative, and "need-to-know" clearance. As can be seen, the enormous financial cost of an InfoSec breach from lost revenue, government fines, and lost consumer trust, as well as financial value of digital records, data is one of the most coveted and valuable resources that corporations must protect.

References

Acquisti, A., Friedman, A., & Telang, R. (2006). Is There a Cost to Privacy Breaches? An Events Study. *Fifth Workshop on the Economics of Information Security*, 1563-1580.

Afroz, S., Islam, A. C., Santell, J., Chapin, A., & Greenstadt, R. (2012). How Privacy Flaws Affect Consumer Perception. *Intel Science & Technology Center* (ISTC) *for Secure Computing, Working Paper*.

Aggarwal, N., Dai, Q., & Walden, E. A. (2006). Do Markets Prefer Open or Proprietary Standards for XML Standardization? *International Journal of Electronic Commerce, 11*(1), 117-136.

Agrawal, M., Kishore, R., & Rao, H. R. (2006). Market Reactions to E-business Outsourcing Announcements: An Event Study. *Information & Management, 43*(7), 861-873.

Altman, E. I. (1983). Corporate Financial Distress. *New York, New York: John Wiley and Sons*.

Andoh-Baidoo, F. K. (2013). Explaining Investors' Reaction to Internet Security Breach using Deterrence Theory. *International Journal of Electronic Finance, 7*(1), 1-14.

Andoh-Baidoo, F. K., & Osei-Bryson, K. M. (2007). Exploring the Characteristics of Internet Security Breaches that Impact the Market Value of Breached Firms. *Expert Systems with Applications*, *32*(3), 703-725.

Andrews, S. (2002). Privacy and Human Rights: An International Survey of Privacy Laws and Developments. http://www.privacyinternational.org/survey/phr2002/.

Anthony, J. H., Choi, W., & Grabski, S. (2006). Market Reaction to e-Commerce Impairments Evidenced by Website Outages. *International Journal of Accounting Information Systems*, *7*(2), 60-78.

Armerding, T. (2016, October). The OPM breach report: A long time coming. Retrieved from https://www.csoonline.com/article/3130682/the-opm-breach-report-a-long-time-coming.html.

Armerding, T. (2018, December). The 18 biggest data breaches of the 21st century. Retrieved from https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html.

Awad, N. F., & Krishnan, M. S. (2006). The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to be Profiled Online for Personalization. *MIS Quarterly, 30*(1), 13 – 28.

Aytes, K., Byers, S., & Santhankrishnan, M. (2006). The Economic Impact of Information Security Breaches: Firm Value and Intra-industry Effects. *Americas Conference on Information Systems*, 3305-3312.

Bayer, R., & Colgrove, J. (2002). Bioterrorism, public health and the law. *Health Affairs, 21*(6), 98–101.

Beaver, W. H. (1968). The Information Content of Annual Earnings Announcements. *Journal of Accounting Research, (Supplement Empirical Research in Accounting: Selected Studies), 6*, 67-92.

Belanger, F., Hiller, J. S., & Smith, W. J. (2002). Trustworthiness in electronic commerce: The role of privacy, security, and site attributes. *Journal of Strategic Information Systems, 11*(3-4), 245-270.

Bélanger, F., & Crossler, R. E. (2011). Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. *MIS Quarterly 35*(4), 1017–41.

Benbunan-Fich, R., & Fich, E. M. (2004). Effects of Web Traffic Announcements on Firm Value. *International Journal of Electronic Commerce, 8*(4), 161-181.

Benbunan-Fich, R., & Fich, E. M. (2005). Measuring the Value of Refining a Web Presence. *Journal of Electronic Commerce in Organizations, 3*(1), 35-52.

Benco, D. C., & Prather, L. (2008). Market Reaction to Announcements to Invest in ERP Systems. *Quarterly Journal of Finance & Accounting, 47*(4), 145-169.

Berghel, H. (2017). Equifax and the Latest Round of Identity Theft Roulette. *IEEE Computer Society, 50*(12), 72-76.

Bergkamp, L. (2002). EU data protection policy: the privacy fallacy—adverse effects of Europe's data protection policy in an information-driven economy. *Computer Law & Security Report 18*(1), pp. 31–47.

Bharadwaj, A., & Keil, M. (2001). The effects of Information technology failures on the market value of firms: an empirical examination. Working paper, Emory University.

Bharadwaj, A., Keil, M., & Mähring, M. (2009). Effects of information technology failures on the market value of firms. *The Journal of Strategic Information Systems, 18*(2), 66-79.

Boehmer, E., Masumeci, J., & Poulsen, A. B. (1991). Event-study methodology under conditions of event-induced variance. *Journal of Financial Economics, 30*(2), 253-272.

Bollerslev, T. (1986). Generalized autoregressive conditional heteroskedasticity. *Journal of Econometrics, 31*(3), 307-327.

Bollerslev, T. (1987). A conditionally heteroskedastic time series model for speculative prices and rates of return. *Review of Economics and Statistics, 69*(3), 542-547.

Bollerslev, T., Engle, R. F., & Wooldridge, J. M. (1988). A capital asset pricing model with time-varying covariances. *Journal of political Economy, 96*(1), 116-131.

Bose, I., & Leung, A. C. M. (2014). Do Phishing Alerts Impact Global Corporations? A Firm Value Analysis. *Decision Support Systems, 64*, 67-78.

Brock, L. (2012). The Market Value of Information System (IS) Security: An Event Study of e-Banking Service Providers, *Dissertation* (Nova Southeastern University).

Brown, S. J., & Warner, J. B. (1980). Measuring security price performance. *Journal of Financial Economics, 8*(3), 205-258.

Brown, S. J., & Warner, J. B. (1985). Using Daily Stock Returns: The Case of Event Studies. *Journal of Financial Economics, 14*, 3-31.

Brumfield, C. (2019, July). Equifax's data breach disaster: Will it change executive attitudes toward security? Retrieved from https://www.csoonline.com/article/3411139/equifax-s-billion-dollar-data-breach-disaster-will-it-change-executive-attitudes-toward-security.html.

Brynjolfsson, E., & Hitt, L. (1996). Paradox lost? Firm-level evidence on the returns to information systems spending. *Management Science, 42*(4), 541–558.

Brynjolfsson, E. (1993). The productivity paradox of information technology. *Communications of the ACM, 36*(12), 66–77.

Brynjolfsson, E. (1994). Information assets, technology, and organization. *Management Science, 40*(12), 1645–1662.

Brynjolfsson, E., & Hitt, L. (1993). Is information system spending productive? New evidence and new results. *Proceedings of the 14th International Conference of Information Systems,* 47–64.

Brynjolfsson, E., & Hitt, L. (1998). Beyond the productivity paradox. *Communications of the ACM, 41*(8), 49–55.

Brynjolfsson, E., & Yang, S. (1996). Information technology and productivity: A review of the literature. *Advanced Computers, 43*, 179–214.

Calcutt, D. (1990). Report of the Committee on Privacy and Related Matters, Cmnd. *1102, London, HMSO*, p. 7.

Campbell, A. J. (1997). Relationship marketing in consumer markets: A comparison of managerial and consumer attitudes about information privacy. *Journal of Direct Marketing, 11*(3), 44–57.

Campbell, C. J., Cowan, A. R., & Salotti, V. (2010). Multi-country event-study methods. *Journal of Banking & Finance*, *34*(12), 3078-3090.

Campbell, K., Gordon, L., Loeb, M. P., & Zhou, L. (2003). The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market. *Journal of Computer Security*, *11*, 431-448.

Canace, T. G., & Mann, S. V. (2014). The impact of technology-motivated M&A and joint ventures on the value of IT and non-IT firms: a new examination. *Review of Quantitative Finance and Accounting*, *43*(2), 333-366.

Cardenas, J., Coronado, A., Donald, A., Parra, F., & Mahmood, M. A. (2012). The economic impact of security breaches on publicly traded corporations: an empirical investigation. *AMCIS Proceedings*.

Case, C. J., King, D. L., & Gage, L. M. (2015). Online Privacy and Security at the Fortune 500: An Empirical Examination of practices. *American Society of Business and Behavioral Sciences, 11*(1), 59 – 67.

Cate, F. H. (2005). Information Security Breaches and the Threat to Consumers. *The Center for Information Policy Leadership at Hunton & Williams*, LLP.

Caudill, E. M., & Murphy, P. E. (2000). Consumer online privacy: Legal and ethical issues. *Journal of Public Policy Marketing 19*(1), 7–19.

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. *International Journal of Electronic Commerce*, *9*(1), 69–104.

Chai, S., Kim, M., & Rao, H. R. (2011). Firms' information security investment decisions: Stock market evidence of investors' behavior. *Decision Support Systems*, *50*, 651-661.

Chatterjee, D., Richardson, V. J., & Zmud, R. W. (2001). Examining the Shareholder Wealth Effects of Announcements of Newly Created CIO Position. *MIS Quarterly, 25*(1), 43-70.

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.

Chávez, G., & Lorenzo, O. (2006). The Impact of Supply Chain Applications Announcements on The Market Value of Firms. *Supply Chain Forum*, *7*(2), 36-42.

Chen, A. H., & Siems, T. F. (2001). B2B eMarketplace Announcements and Shareholder Wealth. *Economic & Financial Review*, 12-22.

Chen, J. V., Li., H-C., Yen, D. C., & Bata, K. V. (2011). Did IT consulting firms gain when their clients were breached? *Computers in Human Behavior, 28*, 456-464.

Chen, K., & Rea Jr, A.I. (2004). Protecting personal information online: A survey of user privacy concerns and control techniques. *The Journal of Computer Information Systems, 44*(4), 85-92.

Cheng, J. M. -S., Tsao, S. -M., Tsai, W. -H., & Tu, H. H. -J. (2007). Will eChannel Additions Increase the Financial Performance of the Firm? - The Evidence from Taiwan. *Industrial Marketing Management, 36*(1), 50-57.

Cherdantseva, Y., & Hilton, J. (2013). A Reference Model of Information Assurance & Security. *Availability, Reliability and Security, Eighth International Conference, IEEE*, 546-555.

Cherdantseva, Y., & Hilton, J. (2013). Information Security and Information Assurance: The Discussion about the Meaning, Scope and Goals in Organizational, Legal, and Technological Dimensions of IS Administrator. *IGI Global Publishing*.

Choi, B., & Jong, A. M. (2010). Assessing the impact of knowledge management strategies announcements on the market value of firms. *Information & Management, 47*(1), 42-52.

Constantin, L. (2016, September). Here's what you should know, and do, about the Yahoo breach. Retrieved from https://www.csoonline.com/article/3123403/heres-what-you-should-know-and-do-about-the-yahoo-breach.html.

Corrado, C. J. (1989). A Nonparametric Test for Abnormal Security Price Performance in Event Studies. *Journal of Financial Economics, 23*(2), 385-396.

Cowan, A. (1992). Nonparametric Event Study Tests. *Review of Quantitative Finance And Accounting, 2*(4), 343-358.

Cowan, A. R. (1993). Tests for cumulative abnormal returns over long periods: Simulation evidence. *International Review of Financial Analysis*, *2*(1), 51-68.

Cullen, R. (2009). Culture, identity and information privacy in the age of digital government. *Online Information Review, 33*(3), 405-421.

Culnan, M. J. (1993). "How did they get my name?": An exploratory investigation of consumer attitudes toward secondary information use. *MIS Quarterly, 17*(3), 341-363.

Culnan, M. J. (2000). Protecting privacy online: Is self-regulation working? *Journal of Public Policy Marketing, 19*(1) 20–26.

Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science, 10*(1), 104-115.

Culnan, M. J., & Williams, C. C. (2009). How ethics can enhance organizational privacy: Lessons from the Choice Pointe and TJX data breaches. *MIS Quarterly, 33*(4), 673-687.

Culnan, M. J., & Bies, R. J. (2003). Consumer privacy: Balancing economic and justice considerations. *Journal of Social Issues, 59*(2), 323–342.

Cybersecurity Information Sharing Act of 2015 (2015).

D'Amico, A. (2000). What Does a Computer Security Breach Really Cost? *The Sans Institute*.

Daniel, E., Kodwani, D., & Datta, S. (2009). The Impact of ICT-Enabled Offshoring Announcements on Share Prices. *Journal of Enterprise Information Management, 22*(3), 241-256.

Dardan, M., Stylianou, A., & Dardan, S. (2005). The Valuation of Ecommerce Announcements During Fluctuating Financial Markets. *Journal of Electronic Commerce Research, 6*(4), 312-326.

Dardan, S., Stylianou, A., & Kumar, R. (2006). The Impact of Customer-Related IT Investments on Customer Satisfaction and Shareholder Returns. *Journal of Computer Information Systems*, *47*(2), 100-111.

Davis, A. (2005). Return on security investment – proving it's worth it. *Network Security*, (11), 8–10.

Dehning, B., Richardson, V. J., & Zmud, R. W. (2003). The Value Relevance of Announcements of Transformational Information Technology Investments. *MIS Quarterly, 27*(4), 637-656.

Dehning, B., Richardson, V. J., & Stratopoulos, T. (2003). Reviewing Event Studies in MIS: An Application of the Firm Value Framework. *Proceedings of 36th Hawaii International Conference on System Sciences (HICSS)*.

Dehning, B., Richardson, V. J., Urbaczewski, A., & Wells, J. D. (2004). Reexamining the Value Relevance of Ecommerce Initiatives. *Journal of Management Information Systems (JMIS), 21*(1), 55-82.

Dempsey, J. X., Anderson, P., & Schwartz, A. (2003). Privacy and E-Government: A Report to the United Nations Department of Economic and Social Affairs as Background for the World Public Sector Report: E-government. *Center for Democracy and Technology*. Washington, DC. Retrieved from: www.internetpolicy.net/privacy/20030523cdt.pdf

Dewan, S., & Ren, F. (2007). Risk and Return of Information Technology Initiatives: Evidence from Electronic Commerce Announcements. *Information Systems Research (ISR), 18*(4), 370-394.

Dinev, T. & Hart, P. (2004). Internet privacy concerns and their antecedents – measurement validity and a regression model. *Behavior and Information Technology, Vol. 23*(6), pp. 413-22.

Dinev, T. & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research (ISR), 17*(1), 61-80.

Dinev, T., Bellotto, M., Hart, P., Colautti, C., Russo, V., & Serra, I. (2005). Internet users' privacy concerns and attitudes towards government surveillance – an exploratory study of cross-cultural differences between Italy and the United States. *Proceedings of the 18th Bled e-Conference: e-Integration in Action*; Bled, Slovenia

Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I., & Colautti, C. (2006). Privacy calculus model in e-commerce – a study of Italy and the United States. *European Journal of Information Systems (EJIS), 15*(4), 389-402.

Dinev, T., Xu, H., Smith, J. H., & Hart, P. (2013). Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts. *European Journal of Information Systems (EJIS), 22*, 295 – 316.

Dodd, P. & Warner, J. B. (1983). On corporate governance: A study of proxy contests. *Journal of Financial Economics*, *11*(1-4), 401-438.

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

Dowling, G. R., & Staelin, R. (1994). A model of perceived risk and intended risk-handling activity. *Journal of Consumer Research, 21*(June), 119–134.

Duan, J. C. (1995). The GARCH option pricing model. *Mathematical Finance, 5*(1), 13-32.

Duan, C., Grover, V., & Balakrishnan, N. R. (2009). Business Process Outsourcing: an event study on the nature of processes and firm valuation. *European Journal of Information System (EJIS), 18*(5), 442–457.

Ettredge, M. L., & Richardson, V. J. (2003). Information Transfer among Internet Firms: The Case of Hacker Attacks. *Journal of Information Systems, 17*(2), 71-82.

Fama, E. F., Fisher, L., Jensen, M. C., & Roll, R. (1969). The Adjustments of Stock Prices to New Information. *International Economic Review, 10*(1), 1-21.

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. (1976). *Foundations of Finance,* New York, Basic Books.

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

Ferguson, C., Finn, F., & Hall, J. (2005). Electronic Commerce Investments, the Resource-Based View of the Firm, and Firm Market Value. *International Journal of Accounting Information Systems*, *6*(1), 5-29.

Filbeck, G., Gorman, R., Greenlee, T., & Speh, T. (2005). The Stock Price Reaction to Supply Chain Management Advertisements and Company Value. *Journal of Business Logistics*, *26*(1), 199-216.

Fjetland, M. (2002). Global commerce and the privacy clash. *The Information Management Journal (January/February)*, pp. 54–57.

Florin, J., Bradford, M., & Pagach, D. (2005). Information Technology Outsourcing and Organizational Restructuring: An Explanation of their Effects on Firm Value. *Journal of High Technology Management Research*, *16*(2), 241-253.

Foxman, E. R., & Kilcoyne, P. (1993). Information technology, marketing practice, and consumer privacy: Ethical issues. *Journal of Public Policy Marketing, 12*(1), 106–119.

Franses, P. H., & Van Dijk, D. (1996). Forecasting stock market volatility using (non-linear) Garch models. *Journal of Forecasting, 15*(3), 229-235.

Fruhlinger, J. (2018, November). The OPM hack explained: Bad security practices meet China's Captain America. Retrieved from https://www.csoonline.com/article/3318238/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html.

Garg, A., Curtis, J., & Halper, H. (2003). Quantifying the Financial Impact of IT Security Breaches. *Information Management & Computer Security*, *11*(2-2), 74-83.

Gatzlaff, K. M., & McCullough, K. A. (2010). The Effect of Data Breaches on Shareholder Wealth. *Risk Management and Insurance Review, 13*(1), 61-83.

Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping: An integrated model. *MIS Quarterly*, *27*(1), 51–90.

Gewald, H., & Gellrich, T. (2007). The Impact of Perceived Risk on the Capital Market's Reaction to Outsourcing Announcements. *Information Technology and Management, 8*(4), 279-296.

Geyskens, I., Gielens, K., & Dekimpe, M. G. (2002). The Market Valuation of Internet Channel Additions. *Journal of Marketing*, *66*(2), 102-119.

Goel, S., & Shawky, H. A. (2009). Estimating the Market Impact of Security Breach Announcements on Firm Values. *Information & Management, 46*(7), 404-410.

Goel, S., Miesing, P., & Chandra, U. (2010). The Impact of Illegal Peer-to-Peer File Sharing on the Media Industry. *California Management Review, 52*(3), 6-33.

Goodwin, C. (1991). Privacy: recognition of a consumer right. *Journal of Public Policy and Marketing, 12,* pp. 149–166.

Graham, A. S., Pirie, W. L., & Powell, W. A. (1996). Detecting abnormal returns using the market model with pre-tested data. *Journal of Financial Research, 19*(1), 21-40.

Grazioli, S., & Jarvenpaa, S. L. (2000). Perils of Internet fraud: An empirical investigation of deception and trust with experienced Internet consumers. *IEEE Transaction Systems, Management, Cybernetics, Part A: Systems Humans 30*(4), 395–410.

Greene, T. (2012, February). FAQ About the VeriSign Data Breaches. Retrieved from https://www.csoonline.com/article/2130847/faq-about-the-verisign-data-breaches.html.

Guan, L., Sutton, S. G., Chang, C. J., & Arnold, V. (2006). Further Evidence on Shareholder Wealth Effects of Announcements for Newly Created CIO Positions. *Database for Advances in Information Systems, 37*(2-3), 176 -191.

Gwebu, K., Wang, J., & Xie, W. (2014). Understanding the Cost Associated with Data Security Breaches. *Pacific Asia Conference on Information Systems (PACIS),* 386-395.

Harrington, S. E. & Shrider, D. G. (2007). All events induce variance: Analyzing abnormal re- turns when effects vary across firms. *Journal of Financial and Quantitative Analysis, 42*(1), 229- 256.

Harvey, C. R. (2017). The scientific outlook in financial economics. *Duke I&E Research Paper, 2017*(05).

Hayes, D. C., Hunton, J. E., & Reck, J. (2000). Information Systems Outsourcing Announcements: Investigating the Impact on the Market Value of the Contact-Granting Firms. *Journal of Information Systems*, *14*(2), 109-125.

Hayes, D. C., Hunton, J. E., & Reck, J. L. (2001). Market Reaction to ERP Implementation Announcements. *Journal of Information Systems, 15*(1), 3-18.

Henderson, S. C. & Snyder, C. A. (1999). Personal information privacy: implications for MIS managers. *Information & Management, 36*(4), pp. 213–220.

Hendricks, K., & Singhal, V. (1996). Quality awards and the market value of the firm: An empirical investigation. *Management Science, 42*(2), 415-436.

Hendricks, K., & Singhal, V. (1997). Delays in new product introductions and the market value of the firm: The consequences of being late to the market. *Management Science, 43*(4), 422-436.

Herath, H. S. B., & Herath, T. C. (2008). Investments in information security: a real options perspective with Bayesian Post-audit. *Journal of Management Information Systems, 25*(3), 337–375.

Herath, H., & Herath, T. (2011). Copula-based actuarial model for pricing cyber-insurance policies. *Insurance Markets and Companies: Analyses and Actuarial Computations, 2*(1), 7–20.

Herath, H. S. B., & Herath, T. C. (2014). IT security auditing: a performance evaluation decision model. *Decision Support Systems, 57,* 54–63.

Higgins, E. J. & Peterson, D. R. (1998). The power of one and two sample t-statistics given event- induced variance increases and nonnormal stock returns: A comparative study. *Quarterly Journal of Business and Economics*, 27-49.

Hinz, O., Nofer, M., Schiereck, D., & Trillig, J. (2014). The influence of data theft on the share prices and systematic risk of consumer electronics companies. *Information & Management, 52*, 337-347.

Hinz, O., Muntermann, J., & Robnagel, H. (2014). The Economic Impact of Privacy Violations and Security Breaches. *Business & Information Systems Engineering,* 339-348.

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. (2004). The Impact of Virus Attack Announcements on the Market Value of Firms. *Information Systems Security, 13*(3), 32-40.

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

Hovav, A., Andoh-Baidoo, F. K., & Dhillion, G. (2007). Classification of security breaches and their impact on the market value of firms. *Proceedings of the Sixth Annual Security Conference,* 14-25.

Hovav, A., & D'Arcy, J. (2012). Applying an Extended Model of Deterrence across Cultures: An Investigation of Information Systems Misuse in the US and South Korea. *Information & Management, 49*(2), 99-110.

Hovav, A., & Gray, P. (2014). The Ripple Effect of an Information Security Breach Event: A Stakeholder Analysis. *Communications of the AIS, 34*(50), 893-912

Hovav, A., Han, J. Y., & Kim, J. (2017). Market Reaction to Security Breach Announcements: Evidence from South Korea. *ACM Advances in Information Systems, 48*(1), 11-52.

Hsu, C. (2006). Privacy concerns, privacy practices and web site categories: Toward a situational paradigm. *Online Information Review, 30*(5), 569-586.

Huang, C. D., & Behara, R. S. (2013). Economics of information security investment in the case of concurrent heterogeneous attacks with budget constraints. *International Journal of Production Economics, 141*(1), 255–268.

Hunter, S. D. (2003). Information Technology, Organizational Learning, and the Market Value of the Firm. *Journal of Information Theory and Application, 5*(1), 1-28.

Im, K. S., Dow, K. E., & Grover, V. (2001). A Reexamination of IT Investment and the Market Value of the Firm - An Event Study Methodology. *Information Systems Research, 12*(1), 103–117.

Jeong, B. K., & 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. K., & Stylianou, A. C. (2010). Market Reaction to Application Service Provider (ASP) Adoption: An Empirical Investigation. *Information & Management, 47*(3), 176-187.

Junius, D. (2014). Poll: Credit and debit card security breaches not changing people's habits. *Associated Press*.

Kannan, K., Rees, J., & Sridhar, S. (2007). Market Reactions to Information Security Breach Announcements: An Empirical Analysis. *International Journal of Electronic Commerce, 12*(1), 69-91.

Karolyi, G. A. (2011). The ultimate irrelevance proposition in finance? *Financial Review, 46*(4), 485-512.

Kelly, B. J. (1999). Preserve, Protect, and Defend. *Journal of Business Strategy, 20*(5), 22-26.

Khallaf, A., & Skantz, T. R. (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). Valuing the flexibility of investing in security process innovations. *European Journal of Operational Research, 192*(1), 216–235.

Khansa, L., Cook, D. F., James, T., & Bruyaka, O. (2012). Impact of HIPAA provisions on the stock market value of healthcare institutions, and information security and other information technology firms. *Computers & Security, 31*, 750-770.

Kiesnoski, K. (2019, July). 5 of the biggest data breaches ever. Retrieved from https://www.cnbc.com/2019/07/30/five-of-the-biggest-data-breaches-ever.html.

Kim, S. H., Kim, W. G., & Hancer, M. (2009). Effect of IT Investment Announcements on the Market Value of Hospitality Firms using Event Study Methodology. *Tourism Economics*, *15*(2), 397-411.

Kliger, D., & Gurevich, G. (2014). *Event Studies for Financial Research – A Comprehensive Guide*. New York, NY: Palgrave Macmillan

Klosek, J. (2000). Data Privacy in the Information Age. *Quorum Books*.

Ko, M., & Dorantes, C. (2006). The Impact of Information Security Breaches on Financial Performance of the Breached Firms: An Empirical Investigation. *Journal of Information Technology Management, 17*(2), 13-22.

Koh, J., & Venkatraman, N. (1991). Joint Venture Formation and Stock Market Reaction: An Assessment in the Information Technology Sector. *Academy of Management Journal, 34*(4), 869-892.

Kolari, J. W. & Pynnönen, S. (2010). Event study testing with cross-sectional correlation of ab- normal returns. *Review of Financial Studies, 23*(11), 3996-4025.

Kumar, A. (2016, October). What have we learned from the Yahoo breach? Retrieved from https://www.csoonline.com/article/3129785/what-have-we-learned-from-the-yahoo-breach.html.

Laufer, R. S., & Wolfe, M. (1977). Privacy as a concept and a social issue: A multidimensional development theory. *Journal of Social Issues, 33*(3), 22–42.

Leamer, E. E. (1983). Let's take the con out of econometrics. *American Economic Review, 73*(1), 31-43.

Lee, H. G., Cho, D. H., & Lee, S. C. (2002). Impact of e-Business Initiatives on Firm Value. *Electronic Commerce Research and Applications, 1*(1), 41-56.

Lee, S. Y. T., & Lim, K. S. (2006). The Impact of M&A and Joint Ventures on the Value of IT and non-IT Firms. *Review of Quantitative Finance and Accounting, 27*(2), 111-123.

Lee, D., Ahn, J., & Bang, Y. (2011). Managing consumer privacy concerns in personalization: A strategic analysis of privacy protection. *MIS Quarterly, 35*(2), 423-444.

Lewis, D. (2014, October). JP Morgan data breach confirmed affecting at least 83 million customers. Retrieved from https://www.csoonline.com/article/2691596/jp-morgan-data-breach-confirmed-affecting-at-least-83-million-customers.html.

Li, Y., Stewart, W., Zhu, J., & Ni., A. (2012). Online Privacy Policy of the Thirty Dow Jones Corporations: Compliance with FTC Fair Information Practice Principles and Readability Assessment. *Communications of the International Information Management Association, 12*(3), 65-90.

Lin, J. S. C., Jang, W. Y., & Chen, K. J. (2007). Assessing the Market Valuation of e-Service Initiatives. *International Journal of Service Industry Management, 18*(3), 224-245.

Lin, Y., & Wu, H. Y. (2008). Information privacy concerns, government involvement, and corporate policies in the customer relationship management context. *Journal of Global Business and Technology, 4*(1), 79-91.

Liu, C., Marchewka, J. T., Lu, J., & Yu, C. S. (2005). Beyond concern – a privacy-trust-behavioral intention model of electronic commerce. *Information & Management, 42*(2), 289-304.

Liu, C., & Arnett, K. P. (2002a). Raising a red flag on global www privacy policies. *The Journal of Computer Information Systems, 43*(1), 117-127.

Liu, C., & Arnett, K. P. (2002b). An examination of privacy policies in Fortune 500 web sites. *American Journal of Business, 17*(1), 13-22.

Loderer, C. F., & Mauer, D. C. (1992). Corporate Dividends and Seasoned Equity Issues: An Empirical Investigation. *The Journal of Finance, 47*, 201-225.

Lubatkin, M. H., Chung, K. H., Rogers, R. C., & Owers, J. E. (1989). Stockholder Reaction to CEO Changes in Large Corporations. *Academy of Management Journal 32*(1), 47-68.

MacKinlay, C.A. (1997). Event Studies in Economics and Finance. *Journal of Economic Literature, 35*(1), 13-39.

Malhotra, N. K. (2004). Marketing Research: An Applied Orientation. *Upper Saddle River, NJ: Prentice Hall*, 4th ed.

Malhotra, A., & Malhotra, C. K. (2011). Evaluating Customer Information Breaches as Service Failures: An Event Study Approach. *Journal of Service Research, 14*(1), 44-59.

Malkiel, B. (2003). The efficient market hypothesis and its critics. *The Journal of Economic Perspectives 17*(1), 59–82.

Markides, C. C. (1992). Consequences of Corporate Refocusing: Ex Ante Evidence. *Academy of Management Journal, 35*(2), 398-412.

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

Meng, Z., & Lee, S. Y. T. (2007). The Value of IT to Firms in a Developing Country in the Catch-Up Process: An Empirical Comparison of China and the United States. *Decision Support Systems, 43*(3), 737-745.

Messmer, E. (2009, January). Heartland: 'Largest Data Breach Ever'. Retrieved from https://www.csoonline.com/article/2123599/heartland---largest-data-breach-ever-.html.

Milberg, S. J., Burke, S. J., Smith, H. J., & Kallman, E. A. (1995). Values, personal information privacy concerns, and regulatory approaches. *Communications of the ACM, 38*(12), 65–74.

Milberg, S. J., Smith, H. J., & Burke, S. J. (2000). Information privacy: Corporate management and national regulation. *Organization Science, 11*(1), 35-57.

Misra, L., & Rao, V. S. (2009). The Launching of Transactional Web Sites: Market Response to Announcements by Incumbent B2C Companies. *Journal of Organizational Computing & Electronic Commerce, 19*(1), 50-82.

Mitra, S., & Singhal, V. (2008). Supply Chain Integration and Shareholder Value: Evidence from Consortium Based Industry Exchanges. *Journal of Operations Management, 26*(1), 96-114.

Mohammed, Z. A., Gurvirender P. T., & Squillace, J. M. (2017). Utilizing normative theories to develop ethical actions for better privacy practices. *Journal of Information Privacy and Security, 13*(4), 296-315.

Moor, J. H. (1997). Towards a theory of privacy in the Information Age. *Computers & Society, 27*(3), pp. 27–32.

Moore, T., Dynes, S., & Chang, F. R. (2015). Identifying how firms manage cybersecurity investment. *Southern Methodist University*, 32.

Moores, T. (2005). Do consumers understand the role of privacy seals in e-commerce? *Communications of the ACM, 48*(3), 86-91.

Morse, E. A., Raval, V., & Wingender Jr, J. R. (2011). Market Price Effects of Data Security Breaches. *Information Security Journal: A Global Perspective, 20*(6), 263-273.

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.

Nemati, H., Tao, W., & Gold, J. (2003). Understanding tradeoffs: the link between knowledge and privacy concerns. *Proceedings of the 34th Annual Meeting of the Decision Sciences Institute Meeting*. Washington, DC.

Nicholas-Donald, A., Matus, J. F., Ryu, S., & Mahmood, A. M. (2011). The economic effect of privacy breach announcements on stocks: a comprehensive empirical investigation. *AMCIS Proceedings*.

Noyes, K. (2016, March). Home Depot will pay up to $19.5 million for massive 2014 data breach. Retrieved from https://www.csoonline.com/article/3041994/home-depot-will-pay-up-to-195-million-for-massive-2014-data-breach.html.

Office of the Director of National Intelligence (DNI Home). Background Authorities of ISE. Retrieved from https://www.dni.gov/index.php/who-we-are/organizations/national-security-partnerships/ise/about-the-ise/ise-background-and-authorities.

Oh, W., Gallivan, M. J., & Kim, J. W. (2006). The Market's Perception on the Transactional Risks of Information Technology Outsourcing Announcements. *Journal of Management Information Systems, 22*(4), 271-303.

Oh, W., Kim, J. W., & Richardson, V. J. (2006). The Moderating Effect of Context on the Market Reaction to IT Investments. *Journal of Information Systems, 20*(1), 19-44.

Pardue, J. H., Higgins, E., & Biggart, T. (2000). The Impact of New Product Announcements on Firm Value in Information Technology Producing Industries: An Examination of Industry-Level Evolutionary Eras. *Engineering Economist, 45*(2), 144-157.

Parker, D. (2010). Our Excessively Simplistic Information Security Model and How to Fix It. *ISSA Journal*, 12-21.

Patel, N. (2010). The Effect of IT Hack Announcements on the Market Value of Publicly Traded Corporations. *Working Paper* (Duke University).

Patell, J. M. (1976). Corporate Forecasts of Earnings Per Share and Stock Price Behavior: Empirical Tests. *Journal of Accounting Research, 14*(2), 246-276.

Pavlou, P., (2011). State of the Information Privacy Literature: Where Are We Now and Where Should We Go? *MIS Quarterly, 35*(4), 977–88.

Pavlou, P. A., Liang, H., & Xue, Y. (2007). Understanding and mitigating uncertainty in online exchange relationships: A principal-agent perspective. *MIS Quarterly, 31*(1), 105-136.

Peak, D. A., Windsor, J. C., & Conover, J. (2002). Risks and Effects of IS/IT Outsourcing: A Security Market Assessment. *Journal of Information Technology Cases and Applications, 4*(1), 6-33.

Peslak, A.R. (2006). Internet Privacy Policies of the Largest International Companies. *Journal of Electronic Commerce in Organizations, 4*(3), 46-62.

Polinsky A.M., & Shavell, S. (2007). Handbook of Law and Economics. *Amsterdam: North-Holland, Vol* (2).

Pruit, S. W., & Peterson, D. R. (1986). Security Price Reactions around Product Recall Announcements. *Journal of Financial Research, 9*(2), 113-122.

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

Ragan, S. (2014, September). What you need to know about the Home Depot data breach. Retrieved from https://www.csoonline.com/article/2604320/what-you-need-to-know-about-the-home-depot-data-breach.html.

Ragan, S. (2016, November). 412 million Friend Finder accounts exposed by hackers. Retrieved from https://www.csoonline.com/article/3139311/412-million-friendfinder-accounts-exposed-by-hackers.html.

Raghu, T. S., Wo, W., Mohan, S. B., & Rao, H. R. (2008). Market Reaction to Patent Infringement Ligations in the Information Technology Industry. *Information Systems Frontiers, 10*(1), 61-75.

Ranganathan, C., & Brown, C. V. (2006). ERP Investments and the Market Value of Firms: Toward an Understanding of Influential ERP Project Variables. *Information Systems Research, 17*(2), 145-161.

Roberts, P. (2007, January). Massive TJX Security Breach Reveals Credit Card Data. Retrieved from https://www.csoonline.com/article/2121609/massive-tjx-security-breach-reveals-credit-card-data.html.

Roman, J., & Ross, R. (n.d.). Chase Breach Affects 76 Million Households. Retrieved from https://www.bankinfosecurity.com/chase-breach-affects-76-million-households-a-7395.

Rose, E. A. (2006). An examination of the concern for information privacy in the New Zealand regulatory context. *Information & Management, 43*(3), 322-335.

Roztocki, N., & Weistroffer, H. R. (2006). Stock Price Reaction to the Investments in IT: Relevance of Cost Management Systems. *Electronic Journal of Information Systems Evaluation, 9*(1), 27-30.

Roztocki, N., & Weistroffer, H. R. (2007a). How Do Investments in Enterprise Application Integration Drive Prices? *Proceedings of the 40th Hawaii International Conference on System Sciences (HICSS*).

Roztocki, N., & Weistroffer, H. R. (2007b). Identifying Success Factors for Information Technology Investments: Contribution of Activity Based Costing. *Proceedings of the 15th European Conference on Information Systems (ECIS)*, 1031-1040.

Roztocki, N., & Weistroffer, H. R. (2008a). Event Studies in Information Systems Research: A Review. *Proceedings of the Fourteenth Americas Conference on Information Systems (AMCIS)*.

Roztocki, N., & Weistroffer, H. R. (2008b). Stock Price Reaction to Investments in EAI and ERP: A Comparative Event Study. *Proceedings of the Proceedings of the 41th Hawaii International Conference on System Sciences (HICSS)*.

Roztocki, N., & Weistroffer, H. R. (2009). Event Studies in Information Systems Research: An Updated Review. *Proceedings of the Fifteenth Americas Conference on Information Systems (AMCIS 2009)*.

Roztocki, N., & Weistroffer, H. R. (2009a). The Impact of Enterprise Application Integration on Stock Prices. *Journal of Enterprise Information Management, 22*(6), 709-721.

Roztocki, N., & Weistroffer, H. R. (2009b). Information Technology Investments: Does Activity Based Costing Matter? *The Journal of Computer Information Systems, 50*(2), 31-41.

Roztocki, N., & Weistroffer, H. R. (2009). Stock Market Reaction to Information Technology Investments: Towards An Explanatory Model. *European Conference on Information Systems*, 883-994.

Roztocki, N., & Weistroffer, H. R. (2011, October). Event studies in information systems research: past, present and future. *European Conference on Information Systems (ECIS)*, 235-247.

Sabherwal, R., & Sabherwal, S. (2005). Knowledge Management Using Information Technology: Determinants of Short-Term Impact on Firm Value. *Decision Sciences, 36*(4), 531-567.

Sabherwal, R., & Sabherwal, S. (2007). How Do Knowledge Management Announcements Affect Firm Value? A Study of Firms Pursuing Different Business Strategies. *IEEE Transactions on Engineering Management, 54*(3), 409-422.

Saltzer, J., & Schroeder, M. (1975). The protection of information in computer systems. *Proceedings of the IEEE, 63*(9), 1278-1308.

Savino, W. M. (2003). Bank privacy disputes reach the courts. *Banking Law Journal, 120*(1), 5–18.

Schatz, D., & Bashroush, R. (2017). Economic Valuation for Information Security Investment: A Systematic Literature Review. *Information Systems Frontiers, 19,* 1205-1228.

Schwaig, K. S., Kane, G. C., & Storey, V. C. (2006). Compliance to the fair information practices: How are the Fortune 500 handling online privacy disclosures? *Information & Management, 43*(7), 805-820.

Swartz, N. (2003). Information at a price: liberty vs security. *Information Management Journal, Vol. 37*(3), p. 14.

Schwartz, M. J. (2015, October). Experian Breach: Lessons Learned. Retrieved from https://www.bankinfosecurity.com/interviews/experian-breach-lessons-learned-i-2936.

Schwartz, M. J., & Ross, R. J. (2019, July). Equifax Negotiates Potential $700 Million Breach Settlement. Retrieved from https://www.bankinfosecurity.com/equifax-eyes-700-million-data-breach-settlement-a-12808.

Sewell, M. (2011). History of the Efficient Market Hypothesis. *UCL Department of Computer Science* (Research Note), 1-14.

Sharpe, W. F. (1964). Capital asset prices: a theory of market equilibrium under conditions of risk. *Journal of Finance, 19*(3), 425–442.

Siponen, M. (2005). An analysis of the traditional IS security approaches: implications for research and practice. *European Journal of Information Systems (EJIS), 14* (3), 303–315.

Siponen, M. T., & Oinas-Kukkonen, H. (2007). A review of information security issues and respective research contributions. *SIGMIS Database, 38*(1), 60–80.

Smith, H. J. (1993). Privacy policies and practices: inside the organizational maze. *Communications of the ACM, 36*(12), 104 – 122.

Smith, H. J. (1994). Managing Privacy: Information Technology and Corporate America. *Chapel Hill, NC: University of North Carolina Press*

Smith, H. J., Milberg, S. J., & Burke, S.J. (1996). Information privacy measuring individuals' concerns about organizational practices. *MIS Quarterly, 20*(2), 167-196.

Smith, H. J., Dinev, T., & Xu, H. (2011). Information Privacy Research: An Interdisciplinary Review. *MIS Quarterly, 35*(4), 989 – 1015.

Solove, D. J. (2005). A taxonomy of privacy. *George Washington University Public Law Research Paper, No. 129*. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id.667622.

Solove, D. J. (2006). A Taxonomy of Privacy. *University of Pennsylvania Law Review, 154*(3), 477 - 560

Song, Y. I., Woo, W., & Rao, H. R. (2007). Interorganizational Information Sharing in the Airline Industry: An Analysis of Stock Market Responses to Code-Sharing Agreements. *Information Systems Frontiers*, *9*(2-3), 309-324.

Spanos, G., & Angelis, L. (2016). The impact of information security events to the stock market: A systematic literature review. *Computers & Security, 58*, 216–229.

Stewart, K. A., & Segars, A. H. (2002). An empirical examination of the concern for information privacy instrument. *Information Systems Research, 13*(1), 36-49.

Stone, E. F., Gardner, D. G., Gueutal, H.G., & McClure, S. (1983). A Field Experiment Comparing Information-Privacy Values, Beliefs, and Attitudes Across Several Types of Organizations. *Journal of Applied Psychology*, *68*(3), pp. 459-468.

Stone, E. F., & Stone, D. L. (1990). Privacy in Organizations: Theoretical Issues, Research Findings, and Protection Mechanisms. *Research Findings in Personnel and Human Resources Management, K. M. Rowland and G. R. Ferris (Eds.), Greenwich, CT: JAI Press*, pp. 349-411.

Stratford, J. S. & Stratford, J. (1998). Data protection and privacy in the United States and Europe. *IASSIST Quarterly (Fall)*, pp. 17–20.

Straub, D. W. Jr., & Collins, R. W. (1990). Key information liability issues facing managers: Software piracy, proprietary databases, and individual rights to privacy. *MIS Quarterly, 14*(2), 143–156.

Subramani, M., & Walden, E. (2001). The Impact of E-Commerce Announcements on the Market Value of Firms. *Information Systems Research, 12*(2), 135-154.

Surveillance Under the USA PATRIOT Act (2018). *American Civil Liberties Union*. Retrieved from https://www.aclu.org/other/surveillance-under-usapatriot-act.

Svensson, A. (2003). Analyzing information systems security. *Department of Informatics, School of Economics and Management*. Lund University.

Swinhoe, D. (2019, July). The biggest data breach fines, penalties and settlements so far. Retrieved from https://www.csoonline.com/article/3410278/the-biggest-data-breach-fines-penalties-and-settlements-so-far.html.

Swire, P. P. (1997). Markets, Self-Regulation, and Government Enforcement in the Protection of Personal Information, in Privacy and Self-Regulation in the Information Age. *U.S. Department of Commerce, Washington, DC*, pp. 3–20.

Swire, P. P., & Steinfeld, L. (2002). Security and privacy after September 11: The health care example. *Proceedings of the 12th Annual Conference on Computers, Freedom and Privacy*, 1-13.

Tavani, H. (1999). KDD, data mining, and the challenge for normative privacy. *Ethics and Information Technology, 1*, pp. 265–273.

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.

Teoh, S.H., Welch, I., & Wazzan, S. P. (1999). The Effect of Socially Activist Investment Policies on the Financial Markets: Evidence from the South African Boycott. *Journal of Business*, *72*(1), 35-89.

The USA PATRIOT Act: Preserving Life and Liberty (2001). What Is the USA Patriot Act. Retrieved from https://www.justice.gov/archive/ll/highlights.htm.

The White House (2015). Executive Order – Promoting private sector cybersecurity information sharing. *Office of the Press Secretary*

Toomey, P. (2018). The NSA Continues to Violate Americans' Internet Privacy Rights. *American Civil Liberties Union*. Retrieved from https://www.aclu.org/blog/national-security/privacy-and-surveillance/nsa-continues-violate-americans-internet-privacy.

Uhlenbruck, K., Hitt, M. A., & Semadeni, M. (2006). Market value effects of acquisitions involving internet firms: a resource-based analysis. *Strategic Management Journal, 27*(10), 899-913.

Vijayan, J. (2007, March). TJX data breach: At 45.6M card numbers, it's the biggest ever. Retrieved from https://www.computerworld.com/article/2544306/tjx-data-breach--at-45-6m-card-numbers--it-s-the-biggest-ever.html.

Walden, E., & Browne, G. J. (2008). Rational Fads in Investor Reactions to Electronic Commerce Announcements: An Explanation of the Internet Bubble. *Electronic Commerce Research and Applications*, *7*(1), 44-54.

Warren, S. D. & Brandeis, L. D. (1890). The Right to Privacy. *Harvard Law Review, Vol.4*(5), pp. 193-220.

Webster, J., & Watson, R. T. (2002). Analyzing the Past to Prepare for the Future: Writing a Literature Review. *MIS Quarterly 26*(2), 13-23.

Weise, E., & Guynn, J. (2014). 24% of Americans stopped buying online because of breaches. *USA TODAY*, June 3.

Westin, A. F. (1967). Privacy and Freedom. *Atheneum, New York.*

Westin, A. F. (1991). Domestic and International Data Protection Issues: How the American Public Vies Consumer Privacy Issues in the Early 90s—and Why. *Testimony before the Subcommittee on Government Information and Agriculture, Committee on Government Relations, U.S. House of Representatives, Washington, D.C., U.S. Government Printing Office*, pp. 54-68.

Westin, A. F. (1997). Commerce, Communication, and Privacy Online. *Center for Social and Legal Research, Hackensack, NJ*.

Whitman, M., & Mattord, H. (2012). Principles of Information Security, 4th ed. *Cengage Learning*.

Whittaker, Z. (2014). In security: The biggest hacks, leaks, and data breaches. *Zdnet.com,* December 28.

Williams, M. (2017, October). Inside the Russian hack of Yahoo: How they did it. Retrieved from https://www.csoonline.com/article/3180762/inside-the-russian-hack-of-yahoo-how-they-did-it.html.

Yang, J., & Klassen, K. J. (2008). How Financial Markets Reflect the Benefits of Self-Service Technologies. *Journal of Enterprise Information Management, 21*(5), 448-467.

Yayla, A. A., & Hu, Q. (2010). The Impact of Information Security Events on the Stock Value of Firms: The Effect of Contingency Factors. *Journal of Information Technology, Advance Online Publication*, X, 1-2.

Yayla, A. A., & Hu, Q. (2011). The impact of information security events on the stock value of firms: The effect of contingency factors. *Journal of Information Technology, 26*(1), 60–77.

Zhang, L., & Huang, J. (2009). The Review of Empirical Researchers on IT Investments Announcements on the Market Value of Firms. *International Journal of Business and Management 4*(10), 14-27.

Zwass, V. (2018). Information System | Definition, Examples, & Facts. *Encyclopedia Britannica Online*.