2020

# Identifying Managerial Factors Affecting Security Breaches within Publicly Traded Organizations

Jodi Bouvin
*Walden University*

# Walden University

College of Management and Technology

This is to certify that the doctoral dissertation by

Jodi L. Bouvin

has been found to be complete and satisfactory in all respects,
and that any and all revisions required by
the review committee have been made.

Review Committee
Dr. Judith Forbes, Committee Chairperson, Management Faculty
Dr. Carol Wells, Committee Member, Management Faculty
Dr. Mohammad Sharifzadeh, University Reviewer, Management Faculty

Chief Academic Officer and Provost
Sue Subocz, Ph.D.

Walden University
2020

Abstract

# Identifying Managerial Factors Affecting Security Breaches within Publicly Traded Organizations

by

Jodi L. Bouvin

MBA, American University, 2006

BS, American University, 2004

Dissertation Manuscript Submitted in Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Management

Walden University

June 2020

# Abstract

Increased vulnerabilities and attacks of business information in recent years was linked to unauthorized access for employees utilizing corporate systems. Research noted a lack of planning was a factor leading to 50-80% of annual security breaches since 2014, with greater than $20 billion of noted damages a year for firms operating in the United States. The quantitative correlational study addressed the connection with public firms, announcements pertinent to systems breaches, and a reduction of corporate revenues. The context of constraints provided the lens that guided the examination of system violations and breaches. A random sample of 134 annual reports of public firms listed with the NASDAQ exchange assisted with examining events, corporate reports, and utilizing Pearson's Correlation to test variable relationships. The dependent variable was corporate performance and revenues as denoted by annual and quarterly reports. The independent variables were the degree of systems security and the availability of technical assistance. The study confirmed that there was a statistically significant correlation between level of systems security policy and the number of security breaches. Similarly, there was also a statistically significant correlation between the level of systems security policy and the self-reported loss in corporate earnings associated with the security breach as a percentage of revenue. Findings from the project data suggested that leaders might improve performance by ensuring security policies include a training component to more fully equip all stakeholders with best practices in the workplace. Social change benefits are evidenced by managers having a stronger ability to navigate security risks, and thus creating healthier companies.

# Identifying Managerial Factors Affecting Security Breaches within Publicly Traded Organizations

by

Jodi L. Bouvin

MBA, American University, 2006

BS, American University, 2004

Dissertation Manuscript Submitted in Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Management

Walden University

June 2020

# Dedication

I dedicate this dissertation to my beloved husband David Bouvin, my children, my family, and lifelong friends at Walden University.

# Acknowledgments

It is a true honor to have the opportunity to pursue a doctoral degree at Walden University.  I would like to thank Dr. Judie Forbes, Dr. Carol Wells, and Dr. Mohammad Sharifzadeh who have continuously inspired me while serving as leaders on my dissertation committee.  Thank you also Dr. Sandy Kolberg for your valuable guidance and support throughout my graduate studies and doctoral course work.

Table of Contents

# List of Tables

# List of Figures

# Chapter 1: Introduction to the Study

Business leaders continued to maintain a lens on the prevention of vulnerable touch points to corporate information; the value of the continuity of business processes; the reduction of security-based shortfalls and occurrences; and the opportunity for integrity, maintenance, and confidentiality of business data and assets pertinent to obtained information (Akey, Lewellen, & Liskovich, 2018). Security systems were comprised of a balance between technical and social factors, ranging from the solely technical to the focus being dominantly social and behavioral (Yahaya, Basir, & Deraman, 2015). The significance of systems security in an organizational environment is paramount, as nearly all forms of data are compiled and procured electronically (Belle, Burley, & Long, 2015). In 2015, Chukudi and Daddie posited that 91% of participants voiced concern over employees as a potential flaw in security systems and 79% of participants considered human error to be the underlying source of the systems failure. A lingering obstacle was to ascertain the prominent circumstances that can benefit with diminishing organizational security vulnerabilities and attacks.

According to Duxbury and Halinski (2014), 91% of employees did not adhere to regulatory security protocol. A lack of employee education has been recorded as a primary cause of estimates between one-half to three-quarters of systems security infringements, culminating in an excess of $20 billion in damages for establishments in the United States. In other words, security transgressions may cost an institution up to 2-3% of its annual revenue (Dockery & Bawa, 2014). In the research study, I scrutinized the elements that affect organizational recognition pertaining to systems security and the breaches of publicly traded companies listed with the National Association of Securities Dealers Automatic Quotation (NASDAQ).

Multiple researchers performed analyses with a goal to identify, investigate, and recognize the aspects that tie levels of end-user awareness of security systems (Ho & Carol, 2015; Yun, Kettinger, & Lee, 2012). The phrase level of awareness was significant and implied a degree or scale of understanding that is important for security functions. Reduced awareness levels signified a substantial negligence of security risk that can led to damages beyond repair. The conducted study was devised to will be conducted to review the correlation among established policies on systems, security breach intensity, and the earnings noted for public firms listed with the exchange on the NASDAQ. The NASDAQ was selected as a main component of the research study, because Belzuegui, Erro, and Pastor (2014) argued that, traditionally, smaller and younger organizations are listed on the exchange with the NASDAQ. An exchange for stock purchases with a propensity of smaller and younger firms was an ideal environment to examine information assurance levels of awareness. Results yielded that productive business administrators have in place protocols for addressing security concerns within public entities traded on the NASDAQ exchange.

The governance of organizational information systems encompassed the establishment of management levers within the business community to incorporate information and communications technologies that ensured consistent interchanges and connections. Incorporating pertinent systems granted users a great ability to leverage the requirements for project-based constraints, financial needs, and completed activities

(Golden & Watt, 2013). Continued returns stemmed from the successful incorporation of security systems, policies, training programs, and evidenced via heightened company profits.

After 2016, more than 29% of establishment leaders recognized the utilization of operational instructions, security systems policies, and training curriculum for employees (Akey, Lewellen, & Liskovich, 2018). Statisticians have examined constraints pertinent to variables that can impact the integration of policies for information system guidelines and breach preventions for all corporate personnel (Greenhaus & Kossek, 2014). Greer and Payne (2014) studied the impact of business systems procedures in federal agencies, state institutions, and discovered business leaders were more likely to report the breaches of systems when resources were available to utilize to effectively manage occurrence of security violations. Hall, Kossek, Briscoe, Pichler, and Lee (2013) examined the notes of seasoned business leaders which framed how barriers existed in the workplace that were tied to training, culture, and even the utilization of technologies. Harrington and Santiago (2015) suggested that the lack fortified infrastructures, training, and maintaining of systems steps led to shortcomings when policies were not in place. The identified goal was then to establish and maintain policies that can be utilized during all organizational events.

Competitive firms were then those with managers who led by setting the example of problem identification, training deficits, shortcomings pertinent to security knowledge, and applications for busy project environments. During all organizational activities, it became clear that business leaders must instill a culture focused on acquiring the skills needed to maintain healthy systems and the avoidance of security breaches (Hilbrecht, Shaw, Johnson, & Andrey, 2013). After federal events, state activities, and via published findings, the sharing of information was noted has highly important for preparing for and preventing information systems security breaches. Managers and researchers touted solutions pertinent to interagency sharing, planning steps, minimizing known risks, incorporating barriers, utilizing biometrics, and leveraging token-based accounts to not only prepare organizational environments for potential security breaches, but to also thwart unforeseen attacks. The challenges associated with data management, information sharing, and training initiatives were noted to serve as potential barriers; however, these can be reduced or eliminated by continued collaborations and partnerships across institutions. The obstacles remained for not only government agencies, but also for firms publicly traded on the NASDAQ exchange. The identified initiatives of information sharing, instilling executive champions, developing policies pertinent to information systems security breaches, integrating controls, and encouraging increases training can all provide the greatest returns. The greatest returns were easily identified via corporate earnings and increased revenues; however, other drivers also surfaced as investor sentiment and the satisfaction of customers, stakeholders, and even from current employees.

An identified challenge in the business environment was to ensure collaborations and information sharing occurred via protected communication modalities. In this regard, secure collaborations and communications can also be linked to project performance and the overall productivity of business initiatives. Anderson, Kaplan, and

Vega (2014) posited that in many successful business environments, diverse forms of communications were utilized for collaborative purposes and to accomplish tasks at hand. A continued challenge was to ensure guidelines were in place that assisted with guiding effective communications, protecting information sharing, and securing valuable industry data. Golden and Watt (2013) also suggested that pivotal and popular technologies assisted with project team collaborations, information sharing, and distributing findings across organizational teams, departments, agencies, and even throughout supply-chain partners. The remaining goal was to ensure that information systems security policies existed that guided and protected all collaborations and information sharing.

There was a constant theme in the literature about level of risk and how this information is applied to the work environment. Weisberg and Porell (2011) noted that risk level should be included within training programs and policy considerations to ensure stakeholders are knowledgeable about the potential severity of threats. Studies have also been conducted that support risk level integration within both quarterly and annual training events (Hosseinnezhad, 2013). Ho and Carol (2015) reported that many security breaches occur because of identified vulnerabilities in a system, which can be due to personnel activities and even to a lack of system updates. Business leaders should constantly challenge themselves and team members to be vigilant with all preparations.

There are a variety of factors that have led to identified information security breaches for publicly traded companies. In regard to the variety of vulnerabilities that can occur, Jakobsn and Lueg (2014) identified factors pertaining to frequency of training for employees, the curriculum that is utilized during training events, the stakeholders engaged in preparation activities, and the policies utilized throughout an organization. The trend with policy development appeared to focus more on intent, curriculum, participants, and frequency versus the specific information systems utilized to thwart potential breaches.

A key ingredient within information systems security policy and training development was the value of stakeholder awareness. Yinat (2014) provided an overview of substantiated training approaches that have led to the greatest return for employee awareness, comprehension, and even for application within a work environment. The research framed the significance of leader involvement in policy development, implementation, and with training opportunities. For example, some findings purported that gestalt approaches can enhance planned processes, enhanced focus on provided information, and with respect to enhanced awareness levels. Reflection steps highlighted that more engaged business leaders had a positive impact on employee and stakeholder willingness to ascertain training guidance and also to implement the recommendations provided. The motivation for employees certainly is a straightforward consideration to implement all provided guidance; however, the ability for executives, managers, and project leaders to engage stakeholders on the periphery of the company should also lead to positive returns for implantation and the eventual reduction in successful security breaches.

The enhancement of curriculum in training sessions has a lasting impact on participants. James and Griffiths (2014) posited that the incorporation of relevant and applicable information served as a key motivator and vital resource for active learners who participated in training sessions. The foundational concept appeared to center on the relevance of data and information provided for the participants. A look at training sessions pertinent to information systems security made it quite clear that systems attacks and breaches were tied to recent events, so the same timely information and content are needed within all planned training activities. Incorporating recent information that stemmed from information systems security breaches, attacks, and even thwarted activities should follow the same guidance and lead to operational environments centered on proactive stakeholders actively looking to thwart potential breaches.

Research findings provided a lens focused on traditional technical challenges connected to corporate training sessions. Shekarhizadeh, Ghasemi, Tadi, Soltani, and Nili (2015) highlighted the established challenges tied to technical access and availability for employee training events. One challenged was derived directly from the need to provide computer workstations available for participants to utilize and work on during instruction activities. Examples were tied to the lack of access to computer systems, how virtual workers were engaged, resources that kept of interest of participants, and information that can be utilized right away. In regard to virtual workers, additional considerations pertained to balance work life with homelife for those participating in training sessions at a distance and how current technologies were also leveraged to meet the needs of participants.

Business leaders were challenged to consider all available resources when preparing a workforce for information systems security training. Yao (2012) lobbied that virtual workers were not the only ones who need technical considerations when planning policy development steps and providing training sessions.  In a modern and competitive marketplace, policies and training resources must be planned for and utilized for all pertinent stakeholders.  The utilization of available technologies and resources will also be needed for dispersed employees, working on disparate projects, and for stakeholders partnered on foundational initiatives; such as, via supply-chain partnerships and firms connected via distribution processes, procurements, marketing, and via targeted sales. Leaders need to be cognizant and motivated for the planning and utilization of all pertinent resources throughout the enterprise; whether, technology, communication, or policy based.

During the planned review of organizational security systems, managers have found success with identifying and sharing potential risks with all stakeholders.  Margo, Prybutok, and Ryan (2014) suggested that information systems security risks have stemmed from system vulnerabilities due to technical deficiencies as well as from the contributions of personnel.  In some regards, the greatest risks stem from personal activities, social engineering, and even from training deficits (Maruyama & Tietze, 2012).  For example, business leaders were most prudent to provide support services for the employees of an organization.  Providing social support as well as effective policies, enhanced training sessions, and strengthened systems had a lasting effect on the success of managerial steps.  In regard to support services, business leaders strengthened corporate systems by not only enhancing training, policies, and available resources, but also via the integration of planned and structured wellness opportunities.

The value of social collaborations remained evident during the review of personnel engagement within organizations. Cocco and Tuzzi (2013) noted that personnel were more likely to adhere to established guidelines and procedures when integrated or welcomed within the social environment. The expansion of social media resources provided for enhanced opportunities for managers to engage stakeholders and enhance the feelings of involvement for employees, staff, partners, and even for executive leaders. Maintaining a socially connected workforce should have the increased ability to enhance feelings of connections, collaborations, and reduce the potential of apathy for information systems security attacks.

Engaged, trained, and motivated stakeholders may be the difference between increased information systems security breaches and a heightened sense of thwarting attacks. Effective business leaders must have the proactive attitude of planning, policy development, and guiding engaging training sessions to develop a culture designed to withstand system attacks and to reduce the severity of breaches. The strength of a company will certainly be evidenced via the willingness of the personnel to support the mission, objectives, and operational activities.

## Background of the Study

A review of structured security surveys noted that more than 25 percent of federal government personnel had been exposed to information systems security challenges in the workplace (Bernardino, Roglio, & Del Corso, 2012). In 2015, Harrington and Santiago stated that a heightened exposure to security breaches and attacks can lead directly to increased vulnerabilities in the work environment. In 2016, only 10 percent of federal government personnel noted information systems security challenges; which, framed a stark trend in a highly protected environment for a significant increase in security concerns over a 15 year period (Lending, Minnick, & Schorno, 2018). In 2012, more than three million employees were involved or exposed to security breaches in the US work environment. Additionally, more than thirteen million workers in the US noted exposure to information systems security risks throughout a traditional work week (Zissis & Lekkas, 2012). The clear directive for managers today will be to incorporate information systems security policies, training, and an environment of proactive collaborations to effectively mitigate and thwart potential security breaches.

The driving emphasis of this research endeavor was to ascertain the level of connection with public companies, communications pertinent to breaches of security, and a reduction of revenues due to reported losses. The persistence of breakdowns with information systems security practices within organizations was noted to have a negative impact on price of stock and company revenues. The timing, length, and cost of information systems security vulnerabilities provided a framework to analyze identified constraints and to provide operational best practices. Zhu (2013) discovered that previous statistical analyses ignored triggers that impacted working conditions and perceptions tied to systems vulnerabilities and breaches. The annual and quarterly public reports of listed firms on the NASDAQ exchange provided the baseline to analyze results and trends pertinent to US operations. The connections, predictions, and relationships provided the backdrop to garner best practices for public companies, corporate policy notes pertaining to security considerations, financial reports, and market guidance pertaining to preparations for current and future information systems security breaches.

## Problem Statement

Based on information systems serving as a foundational backbone for competitive firms today, systems breaches and violations have grown in occurrence and severity pertinent to financial losses and operational downtime (Akey, Lewellen, & Liskovich , 2018; Thomas, Sargent, and Hardy, 2011).  Researchers have identified a growing trend of approximately 20% of personnel who noted inabilities to remedy breaches of security and a similar 10% of workers who were dissatisfied with training and felt unprepared to navigate the complex information systems security attacks and vulnerabilities (Akey, Lewellen, & Liskovich, 2018).  In 2015, Shekarhizadeh, Ghasemi, Tadi, Soltani, and Nili discussed how a growing occurrence of information systems breaches were leading to undiscerning employees who were unsure of proper courses of action for system attacks and vulnerabilities.  The noted corporate system shortcomings provided the framework for a general business problem to ascertain quarterly and annual reports of public firms listed on the NASDAQ exchange and provided a key lens to analyze market results and trends for organizational operations within the US.  An examination of the predictions and connections provided the diagnostic to ascertain relationships and to garner specific guidance for public company operations, policy notifications, annual revenues, and best practices pertinent to information systems security operations.

## Purpose of the Study

The purpose of this correlational research initiative was to ascertain the association and connections with public companies, notices pertinent to breaches of security, and reported earnings. A persistence of system vulnerabilities in organizations had a significant impact on the price of stocks and annual revenues for public firms partnered with the NASDAQ exchange. Derived data were reviewed via the Pearson Correlation to examine the relationship with the identified independent and dependent variables. A review of the predictions and connections was used as the lens to ascertain relationships and to garner specific guidance for public company operations, policy notifications, annual revenues, and best practices pertinent to information systems security operations. The dependent variable was corporate performance and revenues as denoted by annual and quarterly reports. The independent variables were degree of secure systems and the availability of technical assistance. The population for the research initiative stemmed from a calculated sample of public companies partnered with the NASDAQ exchange. The research study can be seen as a resource to promote social change best practices via development and training steps to assist with the management of corporate policies.

## Research Question(s) and Hypotheses

The foundational inquiry that provided the lens for this research activity was: What were the analyzed and unique aspects pertinent to public company operations, policy notifications, annual revenues, and best practices for information systems security operations? Two research questions guided this analysis:

RQ1. What was the relationship between the level of information systems security policy and the number of security breaches?

RQ2. What was the relationship between the level of information systems security policy and the self-reported loss in corporate earnings associated with the security breach as a percentage of revenue?

The following hypotheses were tested in this initiative.

$H1_0$: There was a not a statistically significant correlation between the independent variable of level of information systems security policy and the dependent variable of the number of security breaches.

$H1_a$: There was a statistically significant correlation between the independent variable of the level of information systems security policy and the dependent variable of the number of security breaches.

$H2_0$: There was a not a statistically significant correlation between the independent variable of the level of information systems security policy and the dependent variable of the self-reported loss in corporate earnings associated with the security breach as a percentage of revenue.

$H2_a$: There was a statistically significant correlation between the independent variable of the level of information systems security policy and the dependent variable of the self-reported loss in corporate earnings associated with the security breach as a percentage of revenue.

## Theoretical Foundation

The foundational theory incorporated in this research initiative was the Theory of Constraints (TOC). An examination of potential constraints were presented by Linden (2014) during the development of a review of constraints. Kane (2014) posited that factors influencing or limiting a system from heightened performance can be considered as a constraining component to operations. The overall intent of using the TOC in the research study was to develop a heightened perspective pertaining to public company operations, policy notifications, annual revenues, and best practices for information systems security operations. Foundational considerations in the theory were (a) constraint identification, (b) effective constraint management, (c) ancillary activities pertinent to constraints, (d) clearly identify and label constraints, and (e) necessary corrections to reduce constraint influences (Rahman, 1998; Shamsur-Rahman, 1998). These identified and organized TOC ideals are examine in detail throughout the Chapter 2 literature review. In the research initiative, the TOC was utilized as a lens to review public company operations, policy notifications, annual revenues, and best practices pertinent to information systems security operations. The persistence of system vulnerabilities and attacks in an organization were confirmed to have a significant impact on earnings per share via public companies on the NASDAQ exchange.

Important aspects of the research project were the identified dependent and independent variables. The dependent variable was corporate performance and revenues as denoted by annual and quarterly reports. The independent variables were degree of secure systems and the availability of technical assistance. The degree of corporate performance was noted via annual disclosures and reports. Degree of information secure systems planning was noted as the availability of clearly articulated policies within annual and quarterly reports. Degree of technical assistance was noted as the information systems security training and support available for workers throughout a company as listed within required reporting documents.

A foundational tenet of the research study was to clearly link the importance of variable association with positive outcomes. Establishing this completed linkage of constraints and outcomes provided the mechanism to utilize the TOC to confirm both financial and operational benchmarks as constraints (Bailey & Kurland, 2002; Weinert, Maier, Laumer, & Weitzel, 2014). In recent years, more seminal studies have assisted with examining information systems considerations within a variety of industries; to include, manufacturing, aviation, maintenance, financial sectors, and even via international business activities. Babbie, Wagner, and Zaino (2015) suggested that information systems security has not been an area of emphasis pertinent to constraint-based research and analysis. The research project serves as a potential next step to build on the research of Babbie, et al. and to assist with developing a connection of security breaches, training programs, operational deficits, and financial loses with constraint considerations.

An important area for constraint analysis was also with training program availability and a focus on information systems security. Teo, Wong, and Chai (2008) framed the value of training programs to assist all employees within an organization, especially firms positioned for market expansion where virtual workers and those who telecommute need to have access to training materials. The identification of serving all pertinent stakeholders within an organization is a key component of information systems security preparations and the acknowledgement of a clearly marked constraint.

In 2015, Naser wrote that a constraint can be seen as an organizational factor that can impede progress and possibly slow down or fully halt project activities within an organization. Researchers have also written about the challenge of not addressing constraints within a system as a process that can build up over time, gain momentum, and even collapse a system (Shaw, Chen, Harris, & Huang, 2009). The same was true for information systems security, where effective business leaders and managers needed to embrace the factors of policy development and training and the confirmed influences of these factors on overall corporate financial performance. The utilization of the Theory of Constraints assisted with shining a light on the importance of training programs and policy development for public firms looking to compete in the competitive marketplace.

## Nature of the Study

The quantitative method with a correlational design were utilized for this research initiative. The selection of a quantitative method was utilized to focus specifically on the identified variables and confirmed relationships. The foundational variables utilized were the dependent variable focused on annual reported earnings of publicly traded companies on the NASDAQ Stock Exchange and an examination of overall business performance, based on the submitted filings with the Security and Exchange Commission. Similarly, the independent variables focused on level or degree of technical assistance provided to stakeholders and policies pertaining to information systems security considerations. The population utilized for the study involved 3,200 firms listed on the NASDAQ exchange and reviewed via random sampling techniques. The specific data and information utilized in the study stemmed from the annual published filings with the SEC. The study was quite beneficial as security violations and attacks were confirmed to have a significant impact on the price of stocks and reported earnings. The timing and duration of information systems security attacks served as the lens to examine constraints. The Theory of Constraints served as the foundational theory and guiding direction to examine information systems security breaches for publicly traded firms listed on the NASDAQ. Annual filings of public NASDAQ companies provided the data and information needed to examine results and confirmed trends for operations within the US.

The size of the sample was calculated via the utilization of G*Power 3.1.5; which included, a two-tailed analysis and a medium effect size. The population of 3,200 firms on the NASDAQ exchange were examined in detail to derive the needed size of the sample. Key considerations involved with deriving the sample size included distribution, level of confidence, margin of error, and the overall size of the targeted population. The study consisted of an examination of 134 annual filings via a review of annual earnings and noted security policies for firms operating via the NASDAQ exchange.

## Definitions

A guiding component of this initiative was to include pertinent operational and managerial definitions. The utilized definitions in the study are listed below:

*Annual Reports*: Financial 10-K submissions submitted to the SEC and similar governing bodies.

*Level or Degree of Information Systems Security Policy:* A systems policy established to effectively identify, facilitate, utilize, and manage security attacks and vulnerabilities.

*Publicly-Traded Firms*: For the purposes of this study, public firms were identified as those listed on the NASDAQ exchange.

*Security Attacks, Breaches, or Vulnerabilities:* This occurs when protected systems are accessed by those who were not given formal access or permissions.

*Technical Approaches or Solutions*: Training approaches or solutions were available via both software and hardware resources.

*Training Approaches or Solutions*: Training approaches or solutions were available via planned activities for organizational stakeholders via online and face-to-face instruction.

## Assumptions

There were assumptions that persisted throughout the research study. A guiding assumption was that a random selection of publicly traded companies listed on the NASDAQ Stock Exchange served as a reliable representation of the targeted public companies. In addition, the presented definitions provided a frame of reference throughout the imitative. The established statistical measurements were also trusted to provide a reliable lens for the review of research questions and the null and alternative hypotheses.

## Scope and Delimitations/ Limitations

The scope of the quantitative research project involved the analysis of companies positioned with the NASDAQ exchange. A derived random sample was established to review a concise listing of 3,200 firms on the exchange. Limitations and delimitations for the research initiative provided the parameters to review qualifications, reservations, and exceptions throughout the project (Cha & Cha, 2014; Simon, 2011; Teo & Noyes, 2011). One limitation of the project involved a focus on only companies listed with the NASDAQ exchange (Swift & Virick, 2013). An additional limitation of the research study was the fact that the researcher also actively trades and sells stock on various exchanges in the US. The intent of identifying limitations was to reduce the likelihood of bias and to ensure adherence was in accordance with the Walden University IRB and established US guidelines.

## Significance of the Study

The significance of the study can be seen by even though the growth and maturity of information is widespread throughout the market, there still seem to be many organizational challenges and impacts involved with information systems security breaches (Edwards, Grinter, Mahajan, & Wetherall, 2011: Wyrzykowska, 2014). The next step is evidenced with the identified importance of tracking corporate security policies, systems attacks, vulnerabilities, and the associated stock price and earnings for the same firms listed with the NASDAQ Stock Market (Al-Haderi, 2013). The identified results of the study should serve as a resource for the establishment of a body of knowledge to frame the importance of identifying and addressing connections with information systems security breaches, organizational policies, and corporate earnings for public firms listed on the NASDAQ exchange.

Progress has been established via the continued focus on challenges associated with network security considerations (Glenn, 2012), social challenges throughout the company (Raghuram & Fang, 2014) and the balance of work and personal responsibilities (Naor, Bernardes, & Coman, 2013); however, few researchers have studied the impact of corporate performance tied to system vulnerabilities and attacks (Lending, Minnick, & Schorno, 2018). The importance of the topic of this research project became more apparent as information systems security breaches continue to occur, increase, and have become more pervasive throughout the marketplace (Lending, Minnick, & Schorno, 2018; Lister & Harnish, 2012).

## Significance to Theory

The theory utilized as the lens for the research study involved a focus on the examination of identified constraints. Researchers have continued to note that complex systems may be examined best via the utilization and review of constraints. The TOC was utilized to examine the confirmed connection with organizational policies, corporate earnings, and security vulnerabilities for public companies. The results of the study confirm the direct association between security breaches, organizational policies, and reported earnings for public companies listed on the NASDAQ exchange.

The advantage of effective security policies were evidenced by the support provided via established systems and training programs to guide operations and to assist personnel. Raghuram and Fang (2014) suggested that the identification of one constraint provided the foundation to examine potential associations and subsequent impacts within an organization.  Similarly, Coene and Kok (2014) noted that the TOC assisted managers and business leaders with improving the identification, management, and facilitation of organizational processes.  Librelto, Lacerda, Rodrigues, and Veit (2014) argued that business leaders had the greatest benefit by incorporating identified constraints into strategic planning and operational activities.

### Significance to Practice

The confirmed results of the study should serve as resources for managers working to guide and implement information systems security plans and policies. Sharing the importance of the findings with managers, project leaders, and employees will assist with the incorporation of security guidance, training, and implementation throughout publicly traded companies.  The emphasis of security best practices throughout training and organizational activities should assist with the adoption of best practices for employees (Harandi, 2012; Lin, 2011).  Maintaining information systems security considerations with organizational practices should also contribute to more sustainable corporate projects and services.

### Significance to Social Change

The results of the study may assist with spreading the value of information systems security research, implantation techniques, and best practices.  The findings may improve the perception of information system security considerations for all organizational stakeholders; to include, consumers, partners, and community shareholders.  Provisions for social change will tie directly to how systems, security, and training are utilized throughout a community and may also lead to enhanced technological innovations.

The findings from the research project supported by the review of germane literature may enhance how all stakeholders perceive systems security, advantages of technologies, potential vulnerabilities, and the value of preparation.  The ability to champion and promote secure systems can have a lasting impact on social change throughout a community, industry, and even marketplace by increasing the number of more knowledgeable technology users.  The findings may also assist with removing barriers to technological change and instilling a greater confidence with those who use and plan for secure systems.  Lastly, a focus on information systems security planning and policies can enhance overall organizational operations and earnings for publicly traded firms listed on the NASDAQ Stock Market.

## Summary and Transition

The development of Chapter 1 began with a focus on background considerations, motivation for systems security research, and a framework that was utilized as a lens throughout the study.  Early evidence has surfaced for the need for effective and secure systems within government environments; however, the same rationale and guidance were proven to also serve as important tenets for leaders within public organizations. Seminal and current research was introduced to provide framing guidance for the focus of information systems security vulnerabilities, attacks, and preventative steps.  The framing thoughts also served as the supported and championed problem statement and purpose of the research initiative.  The research initiative may assist with filling a gap in the literature pertinent to the planning and management of information systems security policies, training, and practices throughout public firms listed on the NASDAQ.

The presentation of Chapter 2 served as a detailed and exhaustive review of the literature surrounding the topic of information systems security breaches, considerations, development, and implementation techniques. The establishment of the literature review assisted with garnering initial questions and hypotheses to guide an examination of public companies traded on the NASDAQ exchange. The transition to Chapter 3 then served as the framework to examine the research questions, hypotheses, gather data, conduct the determined statistics, and to make application to the larger community of companies traded on the NASDAQ.

# Chapter 2: Literature Review

The general business problem was to analyze the yearly filings of public companies partnered with the NASDAQ exchange to garner market patterns and financial operations for corporate activities within the US.  The examination of the connections with publicly traded firms, annual reports, corporate earnings, and security breaches was confirmed and signified the importance of proper planning, policies, and training activities.  The specific business problem was the actual connections between corporate attacks, a decline in company revenues, and the value of systems-based planning, policy development, and planning to eliminate or reduce the financial aftermath of security breaches.  The pervasiveness of corporate vulnerabilities and attacks was verified to have a direct impact on the price of stocks and the progression of company revenues.

The inclusion of Chapter 2 assisted with the development of a literature review pertaining to information systems security.  The main points presented in Chapter 2 consisted of an analysis of the connections with public companies, notices pertaining to security attacks, and confirmed financial losses.  The pervasiveness of organizational security attacks was verified to significantly impact the reported revenues for publicly traded firms listed with the NASDAQ exchange.  The timing and duration of security attacks provided the framework for the utilization of the TOC.  Akey, Lewellen, and Liskovich (2018) posited that previous studies ignored the identified constraints and the resulting impacts on stakeholder morale and organizational performance.  The yearly financial statements reported to the SEC provided an additional lens to evaluate the performance of public companies operating in the US.  The examination of the confirmed connections provided the framework to make recommendations for managers and business leaders pertinent to planning, policies, and training activities to deter or prevent information systems security breaches.

As illustrated in Figure 1, the ability to utilize established theory and organizational best practices provided the foundation; however, business leaders continued to face challenges pertinent to the planning and management of security vulnerabilities and attacks.

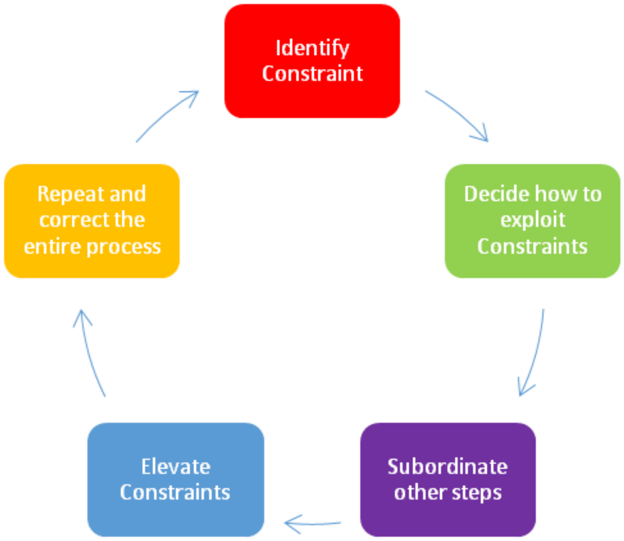

Identify Constraint
Decide how to exploit Constraints
Subordinate other steps
Elevate Constraints
Repeat and correct the entire process

*Figure 1*: Research design developed by researcher.

## Literature Search Strategy

The reviewed, cited, and referenced readings for the research study consisted of peer-reviewed publications, journals, and industry resources.  The academic databases via the Walden University online library were utilized throughout the study.  Phrases and pertinent search terms consisted of security attacks, system vulnerabilities, cloud computing, firewalls, intrusion detection systems, training, public companies, financial reports, policy development, stakeholder morale, information systems, computer security, network safeguards, telecommuting, and communications.  A combined review of 312 resources and articles served as the foundation to frame the research questions and hypotheses.

## Gap in the Literature

The goal of the research project was to ascertain the connections between public companies, systems security notices, and corporate earnings.  The persistence of organizational systems vulnerabilities and attacks was verified to have a significant connection to the revenues of public companies.  The timing and frequencies of system attacks provided the lens to review the TOC and to provide best practices for managers and business leaders within public firms.  Akey, Lewellen, and Liskovich (2018) suggested that previous quantitative studies avoided the review of drivers impacting stakeholder morale with system vulnerabilities and attacks.  The reviewed financial statements of public companies partnered with the NASDAQ exchange served as valuable resources to ascertain results and trends for operations in the US.  The analyzed predictions and connections provided the statistical basis for the confirmed relationships and subsequent recommendations pertinent to policy development, corporate revenues, training, and system vulnerabilities.

The pervasiveness of technical system integrations, subsequent vulnerabilities, and attacks has had a negative impact on stakeholder morale and public company performance for many years (Corrêa, 2013; Forgacs, 2010; Joice, 2007).  An important challenge that stems from system vulnerabilities, attacks, and inadequate training was confirmed to tie directly to a reduced interest in system integration, new product development, and a lack of recommendations for creative business solutions.  In regard to effective system preparations and training, Gupta, Sahi, and Chahal (2013) posited system vulnerabilities and attacks promote negative consequences for all stakeholders within an organization.  Almeida, Penaforte, and Yamashita (2013) framed the withdrawing of  personnel from the utilization of existing and new systems as a direct result of information systems security breaches.  The withdrawing of personnel was seen as a major event, because disengaged employees can continue a cycle of low productivity, poor performance, and losses in corporate revenues.

In 2014, Julsru and Rolan highlighted how 21% of organizational personnel did not have the interest or ability to identify system vulnerabilities and 7% of the same participants noted inadequate training as a direct influence on how breaches were managed.  To address these important considerations, the research study assisted with targeting a general business problem to analyze the yearly filings of public companies partnered with the NASDAQ exchange to garner market patterns and financial operations for corporate activities within the US.  The examination of the connections with publicly traded firms, annual reports, corporate earnings, and security breaches was confirmed and signified the importance of proper planning, policies, and training activities.  The specific business problem was then the actual connections between corporate attacks, a decline in company revenues, and the value of systems-based planning, policy development, and planning to eliminate or reduce the financial aftermath of security breaches.

## Theoretical Foundation

The theoretical foundation consisted of an acceptance model for technology (Sadat, Carter, & Golden, 2013) and a unified acceptance theory (Golden & Fromen, 2011; Schulte, 2015) as the cornerstones for the review of information systems security breaches. In the project, the TOC was utilized to ascertain connections between identified constraints and led to the development of industry recommendations. The theoretical foundation served as a guide to examine the predictions and relationships between information systems security breaches, corporate announcements, and revenue losses for publicly traded firms.

### Technology Acceptance Model

The Technology Acceptance Model (TAM) was developed to ascertain technology acceptance by organizational stakeholders. The TAM has been verified as a reliable lens to examine technology acceptance in a variety of settings and disciplines (Mupepi & Mupepi, 2014). For example, the TAM has been utilized in government, business, and even educational settings to examine technology acceptance. In addition, utilizations of the TAM can be broken down into a detailed examination of perceptions and via the potential utilization of technologies (Gregg, 2011; Lim & Teo, 2000; Troup & Rose, 2012). Considerations pertinent to technology acceptance continue to serve as benchmarks via recent and planned research activities.

In 2015, Chukudi and Daddie utilized the TAM to frame the value tied to security policies throughout international organizations. In the international research project, the researchers discovered that a pertinent factor of technology acceptance was tied to the perception of productivity that can stem for an introduced product or service. In addition, participants also noted that technology that assisted with garnering a safe and ethical environment would assist with acceptance steps. During the international project, the researchers framed an additional benefit of the TAM as a model that builds solidly off of seminal information systems guidelines stemming out of historical data center utilizations. Chukudi and Daddie (2015) also posited that additional research could assist with an examination of financial repercussions tied to security breach vulnerabilities and occurrences.

## Unified Theory of Acceptance

The utilization of the Unified Theory of Acceptance and use of Technology (UTAUT) served as a strong support within the theoretical framework of the study. The UTAUT was developed to work hand-in-hand with planners, managers, and users to encourage a technically supportive environment (Silberman & Kahn, 2011). The UTAUT was utilized to confirm an even stronger connection between information systems security breaches, corporate policy announcements, and the reported revenues for public firms listed on the NASDAQ Stock Market.

The UTAUT maintains four pillars to assist researchers and managers with technology acceptance techniques. The four pillars were leveraged as constructs and tied directly to project completion, resources utilized, social factors, and organizational support (Teo, Lim, & Wai, 1998). The benefit of UTAUT in the research project can be seen via the confirmed relationship with system vulnerabilities, attacks, available training, and overall company performance. The rationale of an organization with highly trained employees who were vigilant to thwart system breaches can be traced to overall company performance via higher stock prices and maintained or improved annual revenues. The incorporation of the UTAUT meshed well with TAM and TOC to form the theoretical framework for the study.

## Theory of Constraints

The foundational theory incorporated in this research initiative was the Theory of Constraints. An examination of potential constraints was presented by Eliyahu Goldratt in 1984. Rahman (1998) posited that factors influencing or limiting a system from heightened performance can be considered as a constraining component to operations. The overall intent of using the TOC in the project was to develop a heightened perspective pertaining to public company operations, policy notifications, annual revenues, and best practices for information systems security operations (Munoz-Leiva, Sanchez-Fernandez, Montoro-Rios, & Ibanez-Zapata, 2010; Spector, 2011). Foundational considerations in the theory were (a) constraint identification, (b) effective constraint management, (c) ancillary activities pertinent to constraints, (d) clearly identify and label constraints, and (e) necessary corrections to reduce constraint influences. These identified and organized TOC ideals are examine in detail throughout the Chapter 2 literature review. In the research initiative, the TOC was utilized as a lens to review public company operations, policy notifications, annual revenues, and best practices pertinent to information systems security operations. The persistence of system vulnerabilities and attacks in an organization were confirmed to have a significant impact on earnings per share via public companies on the NASDAQ exchange.

Important aspects of the research initiative were the identified dependent and independent variables. The dependent variable was corporate performance and revenues as denoted by annual and quarterly reports. The independent variables were degree of secure systems and the availability of technical assistance. The degree of corporate performance was noted via annual disclosures and reports. Degree of information secure systems planning was noted as the availability of clearly articulated policies within annual and quarterly reports. Degree of technical assistance was noted as the information systems security training and support available for workers throughout a company as listed within required reporting documents.

A foundational tenet of the research study was to clearly link the importance of variable association with positive outcomes. Establishing the connection of constraints and outcomes provided the mechanism to utilize the TOC to confirm both financial and operational benchmarks as constraints (Baard & Thomas, 2010; Swanberg, McKechnie, Ojha, & James, 2011). In recent years, more seminal studies have assisted with examining information systems considerations within a variety of industries; to include, manufacturing, aviation, maintenance, financial sectors, and even via international business activities. Unfortunately, Dehabi, Shokri, Ganbarvand, and Sohrabi (2014) suggested that information systems security has not been an area of emphasis pertinent to constraint-based research and analysis. The research study findings may assist with developing a connection of security breaches, training programs, operational deficits, and financial loses with constraint considerations.

An important area for constraint analysis was also with training program availability and a focus on information systems security. Aboelmaged and El Subbaugh (2012) framed the value of training programs to assist all employees within an organization, especially firms positioned for market expansion where virtual workers and those who telecommute need to have access to training materials. The identification of serving all pertinent stakeholders within an organization is a key component of information systems security preparations and the acknowledgement of a clearly marked constraint.

In 2012, Galve, Martinez, and Perez wrote that a constraint can be seen as an organizational factor that can impede progress and possibly slow down or fully halt project activities within an organization. Researchers have also written about the challenge of not addressing constraints within a system as a process that can build up over time, gain momentum, and even collapse a system (Sharma & Yetton, 2011). The same was true for information systems security, where effective business leaders and managers needed to embrace the factors of policy development and training and the confirmed influences of these factors on overall corporate financial performance. The utilization of the Theory of Constraints assisted with shining a light on the importance of training programs and policy development for public firms looking to compete in the competitive business environment.

## Literature Review

The evolving marketplace maintained a continuance of expansion across multiple industries. The growth of the marketplace was attributed to an increase in technology utilization, increasing company profits, and positive consumer sentiment. Sato (2013) framed the role of information technology and systems utilization as a powerful force throughout the business environment, especially within the United States. The need to integrate IT and systems development has provided the means to improve product development, service to consumers, and the integration of continued innovation. Shekarhizadeh, Ghasemi, Tadi, Soltani, and Nili (2015) posited that at the heart of a greater utilization of systems integration was the growing concern of information systems security procedures.

Researchers have begun to champion the need for information systems security considerations in all business environments (Barron, 2007; Frankfort-Nachmias & Nachmias, 2008; Sardeshmukh, Sharma, & Golden, 2012). Initial research has centered on technical components and steps to secure computers and networks. These steps have bene important gauges of progress and as a foundation to dig deeper into a review of systems security. Harrington and Santiago (2015) suggested that additional research steps were also needed to support the impact of security vulnerabilities and attacks on organizational performance. The importance of company performance for publicly traded firms was deemed an appropriate next step.

An important step during the examination of information systems security was to ascertain the path of empirical research and reviews. Vesala and Tuomivaara (2015) highlighted the detailed research available on network and computer systems pertinent to technical advancements and system updates. The technical advancements pertinent to security initiatives seemed to follow the same path as the growth in system vulnerabilities and attacks. An important consideration of how business leaders report and thwart security breaches surfaced as a need for future research.

A seamless operating environment where projects can be completed on time and with the planned resources was vital to business success. Turetken, Jain, Quesenberry, and Ngwenyama (2011) argued that project sustainability was a cornerstone for successful business initiatives. In this regard, sustainable and productive business initiatives often had many moving components reliant on partnering activities. The multiple intricacies and complexities of modern day projects can be evidenced via the numerous supply-chain partnerships throughout industries and across the marketplace. To maintain sustainable projects and business performance, secure systems need to be championed and maintained.

The importance of information sharing was also ascertained as a key component of organizational success and sustainment. Wright, Abendschein, Wombacher, O'Connor, Hoffman, Dempsey, Krull, Dewes, and Shelton (2014) discussed the need to maintain a consistent flow of data and information for effective decision making. In regard to proper data management and storage, security was of paramount importance. Secure and reliable data were attributed to the highest levels of quality-based information. The opportunity to leverage information that was accurate and reliable led to the most productive project deliverables (Demers, 2007; Harris, 2003; Santos, Romero, Arcelus, & Errasti, 2011). An important question raised was the heightened need for thorough training programs to keep stakeholders prepared to monitor and leverage rich deposits of data mining.

Monitoring and managing a rich data environment was seen as a needed step to the progression of effective information sharing. Harrington and Santiago (2015) posited that secure data repositories would lead to more enhanced information sharing and decision making. The need to provide effective training programs continued to surface as a paramount component of productive business development and growth. During the review of information sharing and management articles, the theme of targeted decision making surfaced repeatedly as a need for organizational success (Corwin & Harris, 2001; Schulte, 2015). An example of effective information sharing was framed as an ability to share timely information to decision makers and customer support during all collaborations and planning steps. An additional example of effective corporate information sharing surfaced via the need for timely and thorough announcements for stakeholder reviews as required via SEC guidelines. Maintaining a clear announcement protocol for organizational stakeholders would directly support internal processes of clear policy development, information sharing, and the confirmed requirement of a secure operating environment for all organizational activities.

## Security Benefit

The benefits of information systems security were universal throughout all organizational departments. Weinert (2015) monitored the progress of project completion cycles and learned that trustworthiness of personnel, data, information, and systems were paramount for successful initiatives. Weinert (2015) garnered that employees will often spend the time, effort, and energy needed to support key projects if leadership supported the initiative. Likewise, throughout the project steps, stakeholders will rally to project completion if colleagues support the effort, data are reliable, and there is ample information sharing.  The challenge for business leaders was to ensure secure systems were in place to assist with effective data storage, mining techniques, information sharing, and supportive training sessions to reinforce project milestones.

An ability to initiate well-planned projects was an important step; however, a continued focus on information systems security was seen as paramount throughout business initiatives.  Schragenheim (2011) promoted the need to champion information systems security policies and processes at all times throughout a competitive organizational environment.  Shekarhizadeh, Ghasemi, Tadi, Soltani, and Nili (2015) emphasized that information systems security was seen as a pillar for productive business development and growth regardless of the diversity of participants.  For example, ethnicity, age, and gender all appeared to have the same relationship to systems security; whereas, the value of a secure operating environment would promote sustained projects and the potential for growth opportunities (Finna & Forgacs, 2010; Niles, 1997; Wicks, 2002).  The same proved to be true for novice and experienced users throughout the business environment.

The examination of information systems security often began with government protocols.  Neirotti, Paolucci, and Raguseo (2013) posited that government regulations and policies provided the framework for beneficial initial steps for secure operating environments.  Examples can be evidenced via the Paperwork Reduction Act to promote more utilization of secure systems and the Clinger-Cohen Act to integrate leadership positions for information systems management and a continued focus on security considerations. The development of federal Chief Information Officer and Chief Information Security Officer positions also supported the rollout of information assurance requirements to maintain and support secure infrastructures.

An expansion of information systems security guidance was promoted via government guidance and regulations. Fortunately, the focus on secure systems continued to progress to the business sector across all industries. Leedy and Ormrod (2010) noted that the advantage of adhering to federal regulations and industry best practices served as forward leaning approach to organizational management. The value of adherence to governmental guidance and the positive effects of information systems security was evidenced in many markets. The challenge identified via the genesis of this research study was to translate the value of information systems security to sustained operational steps throughout publicly traded firms on the NASDAQ exchange.

## Senior Management Support

A key factor for successful business activities was noted to have a direct relationship to senior leader guidance and support. Freeman and Hasnaoui (2011) defended the need to have executive managers leading and championing in the front for productive business initiatives. The confirmed importance of executive champions was to instill confidence in all stakeholders that the organizational mission and objectives were planned and positioned appropriately for positive outcomes. The value of senior leader guidance appeared to provide a building block throughout the research study in support of stakeholder attitudes and effort. Maintaining a high level of executive support and stakeholder participation was a vital factor when examining the role of information systems security processes.

Empirical research supported the role of executive managers for information systems security initiatives throughout an organization. Georg, McGahan, and Prabhu (2012) reflected on the role of senior leader support for virtual and complex project completions throughout the global environment. In regard to executive champions, team members working in a virtual environment were noted to have a higher confidence level of project completion on complex activities when supported by project leaders and senior managers. The impact of information systems security activities looked to be reinforced similarly when executive leaders promoted and supported training, policy, and notification processes throughout firms.

## Level of Security

The frequency and timing of information systems security initiatives was a guiding focus throughout the research study. Vesala and Tuomivaara (2015) assessed the level or degree of security focus by business leaders and managers throughout annual planning activities. Naser (2015) suggested that a heightened degree of information systems security provided the overarching guidance for policy development, business leader involvement, and stakeholder support. Championing a heightened focus on information systems security planning and involvement by all organizational stakeholders served as a key component for a productive business environment. The necessity rested on the need to have consistency with respect to the frequency and timing for secure systems guidance throughout quarterly and annual processes.

A focus on information systems security should be a mandate for all organizational stakeholders. Grant, Wallace, and Spurgeon (2013) framed the significance that stemmed from stakeholder involvement in all planning and training steps to support the overall mission of the firm. An example of stakeholder participation can be evidenced via executive participation as well as managerial support throughout all organizational departments. Executive and senior manager support can then be followed by employee participation and a proactive request to seek partner involvement. The last step can then include a sample of customer participation as well as community participants who may reside adjacent to corporate, manufacturing, distribution, and retail locations. Involving all potential stakeholders in systems steps was noted a foundational component for a sustained focus on information assurance guidance and best practices.

Incorporating a consistent and overarching focus on information systems security will provide the framework for sustained and productive business activities. Montero-Marín, Carrasco, Roca, Serrano-Blanco, Gili, Mayoral, Luciano, Lopez-del-Hoyo, Olivan, Collazo, Araya, Banos, and Botella (2013) articulated the requirement to have consistent and proactive messages throughout a firm in order to maintain a heightened focus on mission critical areas. Secure systems has proven to be a mission critical area that all stakeholders need to champion. Including all stakeholders in planning steps provided an additional foundation to assist with rolling-out training programs for executives, managers, supervisors, project leaders, team members, and other identified key stakeholders.

## Security Training

Once a focus on all stakeholders was secured, managers could then ensure an organizational wide training program was planned, developed, and integrated throughout the firm. A pertinent step in the planning and development of training programs was to have a continuous focus on all available stakeholders to participate through each phase (Domiinique & Der, 2010; Morganson, Major, Oborn, Verive, & Heelan, 2010; Scholefield & Peel, 2009). The planning of training programs looked to be most effective when both internal and external stakeholders were included in all organizational activities. The notion to speed through planning steps should be avoided at all costs. Taking the time to include members of the executive team as champions, senior managers, departmental leaders, and team members was paramount for success. In addition, research touched on the value of business partners, customers, and community members to share in value-added company activities (Baruch, 2001; Watson, Blackstone, & Gardiner, 2007; Shahangian, 2007). Taking a holistic approach proved to be most effective during the planning, development, and implantation of information systems security programs.

Incorporating a holistic approach to planning focused on training programs, implementation steps, and flexibility for training sessions was also a desired component for business leaders. Potential options that assisted stakeholder participation included asynchronous and synchronous training sessions. Valmohammadi (2012) presented the need for diversity of participation for effective training programs. Similarly, Vesala and Tuomivaara (2015) posited that comprehensive and user focused training initiatives proved to have the longest lasting outcomes. In regard to stakeholder involvement, researchers also discussed the value stemming from active participation. Examples that stemmed from active stakeholder participation in training sessions included improved sense of connectiveness to the firm, heightened morale, less social anxiety via organizational initiatives, and a stronger identification to company activities. The value of holistic training programs on information systems security initiatives was strengthened via the completion of this research project.

## Low Acceptance to Security

A low level of security acceptance will have a profound effect on business performance. Van den Broek and Keating (2011) framed the necessity for managers to instill a passion for the acceptance of planned system steps and integration throughout an organization. The necessity for acceptance to information systems security initiatives was confirmed to be just as valuable throughout the research study. Research supported the proposition that security protocols and performance would improve as acceptance was supported and championed throughout a company. The result led to increased revenues for firms with proactive and engaged managers working to champion to security initiative throughout the organization.

Similarly, low security acceptance weakened stakeholder vigilance during corporate projects. The challenge was identified to have a direct connection with business leaders who champion the importance of security initiatives, training events, and protocols throughout all departments (Burke & Cooper, 2008; Caillier, 2011; Nave, 2002). Managers who served as leaders for information systems security considerations assisted with improving the abilities of team members to identify and thwart information systems security vulnerabilities and subsequent attacks.

## Level of Support for Technical Initiatives

Support for technical initiatives included a need to integrate new systems into all facets of a corporation. Beham, Baierl, and Poelmans (2014) reflected on the integration of new systems to maintain a productive and competitive workforce. Examples of system integration included ample access to cloud computing, robust network services, and well equipped personal computing devices. Additional resources confirmed to support a productive workforce are peripheral devices design to target specific functions and project activities. Peripheral devices included smart devices; such as, Internet Protocol enabled systems to include printers, scanners, cameras, phones, storage drives, applications, and media editing tools.

Training remained as a constant for technical and advanced system initiatives throughout organizations. The focused activities used by business leaders involved creative and innovative technical resources; however, training and development steps were paramount for success (Bélaner, Watson-Manheim, & Swan, 2013). Training activities looked to be best planned, developed, and integrated with ample stakeholder assistance via both internal and external participants with the organization.

Established guidelines assisted with the introduction and maintenance of systems throughout competitive firms. Empirical studies centered on the requirement of planning for complex systems and the necessary flexibilities to adapt systems for changes in the marketplace (Crandall & Gao, 2005). Examples of complex systems were evidenced via

Virtual Private Networks and Intrusion Detection System integrations. The example of Virtual Private Networks assisted with sharing private and confidential information across cloud services. On the other hand, Intrusion Detection Systems provided the ability for managers to actively monitored traffic across organizational systems. Lending, Minnick, and Schorno (2018) posited that planning, development, training, and integration served as the necessary guidelines for maintaining secure information systems security within competitive environments.

## Security Risk

The importance of risk liabilities was paramount for all stakeholders throughout publicly traded firms. Lavigne, Vallerand, and Crevier-Braud (2011) stated that risk, performance, and even perception were paramount for active participants working with complex systems. The value of reducing risk had many straightforward benefits for managers and project leaders. Reducing risk had a direct impact on the ability for firms to keep overhead expenses reduced and unnecessary expenses curtailed. Naser (2015) argued that an increase in risk can lead to increases in expenses to offset ramifications that will stem from violations, legal expenses, and even costs associated with shoring up systems, processes, and even access points. Training continued to serve as a pertinent underpinning for organizational performance.

Looking at the value of stakeholder involvement in performance, it was evident that perceptions of risk were maintained on a continuous basis. Encouraging stakeholders to remain vigilant was tied to effective training and development programs throughout companies maintaining operations within the United States (Mann &

Holdsworth, 2003). Incorporating well planned training programs will reinforce best practices introduced to employees, team members, project leaders, and managers. Establishing a solid foundation for operating procedures can provide a starting point for participant preparations. The next step was to reinforce recommended practices throughout each quarter by refresher training activities and even using planned events to incorporate new technologies and reinforcing seminal steps to reduce potential information systems security vulnerabilities and risks.

## Advantage of Security Resources

Information systems security resources served as key tools for stakeholders working within publicly traded firms listed on the NASDAQ Stock Market. The advantages of available and useful resources served as a framework for employees looking to focus on project performance and security considerations (Mamaghani, 2012). Examples of versatile technologies are biometrics to ensure identity and authentication. Also, working in secure operating environments, web-based conferencing tools can assist with bringing in partners on all projects regardless of security authorization clearances provided and maintained.

Planning for information systems security tools was an important step for information assurance initiatives. Fonne and Roloff (2012) discussed the significant returns available to participants by planning and also by thoughtful integration techniques. The steps required for integration of information systems security resources involved the introduction of tools, techniques, and also a consistent reinforcement of recommendations of best practices and lessons learned. Training steps were reinforced to have lasting benefits by annual requirements and quarterly refresher or reinforcement sessions that can encourage continued perseverance and performance.

The planning and integration of information systems security resources were paramount for successful business practices. In 2013, editors of the Status of Security in the Federal Government posited that the development of stakeholder centric policies will have a lasting effect throughout competitive firms. In regard to policy development, the requirement for policies is vital for the utilization and maintenance of effective systems. In addition and possibly more importantly, was the development of policies that supported stakeholders actively involved in corporate projects; such as, customer experiences, business partners, project leaders, team members, and managers.

## Disadvantage of Ignoring Security Requirements

One of the paramount aspects of security vigilance is to have information systems security as an incorporated item within the mission of a firm or as a direct strategic objective. Naser (2015) highlighted the significance involved with effective planning to include fundamental operational steps incorporated within the mission, goals, and objectives of an organization. In regard to security vigilance, an important consideration is the adoption and championing of security vigilance by the executive managers and business leaders within a company. The same vigilance served as a guiding sentiment throughout the review of public firms conducting business operations on the NASDAQ stock exchange.

Once the guiding principles of information systems security principles were incorporated within the mission and goals of the firm, policy creation needed to serve as a consistent pillar throughout each operational objective.  Dal Fiore, Mokhtarian, Salomon, and Singer (2014) articulated the reinforced advantages that stemmed from strategic policies and defined operational activities.  In regard to policy development, the survival of a project and even for the company as a whole can be championed via policy introduction and integration throughout annual initiatives.  Framing the significance of security vulnerabilities and attacks, stakeholders were able to ascertain the underpinnings of security vigilance during all training sessions, corporate collaborations, interactions with stakeholders, and via all operational activities.

A continued pathway for security vigilance included the need to engage stakeholders regardless of internal or external affiliations.  For example, internal leaders to the firm should champion security awareness and maintaining vigilance throughout all activities.  Likewise, internal senior managers and project leaders actively participated in training activities to establish the appropriate actions and to provide positive reinforcement for desired outcomes.  Looking at external stakeholders, integrating business partners assisted with maintaining secure supply-chain collaborations, information sharing, and data collection (Dahlstrom, 2013; Gajendran & Harrison, 2007; Taskin & Bridoux, 2010).  Lastly, bringing in customer perspectives on how security vigilance can be championed assisted with reducing complaints when developing more secure applications to better serve stakeholders and to support project completions.

## Security Productivity, Practices, and Policy

Vesala and Tuomivaara (2015) suggested that strategic organizational policies can provide the framework for effective operational steps.  An important competitive step for business leaders working to reduce or eliminate information systems security breaches was the incorporation of clear policies and training activities (Venkaesh & Johnson, 2002; Štemberger, Manfreda, & Kovačič, 2011). Policies assisted with providing the framework for executive and senior leader guidance. The guidance appeared to be most effective when planned via the board members and then championed with the executive team throughout the firm. To assist with long-term success for board guidance, a diverse board often proved to be most influential for lasting policy and guidance.

A diverse board of directors had a lasting impact on organizational structure, the sustainment of the company mission, and the application of the corporate goals and objectives. Lautsc and Kossek (2011) framed the consistent direction available via mission focused board of directors that maintained engagement with all stakeholders. A board level focus on company stakeholders will have a lasting impact on the motivation and involvement of senior leaders, managers, employees, and even external constituents; such as, with customers and business partners. Integrating board guidance with information systems security planning and training activities had a positive impact on the performance of public companies.

The achievement of board of director guidance will set the tone for executive management champions to promote the vigilance needed to address system security vulnerabilities and attacks. Instilling guidance from leaders within an organization will have a lasting impact with directing activities directed toward the corporate mission, goals, and objectives. Multiple researchers have confirmed the value of executive leaders participation via the enhancement of company training, projects, and collaborations on a continued basis (Scott, Dam, Páez, & Wilton, 2012). The continued challenge was to encourage a continued stakeholder focus on information systems security requirements for publicly traded firms listed on the NASDAQ exchange.

## Organizational Focus

An important component for successful organizational activities was noted to have a direct relationship to senior leader guidance and support. Lambert (2013) defended the need to have executive managers leading and championing in the front for productive business initiatives. The confirmed importance of executive champions was to instill confidence in all stakeholders that the organizational mission and objectives were planned and positioned appropriately for positive outcomes. The value of senior leader guidance appeared to provide a building block throughout the study in support of stakeholder attitudes and effort. Maintaining a high level of executive support and stakeholder participation was a vital factor when examining the role of information systems security processes.

To maintain a corporate focus, business leaders should campion and focus on the variables that can motivate sustained interactions. Ellison (2013) framed the true necessity of identifying and incorporating pertinent variables to begin and maintain identified business directives. In a competitive marketplace, researchers have framed the vigilance needed to avoid security breaches and costly damages tied to project delays, information theft, and data loss. Forward looking managers can instill corporate directives into training steps, organizational activities, and via all project initiatives across departments.  A more challenging component was the need to bring in external stakeholders to assist with planning, determining the variables that motivate others, and sustaining positive revenue returns.

## Measures of Security Performance

Bosua, Gloet, Kurnia, Mendoza, and Yong (2013) posited that information systems security metrics were useful for both planning and operational activities. Strategic planning steps were devised with the integration of derived data from cloud-based monitoring tools and intrusion detection systems.  Executive managers can establish policies to ensure stakeholders serve as active participants in training sessions and adhere to annual guidelines for compliance steps.  Information security metrics served as the framework for the establishment of strategic steps as well as operational requirements to assist with project milestones across organizational departments.

The information systems security operational steps that proved most effective were ones that tied directly to active projects for publicly traded firms listed on the NASDAQ Stock Exchange.  Pertinent steps were those associated with the collection of data, sharing of information, and associated with decision making interactions with customers.  Examples were championed that tied to effective system management for updates; utilization of anti-virus and malware applications; monitoring intrusion detection activities via established demilitarized zones for network and cloud-based access; adherence to compliance training; and a proactive environment where open collaborations and information sharing were encouraged by senior leaders, managers, project leads, and team members.

## Potential Indicators of Security Program Success

Research supported the continued requirement for collaborations and information sharing throughout an organization (Diana, 2010; Schulte, 2015). The focus of key indicators for corporations included the adoption of information systems security best practices for seasoned workers, who utilized technology security procedures on a continued basis versus employees who have not utilized information systems security resources. The challenge was for managers to pay close attention to systems security indicators to ensure staff are properly trained and tools were available for utilization via all project team members. The careful monitoring of information systems security indictors can provide a seamless step for annual and quarterly audits.

Schwarz (2012) championed the requirements and benefits associated with continual information systems audits throughout organizations. The value of careful adherence to information systems security indicators was evidenced by a more robust audit process; where, stakeholders are encouraged to participate via the established cycle of review and feedback. In regard to sharing indictors with all participants, active participants can ensure systems are available for managers to review, for auditors to examine, and schedules are managed via a cloud-based system where all pertinent stakeholders can schedule meetings and follow-up discussions. Incorporating active communications via information systems security oversight and auditing steps can lead to proactive employees engaged in information assurance steps to maintain sustainable operations.

## Organizational Change and Challenges

A competitive step for business leaders to champion information systems security best practices was embedded in systematic planning and operational steps. Kossek, Hammer, Kelly, and Moen (2014) articulated the necessity for business leaders to garner industry best practices and to incorporate tested measures throughout organizational activities. An important characteristic was to garner best practices and to, as time permits, incorporate a focus group to verify current approaches that will serve to foster competitive information assurance projects. Focus groups can be developed from traditional advisory committees, where diverse stakeholders are engaged in reviewing best practices and providing operational guidance.

Advisory committee involvement can serve as a beacon for transforming and continuing information systems security activities throughout publicly traded companies operating in the United States. Advisory committee development can be comprised of customers, business partners, employees, team members, project leaders, senior managers, and executives (Fitnes, 2008; Sanchez-Fernandez, Munoz-Leiva, Montoro-Rios, Ibanez-Zapata, 2010). Where appropriate, board members were also challenged to participate in advisory committee activities. The establishment of advisory committees may also have an influential impact on middle managers, where information systems security metrics are established, championed, and carried-out on a quarterly and annual basis throughout the activities of public companies operating on the NASDAQ exchange. The continuation of established procedures for information systems security procedures can establish the long-term strategic goal for secure operations, as well as the guideposts for daily, weekly, monthly, and quarterly steps to complete tasks and to fulfill requirements within established expectations. Incorporating diverse advisory committee support was noted as guiding both strategic planning and operational project steps.

## Relationship of the Study to Previous Research

Past studies have noted pertinent obstacles business leaders undertake with instilling an information assurance atmosphere and the value of ascertaining components that encourage effective operational steps (Robertson, Schleifer, & Huang, 2012). As noted in the review of the literature, few endeavors incorporated the integration of security steps into organizational activities. Industry practices have demonstrated that information systems studies assisted with the integration of cognitive concepts into operational steps. In regard to applying cognitive steps, empirical activities have demonstrated that information assurance activities can invigorate security vigilance if effective training standards were introduced, maintained, reinforced, and audited on a continued basis. Continued integration of information systems security initiatives, programs, and vigilance proved to be effective for the removal of factors pertaining to security weaknesses, vulnerabilities, and the ramifications of attacks.

The factors chosen for review in the research project were anticipated continuations of areas needed for additional analysis in the field of information systems security. Rivera-Rodriguez, McGuire, Carayon, Kleiner, Wears, Robertson, Holden, and Waterson (2013) analyzed the steps needed to obtain stakeholder support and then the subsequent interest of stakeholders to share obtained and gained information with fellow team members and employees. The analysis revealed that an organizational environment that encouraged information sharing would be less susceptible to violations and breaches of established protocols. The same results were proven to exist with the study and the examination on information systems security breaches for publicly traded firms operating in the United States and listed with the NASDAQ Stock Market.

## Summary and Conclusions

The research project was undertaken to ascertain the connections between public companies, systems security notices, and corporate earnings. The persistence of organizational systems vulnerabilities and attacks was verified to have a significant connection to the revenues of public companies. The timing and frequencies of system attacks provided the lens to review the TOC and to provide best practices for managers and business leaders within public firms. Ojala, Nätti, and Anttila (2014) suggested that previous quantitative studies avoided the review of drivers impacting stakeholder morale with system vulnerabilities and attacks. The reviewed financial statements of public companies partnered with the NASDAQ exchange served as valuable resources to ascertain results and trends for operations in the US. The analyzed predictions and connections provided the statistical basis for the confirmed relationships and subsequent recommendations pertinent to policy development, corporate revenues, training, and system vulnerabilities.

The progression of technical system integrations, subsequent vulnerabilities, and attacks have had a negative impact on stakeholder morale and public company performance for many years (Fonner & Stache, 2012; Offstein, Morwick, & Koskinen, 2010). An important challenge that stems from system vulnerabilities, attacks, and inadequate training was confirmed to tie directly to a reduced interest in system integration, new product development, and a lack of recommendations for creative business solutions. In regard to effective system preparations and training, Watad and Will (2003) posited system vulnerabilities and attacks promote negative consequences for all stakeholders within an organization. Yahaya, Basir, and Deraman (2015) framed the withdrawing of personnel from the utilization of existing and new systems as a direct result of information systems security breaches. The withdrawing of personnel was seen as a major event, because disengaged employees can continue a cycle of low productivity, poor performance, and losses in corporate revenues.

The focus of research steps and analytics in Chapter 3 were initiated to frame the research method, design, and subsequent steps. A rigorous focus of the research method, design, participant data, sampling techniques, information gathering, hypotheses, analysis of data, ethical concepts, limitations, and validity were examined. Chapter 4 was developed to provide a detailed analysis of the research questions, hypotheses, and subsequent research findings pertinent to the project. The culmination of the research project surfaced via Chapter 5, where social change considerations, implications, recommendations, and a discussion on garnered information systems security best practices will be provided for business leaders within publicly traded firms listed on the NASDAQ exchange and operating within the United States.

# Chapter 3: Research Method

Based on information systems serving as a foundational backbone for competitive firms today, systems breaches and violations have grown in occurrence and severity pertinent to financial losses and operational downtime (Burbah & Day, 2012). In 2015, Naser discussed how a growing occurrence of information systems breaches were leading to undiscerning employees who were unsure of proper courses of action for system attacks and vulnerabilities. The noted corporate system shortcomings provided the framework for a general business problem to ascertain quarterly and annual reports of public firms listed on the NASDAQ exchange and provided a key lens to analyze market results and trends for organizational operations within the US. An examination of the predictions and connections provided the diagnostic to ascertain relationships and to garner specific guidance for public company operations, policy notifications, annual revenues, and best practices pertinent to information systems security operations.

## Research Design and Rationale

This study consisted of a correlational research initiative to ascertain the association and connections of vigilant corporate policies and stakeholder involvement with public companies, notices pertinent to breaches of security, and reported earnings. A persistence of system vulnerabilities in organizations had a significant impact on the price of stocks and annual revenues for public firms partnered with the NASDAQ exchange. Derived data were reviewed via the Pearson Correlation to examine the relationship with the identified independent and dependent variables. A review of the predictions and connections was used as the lens to ascertain relationships and to garner specific guidance for public company operations, policy notifications, annual revenues, and best practices pertinent to information systems security operations. The dependent variable was corporate performance and revenues as denoted by annual and quarterly reports. The independent variables were degree of secure systems and the availability of technical assistance. The population for the research initiative stemmed from a calculated sample of public companies partnered with the NASDAQ exchange.

## Methodology

### Population

The quantitative method with a correlational design were utilized for this research initiative. The selection of a quantitative method was utilized to focus specifically on the identified variables and confirmed relationships. The foundational variables utilized were the dependent variable focused on annual reported earnings of publicly traded companies on the NASDAQ Stock Exchange and an examination of overall business performance, based on the submitted filings with the Security and Exchange Commission. Similarly, the independent variables focused on level or degree of technical assistance provided to stakeholders and policies pertaining to information systems security considerations. The population utilized for the study involved 3,200 firms listed on the NASDAQ exchange and reviewed via random sampling techniques.

### Sampling Procedures

The specific data and information utilized in the study stemmed from the annual published 10-K filings with the SEC. The study was quite beneficial as security violations and attacks were confirmed to have a significant impact on the price of stocks and reported earnings. The timing and duration of information systems security attacks served as the lens to examine constraints. The Theory of Constraints served as the foundational theory and guiding direction to examine information systems security breaches for publicly traded firms listed on the NASDAQ. Annual filings of public NASDAQ companies provided the data and information needed to examine results and confirmed trends for operations within the US.

### Sample Size Estimate

The size of the sample was calculated via the utilization of G*Power 3.1.5; which included, a two-tailed analysis and a medium effect size. The population of 3,200 firms on the NASDAQ exchange were examined in detail to derive the needed size of the sample. Key considerations involved with deriving the sample size included distribution, level of confidence, margin of error, and the overall size of the targeted population. The study consisted of an examination of 134 annual filings via a review of annual earnings and noted security policies for firms operating via the NASDAQ exchange.

### Procedures for Recruitment, Participation, and Data Collection (Primary Data)

The population for the project involved of a 3,200 sample of public companies partnered with the NASDAQ exchange. The foundational components of the project were the dependent variable; which included, the degree of earnings for randomly selected public firms listed with the NASDAQ exchange and the identified independent variables. The independent variables additionally served as foundational precepts and included the amount of technical assistance and degree of systems security strength and vulnerability. The information was gathered via the yearly 10-K filings for public companies working within the SEC guidelines.  The consistent occurrence of information systems security vulnerabilities and attacks was determined to have a significant connect with annual revenues for the randomly selected public firms.  The timing and duration of system attacks was established as the framework to analyze the TOC.  Utilizing a focus on constraints provided the lens to review information systems security vulnerabilities and attacks in more detail.  Analyzing yearly 10-K submissions for public firms adhering to SEC requirements provided the backdrop to ascertain trends and best practices for business leaders guiding US activities and operations.

The continued growth of electronic commerce, business-to-business activities, customer-to-business interactions, and via business-to-government filings provided a wealth of resources to review throughout the research project (Dailey, 2010; Goodan & Wood, 2004; O'Driscoll, Brough, Timms, & Sawang, 2010; Reinsch, 1999).  The business-to-government interactions provided a means to track the progress of public firms listed on the NASDAQ Stock Market.  Taking the time to analyze the 10-K filings for randomly select firms established a framework to scrutinize data points, information sharing, planned activities, completed tasks, vulnerabilities, trends, and recommendations for continued corporate performance (Mitchell, Gagné, Beaudry, & Dyer, 2013).

Pertinent data points and information sharing were core tenets of the planned and conducted research study.  The first step began with the review of literature to ascertain identified gaps and opportunities for research.  The next steps included a research plan to develop the needed questions, hypotheses, and methodology required for the collection of data, analysis of information, and for the providing of recommendations.  The randomly selected public firms were listed via the open trading process on the NASDAQ stock exchange. The collected data points underwent an examination via statistical analytics with the utilization of the Statistical Package for Social Science (SPSS) software application.

## Instrumentation

The framed project was completed via the utilization and analysis pertinent to the SPSS application. Analytical software garnered numerous advantages beyond basic analysis of information; to include, managing time limitations, coordinating required costs, and for the analyzation of organized information and data points. The continued advantages that stemmed from the utilization of SPSS analytics provided the means to review larger sets of data, reviewing available statistical steps for appropriateness, organizing selected computations, and analyzing the provided outputs (Dimitrova, 2003; Smith & Mateas, 2011; Swink, 2001). The ability to utilize statistical software applications provided the researcher with the ability to analyze the data sets, data outputs, to organize key groupings of data and information, and to establish overarching conclusions for application to larger communities.

The random selection of public companies maintain operations in the United States and partnered with the NASDAQ exchange provided the backdrop for the research study. A complete list of firms partnered with the NASDAQ were reviewed via reported yearly earnings via SEC filing guidelines. The organized firms were listed via three sections labled as high, medium, and low yearly earnings, as reported via 10-K filings. The companies were next provided with a number for identification via the utilization of a software application for the generation of labels for the random review process. The garnered sample was verified to assist with an adequate portion of all publicly traded firms on the identified exchange. Garnered information was reviewed via correlational analytics; such as, with the Pearson tool, to ascertain the confirmed connections via the dependent and independent variable components for further utilization in the research project.

## Operationalization

### Levels of Measurement

The measurement degree provides the framework of variables established via the garnered numerical values. The four measurement levels were labeled as ratio, interval, ordinal, and nominal. The measurement degree or levels additionally provided an informative descriptive label for the variables that were utilized during each statistical step. Throughout the research project, the variables and analytic steps were initialized and continued to maintain a focus on the dependent and independent components of the study. Important aspects of the research initiative were the identified dependent and independent variables. The dependent variable was corporate performance and revenues as denoted by annual and quarterly reports. The independent variables were labeled as the degree of secure systems and the availability of technical assistance. The degree of corporate performance was noted via annual disclosures and reports. Degree of information secure systems planning was noted as the availability of clearly articulated policies within annual and quarterly reports. Degree of technical assistance was noted as the information systems security training and support available for workers throughout a company as listed within required reporting documents.

## Data Analysis

The Statistical Package for the Social Sciences (SPSS) version 20.0 is the software tool that was utilized to analyze annual reports of publicly traded organizations listed with the NASDAQ Stock Market can assist with establishing trends and examining industry results for firms operating within the United States. Babbie, Wagner, and Zaino (2015) noted that SPSS was produced by an IBM company in 2009 in Chicago, Illinois. They concluded that SPSS is still the most popular professional program available for social science data analysis.

Different type of tests in this quantitative research study were performed. Descriptive statistics have two important purposes in quantitative research studies. Ho and Carol (2015) suggested that descriptive statistics summarize a data set and describe the sample size and occurrences. The following are analysis procedures that were performed in this study:

1. Raw data were converted to statistics.
2. Means, standard deviations, and correlations of all variables were produced.
3. Summary to describes groups and their responses was calculated using Pearson's Correlation.
4. Charts and diagrams were prepared to interpret statistical information.

## Threats to Validity

The importance of validity was seen via the completeness of the research steps, the importance, and with the accurateness of the reported results (Gibbs, Scott, Kim, & Lee, 2010; Haddo & Brynin, 2010; Rau & Hyland, 2002). Validity pertinent to empirical research, content considerations, and via constructs were all utilized to strengthen the instrumentation processes (Fink, 2005). During the project, validity pertinent to constructs were examined and factored to ensure instrument estimations were maintaining an alpha of more than .70 for variables as planned. Additional steps included a focus on validity pertinent to content to ensure findings, results, and processes were accurate and ascertainable as the study progressed. The consistent goal throughout the research project was to ensure the identified gap from the literature tied directly to the established relationships with the research questions, dependent variable, and independent variables. In regard to the established relationships between the variables and utilized instrumentation, validity pertinent to empirical standards remained as a constant throughout the project (Simon, 2011). A consistent program of instrumentation and measurement assisted with confirming the strength of correlation between dependent and independent variables. Careful and thoughtful steps served as a pathway throughout the study to ensure the analyses could be replicated with similar results in upcoming research activities (Mateyka, Rapino, & Landivar, 2012). The incorporation of Cronbach’s alpha pertinent to instrumentation reliability and variable review served as a recommended research standard.

A focus on quality served as an asset throughout the research study; whereas, collegial researchers will be able to utilize the validity, reliability, and consistent analytical steps to replicate similar studies. An application connecting this research project to future studies may include a bridging of steps to further examine satisfaction and acceptance of information systems security protocols within public companies listed on the NASDAQ exchange. A pivotal aspect of the research project was the reinforcement of internal validity throughout the research study. The focus on validity also tied to the value of external validity and support for colleagues looking to replicate key aspects of the activity (Albiero, Verive, Cooper, & Knott, 2010; Guimaraes & Dallow, 1999). The results of the study may not have a confirmed generalizability to all publicly traded firms throughout the international environment; however, a strong and consistent internal validity will be seen as a powerful connection to external validation steps for researchers and statisticians.

In 2011, Kanellopoulos proposed that quantitative research techniques were valuable to cobble together the benefits of internal validity with mathematical conclusions to champion the likelihood of causal effects. A follow-on step may then be future studies and the significance of generalization to other environments due to the likelihood of sound construct and external validity. Subsequent drawbacks pertaining to validity throughout the project mandated the need to note that proven analytics were, by themselves, not enough to generalize findings to a larger community. In addition, the heightened focus on random sampling procedures provided confidence that sources of information and intrinsic data steps were sufficient for the successful completion of the planned research steps and overall project.

## Ethical Procedures

An important aspect of research procedures was the incorporation of ethical considerations throughout each step of the study. During the planned and developed research initiative, professional protocols were implemented to assist with maintaining data protections and confidentiality for each randomly selected company (Asgari,H. & Mohseni, 2014; Olaniran, 2009). The IRB Department at Walden University provided established protocols, guidance, and recommended steps for sound research and ethical procedures. During the doctoral research process at Walden University, students continue to participate in training, guidance, and instructional steps to apply and implement all required processes throughout research initiatives. In regard to the research process, the Walden IRB Department served as a continued source of guidance for data collection and ethical best practices throughout the research initiative. In the research study, data were gathered from the annual filings of 10-K reports via SEC guidelines. The annual reports of publicly traded companies listed on the NASDAQ exchange served as the source of data points and information that were utilized during the statistical analysis steps. In the research study, participants were not required, because the quantitative initiative focused on an analysis of correlational data targeting the established research questions and hypotheses. Confidentiality will be maintained by ensuring that corporations and responding data will continue to be protected, public company anonymity was achieved via coding, and at a recommended date, all data and information will be destroyed in accordance with established procedures.

## Summary and Conclusions

The goal of the correlational research study was to ascertain the association and connections of vigilant corporate policies and stakeholder involvement with public companies, notices pertinent to breaches of security, and reported earnings. A persistence of system vulnerabilities in organizations had a significant impact on the price of stocks and annual revenues for public firms partnered with the NASDAQ exchange. Derived data were reviewed via the Pearson Correlation to examine the relationship with the identified independent and dependent variables. A review of the predictions and connections was used as the lens to ascertain relationships and to garner specific guidance for public company operations, policy notifications, annual revenues, and best practices pertinent to information systems security operations. The dependent variable was corporate performance and revenues as denoted by annual and quarterly reports. The independent variables were degree of secure systems and the availability of technical assistance. The population for the research initiative stemmed from a calculated sample of public companies partnered with the NASDAQ exchange. The research activity may be noted as a guide to champion social change initiatives via the effective management of training and policy development pertinent to corporate security activities.

The pervasiveness of technical system integrations, subsequent vulnerabilities, and attacks have had a negative impact on stakeholder morale and public company performance for many years (Fonner & Stache, 2012; Offstein, Morwick, & Koskinen, 2010). An important challenge that stems from system vulnerabilities, attacks, and inadequate training was confirmed to tie directly to a reduced interest in system integration, new product development, and a lack of recommendations for creative business solutions. In regard to effective system preparations and training, Watad and Will (2003) posited system vulnerabilities and attacks promote negative consequences for all stakeholders within an organization. Yahaya, Basir, and Deraman (2015) framed the withdrawing of personnel from the utilization of existing and new systems as a direct result of information systems security breaches. The withdrawing of personnel was seen as a major event, because disengaged employees can continue a cycle of low productivity, poor performance, and losses in corporate revenues.

The intent of research steps and analytics in Chapter 3 were initiated to frame the research method, design, and subsequent steps. A detailed focus of the research method, design, participant data, sampling techniques, information gathering, hypotheses, analysis of data, ethical concepts, limitations, and validity were examined. Chapter 4 was developed to provide a detailed analysis of the research questions, hypotheses, and subsequent research findings pertinent to the project. The culmination of the research project surfaced via Chapter 5, where social change considerations, implications, recommendations, and a discussion on garnered information systems security best practices will be provided for business leaders within publicly traded firms operating in the US and listed on the NASDAQ exchange.

# Chapter 4: Results

## Introduction

One important aspect of this correlational quantitative project was the analyzation of the posed connections between security breaches and the abundance of information systems utilizations framed in Chapter 3. I organized Chapter 4 via a framework of the purpose of the project, research questions, provided hypotheses, preparation process, collection of data, the analyses performed on the data and garnered information. The analyses were conducted to examine the hypotheses. I framed the value of descriptive statistics pertinent to this study to include correlational considerations, utilization of analysis of variance, regression analyses, and a summary of results.

The theme focused on how an overabundance of information system uses by corporate stakeholders (i.e., employees) may be leading to the demise of information security protections. A continuous exposure to technology tools, resources, and applications may be making it challenging for stakeholders to see the true connection with activities and potential security vulnerabilities throughout an organization. From 2010 through 2016, the number of reported information systems breaches, via public announcements, increased by 14%—occurrences reported by more than 800 companies (Antoniou & Cooper, 2013; Rasmusen & Corbett, 2008). There may have also been a larger percentage of breaches not reported via publicly-traded firms throughout the US-based stock exchanges. In 2010, there were 6,687 reported security breach incidents, which increase to more than 8,268 in 2016 and subsequent years. The increase in security breaches in 2016 reveals a 19% growth in occurrence and continues the discussion of how can such events be thwarted and reduced (Lo, van Breukelen, Peters, & Kok, 2013). The dependent variable was consistently defined as the number of security breaches and the self-reported loss in corporate earnings associated with the security breach as a percentage of revenue. The dependence of security breaches was determined to have directional linkage to information systems utilization, increased application usage, and an almost numbness to potential threats due to the overabundance of technology throughout all departments of an organization. In Chapter 4, I answer both posed research questions framed earlier in the study and revisited in this section.

## Data Review

Data were gathered based on the established Walden University IRB research protocols. The collection steps stemmed from a review of 134 randomly selected companies on the NASDAQ Stock Exchange. Data were organized via an alphabetical label to maintain anonymity. The company labels began with an A, progressed to AA, AB, and ended with DE. The collected data were also organized based on the identified variables of Level of ISS Policy, Loss of Revenue, and Number of ISS Breaches. The Level of ISS Policy gathered data was based on a 1-5 Likert Scale. The Loss of Revenue was tied to the percentage of revenue for the reviewed company. The Number of ISS Breaches was based on the number reported annually. The Level of ISS Policy had scores ranging from 1 to 5 with an average for all reviewed companies of 3.17. The Loss of Revenue data had a range from 0 to .19 or 0% to 19% and an average of .051 or 5.1% for all reviewed companies. The Number of ISS Breaches had scores ranging from 0 to 7 with an average for the reviewed companies of 2.40.

The phrase level of ISS Policy looked to be significant and implied a degree or scale of understanding that is important for security functions. Reduced awareness levels signified a substantial negligence of security risk that can led to damages beyond repair. The conducted study was devised to review the correlation among established policies on systems, security breach intensity, and the earnings noted for public firms listed with the exchange on the NASDAQ. The NASDAQ was selected as a main component of the research study, because Kassinis and Stavrou (2013) argued that, traditionally, smaller and younger organizations are listed on the exchange with the NASDAQ. An exchange for stock purchases with a propensity of smaller and younger firms was an ideal environment to examine information assurance levels of awareness. Results yielded that productive business administrators have in place protocols for addressing security concerns within public entities traded on the NASDAQ exchange.

The governance of organizational information systems encompassed the establishment of management levers within the business community to incorporate information and communications technologies to ensure consistent interchanges and connections. Incorporating pertinent systems granted users a great ability to leverage the requirements for project-based constraints, financial needs, and fulfilled activities (Khoda-yari & Rahnavard, 2013). Continued returns stemmed from the successful incorporation of security systems, policies, training programs, and evidenced via heightened company profits.

After 2013, more than 29% of establishment leaders recognized the utilization of operational instructions, security systems policies, and training curriculum for employees

(Woodman, 2014). Statisticians have examined constraints pertinent to variables that can impact the integration of policies for information system guidelines and breach preventions for all corporate personnel (Ko, Hur, & Smith-Walter, 2013). Ko and Hur (2014) studied the impact of business systems procedures in federal agencies, state institutions, and discovered business leaders were more likely to report the breaches of systems when resources were available to utilize to effectively manage occurrence of security violations. Belle, Burley, and Long (2015) examined the notes of seasoned business leaders which framed how barriers existed in the workplace that were tied to training, culture, and even the utilization of technologies. Akey, Lewellen, and Liskovich (2018) suggested that the lack fortified infrastructures, training, and maintaining of systems steps led to shortcomings when policies were not in place. The identified goal was then to establish and maintain policies that can be utilized during all organizational events.

Competitive firms were then those with managers who led by setting the example of problem identification, training deficits, shortcomings pertinent to security knowledge, and applications for busy project environments. During all organizational activities, it became clear that business leaders must instill a culture focused on acquiring the skills needed to maintain healthy systems and the avoidance of security breaches (Belle, Burley, & Long, 2015). After federal events, state activities, and via published findings, the sharing of information was noted has highly important for preparing for and preventing information systems security breaches. Managers and researchers touted solutions pertinent to interagency sharing, planning steps, minimizing known risks, incorporating barriers, utilizing biometrics, and leveraging token-based accounts to not only prepare organizational environments for potential security breaches, but to also thwart unforeseen attacks.

The challenges associated with data management, information sharing, and training initiatives were noted to serve as potential barriers; however, these can be reduced or eliminated by continued collaborations and partnerships across institutions. The obstacles remained for not only government agencies, but also for firms publicly traded on the NASDAQ exchange. The identified initiatives of information sharing, instilling executive champions, developing policies pertinent to information systems security breaches, integrating controls, and encouraging increases training can all provide the greatest returns. The greatest returns were easily identified via corporate earnings and increased revenues; however, other drivers also surfaced as investor sentiment and the satisfaction of customers, stakeholders, and even from current employees.

An identified challenge in the business environment was to ensure collaborations and information sharing occurred via protected communication modalities. In this regard, secure collaborations and communications can also be linked to project performance and the overall productivity of business initiatives. Alizadeh (2012) posited that in many successful business environments, diverse forms of communications were utilized for collaborative purposes and to accomplish tasks at hand. A continued challenge was to ensure guidelines were in place that assisted with guiding effective communications, protecting information sharing, and securing valuable industry data. Bratton (2013) also suggested that pivotal and popular technologies assisted with project team collaborations, information sharing, and distributing findings across organizational teams, departments, agencies, and even throughout supply-chain partners. The remaining goal was to ensure that information systems security policies existed that guided and protected all collaborations and information sharing.

A constant theme in the literature about level of risk and how this information is applied to the work environment was observed. Naser (2015) noted that risk level should be included within training programs and policy considerations to ensure stakeholders are knowledgeable about the potential severity of threats. Studies have also been conducted that support risk level integration within both quarterly and annual training events (Orttung & Overland, 2011). Belle, Burley, and Long (2015) reported that many security breaches occur because of identified vulnerabilities in a system, which can be due to personnel activities and even to a lack of system updates. Business leaders should constantly challenge themselves and team members to be vigilant with all preparations.

A variety of factors have led to identified information security breaches for publicly traded companies. In regard to the variety of vulnerabilities that can occur, Belle, Burley, and Long (2015) identified factors pertaining to frequency of training for employees, the curriculum that is utilized during training events, the stakeholders engaged in preparation activities, and the policies utilized throughout an organization. The trend with policy development appeared to focus more on intent, curriculum, participants, and frequency versus the specific information systems utilized to thwart potential breaches.

A key ingredient within information systems security policy and training development was the value of stakeholder awareness. Chukudi and Daddie (2015) provided an overview of substantiated training approaches that have led to the greatest return for employee awareness, comprehension, and even for application within a work environment. The research framed the significance of leader involvement in policy development, implementation, and with training opportunities. For example, some findings purported that gestalt approaches can enhance planned processes, enhanced focus on provided information, and with respect to enhanced awareness levels. Reflection steps highlighted that more engaged business leaders had a positive impact on employee and stakeholder willingness to ascertain training guidance and also to implement the recommendations provided. The motivation for employees certainly is a straightforward consideration to implement all provided guidance; however, the ability for executives, managers, and project leaders to engage stakeholders on the periphery of the company should also lead to positive returns for implantation and the eventual reduction in successful security breaches.

The enhancement of curriculum in training sessions has a lasting impact on participants. Sikes, Mason, and VonLehmden (2011) posited that the incorporation of relevant and applicable information served as a key motivator and vital resource for active learners who participated in training sessions. The foundational concept appeared to center on the relevance of data and information provided for the participants. A look at training sessions pertinent to information systems security made it quite clear that systems attacks and breaches were tied to recent events, so the same timely information and content are needed within all planned training activities. Incorporating recent information that stemmed from information systems security breaches, attacks, and even thwarted activities should follow the same guidance and lead to operational environments centered on proactive stakeholders actively looking to thwart potential breaches.

## Research Intent and Rationale

The foundational theory incorporated in this research initiative was the TOC. An examination of potential constraints were presented by Shekarhizadeh, Ghasemi, Tadi, Soltani, and Nili (2015) during the development of a review of constraints. Venkaesh, Morris, Davis, and Davis (2003) posited that factors influencing or limiting a system from heightened performance can be considered as a constraining component to operations. The overall intent of using the TOC in the research initiative was to develop a heightened perspective pertaining to public company operations, policy notifications, annual revenues, and best practices for information systems security operations. Foundational considerations in the theory were (a) constraint identification, (b) effective constraint management, (c) ancillary activities pertinent to constraints, (d) clearly identify and label constraints, and (e) necessary corrections to reduce constraint influences. These identified and organized TOC ideals are examine in detail throughout the Chapter 2 literature review. In the research initiative, the TOC was utilized as a lens to review public company operations, policy notifications, annual revenues, and best practices pertinent to information systems security operations. The persistence of system vulnerabilities and attacks in an organization were confirmed to have a significant impact on earnings per share via public companies on the NASDAQ exchange.

Important aspects of the research initiative were the identified dependent and independent variables. The dependent variable was corporate performance and revenues as denoted by annual and quarterly reports. The independent variables were the degree of systems security and the availability of technical assistance. The degree of corporate performance was noted via annual disclosures and reports. Degree of information secure systems planning was noted as the availability of clearly articulated policies within annual and quarterly reports. Degree of technical assistance was noted as the information systems security training and support available for workers throughout a company as listed within required reporting documents.

A foundational tenet of the research study was to clearly link the importance of variable association with positive outcomes. Establishing the linkage of constraints and outcomes provided the mechanism to utilize the TOC to confirm both financial and operational benchmarks as constraints (Pfeffer, 2010). In recent years, more seminal studies have assisted with examining information systems considerations within a variety of industries; to include, manufacturing, aviation, maintenance, financial sectors, and even via international business activities. Unfortunately, Pan, Woodside, and Meng (2014) suggested that information systems security has not been an area of emphasis pertinent to constraint-based research and analysis.

The conducted Pearson Correlation established a clear association between information security breaches, losses in corporate earnings, and the value of information systems security policies to effectively manage and reduce the potential severity of damages. Appendices A and B denote the correlation at .858 and .764. The descriptive statistics assisted with shining a light on the associations between all pertinent variables. In this regard, a loss of corporate earnings, listed via a percentage of revenue, produced a mean of .051, a standard error of .004, a median of .031, and a mode of 0. The standard deviation for revenue losses was .050 and a sample variance of .003. The kurtosis was determined at .071 and the skewness at .974.

The findings from the level of information systems security policy, listed via Likert score of 1 to 5, and the number of security breaches annually produced similar associations. The correlation at .858 and .764 strengthens the likelihood of a clear association between variables. In this regard, the level of information systems security policy produced a mean of 3.17, a standard error of .108, a median of 3, and a mode of 4. The standard deviation for revenue losses was 1.25 and a sample variance of 1.56. The kurtosis was determined at 1.02 and the skewness at .143. Similarly, the level of information systems security breaches produced a mean of 2.40, a standard error of .173, a median of 2, and a mode of 1. The standard deviation for revenue losses was 2.00 and a sample variance of 4.02. The kurtosis was determined at .800 and the skewness at .5.

An important area for constraint analysis was also with training program availability and a focus on information systems security. Chukudi and Daddie (2015) framed the value of training programs to assist all employees within an organization, especially firms positioned for market expansion where virtual workers and those who telecommute need to have access to training materials. The identification of serving all pertinent stakeholders within an organization is a key component of information systems security preparations and the acknowledgement of a clearly marked constraint.

In 2015, Naser wrote that a constraint can be seen as an organizational factor that can impede progress and possibly slow down or fully halt project activities within an organization. Researchers have also written about the challenge of not addressing constraints within a system as a process that can build up over time, gain momentum, and even collapse a system (Azarbuyeh & Naini, 2014). The same was true for information systems security, where effective business leaders and managers needed to embrace the factors of policy development and training and the confirmed influences of these factors on overall corporate financial performance. The utilization of the Theory of Constraints assisted with shining a light on the importance of training programs and policy development for public firms looking to compete in the competitive marketplace.

The quantitative method with a correlational design were utilized for this research initiative. The selection of a quantitative method was utilized to focus specifically on the identified variables and confirmed relationships. The foundational variables utilized were the dependent variable focused on annual reported earnings of publicly traded companies on the NASDAQ Stock Exchange and an examination of overall business performance, based on the submitted filings with the Security and Exchange Commission. Similarly, the independent variables focused on level or degree of technical assistance provided to stakeholders and policies pertaining to information systems security considerations.

The population utilized for the study involved 3,200 firms listed on the NASDAQ exchange and reviewed via random sampling techniques. The specific data and information utilized in the study stemmed from the annual published filings with the

SEC. The study was quite beneficial as security violations and attacks were confirmed to have a significant impact on the price of stocks and reported earnings. The timing and duration of information systems security attacks served as the lens to examine constraints. The Theory of Constraints served as the foundational theory and guiding direction to examine information systems security breaches for publicly traded firms listed on the NASDAQ. Annual filings of public NASDAQ companies provided the data and information needed to examine results and confirmed trends for operations within the US.

The size of the sample was calculated via the utilization of G*Power 3.1.5; which included, a two-tailed analysis and a medium effect size. The population of 3,200 firms on the NASDAQ exchange were examined in detail to derive the needed size of the sample. Key considerations involved with deriving the sample size included distribution, level of confidence, margin of error, and the overall size of the targeted population. The study consisted of an examination of 134 annual filings via a review of annual earnings and noted security policies for firms operating via the NASDAQ exchange.

## Preparation and Collection

The necessary data required for the conducted research study were obtained with secondary data via a public website managed by NASDAQ. The NASDAQ Stock Market requires all listed firms to provide annual and quarterly reports of necessary data and metrics. The collected data were in the form of numerous cells holding numerical values based on pre-defined categories; such as, number of employees and financial earnings. The collected data were then made available, via downloaded files, for stakeholder review and analysis and for NASDAQ observations for compliance and pertinent organizational activities.

The necessary data provided and collected via NASDAQ are made possible with the assistance of the Freedom of Information Act within the 5 USC 552. An important step pertinent to data analysis was the ability to participate in a free and open marketplace, where researchers, investors, consumers, and fellow stakeholders can access the data and information needed. The accessed data can then be organized, categorized, and analyzed to review pertinent areas for research and investment. For the purposes of this study, data were analyzed to determine if information security policies, breaches, violations, and potential losses can be traced to a lack of focus on system usage and possibly a casual observance of necessary protocols.

Walden University maintains an Institutional Review Board approval process for proposed research initiatives throughout each college. IRB application associated with this conducted study was submitted via the establish process and approved with the following IRB number of 0473803.

The NASDAQ Stock Market website provided a wealth of data to organize and analyze for the research study. The goal was to locate and isolate data pertinent to the framed research questions and established hypotheses. The obtained data were downloaded and organized for review pertinent to the results of the sample size computation using G*Power 3.1.5 statistical software indicated that a minimum sample size of 134 companies were necessary to achieve an acceptable level of significance. The G*Power 3.1.5 statistical software was utilized with a medium effect size of .3 and an alpha of .05. Utilizing the provided values, a sample size was calculated at 134 publicly traded firms listed on the NASDAQ. Once the needed firms were obtained and organized, ratios were established. For the ratios, I organized the data to sort the top one-third and top 10%, which were labeled as *very high reliance* and *high reliance* to assist with the overall dataset analysis. The segmented ratios framed the range of data from 2010 to 2016 for all the targeted NASDAQ firms with a direct focus on the established variables for the remainder of the study.

## Identified Fiscal Years

The identified fiscal years for the conducted study had a date range from 2010 to 2016. The identified fiscal years were selected due to a 25% increase in information systems security breaches during this time period and for the opportunity to review established data via the NASDAQ Stock Market site (Davis & Cates, 2013; Ghanbari & Bakhtjoo, 2011). Leveraging a motivation to serve the larger business community assist with a social science service to fellow professionals and organizations. The goal then is to utilize the findings as a mechanism to share lessons learned and best practices with the larger research and professional communities.

Organizational stakeholders are becoming increasingly reliant on information systems and developing an increased comfort with utilizing tools in the workplace (Broadfoot, 2001; Pham, 2010; Siha & Monroe, 2006). An increased comfort and familiarity with technology may be leading to more breaches within the business community. The developed and conducted study looked to analyze breaches via required reporting steps of publicly traded companies on the NASDAQ Stock Market with earnings prior to occurrences and results after noted events. The findings proved to be quite useful with organizing recommendations and providing additional insights.

Looking at the history of information systems within the workplace proves to be a useful backdrop as to how company stakeholders became so reliant on technology tools, applications, and resources. The growth of the marketplace was attributed to an increase in technology utilization, increasing company profits, and positive consumer sentiment. Belle, Burley, and Long (2015) framed the role of information technology and systems utilization as a powerful force throughout the business environment, especially within the United States. The need to integrate IT and systems development has provided the means to improve product development, service to consumers, and the integration of continued innovation. Naser (2015) posited that at the heart of a greater utilization of systems integration was the growing concern of information systems security procedures.

Researchers have begun to champion the need for information systems security considerations in all business environments (Schnijdirberg, 2011). Initial research has centered on technical components and steps to secure computers and networks. These steps have bene important gauges of progress and as a foundation to dig deeper into a review of systems security. Pirdavani, Bellemans, Brijs, Kochan, and Wets (2014) suggested that additional research steps were also needed to support the impact of security vulnerabilities and attacks on organizational performance. The importance of company performance for publicly traded firms was deemed an appropriate next step.

An important step during the examination of information systems security was to ascertain the path of empirical research and reviews. Aryanezhad, Badri, and Rashidi

Komijan (2010) highlighted the detailed research available on network and computer systems pertinent to technical advancements and system updates. The technical advancements pertinent to security initiatives seemed to follow the same path as the growth in system vulnerabilities and attacks. An important consideration of how business leaders report and thwart security breaches surfaced as a need for future research.

A seamless operating environment where projects can be completed on time and with the planned resources was vital to business success. Shekarhizadeh, Ghasemi, Tadi, Soltani, and Nili (2015) argued that project sustainability was a cornerstone for successful business initiatives. In this regard, sustainable and productive business initiatives often had many moving components reliant on partnering activities. The multiple intricacies and complexities of modern day projects can be evidenced via the numerous supply-chain partnerships throughout industries and across the marketplace. To maintain sustainable projects and business performance, secure systems need to be championed and maintained.

The importance of information sharing was also ascertained as a key component of organizational success and sustainment. Lending, Minnick, and Schorno (2018) discussed the need to maintain a consistent flow of data and information for effective decision making. In regard to proper data management and storage, security was of paramount importance. Secure and reliable data were attributed to the highest levels of quality-based information. The opportunity to leverage information that was accurate and reliable led to the most productive project deliverables (Naser, 2015). An important question raised was the heightened need for thorough training programs to keep stakeholders prepared to monitor and leverage rich deposits of data mining.

Monitoring and managing a rich data environment was seen as a needed step to the progression of effective information sharing. Shekarhizadeh, Ghasemi, Tadi, Soltani, and Nili (2015) posited that secure data repositories would lead to more enhanced information sharing and decision making. The need to provide effective training programs continued to surface as a paramount component of productive business development and growth. During the review of information sharing and management articles, the theme of targeted decision making surfaced repeatedly as a need for organizational success (Belle, Burley, & Long, 2015). An example of effective information sharing was framed as an ability to share timely information to decision makers and customer support during all collaborations and planning steps. An additional example of effective corporate information sharing surfaced via the need for timely and thorough announcements for stakeholder reviews as required via SEC guidelines. Maintaining a clear announcement protocol for organizational stakeholders would directly support internal processes of clear policy development, information sharing, and the confirmed requirement of a secure operating environment for all organizational activities.

## Variable Naming Conventions

To assist with data review, organization, and dissemination, I was able to organize pertinent and traditional naming conventions for key data attributes during the organization and analyzation steps. Table 1 frames utilized naming conventions for variables incorporated during the identified review period for the selected NASDAQ companies.

Table 1
*Variable Naming Conventions*

| Naming convention | In-text reference |
|---|---|
| CRT | The NASDAQ credentialing identification is unique to each company publicly traded within the financial exchange system. |
| AST | The assets of the selected publicly-traded companies listed on the NASDAQ Stock Market. |
| NNI | The NNI represents the total or complete revenues stemming from non-interest income, activities requiring fiduciary oversight, charges for services, account costs, and other potential incomes that can stem from recognized profits and losses. |
| ISRCHG | Company losses that can be attributed to non-security breaches; such as, losses stemming from mergers and acquisitions. |
| NTINC | The total income stemming from net revenue activities, which would minus taxes, credits, and grant funding resources. |
| HReliance | Refers to publicly-traded companies on the NASDAQ Stock Market that have an above average reliance on technology resources and a heightened exposure to financial risk. |
| VHReliance | Refers to publicly-traded companies on the NASDAQ Stock Market that have an extreme reliance on technology resources and a heightened exposure to financial risk. |

The ability to utilize naming convention for variables assists with making the data organization, review, analysis, and recommendation steps much more straightforward for the researcher and for managers or stakeholders who may benefit from a review of the findings.

## Company Statistics Related to Research Questions 1 and 2

During 2010 and 2016, there is a notable increase in information security breaches and notices submitted for publicly-traded companies operating on the NASDAQ Stock Market.  The United States economy was also recovery from a great recession, so managers and business leaders were looking for every advantage possible to improve business operations. As of 2010, there were 1,753 fewer companies operating in the United States as compared to previous fiscal years (Putnam, Myers, & Gailliard, 2013; Pyöriä, 2011). In this regard, reviewing the data of 1,753, it is evident that 32% (560) of the reduction was a result of company closures, and the remaining 68% (1,193) stemmed from acquisitions and mergers.

From 2010 to 2016 there were 1,042 new companies entering the publicly traded environment within the United States. Historically, the number of companies entering the marketplace would be much more sizable; however, the recession and external pressures may have added to the slow increase in new organizations. Looking at the flow of new entrants to the marketplace and at closures is important to establish a baseline for comparison when evaluating the impacts of information security breaches on publicly traded companies on the NASDAQ. The goal, as much as possible, is to isolate financial losses and business activities and decisions to the targeted activities and variables stemming from information systems security breaches.

From 2010 to 2016, the number of publicly traded companies in the United States declined by 19.82%. Reviewing this occurrence, it is clear that even though the number of public companies declined, the amount of total revenues in the marketplace increased from $7.14 trillion to $10.82 trillion (Aboelmaged & Elamin, 2011). It is evident that the great recession had an impact on new business creation; however, the management of security breaches also served as a major driver in how funds were utilized and possibly why certain organizations thrived and grew, while other firms lost revenues or ended business operations.

## Research Question 1 and 2 Findings

The gathered data and analysis provided the ability to reject the null hypotheses and support the assertion that a robust information systems security policy and ample training assisted with reducing security breaches and revenue losses. It is evident that proactive business leaders can have a positive impact on a company by establishing an information systems security policy that provides the parameters for internet usage, personal devices, mobile devices, hotspots, access points, sharing data, information sharing, and the importance of training. The Research Question 1 and 2 findings are noted below via each pertinent section.

### Research Question 1

The Research Question 1 was developed as follows: What is the relationship between the level of information systems security policy and the number of security breaches? The subsequent hypotheses were then:

$H1_0$: There is a not a statistically significant correlation between the independent variable of level of information systems security policy and the dependent variable of the number of security breaches.

$H1_a$: There is a statistically significant correlation between the independent variable of the level of information systems security policy and the dependent variable of the number of security breaches.

Appendix A demonstrated a normal distribution of data via the normal probability plot. Appendix B then highlighted a conducted Pearson Correlation for Research Question 1. The calculation revealed a significant correlation between information systems security policy and the number of breaches via a score above +/- .7, calculated as -.857.

### Research Question 2

The Research Question 2 was developed as follows: What is the relationship between the level of information systems security policy and the self-reported loss in corporate earnings associated with the security breach as a percentage of revenue? The subsequent hypotheses were then:

$H2_0$: There is a not a statistically significant correlation between the independent variable of the level of information systems security policy and the dependent variable of the self-reported loss in corporate earnings associated with the security breach as a percentage of revenue.

$H2_a$: There is a statistically significant correlation between the independent variable of the level of information systems security policy and the dependent variable of the self-reported loss in corporate earnings associated with the security breach as a percentage of revenue.

Appendix A demonstrated a normal distribution of data via the normal probability plot. Appendix B then highlighted a conducted Pearson Correlation for Research Question 2. The calculation revealed a significant correlation between information systems security policy and a loss in corporate earnings due to security breaches via a score above +/- .7, calculated as -.764.

## Summary and Conclusions

The research plan for the identified project was to ascertain the connection of system vulnerabilities and attacks with constraints for public firms listed on the NASDAQ exchange. The project was developed with a focus on constraint identification and management for business leaders working in publicly traded companies. The identified data and information were quantitative and incorporated via a correlational analysis of the connections with degree of security utilized, social considerations, availability of technical assistance, and satisfaction of the working environment.

The over utilization of technical system integrations, subsequent vulnerabilities, and attacks have had a negative impact on stakeholder morale and public company performance for many years (Fonner & Stache, 2012; Offstein, Morwick, & Koskinen, 2010). An important challenge that stems from system vulnerabilities, attacks, and inadequate training was confirmed to tie directly to a reduced interest in system integration, new product development, and a lack of recommendations for creative business solutions. In regard to effective system preparations and training, Watad and Will (2003) posited system vulnerabilities and attacks promote negative consequences for all stakeholders within an organization. Yahaya, Basir, and Deraman (2015) framed the withdrawing of personnel from the utilization of existing and new systems as a direct result of information systems security breaches. The withdrawing of personnel was seen as a major event, because disengaged employees can continue a cycle of low productivity, poor performance, and losses in company earnings.

Chapter 4 provided the data, information, and calculations needed to reject the null hypotheses for Research Question 1 and Research Question 2. The research initiative was conducted to address the identified hypotheses; research questions; sample size and population; data collection and instrumentation; procedures for data analysis; and via a consistent focus on ethical practices. The identified descriptions were clearly evident via the examination of degree of systems vulnerabilities, attacks, policy development, corporate earnings, and training initiatives. The presented chapter demonstrated the value of utilized framework for research that incorporated a correlational framework to examine the hypotheses and to provide a research-based response to the posed questions.

# Chapter 5: Summary, Conclusion, and Recommendations

## Introduction

The importance for leaders within an organizational environment to remain steadfast and focused on ISS was a valuable takeaway from the research study. Establishing a culture that championed ISS concepts and best practices as a key first step. Information systems training, technology integration, and clear communications with all company stakeholders were additional important points to note. The study revealed that effective supervisors and managers integrated a continuous focus on the prevention of vulnerable touch points to corporate information; the value of the continuity of business processes; the reduction of security-based shortfalls and occurrences; and the opportunity for integrity, maintenance, and confidentiality of business data and assets pertinent to obtained information (Hill & Fellows, 2014). Security systems were comprised of a balance between technical and social factors, ranging from the solely technical to the focus being dominantly social and behavioral (Ahmad, Bosua, & Scheepers, 2014). The significance of systems security in an organizational environment is paramount, as nearly all forms of data are compiled and procured electronically (Martin & MacDonnell, 2012). In 2015, Naser posited that 91% of participants voiced concern over employees as a potential flaw in security systems and 79% of participants considered human error to be the underlying source of the systems failure. A lingering obstacle was to ascertain the prominent circumstances that can benefit with diminishing organizational security vulnerabilities and attacks.

## Interpretation of Findings

The research project provided the ability to reject the null hypotheses and support the importance of a robust information systems security policy and ample training throughout companies.  The utilization of an information systems security policy and training opportunities for personnel assisted with reducing security breaches and revenue losses (Rabiee, Taghi-Amini, & Pirayesh, 2014).  It is evident that proactive business leaders can have a positive impact on a company by establishing an information systems security policy that provides the parameters for internet usage, personal devices, mobile devices, hotspots, access points, sharing data, information sharing, and the importance of training.  An important takeaway is the value involved with engaging all stakeholders during planning and development of information systems security policies.

## Limitations of the Study

The limitations of the research study are tied to the method, design, and to additional considerations for future studies.  In regard to the research method selected, a quantitative study was incorporated with a data analysis design via a Pearson's Correlation to ascertain the connection with the dependent and independent variables. Examination of the connections and predictions served as the measurement to determine guidance for public firms, notices pertaining to systems security, corporate revenues, and market-based recommendations that highlighted best practices for training programs and oversight.  Utilizing a robust quantitative method and design assisted with having confidence to reject the null hypotheses in support of the alternate hypotheses.  An overall limitation tied to the quantitative study can be evidenced via a focused examination of the literature and analyzed data. In the research study, qualitative methods were not utilized; however, the inclusion of these techniques may be included in future studies and could provide additional depth of analysis via interviews and observations. Recommendations for future studies provides additional support for qualitative considerations with the potential of planned follow-on studies.

## Recommendations for Future Studies

Recommendations for future studies includes the potential value of a qualitative research method and applicable designs to obtain an additional depth of information. For example, incorporating a qualitative research method, one could spend additional time conducting interviews and making pertinent observations. Conducting interviews could assist with garnering additional insight to examine marketplace stimuli that may be influencing information systems security breaches and the importance of robust organizational training programs. Interviews could also assist with achieving saturation and increasing stakeholder collaborations. Observations could potential assist with grounded theories and research-based emersion techniques.

## Implications for Positive Social Change

The implications for positive social change are evident via the collected and analyzed data. The data revealed that corporate information systems security policies can have a very positive impact on stakeholder understanding and performance. In regard to stakeholder understanding and performance, a robust information systems security policy and training environment can assist company stakeholders with ascertaining security best practices and considerations pertinent to data usage, sharing, storage, access points, personal devices, mobile technologies, and password or biometric login device protections. Employing sound information systems security practices can assist with keeping organizational stakeholders safe, reducing unexpected corporate financial losses due to breaches, and improve the overall business operating environment throughout the global marketplace.

## Conclusion

The goal of the correlational research study was to ascertain the association and connections with public companies, notices pertinent to breaches of security, and reported earnings. A persistence of system vulnerabilities in organizations had a significant impact on the price of stocks and annual revenues for public firms partnered with the NASDAQ exchange. Derived data were reviewed via the Pearson Correlation to examine the relationship with the identified independent and dependent variables. A review of the predictions and connections was used as the lens to ascertain relationships and to garner specific guidance for public company operations, policy notifications, annual revenues, and best practices pertinent to information systems security operations. The dependent variable was corporate performance and revenues as denoted by annual and quarterly reports. The independent variables were degree of secure systems and the availability of technical assistance. The population for the research initiative stemmed from a calculated sample of public companies partnered with the NASDAQ exchange. The research activity can serve as a lens for social change by providing recommendations to assist business leaders with maintaining a safe operating environment for all organizational stakeholders.

The intent of research steps and analytics were initiated to frame the research method, design, and subsequent steps.  A detailed focus of the research method, design, participant data, sampling techniques, information gathering, hypotheses, analysis of data, ethical concepts, limitations, and validity were examined.  The study was developed to provide a detailed analysis of the research questions, hypotheses, and subsequent research findings pertinent to the project.  The culmination of the research project surfaced via the detailed reviews, where social change considerations, implications, recommendations, and a discussion on garnered information systems security best practices will be provided for business leaders within publicly traded firms operating in the US and listed on the NASDAQ exchange.

## References

Aboelmaged, M. G., & El Subbaugh, S. M. (2012). Factors influencing perceived productivity of Egyptian security workers: An empirical study. *Measuring Business Excellence, 16*(2), 3-22. doi:10.1108/13683041211230285

Aboelmaged, M. G., & Elamin, A. M. (2011). Security in United Arab Emirates (UAE): An empirical study of influencing factors, facilitators, and inhibitors. *Operations Management: A Modern Approach*, pp. 183-212. doi:10.1201/b12879-11

Ahmad, A., Bosua, R., & Scheepers, R. (2014). Protecting organizational competitive advantage: A knowledge leakage perspective. *Computers & Security*, *42*, 27-39. doi:10.1016/j.cose.2014.01.001

Akey, P., Lewellen, S., & Liskovich, I. (2018). Hacking corporate reputations. *Rotman School of Management*, No. 3143740, 1-37. Retrieved from http://www.rotman.utoronto.ca

Albiero, R., Verive, J., Cooper, C., & Knott, S. (2010). The secret to making security work: Moving beyond planning as the next logical step. *TDM Review*, *17*(2), 1-34. Retrieved from https://www.actweb.org

Al-Haderi, S. (2013). The effect of self-efficacy in the acceptance of information technology in the public sector. *International Journal of Business and Social Science*, *4*(9), 188-198. Retrieved from http://www.ijbssnet.com/

Alizadeh, T. (2012). Security user characteristics in live/work communities: Lessons from the United States and Australia. *Journal of Urban Technology*, *19*(3), 63-84. doi:10.1080/10630732.2011.642569

Almeida, C. F., Penaforte, M. F., & Yamashita, Y. (2013). Using the theory of constraints to analyze bottlenecks in the freight transportation system: The case of the center-north corridor in Brazil. *Transportation Research Board 92nd Annual Meeting*, (No. 13-0562).

Anderson, A. J., Kaplan, S. A., & Vega, R. P. (2014). The impact of security on emotional experience: When, and for whom, does security improve daily affective well-being? *European Journal of Work and Organizational Psychology*, 1-16. doi:10.1080/1359432x.2014.966086

Antoniou, A.S., & Cooper, C.L. (2013). *The psychology of recession in the workplace.*, Cheltenham, UK and Northampton, MA, USA: Edward Elgar Publishing.

Aryanezhad, M. B., Badri, S. A., & Rashidi Komijan, A. (2010). Threshold-based method for elevating the system's constraint under theory of constraints. *International Journal of Production Research*, *48*(17), 5075-5087. doi:10.1080/00207540903059505

Asgari,H., Jin, X., & Mohseni, A. (2014). Choice, frequency, and engagement: A framework for telecommuting behavior analysis and modeling. *Transportation Research Board Record: Journal of the Transportation Research Board, 2413*(2), 101-109. doi:10.3141/2413-11

Azarbuyeh, A., & Naini, S. (2014). A study on the effect of security on quality of work life. *Management Science Letters*, *4*(6), 1063-1068. doi:10.5267/j.msl.2014.5.027

Baard, N., & Thomas, A. (2010). Security practices in South Africa: Employee benefits and challenges: Original research. *SA Journal of Human Resource Management,* *8*(1), 1-10. doi:10.4102/sajhrm.v8i1.298

Babbie, E., Wagner III, W. E., & Zaino, J. (2015). *Adventures in social research: Data analysis using IBM SPSS Statistics.* Sage Publications.

Bailey, D.E. & Kurland, N.B (2002). A review of security research: Findings, new directions, and lessons for the study of modern work. *Journal of Organizational Behavior, 23,* 383-400. doi:10.1002/job.144

Barron, J. (2007). Making the virtual leap: Ten issues to consider about telecommuting. *Industrial and commercial training, 39*(7), 396-399. doi:10.1108/00197850710829111

Baruch, Y. (2001). Security benefits and pitfalls as perceived by professionals and managers. *New Technology, Work and Employment, 15*(1), 34-50. doi:10.1111/1468-005x.00063

Beham, B., Baierl, A., & Poelmans, S. (2014). Managerial security allowance decisions–a vignette study among German managers. *The International Journal of Human Resource Management,* (ahead-of-print), 1-22. doi:10.1080/09585192.2014.934894

Bélaner, F., Watson-Manheim, M. B., & Swan, B. R. (2013). A multi-level socio-technical systems telecommuting framework. *Behaviour & Information Technology, 32*(12), 1257-1279. doi:10.1080/0144929x.2012.705894

Belle, M., Burley, D. L., & Long, S. D. (2015). Where do I belong? High-intensity securityers' experience of organizational belonging. Human Resource Development International, 18(1), 76-96.

Belzuegui, Á., Erro, A., & Pastor, I. (2014). The security as an organizational innovation in the entities of the third sector. *Journal of Electronic Commerce in Organizations (JECO)*, *12*(1), 1-15. doi:10.4018/jeco.2014010101

Bernardino, A. F., Roglio, K. D. D., & Del Corso, J. M. (2012). Telecommuting and HRM: A case study of an information technology service provider. *Journal of Information Systems and Technology Management: JISTEM*, 9(2), 285-306. doi:10.4301/s1807-17752012000200005

Bosua, R., Gloet, M., Kurnia, S., Mendoza, A., & Yong, J. (2013). Security, productivity and wellbeing: An Australian perspective. *Telecommunications Journal of Australia, 63*(1), 1-12. doi:10.7790/tja.v63i1.390

Bratton, D. (2013). Federal employee motivation during government downsizing: A literature review. *Australian Journal of Business and Management Research, 3*(1), 1-7. Retrieved from http://www.ajbmr.com/articlepdf/aus-29-54i01n3a1.pdf

Broadfoot, K. J. (2001). When the cat is away, do the mice play: Control/autonomy in the virtual workplace. *Management Communication Quarterly*, *15*(1), 110–114. doi:10.1177/0893318901151006

Burbah, M. E., & Day, F. C. (2012). Does organization sector matter in leading security teams? A comparative case study. *International Journal of Business Information and Technology (IJBIT), 1*(1). Retrieved from https://www.sciencetarget.com/Journal/index.php/IJBIT

Burke, R.J., & Cooper, C.L. (2008). *The long work hour culture: Causes, consequences and choices,* Bingley, UK: Emerald Publishing.

Caillier, J. G. (2011). Are technology managers less likely to report leave intentions in the United States federal government? *The American Review of Public Administration*, *43*(1), 72-88. doi:10.1177/0275074011425084

Caillier, J. G. (2011). The impact of security on work motivation in a US federal government agency. *The American Review of Public Administration*, *4*(3), 10-15. doi:10.275074011409394

Caillier, J. G. (2014). Do role clarity and job satisfaction mediate the relationship between security and work effort? *International Journal of Public Administration, 37*(4), 193-201. doi:10.1080/01900692.2013.798813

Cha, J., & Cha, J. S. (2014). The common challenges to the successful implementation of smart work program. *International Journal of Multimedia & Ubiquitous Engineering*, *9*(2). doi:10.14257/ijmue.2014.9.2.12

Chukudi, C. G., & Daddie, J. A. (2015). An examination of the strategic contributions of telecommuting on organizational performance. *International Journal of Research, 2*(2), 1476-1486. Retrieved from http://internationaljournalofresearch.com/

Cocco, M., & Tuzzi, A. (2013). New data collection modes for surveys: a comparative analysis of the influence of survey mode on question-wording effects. *Qual Quant. 47*(6), 3135–3152. doi:10.1007/s11135-012-9708-1

Coene, M., & Kok, R. A. (2014). Workplace flexibility and new product development performance: The role of security and flexible work schedules. *European Management Journal, 32*(4), 564-576. doi:10.1016/j.emj.2013.12.003

CorrêaH. L. (2013). Changes in the role of production and operations management in the new economy. *Journal of Operations and Supply Chain Management, 1*(1), 1-11. Retrieved from http://bibliotecadigital.fgv.br/ojs/index.php/joscm

Corwin, S., & Harris, J. (2001). The initial listing decisions of firms that go public. *Financial Management, 30*(1), 35-55. Retrieved from http://www.jstor.org

Crandall, W. & Gao, L. (2005). An update on telecommuting: Review and prospects for emerging issues. *S.A.M. Advanced Management Journal, 70*(3), 30-37. Retrieved from http://thefreelibrary.com/An+update+on+telecommuting%3a+review+and+prospects+for+emerging+issues.-a0128011934

Dahlstrom, T. R. (2013). Telecommuting and leadership style. *Public Personnel Management, 42*(3), 438-451. doi:10.1177/0091026013495731.

Dailey, D. (2010). Information technology consultation service assists companies in the Denver metro area. *TDM Review, 17*(2). pp 30-31. Retrieved from https://www.actweb.org/eweb/startpage.aspx

Dal Fiore, F., Mokhtarian, P. L., Salomon, I., & Singer, M. E. (2014). “Nomads at last”? A set of perspectives on how mobile technology may affect travel. *Journal of Transport Geography, 41*, 97-106. doi:10.1016/j.jtrangeo.2014.08.014

Davis, R., & Cates, S. (2013). The dark side of working in a virtual world: An investigation of the relationship between workplace isolation and engagement among securityers. *Journal of Human Resource and Sustainability Studies, 1*, 9. doi: 10.4236/jhrss.2012.12002

Dehabi, H. A., Shokri, S. T., Ganbarvand, H., & Sohrabi, A. (2014). How employers decide to accept and implement security best practices? (A survey in Iranian Organizations). *International Journal of Research in Organizational Behaviour and Human Resource Management*, *2*(1), 157. Retrieved from http://www.indianjournals.com/ijor.aspx?target=ijor:ijrobhrm&type=home

Demers, C. (2007). *Organizational change theories: A synthesis.* Thousand Oaks, CA: Sage.

Diana, A. (2010, September 30). Executives demand communications arsenal. *InformationWeek: Technology for Small and Midsize Business*, Retrieved from http://www.networkcomputing.com/networking/executives-demand-communications-arsenal/d/d-id/1092914?

Dimitrova, D. (2003). Controlling security expectations: supervision and flexibility revisited. *New Technology, Work and Employment*, *18*, 181–195. doi:10.1111/1468-005X.00120

Dockery, A. M., & Bawa, S. (2014). Is working from home good work or bad work? Evidence from Australian employees. Australian Journal of Labour Economics, 17(2), 163.

Domiinique, V., & Der, M. (2010). *Modeling the choice of security frequency and its effects on productivity and work/life balance*. (Master dissertation). Erasmus University, Rotterdam, Netherlands

Duxbury, L., & Halinski, M. (2014). When more is less: An examination of the relationship between hours in security and role overload. *Work: A Journal of Prevention, Assessment and Rehabilitation*, *49*(1), 91-103. doi:10.3233/WOR-

141858

Edwards, W. K., Grinter, R. E., Mahajan, R., & Wetherall, D. (2011). Advancing the state of home networking. *Communications of the ACM, 54*(6), 62-71. doi:10.1145/1953122.1953143

Ellison, J. K. (2013). Ergonomics for telecommuters & other remote workers. Retrieved from http://www.asse.org/assets/1/7/Ergo-PS-Webinar-Telecommuting-Ergonomics.pdf

Ellison, N. B. (2004). *Security and social change: How technologies reshaping the boundaries between home and work*. New York, NY: Greenwood Publishing Group.

Fay, M. J., & Kline, S. L. (2012). The influence of informal communication on organizational identification and commitment in the context of high-intensity telecommuting. *Southern Communication Journal*, *77*(1), 61-76. doi:10.1080/1041794x.2011.582921

Fink, A. (2005). *Conducting research literature reviews: From the Internet to paper* (2nd ed.). Thousand Oaks, CA: Sage.

Finna,H., & Forgacs, T. (2010). Enhancement of human performance with developing ergonomic workplace environment and providing work-life balance. *Perspectives of Innovations, Economics and Business, PIEB*, (2 (5), 59-61. doi:10.15208/pieb.2010.50

Fitnes, J. (2008). Fear and loathing in the workplace. *Research Companion to Emotion in Organizations*, pp. 656. doi:10.4337/9781848443778.00012

Fonne, K. L., & Roloff, M. E. (2012). Testing the connectivity paradox: Linking communication media use to social presence, stress from interruptions, and organizational identification. *Communication Monographs*, *79*(2), 205-231. doi:10.1080/03637751.2012.673000

Fonner, K. L., & Stache, L. C. (2012). All in a day's work, at home: Management of micro role transitions and the work–home boundary. *New Technology, Work and Employment*, *27*(3), 242-257. doi:10.1111/j.1468-005x.2012.00290.x

Forgacs, T. (2010). Empirical research findings on security: Management experiences and attitudes. *Business and Economic Horizons*, (1), 6-13. doi:10.15208/beh.2010.02

Frankfort-Nachmias, C., & Nachmias, D. (2008). *Research methods in the social sciences* (7th ed.). New York: Worth

Freeman, I., & Hasnaoui, A. (2011). The meaning of corporate social responsibility: The vision of four nations. *Journal of Business Ethics, 100*(3), 419-443. doi:10.1007/s10551-010-0688-6

Gajendran, R. S. & Harrison, D. A. (2007). The good, the bad, and the unknown about security: Meta-analysis of psychological mediators and individual consequences. *Journal of Applied Psychology, 92*, 1524–1541 doi:10.1037/0021-9010.92.6.1524

Galve, A. Martinez, M. & Perez, C. (2012). Security and work-life balance: Some dimensions for organizational change. *Journal of Workplace Rights, 16*(3), 273-297. doi:10.2190/wr.16.3-4.b

Georg, G., McGahan, A. M., & Prabhu, J. (2012). Innovation for inclusive growth:

Towards a theoretical framework and a research agenda. *Journal of Management Studies, 49*(4), 661-683. doi:10.1111/j.1467-6486.2012.01048.x

Geri, N., & Ahituv, N. (2008). A theory of constraints approach to inter-organizational systems implementation. *Information System E-Business Management*, *6,* 341-360. doi:10.1007/s10257-007-0075-8

Ghanbari. A, Bakhtjoo.SH. (2011). *Security planning (foundations, principles and methods, including the administration of security projects)* (1st ed.). Tehran, Iran: Frazma.

Gibbs, J. L., Scott, C. R., Kim, Y. H., & Lee, S. K. (2010). Examining tensions in security policies. *Communication, relationships, and practices in virtual work*, pp. 1-25. doi:10.4018/978-1-61520-979-8.ch001

Glenn, D. E. (2012). The effects of telecommuting on productivity: An experimental examination. The role of dull and creative tasks. *Journal of Economic Behavior & Organization*, *84*(1), 355-363. doi:10.1016/j.jebo.2012.04.009

Golde, T. (2007). Co-workers who security and the impact on those in the office: Understanding the implications of virtual work for co-worker satisfaction and turnover intentions. *Human Relations*, *60*(11), 1641-1667. doi:10.1177/0018726707084303

Golden, T. (2007). Co-workers who security and the impact on those in the office: Understanding the implications of virtual work for co-worker satisfaction and turnover intentions. *Human Relations*, *60*(11), 1641-1667. doi:10.1177/0018726707084303

Golde, T. D. (2005). The impact of extent of telecommuting on job satisfaction: Resolving inconsistent findings. *Journal of Management*, *31*(2), 301-318. doi:10.1177/0149206304271768

Golden, T. D., & Fromen, A. (2011). Does it matter where your manager works? Comparing managerial work mode (traditional, security, virtual) across subordinate work experiences and outcomes. *Human Relations*, *64*(11), 1451-1475. doi:10.1177/0018726711418387

Golden, T. D., & Watt, A. (2013). Toward a deeper understanding of the willingness to seek help: The case of security implementation. *Work: A Journal of Prevention, Assessment and Rehabilitation*, *48* (1), 83-90. doi:10.3233/WOR-131818

Golden, T. D., Veiga, J. F., & Dino, R. N. (2008). The impact of professional isolation on job performance and turnover intentions: Does time spent with technology, interacting face-to-face, or having access to communication-enhancing technology matter? *Journal of Applied Psychology*, *93*(6), 1412. doi:10.1037/a0012722

Golden, T.D., Veiga, J.F., & Simsek, Z. (2006). Security violations in the office and the differential impact on organizational conflict: Is there no place like home? *Journal of Applied Psychology, 91*(6), 1340–1350. doi:10.1037/0021-9010.91.6.1340

Goodan, J.S. & Wood, R.E. (2004). Feedback specificity, learning opportunities, and learning. *Journal of Applied Psychology, 89*(5), 809-821. doi:10.1037/0021-9010.89.5.809

Grant, C. A., Wallace, L. M., & Spurgeon, P. C. (2013). An exploration of the psychological factors affecting remote e-worker's job effectiveness, well-being and work-life balance. *Employee Relations*, *35*(5), 527-546. doi: 10.1108/er-08-2012-0059

Greenhaus, J. H., & Kossek, E. E. (2014). The contemporary career: A work–home perspective. *Annual Review of. Organizational Psychology. 1*(1), 361-388. doi:10.1146/annurev-orgpsych-031413-091324

Greer, T. W., & Payne, S. C. (2014). Overcoming security challenges: Outcomes of successful security strategies. *The Psychologist-Manager Journal*, *17*(2), 87. doi:10.1037/mgr0000014

Gregg, M. (2011). *The intimacies of the work environment*. Cambridge: Polity Press.

Guimaraes, T. & Dallow, P. (1999). Empirically testing the benefits, problems, and success factors for security programs. *European Journal of Information Systems, 8*, 40–53. Retrieved from http://www.palgrave-journals.com/ejis/index.html

Gupta, A., Bhardwaj, A., & Kanda, A. (2010). Fundamental concepts of theory of constraints: An emerging philosophy. *International Science Index, 4*(10), 595-601. Retrieved from waset.org/Publication/83

Gupta, M. C., Sahi, G. K., & Chahal, H. (2013). Improving market orientation: the theory of constraints-based framework. *Journal of Strategic Marketing*, *21*(4), 305-322. doi:10.1080/0965254x.2013.790467

Haddo, L., & Brynin, M. (2005). The value of security and the characteristics of security workers. *New Technology, Work and Employment*, *20*(1), 34-46.

doi:10.1111/j.1468-005x.2005.00142.x

Halford, S. (2005). Hybrid workspace: Re-specialization of work, organization, and management. *New Technology, Work and Employment, 20*, 19-33. doi:10.1111/j.1468-005x.2005.00141.x

Hall, D. T., Kossek, E. E., Briscoe, J. P., Pichler, S., & Lee, M. D. (2013). Network orientations relative to career: A multidimensional measure. *Journal of Vocational Behavior*, *83*(3), 539-550. doi:10.1016/j.jvb.2013.07.005

Harandi, A. A. H. (2012). Investigation of the requirement and constraints affecting security in government institutes; case study: Research institutes of ministry of roads and urban development. *International Journal of Information Security, 1*(2), 96-103. Retrieved from http://www.ijnngt.org/blog_post.php

Harrington, S. J., & Santiago, J. (2015). Organizational culture and telecommuters' quality of work life and professional isolation. *Communications of the IIMA, 6*(3), 1. Retrieved from http://www.iima.org

Harrington, S. J., & Santiago, J. (2015). Organizational culture and telecommuters' quality of work life and professional isolation. *Communications of the IIMA*, *6*(3), 1. Retrieved from http://www.iima.org

Harris, L. (2003). Home based security and the employment relationship:  Managerial challenges and dilemmas. *Personnel Review*, *32*(4), 422-439. doi:10.1108/00483480310477515

Hilbrecht, M., Shaw, S. M., Johnson, L. C., & Andrey, J. (2013). Remixing work, family and leisure: Technology worker experiences of everyday life. *New Technology,* *Work, And Employment, 28*(2) 130-144. doi:10.1111/ntwe.12010

Hill, E. J., & Fellows, K. J. (2014). Telecommuting. *Encyclopedia of Quality of Life and Well-Being Research,* 6599-6600. doi:10.1007/978-94-007-0753-5_2985

Ho, A. D. & Carol, C. Y. (2015). Descriptive statistics for modern test score distributions skewness, kurtosis, discreteness, and ceiling effects. *Educational and Psychological Measurement, 75*(3), 365-388.

Hosseinnezhad, S. (2013). Security in governmental organizations, infrastructures, advantages and disadvantages of security implementations. *Journal of American Science, 9*(5s). Retrieved from http://www.jofamericanscience.org/

Jakobsn, M., & Lueg, R. (2014). Balanced scorecard and controllability at the level of middle managers–The case of unintended breaches. *Journal of Accounting & Organizational Change*, *10*(4), 516-539. doi:10.1108/jaoc-03-2013-0023

James, P., & Griffiths, D. (2014). A secure portable execution environment to support security practices. *Information Management & Computer Security, 22*(3), 309-330. doi:10.1108/IMCS-07-2013-0052

Joice, W. (2007). Implementing security: the technology issue. *Public Manager, 36*(2), 64- 68. Retrieved from http://www.astd.org/Publications/Magazines/The-Public-Manager

Julsru, T. E., & Rolan M. D. G. Z.  (2014). Mobile phones and business networks among Malaysian micro and small enterprises: A comparative network approach. *Asia-Pacific Social Science Review*, *14*(1), 21-42. Retrieved from http://www.dlsu.edu.ph/offices/publishing-house/journals/apssr/publication.asp

Kacmr, K.M., Witt, L.A., Zivnuska, S., & Gully, S.M. (2003). The interactive effect of leader-member exchange and communication frequency on performance ratings. *Journal of Applied Psychology, 88*(4), 764-772. doi:10.1037/0021-9010.88.4.764

Kane, M. T. (2006). Validation. *Educational measurement, 4,* 17–64.

Kane, L. M. (2014). *Security and organizational citizenship behaviors: The underexplored roles of social identity and professional isolation.* (Unpublished doctoral dissertation). City University of New York, Graduate Center, New York, NY.

Kanellopoulos, D. N. (2011). How can securitying be pro-poor? *Journal of Enterprise Information Management*, *24*(1), 8-29. doi:10.1108/17410391111097401

Anderson, A. J., Kaplan, S. A., & Vega, R. P. (2014). The impact of security on emotional experience: When, and for whom, does security improve daily affective well-being? *European Journal of Work and Organizational Psychology*, 1-16. doi:10.1080/1359432x.2014.966086

Kassinis, G. I., & Stavrou, E. T. (2013). Non-standard work arrangements and national context. *European Management Journal, 31*(5), 464-477. doi:10.1016/j.emj.2013.04.005

Khoda-yari, M., & Rahnavard, F. (2013). Study of factors inhibiting establishment of security systems in the public sector. *International Journal of Physical and Social Sciences, 3*(1), 101-113. Retrieved from http://www.ijmra.us/2013ijpss_january.php

Ko, J., & Hur, S. (2014). The impacts of employee benefits, procedural justice, and managerial trustworthiness on work attitudes: Integrated understanding based on social exchange theory. *Public Administration Review, 74*(2), 176-187. doi:10.1111/puar.12160

Ko, J., Hur, S., & Smith-Walter, A. (2013). Family-friendly work practices and job satisfaction and organizational performance moderating effects of managerial support and performance-oriented management. *Public Personnel Management*, *42*(4), 545-565. doi:10.1177/0091026013505503

Kossek, E. E., Hammer, L. B., Kelly, E. L., & Moen, P. (2014). Designing work, family & health organizational change initiatives. *Organizational dynamics*, *43*(1), 53-63. doi:10.1016/j.orgdyn.2013.10.007

Lambert, J. (2013). *Digital storytelling: Capturing lives, creating community*. New York, NY: Routledge.

Lautsc, B. A., & Kossek, E. E. (2011). Managing a blended workforce: Telecommuters and non-telecommuters. *Organizational Dynamics*, *40*(1), 10-17. Retrieved from www.elsevier.com/locate/orgdyn

Lavigne, G. L., Vallerand, R. J., & Crevier-Braud, L. (2011). The fundamental need to belong: On the distinction between growth and deficit-reduction orientations. *Personality and Social Psychology Bulletin, 37*(9), 1185-1201. doi:10.1177/0146167211405995

Leedy, P. D., & Ormrod, J. E. (2010). *Practical research: Planning and design* (9th ed.). Boston, MA: Pearson

Lending, C., Minnick, K., & Schorno, P. (2018). Corporate governance, social responsibility, and data breaches. *The Financial Review, 53*(2), 413-455. doi.org/10.1111/fire.12160

Librelto, T. P., Lacerda, D. P., Rodrigues, L. H., & Veit, D. R. (2014). A process improvement approach based on the value stream mapping and the theory of constraints thinking process. *Business Process Management Journal*, *20*(6). doi:10.1108/bpmj-07-2013-0098

Lim, V. & Teo, T. (2000). To work or not to work at home: An empirical investigation of factors affecting attitudes towards security. *Journal of Managerial Psychology, 15*(6), 560-586. doi:10.1108/02683940010373392

Lin, H. F. (2011). The effects of employee motivation, social interaction, and knowledge management strategy on KM implementation level. *Knowledge Management Research & Practice, 9*(3), 263-275. doi:10.1057/kmrp.2011.21

Linden, M. (2014). Security research and practice: Impacts on people with disabilities. *Work: A Journal of Prevention, Assessment and Rehabilitation*, pp. 1-3. doi:10.3233/WOR-141857

Lister, K., & Harnish, T. (2011). The State of Security in the US. *Security Research Network*. Retrieved from http://www.workshifting.com/downloads/downloads/Security-Trends-US.pdf

Lo, S. H., van Breukelen, G. J., Peters, G. J. Y., & Kok, G. (2013). Pro-environmental travel behavior among office workers: A qualitative study of individual and organizational determinants. *Transportation Research Part A: Policy and Practice, 56*, 11-22. doi:10.1016/j.tra.2013.09.002

Major, D. A., Verive, J. M., & Joice, W. (2008). Security as a dependent care solution: Examining current practice to improve security management strategies. *The Psychologist-Manager Journal*, *11*(1), 65-91. doi:10.1080/10887150801967134

Mamaghani, F. (2012). Impact of telecommuting on organization productivity. *European Journal of Management*, *12*(3). Retrieved from http://www.journals.elsevier.com/european-management-journal/

Mann, S., & Holdsworth, L. (2003). The psychological impact of security practices: Stress, emotions and health. *New Technology, Work and Employment, 18*(3), 196-211. doi:10.1111/1468-005x.00121

Martin, B. H., & MacDonnell, R., (2012). Is security effective for organizations? A meta-analysis of empirical research on perceptions of security and organizational outcomes. *Management Research Review*, *35*(7), 602 – 616. doi:10.1108/01409171211238820

Maruyama, T., & Tietze, S. (2012). From anxiety to assurance: Concerns and outcomes of security. *Personnel Review*, *41*(4), 450-469. doi:10.1108/00483481211229375

Margo, M. J., Prybutok, V. R., & Ryan, S. D. (2014). How survey administration can affect response in electronic surveys. *Quality & Quantity, 3*(4)1-10. doi:10.1007/s11135-014-0098-4

Mateyka, P. J., Rapino, M., & Landivar, L. C. (2012). *Home-Based Workers in the United States: 2010*. US Department of Commerce, Economics and Statistics Administration, US Census Bureau.

Mitchell, J. I., Gagné, M., Beaudry, A., & Dyer, L. (2012). The role of perceived organizational support, distributive justice and motivation in reactions to new information technology. *Computers in Human Behavior*, *28*(2), 729-738. doi:10.1016/j.chb.2011.11.021

Montero-Marín, J., Carrasco, J.M., Roca, M., Serrano-Blanco, A., Gili, M., Mayoral, F., Luciano, J. V., Lopez-del-Hoyo, Y., Olivan, B., Collazo, F., Araya, R., Banos, R., & Botella, C. (2013). Expectations, experiences and attitudes of patients and primary care health professionals regarding online psychotherapeutic interventions for depression: Protocol for a qualitative study. *BMC Psychiatry* *13*(1), 64. doi:10.1186/1471-244x-13-64

Morganson, V. J., Major, D. A., Oborn, K. L., Verive, J. M., & Heelan, M. P. (2010). Comparing security locations and traditional work arrangements: Differences in work-life balance support, job satisfaction, and inclusion. *Journal of Managerial Psychology, 25*(6), 578-595. doi:10.1108/02683941011056941

Munoz-Leiva, F., Sanchez-Fernandez, J., Montoro-Rios, F., & Ibanez-Zapata, J. (2010). Improving the response rate and quality in web-based surveys through the personalization and frequency of reminder mailings. *Qual. Quant.* ***44***(5), 1037–1052. doi:10.1007/s11135-009-9256-5

Mupepi, M. G., & Mupepi, S. C. (2014). Appreciating rapid technology integration in creating value in enterprises. *Journal of Electronic Commerce in Organizations (JECO)*, *12*(1), 53-75. doi:10.4018/jeco.2014010104

Naor, M., Bernardes, E. S., & Coman, A. (2013). Theory of constraints: Is it a theory and a good one? *International Journal of Production Research*, *51*(2), 542-554.

doi:10.1080/00207543.2011.654137

Naser, A. W., (2015). Establishment and development of a system dynamics model based on security best practices. *Epistemologia, 12*(01), 1-5. Retrieved from http://epistemologia-journal.com/

Nave, D. (2002). How to compare six sigma, lean, and the theory of constraints. *Quality Progress*, *35*(3), 73-80. Retrieved from http://asq.org/qualityprogress/index.html

Neirotti, P., Paolucci, E., & Raguseo, E. (2013). Mapping the antecedents of security diffusion: Firm-level evidence from Italy. *New Technology, Work and Employment*, *28*(1), 16-36. doi:10.1111/ntwe.12001

Nilles, J. M. (1997). Security: Enabling distributed organizations. *Information Systems Management, 14*(4), 7-15. doi:10.1080/10580539708907069

O'Driscoll, M. P., Brough, P., Timms, C., & Sawang, S. (2010). Engagement with information and communication technology and psychological well-being. *Research in occupational stress and well-being*, *8*, 269-316. doi:10.1108/s1479-3555(2010)0000008010

Offstein, E., Morwick, J., & Koskinen, L. (2010). Making security work: Leading people and leveraging technology for competitive advantage. *Strategic Review, 9*(2) 32-37. doi:10.1108/14754391011022244

Ojala, S. (2011). Supplemental work at home among Finnish wage earners: Involuntary overtime or taking the advantage of flexibility? *Nordic Journal of Working Life Studies*, *1*(2), pp-77. Retrieved from http://www.nordicwl.com/

Ojala, S., Nätti, J., & Anttila, T. (2014). Informal overtime at home instead of security:

Increase in negative work-family interface. *International Journal of Sociology and Social Policy*, *34*(1/2), 5-5. doi:10.1108/ijssp-03-2013-0037

Ojala, S., Nätti, J., & Anttila, T. (2014). Informal overtime at home instead of security: Increase in negative work-family interface. *International Journal of Sociology and Social Policy*, *34*(1/2), 5-5. doi:10.1108/ijssp-03-2013-0037

Olaniran, B. A. (2009). Organizational communication: Assessment of videoconferencing as a medium for meetings in the workplace. *International Journal of Technology and Human Interaction (IJTHI), 5*(2), 63-84. Retrieved from http://www.scimagojr.com/journalsearch.php?q=11900154401&tip=sid

Orttung, R. W., & Overland, I. (2011). A limited toolbox: Explaining the constraints on Russia's foreign energy policy. *Journal of Eurasian Studies, 2*(1), 74-85. doi:10.1016/j.euras.2010.10.006

Pan, B., Woodside, A. G., & Meng, F. (2014). How contextual cues impact response and conversion rates of online surveys. *Journal of Travel Research*, *53*(1), 58-68. doi:10.1177/0047287513484195

Pfeffer, J. (2010). Building sustainable organizations: The human factor. *Academy of Management Perspectives, 24*(1), 34-45. doi:10.5465/amp.2010.50304415

Pham, M. H. (2010). *An investigation on the constraints to security implementation in New Zealand businesses* (Doctoral dissertation, School of Information Management, Victoria University of Wellington).

Pirdavani, A., Bellemans, T., Brijs, T., Kochan, B., & Wets, G. (2014). Assessing the road safety impacts of a security policy by means of geographically weighted regression method. *Journal of transport geography, 39*, 96-110. doi:10.1016/j.jtrangeo.2014.06.021

Putnam, L. L., Myers, K. K., & Gailliard, B. M. (2013). Examining the tensions in workplace flexibility and exploring options for new directions. *Human Relations, 67*(4), 413-440. doi:10.1177/0018726713495704

Pyöriä, P. (2003). Knowledge work in distributed environments: issues and illusions. *New Technology, Work and Employment, 18*(3), 166-180. doi:10.1111/1468-005x.00119

Pyöriä, P., (2011). Managing security: Risks, fears and rules. *Management Research Review, 34* (4), 386 – 399. doi:10.1108/01409171111117843

Rabiee, A., Taghi Amini, M., & Pirayesh, Z. (2014). Examining the security linkage with improvement of work and social life balance. *Social Welfare Quarterly, 13*(51), 69-108. Retrieved from http://refahj.uswr.ac.ir/browse.php?a_code=A-10-817-163&slc_lang=en&sid=1

Raghuram, S., & Fang, D. (2014). Telecommuting and the role of supervisory power in China. *Asia Pacific Journal of Management, 31*(2), 523-547. doi:10.1007/s10490-013-9360-x

Rahmn, S. (1998). Theory of constraints: A review of the philosophy and its applications. *International Journal of Operations & Production Management, 18*(4), 336. doi10.1108/01443579810199720

Rasmusen, E., & Corbett, G. (2008). Why isn’t security working? *New Zealand Journal of Employment Relations, 33*(2), 20-32. Retrieved fromhttp://www.nzjournal.org/33(2)Rasmussen.pdf

Rau, B. L., & Hyland, M. A. M. (2002). Role conflict and flexible work arrangements: The effects on applicant attraction. *Personnel Psychology, 55*(1), 111-136. doi:10.1111/j.1744-6570.2002.tb00105.x

Reinsch, N.L. (1999). Selected communication variables and security participation discussions: Data from security workers. *Journal of Business Communication, 36*(3), 247-261. doi:10.1177/002194369903600302

Rivera-Rodriguez, A. J., McGuire, K., Carayon, P., Kleiner, B., Wears, R., Robertson, M., Holden, R., & Waterson, P. (2013). Multi-level ergonomics determining how to bound your system. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 57*(1), 1104-1108. doi:10.1177/1541931213571246

Robertson, M. M., Schleifer, L. M., & Huang, Y. H. (2012). Examining the macro-ergonomics and safety factors among security systems: Development of a conceptual model. *Work: A Journal of Prevention, Assessment and Rehabilitation, 41*, 2611-2615. Retrieved from http://www.iospress.nl/journal/work/

Sadat, S., Carter, M. W., & Golden, B. (2013). Theory of constraints for publicly funded health systems. *Health care management science*, *16*(1), 62-74. doi:10.1007/s10729-012-9208-9

Sanchez-Fernandez, J., Munoz-Leiva, F., Montoro-Rios, F., Ibanez-Zapata, J. A. (2010). An analysis of the effect of pre-incentives and post-incentives based on draws on response to web surveys. *Qual Quant*, *44*(2), 357–373. doi:10.1007/s11135-008-9197-4

Santos, J., Romero, R., Arcelus, M., & Errasti, A. (2011). Teaching theory of constraints in 10 hours using open-source simulator. *International Journal of Information and Operations Management Education*, *4*(1), 69-82. doi:10.1504/ijiome.2011.037921

Sardeshmukh, S. R., Sharma, D., & Golden, T. D. (2012). Impact of security on exhaustion and job engagement: A job demands and job resources model. *New Technology, Work and Employment*, *27*(3), 193-207. doi:10.1111/j.1468-005x.2012.00284.x

Sato, A. (2013). Security and the changing workplaces. *Labor Review*, *10*(3), 56. Retrieved from http://www.bls.gov/mlr/

Schnijdirberg, S.J. (2011). *New ways to work-new ways to manage. Security and organizational control in small and medium enterprises.* (Thesis). Maastricht University, Maastricht, Netherlands

Scholefield, G., & Peel, S. (2009). Managers' attitudes to security training. *New Zealand Journal of Employment Relations, 34*(3), 1-13. Retrieved from www.nzjournal.org/

Schragenheim, E., (2010). Ever improve–a guide to managing production the TOC way by O. Cohen. *International Journal of Production Research, 48*(18), 5545-5546. doi:10.1080/00207541003737685

Schulte, M. (2015). Distance faculty experiences: A personal perspective of benefits and detriments of telecommuting. *The Journal of Continuing Higher Education, 63*(1), 63-66. doi:10.1080/07377363.2014.998048

Schwarz, G. M. (2012). The logic of deliberate structural inertia. *Journal of Management*, *38*(2), 547-572. doi:10.1177/0149206309361206

Scott, D. M., Dam, I., Páez, A., & Wilton, R. D. (2012). Investigating the effects of social influence on the choice to security. *Environment and Planning-Part A*, *44*(5), 1016. doi:10.1068/a43223

Shahangian, R. S. (2007*). The combined effect of feasibility of security on the willingness of employees towards accessing technology, from the employees and managers stand point of view, a master's thesis of civil engineering.* (Unpublished thesis). Sharif University, Tehran, Iran.

Shamsur-Rahman, S. (1998). Theory of constraints: A review of the philosophy and its applications. *International Journal of operations management*, *18*(4), 336-355. doi:10.1108/01443579810199720

Sharma, R., & Yetton, P. (2011). Top management support and IS implementation: Further support for the moderating role of task interdependence. *European Journal of Information Systems, 20*(6), 703-712. doi:10.1057/ejis.2011.39

Shaw, R., Chen, C. C., Harris, A. L. & Huang, H.-J. (2009). The impact of information richness on information security awareness training effectiveness. *Computers & Education*, *52*(1), 92-100. doi:10.1016/j.compedu.2008.06.011

Shekarhizadeh, A., Ghasemi, L., Tadi, M. J., Soltani, A., & Nili, M. (2015). Security and its impact on institutional control in organizations. *Sains Humanika, 5*(2). Retrieved from http://www.sainshumanika.utm.my

Silberman, G., & Kahn, K. L. (2011). Burdens on research imposed by institutional review boards: The state of the evidence and its implications for regulatory reform. *Milbank Quarterly*, *89*, 599–627. doi:10.1111/j.1468-0009.2011.00644.x

Siha, S. M., & Monroe, R. W. (2006). Telecommuting's past and future: A literature review and research agenda. *Business Process Management*, *12*(4), 455-482. doi:10.1108/14637150610678078

Sikes, N., Mason, K., & VonLehmden, S. (2011). Telecommuting advantages and challenges for IT management and staff. *ACM*, 20-25. Retrieved from http://www.acm.org/

Simon, M. K. (2011). *Dissertation and scholarly research: Recipes for success* (2011 ed.). Seattle, WA: Dissertation Success, LLC.

Smith, A. M., & Mateas, M. (2011). Answer set programming for procedural content generation: A design space approach. *Computational Intelligence and AI in Games, IEEE Transactions on*, *3*(3), 187-200. doi:10.1109/tciaig.2011.2158545

Spector, Y. (2011). Theory of constraint methodology where the constraint is the business model. *International Journal of Production Research*, *49*(11), 3387-3394. doi:10.1080/00207541003801283

Status of Security in the Federal Government. (2013). Annual Reports to Congress. Retrieved from http://www.security.gov/Reports_and_Studies/Annual_Reports/2013securityreport.pdf

Štemberger, M. I., Manfreda, A., & Kovačič, A. (2011). Achieving top management support with business knowledge and role of IT/IS personnel. *International Journal of Information Management*, *31*(5), 428-436. doi:10.1016/j.ijinfomgt.2011.01.001

Swanberg, J. E., McKechnie, S. P., Ojha, M. U., & James, J. B. (2011). Schedule control, supervisor support and work engagement: A winning combination for workers in hourly jobs? *Journal of Vocational Behavior, 79*(3), 613-624. doi:10.1016/j.jvb.2011.04.012

Swift, M. L., & Virick, M. (2013). Perceived support, knowledge, and provider knowledge sharing. *Group & Organization Management*, *38*(6), 717-742. doi:10.1177/1059601113507597

Swink, D.R. (2001). Telecommuter law: A new frontier in legal liability. *American Business Law Journal, 38*(4), 857-901. doi:10.1111/j.1744-1714.2001.tb00909.x

Taskin, L., & Bridoux, F. (2010). Security: a challenge to knowledge transfer in organizations. *The International Journal of Human Resource Management, 21*(13), 2503-2520. doi:10.1080/09585192.2010.516600

Teo, T. S., Lim, V. K., & Wai, S. H. (1998). An empirical study of attitudes towards security among information technology (IT) personnel. *International Journal of Information Management, 18*(5), 329-343. doi:10.1016/s0268-4012(98)00023-1

Teo, T, & Noyes, J. (2011). An assessment of the influence of perceived enjoyment and attitude on the intention to use technology among pre-service teachers: A structural equation modeling approach. *Computers & Education*, *57*(2), 1645-1653. doi:10.1016/j.compedu.2011.03.002

Teo, T., Wong, S. L., & Chai, C. S. (2008). A cross-cultural examination of the intention to use technology between Singaporean and Malaysian pre-service teachers: An application of the technology acceptance model (TAM). *Educational Technology & Society, 11*(4), 265-280. Retrieved from www.ifets.info/

Thomas, R., Sargent, L. D., & Hardy, C. (2011). Managing organizational change: Negotiating meaning and power-resistance relations. *Organization Science*, *22*(1), 22-41. doi:10.1287/orsc.1090.0520

Troup, C., & Rose, J. (2012). Working from home: Do formal or informal security arrangements provide better work–family outcomes? *Community, Work & Family*, *15*(4), 471-486. doi:10.1080/13668803.2012.724220

Turetken, O., Jain, A., Quesenberry, B., & Ngwenyama, O. (2011). An empirical investigation of the impact of individual and work characteristics on telecommuting success. *Professional Communication, IEEE Transactions, 54*(1), 56-67. doi:10.1109/tpc.2010.2041387

Valmohammadi, C. (2012). Investigating the perceptions of Iranian employees on security implementations. *Industrial and Commercial Training*, *44*(4), 236-241. doi:10.1108/00197851211231513

Van den Broek, D., & Keating, E. (2011). Rights to a process for the masses or select privileges for the few? Security policy and labour market inequality in Australia. *Policy Studies*, *32*(1), 21-33. doi:10.1080/01442872.2010.520559

Venkaesh, V., & Johnson, P. (2002). Security technology implementation: A within-and between-subjects longitudinal field study. *Personnel Psychology, 55*(3), 661-668.

doi:10.1111/j.1744-6570.2002.tb00125.

Venkaesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS quarterly*, *27*(3), 425-478. Retrieved from http://www.misq.org/

Vesala H., & Tuomivaara, S. (2015). Slowing work down by security challenges periodically in rural settings? *Personnel Review*, *44*(4). 511-528. doi:10.1108/pr-07-2013-0116

Vitola, A., & Baltina, I. (2013). An evaluation of the demand for security and smart work centers in rural areas: A case study from Latvia. *European Countryside*, *5*(3), 251-264. doi:10.2478/euco-2013-0016

Watad, M. M., & Will, P. C. (2003). Telecommuting and organizational change: A middle managers' perspective. *Business Process Management Journal*, *9*(4), 459-472.

Watson, K. J., Blackstone, J. H., & Gardiner, S. C. (2007). The evolution of a management philosophy: The theory of constraints. *Journal of Operations Management, 25*(2), 387-402. doi:10.1016/j.jom.2006.04.004

Weinert, C. (2015). *Why are technology workers stressed? An empirical analysis of the causes of security-enabled stress.* (Unpublished doctoral dissertation). University of Bamberg, Bamberg, Germany

Weinert, C., Maier, C., Laumer, S., & Weitzel, T. (2014). Do security requirements negatively influence IT professionals? An empirical analysis of IT personnel's security-enabled stress. *ACM*, 139-147. Retrieved from http://www.acm.org/

Weisberg, A., & Porell, M. (2011). Moving security from compliance to competitiveness. *The Public Manager*, 12-14. Retrieved from http://www.astd.org/Publications/Magazines/The-Public-Manager

Wicks, D. (2002). Successfully increasing technological control through minimizing workplace resistance: Understanding the willingness to security. *Management Decision*, *40*(7), 672-681. doi:10.1108/00251740210438508

Woodman, R. W. (2014). The role of internal validity in evaluation research on organizational change interventions. *The Journal of Applied Behavioral Science, 50*(1), 40-49. doi:10.1177/0021886313515613

Wright, K. B., Abendschein, B., Wombacher, K., O'Connor, M., Hoffman, M., Dempsey, M., Krull, C., Dewes, A., & Shelton, A. (2014). Work-related communication technology utilization outside of regular work hours and work life conflict the influence of communication technologies on perceived work life conflict, burnout, job satisfaction, and turnover intentions. *Management Communication Quarterly*, *28*(4), 507-530, doi:10.1177/0893318914533332

Wyrzykowska, B. (2014). Security and personnel risk. *Warsaw University of Life Sciences (SGGW), 14*(4), 215-225. Retrieved from http://www.sggw.pl/

Yahaya, J. H., Basir, M. M., & Deraman, A. (2015). Unified communication and collaboration model for virtual distributed team work: A study in Malaysia. *International Journal of Software Engineering and Its Applications, 9*(2), 125-142. doi:10.14257/ijseia.2015.9.2.11

Yao, D. Q. (2012). Application of the theory of constraints (TOC) to batch scheduling in process industry. *International Journal of Applied Industrial Engineering (IJAIE)*, *1*(1), 10-22. doi:10.4018/ijaie.2012010102

Yinat, J. (2014). *Relationship of management performance practices on security resistance outcomes in the US federal government* (Doctoral dissertation). Available for ProQuest Dissertations Full Test database. (UMI No. 3639047)

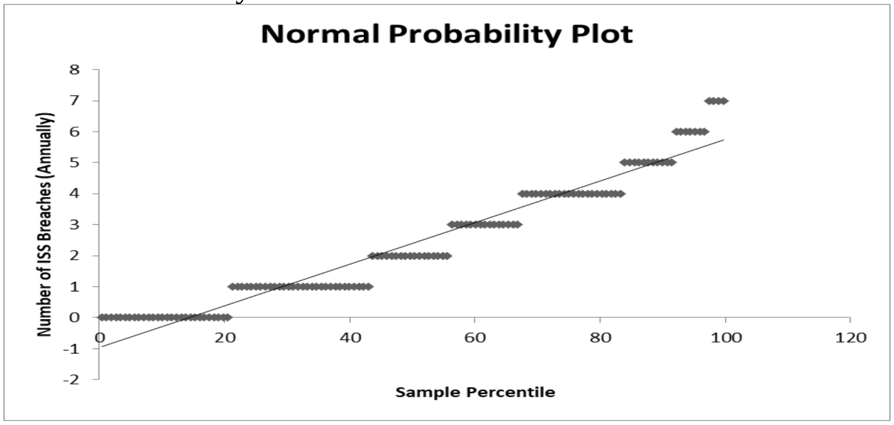
Yun, H., Kettinger, W. J., & Lee, C. C. (2012). A new open door: The Smartphone’s impact on work-to-life conflict, stress, and resistance. *International Journal of Electronic Commerce*, *16*(4), 121-152. doi:10.2753/jec1086-4415160405

Zhu, P. (2013). Telecommuting, household commute and location choice. *Urban Studies*, *50*(12), 2441-2459. doi:10.1177/0042098012474520

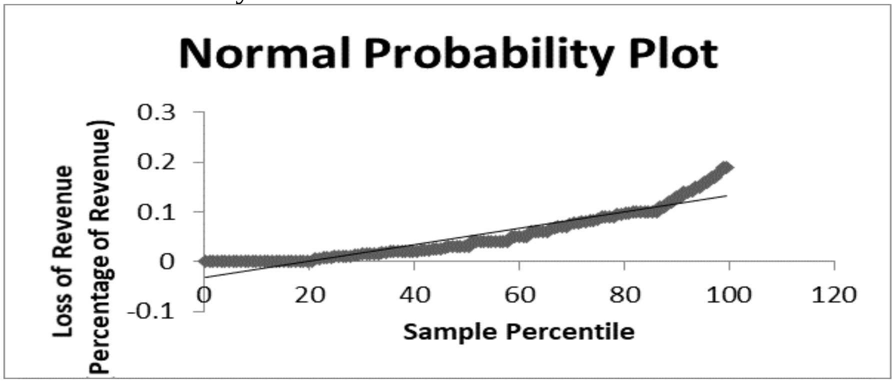
Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation Computer Systems*, *28*(3), 583-592. doi:10.1016/j.future.2010.12.006

# Appendix A

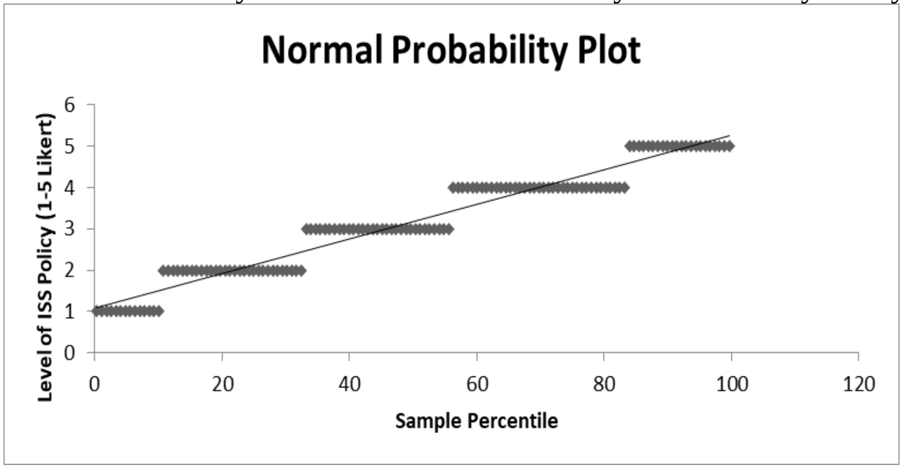
Normal Probability Plot Number of IS Breaches



Normal Probability Plot Loss of Revenue



Normal Probability Plot Level of Information Systems Security Policy



# Appendix B

Pearson 1

| | *Level of ISS Policy (1-5 Likert)* | *Number of ISS Breaches (Annually)* |
|---|---:|---:|
| Level of ISS Policy (1-5 Likert) | 1 | |
| Number of ISS Breaches (Annually) | -0.857721658 | 1 |

Pearson 2

| | *Level of ISS Policy (1-5 Likert)* | *Loss of Revenue (Percentage of Revenue)* |
|---|---:|---:|
| Level of ISS Policy (1-5 Likert) | 1 | |
| Loss of Revenue (Percentage of Revenue) | -0.764187687 | 1 |