Examining the Outcomes and Organizational Responses of IT Security Breaches

BY

Atiya Avery
Honors B.B.A., Georgia State University, Atlanta 2008
M.S., Georgia State University, Atlanta 2013

THESIS

Submitted as partial fulfillment of the requirements
for the degree of Doctor of Philosophy in Management Information
Systems in the Graduate College of the
University of Illinois at Chicago, 2018

Chicago, Illinois

Defense Committee:

Ranganathan Chandrasekaran, Chair and Advisor
Stanley Sclove
Sajna Ibrahim, Marketing
Chris Kanich, Computer Science
Ali Tafti

I dedicate to this thesis to my husband, best friend, and life partner, Musha, my mother Karen, and my father Vince for their unwavering support of my doctoral studies. I also dedicate this thesis to my very dear siblings, Noah, Aamela, Ishmael, Ninti, Ninurta, Kedar, Shakiyra, and Aniecia for providing me with the inspiration for most all of my research projects including this dissertation and allowing me to discuss my many thoughts and musings with them. Finally, I am grateful to the Creator and my ancestors for bestowing upon me the gifts of courage, resiliency, intelligence, and discernment without which the completion of my doctoral studies at the University of Illinois at Chicago would not have been possible.

Acknowledgments

I want to acknowledge my dissertation chair Dr. Ranganathan Chandrasekaran and the thesis committee members, Dr. Sajna Ibrahim, Dr. Ali Tafti, Dr. Chris Kanich, and Dr. Stanley Sclove for taking their time to provide me valuable feedback and assistance in the completion of this research study and manuscript.

I would like to acknowledge my longtime mentor, very dear friend, and IT infrastructure expert Dream Gomez and UIC Information and Decision Sciences lecturer and IT security expert LeRoy Foster for their strategic support, technical guidance, practical and cultural subject matter expertise, and for providing me access to their network resources which was essential for the proper development and completion of this research study and manuscript.

I would also like to acknowledge Dr. Matt Liotine in the Department of Information and Decision Sciences for his subject matter expertise and thoughtful words during the final stages of the study. I would also like to acknowledge the national Women in Cybersecurity organization as well as Dr. Kyle Cheek and John Fyfe at the Center for Research in Information Management (CRIM) at UIC for providing me access to potential research participants.

This research study was partially funded by the UIC Electronic Security and Privacy Integrative Graduate Education and Research training (ESP-IGERT) program funded by the National Science Foundation (NSF) under NSF grant number 1069311. I am appreciative for their financial support.

Lastly, I would like to thank the many new and old professional acquaintances, associates, and friends who went out of their way to participate in this study despite being a little nervous and in turn encouraging their colleagues to participate in the study. I am forever grateful to everyone!

TABLE OF CONTENTS

PART 1: QUALITATIVE CONCEPTUALIZATION OF THE RESEARCH MODEL

CHAPTER 1: INTRODUCTION

CHAPTER 2: LITERATURE REVIEW OF IT SECURITY BREACHES

CHAPTER 3: CONCEPTUALIZING IT SECURITY BREACH EVENTS

CHAPTER 4: STUDY 1 CONCEPTUALIZING ORGANIZATIONAL RESPONSE TACTIC DIMENSIONS

CHAPTER 5: RESEARCH MODEL AND HYPOTHESES

PART 2: QUANTITATIVE RESEARCH DESIGN, DATA ANALYSIS, AND FINDINGS

CHAPTER 6: FIELD SURVEY AND OVERVIEW OF RESEARCH METHODOLOGIES

CHAPTER 7: EVALUATION OF RESEARCH MODELS

CHAPTER 8: QUALITATIVE ANALYSIS OF UNEXPECTED RESULTS AND IMPLICATIONS OF STUDY FOR RESEARCH AND PRACTICE

CHAPTER 9: CONTRIBUTIONS, LIMITATIONS, AND FUTURE WORK

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

CERT-Community Emergency Response Team

CIO- Chief Information Officer

CISSP- Certified Information Systems Security Professional

COBIT- Control Objectives for Information and Related Technologies

CTO- Chief Technology Officer

ISACA- Information Systems Audit and Control Association

NIST- National Institute of Standards and Technology

PCI DSS- Payment Card Industry Data Security Standard

PLS- Partial Least Squares

SEM- Structural Equation Modeling

SUMMARY

As transactions and organizational infrastructures become increasingly digitized, this has led to the collection and storage of large volumes of data, information, and records. Digitization provides essential benefits to organizations such as enhanced record keeping and increases in efficiency; however, it also increases the likelihood of IT security breach events. This mixed method research study seeks to understand the relationship among organizational response tactics to IT security breach events and the organizational losses from IT security breach events. First, by utilizing a qualitative, grounded theory approach this study finds that there are seven distinct types of organizational response tactics to IT security breach events that can be implemented proactively or reactively in response to an IT security breach event. The grounded theory approach also finds that there are four distinct types of losses related to IT security breach events these losses include *financial losses*, *reputational losses*, *competitive losses*, and *business productivity losses*. Second , by utilizing the quantitative analysis technique of partial least squares based structural equation modeling, this study finds that both proactive and reactive *governance*, *relationship management*, and *security strategic management* tactics can be helpful in reducing losses after an IT security breach event for organizations. However, the findings indicate that organizations should exercise extreme caution in implementing reactive *communication management*, *morale management*, and *IT resource management* tactics so as not to further exacerbate organizational losses from an IT security breach event.

CHAPTER 1: INTRODUCTION

1.1 Motivation

The number of organizations experiencing data breach events has significantly increased over the last decade. In 2005, there was approximately one data breach every two days, and as of 2015, there were two data breaches a day (Identity Theft Resource Center, 2015). It is difficult for experts to measure the costs of data breach events on organizations. A recent study of 350 companies by International Business Machines (IBM) across 11 countries, estimated that on average each data breach will cost an organization 3.8 million dollars a year in losses or an estimated loss of $154 per breached record (IBM, 2015). One of the central questions in the information security and cybersecurity literature is "what are the organizational responses to information technology security breaches"? There is a very limited discussion in the literature on the incident response processes, prevention measures, loss mitigation tactics, and intra-organizational and inter-organizational losses from IT security breaches.

As transactions and organizational infrastructures become increasingly digitized, this has led to the collection and storage of large volumes of data, information, and records. Digitization provides essential benefits to all types of organizations such as enhanced record keeping and increases in inefficiency; however, it also increases the opportunities for IT security breach events. As the digitization of organizational infrastructures continues to rise, the risks of and from IT security breach events will increase as well. It is vital for research and practice to understand and articulate the best practices for managing these events within organizations. Negative losses from IT security breaches can range from decreases in revenue and sales, increases in the cost of doing business, and disclosure of confidential information such as company trade secrets and the personal information of private citizens.

Intuitively, we know that the losses from IT security breaches on organizations are not equal. Some organizations have experienced no apparent negative losses from IT security breach events, others have struggled to regain momentum, others have actually experienced enhanced performance, and still, other organizations have become insolvent. Much of the extant academic research has focused on publicly traded organizations, which by nature are also inherently large. However, the consequences of an IT security breach event may be more pronounced for smaller firms. An understanding of organizational responses and losses from these events will enable not only large firms but also smaller and private firms to better prepare for and withstand breach events. The purpose of Table 1 is to highlight how the short-term and long-term losses can vary and the types losses from IT security breaches could be widely different.

Company	IT Breach Event	Short-Term Negative Losses	Long-Term Negative Losses	Source
Target	40 million credit card accounts exposed over a two week period caused by breach of payment systems from unrelated third party vendor	Stock market declines	$18.5 Million Fine 4 years later and new standards set for the retail industry regarding electronic payments	Safdar & Beilfuss, 2016; Kedmey, 2014; McGinty, 2015
Ashley Madison	Unknown; however, it is estimated that approximately 11 million passwords were hacked over a period of time	Personal harm including self-harm attempts, extortion /blackmail, professional, and legal	$11.2 Million Settlement	Greene, 2015 Zetter, 2015
Home Depot	56 million credit card records exposed	Stock Market Declines	$159.5 Million settlement with payment card vendors	Associated Press, 2014; Hackett, 2015
U.S. Office of Personnel Management	Breach of HR records of 21.5 Million people	None	Potential Blackmail of Employees	Davis, 2015 Armerding, 2016

Table 1: Long- and Short-Term Losses from IT Security Breaches

In summary, the research and practice gaps in the information systems and broader cybersecurity literature are as follows:

1. Outside of short-term changes to firm market value, there is a lack of research on the long-term and short-term organizational consequences of IT security breaches.
2. Lack of research regarding organizational responses within organizations when IT security breaches do occur.

3. The lack of documentation of the relationship between characteristics of the IT security breaches, organizational responses, and organizational losses.

The research goals are:

1. To examine if the differences in organizational losses vary due to the varied organizational responses undertaken by organizations
2. To understand organizational management strategies pertaining to IT security breaches.

1.2 Conceptual Model

A simple conceptual model noted in Figure 1, guides this dissertation. The conceptual model illustrates that when an IT Security breach occurs, there are organizational losses to that event mitigated by organizational responses and IT security breach characteristics. The primary focus of this study is on the organizational responses. To better understand this phenomenon, this dissertation is comprised of two phases. Phase 1 encompasses a completed literature review, field insights, research models, hypotheses, and specific construct measures for a survey instrument. Phase 2 will consist of the data collection processes, the analytics processes, the results of the hypothesis testing, and the discussion and conclusion.

The findings of this dissertation will increase the understanding of how organizations handle IT security breach events internally, the short and long-term losses of these events on those organizations, and the best practices for mitigating these events. Figure 1 is the broad conceptual model that expands into a detailed research model for hypotheses testing.

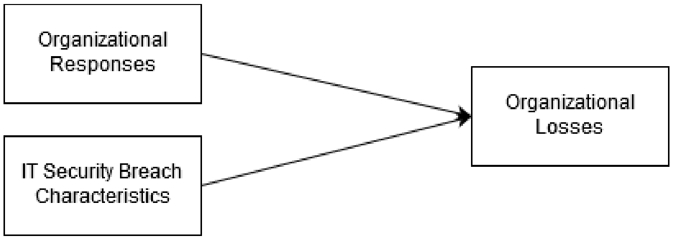


Figure 1: Broad Conceptual Model

1.3 Dissertation Overview

This dissertation consists of nine chapters and takes advantage of a mixed methods research design. The research goals benefit immensely from a mixed method approach wherein the qualitative portion of the mixed methods study will allow for the exploration of IT security breaches in-depth, guided by both a structured literature review and structured interviews. The qualitative methodologies enable us to collect rich data. The quantitative portion of the mixed methods study is in the form of a large-scale survey. This quantitative study will allow us, with some level of quantitative accuracy to better understand the most optimal strategies for managing IT security breach events. The quantitative methods and the qualitative methods complement each other in that the qualitative study components provide the much-needed context in the form of use cases to the survey results and will help guide the ensuing analysis of the survey data.

The motivation for this research study has already been discussed and overview has been given of the research gaps and the research questions, A conceptual model was then presented to better guide later theoretical development. For the remainder of Chapter 1, an extensive overview of the remaining chapters of this dissertation is provided.

Chapter 2 discusses the existing literature on IT security breach events and losses to organizations when these events occur. The financial, reputational, competitive, and business productivity losses of IT security breaches from the literature are conceptualized as dimensions for further study and examination as part of the research model. Chapter 3 conceptualizes IT Security breach events for the purposes of the research model based on the extant academic literature, practitioner white papers, and anecdotes and makes the argument for the use of the term "IT security breach" in lieu of other commonly used terms such as "data breach" or "privacy breach". Chapter 3 also discuss the implications to research when scholars do not use uniform research terms to describe a phenomenon. Chapter 4 discusses the utilization of an inductive and deductive approach to conceptualize organizational responses surrounding IT security breach events. The inductive study consists of a semi-structured literature review of both academic and practitioner research to derive seven sets of organizational responses to IT security breach events. After this discussion, a semi-structured interview of IT security executives will ensue. In Chapter 5, the conceptual model from Figure 1 is expanded into a research model with testable hypotheses to answer the research questions. Chapter 6 discusses the rationale for the dissertations research approach and methodology, the research design, participant recruitment, as well as the data collection and analysis methodology. In this chapter feedback is obtained from key informants and an academic expert. A discussion ensues regarding the research design feasibility and the validation of the research constructs. Chapters 7 is the evaluation of the research models utilizing partial least squared based structural equation modeling techniques. Chapter 8 is the discussion of the findings and post-hoc analysis. Chapter 9 is a discussion of contributions this study makes to research and practice, limitations, and extensions of the study. The chapter that follows is an overview of the IT security breach literature and discussion of the losses from these events.

CHAPTER 2: LITERATURE REVIEW OF IT SECURITY BREACHES

2.1 Prologue

In this chapter, a literature review of the existing research on IT security breaches is conducted. The literature review focuses on articulating the specific losses related to IT security breaches on organizations. The literature review encompasses both academic and practitioner research. It is discovered that the losses from IT security breaches are segmented into the four broad categories of 1) financial losses 2) reputation losses 3) competitive losses and 4) business productivity losses.

Non-financial losses merit attention because non-financial losses can assist front-line practitioners and managers with decision-making. Many practitioners are not only evaluated on financial losses, i.e. dollars, and cents but also other measures such as social media sentiment, count of new customers and customers loss, relationships established, and units of time such as the count of system downtime. Financial measures fall short in that they may not adequately provide the proper context for pre-breach and post-breach remediation and decision making for frontline practitioners and managers.

The existing literature on IT security breaches has focused primarily on so-called "data breach events" and their financial losses to firms. The extant research has examined the losses of these events on organizations in a number of contexts such as the effects to the focal firm, to partners, and even competitors (Spanos & Angelis, 2016). In particular, researchers have attempted to measure the losses of data breach events by examining changes to market value in the days following a breach. The changes to market values after an event are based on the efficient market hypothesis, which theorizes that changes to market value from an event will and should capture all relevant information that can be attributed to that event (Basu S., 1997). In the context of breach events, these changes include losses to organizational reputation, decreased sales, internal issues, and disrupted business relationships.

The downside of utilizing market value measures are that most of the effects are only captured within 1-3 days after a breach disclosure and in some cases up to 10-25 days after a breach disclosure (see Cavusoglu, Mishra, & Raghunathan, 2004; Chen, Li, Yen, & Bata, 2012; Garg, Curtis, & & Halper, 2003). Some researchers have attempted to utilize firm financial performance measures to capture the more long-term losses of IT security breaches on organizations, i.e. 1-4 quarters or 3-12 months after the event (Ko & Dorantes, 2006; Zafar, Ko, & Osei-Bryson, 2012; Ko, M., & Dorantes, 2009). However, this view perpetually postulates the losses of breach events on organizations as only being financial; albeit, there have been some knowledge gains where the characteristics of the firm or the breach event itself have been associated with mitigating changes in market value or the financial performance of impacted firms.

2.2 IT Security Breach Losses

One of the research questions this dissertation seeks to answer is "what are the organizational losses of IT security breaches?" Specifically, this study seeks to document the losses from breach events on organizations in addition to understanding the roles that organizational responses and the IT security breach itself played in the organization's recovery process after such an event. Unlike prior research which treats breach events as financial loss events to the focal firm, this dissertation theorizes that IT security failures have measurable losses to the financial, reputational, competitive and business productivity within the affected organizations. In the next two sections that follow, the specific losses related to IT security breaches are evaluated and described based on the existing academic and practitioner literature.

2.3 Financial & Reputational Losses from IT Security Breaches

After an extensive literature review, the financial and reputational losses from IT security breach events can be categorized as market value losses, financial performance losses, and to some extent intangible losses of goodwill. Market value losses include declines in the stock prices and subsequently the market values of the breached firm and in some cases declines in the stock prices and market values of related firms in what is known as network effects (Cavusoglu, Mishra, & Raghunathan, 2004; Hinz, Nofer, Schiereck, & Trillig, 2015). Financial performance losses include changes in the breached firms costs of goods sold, total operating expenses, net, and operating income, total assets, and sales (Ko, M., & Dorantes, 2009) intangible assets and goodwill are also measured on a firms financial statements and can be considered reputational losses. Just as with market value losses, the losses to financial performance from a breach event may also spillover onto related firms as network effects as well (Zafar, Ko, & Osei-Bryson, 2012).

The financial and reputational losses of information security breaches have typically been measured by changes in the firm's market values in the days following the information security breach disclosure and to a lesser extent changes to financial performance. In the market value context, the theory is that stock price changes in the days following a breach disclosure will capture the assessment of a large body of shareholders to the breach event and this assessment would, therefore, be reflected in the stock prices (Cavusoglu et al. 2004; Chen et al. 2012; Garg et al. 2003; Hovav & D'Arcy, 2003). Generally speaking, the findings surrounding the losses of IT security breaches on organizations are that they are valued declining adverse events. Research in this area spans the period from about 2003 to the present. Spanos & Angelis 2016 conducted an extensive literature review of market value losses from IT security breaches. The researchers estimated that as of 2015, approximately thirty-seven research studies had been conducted measuring the losses from IT security breaches on firms. Twenty-five of these studies have noted that these events have negative losses to firms; seven of these studies indicated that these events have neutral results; five studies have shown that these events have actually had positive impacts to the breached firm.

Despite the large proportion of IT security breach research that evaluates the market value losses, there are limitations to this research stream. First, it has been challenging to develop and advance theoretical framework, as the primary research method, event study methodology, becomes wieldy in the development and testing of theoretical frameworks. Second, many times the real impact of the IT security breach is unknown, as stakeholders may take time to react. A survey by the consulting firm SafeNet indicated that 54% of these consumers are very unlikely to do business with companies that experience a breach of financial information. 45% are somewhat unlikely to do business with companies that experienced *any* type of breach event. While 39% are somewhat unlikely to do business with companies that experienced a breach of personally identifiable information; which can include social security and driver’s licenses numbers, but also arguably benign information such as email addresses (SafeNet Survey, 2016). Third, market value measures cannot tell us may be occurring inside the firm or the impact on operations. Event study methodology, which has been the primary methodology for measuring changes to firm market value, cannot tell us what occurred 1-month later, 3 months or 1 year later. To resolve issues caused by utilizing measurements of firm market value, some researchers have begun to utilize common measures of firm financial performance such as evaluating changes to profits and costs.

The consulting firm Aon estimated that 80 % of “data security incidents” result in costs and damages less than $1 million. The costs and damages include expenses from legal settlements, business outages, digital investigation and forensic service fees, remediation of the IT infrastructure, identity fraud alert services for impacted consumers, and PR fees (Dempsey, 2015). In another study, IBM surveyed 350 companies across 11 countries and estimated that on average data breaches cost organizations 3.8 million dollars a year in losses or an estimated $154 per record that is breached (IBM, 2015). In spite of the plethora of practitioner research, it has proven difficult for industry experts to measure the costs of IT security breach events on organizations.

Academic researchers have empirically evaluated the cost impact of IT security breaches on firm financial performance by utilizing publicly available quarterly and annual financial statements. Financial statements are used for a wide range of business analysis and decision-making needs. Leadership within organizations use them to monitor and judge their performance relative to competitors, to communicate with external investors, to help determine what financial policies they implement and for valuing and analyzing prospective buyouts, mergers, and acquisitions (Gibson C. , 2007). To better articulate the costs of IT security breach events Ko & Dorantes, 2006 pg. 14-15; have segmented costs losses that would impact financial performance into either short-term or long-term costs. Examples of short-term cost losses include costs of repairs, costs of replacement of the information systems, lost business due to business disruption of operations and lost productivity of employees. Long-term costs include the loss of existing customers, loss of new and potential customers, negative reputation, loss of business partners, legal liabilities, and payment of damages to injured third parties. Both long and short-term costs will manifest in the financial statements.

Furthermore, like the research on market value and stock market changes; the financial performance research has explored network effects of an IT security breach on competitor and complementary firms (Hinz, Nofer, Schiereck, & Trillig, 2015; Ettredge & Richardson 2003). Some network effects include consulting firms experiencing increased financial performance (Chen, Li, Yen, & Bata, 2012)and technology firms being more likely than other types of firms to experience more pronounced negative contagion effects from IT security breach events (Zafar, Ko, & Osei-Bryson, 2012).

In addition, there is a large body of literature in the law and insurance domains concerning liability, tort, and negligence and these topics are a significant concern for organizations during and after an IT security breach event. According to (Epstein, 1973) an entity is found to be legally liable when they hold legal and financial responsibility for something. Epstein 1973 also notes that legal liability can comprises of both civil law and criminal law. Legal liability can arise from various areas of law, such as contracts, tort judgments or settlements, taxes, or fines given by government agencies (Epstein, 1973). An analysis of 1,700 legal actions surrounding IT security breach events indicates that 83% of the cases were considered civil and 17% considered criminal (Ashenmacher, 2016). It also possible that a federal or state government entity conducts their own investigation and assessment for potential liability and subsequent financial remediation after an IT security breach event as the cases with J.P. Morgan, Target, Home Depot, Experian, and Zappos illustrate (Jaeger, 2015). For private citizens, damages from an organizations IT security breach involving their information or data can be articulated as 1) lost time and money resolving fraudulent charges, 2) lost time and money for individuals to protect themselves against future ID theft, 3) the financial loss of using the services or purchasing the product had they known the organization was prone to a breach, 4) the loss of control over the value of their personal information (Romanosky, 2016). The long-term effects of these seemingly innocuous “personal” inconveniences are not yet understood.

The literature hypothesizes that negative losses from breach events will not only hurt an organizations reputation by influencing the market and financial performance but can also have losses to the organization's competitiveness and business productivity. Salmela 2008, posits that losses from breaches can come from nine sources which include 1) losses from operations, 2) decreased revenues, 3) opportunity losses from subsequent bad decision making, 4) loss of competitiveness from the disclosure of propriety information, 5) business losses from tangible money or goods taken during the breach, 6) company reputation losses 7) losses to existing shareholders, 8) legal losses, and 9) IT losses. Despite the broad consensus amongst industry and practice that IT security breaches can have adverse effects on the competitive losses and business productivity of an organization after an event; it is not well documented in the academic literature what exactly those losses may be. A cursory review of practitioner research reveals that the aforementioned sources of loss from a breach event are described in financial terms and not necessarily in the context of specific losses (for some examples of this see Verizon, 2015; Mossburg, Fancher, & Gelinne, 2016; IBM, 2015). For example, there may be mention of how much money was spent on IT upgrades but no details on what specifically those upgrade choices were or if they were the most optimal choices for the organization or what caused an organization to select a particular decision.

2.4. Competitive and Business Productivity Losses from IT Security Breaches

The literature on the losses of IT security breaches to organizational competitiveness and business productivity discusses such losses as changes to customer retention, customer downtime, loss of IT control, employee downtime, data/information loss, severed relationships, and post-breach tracking of system users.

A number of competitive and business productivity losses can be broadly clustered into productivity losses. Productivity losses due to a security incident can be seen in several ways, downtime for an end user while the application they need to work in is offline or idle time spent by an employee while the system is down. In addition, security events can cause data corruption or data loss. For instance, when a virus infects a server that houses important files for an organization, the organization will now have to invest and utilize backup servers; this may cause a rework of the business processes. While the rework costs to produce specific data can is managable, the amount of data that could be damaged by malicious code could range from one file to several servers and may not be recoverable at all (Poole, 2009).

Also, IT security breaches have the potential to influence the focal organization's partnerships and relationships with other organizations. A 2017 survey by Cisco found that nearly a quarter of the organizations that have suffered a malicious IT security breach lost business opportunities (CISCO, 2017). Companies also temporarily lose the ability to engage in their standard business practices that may influence perceptions of the organization's reliability and dependability as viable trading partners.

Furthermore, when an IT security breach occurs, organizations not only have to contend with the disclosure of client and consumer data; such as passwords and logins, but also with the disclosure of credentials for its employees. At the organizational level, this allows nefarious agents to potentially change browser and operating settings, disable antivirus products, and implement mechanisms to track users long after the breach event (CISCO, 2017). The unauthorized collection of personal information of employees of the organization or consumers can be used without their consent or used to harass them with unsolicited communication (Romanosky, 2016).

2.5 Dimensions of Losses from IT Security Breach Events

Table 2 lists the exhaustive set of losses from IT security breaches. In summary, an extensive literature review of academic and practitioner research was conducted to articulate the losses of IT security breach events on organizations. It is noted that there is extensive academic literature regarding the financial and reputational losses of breach events on organizations, however; there is very little reliable research on the losses to competitiveness and business productivity within the impacted organizations. Much of the literature stream on competitiveness and business productivity losses consists of news articles and practitioner whitepapers and while high quality it cannot be ignored that this research is being conducted by for-profit organizations which have a financial incentive in publishing their research.

Losses from IT Security Breaches	
Breach Loss Summary	**Source**
Reputational Losses	
Damaged Company Reputation & Image	Ettredge & Richardson 2003, Goel and Shawky 2009, Hinz et al. 2015; Modi et al. 2015
Loss of Public Goodwill & Trust	Olmstead & Smith, 2017; Farrell, 2017; Macri, 2016; Vinton, 2014
Financial Losses	
Declines in One or More Measures of Revenue Increases in Cost of Operations	Ko & Dorantes 2006, Ko & Dorantes 2006, Zafar et al 2012; Salmela 2008;Mossburg et al 2016

A decline in Stock Prices	Cardenas et al. 2008, Bose and Leung 2014, Cavusoglu et al. 2004; Chen et al. 2012; Garg et al. 2003; Hovav and D'Arcy 2004; Yayla and Hu 2011
Legal Costs	Khansa et al. 2012; Romanosky, Telang, & Acquisti, 2011;
Competitive Losses	
Severed Relationships Loss of Existing Customers Loss of Potential/New Customers	CISCO, 2017 Annual Cybersecurity Report, SafeNet 2016 Survey
User Tracking	CISCO, 2017 Annual Cybersecurity Report; Sanger, Chan, & Scott, 2017; Gelsomini et al. 2015
Business Productivity Losses	
System Downtime Loss of Employee Productivity	Pool, E, 2009; Satin & Bernardi, 2015
Delay in Business Operations	Pool, E, 2009; Blatnik, 2017; National Cybersecurity Institute, 2016

Table 2: Summary Literature Review of Losses Related to IT Security Breaches

The chapter that follows conceptualizes IT security breach events including articulating the characteristics that an IT security breach event can have.

CHAPTER 3: CONCEPTUALIZING IT SECURITY BREACH EVENTS

3.1 Prologue

This chapter conceptualizes the features that encompass IT security breach events. The conceptualization begins by deriving a working definition from the existing literature. IT security breach events are then conceptualized along four characteristics that include 1) extent of the breach, 2) intentionality, 3) source and 4) sensitivity. This chapter concludes with a theoretical framework tying the four characteristics of an IT security breach together allowing a more complete view of the risks from these types of events on organizations.

3.2 Working Definition of IT Security Breaches

A breach in the context of information technologies and in particular information systems is defined as a "particular circumstance wherein a violation against a set of regulations or rules has occurred to effect an entrance into whatever the established rules and regulations were promulgated to prevent unauthorized access. It is also a term used to describe a break in continuity" (Chen, Li, Yen, & & Bata, 2012, pg. 47). As technologies evolve characteristics of security breaches, can and have changed over time (Kelly 1999, Hovav & D'Arcy 2003). The literature has used many different definitions to discuss IT security breaches including denial of service attacks (Hovav & D'Arcy 2003), phishing attacks (Bose & Leung 2014, Chen,Bose, Leung, Guo 2011), information security breaches (Spanos and Angelis 2016), data breaches (Harris,2015), privacy breaches (Liginlal, Sim, Khansa , 2009), internet security breaches (Cavusoglu, Mishra, Raghunatahn 2004), and information or information system security breach (Cardenas, Coronado, Donald, & Parra, 2012;Goel & Shawky 2009). This section the delineations and intersections amongst these terms. In addition, a discussion of the rationale for using the term "IT security breaches" for this dissertation ensues.

It is important that terms are appropriately defined to extend prior research and compare findings across research studies. Cardenas et al. 2012, found that when the terms "privacy breach" and "security breach" were not clearly defined or were improperly combined this might have led to research results surrounding the market value losses of security failures on firms to not be consistent throughout the literature. In this dissertation, to ensure consistency and increase semantic precision, in lieu of synthesizing definitions for the most common breach terms, it was the common breach terms are described directly from the associated literature specifically. Table 3, lists the most common breach terms used in the information systems domain and their sources. Furthermore, listing the direct source of common breach term definitions instead of synthesizing the terms is beneficial in this context because many of the research papers provide no formal definition for terms and instead the type of breach event that is being studied has to be intimated from the datasets used in the research. This is further complicated by the fact that "security breach" definitions have evolved over time whereas terms such as "internet security breach" may be outdated. Furthermore, breach terms and their definitions are not necessarily exhaustive or exclusive, for instance, a privacy breach can encompass an information (system) security breach and data breach.

Term	Definition
Internet Security Breach	An ‘‘internet security breach’’ is defined as ‘‘a violation of an information system’s security policy. Examples of an internet security breach range from the tampering of computer programs to interruption of internet services and unauthorized access. (Ettredge & Richardson, 2001; Straub, 1990). Can be insinuated from the data set used in the research. For example, Liginlal et al. 2009 classified reports of ‘‘privacy breach," ‘‘information security breach," and general ‘‘computer security" events. In addition to events reported by the organization "Privacy Rights Clearinghouse" which uses the term "data breaches" to describe the events that they report. (Liginlal et al. 2009)

Privacy Breach	There are privacy breach events which encompass both ‘‘internet security breaches’’ and ‘‘data breaches’’. To consolidate all these breach events, a framework known as the CIA model was developed to better classify and converge all the breach events within a framework. The breach events are reclassified as follows: confidentiality, integrity, and availability breaches. (Chen et al. 2012(1))
Denial of Service Attacks	Distributed Denial-of-Service-Attack (DDOS) is a breach type characterized by rendering computer resources and services unavailable. (Chen et al. 2012) An attacker carries out a DOS attack by making resources inoperative by taking up so much of a shared resource that none of the resources is left for others to use or by degrading the resource, so that is less valuable to users. (Ettredge & Richardson 2003)
Data Breaches	A data breach occurs when the requirement to notify is triggered by the acquisition, or reasonable belief of acquisition, of personal information by an unauthorized person. (Kamala 2015). Defined as an incident in which sensitive, protected, or confidential data has been potentially, stolen, or used by an unauthorized individual (Rouse, 2016).
Information and Information System Related Security Breach	A security breach is an attack that compromise the confidentiality and integrity of a firm’s data and information assets (e.g., social security numbers, credit card numbers, bank account numbers, driver’s license numbers, and identity theft). (Cardenas 2012) Information security breach where an individual's name plus confidential information such as social security number, credit/debit card records. (S.B. Modi et al. 2015) Security breaches are defined as an announcement from a firm which contains the using the keywords "attack," "breach," and "break-in" in the same search string as the words "hacker," "Internet," and "security." (Cavusoglo, Mishra, Raghunathan 2004) Information security breaches, one must clearly define these breaches and use a reliable and comprehensive technique to measure its impact. In the present research security violations are defined, to avoid any confusion between privacy and security breaches, using the National Institute of Standards and Technology (2007) guidelines, as any external, IT-based act that results in violations of NIST security elements such as identification, authentication, authorization, integrity, non-repudiation, and confidentiality (Singhal, Winograd, and Scarfone, 2007). Information security research is any research where the breach is called any of the following: ((“Information Security” OR “Computer Security” OR “Network Security” OR “Internet Security” OR “Information System Security” “IT Security” OR “Software Security” OR “Application Security”))) from Spanos and Angelis 2016) Security breaches are denial of service attacks, unauthorized access to customer data, unauthorized access to employee data, IB site alteration/defacement, unauthorized access to company data (Yayla & Hu 2011)
IT Security Breach	IT security breaches can include access attacks, modification attacks,

	and DOS attack. A characteristic of a breach is a loss of confidentiality of customer information, the integrity of information, and availability of applications and services." (Cardenas et al. 2008)

Table 3: Common Breach Terms from the Literature

This study will use the term information technology security breach (IT security breach) to refer to one or more of an internet security breach, privacy breach, denial of service attack, data breach, or any information or information system-related security breach event.

Information technology security breach (IT Security Breach) includes one of the following: an internet security breach, privacy breach, denial of service attack, data breach, or information or information system-related security breach event.

3.3 Characteristics of an IT Security Breach

In addition to defining IT Security Breaches, it must also be conceptualized it for this dissertation. In the information systems literature, IT Security Breaches have been conceptualized primarily by the type of breach that has occurred, e.g. a phishing event or virus attack (Bose and Leung 2014; Hovav and D'Arcy 2003). In addition, there are a number of frameworks to classify IT security breach characteristics (see National Institute of Standards and Technology, 2014; Hovav, Andoh-Baidoo, & Dhillion, 2007; U.S.Computer Emergency Readiness Team, 2015). For the purposes of this research, the characteristics of IT security breaches within organizations need to be articulated into a single framework to more thoroughly study these types of events, particularly if empirical testing is to be conducted. In evaluating the literature on IT security breach events, it is noted that IT security breach events are comprised of the following dimensions indicated in Figure 2.

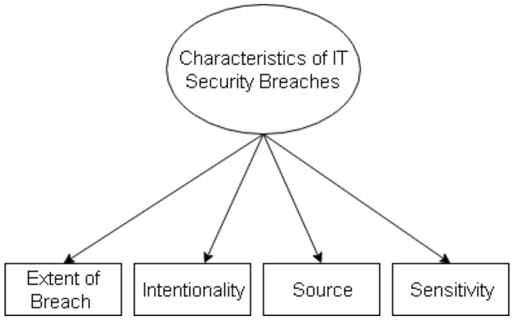


Figure 2: IT Security Breach Characteristics

As noted previously in this chapter, there are many existing frameworks for classifying causes and sources of IT security breach events. The extent of the breach for the purposes refers to both the subjects of the breach and the origins of the breach. The cause of the IT security breach is the action that led to the information technology system being compromised. Section 1.2 articulated that this dissertation would be studying so-called "IT security breaches" and this includes internet security breaches, privacy breaches, denial of service attacks, data breaches, and/ or any information system-related security breach event. There can be many causes of IT security breaches including hacking, malware, payment card fraud, physical loss, lost or discarded mobile devices, lost or discarded stationary devices and the subjects of the breaches can be customers, suppliers, products, services, and staff.

Regarding the breach subject, it can also be sensed that losses related to IT security breaches within organizations may vary depending on whether or not the breach impacted an application interface, the internal network infrastructure or if the breach involved physical IT components such as network cables and laptops. The various layers of an organization’s IT infrastructure can be nicely articulated into a framework called the “OSI Model” (Clark, 2014). However, since there is minimal research on this particular dimension of breach events; it is essential that this characteristic of the IT security breach event be empirically documented.

The second characteristic of IT security breach event is the breach intentionality. For the research purposes, rather simplistic two by two framework is utilized which is based on an actor's intentionality surrounding the breach event and the actors' relationship to the focal organization that was breached. In this way, most all IT security breach events will fit neatly into this framework ranging from denial of service of attacks to incorrect security configurations caused by a trusted employee. Table 4, illustrates the framework for intentionality of an IT security breach event.

Trusted Insider Unintentional	**Trusted Insider Intentional**
Outsider Unintentional	**Outsider Intentional**

Table 4: Intentionality of IT Security Breaches

IT security breach events can be caused by actors within and outside the organization and the actions of these actors can be intentional or unintentional. Breaches can also involve various combinations of the four categories. An insider is defined as an individual currently or at one time authorized to access an organizations information system, data, or network; where such authorization implies a degree of trust in the individual (Greitzer, Moore, Cappelli, Andrews, Carroll, & Hull, 2008). Intentional threats from insiders include fraud, theft of intellectual property, and sabotage (Warkentin & Willison, 2009). Similar to other criminal activity, the intentional insider threat consists of a wide range of actors, motives, and techniques. The Software Engineering Institute at Carnegie Mellon reviewed more than 800 insider threat cases and found that 85 percent of insider threats are trusted internal employees of the focal organization (The CERT Insider Threat Center, 2016). Contractors, subcontractors, and trusted business partners accounted for the remaining 15 percent.

On the other hand, unintentional insider threats are primarily caused by noncompliance and/or social engineering (Silowash, Capelli, Moore, Trzeciak, Shimeall, & Flynn, 2012). Social engineering refers to psychological manipulation of people into performing actions or divulging confidential information. An example of an unintentional insider threat is the accidental disclosure of private or proprietary information by an employee.

Intentional outsider threats fall under the broad moniker of hacking and can include the actor employing such tactics as developing phishing attacks for the purpose of hacking, exploiting weak patches in software and information systems infrastructures, and developing worms that utilize brute force to decode passwords and usernames. More recently, outside actors that engage in intentional threats have been using so-called *advanced persistent threats* or APTs. APTs are a special kind of attack that strategically employs a combination of active and passive threats that utilize both inside and outside actors to gain long-term entrance into an organizations information technology infrastructure (Satin & Bernardi, 2015; Virvilis, Gritzalis, & Apostolopoulous, 2014). The most critical step in an APT is to target the credentials of a network administrator because administrator-level credentials can then provide the nefarious actor the opportunity to exploit an entire organization in an attempt to gain valuable intellectual property such as trade secrets and data. A less common type of IT security breach is the unintentional outsider threat. An error or negligence on the part of the focal firm can cause unintentional outsider threats. Examples of this include an unauthorized outsider accessing secure areas of a company's website or private information being left unsecured online and then inadvertently accessed by an outsider. From the perspective of the focal organization, this can also be considered an unintentional insider threat. This type of IT security breach recently occurred with a voter analytics firm which inadvertently left 198 million voter data unsecured in a cloud database for two weeks. A security researcher unintentionally discovered the exposed records. The data not only included how an individual may vote in elections but also offered insights into those individuals' thoughts on gun control, offshoring, and the auto industry (Lapowsky, 2017). The "source" of the IT security breach describes whom or what was the source of the IT security breach event. The source of an IT security breach event can range from a person to a nation state, organized crime, terrorists, or may even be unknown to the organization. Breach source is the third dimension of an IT security breach.

An IT security breach event can involve leaked information and data on private citizens as well as that of organizations. Certain types of leaked data or information can be considered more private and therefore potentially more damaging than other types of data or information. The sensitivity of the data or information related to the breach event is the fifth dimension of an IT security breach event. There is a number of existing intuition or ad-hoc based frameworks that classify the sensitivity of data or information based on their potential impact (University of South Florida, 2010; Quist, 1993; Clark, 2014; Loch, 1992). For the purposes, sensitive information is defined as any data/information that could potentially harm or hinder the organization in achieving its goals if improperly used. For an organization, this information can include trade secrets, customer lists, unreleased financial reports, and all types of intellectual property. In the context of individuals, sensitive information pertains to such private data/information as social security numbers, credit card numbers, and health information and in some cases includes email addresses and phone numbers. The US-CERT Federal Incident Notification Guidelines is the framework that is used in this dissertation to articulate the sensitivity of the data, information, and/or systems that were breached (Department of Homeland Security, 2014)

In summary, this chapter identified four of the most salient dimensions of an IT security breach event that can be articulated as the extent of the breach, reach of the breach, intentionality, source, and sensitivity. In the chapter that follows, organizational responses that may help to mitigate the losses related to IT security breaches on organizations are conceptualized. Chapter 4 consists of a completed research study that includes a literature review and field interviews with executive level IT security practitioners.

CHAPTER 4: STUDY 1 CONCEPTUALIZING ORGANIZATIONAL RESPONSE TACTIC DIMENSIONS

4.1 Prologue

This chapter combines inductive and deductive approaches to conceptualize organizational responses to IT security breaches. In this chapter and the remainder of this dissertation, managerial tactics concerning IT security breaches are referred to as "organizational responses." The conceptualization of the organizational responses are shown in Figure 3 and have three dimensions that include broad organizational response, temporal approach, and organizational response tactic, i.e. the specific action item. This section starts with deriving the broad organizational responses and temporal approaches from the crisis management and organizational resiliency literature. This is followed by a review of the literature on IT security breaches that is utilized to extrapolate the organizational response tactics, i.e. the specific action item that may moderate an IT security breach event.

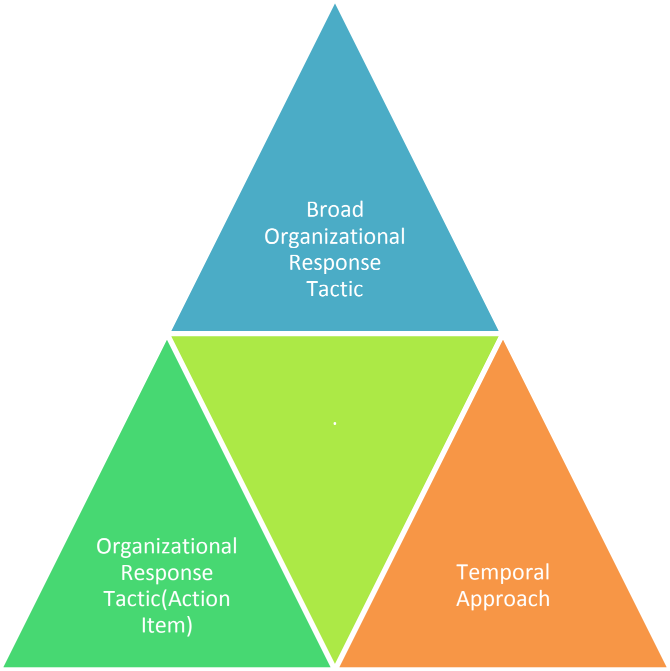

Broad Organizational Response Tactic
Organizational Response Tactic(Action Item)
Temporal Approach

Figure 3: Dimensions of Organizational Responses

Next, the inductive approach is utilized to analyze qualitative data gathered from industry executives with extensive experience in dealing with IT security breaches. We used a semi-structured interview protocol and asked executives to identify some critical IT security breaches they were knowledgeable about and provide information on key organizational mechanisms that were in place before the IT security breach and actions taken after the event. Findings from the literature reviews and interviews are then integrated to illustrate the common organizational responses and their effectiveness in dealing with the IT security breach event.

4.2 Deductive Approach

4.2.1 Insights from Research on Crisis Management

The literature presents multiple definitions for crisis events. Mitroff et al. (1987) defines a crisis as disasters precipitated by people, organizational structures, economics, and/or technology that cause extensive damage to human life and natural and social environments. Organizational crisis have become routine due to human errors; coupled with increasing technological complexities (Pidgeon & O'Leary, 2000; Markus, 2000). In the context of organizations, crisis can cripple the financial structure and the reputation of organizations. Mishra (1996) notes that crisis are events that threaten organizational survival, have little response time, and involve unstructured events which have not occurred before and for which resources are inadequate to cope. Shrivistava and Mitroff (1987) noted that there can be different types of organizational crises where each crisis results from the organizations interactions with the social environment and the technical environment. Along this same line, Quarantelli (1988) posits that there are community crisis, which crises are caused by natural disasters or technological agents. Regardless of the school of thought crisis can challenge a corporation’s efficiency and viability (Marcus, 1991). The crisis management literature has examined organizational crisis as the Exxon Valdez oil spill, racial discrimination at Texaco, glass found in Gerber baby foods, the bankruptcy of Orange County (Koronis, 2012).

The literature on crisis management and resiliency has identified two broad areas in the process of crisis management (Bundy, Pfarrer, Short, & Coombs, 2016). The first area deals with *pre-crisis prevention* that seeks to reduce the likelihood of any crisis. The second one focuses on *post-crisis management* that deliberates on the key actions taken by executives in the immediate aftermath of a crisis.

Researching pre-crisis prevention a set of management scholars has examined organizational preparedness and stakeholder relationships. Organizational preparedness includes the study of high-reliability organizations – those that have developed the ability to manage unexpected adverse events, and how these organizations developed high reliability. Bigley and Roberts (2001) identified three aspects of high-reliability organizations: (i) mechanisms that allow for changing formal structures, switching roles and migrating authority (ii) leadership support for improvisation through tools, rules and routines and, (iii) mechanisms that allow for enhanced sense-making, i.e. efficient situational awareness. Thus, high-reliability organizations can quickly reorient themselves through changes to internal structures, processes, and culture so that they can proactively prevent breakdowns that can lead to a potential crisis. Other studies on organizational preparedness have pointed to the organizational culture, governance, and compensation structures not only making it more likely for a crisis to occur but also impacting the organization's ability to organize for reliability (Bundy, Pfarrer, Short, & Coombs, 2016; Bigley & Roberts, 2001). Furthermore, pre-crisis prevention research has focused extensively on stakeholder relationships; where having positive relationships prior to a crisis can reduce the likelihood of a crisis occurring. However, negative stakeholder relationships may arise from undue social pressures caused by an organization having one or more stakeholder relationships exert undue pressure after a potential crisis event and can lead to actions such as organizational misconduct (Mazzei & Ravazzani, 2015; Majchrzak, Jarvenpaa, & Hollingshead, 2007). However, once a stakeholder relationship is negative the organization risks a crisis occurring due to the increased likelihood of retaliatory action from that stakeholder (Johansen, Aggerholm, & Frandsen, 2012).

The literature on post-crisis management has identified a number of factors that are effective in dealing with adverse events within organizations. Two of the most discussed factors are 1) the importance of organizational leaders leading the organization following a crisis and 2) situational crisis communication, i.e. managing stakeholder perceptions. Jim et al. (2012) point out that the responsibilities of leading an organization during and after the crisis are much larger than dealing with the tactical aspects of managing the crisis. More importantly, leaders who view crisis as opportunities tend to be more open-minded and flexible than those who view crisis as threats, getting limited in their efforts. Researchers have also found flexible governance structures to be effective in managing organizational crisis (Alpaslan, Green, & Mitroff, 2009). For instance, having independent directors, smaller and flexible governance teams, and clear delineation of accountabilities and responsibilities have been found to be effective than the antithesis (Dowell, Shackell, & Stuart, 2011). Another important factor for organizations in successfully managing adversary events is the ability to adapt and change which can enhance coordination and effective communication (Majchrzak, Jarvenpaa, & Hollingshead, 2007). Finally, researchers have emphasized the importance of corporate communication and public relations to effectively manage crisis (Bundy, Pfarrer, Short, & Coombs, 2016). Mazzei and Ravazzani (2015) demonstrated the adverse effects of neglecting to communicate with employees during a crisis, and on the other hand, Mazzei et al. (2012) showed the positive outcomes that can occur from increased engagement with employees. Some scholars have also pointed out the importance of employees becoming outspoken defenders of the organization after the crisis (Frandsen & Johansen, 2011; Johansen, Aggerholm, Frandsen, 2012)

The dominant theory regarding stakeholder perception management is situational crisis communication (Coombs 1995 and 2007) and is based on the notion that the more that stakeholders perceive an organization to be responsible for a crisis the more likely that these stakeholders will have a negative perception of the organization. Attributions of stakeholder perceptions, however, can be negotiated and are subject to social influence (Bundy & Pfarrer, 2015). There are many methods to achieve this including defensive strategies include denial, defiance, and scapegoating and accommodative strategies such as apologies, expressions of sympathy, and promises of corrective actions, manipulating the timing and source of response, bundling negative news with positive news, information to enable stakeholders to avoid harm.

4.2.2 Insights from Research on Resiliency

All organizations are prone to crisis event with some organizations declining after a crisis and other becoming resilient. Although crisis might force organizations to question their mortality, it can lead to either positive or negative organizational losses (Mishra, 1996). Some organizations unexpectedly are able to thrive in the midst of their crisis; these organizations can be considered resilient. Organizational resiliency can also be characterized by an organizations to continue its operations and functions in the midst of a crises. (Bunderson & Sutcliffe, 2002).

Organizational resilience is related to other organizational characteristics such as flexibility, agility, and adaptability. However, resiliency is distinctly different in that firms that are resilient will more than likely exhibit flexibility, agility, and adaptability. Where flexibility is the ability to change on short notice, agility is defined as the ability to develop and implement competitive strategies quickly, and adaptability is the ability of the organization to reintegrate into the environment (Ghemawat & Del Sol, 1998; McCann, 2004; Chakravarthy, 1982). Furthermore, resilience is triggered by an unexpected event or traumatic organizational strain. Based on the definitions of organizational resilience it can be viewed in one of two ways 1) In the post- crisis management context, as an emerging characteristic that is triggered by some event or strain 2) In the pre-crisis management context, as an existing characteristic within an organization. Regarding the post-crisis management view, resilience is a dynamic capacity of organizational adaptability that grows and develops over time (Somers, 2009). It is not considered an inherent attribute within a firm. Instead, it is a byproduct of an organization's interactions with its resources and processes in which resources can become sufficiently flexible, storable, convertible, and malleable which will enable the organization to cope positively with an unexpected event (Sutcliffe & & Vogus, 2003). Furthermore, organizations in which characteristics such as learned resourcefulness, ingenuity, and bricolage are part of the day-to-day operations are more likely to be able to devise unconventional, responses to unexpected challenges and situations such as crisis events (Coutu, 2002). The important caveat is that these characteristics within the organization will only become apparent after a crisis event the organization may not necessarily be consciously taking advantage of or even aware it possesses those traits.

The skills and competencies that lead to learned resourcefulness can improve with experience and practice (Eisenhardt & Tabrizi,1995; Senge, Roberts, Ross, Smith and Kleiner, 1994). In the pre-crisis management view, organizational resiliency is viewed as a conscious and existing characteristic within an organization especially those in turbulent, uncertain, and threatening environments. These organizations may be constantly bombarded by discrete errors, scandals, crisis, shocks, and disruptions of routines leading to constant stresses and strains. Resilient firms actually thrive and become better in part because they have previously faced challenges. Organizations that not only survive but also excel despite ongoing stresses and strains possess resilience; it is a characteristic inherent in the organization. These organizations are consciously aware and take advantage of harnessing and pivoting their resources to address challenges in the midst of stresses and strains. .

In a turbulent, uncertain, and threatening environment, only flexible, agile, and relentlessly dynamic organizations will become resilient, i.e. consistently exceed performance expectations. These organizations are consciously aware of this, and they may move beyond survival to gain long-term competitive advantages and profitability. In addition, resilient organizations within these types of environments presume that challenges and unexpected events can be a source of opportunity not just necessarily a threat and they attempt to capitalize on potential risks (Barnett and Pratt, 2000; Jackson & Dutton, 1988). These organizations may be in a constant state of transformation as a byproduct of its resiliency characteristics (Sutcliffe and Vogus, 2003). Resilience in the general management literature has been widely discussed (Alexander 2013; Sutcliffe & Vogus 2003) where most of the effort has focused on defining and operationalizing the concept (Ghemawat & Del Sol, 1998; McCann, 2004; Chakravarthy, 1982). The extant literature has found that organizational resilience has specific elements of capability endowments to ensure that practices are organized, the organization is durable and to enhance post crisis response. Essentially this is the knowledge, skills, abilities, and processes that facilitate access to and manipulation of resources (Bonanno, Brewin, Kaniasty, & La Greca, 2010; Hobfoll, 1989). The capability endowments include 1) financial 2) cognitive 3) behavioral 4) emotion regulation and 5) relational. Financial capability endowments is a type of capability of durability in which an organization stockpiles resources in anticipation of adversity (Bradley, Shepherd, & Wiklund, 2011; Carmeli & Markman, 2011; George, 2005; Virany, Tushman, & Romanelli, 1992) cognitive capability endowments enable organizations to notice potential adversity and combine and deploy intellectual capital (Lengnick-Hall et al. 2011; Thomas, Clark, & Gioia 1993; Iick 1995). Behavioral capability endowments consist of repertoires of potential actions and behaviors embedded within the organization (Galbraith, 1973; Thompson, 1967). An emotion-regulation capability endowment refers to the notion that organizations can enhance resilience by cultivating emotions such as optimism, hope, and openness (Avey, Luthans, & Jensen 2009; Luthans, Avolio, Walumbwa & Li, 2005). Relational capability endowments provide the environment for the cognitive, behavioral, and emotional capabilities and focuses on the social connections (Shin, Taylor, & Seo, 2012; Baron, Franklin, & Hmieleski, 2016).

4.2.3 Insights from Research on Business Continuity & Disaster Recovery

A disaster can be defined as non-routine events in a community that have the potential to cause human harm and social disruption. An event is the specific occurrence of a disaster (Rao, Eisenberg, & Schmitt, 2007). A hallmark characteristic of a disaster is the incapability of the community to cope using its resources (Alexander, 1997). Disasters have typically referred to social communities. However, a disaster can also impact organizations and furthermore the organization may precipitate a distater through its actions, i.e. cause human harm and social disruption. These events while also crisis can also threaten the continuity of a focal organization. Hecht (2002) posits that business continuity management is an evolution from disaster recovery planning, in that business continuity planning focuses on core organizational functions and their continuance. The literature on business continuity encompasses all organizational types and focuses on business systems. However, as business systems and IT systems become increasingly integrated, it is essential that the lens of business continuity evolve to consider the new, highly digitized environment. Niemimaa (2015), in a review of business continuity literature, notes that the literature covers three perspectives: 1) integration and understanding of organizational capabilities, 2) ensuring that standard organizational are restored after a disruptive event, and 3) achieving an organizational state to continue operations.

Customers now expect that businesses operate continuously in order to survive. Most organizations have business continuity plans in place, but many but do not have an actual methodology to implement their business continuity plans; nor do they have maintenance procedures for business continuity, continuous education, and engagement of organizational stakeholders including employees in their plans (Botha & Von Solms; 2002). To resolve these issues, the authors suggest a multicyclic approach to business continuity planning in which there is a backup cycle, disaster recovery cycle, contingency planning cycle and continuity planning cycle. Hecht (2002), notes that business continuity planning in the context of IT systems should not only consider IT security threats such as human error and hacking but also environmental threats such as network outages, arson, earthquakes, floods, and hurricanes, as they all pose risks to the IT systems. Hecht suggests a single point of contact in the organization to handle these risks and that organizations should view business continuity planning as an ongoing process subject to organizational evolution.

Lindstrom et al. (2010), argues that during the planning and development for business continuity plans as well as training for business continuity plans there is no reliable method in place to explain the importance of such exercises to senior management. Without senior management, full engagement business continuity becomes a checklist of items in case of a crisis when it should be embedded into the organization. The senior management needs to understand that during the planning, development, and training phases of business continuity planning is when real threats to business continuity are evaluated and senior management needs to be at the proverbial table when that happens. Furthermore, Jarvelainen (2013) found that embeddedness of business continuity practices can decrease negative impacts to the business from IT incidents specifically those incidents that lead to data unavailability.

4.2.4 Integration of crisis Management, Resiliency, Business Continuity & Disaster Recovery Literature

In the previous three sections, the insights from the crisis management, resiliency, and business continuity & disaster recovery academic literature were discussed. Despite the extensive extant literature in crisis management and organizational resilience, there has been a relatively little discussion of the relationships between resilience and crisis management (Comfort, Boin, & Demchak, 2010). This in part can be explained by the fact that each literature stream views organizational adversity in its unique way. In the crisis management literature, the focus is on understanding the causes, dynamics, and the aftermath of crisis events, whereas most of the focus in the resiliency literature is on how organizations can resist the negative losses of adversity. Recent research has sought to integrate the crisis management and resiliency literature as crisis can be not only adversarial but also evolutionary for an organization. By integrating the two literature streams, researchers will be better able to understand how organizations are not only able to adjust but even thrive after a crisis (Williams, Gruber, Sutcliffe, & Shepherd, 2017). Hence, the literature is integrated for better understanding organizational IT security breach events.

From the three literature streams of crisis management, resiliency, and business continuity & disaster recovery; the seven broad organizational responses were derived and are summarized in Table 5. The seven broad organizational responses include e *liability management, governance, communication management, IT resource management, security strategic thinking, morale management, and relationship management.* These broad organizational responses are then used to classify specific organizational responses from the IT security breach literature. Table 5 presents descriptions of each of the seven broad organizational responses. As stated previously, the literature on crisis management and resiliency have identified two broad areas in the process of crisis management, i.e. pre- crisis prevention and post-crisis management (Bundy, Pfarrer, Short, & Coombs, 2016). For the purposes of this research study, these two broadly identified approaches to organizational responses to manage IT security breach events are referred to as the 1) *proactive*, prevention approach to minimize the possibility of IT breach, and the 2) *reactive* approach to manage the crisis after an IT security breach occurs.

Broad Organizational Response Tactic	Description	Source
Liability Management	Organizational response actions pertaining to legal and financial liabilities that could arise from potential adverse events.	Bundy et al. 2016; Bradley, Shepherd, & Wiklund 2011; Carmeli & Markman, 2011; George 2005, Virany, Tushman, & Romanelli,1992
Governance	Organizational response actions pertaining to the creation or modification of formal and informal structures and mechanisms focused on accountability and response to an adverse event.	Bundy et al. 2016; Bigley and Roberts 2001; Lindstrom et al. 2010.
Communication Management	A set of organizational responses and strategies pertaining to formal and informal communication about adverse events with both internal and external stakeholders.	Majchrzak, Jarvenpaa, & Hollingshead, 2007; Frandsen & Johansen, 2011; Johansen, Aggerholm, & Frandsen, 2012; Bundy & Pfarrer, 2015
IT Resource Management	Organizational response actions pertaining to hardware, software, telecom, and digital infrastructure and IT related resources within organizations.	Pidgeon & O'Leary, 2000; Markus, 2000Lengnick-Hall, et al. 2011; Thomas, Clark, & Gioia 1993; Lick 1995; Niemimaa, 2015
Security Strategic Thinking	Organizational response actions at the senior level to enforce security related awareness and thinking across organizational business units.	Galbraith, 1973; Thompson,1967; Lindstrom et al. 2010.
Morale Management	Organizational response actions to enforce or maintain a healthy psychological climate within the organization.	Avey, Luthans, & Jensen 2009; Luthans, Avolio, Walumbwa & Li, 2005; Lindstrom et al. 2010.
Relationship Management	Organizational response actions pertaining to (i)external relationships with IT vendors, consultants, suppliers, partners and (ii) internal business units	Shin et al., 2012, Baron et al., 2016; Hecht 2002

Table 5: Broad Organizational Responses to Adverse Events from Business Continuity, Disaster Recovery, crisis Management, and Resiliency Literature Streams

4.2.5 Insights from Literature on IT Security Breaches

The previous section utilizes the crisis management and resiliency literature to derive seven broad organizational responses to adverse events. This section focuses on deriving organizational response tactics specific to IT security breach events. The literature on IT security breaches regarding organizational responses is best described as sparse and prescriptive with vendor-oriented literature and with very few empirically grounded studies. Early IT security breaches had the potential to lead to catastrophic losses in that they were considered crisis events. Presumably, this perspective has caused continued interest by information systems researchers in the value declining, financial perspective of these events on firms and technical researchers have focused on ensuring security at the application level at the expense of strategy development in response to these events.

As stated in Chapter 2, much of the IT security literature has focused on changes to market values, with organizational responses considered secondary to understanding the financial losses of these events on firms. The organizational responses are typically conceptualized as moderators in the form of simple binary or categorical variables, or the research may focus on a specific research question from which the solution can only come from a pre-defined solution set forth by the authors. Through a review of the literature on IT security, the seven broad organizational responses are classified into those responses pertaining to *technology, organizational strategy, and processes***.** A pragmatic approach is taken to define technology, organizational strategy, and process tactics. Technological tactics can be defined as organizational responses that are related to technology. These include broad organizational responses such as IT resource management and relationship management. Organizational strategy tactics can be defined as those organizational responses, which are used to set priorities, focus energy, and resources, strengthen operations, and ensure that employees and other stakeholders are working toward common goals (O'Dell & Combes, 2009). Organizational strategy tactics also pertain to tactics that ensure the organization can assess and adjust responses to a changing environment. Organizational strategy tactics include security strategic thinking and governance activities. Process-based organizational responses are any series of actions or operations within one or more organizational business units but are not technology based.

Process-based organizational responses include liability management, morale management, and communication management.

Broad Managerial Category	Broad Managerial Tactic Definition
Process	Process-based managerial tactics are any series of actions or operations within one or more organizational business units that are not technology based. Process-based broad managerial tactics include liability management, morale management, and communication management.
Organizational Strategy	Organizational strategy tactics are defined as those managerial tactics that used to set priorities, focus energy and resources, strengthen operations, and ensure that employees and other stakeholders are working toward common goals. Organizational strategy also pertains to the organization's ability to assess and adjust to a changing environment. Organizational strategy tactics include security strategic thinking and governance activities
Technological	Technological tactics can be defined as managerial tactics that are related to technology. These include broad managerial tactics such as IT resource management and relationship management.

Table 6: Broad Managerial Categories of Organizational Responses

This sub-classification of the broad organizational responses was helpful in the initial identification and classification of IT security breach organizational responses from the literature. In addition, organizational responses were classified as proactive or reactive or both, and research type was denoted as academic or practitioner. The classification of academic or practitioner was dependent on whether the intended audience is frontline practitioners or other researchers. To derive the specific organizational response tactics, a semi-structured literature review was conducted by first utilizing a keyword search in the IS scholars' basket of 8[1] For the term’s "cybersecurity" and "information security" and "breaches." From these articles, forward and backward searches of the literature were then conducted. After the academic literature review was conducted, a search and review of the practitioner research ensued. This consisted first of a review of articles published in standard academic and practitioner research outlets such as Harvard Business Review . Second, a review of the research, guidelines, and reports published

[1] The Information Systems (IS) Basket of 8 refers to the list of the most recognized academic research journals for information systems research. The IS Basket of 8 includes the following: European Journal of Information Systems, Information Systems Journal, Information Systems Research, Journal of AIS, Journal of Information Technology, Journal of MIS, Journal of Strategic Information Systems, MIS Quarterly. Source: Association of Information Systems https://aisnet.org/page/SeniorScholarBasket

by the United States government commenced. This was followed by a review of the literature in which cybersecurity industry certifications are based.

It should be noted that the IT security industry has a long-standing developed body of knowledge for which practitioners receive certifications validating their expertise. Such certifications include CISSP, Security+, and Certified Ethical Hacker among others. Lastly, a search and review of white papers published by professional organizations and associations ensued. Tables 7-13 that follow are the results of these reviews.

Liability Management Tactic Constructs	Temporal Approach	Academic Research	Practitioner Research
1.Obtaining cyber insurance coverage	Proactive	Young et al., 2016	NAIC, 2017
2. Review of contractual protections and vendor liabilities related to breaches	Proactive	August & Tunca 2011	X
3. Purchasing cybersecurity insurance to manage regulatory compliance	Proactive	Trang,2017	Department of Homeland Security, 2016
4. Liability provisions in contractual agreements with external organizations who collect, store, use or access data	Proactive	Sherwood, 1997	AAAA.org,2016
5. Post-breach review of vendor liability policies	Reactive	X	X
6. Review of current cyber-insurance provisions after the breach	Reactive	X	AAAA.org,2016
7. Additional insurances for addressing potential future breaches	Reactive	Zhao et al. 2013	Johnson et al. 2016

Table 7: Liability Management Organizational Response Tactics

IT Resource Management Tactic Constructs	Temporal Approach	Academic Research	Practitioner Research
1. Dedicated team for real-time monitoring	Proactive	Bhatt et al., 2014	Torres, 2015; InfoSec Institute, 2017
2. Automated security incident management systems	Proactive	Li et al., 2016; Mitropoulos et al. 2007	Haber, 2013
3. Use of advanced biometric authentication techniques	Proactive	Mohammad & Stergioulas2010	Gibson D., 2014; Clarke, 2013
4. Use of device specific or location based authentication methods	Proactive	Whitley et al. 2014, Steinbart et al. 2016	X
5. Regular assessment of IT security risks (e.g., vulnerability scanning, penetration testing, etc.)	Proactive	Jamieson & Low, 1990, Sun et al. 2006; August, T., & Niculescu, M. F. 2013	Basu E., 2013; Scarfone et al. 2008
6.Mock crisis-exercises for managing potential IT security breaches	Reactive	Iqbal et al. 2016	**X**
7. Hiring of additional IT security staff	Reactive	**X**	
8.Resizing of internal teams	Reactive	**X**	**X**
9. Investments in newer systems or applications for IT security	Reactive	Wu et al. 2015; Kwon, J., & Johnson, M. E. 2014	Gelbstein, 2015

Table 8: IT Resource Management Organizational Response Tactics

Relationship Management Tactic Constructs	Temporal Approach	Academic Research	Practitioner Research
1. Adequate coverage of IT security issues in agreements with suppliers, customers, and other business partners	Proactive	Berghmans & Van Roy, 2011; Sutton et al. 2008	IBM, 2015; ISACA, 2017
2. Engagement of external partners in reviewing IT security arrangements	Proactive	Ransbotham & Mitra 2009; Robnage et al. 2014; Kim et al. 2015	Shinn, 2008
3. Periodic review of security and privacy policies and practices of business partners	Proactive	Arora et al.,2010; Bossong, R., & Wagner, B.,2017	**X**
4. Periodic review of agreements and work arrangements with IT security vendors	Proactive	Lee et al. 2012	**X**
5. Post-breach review of IT security provisions in agreements with business partners.	Reactive	**X**	Experian, 2013; Filkins & Fogarty 2015; AAAA.org 2016
6.Discussion with affected external parties	Reactive	**X**	Experian, 2013; Filkins & Fogarty 2016
7.Changed agreements with IT security vendors	Reactive	**X**	Experian, 2013; Filkins & Fogarty 2017

Table 9: Relationship Management Organizational Response Tactics

Communication Management Tactic Constructs	Temporal Approach	Academic Research	Practitioner Research
1. Decide on the extent of information disclosure pertaining to the breach.	Reactive	Hinz et al. 2015; Gordon et al. 2010	**X**
2. Timely notification of the security incident to all internal and external stakeholders.	Reactive	**X**	Gordon, 2006
3. Clear, strategy-based public relations response about the breach.	Reactive	**X**	Silverman,2016
4. Designation of specific personnel to communicate about any IT security breaches	Proactive	**X**	Rogers & Traurig, 2016
5. Official plan for communicating internally and externally in the event of a breach	Proactive	**X**	Wired.com 2011

Table 10: Communication Management Organizational Response Tactics

Security Strategy Management Tactic Constructs	Temporal Approach	Academic Research	Practitioner Research
1. Engagement of senior business executives	Proactive	Wang et al. 2012; McFadzean et al., 2007	**X**
2. Formal plan for managing IT security	Proactive	Sen & Borle, 2015;Hovav & D'Arcy 2003;Kannan et al 2016	Elky, 2007
3. Formal training program(s) to increase IT security awareness	Proactive	D'Arcy et al. 2009; Puhakainen & Siponen, 2010; Hu et al. 2012	Sanghavi, 2015; Deloitte Canada, 2017; Egan, 2015
4. Implementing non- technical solutions such as deterrence, deception, detection in order to protect information systems	Proactive, Reactive	Ahmad et al. 2012; Werlinger et al.; Evans et al. 2004	CERT, 2017
5. Comprehensive coverage of all digital assets (hardware, software, and applications) and data hosted internally as well as externally.	Proactive	Vurukonda & B.Thirumala, 2016;Fernandez-Medina et al2007	Sanderson, 2011
6. Coverage of external IT vendors or third parties we use for any IT or data related work.	Proactive	Arora et al. 2010; Hui et al. 2012	**X**
7. Coverage of employee-owned IT, mobile devices and digital accessories	Proactive	Oetzel & Spiekermann, 2013	**X**
8. Investments in IT security	Proactive	Cavusoglu et al. 2009; Wang et al. 2008	Gordon et al. 2003; Kassner, 2015
9. Post-breach ad-hoc planning	Reactive	Njenga & Brown, 2012	**X**
10. Review and revisions to any existing IT security plan	Reactive	Parks et al. 2016; Baskerville, R., Spagnoletti, P., & Kim, J. 2014	**X**
11. Post-breach investments	Reactive	Angst, Block, D'Arcy, & Kelley, 2017	Zacks Equity Research 2017

Table 11: Security Strategy Management Organizational Response Tactics

Morale Management	Temporal Approach	Academic Research	Practitioner Research
1. Engagement of employees enterprise-wise on IT security issues	Proactive	Ifinedo, 2012; Siponen et al. 2014	**X**
2. Reward and punishment approaches for compliance/non-compliance	Proactive	Chen et al, 2012; D'Arcy et al, 2009;Moody et al 2017;Siponen & Vance, 2010	**X**
3.Autonomy to IT professionals to handle breach mitigation response	Proactive	Irlinger, 2009	**X**
4.Post-breach discussion with employees	Reactive	**X**	Hess, 2015; Leonard, 2015
5.Periodic updates regarding IT security related developments and issues	Proactive	**X**	X
6.Specific activities to boost employee morale after the breach	Reactive	**X**	Heiser, 2017; Leonard 2015

Table 12: Morale Management Organizational Response Tactics

Governance	Temporal Approach	Academic Research	Practitioner Research
1. Establishment of a senior position for overseeing IT security	Proactive	Z.A. Soomro et al., 2016; Hu et al. 2007	International Organization for Standardization, 2013
2. Shared responsibility for IT security between IT and functional units		Spears & Barki, 2010; Hsu et al. 2014	**X**
3. Establishment of formal procedures and rules for managing IT security incidents	Proactive	Rebollo et al. 2015; Anderson & Choobineh, 2006	IT Governance Institute, 2006
4. Implementing one or more international standards	Proactive	Hidayah et al. 2014; Backhouse et al. 2006; Hsu, 2009	National Institute of Standards and Technology, 2012; Kanatov et al. 2014
5. Formal unit or team to handle IT security	Proactive	Rajivan et al. 2013	Ghosh, 2014
6. Ad-hoc teams to manage the fall-outs	Reactive	Reed et al. 2014;Steinke et al., 2015	**X**
7. Contract with an external vendor to manage the incident and fall-outs	Reactive	Cezar, et al. 2013	**X**

Table 13: Governance Organizational Response Tactics

4.3 INDUCTIVE APPROACH

4.3.1 Study Design

IT security breaches have the potential to inflict considerable damage upon organizations. Researchers are still unclear about what occurs within organizations surrounding the broader function of the information security domain. This section discusses the qualitative field study that was undertaken to understand organizational responses surrounding these events.

The target sample for this qualitative study were practitioners who were leaders of the information security function within their respective organizations and who would have had experience with IT security breach events. Depending on the size and complexity of the organization, these roles ranged from director to executive vice president. To begin, a list was created of Chicago based organizations that experienced an IT security breach event over the last five years, and an internet search engine was utilized to 1) determine who was responsible for the IT security function within these organizations 2) obtain contact information for these individuals. The list consisted 90 firms, and contact information was obtained for 27 of those firms. Individuals within those organizations were contacted via a preformatted form letter on the professional social networking site "Linkedin.com," and via publicly available business emails, three people responded. One of the respondents was able to utilize his personal contacts to secure an additional four interviews for the study. Six interviews were conducted across seven participants. A summary description of participants is noted in Table 14. The interviews utilized a semi-structured interview questionnaire, and the participants received the script prior to the interviews. The interview questions were developed from gaps in the literature. The interview script for the interview questions is located in (Appendix A). The interview questions focused on the IT security breach event in the context of organizational technologies, business processes, governance, strategy, and human resources. In addition, based on the responses from the study participants probing methods were utilized to obtain additional information on the research constructs. Respondents were also asked if there were questions that we should have asked but did not and built these questions onto the interview script for subsequent interviews.

Respondent	1	2	3	4	5	6	7
IT Experience(Yrs.)	23	32	20	12	19	23	28
IT Security Experience(Yrs.)	17	30	20	3	5	19	17
Primary Organization Type	Public	Private	Public	Public	Private	Public	Private
Primary Industry	Public Services	Financial Services	Technology	Transportation	Education	Healthcare	Education

Table 14: Semi-Structured Interviews Respondent Demographics

The respondents were promised that their identities and organizational affiliations would be kept in complete confidence.

4.3.2 Qualitative Analysis of Interviews (Method)

The qualitative analysis of interviews was conducted in three steps. The data collected from the interviews were in the form of detailed field notes of the interview conversation including quotes for salient points. In the first step, field notes were aggregated into a single Microsoft Word document and coded based on whether the temporality was prior to the IT security breach or after, i.e. proactive vs. reactive. The purpose of this was to illustrate and tell the story that occurs when an IT security breach happens in an organization. Kendall & Kendall 2012 noted that storytelling could be an important qualitative research method and researchers can understand a story through reacting, matching, eliciting, and collaborating. Sections 4.3.3 and 4.3.4, integrate the salient quotes from the IT security executives to illustrate proactive and reactive organizational responses to an IT security breach. In the second step, related themes and their associated quotes were arranged together. The emerging organizational response tactics were classified into the three broad managerial tactics of process, organizational strategy, and technological. This was the same initial classification utilized for the IT security breach literature review. It should be noted that some themes did recur across multiple broad managerial tactics. In the third and final step, salient quotes were matched into the organizational response tactic framework as supporting evidence of the organizational response tactics where the academic and practitioner research served as primary evidence for the existence of a particular organizational response tactic. The results of this exercise are noted in Tables 15-21. Lastly, from the rich longitudinal information on proactive and reactive responses to IT security breach events, two mini-cases are developed highlighting variables and constructs. The purpose of the mini-cases is to show how the qualitative assessment informs the research by providing ground-level truths for the literature review findings and their integration with the informal interviews.

4.3.3 Proactive Organizational Responses

At the functional, technical level, the organization may employ prevention and detection tactics, however; resources are not spent equally amongst these two tasks. One participant noted that most Americans have had their data stolen, and it is well known that there are daily breach events. This may cause some organizations to assume that a breach event will occur no matter how robust its IT security program. One participant noted that,

"In the last few years, firms have shifted from more prevention mode to detection mode. There is an underlying assumption that they will get in no matter what; can we detect them when it happens? Companies are sloppy about preventions many companies are not very strong on the prevention side, and they overcompensate by focusing on detection." Respondent #3

In preparation of an IT security breach event, an organization may begin to think about the impacts of a potential event on the entire enterprise, especially for events it has not experienced before. This perspective is that of an enterprise risk management view. However, in many organizations, the IT function is still solely responsible for IT security. The measurement losses are based on what occurs within and to the IT function. Respondent #6 states the following:

"Well, you typically have incident response process in place to respond to the event, eradicate the event, and do forensics on the event. Forensics is dicey when it gets to that point a lot of IT teams may want to try and to handle things themselves may not get to that point. The IT processes typically have those in place (processes for security management). It is the other business processes that are typically lacking. Many organizations for the most part already have processes in place to handle the event. If they do have processes in place, IT will have them. Respondent #6

Smaller organizations despite having an IT function may be proactive in managing potential events by entering into outsourcing arrangements with third parties. However, there is a risk when organizations engage in outsourcing arrangements.

"Some small companies do not have forensic capabilities. They think that third-party organizations can help to fill the gaps. The organization may begin to look at outsourcing some of the IT function. There are a lot of the third-party service providers. Organizations will be looking to see if some of the operations can be done by a managed service provider. Security operations center activities a good place to have the organization outsource the tasks. Amazed at companies which have 1-2 people, this is not good enough. You cannot completely outsource stuff." Respondent #1

Some organizations, however, have robust IT architectures as an inherent part of their business processes and essentially a disruption in the information systems is a disruption to one or more business functions. An IT security breach event no longer is just an IT issue. An organization may begin to actively incorporate the participation of other functions such as legal in the IT security breach event management processes via periodic scenario modeling exercises.

"So we have different use cases for different things, data security, data vulnerability, data loss, privacy. We can name them all generally as workbooks, this includes people you need to call at the beginning of the process, people you need to call later in the process, It is very thorough." Respondent #4

With scenario modeling exercises involving multiple organizational stakeholders and complex use cases, the organization may begin to automate these exercises to ensure that plans are robust.

"Software available now to do simulation rather than table topics it helps to get all parties engaged. Typically, they do not start out as a security incident. Maybe just service unavailable. Might be a systems area or security area. Depending on the type of incident, the breach of customer's information can have a significant impact because it may have implications for the customer's." Respondent #2

During the interviews, it was noted that many proactive resiliency tactics centered around the legal and governance concerns. The legal and regulatory environment drives organizational governance. Governance is driven by an organization's need to increase revenue and value, manage cost and complexity, and ensure the survival of the company through risk management mechanisms (Thomas, 2006). The purpose of corporate governance is to foster ethical behavior, enhance the reputation of the organization, comply with applicable laws and regulations, and ensure the business is efficient and effective (Willis, 2005). For instance, when a potential security incident occurs that does not necessarily mean it was a breach, IT may work with the legal department to determine if the security incident is a breach and if so, work on notifying the Chief Information Security Officer and the Chief Technology Officer.

"There is a greater appreciation in the business that this about protection of information and that we are in compliance with laws and regulations and that we reduce the liabilities of the companies. Moreover, it enables the business to do things that they would not be able to do otherwise. We think management has that now. So, the issue has moved up to the boardroom. Security is still within the IT organizations. In fact, most security officers report to a CIO officer in 60% of organizations." Respondent #1

The organizational governance initiatives play a strong role in the organization's proactive resiliency tactics. A participant noted that good governance reduces the likelihood and potential losses of breach however it does not prevent them. Another participant took a more pragmatic view of governance and believed it could be segmented into requirements and best practices, and there is a strong line of demarcation between the two. These two views can lead to varying organizational losses.

"Think of the world as compliance and security. Most publicly traded companies have some compliance or regulatory framework they must prescribe to whether its SOX, HIPAA, PCI, FERPA, there are requirements out there, then best practices such as COBIT. There are best practices, and then there are requirements. It is important to tease the two. It is important because organizations that say they are compliant are not necessarily secure however organizations that are not compliant to regulatory or best practice frameworks we can guarantee that they are not secure." Respondent #1

4.3.4 Reactive Organizational Responses

Notably missing from the literature and extensively brought up during the semi-structured is the reputation management processes stemming from IT security breach events. The extant literature has already documented that the actual breach disclosure itself is a negative event that has been publicly disclosed about an organization which in turn losses stock prices (for some examples see Cavusoglu, Mishra, & Raghunathan, 2004; Chen, Li, Yen, & Bata, 2012; Garg, Curtis, & & Halper, 2003; Spanos & Angelis, 2016; Acquisti, Friedman, & Telang, 2006). As IT security breaches are now daily events organizations can choose whether even to acknowledge the event publicly. With one participant stating that:

“Public relations address the media and can choose or not choose to respond. The information security function has a close relationship with public relations.” Respondent #4

If an organization does choose to release a statement regarding the IT security breach, it will release a statement both internally and externally, and organizations with specialized public relations functions will release the same statements. With a participant noting

“It is wise that the organization is forthcoming. Internal and external communications are communicated the same way. Therefore, you cannot have different types of communication. Any public statements are repeated internally. If there is more information on internal statement, it will be released, and it will find its way out to the news media. However, you will always have trusted insiders who will know more. ” Respondent #6

“*The good companies put on their website what happened, what customers should do. Bad companies try to shelter the damage. For example, Michaels tried to minimize it by putting it in terms of percentage.” Respondent #6*

A severe IT security breach event may force an organization that did not already have a distinct IT security function to create one distinct from the general IT function. This is true especially if a thorough investigation needs to be conducted this is also important so that IT security leaders can take advantage of resources the organization may now be willing to expend in regards to IT security.

“If the information security function was not already secured off from the information technology function an information security failure may cause this to happen especially if an extensive investigation is being conducted. Information access changes to a need to know basis which warrants information security having its own space.” Respondent #4

From the opinion of Respondent #4, the IS/ IT security function within the organization may find that it requires resources from other functions to better manage the IT security breach event. Furthermore, the organization going forward may include other organizational functions as part of the risk management processes for these events.

“Day to day processes in the organization do not change as much due to an information security failure. However, the information technology processes will change including identification and reevaluation of contractual obligations. Also, there is a discussion about how to improve the event management processes which may warrant discussions with Legal, IT, Finance, and Risk Management." Respondent #6

"Any technology program should have an information security response processes in place. If you do not have one, it is the first thing you (it should) should be across the organization and should include HR, Finance, and Risk, and Legal." Respondent #6

Respondent #6, in summary, notes that other reactive resiliency tactics center on the specific management of the IT security breach events and the decision to insource or outsource the incident response processes. The IT function particularly the IT security function may not have been able to articulate the need for resources and which may cause an organization to have underinvested in the IT security function, which would have only been made apparent after a breach, has occurred.

"Security organization will almost always underinvest in the security because it is not required and the risks and costs associated with a breach are not well understood. So, an org, for the most part, will almost always underinvest in security because the risks are not fully understood, and losses not fully understood. Hard to justify spend and underlying missed opportunity when you cannot clearly articulate the cost of the breach or even the likelihood of the breach, not just likelihood but impact." Respondent #1

Sometimes the organization does not have expertise in a particular breach event type that has occurred or maybe a smaller organization with a handful of IT staff that are also responsible for the security function. One of the study participants made a point that the IT function at best is 35 years old and the information security function is at best 20 years old. Technology has transformed organizations in unimaginable ways, and no business can survive without technology. The information security function itself has not had the time to build clear bodies of knowledge or measures of success that other sectors such as banking have had which is 700 years old and insurance which is 300 years old. These can all be considered mature functions within organizations however information security is not. Another participant stated

"Different companies are at different stages of maturity, and all companies at all stages of maturity are subject to breaches. For some companies, you will have roles established and aligned but in other organizations like Target they did not have CISO." Respondent #2

In cases where the IT functions are not mature or requires additional resources, the organization has to get creative around the incident response processes and the creative use of resources. One way this may be done is via outsourcing. A participant stated that:

"If an event is serious enough you want to operate under client-attorney privilege so that the context related to it is not discoverable with that in mind you engage some type of legal service and the legal service would like to bring in its own forensic analytics and so forth, so it increases the usages of third parties and its primarily to protect the organizations. One of two ways: The service provided by the 3rd party can be good, and you move on. Alternatively, sometimes the 3rd party can drag it out. It is important that the responsibility of the third party relationship be defined making sure scope is defined. If you want, the third party to assist in making sure the perpetrator is not in the environment is one thing but if you want them to do analytics on data is another. That normally included in the service process." Respondent #6

Tables 15-21 present the 7 broad organizational response tactics in the context of the aforementioned interviews where specific tactics that had support from the field interviews are noted with quotes and specific tactics without support from the field interviews are denoted with an “X” in the supporting research column.

Liability Management Tactic Constructs	Supporting Research(Interviews)
1.Obtaining cyber insurance coverage	X
2.Review of contractual protections and vendor liabilities related to breaches	X
3. Purchasing cybersecurity insurance to manage regulatory compliance	X
4. Liability provisions in contractual agreements with external organizations who collect, store, use or access data	X
5. Post-breach review of vendor liability policies	"The information technology processes will change including an identification and reevaluation of contractual obligations." Respondent #6
6. Review of current cyber-insurance provisions after the breach	X
7. Additional insurances for addressing potential future breaches	X

Table 15: Liability Management Organizational Response Tactic Supporting Research

IT Resource Management Tactic Constructs	Supporting Research(Interviews)
1. Dedicated team for real-time monitoring	"In the last few years, firms have shifted from more prevention mode to detection mode." Respondent #3
2. Automated security incident management systems	"There is an underlying assumption that they will get in no matter what; can we detect them when it happens? Companies are sloppy about preventions a lot of companies are not very strong on the prevention side, and they overcompensate by focusing on detection." Respondent #3
3.Use of advanced biometric authentication techniques	**X**
4.Use of device specific or location based authentication methods	**X**
5. Regular assessment of IT security risks (e.g., vulnerability scanning, penetration testing, etc.)	**X**
6.Mock crisis-exercises for managing potential IT security breaches	"So we have different use cases for different things, data security, data vulnerability, data loss, privacy. We can name them all generally workbooks, include people you need to call at the beginning of the process, people you need to call later in the process, It is very thorough. Software available now to do simulation rather than table topics it helps to get all parties engaged." Respondent #4
7. Hiring of additional IT security staff	"Hard to justify spend and underlying missed opportunity when you can't clearly articulate the cost of the breach or even the likelihood of the breach, not just likelihood but impact." Respondent #1
8.Resizing of internal teams	**X**
9. Investments in newer systems or applications for IT security	**X**

Table 16: IT Resource Management Organizational Response Tactic Supporting Research

Relationship Management Tactic Constructs	Supporting Research(Interviews)
1. Adequate coverage of IT security issues in agreements with suppliers, customers, and other business partners	**X**
2. Engagement of external partners in reviewing IT security arrangements	"Some small companies don't have forensic capabilities. Thinks that third-party organizations can help to fill the gaps. The organization may begin to look at outsourcing some of the IT function. A lot of the third-party service providers are looking at some of the operations can be done by a managed service provider. Security operations center activities a good place to have the organization outsource the tasks. Amazed at companies which have 1-2 people which are good not enough. You cannot completely outsource stuff." Respondent #1
3.Periodic review of security and privacy policies and practices of business partners	**X**
4.Periodic review of agreements and work arrangements with IT security vendors	**X**
5. Post-breach review of IT security provisions in agreements with business partners.	"The information technology processes will change including an identification and reevaluation of contractual obligations." Respondent #6
6.Discussion with affected external parties	**X**
7.Changed agreements with IT security vendors	"The information technology processes will change including an identification and reevaluation of contractual obligations." Respondent #6

Table 17: Relationship Management Organizational Response Tactic Supporting Research

Communication Management Tactic Constructs	Supporting Research(Interviews)
1. Decide on the extent of information disclosure pertaining to the breach.	"The good companies put on their website what happened, what customers should do. Bad companies try to shelter the damage. For example, Michaels tried to minimize it by putting it in terms of percentage." Respondent #6
2. Timely notification of the security incident to all internal and external stakeholders.	"The good companies put on their website what happened, what customers should do. Bad companies try to shelter the damage. For example, Michaels tried to minimize it by putting it in terms of percentage." Respondent #6
3. Clear, strategy-based public relations response about the breach.	"Public relations addresses the media and can choose or not choose to respond. The information security function has a close relationship with public relations." Respondent #4
4. Designation of specific personnel to communicate about any IT security breaches	**X**
5. Official plan for communicating internally and externally in the event of a breach	"Internal and external communications are communicated the same way. So, you cannot have different types of communication. Any public statements are repeated internally. If there is more information on internal statement, it will be released, and it will find its way out to the news media. However, you will always have trusted insiders who will know more. " Respondent #6

Table 18: Communication Management Organizational Response Tactic Supporting Research

\

Security Strategy Management Tactic Constructs	Supporting Research(Interviews)
1.Engagement of senior business executives	X
2. Formal plan for managing IT security	X
3. Formal training program(s) to increase IT security awareness	X
4. Implementing non- technical solutions such as deterrence, deception, detection in order to protect information systems	X
5. Comprehensive coverage of all digital assets (hardware, software, and applications) and data hosted internally as well as externally.	X
6. Coverage of external IT vendors or third parties we use for any IT or data related work.	X
7. Coverage of employee-owned IT, mobile devices and digital accessories	X
8. Investments in IT security	X
9. Post-breach ad-hoc planning	"Well, you typically have incident response process in place to respond to the event, eradicate the event, and do forensics on the event. Forensics is dicey when it gets to that point a lot of IT teams may want to try and to handle things themselves may not get to that point. The IT processes typically have those in place (processes for security management). It is the other business processes that are typically lacking. Most organization for the most part already have processes in place to handle the event. If they do have processes in place, IT will have them." Respondent #6
10. Review and revisions to any existing IT security plan	"There is a greater appreciation in the business that this about protection of information and that we are in compliance with laws and regulations and that we reduce the liabilities of the companies. Moreover, also it enables the business to do things that they would not be able to do otherwise. We think management has got that now. So, the issue has moved up to the boardroom. Security is still within the IT organizations. In fact, most security officers report to a CIO officer in 60% of organizations. " Respondent #1
11. Post-breach investments	X

Table 19: Security Strategy Management Organizational Response Tactic Supporting Research

Morale Management	Supporting Research(Interviews)
1. Engagement of employees enterprise-wise on IT security issues	**X**
2. Rewards/punishment approaches for compliance/non-compliance	**X**
3. Autonomy to IT professionals to handle breach mitigation response	"If the information security function was not already secured off from the information technology function an information security failure may cause this to happen especially if an extensive investigation is being conducted. Information access changes to a need to know basis which warrants information security having its own space." Respondent #4
4.Post-breach discussion with employees	"Tell employees to refer to corporate communications to address the situation." Respondent 1
5.Periodic updates regarding IT security related	**X**
6.Developments and issues	
7.Specific activities to boost employee morale after the breach	"Have a secure channel to communicate with folks at different tiers so that they can understand at their level" Respondent#2

Table 20: Morale Management Organizational Response Tactic Supporting Research

Governance	Supporting Research(Interviews)
1. Establishment of a senior position for overseeing IT security	" Historically information security includes all of the governance and privacy mechanisms. They were holistically responsible for these things. What we see now is data as a business advantage. Chief data officer and chief privacy officer. What we are seeing is the overall delegation of responsibilities. Must be joined at the hip with their counterparts. Seeing more of a movement. CISO organization typically reports to IT. The other roles those do not report to IT. The Chief data officer and chief privacy offer is a C-Suite role. Thinks that the CISO will be more important to the CIO. The CIO and CISO will become." Respondent 1
2. Shared responsibility for IT security between IT and functional units	"A lot of the issues that we are dealing with these days are associated with technology issues. A lot of the procedures that should be followed by humans are not being followed. Bad practices and bad discipline. Results in technology risk being exploited." Respondent 2
3. Establishment of formal procedures and rules for managing IT security incidents	"Think of the world as compliance and security. Most publicly traded companies have some type of compliance or regulatory framework they must prescribe to whether its SOX, HIPAA, PCI, FERPA, there are requirements out there, then there are best practices such as COBIT. There are best practices, and then there are requirements. It is important to tease the two. It is important because an organization that says they are compliant are not necessarily secure however organizations that are not compliant to regulatory or best frameworks we can guarantee that they are not secure." Respondent #1
4. Implementing of one or more international standards	**X**
5. Formal unit or team to handle IT security	"Different companies are at different stages of maturity, and all companies at all stages of maturity are subject to breaches. For some companies, you will have roles established and aligned but in other organizations like Target they did not have CISO." Respondent #2
6. Ad-hoc teams to manage the fall-outs	"Any technology program should have an information security response processes in place If you do not have one, it is the first thing you (it should) should be across the organization and should include HR, Finance, and Risk, and Legal." Respondent #6
7. Contract with an external vendor to manage the incident and fall-outs	"If an event is serious enough you want to operate under client-attorney privilege so that the context related to it is not discoverable with that in mind you engage some type of legal service and the legal service would like to bring in its own forensic analytics and so forth, so it increases the usages of third parties and its primarily to protect the organizations. 1 of two ways. The service provided by the 3rd party can be good, and you move on. Alternatively, sometimes the 3rd party can drag it out. It is important that the responsibility of the third party relationship be defined making sure scope is defined. If you want, the third party to assist in making sure the perpetrator is not in the environment is one thing but if you want them to do analytics on data is another. That normally included in the service process." Respondent #6

Table 21: Governance Organizational Response Tactic Supporting Research

4.4 Mini Cases

In this section, two mini cases are constructed from the interview data. In conjunction with the literature reviews, these mini-cases help to highlight the variables and constructs in the study. Selected characteristics of the breach events including proactive and reactive organizational responses and selected organizational losses are highlighted in each mini-case.

Mini Case 1: A Major U.S. Personal Transport Company

The first mini-case involves a major United States personal transport company. This breach was caused by a type of spear phishing attack that targeted a subset of the focal organization's customers. A spear phishing attack is a type of phishing attack that targets a specific person or group of people. Unlike a phishing attack, a spear phishing attack is customized to the recipients(s) in that is it more realistic and specifically addressed to an individual or group of individual, making it more likely that the intended victim will click on the corrupted link. Negative organizational losses from this event were twofold and included competitive losses because of the impact on existing customers and reputational losses such as the loss of goodwill because of bad press.

Prior to the breach event, the organization engaged in a number of proactive response tactics including cross-functional threat modeling exercises and regularly designed and tested use cases as part of its business processes. After the event, the organization involved legal and ethics in the incident response responses. In addition, the human resources dedicated to the IT security function increased exponentially among other organization-specific reactive responses.

Mini Case 2: A U.S. Regional Financial Services Company

The second mini-case involves a U.S. Regional Financial Service Company. This company is considered a small business however assets under control or owned are well over $1 billion. Prior to the IT security breach event, the organization required IT security executives to hold the CISSP (Certified Information Systems Security Professional) certification. In addition, the organization had adequate security incident response plans in place including holding mock exercises twice a year. Furthermore, the organization, being a small company, was self-aware of the phase it was in concerning the maturity of its IT security function.

The breach to the U.S. Regional Financial Services Company occurred because of what essentially an unintentional insider threat which caused a defect in the IT systems. This defect, however, was only considered unintentional (a non-nefarious mistake) after some investigation. The U.S. Regional Financial Services company reacted to the event by first determining if a public notification was required. Second, the organization immediately integrated external and internal labor so that they shared not only the same resources but also shared business processes to prevent a repeat of the processes that lead to the breach event. In addition, there were a number of positive responses to the IT security breach event including exponential increases in executive engagement in mock exercises. The organizational losses for the U.S. Regional Financial Services Company included financial losses and decreased productivity. However, financial losses were decreased because of savvy reactive responses concerning mitigating damages from the breach event.

4.5 Summary of Organizational Response Tactic Derivations

In this chapter, both a deductive and inductive research approach was conducted to document and articulate organizational responses related to IT security breach events. An analysis of crisis management, resiliency, and IT security breach literature was used for the deductive approach. Field interviews with IT security leaders were conducted for the inductive approach. In total, fifty-three distinct organizational responses tactics were identified that organizations utilize to manage an IT security breach event. In the chapter that follows, a discussion of the research model and research model ensues.

CHAPTER 5: RESEARCH MODEL AND HYPOTHESES

5.1 Prologue

To review, in chapters 2-4, key constructs from the conceptual model in Chapter 1 were expanded on and discussed. This discussion included understanding the types of losses organizations can incur from IT security breaches, defining and conceptualizing IT security breach characteristics, and conceptualizing organizational responses to IT security breach events. This research study was commenced by an extensive literature review of academic and practitioner literature to document the types of losses that are related to IT security breach events within organizations. Then utilizing both inductive and deductive research approaches the most common organizational responses to manage IT security breach events were derived. As stated previously, two of the goals of this study are to i) examine if the differences in organizational losses vary due to the varied organizational responses undertaken by the organization before and after an IT security breach event and ii) to understand organizational, managerial strategies pertaining to IT security breaches. In this chapter, the research model noted in Figure 4 is expanded upon for testing through the development of hypotheses.

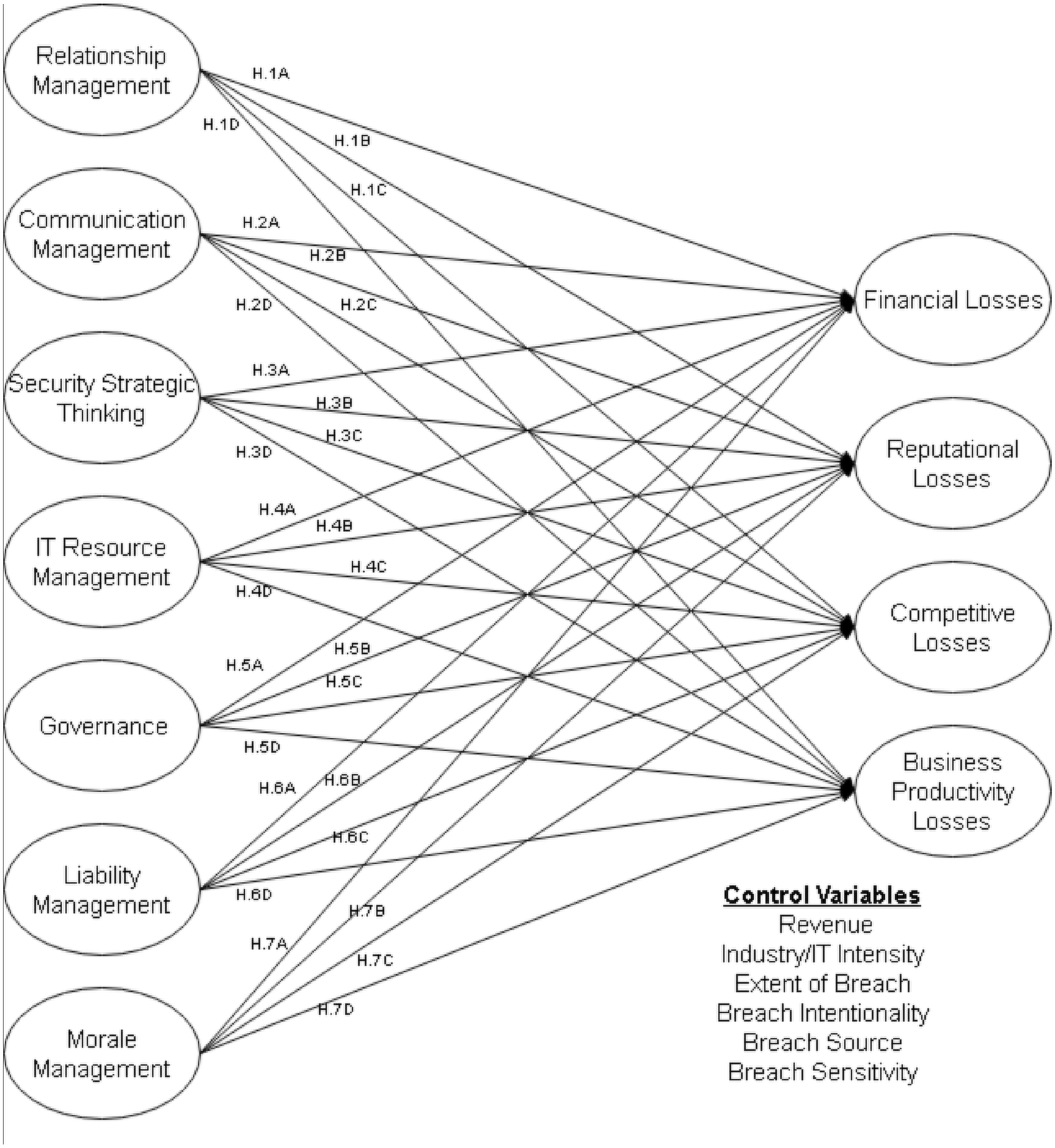


Figure 4: Conceptual Research Model

5.2 Hypotheses

The academic business literature has done little to recognize that losses from IT security breaches can go beyond financial and reputational harm. Intuitively, we know that IT security breaches can have an impact on the technology and operations within organizations and that the incident response lifecycle can play a role in the types and severity of losses from a breach event. Chapter 2 articulated that losses from IT security breach events could also be considered competitive losses and business productivity losses; in addition to financial and reputational losses (where historically these types of losses were measured by changes in the market value of the firm and financial losses are a proxy to measure reputational losses). One of the most important contributions of this research is to understand better the association between organizational responses and organizational losses resulting from IT security breaches. In chapter 4, a theoretical framework of organizational responses to IT security breach events was developed based on the crisis' management, resiliency, business continuity & disaster recovery academic literature streams and the practitioner-based IT security literature streams. This literature review was supplemented by supporting research in the form of interview data and two mini-case studies from executive IT security practitioners. The framework that was developed was then used to succinctly document some of the actions that firms may take to prevent breach events, to better position themselves in case of a breach event, and some of the actions that they may take to manage a breach event after it has occurred. The conceptual model noted in Chapter 1 positions that organizational responses are associated with organizational losses from IT security breaches, where the conceptual model serves to outline the theorized relationships for research purposes. The research model in this chapter allows us to tease out specific relationships between organizational responses and organizational losses.

The research model in Figure 4 consists of the four organizational losses associated with IT security breach events. These losses include financial losses, reputational losses, competitive losses, and business productivity. For this research study, 28 relationships between organizational response tactics and losses are tested. Some relationships are more strongly theoretically motivated than others are; despite this, it is important to test all relationships to understand better and address the research gaps in the extant literature and to assist frontline practitioners in their decision making processes pertaining to IT security breach events which are a tangential goal of this study.

Hypotheses set 1, pertains to the association of relationship management tactics to organizational losses. To minimize the organizational fall out from IT security breach events, organizations need to take steps to manage relationships with external stakeholders. Relationships with external stakeholders are important because positive relationships help to build a store of intangible and tangible resources in case of an adverse event to an organization and after an event successfully managing external relationships may help to reduce losses. For example, successful relationship management can engage external partners such as suppliers, ethical hackers, and other business partners in reviewing IT security arrangements and helping to ensure adequate coverage of known IT security issues (Berghmans & Van Roy, 2011; ISACA, 2017; Kim, Yim, Sugumaran, & Rao, 2015). One such example of a firm successfully managing relationship towards external stakeholders to manage losses after an IT security breach event occurred with the phone carrier T-Mobile. In 2015, over 15 million T-Mobile customers were impacted by a data breach event, which was caused by its credit check vendor Experian (T-

Mobile, 2015). The president of T-Mobile issued a web-based press release that shifted all responsibility for the data breach onto Experian. Experian communicated that they accepted responsibility for the breach event and offered free credit monitoring as remediation to those customers that were impacted (Legere, John, 2015). Less than a year after the breach disclosure the mobile phone company was considered a leader in its industry for profit and new customers with a reported 2.2 million new customers and 13% increase in revenue (T-Mobile, 2016). The following hypotheses are presented for evaluating relationship management tactics in the context of losses from IT security breach events:

H1A: In organizations that experience an IT security breach event, an increase in the extent of relationship management tactics will be associated with a decrease in financial losses

H1B: In organizations that experience an IT security breach event, an increase in the extent of relationship management tactics will be associated with a decrease in reputational losses

H1C: In organizations that experience an IT security breach event, an increase in the extent of relationship management tactics will be associated with a decrease in competitive losses

H1D: In organizations that experience an IT security breach event, an increase in the extent of relationship management tactics will be associated with a decrease in business productivity losses

The next set of hypotheses associates communication management tactics with organizational losses. Organizations can utilize communication as a management tactic for the purposes of social influence and positioning in the context of adverse organizational events, and this includes IT security breach events. Communication management tactics include such as actions as denial, defiance, apologies, manipulating timing, and source of response among other actions, in response to an adverse event on an organization (Bundy & Pfarrer, 2015). Interviews with IT security executives from Chapter 4 note the importance of communicating the same messages to both internal and external stakeholders regarding an IT security breach event and a consistent internal and external message may help to organizational losses. Furthermore, in the crisis management literature, the theory *of situational crises communication* (Coombs 1995 and 2007) is based on the notion that the more that stakeholders perceive an organization to be responsible for a crisis or adverse event, the more likely that these stakeholders will have a negative perception of the organization. Organizations can take actions in the management of their communications before and after an event such as an IT security breach event to manage how they are perceived in the context of an IT security breach event. More mature organizations have readily available communication tactics at their disposal in the case of an IT security breach (Rollo & Tran, 2016). For example, an executive interviewee in Chapter 4 noted that one of the communication management response tactics that they utilized in response to an event was not to issue a public response at all; this was a strategic tactic for the organization to minimize any potential losses. The potential losses from IT security breach events make the intelligent utilization of communication tactics crucial. The following hypotheses are presented for evaluation:

H2A: In organizations that experience an IT security breach event, an increase in the extent of communication management tactics will be associated with a decrease in financial losses

H2B: In organizations that experience an IT security breach event, an increase in the extent of communication management tactics will be associated with a decrease in reputational losses

H2C: In organizations that experience an IT security breach event, an increase in the extent of communication management tactics will be associated with a decrease in competitive losses

H2D: In organizations that experience an IT security breach event, an increase in the extent of communication management tactics will be associated with a decrease in business productivity losses

The third set of hypotheses relates organizational responses tactics pertaining to security strategic thinking to IT security losses. Security strategic thinking organizational response tactics refer to organizational response actions at the senior level to enforce security related awareness and thinking across an organizations business units. The academic and practitioner literature has found that engagement of senior business executives and formal plans for managing IT security can help the organization mitigate negative financial impacts of IT security breach events (McFadzean, Jean-Noe, & Birchall, 2007; Wang, Chaudhury, & Rao, 2008). Other organizational response tactics that senior business executives can engage in based on evidence from the field interviews in Chapter 4 include (i) decision-making actions to enforce security related awareness across organizational business units, (ii)post-breach ad-hoc planning, and (iii) post-breach investment. An example of organizational losses from an IT security breach that could have been reduced with proper security strategic thinking occurred with the consulting firm Deloitte. The event began as an impersonation attack but evolved quickly to become an attack on the organization's email servers (Mak, 2017). One of the negative implications from this IT security breach was that Deloitte's reputation as an IT security services provider had been tarnished (albeit temporarily). The utilization and implementation of security strategic thinking tactics such as having a plan in place for the IT security coverage of all IT resources may have mitigated the negative impacts of the IT security breach for Deloitte. The following hypotheses are presented for the association between security strategic thinking organizational response tactics and losses from IT security breach events:

H3A: In organizations that experience an IT security breach event, an increase in the extent of security strategic thinking tactics will be associated with a decrease in financial losses

H3B: In organizations that experience an IT security breach event, an increase in the extent of security strategic thinking tactics will be associated with a decrease in reputational losses

H3C: In organizations that experience an IT security breach event, an increase in the extent of security strategic thinking tactics will be associated with a decrease in competitive losses

H3D: In organizations that experience an IT security breach event, an increase in the extent of security strategic thinking tactics will be associated with a decrease in business productivity losses

The fourth set of hypotheses pertains to IT resource management organizational response tactics. IT resource management are response actions encompassing the management of hardware, software, telecom, digital infrastructure and other IT related resources within organizations. IT resource management tactics can be utilized before and after an IT security breach event to decrease organizational losses. However, recent evidence has emerged that organizations have little incentive to invest in IT security even after a security breach has occurred. The likely culprit is that the costs of investing in IT resource management before an IT security breach event have not been made clear to organizations. Some experts fear that government intervention may be required more to protect the public from these events (Dean, 2015). Specific IT resource management organizational responses includes such actions as a dedicated team for real-time monitoring of systems, use of authentication methods, and regular assessment of IT security risks via penetration testing and vulnerability scanning (Jamieson & Low, 1990; Mohammad & Stergioulas2010; Iqbal et al 2016; Torres, 2015; InfoSec Institute, 2017). IT resource management is also vital because proper resource utilization in the context of human capital resource management is considered a potential source of innovation for firms and a lack of adequate human capital have been shown to negatively impact a firm's value (Viedma & Martí 2001; Edvinsson & Malone 1999). Hiring staff with sufficient technical aptitude and skill is essential to an organization's success in the management of IT security breach events; actions such as investments in IT security should prove even more helpful to this effect; although, as noted previously organizations may not readily see the benefits of this (Johnson, M. E. 2014, Gelbstein, 2015). The following hypotheses set are presented to understand the relationships between IT resource management organizational response tactics and organizational losses from IT security breach events:

H4A: In organizations that experience an IT security breach event, an increase in the extent of IT resource management tactics will be associated with a decrease in financial losses

H4B: In organizations that experience an IT security breach event, an increase in the extent of IT resource management tactics will be associated with a decrease in reputational losses

H4C: In organizations that experience an IT security breach event, an increase in the extent of IT resource management tactics will be associated with a decrease in competitive losses

H4D: In organizations that experience an IT security breach event, an increase in the extent of IT resource management tactics will be associated with a decrease in business productivity losses

The fifth set of hypotheses concerns governance organizational response tactics and the association with losses from IT security breach events. Organizational response tactics encompassing governance encompasses action which creates or modify formal and informal structures and mechanisms that are focused on an organizations accountability and response to an adverse event (Bundy, Pfarrer, Short, & Coombs, 2016; Bigley & Roberts, 2001; Lindstrom, Samuelsson, & Hagerfors, 2010). Savvy IT security leaders can utilize governance with the view that crises are opportunities. The extant research on governance in terms of adversarial events have found that organizations with flexible governance structures are better able to recover after an adverse event and flexible governance structures can even be utilized to take advantage of adversarial events (see Alpaslan, Green, & Mitroff, 2009; Dowell, Shackell, & Stuart, 2011). Good governance can also help the organization as a whole adapt and change after an adversarial event (Majchrzak, Jarvenpaa, & Hollingshead, 2007). The following hypotheses set on governance response tactics are presented:

H5A: In organizations that experience an IT security breach event, an increase in the extent of governance management tactics will be associated with a decrease in financial losses

H5B: In organizations that experience an IT security breach event, an increase in the extent of governance management tactics will be associated with a decrease in reputational losses

H5C: In organizations that experience an IT security breach event, an increase in the extent of governance management tactics will be associated with a decrease in competitive losses

H5D: In organizations that experience an IT security breach event, an increase in the extent of governance management tactics will be associated with a decrease in business productivity losses

Regarding liability management, organizations are subjected to mandatory regulations, legal costs, and administrative burdens associated with securing their IT infrastructures before and after an IT security breach event. These factors expose organizations to a wide range of liabilities. Mandatory regulations vary by industry. For example, healthcare organizations must follow a set of standards known as HIPAA (Health Insurance Portability and Accountability Act of 1996) which has specific requirements not only around securing healthcare data but also has specific requirements concerning patient and public notification if a breach does occur. The credit card industry has a standard known as the Payment Card Industry Data Security Standard (PCI-DSS) which sets information security protection standards to reduce credit card fraud (PCI Security Standards Council, 2017). All organizations that utilize credit card services must adhere to PCI-DSS requirements. In addition to a number of mandatory regulatory requirements on securing information technologies, there are many strongly suggested but not necessarily mandatory frameworks and guidelines such as NIST 800-53 and COBIT 5 (ISACA, 2017; U.S. Department of Commerce, 2013). NIST 800-53 is the set of standards that the United States government follows to ensure secure and resilient IT infrastructures across its many agencies. NIST 800-53 has also been adopted by organizations that do business with the United States government. COBIT 5 is the leading IT governance framework for enterprises and includes detailed recommendations for auditing & assurance, risk management, information security, regulatory & compliance, and governance of enterprise IT. Organizations must adhere to many other IT regulatory frameworks and best practices or risk not only legal cost for nonadherence and negligence but also fines.

A critical tactic for liability management is insurance. Insurance is a common risk transfer mechanism which effectively enforces a stop loss on an organizations damages related to crisis events including events such as IT security breaches (Trang, 2017). The importance of liability management via insurance and other risk transfer mechanisms can be illustrated with the cases of Target and Home Depot. The retailer Target experienced a data breach event in 2013 involving 110 million personal records, including credit and debit card information. The expenses from the loss were approximately $252 million; however, insurance reimbursements were $90million, and with savvy tax deductions Target ended up paying only $105 million in net losses which were less than a tenth of one percent of their of their 2014 revenues (Dean, 2015). The home improvement retailer Home Depot experienced a 2014 data breach were losses where $43 million and a $15 million insurance reimbursement brought final losses for home depot to $28 million which is less than one-hundredth of 1% of their 2014 sales (Dean, 2015).

H6A: In organizations that experience an IT security breach event, an increase in the extent of liability management tactics will be associated with a decrease in financial losses

H6B: In organizations that experience an IT security breach event, an increase in the extent of liability management tactics will be associated with a decrease in reputational losses

H6C: In organizations that experience an IT security breach event, an increase in the extent of liability management tactics will be associated with a decrease in competitive losses

H6D: In organizations that experience an IT security breach event, an increase in the extent of liability management tactics will be associated with a decrease in business productivity losses

The last set of organizational response tactics which are hypothesized to be associated with organizational losses are morale management tactics. Morale management tactics can be considered those organizational response tactics which help the organization enforce or maintain a healthy psychological climate. Morale is defined as the “confidence, enthusiasm, and discipline of a person or group at a particular time” (Merriam-Webster, 2018; https://www.merriam-webster.com/dictionary/morale). Organizational morale has been studied extensively in the management domains and has been associated with workplace stability, insufficient staffing levels, verbal abuse, performance, productivity and even violence (David, Dulmus, Maguin, & Cristalli, 2013; Denton & Campbell, 2009).

Morale management tactics not only have the potential to increase or decrease the likelihood of losses, but morale may also influence the severity of losses when they do occur. Employees work attitudes within organizations are important factors affecting organizational outcomes such as performance and productivity. In turn, employees' attitudes are determined by their perceptions of how the organization views them and the actual behavior of the organizations towards them and other employees (Gould-Williams, 2007). Second to hackers, current or former employees and contractors are the second largest information security threats so-called "insider threats" (Greitzer, Moore, Cappelli, Andrews, Carroll, & Hull, 2008). Many information security failures are a result of so-called "unintentional" insider events that can be just as harmful on the firm as intentional threats (for some examples see Privacy Rights Clearinghouse, 2017). It is important that organizations begin to pay attention to their morale in the context of information security breaches. A recent example of why this is important occurred with the NSA, and the breach of its repertoire of intellectual capital referred to as "cybertools." This breach has been detrimental to the morale at the NSA. According to the New York Times, the organization has suffered low morale and slowed operations because of this breach, threatening its continued existence and value (Shane, Perlrothe, & Sanger, 2017). The following hypotheses are presented to examine the association between morale management tactics and losses from IT security breach events:

H7A: In organizations that experience an IT security breach event, an increase in the extent of morale management tactics will be associated with a decrease in financial losses

H7B: In organizations that experience an IT security breach event, an increase in the extent of morale management tactics will be associated with a decrease in reputational losses

H7C: In organizations that experience an IT security breach event, an increase in the extent of morale management tactics will be associated with a decrease in competitive losses

H7D: In organizations that experience an IT security breach event, an increase in the extent of morale management tactics will be associated with a decrease in business productivity losses

5.3 Control Variables & IT Security Breach Characteristics

This research study consists of ten additional variables that will be examined. These variables include revenue, employee size, industry (IT-intensive or non-IT intensive), the extent of the breach, breach intent, breach source, breach sensitivity, breach response team, IT security maturity, and senior in charge. Three of these variables, which include revenue, employee size, and industry are common control variables in the IS business research stream (for some examples see Devaraj & Kohli, 2003; Mithas, Tafti, Bardhan, & Goh, 2012). The control variables help control for confounding differences in the relationship of the independent and dependent variable due to inherent features of an organization such as its size, revenue, and industry. Controlling for these variables allow a more precise analysis of the relationships between the independent and dependent variables tested in the hypotheses. Revenue refers to the annual revenue or sales of an organization, and in this study, revenue is measured in U.S. dollars. In addition, revenue serves as one of two measures for the size of an organization. Employee size refers to the count of employees within the organization and is also used as a measure of an organizations size. In this study, employee size is used to delegate organizations as large or small. The designation of organization size is a derived especially for this study and is based on the features of the sample collected and commonly agreed upon definitions for what constitutes a small business based on the U.S. small business administration (SBA). The SBA positions that small business in the United States can be characterized a business with 500 or fewer employees and with average annual receipts of less than $7.5 million ((U.S. Small Business Administration, 2017). Organizational size is important to assess in the context of the relationship between organizational response tactics and organizational outcomes. Large organizations have been the focus of extensive studies in the context of financial and reputational outcomes of IT security breach events, and these events are perceived as detrimental to the large firms, despite this finding have been mixed (see Spanos & Angelis, 2016 for a literature review of this research stream). The use of employee size as a variable in this study will help us to understand better if losses to IT security breach events are just detrimental to small organizations, which is one of the contributions of this study.

Industry is utilized in this study to assess the distribution of organizations in this study. Industry is also utilized in this study as a proxy for IT intensity where IT intensity industries are industries noted as industries that are amenable to automation based on Dehning, Richardson, & Zmud, 2003. The study notes that "Manufacturing, Financial Services, Transportation, Utilities, Computer Software Products and Services, Telecommunication and Construction" are particularly more IT-intensive than other industries due to their amenability to automation. This study conceptualizes IT intensity based on the aforementioned research study, which has been highly cited. It is important to study IT intensity because the literature has presented evidence that IT intensive industries experience more significant adverse outcomes from IT security breach events (see Chen, Li, Yen, & & Bata, 2012; Ko, M., & Dorantes, 2009) and therefore this relationship will be tested in the study as well. Other control variables that will be assessed in this study but are not included in the research model includes a measure of the whether the organization has a formal unit or team to handle IT security breaches, the maturity of the IT security function within the organization, and whether the organization has a senior executive in charge of IT security. Other control variables that will be assessed in this study but are not included in the research model includes variables pertaining to the characteristics of an IT security breach.

Chapter 3 of this study was devoted exclusively to IT security breach characteristics. As noted in Chapter 3, IT security breach characteristics are those inherent descriptors that are part of every IT security breach event. The characteristics of every IT security breach include extent of breach, breach intentionality, breach source, and breach sensitivity. Succinct descriptions for each of the four IT security breach constructs in addition to other variables that will be empirically evaluated throughout this study are noted in Table 22 below. The IT security breach characteristics are important to study because it will be important to understand if certain breach characteristics lead to an increase or decrease in certain types of losses. This will enable organizations that may be at an inherent risk for certain types of breach events to plan their risk management strategies accordingly.

Construct	Operationalization	Sources
Revenue	Average Annual Revenue in USD. Organizations with annual revenues greater than or equal to $10,000,000 USD are classified as large and organizations with less than $10,000,000 in annual revenue are classified as small	U.S. Small Business Administration, 2017
Employee Size	Count of employees within an organization. Organizations with 1,000 or more employees are classified as large and organizations with less than 1,000 employees are classified as small	U.S. Small Business Administration, 2017
Industry	Industry based on combined NAIC groupings. IT Intensive industries are specifically refer to the Manufacturing, Financial Services, Transportation, Utilities, Computer Software Products and Services, Telecommunication and Construction industries. All other industries are grouped as non-IT intensive.	United States Census Bureau, 2017 Dehning, Richardson, & Zmud, 2003
Extent of Breach	Refers to both the subjects of the breach and the causes of the breach. Subjects can include products, services, internal computers, and email. The cause of the IT security breach is the action that led to the information technology system being compromised such as hacking.	Clark, 2014; Cichonski et al. 2012
Breach Intentionality	Intentional versus unintentional	Greitzer et al. 2008; Warkentin & Willison 2009; Silowash et al. 2012
Breach Source	Who or what was the source of the IT security breach event. The source of an IT security breach event can range from a person to a nation state, organized crime, terrorists, or may even be unknown to the organization	Derived
Breach Sensitivity	Sensitivity of the data or information related to the breach event. It is the likelihood the data or information if exposed can cause harm	Quist 1993;Clark 2014; Loch 1992
Breach Response Team	Formal unit or team to handle IT security breaches after the event	U.S.Computer Emergency Readiness Team, 2015, Rajivan et al. 2013 Reed et al. 2014; Steinke et al., 2015 Interview Respondent 6
IT Security Function Maturity	Process maturity can be categorized as initial, repeatable, defined, managed, and optimized.	Based on IT Governance Maturity framework from COBIT 4.1 IT Governance Institute, 2007; Debreceny & Gray, 2009
Senior in Charge	Presence of a senior executive at the director level or above	Derived

Table 22: Description of Control Variable’s in the Study and Research Model

5.4 Chapter Summary

Utilizing grounded theory this chapter developed a research model and an ensuing set of hypotheses based on the conceptual model in chapter 1. At a high level, the research model positions that IT security breaches lead to negative organizational losses and are mitigated by one or more organizational response strategies. The chapter that follows is a discussion of the quantitative research methodologies that will be utilized to test the research model including a discussion of the validation processes for the research design and the survey instrument.

CHAPTER 6: FIELD SURVEY AND OVERVIEW OF RESEARCH METHODOLOGIES

6.1 Prologue

In this chapter, the data collection and data analysis processes are discussed including results from the statistical testing of the control variables (which include IT security breach characteristics). For clarity and audience accessibility, Figure 5 provides a succinct overview of the identification strategy and quantitative methodologies utilized in this study as well as a brief supporting rationale for their use. Although Figure 5 depicts a linear process, mitigation strategies pertaining to construct reliability and validity are addressed in both the survey pretesting phase and in the assessment of the measurement model.

Four phenomena that may have an impact on the analysis are 1) sample selection bias, 2) missing data, 3) sample non-response bias, and 4) common method bias. A discussion ensues regarding each of these phenomena in the context of this study and remediation's that were taken (if any) to address these concerns. The intent is to provide a complete picture of the advantages and limitations of the survey data collected for this study. This chapter also discusses the unique circumstances of this research study, which increases the likelihood of these phenomena occurring. For clarity and flow, this chapter first discusses the 1) survey pretesting processes, followed by the 2) data collection processes, 3) the data analysis processes, 4) the measurement model, and concludes with 5) hypotheses testing and results.

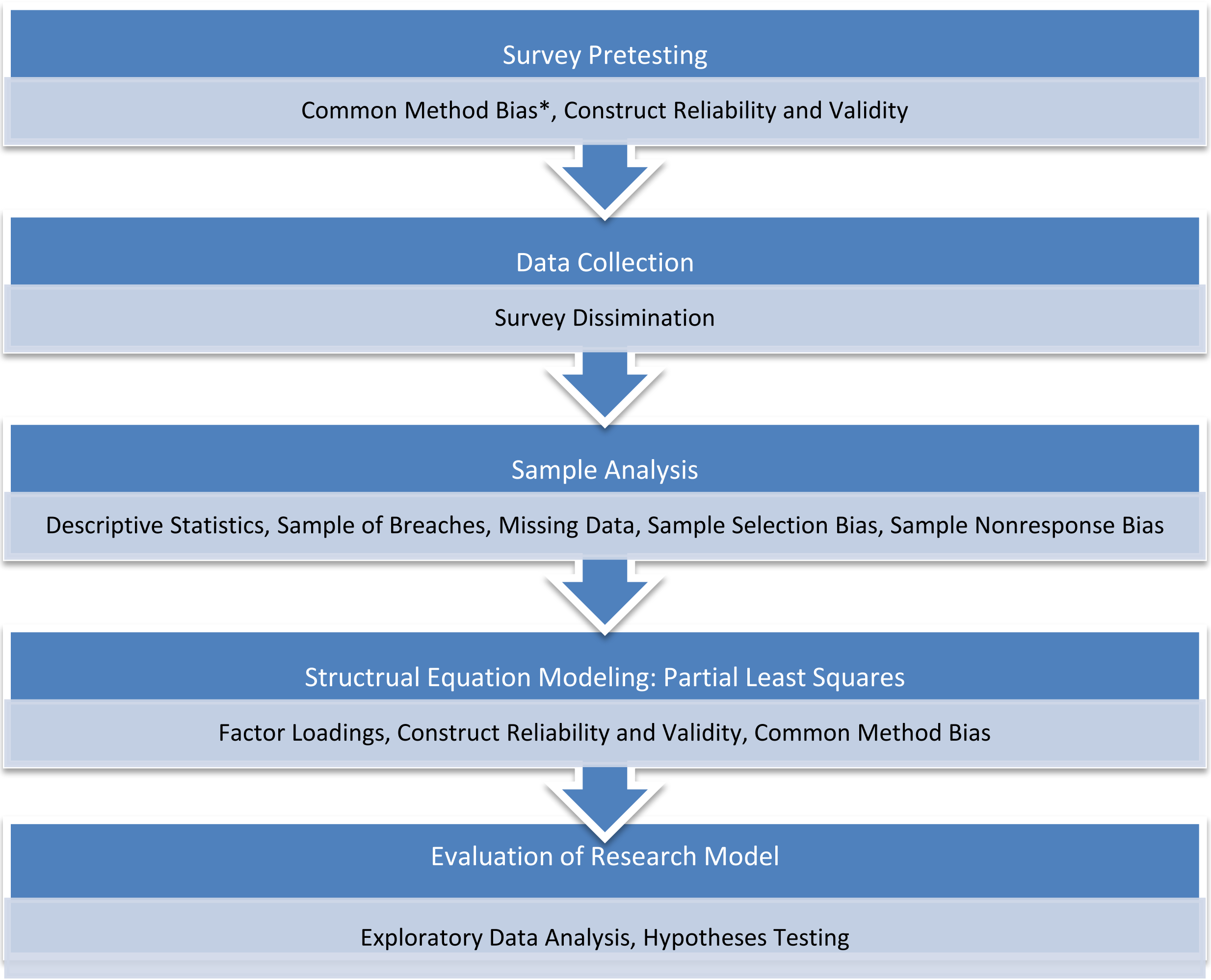

Survey Pretesting
Common Method Bias*, Construct Reliability and Validity
Data Collection
Survey Dissimination
Sample Analysis
Descriptive Statistics, Sample of Breaches, Missing Data, Sample Selection Bias, Sample Nonresponse Bias
Structrual Equation Modeling: Partial Least Squares
Factor Loadings, Construct Reliability and Validity, Common Method Bias
Evaluation of Research Model
Exploratory Data Analysis, Hypotheses Testing

Figure 5: Overview of Identification Strategy and Research Methodologies

6.2 Survey Pretesting and Validation of Research Design

Survey data within the information security research domain presents unique challenges when used to develop and validate theory including issues with the utilization of research methodologies, the statistics applied to the data, and concerns with data collected in a survey (Ryan, 2003). Information security research is frequently disseminated by the popular press and is extensively utilized by policy and decision makers. Flawed research can lead to detrimental losses for society (Ryan, 2003). For this reason, this study took great care during the data collection and research model validation processes in acknowledging and mitigating known risks to prevent flawed findings in the study.

It is important that surveys measure the constructs that they are intended to measure and be free from errors that would unnecessarily influence the results. In order to accomplish this, surveys must meet the criteria of being reliable and valid. Reliability means the survey instrument is consistent across respondents, is absent of poor wording, has clear recording procedures, and clear, standardized instructions (Bagozzi & Yiu, 1988). A survey instrument is valid if it truly measures the constructs it is intended to measure. In order for a survey instrument to be valid, it must first be reliable. A survey instrument can never truly be completely reliable and valid; however, the extent to which the survey is reliable and valid must be measured (Peter, 1979). Biased estimates of reliability and validity can lead to biased parameter estimates for relationships between constructs. This is referred to a "common method bias." This can result from the content of the survey items in the survey, the response format, survey instructions, characteristics of the researcher, and the motives and emotional states of the research participants (Mackenzie & Podsakoff, 2012; Podsakoff, Mackenzie, Lee, & Podsakoff, 2003). Common method bias may result in incorrect claims about the proposed relationships, the mechanisms that connect constructs, and/or boundary conditions for the hypothesized relationships.

The issues with survey reliability, validity, and subsequently common method bias can be addressed apriori by following survey design best practices and post-hoc with statistical analyses. To address common method bias and issues with survey reliability and validity apriori, this study conducted survey calibration and pre-testing. The survey calibration and pre-testing is based on Churchill, 1979; which identified seven common risk factors as having potentially negative outcomes on a survey’s reliability and validity, most of which overlap with the twenty-five “sources of potential common method bias” outlined by Podsakoff et al 2003; which is a popular guide for survey design best practices . Table 23, notes each of the survey risk factors and how they will be mitigated for either in the survey design processes, the survey dissemination processes, or during the data analysis processes of this study.

Common Survey Risk Factors	Research Mitigation Tactics Undertaken
True differences in other relatively stable characteristics which affect the score, e.g., a person's willingness to express his or her true feelings.	Survey is completely anonymous, and no individual will be identified. Results will be reported in the aggregate.
Differences due to transient personal factors, e.g., a person's mood, state of fatigue.	Respondents can take survey at a time that is convenient for them. Make note of estimated completion time to manage expectations.
Differences due to situational factors, e.g., whether the interview is conducted in the home or at a central facility.	Survey is standardized everyone will receive the same survey. Survey will be tested to ensure it can be taken on mobile devices, laptop, and desktop. Device and browser information will be collected to mitigate this.
Differences due to variations in administration, e.g., interviewers who probe differently.	Survey is standardized and self-administered via web
Differences due to sampling of items, e.g., the specific items used on the questionnaire; if the items or the wording of those items were changed	Survey is standardized and self-administered via web
Differences due to lack of clarity of measuring instruments, e.g., vague or ambiguous questions which are interpreted differently by those responding.	Survey pretesting and evaluation was conducted in two iterations of testing.
Differences due to mechanical factors, e.g., a check mark in the wrong box or a response which is coded incorrectly	Survey will utilize modified Likert scale or multiple choice

Table 23: Survey Risk’s Adopted from Gilbert A. Churchill, Jr., 1979

Survey pretesting processes outlined by Li & Calantone, 1998; Jaworski & Macinnis, 1989 were followed, in that the research constructs are defined based on the theory in the applicable literature and in the case of this study we also utilize field interviews as supporting research. Content validity was established by obtaining feedback on the refinement of survey items, the research design, and the survey constructs. Key informants were utilized to provide feedback on the research design and the contextual validity of key constructs, survey items, and the research questions of the study. Since the subject of this study concerned a sensitive topic within organizations, the pretesting was geared toward technically savvy, subject matter experts. The survey pretesting on this group was very important to ensure appropriate syntax and semantics were utilized prior to broader dissemination of the survey. After the review of the survey by the key informants, the survey was reviewed and revised by the author and an academic expert to ensure maximum reliability and validity.

The key informants for this study needed to meet two criteria to participate in the pre-testing. The criteria are based on a framework established by Kumar, Stern, & Anderson, 1993. First key informants needed to be in a position to generalize about patterns of behavior related to the content of inquiry, after summarizing either observed or expected organizational relations, and second, the key informant needed to be knowledgeable about the content of inquiry. An additional requirement was also added that key informants must have met the two criteria mentioned above within the last three years. In the context of this research study, all of the key informants needed to have knowledge about what occurs within organizations in regards to the management of IT security breach events, including knowledge of potential losses, and knowledge of organizational responses. Key informants meeting these requirements allow us to surmise that they are knowledgeable about IT security breaches (the content of inquiry). Key informants who met the criteria were selected from the author's personal network, and participants were randomly assigned to either the first or the second round of pre-testing to provide their expertise to the study. Key informants in the first round were given the completed set of survey questions derived from the literature and theory, feedback from this group of key informants, i.e. first round feedback was then utilized to revise the survey. This revised survey was then presented to the key informants assigned to the second round of pre-testing for their feedback. Participants were randomly assigned to either round 1 or round 2 of pretesting, as it is difficult to accurately access if one set of occupations or experiences have more expertise than another. Criteria for selecting occupations which are considered to be IT security related were based on the March 31, 2017, directive from the Department of Homeland Security (DHS) that identified seven high-level categories of occupations each comprised of several specialty areas, which are considered "cybersecurity"; but no specific occupations, are listed in the directive (National Initiative for Cybersecurity Careers and Studies, 2017). Table 24, provides a demographic description of key informants who were utilized to provide their feedback on the research design, potential survey questions, and construct reliability and validity.

Respondent Number	Round	Occupation	Work Experience	Security Experience	Industry	Organization Type
1	1	Systems Engineer	22 years	12 years	IT/Telecom	Public
2	1	Cloud Cybersecurity Engineer	6 years	2 years	Professional/Business Services	Public
3	1	Cloud Data Solution Architect	9 years	4 years	IT/Telecom	Private
4	1	Software Engineer and Security Researcher	3 years	3 years	Government/Public Sector	Private
5	1	Mobile App Engineer	4 years	4 years	Professional/Business Services	Public
6	1	Senior Information Security Analyst	8 years	8 years	Healthcare	Public
7	1	IT Security and Crises Consultant	7 years	7 years	IT/Telecom	Private
8	1	Data Security User Interfaces Developer	6 years	3 years	IT/Telecom	Private
9	1	Cybersecurity Researcher (Network and Communications)	12 years	7 years	Government/Public Sector	Private
10	2	Web Engineer and Former Corporate Risk Management Consultant	11 years	5 years	IT/Telecom	Private
11	2	Sr. Healthcare Analytics Project Manager	10 years	10 years	Healthcare	Private
12	2	Cloud Architecture Specialist	14 years	6 years	IT/Telecom	Private
13	2	Network Engineer	11 years	7 years	Healthcare	Public
14	2	Large Institution Benefits Consultant	13 years	4 years	Finance/Insurance/Banking	Public

Table 24: Survey Pre-Testing Participants Demographic Description

Key informants could either provide feedback via phone or email at their convenience. In some cases, both email and phone were used to obtain feedback at the participant's request, as some participants had more nuanced feedback regarding the overall study and potential research questions. Table 25 lists suggestions from key informants regarding the study design and potential survey questions. Note that "N/A" denotes participants who only provided feedback that focused specifically on one or more grammar and usage concerns in the questionnaire. In addition, feedback on specific questions are not included as the questions have evolved and were merely examples of how potential questions may be worded, this was done to understand the target sample better.

Participant	Key Informant Feedback
Participant 1	1. You did not discuss how the data would be reported. I suggest it gets reported in aggregate to enhance confidentiality of participants. 2. Answering questions about an organizations security breach may in itself constitute a breach and participants may be concerned 3. Your talking C-level participants who may be able to tell you about the money but not about the technology and director level may be able to tell about the technology but not about the legal costs. I don't know.
Participant 2	1. I do not understand the purpose of collecting browser meta info in Qualtrics 2. Put numbers in words like nine hundred thousand or 9 million etc. Makes it easier to understand. 3. Be sure to mention in the starting description paragraph the estimated completion time for this survey so that people are mentally prepared. 4. A good idea would be to break a set of questions into themes/categories. Having 3-4 questions under each category will definitely help reduce user fatigue
Participant 3	1. I like this study has a focus on governance. It will be nice to see what the "first hand" perceptions of some of the traditional governance tactics are. 2. I think this is easy for the typical professional to relate to.
Participant 4	N/A
Participant 5	1. I feel that the terms and conditions are very long, but you probably need to include them

	2. It might be helpful to restrict the people who take the survey based on how aware of it they are. 3. Also, everyone isn't so well informed about such breaches. There can probably be a question about how well they know about the breach. 4. Beware, that lower-level employees may be given a less detailed survey or asked to fill only what they know for sure so that their ideas and half-baked knowledge of the incident doesn't mess up the survey results.
Participant 6	1. Your study seems to ask some sensitive information. For an information security questionnaire, some of the questions could potentially identify the organization and their breach incident. At my organization, breach incidents are kept very private, usually with attorney-client privilege for the disclosure/communication of information.
Participant 7	1. A risk of this research is a loss of privacy (revealing to others that you are taking part in this study) or confidentiality (revealing information about you to others to whom you have not given permission to see this information). 2. This study could violate employee NDA
Participant 8	N/A
Participant 9	1. In the consent form, For clarity, consider making this into a bulleted or numbered list. 2. In the consent form, I think this statement could use some clarity. Do you mean that the subject is familiar with ITSec issues, mitigation, solutions, all? Also, “within the context of organizations” as opposed to personal ITSec? 3. In the consent form, In this case, “whether or not” should be omitted because it is attempting to modify “decision” when it should really be acting as the noun itself – “Whether you decide to participate.…”. But if you mean to convey the feeling that any relationship between the university and the subject will not be altered regardless of whether the subject participates, then "or not" should be included (e.g., …whether or not you choose to participate….). Here’s a good reference that explains it much better than I did https://afterdeadline.blogs.nytimes.com/2010/03/01/whether-or-not/
Participant 10	1. Questions are easier to read with numbers rather words 2. If I were knowledgeable about a breach, no way I would describe it in a research study in an open-ended form
Participant 11	N/A
Participant 12	N/A
Participant 13	1. One of the things that tend to happen is outages due to a user error. Is this considered a breach event? 2. I can give you ten ways to secure your infrastructure based on network best practices. Have an open-ended question for comments 3. Everything in this study looks good

Participant 14	1. I feel your study captures all the different aspects of a security breach when it does happen. It's very straightforward.

Table 25: Survey Pre-Testing
Key Informant Feedback of Research Study

After evaluating the feedback from key informants, in conjunction with an academic expert, questions were revised for each of the key constructs in the study. The survey utilizes a combination of Likert scale and multiple-choice questions. The majority of questions are 7 item Likert scaled. The question design for the survey follows the processes outlined by (Bradburn, Sudman, & Wansink, 2004) in which the social context of the survey questions was considered, tactics for asking certain questions were employed, and appropriate demographic questions were included. Next, is a discussion of the data collection processes.

6.3 Data Collection Methodology

Data to test the hypotheses were collected via the online survey platform Qualtrics. The survey measured firm-level characteristics, IT security breach characteristics, respondent characteristics, IT security breach losses, and IT security breach response tactics. The eligibility criteria for participation in this study were that participants 1) self-identified as being in a management or decision making role or higher within the organization that experienced an IT security breach event 2) Worked within an organization that experienced an IT security breach in the last three years 3) Role involved one or more aspects of IT security. Potential respondents were identified through the 1) Women in Cybersecurity Organization, 2) The Center for Research in Information Management at the University of Illinois at Chicago, 3) Amazon Mechanical Turk Prime (Verified U.S Citizens Only, Verified IT & Management Only), and 4) Linkedin.com. Eligible participants were personally contacted and recruited via email and messaging in addition and listserv announcements were sent out to each of the respective respondent groups. Survey responses were collected anonymously; however, a number of participants made direct contact to discuss their eligibility for the study and for reassurances of anonymity. A total of 664 eligible participants were identified and personally contacted twice utilizing customized messages. The first contact requesting survey participation occurred in the first three weeks of March 2018, and each eligible participant was then contacted a second time between the last week of March 2018 and the first week of April 2018. The survey was closed on the second week of April 2018. We received 229 responses for an overall response rate of 34%. Out of 229 total responses, there were 101 incomplete responses. Incomplete responses are responses in which participants did not answer all of the required questions. In the research survey, all but one question was required. The single optional question for survey participants was a free-form question asking survey participants to describe details of the IT security breach event. This question was coded as an optional question based on feedback received during the pre-testing phase. Survey responses that were not 100% completed (exclusive of the optional question) were not usable in the analysis. The response rate accounting for incomplete responses is 19.2% or 128 completed responses. Next, is a discussion of the survey data including the presentation of sample descriptive statistics to shed light on any sample selection bias, missing data, and sample nonresponse bias that may provide help to shape understanding of the hypothesized research model.

6.4 Data Analysis

6.4.1 Sample Selection Bias

Sample selection bias is a phenomenon in which measures may be distorted due to the sample not accurately reflecting the target population. Alternately, it can imply that the final study is not representative of the target population and therefore the findings and results are not applicable to the real world, i.e. the findings are generalizable. It occurs when participants who complete a study vary from the target population. There are a number of methods to test for sample selection bias and implement corrections if the bias is present. Any correction for sample selection bias requires that the researcher understand the source and magnitude of the bias (Stolzenberg & Relles, 1997); this obviously requires the researcher to be able to make inferences about the target population. For this study, this was attempted by examining industry characteristics, size, and annual revenue of firms that experienced “data breach events” over the last three years. To do this, the author identified what could arguably be considered the most comprehensive repertoire of IT security breach event data that is publicly available. This database is referred to as "Privacy Rights Clearinghouse Data Breaches," and a sample of data was collected from January 2015- January 2018 (a period going back three years that matches the approximate dates of breaches for respondents to the survey). However, further analysis of this database revealed that it was not meaningful in helping to estimate the population parameters of IT security breaches in the United States mainly because the database is a sample of "reported" breaches that primarily involve data and this data is primarily regarding the personal information of private citizens. There are many other types of IT security failures and breaches, which can include network intrusions, denial of service attacks, and unlawful disclosure of intellectual property, among others types of breaches. At this current time, there is no evidence that researchers are aware of what the estimated population parameters may look like of organizations that have experienced IT security breach events. If the population parameters were known or could be estimated or derived there are a number of methods to correct for sample selection bias including a common procedure, outlined in Heckman, 1979. However, it is not known what the population parameters are to state one way or another whether sample selection bias has occurred or not for the sample used in this study.

With that being said, there is evidence to believe that a potential participant's exclusion from the sample may be systematically related to the underlying phenomenon in question, i.e. taking a survey disclosing details of an IT security breach event at a current or former organization of employment. What is known is that IT security breach events can be significant, negative events to not only organizations but also to the internal human resources within these organizations. This point cannot be understated or glossed over, as these events have led to individuals losing their livelihoods through demotion or termination of employment (Isaac, Benner, & Frenkel, 2017; Bernard & Cowley, 2017; Horowitz & Weiner-Bronner, 2017; O'Neill, 2017). In addition, employees whose roles include internally disclosing IT security breaches sometimes encounter an unusual and counterintuitive risk of termination for even bringing such events to the attention of internal company supervisors (Lannin, 2016). Some companies have attempted to assuage this fear of IT security breach disclosure by implementing bug bounty programs, but those programs are geared towards external security researchers. Bug bounty programs are programs that an organization institutes for ethical and white hat hackers to discover and disclose IT security vulnerabilities in exchange for monetary payment and/or free products or services. For a comprehensive list of organizations with these programs, see hackerone.com (HackerOne, 2018). In addition, two key informants during the survey pretesting process indicated that any potential survey participants were more than likely bound to secrecy by non-disclosure agreements. These non-disclosure agreements are legally binding contracts that companies often use as part of an employment contract to prevent sensitive information such as trade secrets from becoming public; violation of a non-disclosure agreement can lead to civil penalties. More recently, however, an increasing number of IT-related non-disclosure agreements in states such as California, Texas, Florida, and New York take the view that "information" regarding intangible and tangible IT assets within an organization should be viewed as property. These states threaten criminal charges for any type of disclosure, of any information, related to internal IT systems even, after an individual has left an organization (CompTIA Legal Team, 2010). It is unclear however the prevalence of enforcement regarding such agreements.

With the aforementioned in mind, there is evidence that the sample from this study may be more in line with a convenience sample rather than a random sample and should be viewed as such for quantitative analysis purposes. The response rate and the clarifying questions from participants who chose to “de-anonymize” provides evidence that the sample may primarily consist of individuals who have 1)a pre-existing professional relationship with the author and wanted to inform the author of their “support” of the research, 2) the professional network of those individuals with a pre-existing professional relationship to executive level “survey referrers” and who wanted to show their support to the referrer 3) individuals attempting to establish a new personal or professional relationship with the author 4) individuals who were highly satisfied in how an IT security breach was handled by their organization and may have received positive reinforcement surrounding the event 5) individuals who were dissatisfied with how a breach was handled and received negative reinforcement regarding the event and were no longer employed by the organization which experienced the breach . Essentially, for survey participants, the intangible rewards from completing this survey needed to outweigh the tangible risks for the participants. This is not surprising and was expected given the subject of study. Since the population parameters of organizations that have experienced an IT security breach cannot be confidently estimated or derived, the ideal sample for the testing of the research model can only be described as any sample that is a representative, diverse sample that has at least one representative organization for each of the organizational demographics that are being measured. The data collected in this study meets the aforementioned requirement. Furthermore, the aforementioned sample descriptions allow us to reasonably test the hypotheses keeping the aforementioned constraints in mind. Table 26 is a snapshot of IT security breach descriptions from the sample.

Industry	Breach Description
Finance/Insurance/Banking	There was a leak of people's personal information. This includes names and social security numbers.
Retail/Wholesale	Password reset
Logistics/Transportation	While downloading unauthorized personal files, someone unintentionally downloaded a virus
Professional/Business Services	System was recently hacked and several customers credit information was tampered with.
Professional/Business Services	Equifax data breach. They accessed personal information such as social security, address, etc. they also stole credit card information.
IT/Telecom	Data hacking
Healthcare	Stolen desktop with patient health information (PHI) on it.
Government/ Public Sector	Compromised SQL server
Finance/Insurance/Banking	Identity Information Compromised
Manufacturing/Engineering	Email phishing
Government/ Public Sector	New patch was installed causing passwords to be changed

Table 26: Snapshot of IT Security Breach Descriptions from Sample

Next, is a discussion of the behavior of missing data and sample non-responses in this study and potential biases the study may suffer due to missing data and sample non-responses.

6.4.2 Missing Data and Sample Non-Response Bias

For this sample, it is just as important to analyze differences in participants who completed the survey versus those who did not finish the survey to gather additional insights. There were 101 incomplete responses with 75 of these individuals completing the consent form and 27 answering the question describing specific details of the breach event, the only optional question on the survey. Stata Version 13 was utilized to conduct t -testing of differences in the means of questions between responses of participants who completely finished the survey and participants that did not. Participants that did not completely finish the survey are considered the non-response group. Unequal variances were assumed for t-testing due to the differences in sample sizes and assumptions regarding the normality of the data. There were statistically significant demographic differences found between participants who completed the survey and those who did not. This should be viewed as new and insightful information about potential characteristics of the population of organizations that have experienced IT security breach events, and the population of respondents willing to participate in this type of sensitive survey on behalf of an organization and not necessarily something that needs to be statistically corrected and adjusted for.

First, regarding senior executives, survey participants who completed the survey were more likely to answer "Yes" their company has a senior executive responsible for IT security. For, the job title of who has final responsibility for the IT function there were statistically significant differences in the distribution; where survey participants who completed the survey were more likely to have the title of “Director” as having the final responsibility for IT security within an organization compared with non-respondents whose titles for final responsibility of IT security were more evenly distributed (p=0.627, t=0.4866). Survey participants who completed the survey were also more likely to have a formal unit or team in the organization to handle IT security breach events (p=0.0007, t=3.4659). The maturity of the IT security function also varied between respondents and non-respondents where non-respondents were much more likely to answer that their IT security processes and roles that were informal or uncoordinated or were monitored or measured (p=0.0297, t=-2.1945). These corresponded to levels 2 and 5 out of the 6 levels used to measure the maturity of the IT security function. Perhaps indicating these organizations may exhibit too much or too little control regarding their IT security. However, these differences did not reach statistical significance. At this time, there are no theoretical bases for the differences between survey participants and nonparticipants based on the demographic characteristics outlined.

However, there were patterns noted in regards to where survey participants ended the study. For example, there was a noticeable drop off in survey participants at the conclusion of the demographic questions where only six survey participants from the non-response group out of twenty-four survey participants continued onto questions pertaining to the breach event. Out of the six non- respondents who completed the first survey question after the demographic questions, only four of those went on to answer two additional survey questions and one respondent completed 73% of the survey before stopping. Since the survey can be considered lengthy, it was initially theorized that individuals might have stopped at the question pertaining to the “Extent of the Breach” (the first question after the demographic question) since it was a new section and perhaps had made plans to finish the survey at a later time. In examination of survey duration between completed responses and incomplete responses indicates that there are no statistically significant differences in the duration of the survey, providing evidence for this theory, i.e. participants may have stopped the survey on their operating system with the intention of finishing it before finally opting just to close the survey window in their browser. Also, a number of participants made no attempt even to view the survey question which followed the demographic question indicating that many survey participants did a hard stop at the demographic questions. To remedy this issue for future studies, it may be helpful to offer nominal compensation for each survey participant to encourage them to complete the survey considering not only the sensitivity of the topic of interest but also the length of the survey. No statistically significant differences in industry, employee size, or annual revenue were found between respondents and non-respondents.

Demographic Question Mean(NR)-Mean(RS)	Count of Non-Respondents Who Completed Question	Alpha	t value
Duration of Survey Time	93	*p*=.4194	-.8090
Job Title Distribution	43	*p*=.1101	-1.6062
Industry Distribution	35	*p*=.9441	0.0702
Annual Revenue Distribution	28	*p*=.6363	-0.4738
Organizational Employee Size	32	*p*=.2659	-1.1165
Senior Executive for IT Security	27	*p*=.0000	4.4923
Role Responsible for IT Distribution	26	*p*=.6273	0.4866
Formal Team Responsible for IT	26	*p*=.0007	3.4659
Maturity of Processes and Roles	24	*p*=.0297	-2.1945

Table 27: Sample Non-Response Analysis

Since information is not available on the population parameters of organizations that have experienced IT security breach events a follow-up study should be conducted to better understand what may have caused participants to only complete a portion or all demographic questions but not continue onto questions regarding the actual breach event and subsequently not complete the survey. However, in light of the large number of respondents who did complete the demographic questions we are able to have some understanding of not only what non-response bias may look like but also further insights into sample selection bias and some potential inferences on the population characteristics of organizations that have experienced IT security breach events. As stated previously, since we cannot confidently estimate or derive the population parameters of organizations that have experienced an IT security breach the ideal sample can only be described as representative, diverse sample, which has at least one representative organization for each of the organizational demographics that we are measuring. The study sample meets this requirement. The next section explores the characteristics of the study sample in more detail.

6.4.3 Description of Sample

In this section, Table 28 provides the demographic information for the sample of completed responses and Table 29 provide descriptive statistics for the key variables in the study. Table 28 provides some preliminary support for a fairly representative sample as each organizational demographic group is represented at least once; however, certain types of organizations are under-represented or over-represented in the sample. For instance, over 60% of firms in the sample have 10,000 employees or less, with 28% having fewer than1,000 employees. This finding is amenable to a research goal of this study that sought to better understand IT security breach events in the context of small and private organizations. This interest in small and private organizations is due to these organizations being underrepresented in the academic and business research on IT security breaches. The revenue distribution of organizations in this study is normally distributed with 14.1% of organizations earning less than one million dollars and 13.3% earning over ten billion dollars. In terms of industry sectors represented, close to one-third of firms are from the IT/telecom sector. Firms in the Finance/Insurance/Banking sector comprise 17% of the sample, followed by Professional/Business Services sector, which comprises 15.6% of the sample.

*Industry	Sample Distribution Percentage	Count of Respondents
Energy/Utilities	3.1	4
Finance/Insurance/Banking	17.2	22
Government/Public Sector	8.6	11
Healthcare	10.9	14
IT/Telecom	32.1	41
Logistics/Transportation	2.3	3
Manufacturing/Engineering	4.7	6
Professional/Business Services	15.6	20
Retail/Wholesale	5.5	7

*Organization Size (Count of Employees)	Sample Distribution Percentage	Count of Respondents
0-999	28.1	36
1,000 or more	71.9	92

*Organization Revenue	Sample Distribution Percentage	Count of Respondents
Less than ten million dollars (USD)	36.7	47
At least ten million dollars (USD) or more	63.3	81

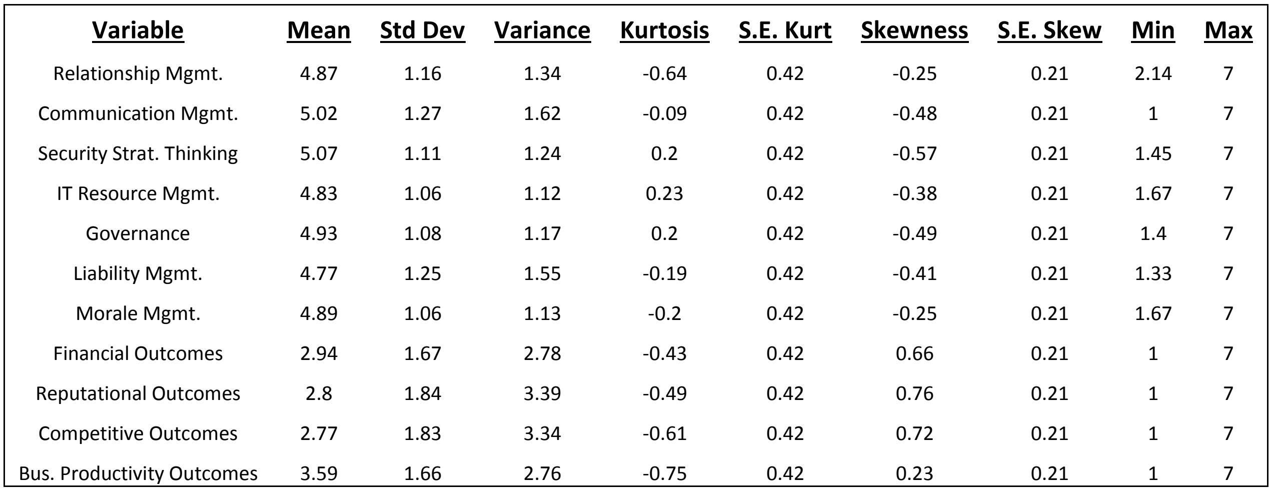
Job Title	Sample Distribution Percentage	Count of Respondents
Professor/Teacher/Researcher	5.5	7
External Consultant	12.5	16
Technical/Engineering	25.8	33
Practitioner/Professional	10.2	13
Supervisor/Manager	37.5	48
Director	3.9	5
Officer	4.7	6

*Senior Executive Responsible for IT	Sample Distribution Percentage	Count of Respondents
Yes	82.8	106
No	17.2	22
Title of Position with Final Responsibility for IT Security	**Sample Distribution Percentage**	**Count of Respondents**
Director	33.5	43
Vice President	21.1	27
Officer	16.4	21
President/CEO	18.8	24
Other	10.2	13
***Formal Unit/Team to Handle IT Security Breaches**	**Sample Distribution Percentage**	**Count of Respondents**
Yes	85.9	110
No	14.1	18
***Maturity of IT Security Roles & Processes**	**Sample Distribution Percentage**	**Count of Respondents**
Non-Existent	6.3	8
Initial	13.3	17
Repeatable	19.5	25
Defined	24.2	31
Managed	25	32
Optimized	11.72	15

Table 28: Demographic Profile of Respondents

The job title of survey respondents varied. All respondents indicated that their roles were considered manager level or above with 46.1% of the sample being exclusively in human capital management roles related to IT security where 53.9% worked in technical roles related to IT security. Technical roles include such occupations as researchers, external consultants, or technical/engineering roles. 82.8% of respondents indicated that their organization had a senior executive responsible for IT security and 89% had at least a director level or above that had final responsibility for IT security and 85.9% had a formal unit or team to handle IT security breaches. Regarding the maturity of the IT security function, only 38.42% of organizations indicated they had roles and processes that were at least defined indicating most organizations did not have a mature IT security function.

Table 29 shows the descriptive statistics of key variables from the sample. All constructs were measured utilizing Likert scaled survey items with ranges 1-7. All constructs can be considered normally distributed with no excess kurtosis or skewness in the distribution of responses noted. Kurtosis ranged between -0.75 to 0.23 and skewness ranged from between -0.57 to 0.76. Table 30 shows the correlations of the key variables in the study.



Variable	Mean	Std Dev	Variance	Kurtosis	S.E. Kurt	Skewness	S.E. Skew	Min	Max
Relationship Mgmt.	4.87	1.16	1.34	-0.64	0.42	-0.25	0.21	2.14	7
Communication Mgmt.	5.02	1.27	1.62	-0.09	0.42	-0.48	0.21	1	7
Security Strat. Thinking	5.07	1.11	1.24	0.2	0.42	-0.57	0.21	1.45	7
IT Resource Mgmt.	4.83	1.06	1.12	0.23	0.42	-0.38	0.21	1.67	7
Governance	4.93	1.08	1.17	0.2	0.42	-0.49	0.21	1.4	7
Liability Mgmt.	4.77	1.25	1.55	-0.19	0.42	-0.41	0.21	1.33	7
Morale Mgmt.	4.89	1.06	1.13	-0.2	0.42	-0.25	0.21	1.67	7
Financial Outcomes	2.94	1.67	2.78	-0.43	0.42	0.66	0.21	1	7
Reputational Outcomes	2.8	1.84	3.39	-0.49	0.42	0.76	0.21	1	7
Competitive Outcomes	2.77	1.83	3.34	-0.61	0.42	0.72	0.21	1	7
Bus. Productivity Outcomes	3.59	1.66	2.76	-0.75	0.42	0.23	0.21	1	7

Table 29 Descriptive Statistics of Key Variables

	Fin. Losses	Rep. Losses	Comp. Losses	Bus. Prod Losses	Rev.	Employ. Size	IT Intensity	Formal Team	IT Mat.	Senior Execs
Fin. Losses	1.00	0.83***	0.83***	0.48***	0.05	0.26***	0.10	0.01	-0.09	-0.06
Rep. Losses	0.83***	1.00	0.88***	0.43***	0.02	0.22***	0.10	0.01	-0.15*	-0.07
Comp. Losses	0.83***	0.88***	1.00	0.57***	-0.05	0.20**	0.17**	0.02	-0.21**	-0.10
Bus. Prod. Losses	0.48***	0.43***	0.57***	1.00	-0.16*	-0.06	0.17**	0.10	-0.06	0.05
Revenue	0.05	0.02	-0.05	-0.16*	1.00	0.54***	-0.08	-0.27***	0.31***	-0.16*
Employee Size	0.26***	0.22***	0.20**	-0.06	0.54***	1.00	-0.12	-0.25***	0.21**	-0.31***
IT Intensity	0.10	0.10	0.17**	0.17**	-0.08	-0.12	1.00	0.03	0.04	0.02
Formal Team	0.01	0.01	0.02	0.10	-0.27***	-0.25***	0.03	1.00	-0.30***	0.59***
IT Maturity	-0.09	-0.15*	-0.21**	-0.06	0.31***	0.21**	0.04	-0.30***	1.00	-0.18**
Senior Execs	-0.06	-0.07	-0.10	0.05	-0.16*	-0.31***	0.02	0.59***	-0.18**	1.00

***** p<0.01, ** p<0.05, * p<0.10**

Table 30: Correlations of Key Variables

The next section is a discussion regarding the use of partial least squares structural equation modeling techniques to test the hypotheses from Chapter 5. The section begins with the rationale for utilizing partial least squares structural equation modeling in the study followed by a brief overview of the technique.

6.5 Structural Equation Modeling: Partial Least Squares

6.5.1 Rationale for PLS and Overview

This research study utilizes a quantitative analysis method referred to as "partial least squares" based structural equation modeling. This is commonly abbreviated as PLS, which is an alternative to OLS regression and covariance-based structural equation modeling techniques. PLS can be used to associate a set of independent variables in a study to multiple dependent variables in the same study (Garson, 2016). PLS can be implemented as both a regression model and as a path model making it useful for the purposes of this research study (Hair, Hult, Ringle, & Sarstedt, 2017). PLS is suitable for research whose purpose is to predict or explain phenomena, which is the purpose of this study. PLS is chosen in cases where 1) sample sizes are small 2) no distribution is assumed, as it doesn't assume normality in data and 3) when formative and reflective construct design is needed for the research model (Barclay, Higgins, & Thompson, 1995; Chin, 1998)[2]. This study does not have non-normal data however the study does have formative constructs, and reflective constructs in the research model and the sample size are considered small; especially by structural equation modeling standards. The research regarding partial least squares is still emerging relative to covariance-based structural equation modeling research, and many aspects of this quantitative technique are topic of great debate among the world's leading business scholars; as it is constraints and limits are continually being defined. However, the consensus is that PLS is a viable alternative to most all aspects of covariance-based structural equation modeling techniques (Ringle, Gotz, Wetzels, & Wilson, 2014; Henseler et al., 2014).

[2] Goodhue et al. (2012) and associated researchers are from a school of thought t that PLS does not have special properties in regards to showing significant relationships in small sample sizes. This is acceptable for our research purposes as it indicates PLS is a conservative estimation approach in regards to small sizes. Despite this, they indicate that PLS is one of the more accurate estimation approaches if accompanied by tests of statistical significance which our quantitative methodology utilizes in addition to bootstrapping.

PLS, like covariance-based structural equation modeling, is comprised of two interconnected models where the first model is focused on establishing the integrity of the constructs in relation to the underlying survey data and the second model is focused on the relationship amongst the constructs in one or more theoretical, relational models. The first model in regards to PLS is called the outer model. This model can also be referred to as the measurement model (which is the standard term used in covariance-based structural equation modeling). The second model is referred to as the inner model in the context of PLS or the structural model (this is the standard term used in covariance-based structural equation modeling). The measurement model utilizes confirmatory factor analysis to evaluate the relationship among a proposed set of latent variables, i.e. the survey constructs. This type of analysis evaluates how well the underlying questions (survey items) cluster together for a particular construct. It is important to gauge how well a particular construct measures what is it is intended to measure and exclusively what it is intended to measure, this is referred to as construct reliability and construct validity. As noted earlier in this chapter, steps were taken in the survey design process to maximize construct reliability and validity. Despite this, additional steps are taken post-hoc to ensure construct reliability and validity as well. There are specific metrics with established thresholds to let us know how reliable and valid a construct is, these are discussed in the next section. Once all the constructs are reliable and valid, the measurement model is said to be logical, valid, and reliable and the theoretical relationships, i.e. hypotheses testing can be done for what is now the structural model.

6.5.2 Overview of Confirmatory Factor Analysis and the Measurement Model

Fornell and Larcker (1981), suggest that the testing system for structural equation modeling first test the measurement model for reliability and validity[3]. This should be followed by a test of the

[3] For a detailed overview of the importance of these measures, please refer to the citations listed

structural model and then a test of the overall model. In this research study, the measurement model for reliability and validity is assessed first. To assess reliability "Cronbach's Alpha," the "Average Variance Extracted," and the "Composite Reliability" for each of the measurement constructs were calculated. The calculation of these measures requires that survey item loadings be known for each of the constructs (the lambdas). Average Variance Extracted for a construct is calculated as the sum of the squared factor loadings divided by the number of items. Cronbach's Alpha for a construct is calculated as $\alpha = \frac{\mathrm{N} \cdot \bar{c}}{\bar{v} + (N-1) \cdot \bar{c}}$ where N is the count of survey items that belong to that construct, c-bar is the covariance among the items that belong to the construct, v-bar is the average variance. Composite Reliability is calculated as CR=$\frac{(\sum \lambda i)\text{^}2}{(\sum \lambda i)\text{^}2 + (\sum 1 - \lambda i\text{^}2)}$ where lambda represents the factor loadings. The minimum recommended Cronbach’s Alpha is 0.70 with the minimum acceptable Average Variance Extracted being 0.50 and the minimum Composite Reliability should be 0.70 or greater. These thresholds are commonly accepted based on the criteria set forth by Fornell and Larcker (1981). Construct validity is evaluated by testing for common method bias. Common method bias is assessed by analyzing the correlation matrices between constructs (Bagozzi, Yi, & Phillips, 1991) where all correlations should be less than .90 indicating the model is free from multicollinearity. The variance inflation factors (VIFS) are also analyzed where all inner VIFS should be less than 3.3 which is an indication the model is not only free from multicollinearity but also common method (Kock & Lynn, 2015). Heterotrait-monotrait ratios were then assessed, where ratios should be less than 1 which is evidence of discriminant validity amongst the constructs (Henseler, Ringle, & Sarstedt, 2015) and it was also ensured that the constructs meet the Fornell & Larcker (1981) criteria of discriminant validity which states that the square root of the Average Variance Extracted for a construct should be greater than its correlation measure to other constructs in the model. We also assess how well the constructs in the model explain the variation in organizational losses utilizing the R-square measure. Since this is a novel study, the only expectation is that R-squared is not insignificant in the context of the research study and the study does not prescribe to a particular threshold for variation explained.

6.5.3 Overview of Hypotheses Testing

For the hypotheses testing there were two options available concerning the implementation of the PLS algorithm. One option implements an algorithm that provides a correction for estimates of reflective constructs in data that significantly vary from a normal distribution, and the other algorithm does not (see Dijkstra & Henseler, 2015). An analysis of skewness and kurtosis in the sample dataset reveals that the data is normally distributed. The normality of the data indicates that the estimates will require no corrections due for non-normality. The PLS algorithm with bootstrapping of 10,000 samples was implemented due to the small sample size, in addition, this enables the testing of structural models and obtains measures of statistical significance. In determining whether to reject or accept the hypotheses first, the coefficients are examined to determine if they are in the direction of the hypothesized relationships and second the coefficients are assessed for statistical significance at $p<0.10$. This research study utilizes a single research model in the quantitative analysis. This single research model is also utilized to conduct confirmatory factor analysis, for derivation of the measurement models and structural models, and for hypotheses testing. The results of each of these processes are presented. The statistical software package SmartPLS version 3 is utilized for the hypotheses testing ((Ringle, Wende, & Becker, SmartPLS 3, 2018). The chapter that follows is the evaluation of the research model and hypotheses outlined in Chapter 5 based on the aforementioned information in this section.

CHAPTER 7 EVALUATION OF RESEARCH MODEL

7.1 Prologue

This chapter develops and evaluates a parsimonious quantitative research model by bridging together the survey data and the conceptual research model. This is done through 1) exploratory data analysis, 2) development and testing of a measurement model (ensuring construct reliability and validity) and 3) development and testing of a structural model (hypotheses testing). Findings from each of these quantitative analyses are presented and the chapter concludes with a high-level discussion of the findings from the hypotheses testing.

7.2 Exploratory Data Analysis

Exploratory data analysis is conducted to better understand the relationships amongst the IT security breach characteristics and breach losses, the organizational response tactics and organizational losses, and finally the sample control variables and organizational losses. It is important to note that the development of the measurement and structural models were done in conjunction with the exploratory data analysis. Bivariate correlations were run for each of the relationships between IT security breach characteristics and breach losses, organizational response tactics and organizational losses, and sample control variables and organizational losses. To better assess the control variables, t-tests were conducted. In the three sections that follow, each of these relationships is explored more in-depth.

7.2.1 Assessment of Associations between Breach Characteristics and Losses

To evaluate the association of breach characteristics to losses, breach intentionality and breach source, were transformed from categorical variables to dichotomous variables. For the transformation, intentional IT security breaches are noted as having a value of 1 and unintentional IT security breaches have a value of 0. For the construct of breach source, breaches which had less than three sources related to the breach event have a value of 0 and breaches which have four or more sources are indicated with a value of 1. Breach sensitivity and extent of breach are continuous variables. The values of breach sensitivity ranged from 1-5 and extent of breach ranged from 1-7. Table 31 shows the bivariate correlations between breach characteristics and breach losses. The organizational losses differed based on the breach characteristics where breach intentionality was significantly and negatively correlated with financial losses, reputational losses and competitive losses with correlations ranging between -0.15 and -0.25 and $p < 0.10$.

In contrast, breach sensitivity is significantly and positively correlated with financial losses, reputational losses and competitive losses with correlations ranging between 0.16 and 0.27 and $p<0.10$. Breach source is significantly and positively correlated with competitive and business productivity losses with both sets of correlations at 0.18 and $p<0.05$. Finally, breach extent is significantly and positively associated with financial losses, competitive losses, and business productivity losses with correlations that range between 0.17 and 0.36 and $p<0.05$. The specific bivariate correlation measures including measures of statistical significance are located in Table 32.

	Breach Intent	Breach Sens.	Breach Source	Breach Extent	Fin. Losses	Rep. Losses	Comp. Losses	Business Prod. Losses
Breach Intent	1.00	-0.13	-0.05	-0.06	-0.25***	-0.15*	-0.24***	-0.12
Breach Sensitivity	-0.13	1.00	-0.05	0.02	0.24***	0.27***	0.16*	0.01
Breach Source	-0.05	-0.05	1.00	0.22***	0.12	0.12	0.18**	0.18**
Breach Extent	-0.06	0.02	0.22***	1.00	0.17**	0.14	0.21**	0.36***
Financial Losses	-0.25***	0.24***	0.12	0.17**	1.00	0.83**	0.83***	0.48***
Reputational Losses	-0.15*	0.27***	0.12	0.14	0.83***	1.00	0.88***	0.43***
Competitive Losses	-0.24***	0.16*	0.18**	0.21**	0.83***	0.88***	1.00	0.57***
Business Productivity Losses	-0.12	0.01	0.18**	0.36***	0.48***	0.43***	0.57***	1.00

***** p<0.01, ** p<0.05, * p<0.10**

Table 31: Bivariate Correlations between Breach Characteristics and Breach Losses

7.2.2 Assessment of Associations between Organizational Responses to IT Security Breaches and Organizational Losses

This section is an analysis of the correlation relationships between organizational response tactics groups and organizational loss constructs. The expectation is that all organizational response tactics are negatively correlated with organizational losses where an increase in the extent of the organizational response tactics decreases the losses. The bivariate correlation analysis finds that for financial losses communication management, IT resource management, liability management, and morale management are significantly and positively correlated. Reputational losses are only significantly correlated with liability management, and the relationship is positive. Business productivity losses have no significant correlations with any of the seven organizational response tactics.

	Losses				Organizational Response Tactics						
	Fin.	Rep	Comp	Bus. Prod.	Relat. Mgmt.	Comm. Mgmt.	Sec. Strat. Think.	IT Resrce.	Gov.	Liab. Mgmt.	Mor. Mgmt.
Fin. Losses	1	0.83***	0.83***	0.48***	0.13	0.18**	0.11	0.22**	0.14	0.26***	0.18**
Rep. Losses	0.83***	1	0.88***	0.43***	0.09	0.13	0.03	0.15	0.07	0.19**	0.12
Comp. Losses	0.83***	0.88***	1	0.57***	0.04	0.05	-0.02	0.15*	0.03	0.14	0.12
Bus. Prod. Losses	0.48***	0.43***	0.57***	1	0.01	0.07	0.03	0.09	-0.1	0.02	0.07
Rel. Mgmt.	0.13	0.09	0.04	0.01	1	0.7***	0.77***	0.77***	0.51***	0.82***	0.76***
Comm. Mgmt.	0.18**	0.13	0.05	0.07	0.7***	1	0.79***	0.68***	0.54***	0.61***	0.61***
Sec. Strat. Thinking	0.11	0.03	-0.02	0.03	0.77***	0.79***	1	0.78***	0.66***	0.72***	0.7***
IT Resource Mgmt.	0.22**	0.15	0.15*	0.09	0.77***	0.68***	0.78***	1	0.56***	0.77***	0.75***
Governance	0.14	0.07	0.03	-0.1	0.51***	0.54***	0.66***	0.56***	1	0.48***	0.54***
Liab. Mgmt.	0.26***	0.19****	0.14	0.02	0.82***	0.61***	0.72***	0.77***	0.48***	1	0.72***
Mor. Mgmt.	0.18	0.12	0.12	0.07	0.76***	0.61***	0.7***	0.75***	0.54***	0.72***	1

***** p<0.01, ** p<0.05, * p<0.10**

Table 32: Bivariate Correlations between Organizational Response Tactics and Losses

7.2.3 Assessment of Associations between Control Variables and Organizational Losses

This section evaluates the relationship amongst the sample control variables and organizational losses from IT security breaches. First bivariate correlations are utilized followed by t-tests to understand if there are differences between groups of a control variable. We find that revenue is negatively correlated with business productivity losses, employee size is positively correlated with reputational losses and competitive losses with correlation measures of 0.22 and 0.20 respectively at p<0.05. IT Intensity is positively associated with competitive losses and business productivity losses with both sets of correlations at 0.17. IT Intensity is the industry sector variable which was converted to a dichotomous variable for the purposes of bivariate correlation analysis and t-test, where an industry is IT Intensive (a value of 1) or Non-IT-Intensive (a value of 0). IT Maturity is negatively associated with reputational losses and competitive losses with correlations of -0.15 and -0.21 respectively at p<0.10 and p<0.05. The status of an organization's formal IT security team and IT security senior executives has no statistically significant correlations to organizational losses related to IT security breach events.

	Losses				Control Variables					
	Fin.	Rep.	Com	Bus Prod	Rev.	Size	IT Intensity	Formal Team	IT Maturity	Snr Execs
Financial Losses	1.00	0.83***	0.83***	0.48***	0.05	0.26	0.10	0.01	-0.09	-0.06
Reputational Losses	0.83***	1.00	0.88***	0.43***	0.02	0.22***	0.10	0.01	-0.15**	-0.07
Competitive Losses	0.83***	0.88***	1.00	0.57***	-0.05	0.20**	0.17**	0.02	-0.21**	-0.10
Bus. Prod Losses	0.48***	0.43***	0.57***	1.00	-0.16*	-0.06	0.17**	0.10	-0.06	0.05
Revenue	0.05	0.02	-0.05	-0.16**	1.00	0.54***	-0.08	-0.27***	0.31***	-0.16**
Employee Size	0.26***	0.22***	0.20**	-0.06	0.54***	1.00	-0.12	-0.25***	0.21**	-0.31***
IT Intensity	0.10	0.10	0.17**	0.17**	-0.08	-0.12	1.00	0.03	0.04	0.02
Formal Team	0.01	0.01	0.02	0.10	-0.27***	-0.25***	0.03	1.00	-0.30***	0.59***
IT Maturity	-0.09	-0.15*	-0.21**	-0.06	0.31***	0.21**	0.04	-0.30***	1.00	-0.18**
Senior Exec	-0.06	-0.07	-0.10	0.05	-0.16*	-0.31***	0.02	0.59***	-0.18**	1.00

***** p<0.01, ** p<0.05, * p<0.10**

Table 33: Bivariate Correlations between Control Variables and Losses

To further understand the relationship between sample control variables and organizational losses a t-test was conducted. Sample control variables measure inherent characteristics regarding the organization and therefore may prove helpful for organizations in gauging their risks from IT security breach events. The software package PSPP was utilized to conduct the t-test for dichotomous control variables. The control variables size and organizational revenue were analyzed where organizations are denoted as large or small based on revenue and employee size. In addition, the t-test is utilized to evaluate differences between organization's that had a senior executive responsible for IT and those that did not, because of duplicity it was not necessary to conduct a t-test evaluating regarding if differences in an IT security leadership job title had any relationship to losses from IT security breach events.

We found that there were statistically significant differences in means for competitive and business productivity losses for IT-intensive organizations (2.96, 3.76) compared to organizations that were not IT-intensive (2.23, 3.1). The results were statistically significant at p<0.05 and p<0.10 respectively where the mean losses for IT-intensive organizations were higher than non-IT intensive organizations. A small organization, i.e. organizations with $10 million or less a year in revenue experience greater business productivity losses compared with larger organizations at p<0.05 (3.99 versus 3.37). Larger organizations i.e. those with 1,000 or more employees have statistically significant differences for financial, reputational, and competitive losses than smaller organizations with more substantial mean losses all differences are statistically significant at p<0.05[4]. Also, there are no statistically significant differences in mean losses from IT security breach events for organizations with an IT security executive and those without one and no statistically significant difference in mean losses from IT security

[4] Based on guidelines from the Small Business Administration a small business is typically considered an organization with annual revenues of $7.5 million or less and/or less than 500 employees. For this study, a small organization is considered an organization with less than $10 million in annual revenues and/or less than 1000 employees these cutoffs are due to constraints in how the data was collected for the study.

breach events for organizations with a formal unit or team to handle IT security breach events and those without one.

	IT Intensive (n=96) Mean	Non-IT Intensive (n=32) Mean	t Value (Sig)
Financial Losses	3.03	2.66	1.09
Reputational Losses	2.91	2.48	1.14
Competitive Losses	2.96	2.23	2.06**
Business Productivity Losses	3.76	3.1	1.94*

***** p<0.01, ** p<0.05, * p<0.10**

Table 34: IT Intensive Industry vs. Non-IT Intensive Industry

	Revenue>=$10,000,000 (n=47) Mean	Revenue <$10,000,000 (n=81) Mean	t Value (Sig)
Financial Losses	2.7	3.07	-1.21
Reputational Losses	2.63	2.91	-0.83
Competitive Losses	2.79	2.99	0.06
Business Productivity Losses	3.99	3.37	2.06**

***** p<0.01, ** p<0.05, * p<0.10**

Table 35 Organizational Revenue >= $10M vs. Revenue < $10M

	Employees >=1,000 (n=92) Mean	Employees <1,000 (n=36) Mean	t Value (Sig)
Financial Losses	3.21	2.24	3.41***
Reputational Losses	3.05	2.17	2.5**
Competitive Losses	3.00	2.19	2.31**
Business Productivity Losses	3.54	3.74	-0.65

***** p<0.01, ** p<0.05, * p<0.10**

Table 36: Count of Employees >=1,000 vs. Count of Employees <1,000

	IT Security Executive (n=106) Mean	No IT Security Executive (n=22) Mean	t Value (Sig)
Financial Losses	2.98	2.73	0.64
Reputational Losses	2.86	2.52	0.79
Competitive Losses	2.85	2.39	1.09
Business Productivity Losses	3.56	3.77	-0.55

***** p<0.01, ** p<0.05, * p<0.10**

Table 37: IT Security Executive vs. No IT Security Executive

	Formal Unit/Team (n=110) Mean	No Formal Unit/Team (n=18) Mean	t Value (Sig)
Financial Losses	2.93	2.99	-0.14
Reputational Losses	2.80	2.86	-0.14
Competitive Losses	2.76	2.86	-0.22
Business Productivity Losses	3.53	4.00	-1.12

***** p<0.01, ** p<0.05, * p<0.10**

Table 38: Formal Unit/Team for IT Security Breaches vs. No Formal Unit/Team for IT Security Breaches

The next section discusses the measurement model, followed by a discussion of the structural model including the results of the hypotheses testing.

7.3 The Quantitative Research Model

7.3.1 Operationalization and Description of Quantitative Research Model

This study utilizes a measurement model that consists of all seven organizational response tactic and organizational outcome variables with reflective item measures. The measurement model also includes the five IT security breach characteristics that were measured as continuous variables or dichotomous variables. Extent of breach was conceptualized as a six-item formative construct due to low convergent validity. Breach source was modeled as a single item dichotomous construct where three or fewer sources for an IT security breach was indicated as 0 otherwise the indicator was 1, breach sensitivity was modeled a single item continuous variable, and breach intentionality was modeled as a dichotomous construct (Intentional or Unintentional). Two control variables were included in the measurement model and structural model, these include a dichotomous variable for Industry sector (IT Intensive vs. Non-IT Intensive) and revenue as a proxy for organizational size These variables were selected as they are two common control variables utilized when organizations or firms are the subject of study in research involving quantitative models as industry and revenue may confound effects, and this needs to be controlled for (for an examples see Karimi et al. 2004, Mithas et al. 2012).

7.3.2 The Measurement Model

The next three tables detail the findings of the measurement model. All items had loadings greater 0.50; Average Variance Extracted was greater than 0.50 for all constructs, Cronbach Alpha's and Composite Reliability were all greater than >0.70, all variables demonstrated discriminant validity based on the Fornell & Larcker (1981) criteria and the Heterotrait-Monotrait ratios being less than 1. Items with loadings less than 0.50 or items that significantly cross-loaded onto constructs that they were not intended to measure were dropped from the measurement model. Table 39, contains a final list of items and their corresponding loadings after dropping of items. Note that single item measures (i.e., loadings with 1.0) are not included in the table but details of the item, e.g. the question wording can be found in the survey located in Appendix B. Single item measures, or formative constructs includes extent of breach, breach sensitivity, breach source, breach intentionality, industry, and organizational revenue. These are the constructs for IT security breach characteristics and the control variables, respectively.

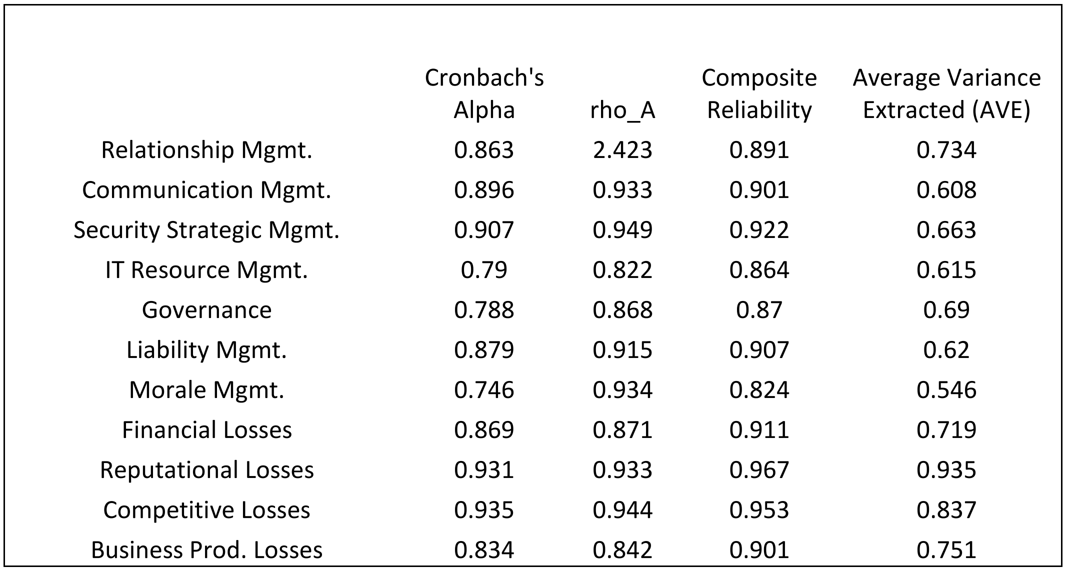
Relationship Management	**Standard Loadings**
My organization regularly reviews the information security and privacy policies, practices and procedures of external parties who collect, store, use or access the data	0.777
My organization regularly reviews agreements and work arrangements with contracted IT security vendors	0.983
My organization regularly engages the external business partners in reviewing IT security arrangements	0.795
Communication Management	
My organization has designated specific personnel to communicate about any IT security breaches	0.631
My organization has an official plan outlining how to communicate internally about IT security breaches	0.721
My organization has an official plan outlining how to communicate externally about IT security breaches	0.619
My organization ensured timely notification to all internal stakeholders about the breach	0.91
My organization ensured timely notification to external stakeholders about the breach	0.897
My organization had a clear, strategy-based public relations response about the breach	0.845
Security Strategic Management	
My organization has a formal plan in place for managing IT security	0.854
My organization's IT security strategy includes both technical and non-technical aspects	0.847
Our IT security strategy covers all digital assets (hardware, software, and applications) and data hosted internally as well as externally	0.888
Our IT security strategy covers external IT vendors or third parties we use for any IT or data related work	0.75
Our IT security strategy covers employee-owned IT, mobile devices and digital accessories that they bring to work	0.828

My organization has formal training program(s) to increase IT security awareness among employees	0.703
IT Resource Management	
My organization uses advanced biometric authentication techniques (e.g., using fingerprint, retina scan, facial identification, etc.)	0.669
After the breach, my organization decided to hire additional IT security staff	0.868
After the breach, my organization made readjustments to internal teams	0.789
After the breach, we invested in newer IT security systems or applications.	0.798
Governance	
My organization has adopted and implemented one or more international standards for handling IT security breaches	0.799
My organization has developed formal procedures and rules for managing any IT security breaches	0.814
In my organization, IT security is the responsibility of both IT and other functional managers	0.877
Liability Management	
My organization has invested in adequate cyber insurance to cover any potential damages arising from cyber-attacks or IT security breaches	0.773
My organization has adequate liability provisions in contractual agreements with external organizations who collect, store, use or access the data	0.791
My organization regularly reviews contractual protections and vendor liabilities related to IT security breaches	0.733
My organization reviewed vendor liability policies after the breach	0.779
My organization reviewed current cyber-insurance provisions after the breach	0.784
My organization invested in additional insurance for addressing potential future breaches	0.859
Morale Management	
My organization has explicit rewards (punishments) for compliance (non-compliance) with organization prescribed IT security protocols	0.629

My organization regularly engages employees from different departments or units to enhance IT security	0.619
My organization engaged in specific activities to boost employee morale after the breach	0.911
My organization provided autonomy to IT security professionals to handle the breach	0.759
Financial Losses	
Decline in stock prices	0.863
Decline in organizational revenue	0.888
Increase in cost of operations	0.812
Legal costs	0.826
Reputational Losses	
Loss of company reputation or image	0.965
Loss of public goodwill	0.969
Competitive Losses	
Loss of competitive advantage	0.896
Severed relationships with suppliers or partners	0.949
Loss of existing customers	0.889
Loss of potential, new customers	0.924
Business Productivity Losses	
System downtime	0.818
Loss in employee productivity	0.875
Time delays in business operations	0.905

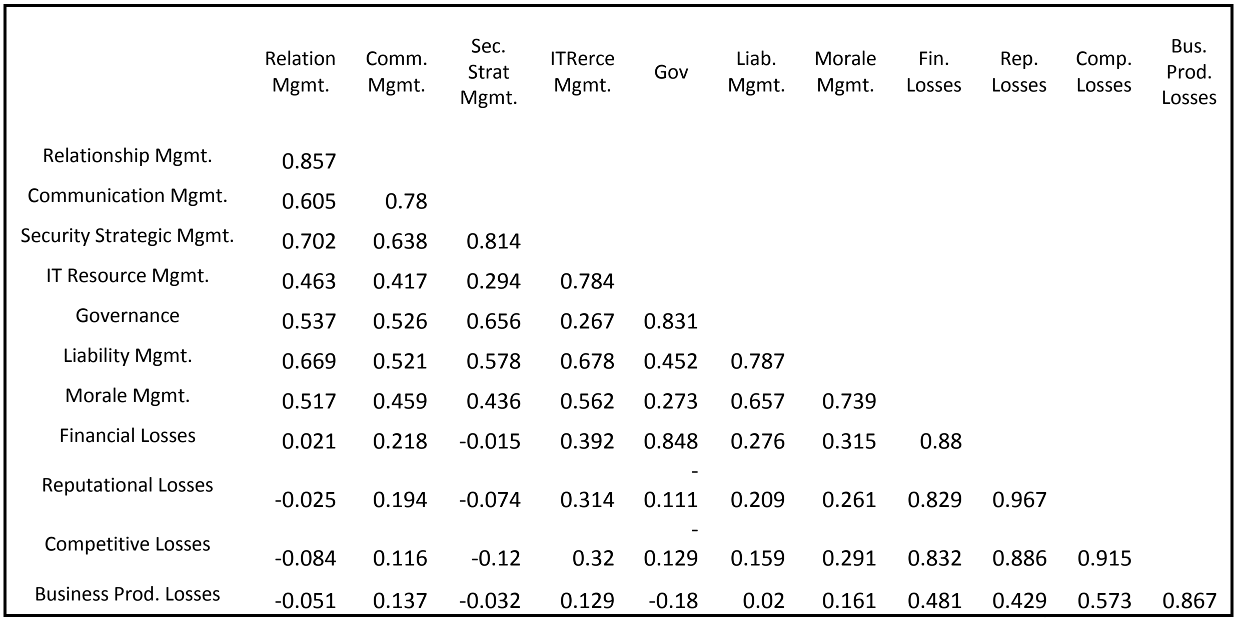
Table 39: Measurement Model Constructs and Factor Loadings[5]

[5] Scale used to measure organizational responses are as follows: 7=Strongly Agree, Agree, Somewhat Agree, Neither Agree nor Disagree, Somewhat Disagree, Disagree, 1=Strongly Disagree. Scales used for organizational losses are as follows 7=A Great Deal, Significantly, A Lot, Moderately, Somewhat, Slightly, 1=None. The following questions were omitted from the measurement model and are listed in Appendix B: Q21.1-21.5, Q22, Q25, Q29.1-Q29.2, Q31-Q33, Q34.3, Q34.8, Q36.1, Q34.2, Q36.4, Q38, Q40.1, Q41.1-Q41.3; Q42.1-Q42.4, Q42.6, Q44.1, Q49.3



	Cronbach's Alpha	rho_A	Composite Reliability	Average Variance Extracted (AVE)
Relationship Mgmt.	0.863	2.423	0.891	0.734
Communication Mgmt.	0.896	0.933	0.901	0.608
Security Strategic Mgmt.	0.907	0.949	0.922	0.663
IT Resource Mgmt.	0.79	0.822	0.864	0.615
Governance	0.788	0.868	0.87	0.69
Liability Mgmt.	0.879	0.915	0.907	0.62
Morale Mgmt.	0.746	0.934	0.824	0.546
Financial Losses	0.869	0.871	0.911	0.719
Reputational Losses	0.931	0.933	0.967	0.935
Competitive Losses	0.935	0.944	0.953	0.837
Business Prod. Losses	0.834	0.842	0.901	0.751

Table 40: Measurement Model Construct Reliability and Validity



	Relation Mgmt.	Comm. Mgmt.	Sec. Strat Mgmt.	ITRerce Mgmt.	Gov	Liab. Mgmt.	Morale Mgmt.	Fin. Losses	Rep. Losses	Comp. Losses	Bus. Prod. Losses
Relationship Mgmt.	0.857										
Communication Mgmt.	0.605	0.78									
Security Strategic Mgmt.	0.702	0.638	0.814								
IT Resource Mgmt.	0.463	0.417	0.294	0.784							
Governance	0.537	0.526	0.656	0.267	0.831						
Liability Mgmt.	0.669	0.521	0.578	0.678	0.452	0.787					
Morale Mgmt.	0.517	0.459	0.436	0.562	0.273	0.657	0.739				
Financial Losses	0.021	0.218	-0.015	0.392	0.848	0.276	0.315	0.88			
Reputational Losses	-0.025	0.194	-0.074	0.314	- 0.111	0.209	0.261	0.829	0.967		
Competitive Losses	-0.084	0.116	-0.12	0.32	- 0.129	0.159	0.291	0.832	0.886	0.915	
Business Prod. Losses	-0.051	0.137	-0.032	0.129	-0.18	0.02	0.161	0.481	0.429	0.573	0.867

Table 41: Measure of Discriminant Validity (Fornell-Larcker Criterion)[6]

The next section discusses the evaluation of the structural model, presents the results of the hypotheses testing, and further explores the results in the context of the relationship between organizational responses to IT security breach events and organizational losses.

[6] The hetero-monotrait ratios are an alternative measure of discriminant validity. All ratios were less than 1.0 demonstrating that the constructs met the requirement of discriminant validity. Not shown due to redundancy.

7.3.3 The Structural Model

The structural model is evaluated for common method bias, multicollinearity, and for how well it explains the variance in the organizational losses from IT security breach events. The evaluation is based on criteria outlined in Chapter 6. This model is not expected to have issues with multicollinearity of constructs or common method bias/variance based on inner VIF's being less than 3.3 except for the "Liability Management" construct which has an inner VIF of 3.7. This construct was kept in the model because it was essential to the research and it is otherwise a reliable and valid construct. Table 42 depicts the variance inflation factors for the constructs in the structural model.

	Business Prod. Losses	Competitive Losses	Financial Losses	Reputational Losses
Communication Mgmt.	2.065	2.065	2.065	2.065
Governance	2.361	2.361	2.361	2.361
IT Resource Mgmt.	2.213	2.213	2.213	2.213
Liability Mgmt.	3.473	3.473	3.473	3.473
Morale Mgmt.	2.095	2.095	2.095	2.095
Relation Mgmt.	2.798	2.798	2.798	2.798
Sec. Strat. Mgmt.	3.208	3.208	3.208	3.208

Table 42: Measure of Common Method Bias and Multicollinearity via Variance Inflation Factors (VIFS)

The organizational response tactics in the model account from between 21% to 27% of the variance in organizational responses based on the range of adjusted R-squares. At first glance, the R-squares appear low, but the range still does provide valuable evidence that organizational responses do indeed influence organizational losses, and the relationship is more than a nominal one.

	R Square	R Square Adjusted
Business Prod. Losses	0.315	0.237
Competitive Losses	0.318	0.240
Financial Losses	0.343	0.268
Reputational Losses	0.316	0.238

Table 43: Research Model Variation Analysis

The structural model in the study tests twenty-eight, theory-driven, hypothesized relationships among organizational responses and organizational losses utilizing the full quantitative research model. The results of the hypotheses testing are noted in Table 44.

Hypotheses	Support	Coefficient	STDEV	P Values	Unexpected Result
H1A: In organizations that experience an IT security breach event, an increase in the extent of relationship management tactics will be associated with a decrease in financial losses	Full	-0.267	0.154	0.083	No
H1B: In organizations that experience an IT security breach event, an increase in the extent of relationship management tactics will be associated with a decrease in reputational losses	Partial	-0.22749	0.170046	0.180	No
H1C: In organizations that experience an IT security breach event, an increase in the extent of relationship management tactics will be associated with a decrease in competitive losses	Full	-0.31875	0.181228	0.078	No
H1D: In organizations that experience an IT security breach event, an increase in the extent of relationship management tactics will be associated with a decrease in business productivity losses	Partial	-0.17496	0.16	0.274	No
H2A: In organizations that experience an IT security breach event, an increase in the extent of communication management tactics	None	0.296	0.154	0.055	Yes

will be associated with a decrease in financial losses					
H2B: In organizations that experience an IT security breach event, an increase in the extent of communication management tactics will be associated with a decrease in reputational losses	None	0.362886	0.187189	0.052	Yes
H2C: In organizations that experience an IT security breach event, an increase in the extent of communication management tactics will be associated with a decrease in competitive losses	None	0.249864	0.162667	0.124	Yes
H2D: In organizations that experience an IT security breach event, an increase in the extent of communication management tactics will be associated with a decrease in business productivity	None	0.285407	0.164462	0.082	Yes
H3A: In organizations that experience an IT security breach event, an increase in the extent of security strategic thinking tactics will be associated with a decrease in financial losses	None	-0.180	0.167	0.280	No
H3B: In organizations that experience an IT security breach event, an increase in the extent of security strategic thinking tactics will be associated with a decrease in reputational losses	None	-0.23461	0.179739	0.191	No
H3C: In organizations that experience an IT security breach event, an increase in the extent of security strategic thinking tactics will be associated with a decrease in competitive losses	None	-0.17799	0.176392	0.312	No
H3D: In organizations that experience an IT security breach event, an increase in the extent of security strategic thinking tactics will be associated with a decrease in business productivity losses	None	0.158821	0.194358	0.413	Yes
H4A: In organizations that experience an IT security breach event, an	None	0.258	0.100	0.010	Yes

increase in the extent of IT resource management tactics will be associated with a decrease in financial losses					
H4B: In organizations that experience an IT security breach event, an increase in the extent of IT resource management tactics will be associated with a decrease in reputational losses	None	0.196464	0.101595	0.053	Yes
H4C: In organizations that experience an IT security breach event, an increase in the extent of IT resource management tactics will be associated with a decrease in competitive losses	None	0.242459	0.107273	0.023	Yes
H4D: In organizations that experience an IT security breach event, an increase in the extent of IT resource management tactics will be associated with a decrease in business productivity losses	None	0.097311	0.13626	0.475	No
H5A: In organizations that experience an IT security breach event, an increase in the extent of governance management tactics will be associated with a decrease in financial losses	Partial	-0.123	0.129	0.339	No
H5B: In organizations that experience an IT security breach event, an increase in the extent of governance management tactics will be associated with a decrease in reputational losses	Partial	-0.1825	0.1353	0.177	No
H5C: In organizations that experience an IT security breach event, an increase in the extent of governance management tactics will be associated with a decrease in competitive losses	Partial	-0.12106	0.123505	0.327	No
H5D: In organizations that experience an IT security breach event, an increase in the extent of governance management tactics will be associated with a decrease in business productivity losses	Full	-0.28536	0.15074	0.058	No
H6A: In organizations that experience an IT security breach event, an increase in the extent of liability management tactics will be associated with a decrease in financial losses	None	0.125	0.151	0.408	Yes

H6B: In organizations that experience an IT security breach event, an increase in the extent of liability management tactics will be associated with a decrease in reputational losses	None	0.099842	0.156001	0.522	Yes
H6C: In organizations that experience an IT security breach event, an increase in the extent of liability management tactics will be associated with a decrease in competitive losses	None	0.028786	0.154158	0.851	Yes
H6D: In organizations that experience an IT security breach event, an increase in the extent of liability management tactics will be associated with a decrease in business productivity losses	Partial	-0.13736	0.176784	0.437	No
H7A: In organizations that experience an IT security breach event, an increase in the extent of morale management tactics will be associated with a decrease in financial losses	None	0.155	0.111	0.161	Yes
H7B: In organizations that experience an IT security breach event, an increase in extent of morale management tactics will be associated with a decrease in reputational losses	None	0.135494	0.1044	0.194	Yes
H7C: In organizations that experience an IT security breach event, an increase in the extent of morale management tactics will be associated with a decrease in competitive losses	None	0.246841	0.111125	0.026	Yes
H7D: In organizations that experience an IT security breach event, an increase in the extent of morale management tactics will be associated with a decrease in business productivity losses	None	0.073866	0.1312	0.573	Yes

Table 44: Results of Hypotheses Testing

The hypothesis testing reveals that nine of the hypothesized relationships are fully supported or partially supported.[7] However, there were hypothesized relationships which were not only

[7] Fully supported hypotheses in this study are hypotheses in which the p-value is equal to or less than 0.10, and the coefficient is in the correct direction for the hypothesized relationship. Partially supported hypotheses are hypotheses in which the p-values are not statistically significant at

unsupported, but the relationships were statistically significant and required further evaluation. A field was added to Table 44 to denote if the results of the hypotheses were expected or unexpected. Expected results are results in which the coefficient is in the correct direction regardless of statistical significance. Unexpected results are results that are in the opposite direction of the hypothesized relationship from the research model outlined in this study. Figure 6 is an illustration of the full research model including path coefficients and p-values for all variables utilized in the study.

$p<0.10$, however, the coefficient is in the correct direction for the hypothesized relationship. No support indicates that the coefficient is greater than >.10 and the coefficient is not in the direction of the hypothesized relationship.

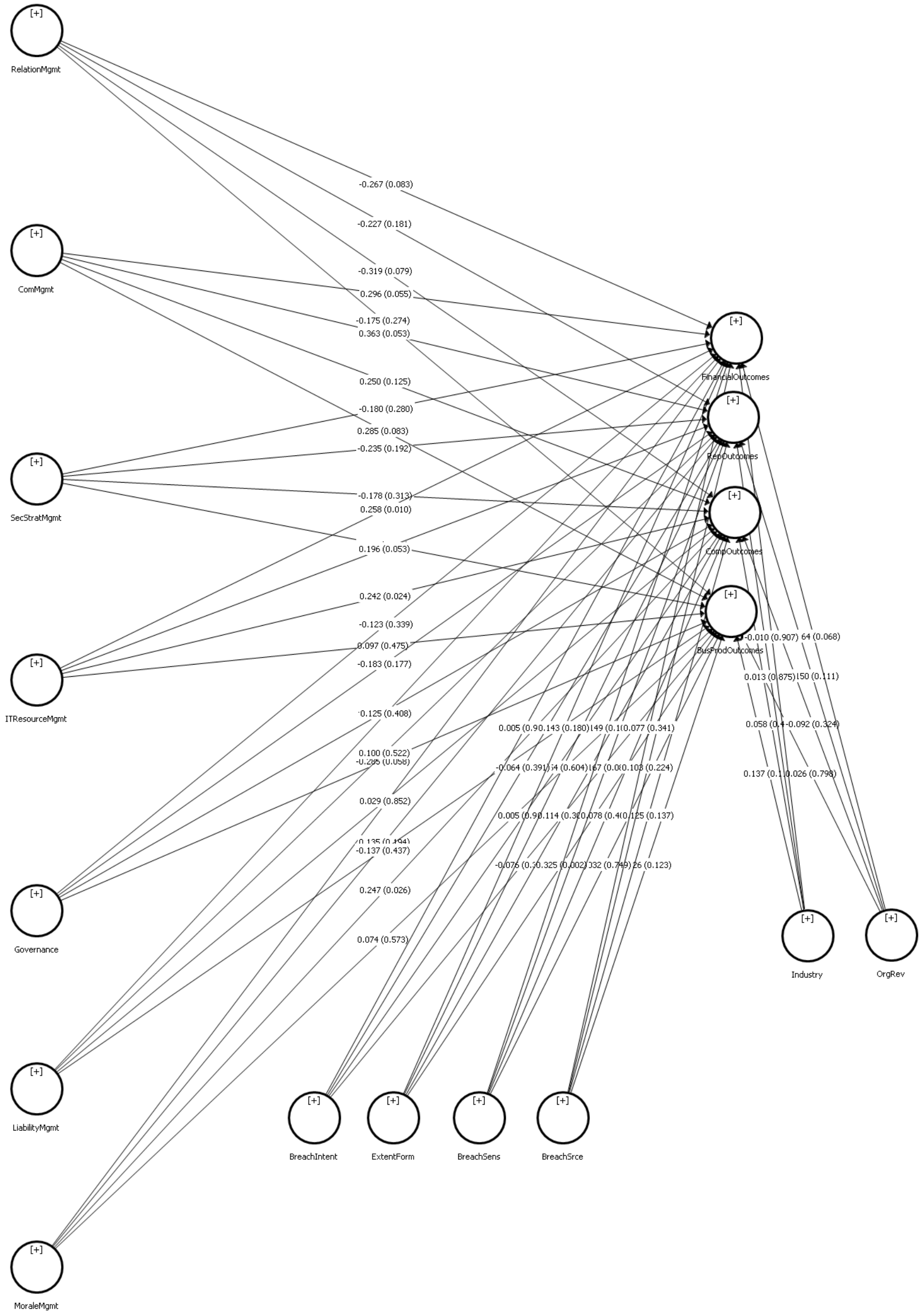


Figure 6: Path Model with Coefficients and P-Values[8]

[8] Note that industry is a dichotomous variable which is a proxy for whether an organization is IT-intensive or not. In addition, organizational revenue is also a dichotomous variable and is a proxy for organizational size. Organizations can either be large or small. Detailed descriptions of the control variables are located on Table 22.

CHAPTER 8: DISCUSSION

8.1 Prologue

This chapter discusses the findings from the testing of the research model. The testing of the research model encompasses twenty-eight hypotheses that examine the relationships between organizational response constructs and organizational loss constructs. To review, the research goals of this study were to 1) understand organizational responses pertaining to IT security breaches and 2) examine if the differences in organizational losses vary due to the varied organizational responses to IT security breach events. Thus far in this research study, a semi-structured literature review of the existing government, practitioner, and academic literature has been conducted. This was then followed by structured field interviews with seven IT security executives. From these field interviews and the literature review, a conceptual model was derived to describe the relationship amongst the three constructs related to IT security breach events. The structural model consists of the three constructs of 1) IT security breach characteristics, 2) organizational response tactics, and 3) organizational losses. The findings from the literature review and field interviews indicate that there are 4 types of IT security breach characteristics, 7 types of organizational response tactics and 4 types of organizational losses from IT security breach events. From this conceptual model, a survey was developed and pre-tested on 14 IT security practitioners. Finally, a survey was deployed for the collection of field data to test twenty- eight hypotheses regarding the relationships between organizational response tactics and organizational losses. The final sample utilized for quantitative analysis including hypotheses testing contains 128 completed survey responses. Finally, PLS-based structural equation modeling techniques were utilized to test the hypothesized relationships in the research model.

Sections 8.2-8.5 discuss organizational responses tactics in the context of each of the four loss types from IT security breach events. Section 8.6 is the post-hoc analysis discussion. For unexpected results a new set of field interviews were conducted with two subject matter IT security expert who combined, have over 60 years of IT security related experience. The subject matter experts have both worked in or consulted for a wide variety of organizations, but their primary subject matter expertise's are in the healthcare and supply chain management fields, respectively. In the passages that follow the subject matter experts are denoted as subject matter expert 1 (SME 1) and subject matter expert 2 (SME 2). The quotes from the full interviews are located in Appendix C. This chapter utilizes the interview data from the subject matter experts to contextualize the unexpected findings from the hypothesis testing. The opinions of the subject matter experts are subjective, despite this; the opinions offer additional insights for which this study otherwise would not have due to the emerging nature of this research stream. From the discussions that follow an understanding develops of what the most optimal organizational response tactics are so that organizations can minimize losses related to IT security breach events. This knowledge will be helpful for IT security practitioners, decision makers, and academic researchers.

8.2 Financial Losses and Organizational Response Tactics

The seven organizational response tactics have nuanced relationships to financial losses. Financial losses from IT security breach events include such losses as declines in one more measure of revenue, increases in the cost of operations, declines in stock prices, and legal costs. PLS analysis indicates that relationship management tactics have a significant negative association with financial losses (-0.267, $p<0.10$), and an insignificant negative association with security strategic thinking (-0.180, p=0.28), and governance (-0.123, p=0.339). Alternately, communication management (0.296, p<0.10) and IT resource management (0.258, p<.001) were found to be significantly and positively associated with financial losses. Liability management (0.125, p=.408), and morale management (0.155, p=.161) were found to be positively associated with financial losses from IT security breach events however the results are not significant.

Some of the aforementioned relationships are unexpected. However, in some ways, it is unsurprising that four out of the seven of the organizational response tactics appear to be unhelpful in the management of IT security breach events related to financial losses. Financial losses may be difficult to avoid as organizations can incur not only legal liabilities towards private citizens (Romanosky, 2016) and the government (Jaeger, 2015); but for publicly traded companies, market value can be lost from declining stock prices and lost revenue (Cavusoglu, Mishra, & Raghunathan, 2004; Chen, Li, Yen, & & Bata, 2012; Garg, Curtis, & & Halper, 2003; Hovav and D'Arcy 2004; Yayla and Hu 2011). These financial losses could occur simply because the IT security breach occurred regardless if there were any adverse impact to individuals. Aside from financial losses being arguably the most prevalent loss types related IT security breach events, the subject matter experts were able to shed light on why the four of the seven organizational response tactics may be ineffective, if not downright harmful in the context of financial losses.

Regarding communication management and financial outcomes, there was a slight difference of opinion where either lack of transparency could cause unexpected results, or the results were due to an increase in management and bureaucracy after the IT security breach. For IT resource management and financial outcomes, unexpected results could occur because of a lack of resources which may cause fines for the organization, or the problem could lie in how an organizations IT group is set up. Determining if the IT group is project driven or driven by the growth needs of the organization will be helpful in utilizing IT resource management tactics. If the IT group is project driven the IT function is less likely to be prepared for a breach event when it occurs. The two subject matter experts agreed that morale management in the context of worsening financial losses could be associated with a superficial implementation of the tactics and were both assuring in that organizational morale will start negative but should increase over time after an IT security breach event. SME 1 states the following:

"Morale will start off bad in the context of finance. Morale will get hit a little"

SME 2 adds that if morale management is focused on behavior modification rather than genuine improvement of the psychological environment, then this may be a culprit for the increase in financial losses associated with morale management organizational response strategies. SME 2 states:

"Is the morale management, genuine, superficial or is it behavior modification. If they're trying to modify company behavior through morale not sure if it will lead to positive outcomes. This is the same for all outcomes related to morality."

In examining the relationship between liability management and financial losses, liability management response tactics may not be helpful because of so called moral hazard risk which is an inherent downside of financial indemnity contracts. SME 1 shared the following:

"In order for you to get a good rating or cyber insurance, you need to have certain things in place, good hygiene. You may not get good insurance rating thus causing an increase in financial losses. If you have issues you may not get cyber insurance, you will get declined, or rate may go up."

SME 2 had a different opinion and theorized that liability management in the context of financial losses might not be successful due to a company's risk appetite. Essentially, organizations may be punished for not being creative in the management of their liabilities. SME 2 states:

"A more risk-averse company may see more risk-averse environment with no risk or innovation taken."

At a high level, the overall results indicate that organizational response tactics with the exception of relationship management may not have any impact at all on reducing financial losses from IT security breach events. Security strategic thinking and governance tactics exhibited a negative association with financial losses, but the results were not statistically significant. This does not mean that security strategic thinking and governance tactics should not be utilized, but perhaps it is important to ensure that the costs of implementing these strategies will pay off in the event of an IT security breach event.

8.3 Reputational Losses and Organizational Response Tactics

Reputational losses from IT security breaches events are measured in this study. Traditionally, in the extant literature, reputational losses from IT security breach events were accounted for by measuring changes in the stock market prices of public traded organizations (Hovav & D'Arcy 2004; Yayla and Hu 2011). This concept of accounting for reputational losses stemmed from the notion that changes to stock market prices following an event (including IT security breach events) could provide the assessment of a large body of diverse stakeholders in regards to the event and its impact on an organization (Cavusoglu et al. 2004; Chen et al. 2012; Garg et al. 2003; Hovav & D'Arcy, 2003) and is measured in financial terms. Although measuring changes to stock market prices after an event can be helpful in gauging the financial health of an organization, this unit of measurement for reputational losses may not be helpful for frontline practitioners and decision makers in regards to providing actionable insights on managerial responses pertaining to IT security breach events. From the extant literature on IT security breach events, reputational losses encompass company image, loss of public goodwill, and loss of trust (Ettredge & Richardson 2003, Goel and Shawky 2009; Olmstead & Smith, 2017; Farrell, 2017). These types of losses are difficult to articulate with observable data as there is a certain measure of intangibility to the construct of reputational losses. However, the use of Likert scaled survey items presents an opportunity to measure this construct within organizations and specifically in relation to IT security breach events. Based on the PLS analysis none of the seven organizational response tactics exhibit significant, negative associations with reputational losses. The results may indicate that reputational losses resulting from IT security breach events are irreparable and despite organizations taking several steps in the form of varied organizational responses, organizations are still likely to suffer reputational harm. Relationship management (-0.217, p=0.170), security strategic thinking (-0.234, p=0.191), and governance (-0.183, p=0.177) organizational response tactics have insignificant, negative relationships with reputational losses. Four of the organizational response tactics exhibited unexpected results in their relationship to reputational losses from IT security breach events. These tactics are communication management (0.362, p<.0.10), IT resource management (0.196, p<.0.10), liability management (0.10, p=0.52), and morale management (0.135, p=0.194)).

It is unclear from the extant literature review and the previous interviews with IT security executives why this may be occurring. To better understand these unexpected relationships, the expertise of subject matter expert 1 and subject matter expert 2 were sought. SME 1 concluded the following:

> *"Not sure why this is happening but if you utilize communication management you can have nothing but positive outcomes. When I think management I think management teams. Notifying them about the breach and new controls is going to trick down to the staff. Reputation will become good if positive communication. PR and marketing tell us how to state things when big issues and breaches happen things are sugarcoated; these are professionals. The process works, and the outcome would be good. "*

SME 2 theorized that lack of transparency during the implementation of communication management organizational response tactics could be to blame and stated the following:

> *"Part of this could be attributed to the reduction in transparency. Reducing transparency causes a reduction in the reputation."*

In regards to why IT resource management organizational response tactics seem to be associated with increases in reputational losses SME 1 notes:

> *"Again, these are the guys who would do the management for you. If you don't have a good team that is the only way it would cause a problem."*

However, SME 2 notes that if organizational IT resources are focused on projects rather than growth, organizations will see this phenomenon occurring with the use of IT resource management organizational response tactics:

> *"Again, the same project focus of IT versus a growth focus of IT can limit agility people are scrambling."*

Liability management and morale management organizational response tactics also exhibited positive associations with reputational losses. However, the associations were not significant. Furthermore, liability management has p-value approaching 0.50 indicating that more than likely its association with reputational losses is no different than what would occur by chance. Morale management has a lower p-value than liability management tactics but the relationship is still insignificant. In regard to this relationship, SME 2 reiterated the importance of having genuine morale management organizational response tactics in place and SME 1 shared the following thoughts regarding this relationship:

> *"Want to let outsiders know the company is sorry. Someone will get fired. Reputation will start off shaky, but you can bounce back. "*

Additional research will need to be conducted to understand better if the punishment of senior leadership for an IT security breach event increases organizational morale. It is common practice that after an IT security breach event occurs within an organization senior leadership within the IT security function of an organization is replaced.

8.4 Competitive Losses and Organizational Response Tactics

In addition to financial and reputational losses from IT, security breach events organizations can also experience competitive losses from such events. Competitive losses from IT security breach events encompass such losses as severed relationships, loss of existing customers, and loss of potential and new customers, and losses from user tracking (CISCO, 2017 Annual Cybersecurity Report, SafeNet 2016 Survey; Sanger, Chan, & Scott, 2017). PLS analysis indicates relationship management to be the only organizational response construct with significant, negative association (-0.318, p <0.10) with competitive losses. Security strategic thinking (-0.177, p=0.31) and governance (-0.121, p=0.33) also exhibited negative, yet insignificant, associations with competitive losses. IT resource management (0.252, p<0.10) and morale management (0.246, p<0.5) exhibited positive, significant associations with competitive losses. Communication management (0.249, p=0.12) and liability management (0.028, p=0.86) exhibited positive but insignificant associations. A reduction in transparency may help to explain the unexpected relationship between communication management organizational response tactics and competitive losses. SME 1 states that:

> *"Proper communication should help to show how competitive the organization is. Will help in outcome when it comes to competition consider transparency of privacy policies."*

SME 2 succinctly stated “reduced transparency” as the sole cause for this phenomenon. The relationship between IT Resource Management and competitive losses could occur if IT teams are not in place or if the IT resources are not agile which can be caused by organizational bureaucracy. Regarding morale management and competitive outcomes, SME 1 notes that improper implementation of morale management response tactics may cause apathy and mistakes amongst employees and this may decrease organizational competitiveness. On a similar note, SME 2 notes that morale management can be genuine or superficial. If morale management is superficial, it will not improve an organization's competitive outcomes from IT security breach events. Lastly, the hypotheses testing found that liability management is positively associated with competitive outcomes however the relationship is not significant with a p=0.85 and a coefficient of 0.028. The high p-value indicates that more than likely there is no relationship whatsoever between liability management and competitive losses.

8.5 Business Productivity Losses and Organizational Response Tactics

The fourth type of loss stemming from IT security breach events is business productivity losses. Business productivity losses are those losses pertaining to system downtime, loss of employee productivity and delays in business operations. Measuring the impact of organizational response tactics on business productivity is perhaps the most significant relationships examined in this study for frontline practitioners and managers. This set of relationships are necessary to examine because many times the performance of frontline practitioners and are not measured in financial terms but rather with other units of measurements such as time and other measures of quantity. Governance tactics (-0.29, p<0.10), are the only set of organizational response tactics which are associated with significant decreases to business productivity losses. Governance tactics are defined as organizational response actions pertaining to the creation or modification of formal and informal structures and mechanisms focused on accountability and response to an adverse event (Bundy et al. 2016; Bigley and Roberts 2001; Lindstrom et al. 2010). Relationship management (-0.174, p=0.27) and liability management tactics (-0.137, p=437) are associated with insignificant, decreases in business productivity losses. The findings for relationship management and liability management tactics indicates that the use of these organizational response tactics should be considered in the context of a full cost benefit analysis.

As with financial losses, reputational losses, and competitive losses; communication management (0.285, p<0.10) organizational response tactics are associated with significant and positive increases to business productivity losses. SME 1 notes that this is related merely to lack transparency and this phenomenon may only be seen in the dataset, i.e. it is possible that if the sample size were larger, the communication management organizational response tactics would not cause losses to business productivity. SME 1 states:

"If you go back and look at morale, again if you tell a story your ahead. It doesn't hurt business productivity because that communication is awareness. Just being on the same page. Sharing information between business units to ensure proper controls are in place."

SME 2 notes that the unexpected relationship between communication management response tactics and business productivity losses is due to bureaucracy.

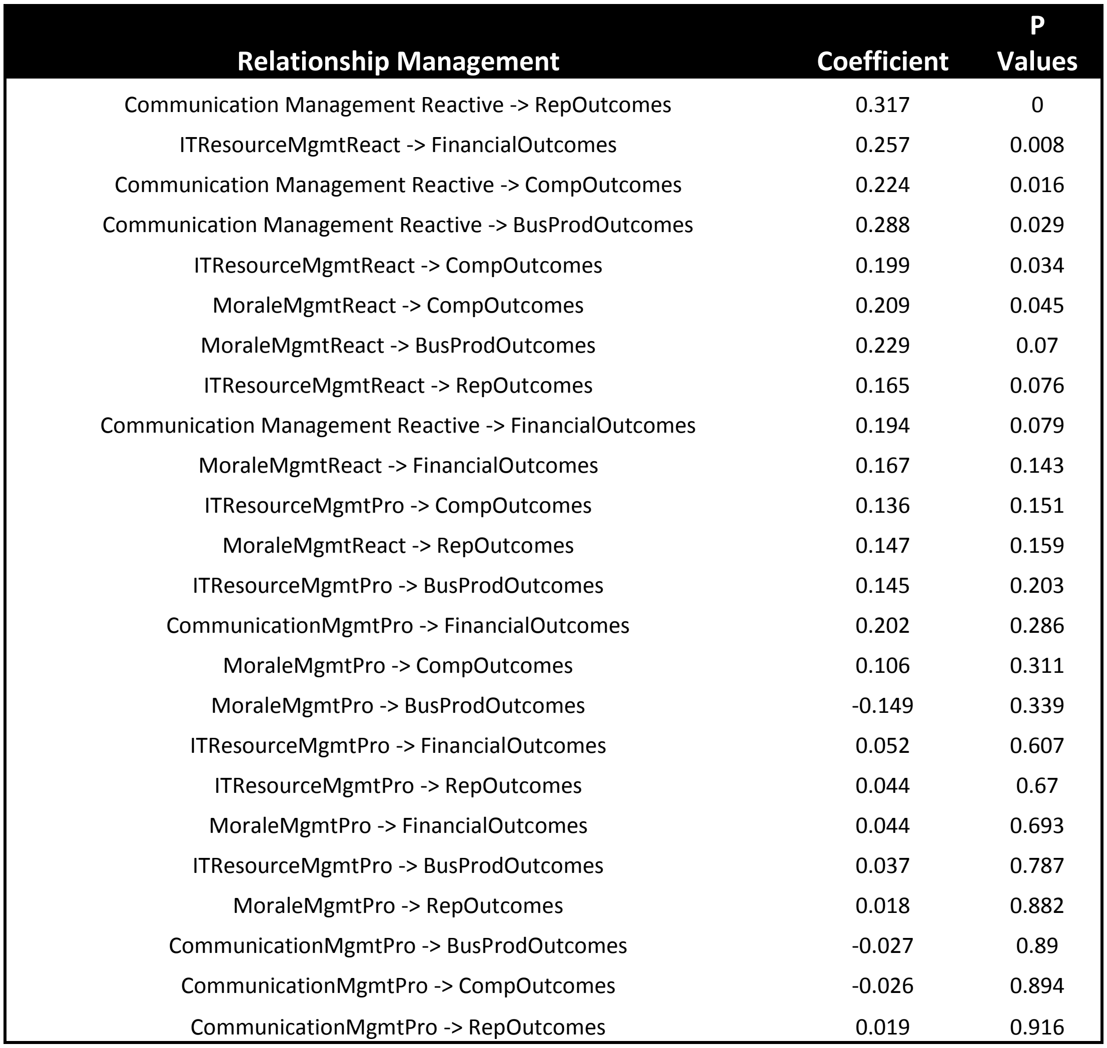
"Same deal of increase in overhead and bureaucracy which can impact business productivity."

An increase in the extent of IT resource management tactics (0.097, p=.475), morale management (0.078, p=0.567), and security strategic thinking (0.158, p=0.41) were found to be associated with increases in business productivity losses, however, the results were not significant and with p-values approaching or exceeding 50%, the likelihood of there being an association between these tactics and business productivity losses is no different than chance. Despite the insignificant relationships, the opinions of the two subject matter experts were obtained, and detailed quotes on why these relationships may be occurring are located in Appendix C.

8.6 Post-hoc Analysis

From the hypotheses testing conducted in Chapter 7, we know that results were either unexpected or expected. Unexpected results from the hypotheses testing are those relationships that showed a significant and positive association between one of the seven organizational response tactics. Unexpected results were noted for communication management, morale management, and IT resource management organizational response tactics. To better understand why there were unexpected results a series of analysis were conducted. First, the survey questions were examined to ensure that they were coded correctly, second the survey items comprising each of the constructs were evaluated for discrepancies or unusual patterns, third, alternative conceptualizations of the research model were constructed and analyzed and lastly, the organizational response tactics were deconstructed into “proactive responses” and “reactive responses” and the quantitative analysis was rerun. The quantitative analysis of the deconstructed survey constructs reveals that when the problematic organizational response tactics were broken into proactive and reactive responses, there is a noticeable trend of statistically significant p-values and relatively high coefficients for those organizational response tactics which are reactive in nature. Table 45 provides the comparison of the results for proactive versus reactive tactics. The table is organized in order of increasing p-values.

The results imply that reactive tactics related to communication management, morale management, and IT resource management may be hurtful and counterintuitive to reducing adverse outcomes from IT security breach events. However, PLS based structural equation modeling is the quantitative method utilized to test hypotheses in this study and is focused on testing associations and do not necessarily imply causality or directionality, per se. It should be noted that some response tactics are mandated by the government such as communication management tactics regarding timely notification and in many cases, the tactics are an inherent part of the post-breach response processes, for example some temporary reallocation of IT resources may be necessary to mitigate an IT security breach event.



Relationship Management	Coefficient	P Values
Communication Management Reactive -> RepOutcomes	0.317	0
ITResourceMgmtReact -> FinancialOutcomes	0.257	0.008
Communication Management Reactive -> CompOutcomes	0.224	0.016
Communication Management Reactive -> BusProdOutcomes	0.288	0.029
ITResourceMgmtReact -> CompOutcomes	0.199	0.034
MoraleMgmtReact -> CompOutcomes	0.209	0.045
MoraleMgmtReact -> BusProdOutcomes	0.229	0.07
ITResourceMgmtReact -> RepOutcomes	0.165	0.076
Communication Management Reactive -> FinancialOutcomes	0.194	0.079
MoraleMgmtReact -> FinancialOutcomes	0.167	0.143
ITResourceMgmtPro -> CompOutcomes	0.136	0.151
MoraleMgmtReact -> RepOutcomes	0.147	0.159
ITResourceMgmtPro -> BusProdOutcomes	0.145	0.203
CommunicationMgmtPro -> FinancialOutcomes	0.202	0.286
MoraleMgmtPro -> CompOutcomes	0.106	0.311
MoraleMgmtPro -> BusProdOutcomes	-0.149	0.339
ITResourceMgmtPro -> FinancialOutcomes	0.052	0.607
ITResourceMgmtPro -> RepOutcomes	0.044	0.67
MoraleMgmtPro -> FinancialOutcomes	0.044	0.693
ITResourceMgmtPro -> BusProdOutcomes	0.037	0.787
MoraleMgmtPro -> RepOutcomes	0.018	0.882
CommunicationMgmtPro -> BusProdOutcomes	-0.027	0.89
CommunicationMgmtPro -> CompOutcomes	-0.026	0.894
CommunicationMgmtPro -> RepOutcomes	0.019	0.916

Table 45: Results of Proactive vs. Reactive Construct Testing for Unexpected Relationships

8.7 Summary

This chapter discussed the results from the hypotheses testing supplemented with interviews from two subject matter experts to understand the unexpected results better. Interviews from subject matter experts were necessary because the extant literature may not provide detailed insights into some of the unexpected relationships in this study. This chapter draws conclusions regarding the relationships of organizational responses to organizational losses in the context of IT security breach events. It was found that financial losses from IT security breach events can be reduced by relationship management organizational response tactics. There is some evidence that reputational losses from IT security breach events may be reduced by relationship management, security strategic thinking, and governance organizational response tactics but the reduction may not be significant or impactful, and a cost-benefit analysis needs to be conducted prior to the use of these tactics within an organization. It is clear however that the reputations of organizations may suffer regardless of what the organization does to reduce such losses. Like financial losses, competitive losses from IT security breach events can be reduced by relationship management organizational response tactics. Lastly, business productivity losses from IT security breach events can be reduced by the implementation of governance organizational response tactics.

CHAPTER 9: CONTRIBUTIONS, LIMITATIONS, AND FUTURE WORK

9.1 Prologue

This chapter discusses the contributions of this research study to the extant academic research and practice literature. In addition, the limitations of the study and potential research extensions of this work are explored.

9.2 Contribution to Research

Over the last thirteen years, the number of IT security breaches in the United States has more than doubled from one IT security breach every two days to almost two IT security breaches a day (Identity Theft Resource Center, 2018). The rapid digitization of organizational infrastructures and business transactions has arguably led to this increase due to the growth in the "surface areas" for breaches. There are many types of IT security breach events which can range from data breaches, to hacks, to denial of service attacks (Rouse, 2016; Ettredge & Richardson, 2003; Straub, 1990). The study of IT security breach events has been difficult for academic researchers due to the stigma and the liability concerns for organizations surrounding these events thus hindering their participation in academic research studies. The most frequent form of research in the management information systems domain in the context of IT security breach events has been the study of breaches and their impacts on the market value of organizations (for examples see Chen, Li, Yen, & Bata, 2012; Garg, Curtis, & & Halper, 2003) as market value data is publicly available for firms. There is minimal understanding in the management information systems research domain and the broader cybersecurity literature on the effectiveness of incident response processes, IT security breach prevention measures, risk management tactics, and to some extent nonfinancial organizational losses. The losses to organizations from IT security breaches have not been equal, some organizations have experienced losses which threatened the viability of their organizations while other organizations seemingly did not experience losses at all, and still others seemed to experience some measure of organizational gains after an IT security breach event (for examples see Safdar & Beilfuss, 2016; Davis, 2015, Armerding, 2016, Kvochko & Pant, 2015). The outstanding research gaps in the extant literature were articulated in this research study as follows:

1. Outside of short-term changes to firm market value, there is a lack of research on the long-term and short-term organizational consequences of IT security breaches.
2. Lack of research regarding organizational responses within organizations when IT security breaches do occur.

This study utilizes a series of empirical research methodologies in a mixed methods approach to shed light on the aforementioned outstanding research gaps. There are four significant research contributions from this study. First, the study finds that in addition to financial losses from IT security breach events there are three other types of losses that organizations can experience as a result of these events. These losses are 1) reputational losses, 2) competitive losses, and 3) business productivity losses. This study clearly articulated descriptions for each of the four types of losses and through the quantitative analysis technique of structural equation modeling, construct reliability and validated were confirmed for each of the four types of losses. The second contribution this study makes to academic research is the discovery that there are seven broad types of organizational response tactics to IT security breach events. These organizational response tactics can further be delineated by their temporal approach which can be proactive responses or reactive responses. The seven organizational response tactics for IT security breaches are 1) liability management, 2) governance, 3) communication management, 4) IT resource management, 5) security strategic thinking, 6) morale management, and 7) relationship management. Structural equation modeling was also utilized to quantitatively verify the reliability and validity of the seven organizational response tactic constructs. The third contribution of this study is the articulation and definition of "Information Technology Security Breach" and the derivation of the four features which define an IT security breach event. These four features include 1) extent of the breach, 2) breach intentionality, 3) breach source, and 4) breach sensitivity. The fourth contribution of this study is the integration of organizational response tactic constructs, organizational outcome constructs, and IT security breach characteristics constructs into both a conceptual model and research model. The testing of the research model and the associated hypotheses allows us to test the relationships and associations among the varying constructs utilizing real-world data from IT security managers. The results from the hypotheses testing regarding optimal and less optimal response tactics will be insightful for future research.

9.3 Contribution to Practice

Research on IT security breach events is arguably more unique than other types of academic research topics due to the intense interest of industry practitioners in facilitating and advancing their own research interests. Research from practice takes the form of government white papers (for examples see Department of Homeland Security, 2016, National Institute of Standards and Technology, 2012; CERT, 2017) and can also take the form of corporate and professional association white papers (for examples see IT Governance Institute, 2006; Zacks Equity Research 2017; Rogers & Traurig, 2016) and this research has saturated the IT security field. Despite the proliferation of practice-oriented research and white papers, there are concerns when organizations utilize these types of research for decision-making purposes. Many industry research papers are sponsored by vendors or consulting practices selling a product or service, and therefore the findings have the potential to be biased and inaccurate or even worse potentially nefarious. One example of the risks of utilizing industry research papers can be illustrated by the recent saga with the well-known IT security consulting firm Kaspersky Labs. In addition to consulting services, Kaspersky Labs produces antivirus software, and it has been alleged that this software has been a potential conduit to spy on the U.S. government (Perlroth, 2018). This saga is fascinating to note as Kaspersky Labs in recent years has been considered a knowledge broker and has produced many research papers on a wide array of IT security topics (see Kaspersky Labs, 2018 url https://usa.kaspersky.com/enterprise-security/resources/white-papers).

Another source of industry research not mentioned above are government white papers. Government white papers are an objective source of information for those who practice IT security within organizations. Government white papers provide detailed information such as recommendations on proactive and reactive responses and best practices so that organizations can better position themselves in the context of IT security breach events. We know from government white papers best practices around the management of IT resources, compliance, and even IT security awareness education. However, one downside of many government whitepapers is there is no quantitative assessment for whether a specific organizational response tactic is actually helpful or hurtful to an organization. The assumption is that all organizational responses prior to and after an IT security breach event is helpful to the focal organization. A major contribution of this study for practitioners' sheds light on the aforementioned mystery. The study finds that not all organizational response tactics are helpful to an organization and that hurtful organizational response tactics may be more prevalent than previously thought.

It is crucial that academic research address practitioners need for clear, concise, and actionable recommendations pertaining to research studies. This study advances that notion by testing twenty-eight hypotheses where the hypothesized relationships were between the seven organizational responses to IT security breach events and the four types of organizational losses from IT security breach events. The findings from the hypothesized relationships immediately contribute to the practice of managing IT security breach events within organizations and enable frontline practitioners and decision makers to utilize the findings in their roles. This study finds that both proactive and reactive relationship management tactics are helpful in reducing financial losses, reputational losses, and competitive losses. Specific relationship management tactics that frontline practitioners and decision makers can implement within their organizations include 1) reviewing the information security and privacy policies, practices and procedures of external parties who collect, store, use or access the data 2) reviewing agreements and work arrangements with contracted IT security vendors and 3) engaging external business partners in reviewing IT security arrangements. Business productivity losses from IT security breach events can be mitigated by utilizing governance organizational response tactics. Specific governance tactics that will be helpful to practitioners include 1) adopting and implementing one or more international standards for handling IT security breaches 2) developing formal procedures and rules for managing any IT security breaches and 3) ensuring that IT security is the responsibility of both IT and other functional managers.

In addition, this study finds that financial losses from IT security breach events can be reduced by relationship management organizational response tactics. There is some evidence that reputational losses from IT security breach events may be reduced by relationship management, security strategic thinking, and governance organizational response tactics but the reduction may not be significant or impactful, and a cost-benefit analysis needs to be conducted before the use of these tactics within an organization. Also, it is possible that no organizational response tactic can reduce reputational losses. Like financial losses, competitive losses from IT security breach events can be reduced by relationship management organizational response tactics. Lastly, business productivity losses from IT security breach events can be reduced by the implementation of governance organizational response tactics.

A major contribution of this study is the finding that IT resource management, morale management, and communication management response tactics may be harmful to organizations such that they may potentially increase losses related to IT security breach events. An analysis of the consultation with two subject matter experts with over 60 years combined IT security experience, indicated that a potential culprit for the unexpected results was issued during implementation and poor pre-planning when the aforementioned organizational response tactics were used by the organizations in this study.

9.4 Limitations and Future Work

This study has five significant limitations, which presents opportunities for future research studies and which places constraints on the interpretations of the findings. First, the data used in the quantitative portion of this study is survey data. Survey data presents many advantages in this study including the ability to conduct an in-depth study on a sensitive topic i.e.IT security breach events. Survey data also allows us to test a custom, theoretically derived model and furthermore survey data allows us to easily measure latent constructs for which observational data may not be readily available or difficult to obtain. Second, this study may suffer from non-response bias. The non-response bias is caused by the sample population potentially being bound to non-disclosure agreements as well as fear that their confidentiality may be compromised. The third limitation of this study is sample selection bias which can be mitigated in the future by increased funding and resources to assist with increasing the sample size in order to derive a random and representative sample of this unique population (IT security managers who have experienced recent IT security breach events). The fourth limitation is that the study suffers from a single respondent bias where a single respondent represents an organization. Future studies would benefit from having two or more respondents within each organization participate in the study. The fifth limitation is that the study has a small sample size. Additional studies should be conducted with a larger sample size, so findings are more generalizable. The findings from this study should be interpreted within the context of the five aforementioned research limitations.

CHAPTER 10: REFERENCES

Zacks Equity Research. (2017). 3 Hot Cybersecurity Stocks in Focus Post Equifax Inc. (EFX) Data Breach. *InvestorPlace*.

(ISC)^2. (2017, June 01). *CISSP- Certified Information Systems Security Professional*. Retrieved from https://www.isc2.org/cissp/default.aspx

Acquisti, A., Friedman, A., & Telang, R. (2006). Is there a cost to privacy breaches? An event study. *ICIS 2006 Proceedings*, 94.

Alexander, D. (2013). Resilience and disaster risk reduction: An etymological journey. *Natural Hazards and Earth System Sciences*, 2707-2716.

Alpaslan, C., Green, S., & Mitroff, I. (2009). Corporate governance in the context of crises: Stakeholder theory of crises management. *Journal of Contingencies and Crises Management*, 38-49.

American Association of Advertising Agencies. (2016). *4A's-MSA Guidance Data SecurityThe Rules of the Road.*

Angst, C. M., Block, E. S., D'Arcy, J., & Kelley, K. (2017). When Do IT Security Investments Matter? Accounting for the Influence of Institutional Factors in the Context of Healthcare Data Breaches. *MISQ*, 893-916.

Aragon-Correa, J. A., & Sharma, S. (2003). A contingent resource-based view of proactive corporate environmental strategy. *Academy of management review*, 71-88.

Ashenmacher, G. (2016). Indignity: Redefining the Harm Caused by Data Breaches. *Wake Forest L. Rev, 51*(1).

Associated Press. (2014, November 18). Home Depot profit rises despite data breach. *Los Angeles Times*.

August, T., & Niculescu, M. F. (2013). The influence of software process maturity and customer error reporting on software release and pricing. *Management Science, 59*(12), 2702-2726.

Avey, J., Luthans, F., & Jensen, S. (2009). Psychological capital: A positive resource for combating employee stress and turnover. *Human Resource Management, 48*(5), 677-693.

Backhouse, J., Hsu, C., & Silva, L. (2006). Circuits of Power in Creating de jure Standards: Shaping an International Information Systems Security Standard. *MISQ*(SI), 413-438.

Bagozzi, R., & Yiu, Y. (1988). On the Evaluation of Structural Equation Models. *Journal of the Academy of Marketing Science, 16*(1), 74-94.

Bagozzi, R., Yi, Y., & Phillips, L. (1991). Assessing construct validity in organizational research. *Administrative Science Quarterly, 36*(3), 421-458.

Balanced Scorecard Institute. (2017, June 1). *Strategy Planning Basics*. Retrieved from BalancedScorecard.org: http://www.balancedscorecard.org/BSC-Basics/Strategic-Planning-Basics

Barclay, D., Higgins, C., & Thompson, R. (1995). The Partial Least Squares (PLS) Approach to Causal Modeling; Personal Computer Adoption and Use an Illustration. *Technology Studies, 2*(2), 285-309.

Barnett, C., & Pratt, M. (2000). From threat-rigidity to flexibility - Toward a learning model of autogenic crisis in organizations. *Journal of Organizational Change Management, 13*(1), 74-88.

Barney, J. (1991). Firm resources and sustained competitive advantage. *Journal of Management, 17*(1), 99-120.

Baron, R., Franklin, R., & Hmieleski, K. (2016). Why entrepreneurs often experience low, not high levels of stres: The joint effects of selection and psychological capital. *Journal of Management, 42*(3), 742-768.

Barron, R., & Kenny, D. (1986). The moderator-mediator variable distinction in social psychological research: Conceptual, strategic, and statistical considerations. *Journal of Personality and Social Psychology, 51*(6), 1173-1182.

Baskerville, R., Spagnoletti, P., & Kim, J. (2014). Incident-centered information security: Managing a strategic balance between prevention and response. *Information & Management, 51*(2), 138-151.

Basu, E. (2013, October 13th). What Is A Penetration Test And Why Would I Need One For My Company? *Forbes*.

Basu, S. (1997). Investment performance of common stocks in relation to their price-earnings ratios: A test of the efficient market hypothesis. . *The journal of finance*, 663-682.

Berghmans, P., & Van Roy, K. (2011). Information security risks in enabling e-Government: The Impact of IT vendors. *Information Systems Management, 28*, 284-293.

Bernard, T., & Cowley, S. (2017, October 3). Equifax breach caused by lone employee's error, former C.E.O says. *The New York Times*.

Bigley, G., & Roberts, K. (2001). The incident commmand system: High reliability organizing for complex and volatile task environments. *Academy of Management Journal*, 1281-1299.

Blatnik, J. (2017, May). The Impact of WannaCry on the Ransomware Conversation. *Security Week*.

Bollen, K. (1989). *Structural equations with latent variables.* Wiley & Sons.

Bollen, K. A. (2013). Eight myths about causality and structural equation models. In *Handbook of causal analysis for social research* (pp. 301-328).

Bonanno, G., Brewin, C., Kaniasty, K., & La Greca, A. (2010). Weighing the costs of disaster consequences, risks, and resilience in individuals, families, and communities. *Psychological Science in the Public Interest*, 1-49.

Bontis, N. &.-E. (2002). InIntellectual capital ROI: a causal map of human capital antecedents and consequents. . *Journal of Intellectual capital*, 223-247.

Bose, I., & Leung, A. C. (2014). Do phishing alerts impact global corporations? A firm value analysis. *Decision Support Systems*, 67-78.

Bossong, R., & Wagner, B. (2017). A typology of cybersecurity and public-private partnerships in the context of the EU. *Crime, Law and Social Change, 67*(3), 265-288.

Bradburn, N., Sudman, S., & Wansink, B. (2004). *Questions-The Definitive Guide to Questionnaire Design-For Market Research, Political Polls, and Social and Health Questionnaires.* San Francisco: Jossey-Bass.

Bradley, S., Shepherd, D., & Wiklund, J. (2011). The importance of slack for new organizations facing "tough" environments. *Journal of Management Studies*, 1071-1097.

Bunderson, J. S., & Sutcliffe, K. M. (2002). Comparing alternative conceptualizations of functional diversity in management teams: Process and performance effects. *Academy of Management Journal, 45*(5), 875-893.

Bundy, J., Pfarrer, M., Short, C., & Coombs, T. (2016). Crises and Crises Management: Integration, Interpretation, and Research Development. *Journal of Management*, 1-32.

Cardenas, J., Coronado, A., Donald, A., & Parra, F. (2012). The Economic Impact of Security Breaches on Publicly Traded Corporations: An Empirical Investigation. *AMCIS 2012 Proceedings 7*, (pp. 1-9). Seattle Washington.

Carmeli, A., & Markman, G. (2011). Capture, governance, and resilience: Strategy implication from the history of Rome. *Strategic Management Journal*, 322-341.

Carpenter, S., Walker, B., Anderies, J. M., & & Abel, N. (2001). From metaphor to measurement: resilience of what to what? *Ecosystems*, 765-781.

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

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers. *International Journal of Electronic Commerce, 9*(1), 70-104.

Cavusoglu, H., Raghunathan, S., & Cavusoglu, H. (2009). Configuration of and Interaction Between Information Security Technologies: The Case of Firewalls and Intrusion Detection Systems. *Information Systems Research, 20*(2), 198-217.

CERT. (2017). *Security Engineering Risk Analysis (SERA.* CERT.

Cezar, A., Cavusoglu, H., & Raghunathan, S. (2013). Outsourcing information security: Contracting issues and security implications. *Management Science, 60*(3), 638-657.

Chakravarthy, B. S. (1982). Adaptation: A promising metaphor for strategic management. *Academy of Management Review,*, 35-44.

Chen, J. V., Li, H. C., Yen, D. C., & & Bata, K. V. (2012). Did IT consulting firms gain when their clients were breached? *Computers in Human Behavior, 28*(2), 456-464.

Chen, X. B. (2011). Assessing the severity of phishing attacks: A hybrid data mining approach. *Decision Support Systems, 50*(4), 662-672.

Chen, Y., Ramamurthy, K., & & Wen, K. W. (2012). Organizations' information security policy compliance: Stick or carrot approach?. *Journal of Management Information Systems*, 157-188.

Chin, W. (1998). The partial least squares approach to structural equation modeling. *Modern Methods for Business Research*, 295-336.

Churchill, G. (1979). A paradigm for developing better measures of marketing constructs. *Journal of Marketing Research, 16*(1), 64-73.

CISCO. (2017). CISCO 2017 Annual Cybersecurity Report.

Clark, G. (2014). *CompTIA Security+ Certification Study Guide.* McGraw-Hill Education.

Clarke, G. (2013). *CompTia Security+ Second Edition.*

Clarkson, M. (1985). A stakeholder framework for analyzing and evaluating corporate social performance. *Academy of Management Review*, 92-117.

Comfort, L., Boin, A., & Demchak, C. (2010). *Designing Resilience.* Pittsburgh, PA: University of Pittsburgh Press.

Comrey, A. (1978). Common methodological problems in factor analytic studies. *Journal of Consulting and Clinical Psychology, 46*(4), 648.

Coombs, W. (1995). Choosing the right words: The development of guidelines for the selection of the "appropriate" crises response strategies. *Management Communication Quarterly*, 447-476.

Coombs, W. (2007). Protecting organization reputations during a crises: The development and application of situational crises communication theory. *Corporate Reputation Review*, 163-176.

Coutu, D. L. (2002). How resilience works. *Harvard business review*, 46-56.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. *Information Systems Research, 20*(1), 79-98.

D'Aubeterre, F., Singh, R., & Iyer, L. (2008). Secure activity resource coordination: empirical evidence of enhanced security awareness in designing secure business processes. *European Journal of Information Systems, 17*(5), 528-542.

Dean, B. (2015, March 05). Sorry consumers, companies have little incentive to invest in better cybersecurity. *Quartz*.

Debreceny, R., & Gray, G. (2009). IT Governance and Process Maturity: A Field Study. *Proceedings of the 42nd Hawaii International Conference on System Sciences* , (pp. 1-10).

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

Deloitte Canada. (2017). *Cybersecurity: Everybody's imperative.*

Dempsey, T. (2015). *Navigating the Digital Age: The Definitive Cybersecurity Guide for Directors and Officers.* Chicago, IL: Caxton Business & Legal, Inc.

Department of Homeland Security. (2014). *US-CERT Federal Incident Notification Guidelines.*

Department of Homeland Security. (2016). *Cybersecurity Insurance.* Department of Homeland Security.

Devaraj, S., & Kohli, R. (2003). Performance Impacts of Information Technology: Is Actual Usage the Missing Link. *Management Science, 49*(3), 273-289.

Dijkstra, T., & Henseler, J. (2015). Consistent partial least squares path modeling. *MISQ*, 297-316.

Donaldson, T., & Preston, L. E. (1995). The stakeholder theory of the corporation: Concepts, evidence, and implications. *Academy of management Review*, 65-91.

Dowell, W., Shackell, B., & Stuart, V. (2011). Boards, CEO's and surviving a financial crises: Evidence from the internet shakeout. *Strategic Management Journal*, 1025-1045.

Duncan, R. B. (1972). Characteristics of organizational environments and perceived environmental uncertainty. . *Administrative science quarterly*, 313-327.

Egan, G. (2015). *Want to Spend Less and Reduce Risk? Train Your Employees.* SecureWorld.

Eisenhardt, K., & Tabrizi, B. (1995). Accelerating adaptive processes: Product innovation in the global computer industry. *Administrative Science Quarterly, 40*(1), 84-110.

Elky, S. (2007). *An introduction to information system risk management.* SANS Institute.

Epstein, R. (1973). *A Theory of Strict Liability.* University of Chicago Law School.

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

Evans, S., Heinbuch, D., Kyle, E., Piorkowski, J., & & Wallner, J. (2004). Risk-based systems security engineering: stopping attacks with intention. *IEEE Security & Privacy*, 59-62.

Farrell, P. (2017, July 7th). Data breaches undermine trust in government's ability to protect our information. *The Guardian*.

Fernandez-Medina, E., Trujillo, J., & Piattini, M. (2007). Model-driven multidimensional modeling of secure data warehouses. *European Journal of Information Systems, 16*(4), 374-389.

Filkins, B., & Fogarty, K. (2015). *Cleaning Up After a Breach Post-Breach Impact: A Cost Compendium.* SANS Institute.

Fornell, C., & Larcker, D. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, 39-50.

Frandsen, F., & Johansen, W. (2011). The study of internal crises communication:Towards an integrative framework. *Corporate Communications: An International Journal*, 347-361.

Galbraith, J. (1973). *Designing complex organizations.* Boston, MA: Addison-Wesley.

Gandel, S. (2015, January 23). Lloyd's CEO: Cyber attacks cost companies $400 billion every year. *Fortune*.

Garg, A., Curtis, J., & & Halper, H. (2003). Quantifying the financial impact of IT security breaches. *Information Management & Computer Security,, 11*(2), 74-83.

Garson, G. (2016). *Partial Least Squares: Regression and Structural Equation Models.* Asheboro, North Carolina: Statistical Associates Publishers.

Gelbstein, E. (2015). Return on Security Investment- 15 Things to Consider. (1).

Gelsomini, J. J. (2015). Anthem's data breach impacts many anthem and non-anthem plans: Necessary employer actions now. *Employee Benefit Plan Review*, 5-7.

George, G. (2005). Slack resources and the performance of privately held firms. *Academy of Management Journal, 36*(6), 661-676.

Ghemawat, P., & Del Sol, P. (1998). Commitment versus flexibility? *California Management Review, 40*(4), 26-42.

Ghosh, P. (2014). N.Y. Regulator Calls for Tougher Cybersecurity Protocols for FIs. *Credit Union Journal, 18*(44).

GIAC.Org. (2017, June 1st). *GIAC Security Expert (GSE) Certification*. Retrieved from https://www.giac.org/certification/security-expert-gse

Gibson, C. (2007). *Financial reporting and analysis 10th Edition.* Mason, OH: Thompson Higher Education.

Gibson, D. (2014). *CompTIA Security+: Get Certified Get Ahead: SY0-401 Study Guide.* CompTia.

Gideon, L. (2012). *Handbook of Survey Methodology for the Social Sciences.* New York, New York: Springer.

Gittell, J. H., Cameron, K., Lim, S., & & Rivas, V. (2006). Relationships, layoffs, and organizational resilience airline industry responses to September 11. *The Journal of Applied Behavioral Science*, 300-329.

Goel, S., & Shawky, H. A. (2014). The impact of federal and state notification laws on security breach announcements. *Communications of the Association for Information Systems,, 34*(1), 37-50.

Gordon, L., Loeb, M. P., & Zhou, L. (2011). The impact of information security breaches: Has there been a downward shift in costs? *Journal of Computer Security, 19*(1), 33-56.

Gordon, L., Loeb, M., & Sohail, T. (2010). Market Value of Voluntary Disclosures Concerning Information Security. *MISQ*, 567-594.

Gordon, P. (2006). *Responding to Security Breaches Under Ohio's and Pennsylvania's New Notice-of-Security-Breach Statutes and Other States' Notice Laws.* Littler.com.

Greitzer, Moore, Cappelli, Andrews, Carroll, & Hull. (2008). Combating the insider cyber threat. *IEEE Security and Privacy*, 61-64.

Haber, M. (2013). *Session Monitoring Provides Context Aware Security for Windows.* BeyondTrust.com.

HackerOne. (2018, May 15th). *About HackerOne*. Retrieved May 15th, 2018, from HackerOne: https://www.hackerone.com/about

Hackett, R. (2015, March 27th). How much do data breaches cost big companies? Shockingly little. *Fortune*.

Hair, J., Hult, T., Ringle, C. M., & Sarstedt, M. (2017). *A primer on partial least squares structural equation modeling.* Thousand Oaks, California: Sage.

Harris, K. (2016). *Data Breach Report California Department of Justice.* Attorney General State of California.

Heckman, J. (1979). Sample Selection Bias as a Specification Error. *Econometrica, 47*(1), 153-161.

Heiser, J. (2008, November). Drop in staff morale increases security threat. *ComputerWeekly.com*.

Henseler, J., Dijkstra, T., Sarstedt, M., Ringle, C., Diamantopoulous, A., Straub, D., et al. (2014). Common Beliefs and Reality About PLS. *Organizational Research Methods*, 182-209.

Henseler, J., Hubona, G., & Ray, P. (2016). Using PLS path modeling in new technology research: updated guidelines. *Industrial management and data systems, 116*(1), 2-20.

Henseler, J., Ringle, C., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance- based structural equation modeling. *Journal of the Academy of Marketing Science, 43*(1), 115-135.

Henson, R., & Robert, J. (2006). Uses of exploratory factor analysis in published research: Common errors and some comment on improved practices. *Educational and Psychological Measurement, 66*(3), 393-416.

Henson, R., & Roberts, J. (2006). Use of Exploratory Factor Analysis in Published Research Common Errors and Some Comment on Improved Practice. *Educational and Psychological Measurement, 66*(3), 393-416.

Herman, B. (2016, March 30th). Details of Anthem's massive cyberattack remain in the dark a year later. *ModernHealthcare.com*.

Hess, A. (2015, November 22). Inside the Sony Hack. *Slate*.

Hinz, O., Nofer, M., Schiereck, D., & Trillig, J. (2015). The influence of data theft on the share prices and systematic risk of consumer electronics companies. *Information & Management, 52*(3), 337-347.

HIPAA Journal. (2016). *IU HEALTH ARNETT SECURITY BREACH IMPACTS 29K PATIENTS.* HIPAA Journal.

Hobfoll, S. (1989). Conservation of resources. *American Psychologist*, 513-524.

Horowitz, J., & Weiner-Bronner, D. (2017, September). Equifax's chief information officer and chief security officer are out. *CNN*.

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

Hovav, A., Andoh-Baidoo, F., & Dhillion, G. (2007). Classification of security breaches and their impact on the market value of firms. *Annual Security Conference*, (pp. 1-11). Las Vegas, NV.

Hsu, C. W. (2009). Frame misalignment: interpreting the implementation of information systems security certification in an organization. *European Journal of Information Systems, 18*(2), 140-150.

Hsu, C., Backhouse, J., & Silva, L. (2014). Institutionalizing operational risk management: an empirical study. *Journal of Information Technology, 29*(1), 59-72.

Hu, Q., Dinev, T., Hart, P., & & Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences*, 615-660.

Hu, Q., Hart, P., & Cooke, D. (2007). The role of external and internal influences on information systems security – a neo-institutional perspective. *The Journal of Strategic Information Systems, 16*(2), 153-172.

Hui, K. L., Hui, W., & Yue, W. T. (2012). Information security outsourcing with system interdependency and mandatory security requirement. *Journal of Management Information Systems, 29*(3), 117-156.

IBM. (2015). *Ponemon Institute’s 2015 Global Cost of Data Breach Study Reveals Average Cost of Data Breach Reaches Record Levels.* Traverse City, MI: IBM.

Identity Theft Resource Center. (2015). *Data Breaches.* Identity Theft Resource Center.

InfoSec Institute. (2017). *Security Operations Center.*

International Organization for Standardization. (2013). *ISO/IEC 27014:2013 Information technology — Security techniques — Governance of information security.* ISO.

Iqbal, S., Kiah, M. L., Dhaghighi, B., Hussain, M., Khan, S., Khan, M. K., et al. (2016). On cloud security attacks: A taxonomy and intrusion detection and prevention as a service. *Journal of Network and Computer Applications, 74*, 98-120.

Isaac, M., Benner, K., & Frenkel, K. (2017, November 21). Uber Hid 2016 Breach, Paying Hackers to Delete Stolen Data. *The New York Times*.

ISACA. (2017, June 1st). *Certified Information Systems Auditor(CISA)*. Retrieved from http://www.isaca.org/Certification/CISA-Certified-Information-Systems-Auditor/Pages/default.aspx

ISACA. (2017). *What is COBIT 5.* ISACA.

IT Governance Institute. (2006). *Information Security Governance: Guidance for Information Security Managers.* ISACA.

IT Governance Institute. (2007). *Control Objectives for Information and Related Technologies (CobiT) 4.1.*

Jackson, S., & Dutton, J. (1988). Discerning threats and opportunities. *Administrative Science Quarterly, 33*(3), 370-387.

Jaeger, J. (2015, February 2nd). JP Morgan Breach Leads to Multi-State Probe. *Compliance Week*.

Jamieson, R., & Low, G. (1990). Local rea network operations: a security, control, and audit perspective. *Journal of Information Technology, 1990*(5), 63-72.

Jaworski, B., & Macinnis, D. (1989). Marketing jobs and management controls: Toward a framework. *Journal of Marketing Research, 26*(4), 406-419.

Jin, Y., Pang, A., & Cameron, G. (2012). Towards a publics-driven, emotion based conceptualization in crises communication: Unearthing dominant emotions in multi-staged testing of the integrated crises mapping. *Journal of Public Relations Research*, 266-298.

Johansen, W., Aggerholm, K., & Frandsen, K. (2012). Entering new territory: A study of internal crises management and crises communication in organizations. *Public Relations Review*, 270-279.

Johnson, D., Mckechnie, J. K., Tishuk, B., & Flournoy, A. (2016). *Cyberinsurance Buying Guide.* American Bankers Association.

Kanatov, M., Atymtayeva, L., & Yagaliyeva, B. (2014). Expert systems for information security management and audit. Implementation phase issues. . *Soft Computing and Intelligent Systems (SCIS), 2014 Joint 7th International Conference on and Advanced Intelligent Systems (ISIS), 15th International Symposium*, 896-900.

Kaspersky Lab. (2015). *Damage Control: The Cost of Security Breaches IT Security Risks Special Report Series.* Kaspersky Lab.

Kassner, M. (2015, April 9th). Data breaches may cost less than the security to prevent them. *TechRepublic*.

Kenny, D. (2015). *Measuring Model Fit.* Davidakenny.net.

Khansa, L., Cook, D., & Bruyaka, O. (2012). Impact of HIPAA Provisions on the Stock Market Value of Healthcare Instituitions, and Information Security, and Other Information Technology Firms. *Computers & Security*, 750-770.

Kim, D., Yim, M.-S., Sugumaran, V., & Rao, R. (2015). Web assurance seal services, trust and consumers' concerns: an investigation of e-commerce transaction intentions across two nations. *European Journal of Information Systems, 25*(2), 252-273.

Ko, M. O.-B., M., K., & Dorantes, C. (2009). Investigating the impact of publicly announced information security breaches on three performance indicators of the breached firms. *Information Resources Management Journal, 22*, #2.

Ko, M., & Dorantes, C. (2006). The impact of information security breaches on financial performance of the breached firms: an empirical investigation. *Journal of Information Technology Management, 17*(2), 13-22.

Kock, N., & Lynn, G. (2015). Lateral collinearity and misleading results in variance based SEM: An illustration and recommendations. *Journal of the Association for Information Systems, 13*(7), 546-580.

Kornhauser, L., & Revesz, R. (1994). *Multidefendent settlements under joint and several liability: The problem of insolvency.* The Journal of Legal Studies.

Kumar, N., Stern, L. W., & Anderson, J. C. (1993). Conducting interorganizational research using key informants. *Academy of Management Journal, 36*(6), 1633-1651.

Kwon, J., & Johnson, M. E. (2014). Proactive Versus Reactive Security Investments in the Healthcare Sector. *MISQ, 38*(2).

Lannin, K. (2016). *Fired employees sue state for 1 million after alleged hack.* GoldenGateXpress.org.

Lapowsky, I. (2017, June 20th). WHAT SHOULD (AND SHOULDN'T) WORRY YOU IN THAT VOTER DATA BREACH. *Wired*.

Lee, C., Geng, X., & Raghunathan. (2012). Contracting Information Security in the Presence of Double Moral Hazard. *Information Systems Research, 24*(2), 295-311.

Legere,John. (2015). *T-Mobile CEO on Experian's Data Breach.* T-Mobile.

Lengnick-Hall, C., Beck, T., & Lengnick-Hall, M. (2011). Developing a capacity for organizational resilience through strategic human resource management. *Human Resource Management Review, 21*(3), 243-255.

Leonard, B. (2015). *Regaining employees' trust after a data breach.*

Li, T., & Calantone, J. (1998). The impact of market knowledge competence on New Product Advantage: Conceptualization and Empirical Examination. *Journal of Marketing, 62*(4), 13-29.

Liginlal, D., Sim, I., & Khansa, L. (2009). How significant is human error as a cause of privacy breaches? An empirical study and a framework for error management. *computers & security*, 215-228.

Lindstrom, J., Samuelsson, S., & Hagerfors, A. (2010). Business continuity planning methodology. *Disaster Prevention and Management: An International Journal, 19*(2), 243-255.

Loch, K. D. (1992). Threats to information systems: today's reality, yesterday's understanding. *MIS Quarterly*, 173-186.

Lord, N. (2017). *Cryptography in the Cloud: Securing Cloud Data with Encryption.* Digital Guardian.

Luthans, F., Avolio, B., Walumbwa, F., & Li, W. (2005). The psychological capital of Chinese workers: Exploring the relationships with performance. *Management and Organization Review, 1*(2), 249-271.

Mackenzie, S., & Podsakoff, P. (2012). Common Method Bias in Marketing: Causes, Mechanisms, and Procedural Remedies. *Journal of Retailing, 88*(4), 542-555.

Macri, G. (2016, November 25). Consumers Are Losing Trust in Hacked Companies. *Inside Sources*.

Majchrzak, A., Jarvenpaa, S., & Hollingshead, B. (2007). Coordinating expertise among emergent groups responding to disasters. *Organization Science*, 147-161.

Markus, L. M. (2000). Towards an integrated theory of IT-related risk control. In R. B. al, *Organizational and Social Perspectives on Information Technology* (pp. 167-178).

Mazzei, A., & Ravazzani, S. (2015). Internal crises communication strategies to protect trust relationships: A study of italian companies. *International Journal of Business Communication*, 319-337.

Mazzei, A., Kim, J., & Dell'Oro, C. (2012). Strategic value of employee relationships and communicative actions: Overcoming corporate crises with quality internal communication. *International Journal of Strategic Communication*, 31-44.

McCann, J. E. (2004). Building Agility and Resiliency During Turbulent Change. *Teleconference sponsored by Human Resource Planning Society*.

McFadzean, E., Jean-Noe, l. E., & Birchall, D. (2007). Perception of risk and the strategic impact of existing IT on information security strategy at board level. *Online Information Review*, 622-660.

Merriam-Webster. (2018). Retrieved from https://www.merriam-webster.com/dictionary/morale

Microsoft. (2017). *How to recognize phishing email messages, links, or phone calls*. Retrieved from Safety and Security Center: https://www.microsoft.com/en-us/safety/online-privacy/phishing-symptoms.aspx

Miles, R. E., Snow, C. C., Meyer, A. D., & Coleman, H. J. (1978). Organizational strategy, structure, and process. *cademy of management review,*, 546-562.

Mishra, A. (1996). Organizational responses to crisis. Trust in Organizations. *Frontiers of theory and research*, 261-287.

Mitchell, R. K., Agle, B. R., & Wood, a. D. (1997). Toward a theory of stakeholder identification and salience: Defining the principle of who and what really counts. *Academy of management review* , 853-886.

Mithas, S., Tafti, A., Bardhan, I., & Goh, J. (2012). Information Technology and Firm Profitability: Mechanisms and Empirical Evidence. *MIS Quarterly, 36*(1), 205-224.

Mitroff, I. I., Shrivastava, P., & Udwadia, F. E. (1987). Effective crisis management. *The Academy of Management Executive* , 283-292.

Moody, G., Siponen, M., & Pahnila, S. (n.d.). Toward a Unified Model of Information Security Policy Compliance. *MISQ*.

Moore, J. W. (2010). From Phishing to Advanced Persistent Threats: The Application of Cybercrime to the Enterprise Risk Management Model. *Review of Business Information Systems, 14*(4).

Mossburg, E., Fancher, D., & Gelinne, J. (2016). The hidden costs of an IP breach: Cyber theft and the loss of intellectual property. *Deloitte Review*, pp. 1-17.

NAIC. (2017). *The national system of state regulation and cybersecurity.* The Center for Insurance Policy and Research.

National Cybersecurity Institute. (2016). *How does a data breach affect your business' reputation?*

National Initiative for Cybersecurity Careers and Studies. (2017). *Cybersecurity Workforce Framework.* Department of Homeland Security.

National Institute of Standards and Technology. (2012). *Computer Security Incident Handling Guide.* U.S. Department of Commerce.

National Institute of Standards and Technology. (2014, February 12). *Framework for Improving Critical Infrastructure Cybersecurity.* Retrieved from http://www.nist.gov/itl/csd/launch-cybersecurity-framework-021214.cfm

Njenga, K., & Brown, I. (2012). Conceptualising improvisation in information systems security. *European Journal of Information Systems, 21*(6), 592-607.

Oetzel, C. M., & Spiekermann, S. (2013). A systematic methodology for privacy impact assessments: a design science approach. *European Journal of Information Systems, 23*(2), 126-150.

Oller, S. D. (2014). Exploratory Factor Analysis as a Tool for Investigating Complex Relationships: When Numbers are Preferred over Descriptions and Opinions. *Sage Research Method Cases*.

Olmstead, K., & Smith, A. (2017). *Americans and Cybersecurity.* Pew Research Center.

O'Neill, P. (2017, February 14). Target hack fallout finally got executives to pay attention to cybersecurity. *Cyberscoop.com*.

Parks, R., Xu, H., Chu, C.-H., & Lowry, P. B. (2016). Examining the intended and unintended consequences of organizational privacy safeguards. *European Journal of Information Systems, 26*(1), 37-65.

PCI Security Standards Council. (2017). *PCI Security*. Retrieved from https://www.pcisecuritystandards.org/pci_security/

Perlroth, N. (2018, January 1). How antivirus software can be turned into a tool for spying. *The New York Times*.

Perlroth, N., Larson, J., & Shane, S. (2013, September). N.S.A. Able to Foil Basic Safeguards of Privacy on Web. *New York Times*.

Peter, P. (1979). A review of psychometric basics and recent marketing practices. *Journal of Marketing Research, 16*(1), 6-17.

Peteraf, M. A. (1993). The cornerstones of competitive advantage: A resource-based view. *Strategic Management Journal, 14*(3), 179-191.

Pidgeon, N., & O'Leary, M. (2000). Man-made disasters: why technology and organizations (sometimes) fail. *Safety Science, 34*(1), 15-30.

Podsakoff, P., Mackenzie, S., Lee, J., & Podsakoff, N. (2003). Common Method Bias in Behavioral Research: A Critical Review of the Literature and Recommended Remedies. *Journal of Applied Psychology, 88*(5), 879-903.

Pool, E. (2009, July 20th). Quantifying Business Value of Information Security. *SANS Institute InfoSec Reading Room*, pp. 1-21.

Poole, E. (2009). Quantifying Business Value of Information Security Projects.

Preacher, K., & Hayes, A. (2004). SPSS and SAS Procedures for estimating indirect effects in simple mediation models. *Behavior Research Methods, Instruments, and Computers*, 717-731.

Privacy Rights Clearinghouse. (2016). *Identity Theft and Data Breaches*. Retrieved from https://www.privacyrights.org/topics/7

Puhakainen, P., & & Siponen, M. (2010). Improving employees' compliance through information systems security training: an action research study. *MISQ*, 757-778.

Quist, A. (1993). *Security Classification of Information.* Oak Ridge, Tennessee: Oak Ridge National Laboratory.

Rajivan, P., Janssen, M., & Cooke, N. (2013). Agent-Based Model of a Cyber Security Defense Analyst Team. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 57*(1), 314-318.

Reed, T., Abbott, R., Anderson, B., Nauer, K., & Forsythe, ,. (2014). Simulation of Workflow and Threat Characteristics for Cyber Security Incident Response Teams. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 58*(1), 427-431.

Reio, T. G., & Shuck, B. (2014). Exploratory Factor Analysis Implications for Theory, Research, and Practice. *Advances in Developing Human Resources, 17*(1), 12-25.

Rigdon, E. (2014). Rethinking partial least squares path modeling: breaking chains and forging ahead. *Long Range Planning, 47*(3), 161-167.

Ringle, C., Gotz, O., Wetzels, M., & Wilson, B. (2014). On the Use of Formative Measurement Specifications in Structural Equation Modeling: A Monte Carlo Simulation Study to Compare Covariance-Based and Partial Least Squares Model Estimation Methodologies. *METEOR Research Memoranda*, 1-43.

Ringle, C., Wende, S., & Becker, J. (2018). SmartPLS 3. Bonningstedt. Retrieved from http://www.smartpls.com

Robnagel, H., Zibuschka, J., Hinz, O., & Muntermann, J. (2014). Users' willingness to pay for web identity management systems. *European Journal of Information Systems*, 36-50.

Rogers, E., & Traurig, G. L. (2016). *Planning and Managing a Data Breach.* LexisNexis.

Rollo, H., & Tran, P. (2016, October 7th). Your Company Needs a Communications Plan for Data Breaches. *Harvard Business Review*.

Romanosky, S. (2016). Examing the Costs and Causes of Cyberincidents.

Romanosky, S., Telang, R., & Acquisti, A. (2011). Do data breach disclosure laws reduce identity theft? . *Journal of Policy Analysis and Management*.

Rouse, M. (2016). *Data Breach Definition.* http://searchsecurity.techtarget.com/definition/data-breach.

Rowley, T. I., & Moldoveanu, M. (2003). When will stakeholder groups act? An interest-and identity-based model of stakeholder group mobilization. *Academy of management review,*, 204-219.

Rowley, T. J. (1997). Moving beyond dyadic ties: A network theory of stakeholder influences. *Academy of management Review*, 887-910.

Ryan, J. J. (2003). The use, misuse, and abuse of statistics in information security research. *Proceedings of the 2003 ASEM National Conference.* St. Louis, MO.

Safdar, K., & Beilfuss, L. (2016, May 16th). Target Gives Weak Forecast as Sales Decline. *The Wall Street Journal*.

SafeNet Survey. (2016). SafeNet Survey of Companies in the United States.

Salancik, G. R., & Pfeffer, J. (1978). A social information processing approach to job attitudes and task design. *Administrative science quarterly,* , 224-253.

Salmela, H. (2008). Salmela, H. (2008). Analysing business losses caused by information systems risk: a business process analysis approach. *ournal of Information Technology,, 23*(3), 185-202.

Sanger, D., Chan, S., & Scott, M. (2017, May 14th). Ransomware's Aftershocks Feared as U.S. Warns of Complexity. *New York Times*.

Sanghavi, M. (2015). *Training Your Employees on Information Security Awareness.* Symantec Corporation.

Sarstedt, M., Ringle, C., Henseler, J., & Hair, J. (2012). On the emancipation of PLS-SEM: A commentary on Rigdon. *Long Range Planning, 47*(3), 154-160.

Satin, A., & Bernardi, P. (2015). Impact of distributed denial of service attacks on advanced metering infrastructure. *Wireless Personal Communication*, 2211-2223.

Scarfone, K., Souppaya, M., Cody, A., & Orebaugh. (2008). *Technical Guide to Information Security Testing and Assessment Special Publication 800-115.* National Institute of Standards and Technology U.S. Department of Commerce.

Senge, P., Kleiner, A., Roberts, C., Ross, R., & Smith, B. (1994). *The Fifth Discipline Fieldbook.* New York, NY: Doubleday.

Shane, N., Perlrothe, N., & Sanger, D. (2017, November 13th). N.S.A. Struggles to Recover After Huge Breach of Spying Tools. *New York Times*.

Sherwood, J. (1997). Managing Security for Outsourcing Contracts. *Computers and Security, 16*(1), 603-609.

Shin, J., Taylor, M., & Seo, M. (2012). Resources for change: The relationships of organizational inducements and psychological resilience to employees attitudes and behaviors toward organizational change. *Academy of Management Journal, 55*(3), 727-748.

Shinn, L. (2008). *Outsourcing Security: Are You Ready?* Inc.

Silowash, G., Capelli, D., Moore, A., Trzeciak, R., Shimeall, T., & Flynn, L. (2012). *Common sense guide to mitigating insider threats.* Software Engineering Institute Carnegie Mellon University.

Siponen, M., & Pahnila, S. (2014). Employees' Adherence to information security policies: An exploratory field study. *Information & Management, 51*(2), 217-244.

Siponen, M., & Vance, A. (2010). Neutralization: New Insights into the Problem of Employee Systems Security Policy Violations. *MISQ, 34*(3), 487-502.

Somers, S. (2009). Measuring Resilience Potential: An Adaptive Strategy for Organizational Crisis Planning. *Journal of Contingencies and Crisis Management*, 12-23.

Somers, S. (2009). Measuring resilience potential: an adaptive strategy for organizational crisis planning. *Journal of Contingencies and Crisis Management, 17*(1), 12-23.

Spanos, G., & Angelis, L. (2016). The impact of information security events to the stock market: A systematic literature review. *58*, 216-229.

Spears, J., & Barki, H. (2010). User Participation in Information Systems Security Risk Management. *MISQ, 34*(3), 503-522.

Steinbart, P., Keith, M., & Babb, J. (2016). Examining the Continuance of Secure Behavior: A Longitudinal Field Study of Mobile Device Authentication. *Information Systems Research, 27*(2), 219-239.

Steinke, J., Bolunmez, B., Fletcher, L., Wang, V., Tomassetti, A. J., Repchick, K. M., et al. (2015, July-Aug). Improving Cybersecurity Incident Response Team Effectiveness Using Teams-Based Research. *IEEE Security & Privacy, 13*(4).

Stolzenberg, R. M., & Relles, D. A. (1997). Tools for Intuition About Sample Selection Bias and Its Correction. *American Sociological Review*, 494-507.

Straub, D. W., & Nance, W. (1990). Discovering and Discipling Computer Abuse in Organizations: A Field Study. *MISQ*, 45-60.

Suhr, D. (2006). The basics of structural equation modeling. *SAS User Group of the Western Region of the United States .*

Sun, L., Srivastava, R., & Mock, T. (2006). An Information Systems Security Risk Assessment Model Under the Dempster-Shafer Theory of Belief Functions. *Journal of Management Information Systems, 22*(4), 109-142.

Sutcliffe, K. M., & & Vogus, T. J. (2003). Organizing for resilience. *Positive organizational scholarship: Foundations of a new discipline*.

Sutton, S., Hampton, C., Khazanchi, D., & Arnold, V. (2008). Risk Analysis in Extended Enterprise Environments: Identification of Critical Risk Factors in B2B E-Commerce Relationships. *Journal of the Association for Information Systems, 9*(4).

Team, C. L. (2010). *Is your NDA helping you commit a federal crime?* CompTIA.

TechRepublic. (2017). *Data breaches may cost less than the security to prevent them .*

The CERT Insider Threat Center. (2016). *Common Sense Guide to Mitigating Insider Threats.* Software Engineering Institute Carnegie Mellon University.

Thomas, J., Clark, S., & Gioia, D. (1993). Strategic sensemaking and organizational performance: Linkages among scanning, interpretation, action, and outcomes. *Academy of Management Journal*, 239-270.

Thompson, J. (1967). *Organizations in action.* New York, New York: McGraw-Hill.

Tinsley, H., & Tinsley, D. (1987). Uses of factor analysis in counseling psychology research. *Journal of Counseling Psychology, 34*(4), 414.

T-Mobile. (2015, October 8). *Frequently Asked Questions about the Experian Incident*. Retrieved from https://www.t-mobile.com/customers/experian-data-breach-faq

T-Mobile. (2016). *T-Mobile Delivers Unparalleled Financial Results – Tops Revenue and Adjusted EBITDA Estimates.* T-Mobile Media Kits.

Torres, A. (2015). *Building a world-class security operations center: A roadmap.* SANS Institute.

Trang, M. (2017). Compulsory Corporate Cyber-Liability Insurance: Outsourcing Data Privacy Regulation to Prevent and Mitigate Data Breaches. *Minn. JL Sci. & Tech.,*, 389.

U.S. Department of Commerce. (2013). *Security and privacy controls for federal information systems and organizations.* Washington, D.C.: U.S. Department of Commerce.

U.S. Small Business Administration. (2017). Table of Size Standards. Washington, District of Columbia, United States. Retrieved September 22, 2018, from https://www.sba.gov/document/support--table-size-standards

U.S. Small Business Administration. (2018). *Size Standards.*

U.S.Computer Emergency Readiness Team. (2015, September 30th). *Federal Incident Reporting Guidelines*. Retrieved from https://www.us-cert.gov/government-users/reporting-requirements

United States Census Bureau. (2017). *Introduction to NAICS*. Retrieved from North American Industry Classification System: https://www.census.gov/eos/www/naics/

University of South Florida. (2010, June 11th). *Sensitivity and criticality of data.* University of South Florida.

Verizon. (2015). *Verizon 2015 Data Breach Investigations Report.* Verizon Enterprises.

Vinton, K. (2014, July 1). How Companies Can Rebuild Trust After A Security Breach. *Forbes*.

Virany, B., Tushman, M., & Romanelli, E. (1992). Executive succession and organization outcomes in turbulent environments: An organization learning approach. *Organization Science, 3*(1), 72-91.

Virvilis, N., Gritzalis, D., & Apostolopoulous, T. (2014). Trusted computing vs. Advanced persistant threats: Can a defender win this game. *Information Security and Critical Infrastructure Protection Research Laboratory* .

Vurukonda, N., & B.Thirumala, R. (2016). A Study on Data Storage Security Issues in Cloud Computing. *Procedia Computer Science*, 128-135.

Wang, J., Chaudhury, A., & Rao, R. H. (2008). Research Note—A Value-at-Risk Approach to Information Security Investmen. *Information Systems Research, 19*(1), 106-120.

Wang, T. W., Rees, J., & & Kannan, K. N. (2008). The Association between the Disclosure and the Realization of Information Security Risk. . *Working Paper*.

Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: The Insider Threat. *European Journal of Information Systems*, 101-105.

Weick, K. (1995). *Sensemaking in organizations.* Thousand Oaks, CA: SAGE.

Werlinger, R., Muldner, K., Hawkey, K., & & Beznosov, K. (2010). Preparation, detection, and analysis: the diagnostic work of IT security incident response. *Information Management & Computer Security*, 26-42.

Whitley, E., Gal, U., & Kjaergaard, A. (2014). Who do you think you are? A review of the complex interplay between information systems, identification and identity. *European Journal of Information Systems, 23*(1), 17-35.

Williams, T., Gruber, D., Sutcliffe, K., & Shepherd, D. (2017). Organizational response to adversity: Fusing crises management and resilience research streams. *The Academy of Management Annals*.

Williamson, G., & Moynihan, M. C. (2014). The liability hole- cybersecurity risks and the apportionment. *The Investment Lawyer, 21*(12), 4-16.

Wired.com. (2011). *Data Breach Notification*. Retrieved from https://www.wired.com/images_blogs/threatlevel/2011/05/Data-Breach-Notification.pdf

Wright, P. M., McMahan, G. C., & McWilliams, A. (1994). Human resources and sustained competitive advantage: a resource-based perspective. *International Journal of Human Resource Management, 5*(2), 301-326.

Wu, Y., Feng, G., Wang, N., & Liang, H. (2015). Game of information security investment: Impact of attack types and network vulnerability. *Expert Systems with Applications, 42*(15-16), 6132-6146.

Zafar, H., Ko, M., & Osei-Bryson, K. M. (2012). Financial impact of information security breaches on breached firms and their non-breached competitors. *Information Resources Management Journal, 25*(1), 21-37.

Zhao, X., Xue, L., & Whinston, A. (2013). Managing Interdependent Information Security Risks: Cyberinsurance, Managed Security Services, and Risk Pooling Arrangements. *Journal of Management Information Systems, 30*(1), 123-152.

CHAPTER 11: APPENDICES

11.1 Appendix A Interview Scripts

Technology Related Measures

How did the organizational information technology infrastructure change as a result of the information security failure?

Did the organization undertake any new technical cybersecurity or information security initiatives?

Prior to the information security failure event were all or part of the information security function sourced by third party vendors? If so, did this increase or decrease after the information security event?

Business Process Related Measures

were daily organizational business processes modified as a result of the information security failure event in any part of the organization? If so, in what ways?

were processes already in place to handle an information security event should it occur? What about this particular event was unique, if anything?

Did the information security failure event in the long run lead to increased efficiencies and/or decreased costs in any part of the organization? If so, please describe this.

Governance Related Measures

How is the information technology function structured? In what context does the information security function fit into the IT function? How is the information security function contextualized in other functions within the organizations ?

Prior to the information security failure event did the organization assign information security as a formal responsibility to someone? Was this changed after the information security failure event?

Prior to the information security failure did the organization have formal IT Governance and/or Data Governance and/or Information Governance measures in place? If so, please describe them? How did these functions operate independently and together(if at all)?

In your opinion, were the governance measures that the organization developed; were they implemented and practiced through the organization like

they should have been? Did this contribute to the information security failure event or alternately did these measures actually help to contain the information security failure event?

Strategy Related Measures

How was the information security failure communicated to internal shareholders?

How was the information security failure communicated to external shareholders?

What specific points did the organization want to hone in on and what specific points did the organization not want to bring attention to?

What role did social media, if any play in the organizations communication of the information security failure event?

What specific resource allocation decisions were made to enable sustainability? What decisions were made to enable resiliency?

Human Resource Related Measures

Did organizational morale consciously or unconsciously play a role in the information security event? If so, in what ways?

Did the information security failure event reveal to the organization any gaps in the knowledge in skillsets within any particular function such as the IT, InfoSec or any other functions?

Did the organization hire additional or more specialized talent because of the information security failure event?

Did information security job descriptions evolve because of the information security failure event ? If so, in what ways?

11.2 Appendix B Constructs and Measures (Final Survey Instrument)

Examining the Organizational Losses and Responses of IT Security Breaches

Start of Block: Prescreening Assessment Questions and Consent

Q1
Prescreen Assessment Question 1 of 3: Is your current or former occupation(s) within the last three years related to one or more aspects of IT security? *(This includes roles responsible for collecting and managing data based on specific guidelines and protocols)*

○ Yes (1)

○ No (2)

○ Decline Response (3)

Q2
Prescreen Assessment Question 2 of 3: Are you familiar with at least one IT security breach or IT security failure within your current or former workplace in the last three years?

○ Yes (1)
○ No (2)
○ Unknown/ Not Sure (3)
○ Decline Response (4)

Q46 Prescreen Assessment Question 3 of 3: Can your current or former occupation(s) within the last three years be considered a leadership or decision making role?

○ Yes (1)
○ No (2)
○ Decline Response (3)

Q3 **University of Illinois at Chicago Research Information and Consent for Participation in Social Behavioral Research** "Examining the Losses and Organizational Responses of IT Security Breaches" You are being asked to participate in a research study. Researchers are required to provide a consent form such as this one to tell you about the research, to explain that taking part is voluntary, to describe the risks and benefits of participation, and to help you to make an informed decision. You should feel free to ask the researchers any questions you may have. **Principal Investigator Name and Title** Atiya Avery, Doctoral Candidate **Department and Institution** University of Illinois at Chicago Department of Information and Decision Sciences **Address and Contact Information** 2404 UH MC 294 601 S. Morgan, Chicago IL 60607-7125 You are being asked to be a subject in a research study to better understand the impacts and managerial tactics related to IT security breaches within organizations. You have been asked to participate in the research because you are an information technology security practitioner or you are familiar with information technology security within the context of organizations. Your participation in this research is voluntary. Your decision whether to participate will not affect your current or future dealings with the University of Illinois at Chicago.If you decide to participate, you are free to withdraw at any time without affecting that relationship. What is the purpose of this research? The purpose of this research is to measure and evaluate the impacts and managerial tactics related to IT security breach events. The research aims to measure and evaluate perceptions of differences between and amongst organizational impacts and managerial tactics related to IT security breaches within organizations. What are the potential risks and discomforts? To the best of the knowledge, the things you will be doing have no more risk of harm than you would experience in everyday life. Online security cannot be guaranteed. Subjects may be identified or tracked via being linked to and or using social media or an email listserve. A risk of this research is a loss of privacy (revealing to others that you are taking part in this study) or confidentiality (revealing information about you to others to whom you have not given permission to see this information). Precautions have been taken to minimize these risks.

Are there benefits to taking part in the research? This study is not designed to benefit you directly. This study is designed to learn more about the impacts of IT security breaches and associated managerial tactics. The study results may be used to help other people in the future. Will I be reimbursed for any of my expenses or paid for my participation in this research? You will not be offered payment for being in this study. Can I withdraw or be removed from the study? If you decide to participate, you are free to withdraw your consent and discontinue participation at any time. The Researchers also have the right to stop your participation in this study without your consent for any reason at any time or if they believe it is in your best interests. What is the expected duration of this study? This study is expected to take on average about 15 minutes to complete.

Whom should we contact if we have questions? Contact the researchers Atiya Avery, Doctoral Candidate at aavery3@uic.edu or Ranganathan Chandrasekaren, Professor at ranga@uic.edu if you have any questions about this study or your part in it. What are my rights as a research subject? If you feel you have not been treated according to the descriptions in this form, or if you have any questions about your rights as a research subject, including questions, concerns, complaints, or to offer input, you may call the Office for the Protection of Research Subjects (OPRS) at 312-996-1711 or 1-866-789-6215 (toll-free) or e-mail OPRS at uicirb@uic.edu. Remember: Your participation in this research is voluntary. Your decision whether to participate will not affect your current or future relations with the University. If you decide to participate, you are free to withdraw at any time without affecting that relationship.
I have read (or someone has read to me) the above informationI have been given an opportunity to ask questions and my questions have been answered to my satisfactionI agree to participate in this research

▼ Yes (1) ... I decline to participate in this research (3)

End of Block: Prescreening Assessment Questions and Consent

Start of Block: Section: Respondent Level Control Variables

Q15 Choose ONE IT security breach that your current or a prior organization experienced within the past 3 years which in your opinion was important and crucial. Briefly describe the breach or attack. (Type Response)

____

Q16 *Keeping the security breach in mind, answer all of the following questions in this section.*

Q6 Which of the following is/was closest to your job title? (Select One)

- ○ Professor/Teacher/Researcher(including graduate research assistants) (1)
- ○ External Consultant (2)
- ○ Technical/Engineering (3)
- ○ Practitioner/Professional (4)
- ○ Supervisor/Manager (5)
- ○ Director (6)
- ○ Officer (7)

End of Block: Section: Respondent Level Control Variables

Start of Block: Section: Firm Level Control Variables

Q18 *Keeping the security breach in mind, answer all of the following questions in this section.*

Q7 In what industry does the organization that experienced the breach event primarily operate? (Select One)

- ○ Energy/Utilities (1)
- ○ Finance/Insurance/Banking (2)
- ○ Government/ Public Sector (3)
- ○ Healthcare (4)
- ○ IT/Telecom (5)
- ○ Logistics/Transportation (6)
- ○ Manufacturing/Engineering (7)
- ○ Professional/Business Services (8)
- ○ Retail/Wholesale (9)

Q8 To the best of your knowledge, approximately how many people were/are employed by the organization that experienced the breach, including all branches, divisions, and subsidiaries? (Select One)

❍ 0-999 (1)

❍ 1,000-4,999 (2)

❍ 5,000-9,999 (3)

❍ 10,000-24,999 (4)

❍ 25,000-49,999 (5)

❍ 50,000-99,999 (6)

❍ 100,000 or more (7)

Q9 To the best of your knowledge, what was/is the annual revenue of the organization that experienced the breach including all branches, divisions, and subsidiaries? (Select One)

❍ Less than one million dollars (USD) (1)

❍ At least one million dollars but less than ten million dollars (USD) (2)

❍ At least ten million dollars but less than one hundred million dollars (USD) (3)

❍ At least one hundred million dollars but less than five hundred million dollars (USD) (4)

❍ At least five hundred million dollars but less than one billion dollars (USD) (5)

❍ At least one billion dollars but less than ten billion dollars (USD) (6)

❍ At least ten billion dollars or more (USD) (7)

Q10 My organization that experienced the IT security breach had/has a senior executive who has exclusive responsibility (e.g. Chief Information Security Officer) for IT security. (Select One)

❍ Yes (1)

❍ No (2)

Q11 To the best of your knowledge, what is the title of the position that has final responsibility for IT security operations in the organization that experienced the IT security breach? (Select One)

○ Director (1)

○ Vice President (2)

○ Officer (3)

○ President/CEO (4)

○ Other (5) ____

Q12 My organization that experienced the IT security breach has/had a formal unit or team to take care of IT security breaches? (Select One)

○ Yes (1)

○ No (2)

Q13 To the best of my knowledge, the processes and roles responsible for IT security within the organization that experienced the IT security breach can best be characterized as? (Select One)

○ Non-existent: Processes and roles are not applied and the institution has not recognized the need for them. (1)

○ Initial: Processes and roles are informal and uncoordinated. (2)

○ Repeatable: Processes and roles follow a regular pattern. (3)

○ Defined: Processes and roles are documented and communicated. (4)

○ Managed: Processes and roles are monitored and measured. (5)

○ Optimized: Best practices for processes and roles are followed, and there are provisions for amending processes. (6)

End of Block: Section: Firm Level Control Variables

Start of Block: Section: IT Security Breach Characteristics

Q19 *Keeping the security breach in mind, answer all of the following questions in this section.*

Q46 Extent of the Breach
To the best of your knowledge, to what extent did the IT security breach involve the following?

	A great deal (1)	Significantly (2)	Alot (3)	Moderately (4)	Somewhat (5)	Slightly (6)	None (7)
A. Unauthorized access to sensitive information about your customers or suppliers (1)	○	○	○	○	○	○	○
B. Unauthorized access to confidential information about your products, services, intellectual property or internal records (2)	○	○	○	○	○	○	○
C. Unauthorized use of computers, networks or servers by staff, even if accidental (3)	○	○	○	○	○	○	○
D. Unauthorized use or hacking of computers, networks, or servers by staff, even if accidental (4)	○	○	○	○	○	○	○
E. Your organization's computers becoming infected with ransomware, spyware or malware (5)	○	○	○	○	○	○	○

F. Attacks that try to take down or disrupt your website or online services (6)	○	○	○	○	○	○	○

Q21
Reach of the Breach
To the best of your knowledge, to what extent did the IT security breach affect the following stakeholders?

	A great deal (1)	Significantly (2)	Alot (3)	Moderately (4)	Somewhat (5)	Slightly (6)	None (7)
A. Employees in one department or location (1)	○	○	○	○	○	○	○
B. Employees in multiple departments or locations (2)	○	○	○	○	○	○	○
C. Customers (3)	○	○	○	○	○	○	○
D. Suppliers (4)	○	○	○	○	○	○	○
E. External Consultants or Contractors (5)	○	○	○	○	○	○	○

Q22
Breach Identification Period
To the best of your knowledge, how long was it, if any time at all, between this IT security breach occurring and it being identified as a breach? (Select One)

- ○ A. Immediate (1)
- ○ B. Within a few hours (2)
- ○ C. Within 24 hours (3)
- ○ D. Within a week (4)
- ○ E. Within a month (5)
- ○ F. Within 90 days (6)
- ○ G. Longer than 90 days (7)

Q23
Breach Intentionality
To the best of your knowledge, was the breach intentional or accidental? (Select One)

- ○ A. Intentional by an insider (1)
- ○ B. Accidental by an insider (2)
- ○ C. Intentional by an outsider (3)
- ○ D. Accidental by an outsider (4)

Q24
Breach Source
To the best of your knowledge, who or what was the source of the breach? (Select All That Apply)

- □ A. 3rd party supplier(s) or vendor(s) (1)
- □ B. Competitor(s) (2)
- □ C. Emails/email attachments/websites (3)
- □ D. Employee(s) (4)
- □ E. Former employee(s) (5)
- □ F. Malware author(s) (6)
- □ G. Nation-state intelligence services (7)
- □ H. Natural (flood, fire, lightning etc.) (8)
- □ I. Non-professional hacker(s) (9)
- □ J. Organized crime (10)
- □ K. Terrorists (11)
- □ L. Unknown / unidentifiable sources (12)

Q25
Breach Exposure
To the best of your knowledge, which best describes the IT security breach event? (Select One)

- ○ A. Information/Data/Records/System Resources were exposed but not retrieved or used by an unauthorized third party (1)
- ○ B. Information/Data/Records/ System Resources were exposed and retrieved but not used by an unauthorized third party (2)
- ○ C. Information/Data/Records/ System Resources were exposed and retrieved and used by an unauthorized third party (3)
- ○ D. Unknown (4)

Q26
Breach Sensitivity
To the best of your knowledge, what was the highest level of sensitivity of the breached data/information/records/systems? (Select One)

○ A. Not Sensitive: Confidentiality was not compromised. (1)

○ B. Somewhat Sensitive: No confirmation exists that confidentiality was compromised. (2)

○ C. Quite Sensitive: The confidentiality of personally identifiable information was compromised. (3)

○ D. Very Sensitive: The confidentiality of proprietary data, information, records, or systems was compromised. (4)

○ E. Extremely Sensitive: The confidentiality of core infrastructure credentials was compromised. (5)

End of Block: Section: IT Security Breach Characteristics

Start of Block: Section: IT Security Breach Impacts

Q27

Keeping the security breach in mind, answer all of the following questions in this section.

To what extent did the IT security breach result in the following losses:

	A great deal (1)	Significantly (2)	Alot (3)	Moderately (4)	Somewhat (5)	Slightly (6)	None (7)
A. Decline in stock prices (1)	❍	❍	❍	❍	❍	❍	❍
B. Decline in organizational revenue (2)	❍	❍	❍	❍	❍	❍	❍
C. Increase in cost of operations (3)	❍	❍	❍	❍	❍	❍	❍
D. Legal costs (4)	❍	❍	❍	❍	❍	❍	❍
E. System downtime (5)	❍	❍	❍	❍	❍	❍	❍
F. Loss in employee productivity (6)	❍	❍	❍	❍	❍	❍	❍
G. Time delays in business operations (7)	❍	❍	❍	❍	❍	❍	❍
H. Loss of competitive advantage (8)	❍	❍	❍	❍	❍	❍	❍
I. Severed relationships with suppliers or partners (9)	❍	❍	❍	❍	❍	❍	❍
J. Loss of existing customers (10)	❍	❍	❍	❍	❍	❍	❍
K. Loss of potential, new customers (11)	❍	❍	❍	❍	❍	❍	❍
L. Loss of company reputation or	❍	❍	❍	❍	❍	❍	❍

image (12)							
M. Loss of public goodwill (13)	❍	❍	❍	❍	❍	❍	❍

End of Block: Section: IT Security Breach Impacts

Start of Block: Governance Tactics

Q28
Keeping the security breach in mind, answer all of the following questions in this section.

For the IT security breach you outlined, to what extent to do you agree with the following statements about your organization?

	Strongly agree (1)	Agree (2)	Somewhat agree (3)	Neither agree nor disagree (4)	Somewhat disagree (5)	Disagree (6)	Strongly disagree (7)
A. My organization has adopted and implemented one or more international standards for handling IT security breaches (3)	○	○	○	○	○	○	○
B. My organization has developed formal procedures and rules for managing any IT security breaches (4)	○	○	○	○	○	○	○
C. In my organization, IT security is the responsibility of both IT and other functional managers (5)	○	○	○	○	○	○	○

Q29
For the IT security breach you outlined, to what extent do you agree with the following statements?

	Strongly agree (1)	Agree (2)	Somewhat agree (3)	Neither agree nor disagree (4)	Somewhat disagree (5)	Disagree (6)	Strongly disagree (7)
A. My organization utilized ad-hoc teams to manage the fall-out from the IT security breach (1)	○	○	○	○	○	○	○
B. My organization worked with an external vendor to manage the fall-outs from IT security breaches (2)	○	○	○	○	○	○	○

End of Block: Governance Tactics

Start of Block: Communication Tactics

Q30

Keeping the security breach in mind, answer all of the following questions in this section.

For the IT security breach you outlined, to what extent to do you agree with the following statements about your organization?

	Strongly agree (1)	Agree (2)	Somewhat agree (3)	Neither agree nor disagree (4)	Somewhat disagree (5)	Disagree (6)	Strongly disagree (7)
A. My organization has designated specific personnel to communicate about any IT security breaches (1)	❍	❍	❍	❍	❍	❍	❍
B. My organization has an official plan outlining how to communicate internally about IT security breaches (2)	❍	❍	❍	❍	❍	❍	❍
C. My organization has an official plan outlining how to communicate externally about IT security breaches (3)	❍	❍	❍	❍	❍	❍	❍
D. My organization ensured timely notification to all internal stakeholders about the breach (4)	❍	❍	❍	❍	❍	❍	❍

E. My organization ensured timely notification to external stakeholders about the breach (5)	○	○	○	○	○	○	○
F. My organization had a clear, strategy-based public relations response about the breach (6)	○	○	○	○	○	○	○

Q31 Which of the following describes the disclosure pertaining to the IT security breach? (Select One)

○ A. Disclosed to very selective personnel who identified the breach (1)

○ B. Disclosed only to limited employees within the IT function (2)

○ C. Disclosed only within IT function (3)

○ D. Disclosed to IT function and to selected units outside the IT function. (4)

○ E. Disclosed organization-wide to all employees and internal stakeholders (5)

○ F. Disclosed to both internal and external stakeholders (6)

○ G. Disclosed to everyone, including general public (7)

Q32
What was the extent of the information disclosed to external stakeholders regarding the breach? (Select One)

- ○ A. No information was disclosed (1)
- ○ B. Disclosure that a breach occurred but no additional details (2)
- ○ C. Disclosure that a breach occurred with some details (3)
- ○ D. Whatever was legally required (4)
- ○ E. Additional information above legal requirement (5)
- ○ F. All details but internal or proprietary information (6)
- ○ G. Full disclosure (7)

Q33 When did your organization issue an official response for the IT security breach? (Select One)

- ○ A. During the breach event as it unfolded (1)
- ○ B. Immediately (within a day) after the breach was discovered (2)
- ○ C. Few days after the breach event was discovered (3)
- ○ D. A week after the breach was discovered (4)
- ○ E. Few weeks / month after the breach was discovered (5)
- ○ F. Only after constituents presented questions or complaints (6)
- ○ G. No official response was issued (7)

End of Block: Communication Tactics

Start of Block: Security Strategy Tactics

Q34

Keeping the security breach in mind, answer all of the following questions in this section.

To what extent to do you agree with the following statements about your organization that experienced the IT security breach?

	Strongly agree (1)	Agree (2)	Somewhat agree (3)	Neither agree nor disagree (4)	Somewhat disagree (5)	Disagree (6)	Strongly disagree (7)
A. My organization has a formal plan in place for managing IT security (1)	❍	❍	❍	❍	❍	❍	❍
B. My organization's IT security strategy includes both technical and non-technical aspects (2)	❍	❍	❍	❍	❍	❍	❍
C. My organization engaged senior business (non-IT) executives in framing policies pertaining to IT security (3)	❍	❍	❍	❍	❍	❍	❍
D. Our IT security strategy covers all digital assets (hardware, software, and applications) and data hosted internally as well as externally (4)	❍	❍	❍	❍	❍	❍	❍
E. Our IT security strategy	❍	❍	❍	❍	❍	❍	❍

covers external IT vendors or third parties we use for any IT or data related work (5)							
F. Our IT security strategy covers employee-owned IT, mobile devices and digital accessories that they bring to work (6)	○	○	○	○	○	○	○
G. My organization has formal training program(s) to increase IT security awareness among employees (7)	○	○	○	○	○	○	○
H. Our organization has made adequate investments in IT security (8)	○	○	○	○	○	○	○

Q35
To what extent did your organization's IT security strategy cover the following? (Choose All That Apply)

- □ A. Company-owned hardware and software (1)
- □ B. Data centers (2)
- □ C. Employee-owned mobile devices (e.g. smart phones, tablets) (3)
- □ D. Employee-owned personal laptops (4)
- □ E. Internal sites or portals (5)
- □ F. Websites or online resources hosted by third parties (6)
- □ G. Digital data or applications on cloud (7)

Q36
To what extent do you agree with the following statements about your organizational actions after the IT security breach?

	Strongly agree (1)	Agree (2)	Somewhat agree (3)	Neither agree nor disagree (4)	Somewhat disagree (5)	Disagree (6)	Strongly disagree (7)
A. After the breach, my organization decided to increase the IT security investments. (1)	○	○	○	○	○	○	○
B. After the breach, my organization came up with additional measures and plans to enhance IT seucirty (2)	○	○	○	○	○	○	○
C. Our IT security strategy was considerably revised after the breach. (4)	○	○	○	○	○	○	○

End of Block: Security Strategy Tactics

Start of Block: Liability Management Tactics

Q37

Keeping the security breach in mind, answer all of the following questions in this section.

To what extent do you agree with the following statements about your organization that experienced the breach?

	Strongly agree (1)	Agree (2)	Somewhat agree (3)	Neither agree nor disagree (4)	Somewhat disagree (5)	Disagree (6)	Strongly disagree (7)
A. My organization has invested in adequate cyber insurance to cover any potential damages arising from cyber-attacks or IT security breaches (1)	❍	❍	❍	❍	❍	❍	❍
B. My organization has adequate liability provisions in contractual agreements with external organizations who collect, store, use or access the data (2)	❍	❍	❍	❍	❍	❍	❍
C. My organization regularly reviews contractual protections and vendor liabilities related to IT security breaches (3)	❍	❍	❍	❍	❍	❍	❍

Q38
In the event of an IT security breach to what extent were the risks of liability (e.g. damages, claims, and legal and compliance burdens) transferable to an insurance provider? (Select One)

- ○ A. Less than 10% (1)
- ○ B. 11 - 25% (2)
- ○ C. 26 - 50% (3)
- ○ D. 51 - 75% (4)
- ○ E. 76 - 100 % (5)

Q39
To what extent do you agree with the following statements about your organizational actions after the IT security breach you outlined?

	Strongly agree (1)	Agree (2)	Somewhat agree (3)	Neither agree nor disagree (4)	Somewhat disagree (5)	Disagree (6)	Strongly disagree (7)
A. My organization reviewed vendor liability policies after the breach (1)	○	○	○	○	○	○	○
B. My organization reviewed current cyber-insurance provisions after the breach (2)	○	○	○	○	○	○	○
C. My organization invested in additional insurance for addressing potential future breaches (3)	○	○	○	○	○	○	○

End of Block: Liability Management Tactics

Start of Block: Relationship Management Tactics

Q40

Keeping the security breach in mind, answer all of the following questions in this section.

To what extent to do you agree with the following statements about your organization?

	Strongly agree (1)	Agree (2)	Somewhat agree (3)	Neither agree nor disagree (4)	Somewhat disagree (5)	Disagree (6)	Strongly disagree (7)
A. IT security is adequately covered in the agreements with suppliers, customers and other business partners (1)	❍	❍	❍	❍	❍	❍	❍
B. My organization regularly reviews the information security and privacy policies, practices and procedures of external parties who collect, store, use or access the data (2)	❍	❍	❍	❍	❍	❍	❍
C. My organization regularly reviews agreements and work arrangements with contracted IT security vendors (3)	❍	❍	❍	❍	❍	❍	❍
D. My organization regularly engages the external business	❍	❍	❍	❍	❍	❍	❍

partners in reviewing IT security arrangements (4)							

Q41 To what extent to do you agree with the following statements about your organization?

	Strongly agree (1)	Agree (2)	Somewhat agree (3)	Neither agree nor disagree (4)	Somewhat disagree (5)	Disagree (6)	Strongly disagree (7)
A. My organization revised IT security related provisions in agreements with the business partners (1)	○	○	○	○	○	○	○
B. My organization made changes to the agreements with IT security vendors (2)	○	○	○	○	○	○	○
C. My organization had discussions with effected external parties (3)	○	○	○	○	○	○	○

End of Block: Relationship Management Tactics

Start of Block: IT Resource Management Tactics

Q42

Keeping the security breach in mind, answer all of the following questions in this section.

To what extent to do you agree with the following statements about your organization that experienced the IT security breach?

	Strongly agree (1)	Agree (2)	Somewhat agree (3)	Neither agree nor disagree (4)	Somewhat disagree (5)	Disagree (6)	Strongly disagree (7)
A. My organization has a dedicated team to monitor IT security incidents in real-time (1)	○	○	○	○	○	○	○
B. My organization regularly engages in mock crisis-exercises for managing potential IT security breaches (2)	○	○	○	○	○	○	○
C. My organization has invested in automated security incident management systems (3)	○	○	○	○	○	○	○
D. My organization regularly engages in assessment of IT security risks (e.g.: vulnerabilityscanning, penetration testing etc.). (4)	○	○	○	○	○	○	○
E. My organization uses advanced biometric authentication techniques (e.g.: using fingerprint, retina scan, facial identification etc.) (5)	○	○	○	○	○	○	○
F. My organization has authentication methods that restricts use of IT systems from specific location(s) or computers(s) (6)	○	○	○	○	○	○	○

Q43
To what extent do you agree with the following statements about your organizational actions after the IT security breach you outlined?

	Strongly agree (1)	Agree (2)	Somewhat agree (3)	Neither agree nor disagree (4)	Somewhat disagree (5)	Disagree (6)	Strongly disagree (7)
A. After the breach, my organization decided to hire additional IT security staff (1)	○	○	○	○	○	○	○
B. After the breach, my organization made readjustments to internal teams (2)	○	○	○	○	○	○	○
C. After the breach, we invested in newer IT security systems or applications. (3)	○	○	○	○	○	○	○

End of Block: IT Resource Management Tactics

Start of Block: Morale Management Tactics

Q44

Keeping the security breach in mind, answer all of the following questions in this section.

To what extent to do you agree with the following statements about your organization?

	Strongly agree (1)	Agree (2)	Somewhat agree (3)	Neither agree nor disagree (4)	Somewhat disagree (5)	Disagree (6)	Strongly disagree (7)
A. My organization regularly informs employees about potential problems to IT security (e.g. new viruses, malware, cyberattacks etc.) (1)	○	○	○	○	○	○	○
B. My organization has explicit rewards (punishments) for compliance (non-compliance) with organization prescribed IT security protocols (2)	○	○	○	○	○	○	○
C. My organization regularly engages employees from different departments or units to enhance IT security (3)	○	○	○	○	○	○	○

Q46
To what extent do you agree with the following statements about your organizational actions after the IT security breach?

	Strongly agree (1)	Agree (2)	Somewhat agree (3)	Neither agree nor disagree (4)	Somewhat disagree (5)	Disagree (6)	Strongly disagree (7)
A. My organization engaged in specific activities to boost employee morale after the breach (1)	○	○	○	○	○	○	○
B. My organization provided autonomy to IT security professionals to handle the breach (2)	○	○	○	○	○	○	○
C. My organization engaged in discussions with employees affected by the breach (3)	○	○	○	○	○	○	○

End of Block: Morale Management Tactics

Start of Block: Section: Additional Questions

Q47
Are there additional **impacts** from IT security breach events that you felt were not captured in this survey? (Type Response)

____

____

____

____

____

Q48
Are there additional **managerial tactics** which may moderate the impacts of IT security breach events that you felt were not captured in this survey? (Type Response)

____

____

____

____

____

End of Block: Section: Additional Questions

11.3 Appendix C Subject Matter Expert Quotes on Unexpected Results

Relationship	Relationship Type	Subject Matter Expert 1	Subject Matter Expert 2
Communication Management -> Reputational Outcomes	Negative	"Not sure why this is happening but if you utilize communication management you can have nothing but positive outcomes. When I think management I think management teams. Notifying them about the breach and new controls is going to trick down to the staff. Reputation will be become good if positive communication. PR and marketing tell us how to state things when big issues and breaches happen things are sugarcoated, these are professionals. The process works and the outcome would be good. "	"Part of this could be attributed to the reduction in transparency. Reducing transparency causes a reduction."
Communication Management -> Financial Outcomes	Negative	"No, only if a breach happens and you get fined for it. If you let everyone know on the financial statements and it sounds positive the idea is to minimize financial outcomes. So you need to tell your story and everyone will make up their own story. "	"Similarly the same for financial, increase in more management leads to bureaucracy."
IT Resource Management -> Financial Outcomes	Negative	"You don't have people in place to do the IT security processes may cause fines."	"It depends up how the IT is setup is it project driven or driven by growth needs, If it lots of projects IT groups cant do anything."
Morale Mgmt -> Competitive Outcomes	Negative	"If you don't really have a manager their to push the morale through the company it may increase apathy, mistakes etc decreasing its competitiveness. Employees are really sensitive to that nowdays may cause a revolving a door. "	"With morale management, is it genuine or superficial moral management. If its superficial it wont improve competitive outcomes."

Communication Management -> Business Productivity Outcomes	Negative	"If you go back and look at moral, again if you tell a story your ahead. It doesn't hurt business productivity because that communication is awareness. Just being on the same page. Sharing information between business units to ensure proper controls are in place. "	"Same deal of increase in overhead and bureaucracy which can impact business productivity."
IT Resource Management -> Competitive Outcomes	Negative	"If the teams are not in place it could create lost opportunities"	"Going back to IT Resource Management (points noted earlier) could be over management reducing the agility of the organization. Has to be optimal amount of management not too much"
Communication Management -> Competitive Outcomes	Negative	"Again, proper communication should help to show how competitive the organization is. Will help in outcome when it comes to competition consider transparency of privacy policies. "	"Reduced transparency"
IT Resource Management -> Reputational Outcomes	Negative	"Again, these are the guys who the management for you if you don't have a good team that is the only way it would cause problem. "	"Again, same project focus IT versus growth IT can limit agility people are scrambling."
Morale Mgmt -> FinancialOutcomes	Negative	"Morale will start off bad in the context of finance. Morale will get hit a little"	"Is the morale management, genuine, superficial or is it behavior modification. If they're trying to modify company behavior through morale not sure if it will lead to positive outcomes. This is the same for all outcomes related to morality."
Moral eMgmt -> Reputational Outcomes	Negative	"Want to let outsiders know company is sorry. Someone will get fired. Reputation will start off shaky but you can bounce back. "	"Is the morale management, genuine, superficial or is it behavior modification. If they're trying to modify company behavior through morale not sure if it will lead to positive outcomes. This is the same for all outcomes related to morality."

Morale Mgmt -> Business Productivity Outcomes	Negative	"Build in controls afterwards to better understand where weaknesses. Where you aware of what vendors were going. "	"Is the morale management, genuine, superficial or is it behavior modification. If they're trying to modify company behavior through morale not sure if it will lead to positive outcomes. This is the same for all outcomes related to morality."
Security Strategic Management -> Business Productivity Outcomes	Negative	"Again, I am looking at management not having a proper program in place. What is a program and what does a program look like. "	"Its always been known that more security controls can limit performance and productivity not even at org level but system level. Classic tug of war."
Liability Management -> Financial Outcomes	Negative	"In order for you to get a good rating or cyberinsurance you need to have certain things in place, good hygiene. You may not get good insurance rating thus causing increase in financial outcomes. If you have issues you may not get cyberinsurance, you will get declined or rate may go up. "	"More risk adverse company, may see more risk adverse environment with no risk or innovation taken."
IT Resource Management -> Business Productivity Outcomes	Negative	"Not having the right resource or compliance in place would impact the business. Also may cause issues with workarounds i.e. cannot utilize credit cards. You want to keep the business focus the most important thing is to tie things back to the business. "	"Same points noted earlier IT tends to have project focus."
Liability Management -> Reputational Outcomes	Negative	"Same thing as financial outcomes, I can think of a merger between two health insurance companies. One company has liability management in place the other did not they trust but did not verify. "	"Too much risk adverse you start to fall behind."

Appendix D University of Illinois at Chicago Institutional Review Board Approval

Approval Notice
Initial Review (Response To Modifications)

February 27, 2018

Atiya Avery
Information and Decision Sciences
University Hall
601 S. Morgan Street 24 Floor
Chicago, IL 60607

RE: Protocol # 2018-0078
"Examining the Organizational Outcomes and Responses of IT Security Breaches"

Dear Ms. Avery:

Your Initial Review (Response To Modifications) was reviewed and approved by the Expedited review process on February 26, 2018. You may now begin your research

Please note the following information about your approved research protocol:

Protocol Approval Period: February 26, 2018 - February 26, 2019
Approved Subject Enrollment #: 500
Additional Determinations for Research Involving Minors: These determinations have not been made for this study since it has not been approved for enrollment of minors.
Performance Sites: UIC
Sponsor: IGERT Integrative Graduate Education and Research Training
PAF#: Not available
Grant/Contract No: Not available
Grant/Contract Title: Not available
Research Protocol(s):

a) Examining the Organizational Outcomes and Responses of IT Security Breaches; 02/07/2018

Recruitment Material(s):

a) Administrative Approval Material; Version 1.0; 02/27/2018
b) Recruitment Material; Version 3.0; 02/27/2018

Informed Consent(s):

a) Consent and Prescreen; Version 2; 02/07/2018
b) A waiver of documentation of consent has been granted under 45 CFR 46.117 for the online survey; minimal risk; subjects will be provided with an information sheet containing all of the elements of consent.
c) A waiver of documentation of informed consent and alteration of consent have been

granted under 45 CFR 46.117(c)(2) and 45 CFR 46.116(d), respectively, for eligibility screening; minimal risk.

Your research meets the criteria for expedited review as defined in 45 CFR 46.110(b)(1) under the following specific category(ies):

(7) Research on individual or group characteristics or behavior (including but not limited to research on perception, cognition, motivation, identity, language, communication, cultural beliefs or practices and social behavior) or research employing survey, interview, oral history, focus group, program evaluation, human factors evaluation, or quality assurance methodologies.

Please note the Review History of this submission:

Receipt Date	Submission Type	Review Process	Review Date	Review Action
01/19/2018	Initial Review	Expedited	01/24/2018	Modifications Required
02/08/2018	Response To Modifications	Expedited	02/26/2018	Approved

Please remember to:

→ Use your **research protocol number** (2018-0078) on any documents or correspondence with the IRB concerning your research protocol.

→ Review and comply with all requirements on the guidance:
"UIC Investigator Responsibilities, Protection of Human Research Subjects"
(*http://research.uic.edu/irb/investigators-research-staff/investigator-responsibilities*)

Please note that the UIC IRB has the prerogative and authority to ask further questions, seek additional information, require further modifications, or monitor the conduct of your research and the consent process.

Please be aware that if the scope of work in the grant/project changes, the protocol must be amended and approved by the UIC IRB before the initiation of the change.

We wish you the best as you conduct your research. If you have any questions or need further help, please contact OPRS at (312) 996-1711 or me at (312) 996-9299. Please send any correspondence about this protocol to OPRS at 203 AOB, M/C 672.

Sincerely,

Allison A. Brown, PhD
IRB Coordinator, IRB # 2
Office for the Protection of Research
Subjects

Please note that stamped *.pdf files of all approved recruitment and consent documents have been uploaded to OPRSLive, and you must access and use only those approved documents to recruit and enroll subjects into this research project. OPRS/IRB no longer issues paper letters or stamped/approved documents.

Enclosure(s): Uploaded to OPRSLive

1. **UIC Investigator Responsibilities, Protection of Human Research Subjects**
2. **Informed Consent Document(s):**
   a) Consent and Prescreen; Version 2; 02/07/2018
3. **Recruiting Material(s):**
   a) Administrative Approval Material; Version 1.0; 02/27/2018
   b) Recruitment Material; Version 3.0; 02/27/2018

cc: Siddhartha Bhattacharyya, Information and Decision Sciences, M/C 294
Ranganathan Chandrasekaran (Faculty Sponsor), Information and Decision Sciences, M/C 294
OVCR Administration, M/C 672

VITA

NAME: Atiya Avery

EDUCATION: B.B.A., Risk Management and Insurance, Georgia State University, Atlanta, Georgia, 2008

M.S., Managerial Sciences, Georgia State University, Atlanta, Georgia, 2013

TEACHING EXPERIENCE: Department of Information and Decision Sciences, University of Illinois at Chicago, Chicago Illinois, Teaching Assistant, Graduate Audit Control Information Systems, 2016

Department of Information and Decision Sciences, University of Illinois at Chicago, Chicago Illinois, Teaching Assistant, Graduate Information Infrastructure Planning and Security, 2016

Department of Information and Decision Sciences, University of Illinois at Chicago, Chicago Illinois, Instructor, Introduction to Management Information Systems Laboratory, 2015

Department of Information and Decision Sciences, University of Illinois at Chicago, Chicago Illinois, Teaching Assistant, Graduate Supply Chain Management, 2015

Department of Information and Decision Sciences, University of Illinois at Chicago, Chicago Illinois, Teaching Assistant, Graduate Operations Management, 2015

Department of Information and Decision Sciences, University of Illinois at Chicago, Chicago Illinois, Teaching Assistant, Graduate Advanced Database Management, 2014

Department of Information and Decision Sciences, University of Illinois at Chicago, Chicago Illinois, Teaching Assistant, Business Systems Project, 2014

Department of Information and Decision Sciences, University of Illinois at Chicago, Chicago Illinois, Teaching Assistant, Business Statistics II, 2014

Department of Information and Decision Sciences, University of Illinois at Chicago, Chicago Illinois, Instructor, Operations Management Laboratory, 2014

Department of Information and Decision Sciences, University of Illinois at Chicago, Chicago Illinois, Instructor, Operations Management Laboratory, 2013

Department of Information and Decision Sciences, University of Illinois at Chicago, Chicago Illinois, Instructor, Business Model Simulation, 2013

PROFESSIONAL MEMBERSHIPS: Women in Cyberesecurity, PhD Project Information & Decision Sciences Doctoral Student Association, Association for Information Systems

TALKS & ABSTRACTS: Lundquist, D., Avery, A., Ouksel, A., A Survey of Recent Ontological Approaches to Cyber-Security; Paper presented (by J.Pendergrass) at Third Franco-American Workshop on Cybersecurity. Lyon, France, 12/17/2014

Avery, A; Tafti, A; Watson-Manheim, MB. IT Enabled Labor Transformations: Offshoring and Contingent Labor as Antecedents to Automation. Presented at 3rd International Workshop on Changing Nature of Work (CNow 2015). Ft. Worth, Texas, 12/12/2015

Avery, A; Ranganathan ,C.; Financial Performance Impacts of Information Security Breaches. Proceedings of the 11th Annual Workshop on Information Security and Privacy (WISP 2016). Dublin, Ireland, 12/10/2016

Obganufe, O; Avery, A; Breaching News: Does Media Coverage Increase the Effects of Data Breach Event Disclosures on Firm Market Value? Proceedings of the 11th Annual Workshop on Information Security and Privacy (WISP 2016). Dublin, Ireland, 12/10/2016

Avery, A.; Ramaprasad, A. Cybersecurity Scenario Modeling for Business Continuity: An Academic Literature Review.Selected Poster Presentation at Women in Cybersecurity Conference (WiCyS 2017). Tucson, Arizona, 03/31/2017

Avery, A; Ranganathan, C; Why Analytics Governance? A Healthcare Application. TREO Talk presented at the 23rd Annual America's Conference on Information Systems (AMCIS 2017). Boston, Massachusetts, 08/11/2017

Avery, A; Ranganathan, C; Managerial Tactics for Addressing IT Security Breaches: An Exploratory Study. Workshop on Information Security and Privacy (WISP) 2017. Seoul, South Korea; 12/09/2017

PUBLICATIONS:

Obganufe, O; Avery, A; Breaching News: Does Media Coverage Increase the Effects of Data Breach Event Disclosures on Firm Market Value? Proceedings of the 11th Annual Workshop on Information Security and Privacy (WISP 2016) .

Avery, A; Ranganathan ,C.; Financial Performance Impacts of Information Security Breaches. Proceedings of the 11th Annual Workshop on Information Security and Privacy (WISP 2016).

Avery, A; Cheek, K; Analytics Governance: Towards a Definition and Framework. Proceedings of the 21st Annual America's Conference on Information Systems (AMCIS 2015).

Avery, A; Just Do IT! Web 2.0 and the Breaking of the Tacit Dimension for Knowledge Acquisition . Proceedings of the 19th Annual Southern Association of Information Systems Conference (SAIS 2016).

Avery, A; Tafti, A; Watson-Manheim; MB., IT-Enabled Labor Sourcing: A Conceptual Framework and Research Agenda. Proceedings of the 22nd Annual America's Conference on Information Systems (AMCIS 2016).