

ABSTRACT

Title of Document:

**IT IS RISKY BUSINESS: THREE ESSAYS
ON ENSURING RELIABILITY, SECURITY
AND PRIVACY IN TECHNOLOGY-
MEDIATED SETTINGS.**

Catherine Anderson, Doctor of Philosophy, 2010

Directed By:

Professor Ritu Agarwal (Chair), Department of
Decision, Operations and Information
Technologies

Today's interconnected technical environment creates unprecedented opportunities while simultaneously introducing risks. With economic, social and personal interactions increasingly occurring in technology-mediated settings new vulnerabilities are continually being introduced. This dissertation seeks to improve extant understanding of how organizations and individuals respond to such risks and manage the new vulnerability. I develop three essays that variously theorize the antecedents, consequences and implications of the risks imposed by the increased ubiquity of technology. The common thread underlying the studies is that the focal risk is inherently caused by the rapid digitization and dependence on information technology that has permeated economic and social activity.

Essay 1 addresses the increasing dependence of organizations on the reliability of their information technology (IT) infrastructure. I draw on organizational reliability literature to classify IT infrastructure failures and theorize how collective mindfulness can change the way organizations respond to each type of failure. The results support

the necessity of examining collective mindfulness at the level of its processes (versus using the omnibus measure) and provide insights into the contingent value of collective mindfulness. I find that mindfulness processes are heterogeneously efficacious for an organization's response to failure depending on the failure type.

Essay 2 synthesizes research from information systems, communication, and psychology to form a conceptual model explicating the role played by type of information requested (general health, mental health, genetic), the purpose for which it is to be used (patient care, research, marketing) and the requesting stakeholder (doctors/hospitals, the government, pharmaceutical companies) in an individual's willingness to disclose personal health information. Further, the model incorporates the impact of emotion linked to one's health condition on willingness to disclose. Results show that emotion plays a significant role in the disclosure decision and suggest that contextual factors related to the requesting stakeholder and the intended purpose of use moderate the relationships between concern and trust on willingness to disclose personal health information.

Essay 3 explores ways to minimize the perception that one is invulnerable to a security violation through an examination of the influence of message cues on computer user security-related optimistic bias and security behavior intentions. I conduct two experiments to understand conditions that minimize the perception that one is invulnerable to a security violation and increase related intentions. Results from experiment 1 confirm an interactive influence of self-view and risk domain frame (social or financial) on security-related intentions. Experiment 2 suggests an interactive relationship between self-view and goal frame on optimistic bias but that influence did not translate into similar changes to intentions.

IT IS RISKY BUSINESS: THREE ESSAYS ON ENSURING RELIABILITY,
SECURITY AND PRIVACY IN TECHNOLOGY-MEDIATED SETTINGS

By

Catherine L. Anderson

Dissertation submitted to the Faculty of the Graduate School of the
University of Maryland, College Park, in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
2010

Advisory Committee:
Professor Ritu Agarwal, Chair
Professor Hank Lucas
Professor Joydeep Srivastava
Assistant Professor Anand Gopal
Assistant Professor Sunil Mithas
Dean Robert Gold
Dr. Judith Shinogle

© Copyright by
Catherine L. Anderson
2009

ACKNOWLEDGEMENTS

This dissertation is the culmination of several years of work and the investment of much energy and emotion. I feel quite fortunate to have finally reached this stage in the academic process. One thing is certain, I could not have reached this point without many people who have helped me both directly and indirectly toward the goal of earning my PhD. I would like to take this opportunity to thank those individuals who helped me in this endeavor.

First, I want to thank my dissertation advisor, Professor Ritu Agarwal, for her invaluable guidance and insight throughout the process. I am grateful to her for helping me set intermediate deadlines and for providing me with the tools to meet them.

I must also thank my committee members for their patience during this process and for their feedback and suggestions which resulted in significant improvements to this dissertation: Professor Hank Lucas, Professor Joydeep Srivastava, Assistant Professor Anand Gopal, Assistant Professor Sunil Mithas, Dean Robert Gold and Dr. Judith Shinogle.

I also want to thank Dr. George Westerman for helping me gain access to the organization that served as my data collection site for my first essay. I also appreciated his ability to challenge me to think about a research question from many different angles.

I must thank Professor Barbara Haley Wixom for encouraging me to apply to the doctoral program. She has been my advocate all along the way, cheering me on from afar.

On a more personal note, there are so many friends, neighbors and family members who supported me in my efforts toward the degree and without whom it would

not have been possible for me to complete the rigors of the program. At various times, family and friends helped distribute surveys, proofread papers, served as sounding boards, carted my boys to baseball games, and countless other tasks which helped tremendously. There are too many people to name individually here, but a few simply must be specifically acknowledged. To Linda Whitaker, my dear friend, thank for listening to me and for your endless offers to help in whatever way possible.

Thanks to all the au pairs I have had since I started the PhD program, including Cynthia Coelho, Annika Boehmer, Hannah Kindermann, Annemarie Koenig, and Priscila Oliveira, for taking such good care of the children so that I could focus on research and coursework.

Although my first husband is not alive to witness this achievement because he succumbed to cancer and died before I actually started the program, he was very supportive of me during the application process and encouraged me to enter the program. My pursuit of a PhD was going to be a sacrifice for him in my lost income during the program and in increased demands on my time, but he was willing to make that sacrifice so that I could realize my dreams. I want to thank him here because I hope that, wherever he is now, he knows I am eternally grateful.

By some miracle, I was fortunate enough to meet a wonderfully supportive man in 2007 and am once again happily married. My husband, Ron Minor, must be thanked for being so understanding when I had to cancel plans to meet deadlines early in our courtship days. More recently, he has watched the kids in the evenings and weekends, cooked dinner, and done whatever he could to help me to focus my energies on completing my research.

Finally, I must thank my parents, sister and brother for their seemingly endless encouragement. I am grateful to all of you for making me feel that you are proud of me no matter what. My parents were always willing to change their plans to come and help with the children so I could work evenings and weekends to complete course assignments or papers. They also stayed with the children so that I could attend conferences. Myrna Anderson was also very helpful in volunteering her time to watch the children for me.

Last, but not least, I cannot forget to thank my children. All 7 of them! But, particularly to Chris, Connor and Scott who have had to see me less than they might otherwise have these past 5 years. Thanks for trying to read my papers aloud and stumbling on the big words!

TABLE OF CONTENTS

ACKNOWLEDGEMENTS	ii
TABLE OF CONTENTS.....	v
LIST OF FIGURES	vii
LIST OF TABLES	viii
CHAPTER 1: OVERVIEW	1
1.1 TECHNOLOGY DEPENDENCE	2
1.1.1 IT Usage Trends.....	2
1.1.2 Public Policy Implications	5
1.2 OBJECTIVE OF THE DISSERTATION.....	7
CHAPTER 2: IT IS RISKY BUSINESS: AN EXAMINATION OF THE INTERACTIONS BETWEEN FAILURE CHARACTERISTICS AND THE PROCESSES OF COLLECTIVE MINDFULNESS.....	11
2.1 INTRODUCTION	12
2.2 THEORETICAL BACKGROUND.....	17
2.2.1 Sources of Failure	18
2.2.2 Addressing Failures with Collective Mindfulness.....	21
2.3 DIMENSIONALITY OF COLLECTIVE MINDFULNESS	28
2.4 CONCEPTUAL MODEL AND HYPOTHESES.....	30
2.5 METHODS	40
2.5.1 Research Site and Data Collection.....	40
2.5.2 Operationalization of Variables	44
2.6 RESULTS	47
2.6.1 Scale Development	47
2.6.2 Pilot Study.....	47
2.6.3 Full Launch Results	48
2.7 LIMITATIONS.....	55
2.8 DISCUSSION AND CONCLUSION	56
2.8.1 Theoretical Implications	61
2.8.2 Practical Implications.....	62
CHAPTER 3: THE DIGITIZATION OF HEALTHCARE: BOUNDARY RISKS, EMOTION, AND CONSUMER WILLINGNESS TO DISCLOSE PERSONAL HEALTH INFORMATION.....	64
3.1 INTRODUCTION	65
3.2 THEORETICAL BACKGROUND.....	70
3.2.1 Privacy Calculus	70
3.2.2 Boundary Management.....	73
3.2.3 Emotion.....	76
3.3 CONCEPTUAL MODEL.....	78
3.4 METHODS	91
3.4.1 Sample and Data Collection.....	91
3.4.2 Operationalization of Variables	93

3.5 RESULTS	94
3.5.1 Boundary/Contextual Considerations	96
3.5.2 Emotion.....	100
3.5.3 Discussion.....	102
3.6 LIMITATIONS.....	103
3.7 IMPLICATIONS AND CONCLUSION.....	107
3.7.1 Theoretical Implications	107
3.7.2 Practical Implications.....	110
3.7.3 Conclusion	111
CHAPTER 4: THE INFLUENCE OF MESSAGE CUES ON COMPUTER USER SECURITY-RELATED OPTIMISTIC BIAS AND INTENTIONS	113
4.1 INTRODUCTION	114
4.2 THEORETICAL BACKGROUND.....	119
4.2.1 The Influence of Self-View on Optimistic Bias	120
4.2.2 The Influence of Message Framing on Optimistic Bias	121
4.3 STUDY 1 – SELF-VIEW AND RISK DOMAIN FRAME	123
4.3.1 Method	127
4.3.2 Analysis.....	131
4.4 STUDY 2 – SELF-VIEW AND GOAL FRAME.....	136
4.4.1 Method	138
4.4.2 Analysis.....	141
4.5 LIMITATIONS.....	144
4.6 DISCUSSION AND CONCLUSION	145
CHAPTER 5: EPILOGUE.....	149
FIGURES.....	154
TABLES	160
APPENDIX A – FAILURE EXAMPLE	171
APPENDIX B – MEASURES AND ITEMS	173
APPENDIX C – SORT RESULTS.....	175
APPENDIX D – FACTOR ANALYSIS	178
APPENDIX E – ESSAY 2 MEASUREMENT ITEMS	179
APPENDIX F – INSTRUMENT USED FOR DATA COLLECTION	182
APPENDIX G – PRINCIPAL COMPONENT ANALYSIS	191
APPENDIX H – STUDY MANIPULATIONS.....	192
APPENDIX I – ESSAY 3, STUDY 1 MEASURES	197
APPENDIX J – ESSAY 3, STUDY 1 FACTOR ANALYSIS.....	199
APPENDIX K – ESSAY 3, STUDY 2 MEASURES	200
APPENDIX L – ESSAY 3, STUDY 2 FACTOR ANALYSIS.....	202
REFERENCES	203

LIST OF FIGURES

FIGURE 2.1 FAILURE MODEL.....	154
FIGURE 2.2 FAILURE MODEL RESULTS.....	154
FIGURE 2.3 INTERACTION GRAPHS FOR DURATION.....	155
FIGURE 3.1 CONCEPTUAL MODEL – HEALTH INFORMATION PRIVACY CALCULUS.....	156
FIGURE 3.2 PURPOSE INTERACTION GRAPHS.....	157
FIGURE 3.3 STAKEHOLDER INTERACTION GRAPHS.....	157
FIGURE 4.1 OPTIMISTIC BIAS GRAPHS.....	158
FIGURE 4.2 INFLUENCE OF MESSAGE CUES ON INTENTIONS.....	158
FIGURE 4.3 OPTIMISTIC BIAS GRAPH (STUDY 1)	159

LIST OF TABLES

TABLE 2.1 SUMMARY OF EMPIRICAL CM RESEARCH	160
TABLE 2.2 INDUSTRY BREAKDOWN OF INCIDENTS.....	162
TABLE 2.3 DESCRIPTIVE STATISTICS.....	163
TABLE 2.4 CM REGRESSION RESULTS	164
TABLE 2.5 CM PROCESS REGRESSION RESULTS.....	165
TABLE 2.6 STUDY RESULTS BY HYPOTHESIS.....	166
TABLE 3.1 DEMOGRAPHICS FOR SAMPLE	167
TABLE 3.2 DESCRIPTIVE STATISTICS	168
TABLE 3.3 RM ANCOVA TABLE FOR WILLINGNESS TO PROVIDE ACCESS TO PHI.....	169
TABLE 4.1 STUDY 1 TABLE OF RISK ESTIMATE MEANS	170
TABLE 4.2 STUDY 2 TABLE OF RISK ESTIMATE MEANS	170

CHAPTER 1: OVERVIEW

In April 2004, a major Customer Relationship Management system crash during an upgrade at AT&T made it impossible for representatives to set up or access new accounts. The problems persisted for several months costing an estimated \$100 million in lost revenue. (Koch 2004).

[Electronic] personal health records contain our most intimate details: information that could affect landing a job, obtaining insurance and even one's social life... the very existence of a detailed health dossier accessible in an instant can make control difficult. (Levy 2008)

In the first 6 months of 2007, home users were the most highly targeted sector by hackers according to a leading security software and services vendor (Turner 2007)

One of the most striking developments of the 21st century, precipitated in part by transition of the Internet from a defense and research network to a global platform for economic and social transactions, is the extent to which information technology (IT) artifacts and the capabilities they offer have become an integral part of everyday lives. Today's interconnected technical environment creates unprecedented opportunities for IT enabled transformations while simultaneously introducing risks of a kind that were previously not envisioned (Cyberspace Policy Review 2009; Westerman and Hunter 2007, p. 1). As the introductory vignettes illustrate, the risks faced by individuals and organizations are multidimensional: with economic, social and personal interactions increasingly occurring in technology-mediated settings, new vulnerabilities are continually being introduced. Reliance on technology has become a key external factor affecting risk and is increasingly important to consider during risk management activities (Clemmons 2008). The broad objective of this dissertation is to improve understanding of how organizations and individuals respond to such risks and manage the new vulnerability. The two sets of actors --

individuals and organizations -- are inextricably linked both in the consequences they experience and in the management of risk because the activities of each affect the other.

The dissertation comprises three distinct studies, each focused on a different type of vulnerability, that theorize the antecedents, consequences and implications of the risks imposed by the increased ubiquity of technology for individuals and organizations. A unifying theme across the studies is that the focal risk is inherently caused by the rapid digitization and dependence on information technology that has permeated all facets of economic and social activity. In this chapter, I provide a brief overview of key trends in technology usage, including the increased interaction between individuals and organizations, summarize recent and highly relevant policy initiatives, and conclude with objectives of the dissertation.

1.1 TECHNOLOGY DEPENDENCE

1.1.1 IT Usage Trends

It is patently evident that information technology has enabled significant transformations such as changes in how we stay connected with others (e.g., social networking sites, text messages), how customer service is provided (e.g., consumers making their own airline reservations and scheduling their own doctor appointments online), and how organizations are structured (e.g., increased outsourcing due to the ease of coordinating across organizational boundaries) (Lucas and Grover 2008). Many technology transformations are becoming widely adopted by both organizations and individuals (Dong et al. 2009; IBISWorld 2009; Lucas et al. 2007; Pew Internet Research 2009).

Consider the transformations in personal and social lives wrought by IT. The number of households in the U.S. with personal computers continues to rise (DeMaria 2002; Day et al. 2003). Reports from recent studies indicate that the number of individuals using the Internet has risen to seventy-nine percent (Pew Internet Research 2009). Approximately sixty-five percent of individuals use email compared to less than fifty percent in 2000. Not only are these individuals using the Internet for personal communication needs, but they are also using the Internet to interact with organizations. Approximately, fifty-five percent of people surveyed this year indicated that they use the Internet to buy a product, compared to less than thirty percent in 2000. Forty-five percent visit government websites to transact official business today as compared to under thirty percent in 2000. Forty percent have looked for a job online up from twenty percent in 2000 and forty percent bank online up from ten percent in 2000 (Pew Internet Research 2009). These statistics suggest that individuals are increasing their use of technology, including using it to engage in more online interactions with organizations.

Organizations are also increasingly becoming more dependent on IT for the conduct of their work. For example, they are increasingly making use of web 2.0 capabilities such as social networking and blogs (Hewlett et al. 2009) to connect employees and generate organizational knowledge. Recent studies indicate that corporate investment in IT continues to grow (Economist 2009; McDonald 2008; Mithas et al. 2009). Despite the current economic crisis, statistics show that corporate spending on IT grew in 2008 by approximately 4 percent (Lohr 2008). Organizations are relying more on packaged software (Harris-Ferrante 2009; Lucas et al. 2007) and

depending on external service providers (ESPs) for technical support at an increasing rate. Maintenance fees paid by organizations to external service providers in 2005 accounted for 41% of the \$210 billion in revenue collected by software vendors (Whiting 2006). That figure is expected to grow by 9.6% to \$127 billion in 2010 (Whiting 2006). In large organizations (500 employees or more), approximately half of all support is provided by external sources (Igou 2007). Among the failures encountered by organizations, over one third is handled by external service providers (Igou 2007). In addition, organizations are demanding 24/7 availability of critical systems (Rivers 1999), in part because customers demand availability. The new functionality and increased availability is required of highly complex, interrelated hardware and software components (Goldberg 2005; Vechio 2001; Wing 2008) and a combination of “legacy”, or older, devices and firmware in addition to “leading edge” technology (Vechio 2001). These statistics suggest that organizations continue to expand their use of IT while simultaneously placing a premium on maintenance of their systems to ensure availability.

The expanding use of technology has created a tight coupling and linkage between organizations and individuals. For example, in the first vignette above, while AT&T experienced a financial loss due to their system outage during an upgrade, individual consumers encountered inconvenience as a result of the outage when representatives were unable to access their existing accounts or create new ones. The second vignette relates to electronic medical records which could benefit both organizations such as hospitals and insurance providers with improved efficiency (e.g. Lohr 2006, Miller et al. 2005), and patients with fewer medical errors

(Institute of Medicine 2000) but must be embraced by individuals who desire a level of confidence in the privacy afforded their information (Walker 2008). The final vignette suggests that individual home users are more likely to be targeted by hackers (Turner 2007). These computers are then used to launch denial of service attacks against company websites (Turner 2007). Thus, the security behavior of individuals can influence organizations. These are just a few examples of the ways in which the behavior of organizations and individuals can influence one another.

While there are doubtless multiple types of value that IT creates, it has been suggested that the increased use of IT can lead to a number of negative outcomes that need to be proactively managed. These include addiction (Byun et al. 2009; Huang et al. 2009), information overload (Wisniewski and Lu 2009), high IT failure costs (Pisello and Quirk 2004; Garg 2003), virus proliferation (Turner 2007), and privacy breaches including identity theft (Krebs 2009; New York Times 2008), to name just a few. An improved understanding of the different aspects of each type of risk and how the relevant party involved responds, can inform theory and practice on the “downside” of widespread technology use, and enhance our ability to mitigate risk and fully leverage the benefits of technology.

1.1.2 Public Policy Implications

*“..with the broad reach of a loose and lightly regulated digital infrastructure, great risks threaten nations, private enterprises, and individual rights.”
(Cyberspace Policy Review 2009)*

It is said that with the election of Barrack Obama as president of the United States, the country now has a “tech savvy” president. The President’s interest in technology is evident in a number of the administration’s key initiatives. The

American Recovery and Reinvestment Act (ARRA), which was signed into law in February 2009, provides for the modernization of healthcare through computerized health records and the investment in clean energy technologies (ARRA 2009). Nineteen billion dollars has been allocated to computerize medical records to reduce costs and improve healthcare quality while ensuring patient privacy (ARRA 2009). These objectives must be balanced and informed by rigorous research (Meingast et al. 2006).

The Act also makes significant funds available for research related in the sciences and technology. For example, ARRA (2009) makes funds available to increase broadband access to rural areas of the U.S. which translates to more people using the Internet. As more people and organizations use the Internet, securing the cyber infrastructure increases in importance. Acknowledging this need, the Obama administration has made cyber security a national priority by establishing a new White House office to integrate policies and coordinate responses for the government (Cyberspace 2009; Krebs 2009). Collectively, these policies signify the commitment of the White House to leverage technology for the benefit of U.S. citizens. The environment is ripe for academic research to understand the risks which might be associated with increased technology dependence.

The new administration's efforts build on prior initiatives established by the government after the attacks of September 11, 2001. The terrorist attack highlighted the vulnerability of the U.S. infrastructure. Consequently, the United States government established the Department of Homeland Security and launched a number of initiatives aimed at improving the stability of the nation's critical

infrastructure (NSHS 2007; NSSC 2003; Rhodes and Willemssen 2004). Critical infrastructure activities include the ability to transport food, administer healthcare and emergency services, provide clean water and electricity, and conduct banking and financial transactions all of which increasingly depend on information technology for their operations (Rhodes and Willemssen 2004). Many of these networks are connected to the Internet which is vulnerable to attack (e.g. Rhodes and Willemssen 2004; Turner 2007). These initiatives have focused on reducing vulnerabilities, improving response to threats, increasing awareness of and training in security resources for protecting cyberspace, and expanding research on security technology (NSSC 2003; Rhodes and Willemssen 2004). More recent reports note that in the rush to create barriers to intrusion, relatively less emphasis has been placed on balancing the need for privacy. Thus, additional research aimed at balancing privacy concerns when implementing cybersecurity technologies is being encouraged (Cyberspace 2009; Meingast et al. 2006; Rhodes and Willemssen 2004).

These recent initiatives aim to increase technology use for the benefit of the public good (e.g. broadband access to rural areas, improved quality of healthcare through computerization), but they also acknowledge the need to protect citizens from any unintended outcomes which may result. Consistent with the objectives of these initiatives, the three studies comprising this dissertation represent an effort toward understanding how to improve response to our increased dependence on technology.

1.2 OBJECTIVE OF THE DISSERTATION

Much of the research on IT transformations in the information systems academic discipline has focused on how transformations translate into such positive outcomes

as innovation (e.g. Swanson 1994; Swanson and Ramiller 2004; Zhu et al. 2006) and business value (e.g. Hitt and Brynjolfsson 1996; Melville et al. 2004; Mishra et al. 2007; Dong et al. 2009;). In contrast, there have been few academic studies focused on the potentially negative outcomes of IT transformations. Exceptions include work related to understanding hacker attack patterns (Ransbotham and Mitra 2009), privacy concerns in online contexts (e.g. Dinev and Hart 2006; Malhotra et al. 2004), and understanding the complexities associated with distributed work (e.g. Kanawattanachai and Yoo 2007). This dissertation contributes to the latter stream of research by examining risks associated with increased technology use by organizations and individuals. Since the IT landscape has changed from one in which many implementations failed to one in which system solutions are highly successful (Lucas et al. 2007), we need to understand the potential costs associated with this success and move toward understanding how to deal with them effectively.

In the first essay, I address the increasing dependence of organizations on the reliability of their information technology (IT) infrastructure¹. The financial implications associated with IT infrastructure downtime can approach a cost of \$1 million per hour for some companies (Pisello and Quirk 2004; Garg 2003); such losses can be devastating. I refer to this as *reliability risk*. Building on and extending theory from the organizational sciences and information systems discipline, the study examines how failure characteristics such as novelty and lack of routine interact with the organization's level of collective mindfulness to influence the organization's

¹ This study was supported by a Dissertation Grant from the Decision, Risk and Management Sciences Program of the National Science Foundation

failure response performance. I conduct a field study and gather survey data on 153 failures experienced by the customers of a large software and services provider. The essay's objectives are compatible with the recent policy objective of improving response to threats through understanding how organizations react differently to IT infrastructure failures. This understanding may help organizations minimize downtime.

The next two studies are focused on the individual level of analysis and in each I examine a distinct area of risk. First, as more of an individual's health information becomes digitized, privacy concerns are heightened due to the sensitive, personal nature of this data and its potential misuse. I refer to this as *privacy risk*. In this study I incorporate consideration for emotions in the cognitive cost-benefit analysis consumers perform when deciding whether or not to disclose personal health information. I also examine the influence of contextual variables, such as the requesting stakeholder and type of information requested, on willingness to disclose personal health information. I test the theory with data from 1,089 respondents from a nationally representative sample using a quasi-experimental, scenario-based survey methodology. This study addresses the recent policy objective of balancing an individual's privacy needs with the benefits of digitization for the particularly sensitive domain of personal health information.

Second, individual online security behavior has the potential to impact not only the individual, but also other users of the Internet by enabling such malicious activity as the spread of viruses. I refer to this as *security risk*. In this study, I examine the influence of message cues on computer user optimistic bias and security

intentions. I utilize an experimental methodology to test my hypotheses. In study 1, I examine the interactive influence of self-view and risk domain frame (stressing either social or financial risks) on the optimistic bias and intentions. In study 2, I examine the interactive influence of self-view and goal frame (positive or negative) on the key dependent variables. This study addresses the recent policy objectives related to increasing awareness of the cyber security issue; it examines ways to increase the security intentions of computer users via persuasive message appeals. The three distinct phenomena examined in this dissertation are approached using alternative research methodologies and theoretical lenses.

In summary, recent discourse in the trade press and activity at the strategic policy level (ARRA 2009; Cyberspace 2009; Koch 2004; Levy 2008; NSSC 2003; Rhodes and Willemssen 2004; Turner 2007) suggest that our dependence on technology has created challenges and opportunities of a critical nature for continued prosperity of both organizations and individuals. There exists a need for rigorous analyses that can inform individuals, managers, and policy makers about appropriate steps and processes for risk minimization. This dissertation represents an attempt to inform both practice and theory on a path toward embracing a world in which the benefits of technology can be exploited without taking advantage of or unduly putting its human benefactors at risk.

The rest of this document is structured as follows. Chapter Two, Three, and Four present the three studies comprising this dissertation. In Chapter Five, I briefly summarize the contributions and implications of the findings and discuss potential avenues for future research.

CHAPTER 2: IT IS RISKY BUSINESS: AN EXAMINATION OF THE INTERACTIONS BETWEEN FAILURE CHARACTERISTICS AND THE PROCESSES OF COLLECTIVE MINDFULNESS

ABSTRACT

With business processes becoming increasingly dependent on IT, availability of critical information systems is now an essential aspect of organizational reliability. We develop a theoretical model to examine the moderating influences of specific collective mindfulness processes on the relationship between failure characteristics and the duration of an organization's response to the failure. A core aspect of our theory is a characterization of failures distinguished along two dimensions: the failure novelty (novel/previously encountered) and lack of routine (i.e. extent of predefined routine). We argue that different dimensions of collective mindfulness grouped together as mindful containment and mindful anticipation processes are required to effectively respond to failures depending on the failure's characteristics. Using survey data on 153 infrastructure failures across a broad range of organizations, we find that examining the processes of mindfulness as a related set explains more variance in failure response performance than the omnibus measure of collective mindfulness. In addition, the processes of mindfulness that improve or impede organizational response to failure varies depending on the failure characteristics. Mindful containment is more useful in reducing the time required to solve problems that occur associated with a lack of routine while mindful anticipation increases the time

required to solve the same type of problems. In addition, high levels of mindful containment increased the time required to solve novel problems.

2.1 INTRODUCTION

In February 2008, Blackberry users experienced the second outage in their wireless email service in less than a year, raising concerns about the reliability of the service many now consider critical. Research in Motion, Blackberry's maker, attributes the recent problems to difficulties encountered after installing new "non-critical" software. Problems associated with switching to a backup system also exacerbated the issue. These outages could hurt the company's long term credibility and sales. (Sorensen and Wong 2008)

With enterprises becoming increasingly dependent on information technology (IT) platforms for managing and executing a wide variety of business processes, 24/7 availability of mission critical information systems is now an essential aspect of business continuity. The need for uninterrupted availability implies that systems are "up" for extended periods of time – thus, the increased dependence simultaneously amplifies vulnerability and threats to reliability. Indeed, it is widely acknowledged that today's organizations are highly susceptible to failures in their IT infrastructure (Govekar 2007; Pultz et al. 2002). We define the IT infrastructure to include platform technologies (hardware and software), network and telecommunications software, databases and a variety of shared services such as email and Internet browsers (Armstrong and Sambamurthy 1999); in essence, the foundation on which the organization runs its information systems applications. As the introductory vignette illustrates, IT infrastructure failure can be devastating to organizations. The financial implications of unreliable systems are significant: downtime costs can approach \$1 million per hour (Garg 2003; Pisello and Quirk 2004). With such a high price tag, it

is not surprising that managing the risks of information systems infrastructure failure is a top management priority (Clemmons 2008; Luftman and Kempaiah 2007).

Our work is motivated by the mounting importance of reliability in IT infrastructures. In spite of the significant economic and reputational losses that firms incur as a result of infrastructure failures, limited research has focused on how such failures can be more effectively addressed. Traditionally, the approach to systems development and maintenance has been routine-based (e.g., Butler and Gray 2006; Dennis and Wixom 2003; Zuboff 1988). While a routine-based approach was arguably highly appropriate when information systems' primary strategic roles were to automate business processes and provide information (Schein 1992; Zuboff 1988), the shift in the role of IT to one that involves transforming and integrating core business functions while simultaneously responding to frequent disruptive technical innovations likely requires an altered approach (Lyytinen and Rose 2003; Swanson 1994).

Butler and Gray (2006) suggested that while routines are a necessary element of ensuring IS reliability, a solely routine-based approach is no longer sufficient. They proposed that collective mindfulness, the ability to be alert to changes in the system combined with a heightened sensitivity to context, is also necessary (Butler and Gray 2006; Weick and Sutcliffe 2007). In contrast to routine-based approaches which tend to improve efficiency in stable environments, collective mindfulness is considered essential to maintaining reliability in the presence of uncertainty (Weick and Sutcliffe 2007). Collective mindfulness is conceptualized as a multi-dimensional construct consisting of 5 subdimensions (deference to expertise, commitment to

resilience, reluctance to simplify, preoccupation with failure and attention to operations) which have been grouped into the processes of mindful containment and mindful anticipation. A majority of organizational literature on collective mindfulness and reliability is based either on anecdotal evidence of catastrophic failures, or on observations of exemplar firms in settings posing high-risks to human life (e.g. Bigley & Roberts 2001; Perrow 1984; Weick and Sutcliffe 1993; Weick and Sutcliffe 2001). The limited existing quantitative research on reliability focuses on work group level outcomes such as perceived safety in swimming pools (Knight 2004) or total medication errors for a nursing unit (Vogus and Sutcliffe 2007a/2007b). Although this prior research provides valuable initial insight into the factors that may contribute to reliability in less extreme contexts at the individual event level, more research is necessary to isolate the mechanisms that enable reliability when dealing with a single failure in settings that do not pose a risk to human life but are, nonetheless, consequential.

In this paper we develop and empirically test a theoretical model that elaborates the situational contingencies underlying the importance of collective mindfulness in response to individual failures. Our qualitative analysis conducted with a leading software and services vendor, given the pseudonym ProtectCo, found the source of problems to range from customer human error, hardware failure, software problems with other vendor's products, process breakdowns, resource constraints and vendor software bugs. Our analysis further suggested that failures can be characterized along two dimensions: the failure novelty for the organization (novel or previously encountered) and lack of routine (i.e. the extent to which a

routine had been defined for the activities preceding the failure). We argue that the type of failure necessitates varying levels of specific collective mindfulness processes to limit the duration of failure response. The vast majority of past empirical CM research has been conducted with the omnibus measure and/or with work group level outcomes (Knight 2004; Mu 2007; Pavlou and El Sawy 2006; Vogus and Sutcliffe 2007a/2007b). It has also implied that higher levels of CM are desired to improve reliability (Weick and Sutcliffe 2007; Woods 2006). We argue that to understand the factors influencing how quickly an organization responds to a failure, we must consider the nuances embodied in each mindful process (i.e. containment and anticipation). For example, deference to expertise, which is part of mindful containment, may yield more value when the failure occurs in a context within which the organization has routines defined. In that case, an organization with high deference to expertise knows who is familiar with the routine and its use and can migrate decisions according to that awareness instead of hierarchical structure. As opposed to a situation in which they do not possess the skills and experience to solve the problem and might involve too many individuals without the appropriate expertise to solve the problem². We pose two research questions to examine the influence of concepts from the routine and collective mindfulness literatures on the duration of the organization's response to failures:

1. Do the dimensions of collective mindfulness (as grouped into mindful processes) explain the variance in the duration of an organization's response to individual failure better than the omnibus measure of collective mindfulness? Relatedly, does an examination of the mindful

² For a more complete example drawn from our qualitative study, see Appendix A.

processes yield more insight into the underlying relationships between collective mindfulness and the duration of the organizational response?

2. Are there mindful processes that are more or less important for solving problems related to failure type (as characterized by lack of routine and the novelty of the failure for the organization)?

We empirically test the proposed model with data collected from a field study of 153 infrastructure failures encountered by the customers of a large software and services vendor. Conducting our study in this setting enables the examination of an increasingly prevalent inter-organizational setting in which organizations pay for support of vendor-provided software. Maintenance fees paid by organizations to external service providers in 2005 accounted for 41% of the \$210 billion in revenue collected by software vendors (Whiting 2006). That figure is expected to grow by 9.6% to \$127 billion in 2010 (Whiting 2006). Most organizations choose to pay maintenance fees to take advantage of future upgrades to the software which represent vendor investments in the product and technical support for any problems which may arise. Approximately half of all support is provided by external sources in organizations consisting of 500 employees or more (Igou 2007). On average, over one third of all support incidents encountered by organizations are handled by external service providers (Igou 2007) making our context salient to many organizations. Our context improves the study's relevance and timeliness.

This study contributes to the organizational sciences and information systems literature in two ways. First, we explore the best way to model collective mindfulness (as two related processes or as an omnibus measure) to yield the highest explained variance and insight into the relationships underlying the duration of an organization's response to failure. Second, we characterize different failure types and

reason about how and why collective mindfulness is differentially important in different circumstances. This can provide a foundation for future inquiry into developing more nuanced failure typologies. Our empirical analysis enables the assessment of the relative importance of failure novelty, and routine and mindful behavior on failure outcomes. In addition to the theoretical implications of our work, there are practical implications for organizations. Currently, managers have limited information available to make informed decisions regarding hiring, training, vendor alliances, structure/ governance and culture/ climate all of which have financial implications and unquantified risks associated with them. To the extent that developing collective mindfulness (CM) within organizations entails significant cost (Swanson and Ramiller 2004; Vogus and Wellbourne 2003), understanding when collective mindfulness is likely to yield maximal benefit is important for efficient resource allocation. Our findings can potentially support decision making in these areas.

The paper proceeds as follows. We begin by briefly describing the relevant literature and characterizing different types of failure. We then present our conceptual model and hypotheses, followed by the research methodology and results. Finally, we conclude by acknowledging the study's limitations, discussing the findings and providing directions for future research.

2.2 THEORETICAL BACKGROUND

The theoretical foundation for this study is grounded in several streams of research. While our qualitative research informed the failure characteristics we examine in this study, the failure characteristics are consistent with the rich literature

on routines as well as normal accident theory (NAT) (Perrow 1984). We first briefly describe this literature which informed our characterization of failures. Next, we summarize collective mindfulness research and its influence on reliability. We argue that the influence of collective mindfulness on the organization's response to the failure depends on the type of failure the organization encounters and, therefore, contingency theory is relevant as well.

2.2.1 Sources of Failure

Failures have been identified as inevitable in any type of complex system (Bertalanffy 1968), and to the degree that organizations in general and IT infrastructures in particular are instantiations of highly complex systems, they are also highly prone to failure. Routines have been identified as a means of improving reliability (Cyert and March 1963; Miner 2002). In this study, we adopt the widely held definition of routine as “a repetitive, recognizable pattern of interdependent actions, involving multiple actors” (Feldman and Pentland 2003: 95). Ironically, while routines are ideally suited for well-defined circumstances, they can fail the organization even in such situations, as explained below. Moreover, organizations will always be faced with the unexpected (Perrow 1984), in which case routines are even less helpful.

While organizational routines can be a source of efficiency and a means of avoiding uncertainty, they also affect the perceptions, the range of alternatives considered and the goals and expectations of organizational actors (Cyert and March 1963; Miner 2002). Thus, the existence and use of routines can yield both positive and negative outcomes. For example, it is desirable for members of an organization

to have a repertoire of routines upon which to draw when responding to an event because it can save time and effort. However, if an employee becomes so accustomed to performing a routine repeatedly, he or she may fail to recognize a warning sign simply because he or she does not expect it to occur.

The potential for both advantages and disadvantages to routines is more easily understood when routines are conceived of as social phenomena embodying a duality of structure and agency (Giddens 1984). Feldman and Pentland (2003) distinguish between the ostensive or structural component of a routine which consists of the underlying abstract idea, and the performative aspect of the routine which consists of the enactment of the routine by individuals at a specific point in time and space. This distinction incorporates the necessary component of agency in the conceptualization of routines and helps explain the variation and subjectivity inherent in the application of routines in organizational life (Feldman and Pentland 2003).

Do routines represent an “iron cage” that tightly circumscribes human behavior? The answer to this question is equivocal. The fact that habituated action perpetuated by the existence of routines may result in an unquestioning attitude to approaches for failure resolution has been acknowledged by prior work. For instance, it has been suggested that routines can lead to inertia (Gilbert 2005) or decreased creativity (Langer and Piper 1987) because they color perception (Langer 1989) and result in inappropriate responses (Clarke 1999). In contrast, other research has found evidence that routines can be flexible and adaptable (Edmondson et al. 2001; Howard-Grenville 2005; Zellmer-Bruhn 2003). As organizations learn, modifications to existing routines are made and new routines created (Zellmer-Bruhn 2003). Events

such as encountering novelty, experiencing a failure, changes in authority or structure, and reaching a significant milestone can all contribute to the creation of new routines (Zellmer-Bruhn 2003). It is incumbent on the organization, however, to recognize a repetitive action and invest the time in creating routine.

Failures with routine parallel their dual nature and can occur either with the ostensive portion of the routine or the performative portion. If the abstract idea or structure of the routine itself is incorrect or the organization has not invested the time to create a formal routine, that would be a failure in the ostensive portion. If an individual skips a step in a well-known routine because she is in a hurry or is simply not paying close attention, that is an instance of a failure in the performative aspect of the routine.

In addition to failures that may arise in spite of or as a result of routine, organizations should expect to have an occasional problem arise with any system that is as complex and highly coupled as their information technology infrastructure (Perrow 1984). Normal accident theory (NAT) suggests that no matter what safeguards and processes are put in place, it is inevitable that failures will occur, even if infrequently.

Building upon the core idea that the source and characteristics of failure may differ, and integrating the two themes in the literature discussed above, we classify IT infrastructure failures along two dimensions: the novelty of the failure and the extent of routine involved (i.e. lack of routine). Failure novelty is characterized by the dichotomy between novel and previously encountered. Novel failures involve a context with which the organization has little experience. In contrast, previously

encountered problems are failures that occur during the course of conducting common activities with which the organization should be familiar. In this paper, we focus on characterizing failure by the extent to which a routine was defined or not, which represent failures in the ostensive portion of routine. If a routine has not been defined, it may be because the organization has not recognized the need for a routine either because they are not paying sufficient attention, do not want or feel the need to make the investment in routine, or because events have not occurred with sufficient frequency to warrant the creation of a routine (Howard-Grenville 2005; Feldman and Pentland 2003; Zellmer-Bruhn 2003). We do not examine why the routine was or was not created, only the extent to which having a routine defined for circumstances involved in failure influences the duration of the outage and how that may interact with collective mindfulness.

2.2.2 Addressing Failures with Collective Mindfulness

Standard operating procedures instantiated in organizational routines represent one mechanism for addressing failures and achieving organizational reliability. A second mechanism is that of collective mindfulness which sustains reliability through highly situated cognition including an attention and alertness to context (Weick and Sutcliffe 2007). As a concept, collective mindfulness has its roots in the psychology literature that describes the notion of individual mindfulness: a cognitive process that involves high levels of alertness and awareness (Langer 1989). Mindfulness requires active information processing and is characterized by an individual's ability to make distinctions and value multiple perspectives. Collective mindfulness (CM) elevates mindfulness from the individual to the collective such as a workgroup or an

organization, and likewise involves careful scrutiny of existing expectations to ensure that subtle changes in the environment are noticed and acted upon appropriately (Weick and Sutcliffe 2007). However, while collective mindfulness may be influenced by the individual mindfulness of key employees, it is more than the sum of the individual mindfulness of employees within the organization (Baker 2007). At the organizational level, the efforts of many individuals must be coordinated to achieve collective mindfulness because the process of perception may be performed by one employee while the appropriate action must be taken by another (Butler and Gray 2006).

Rich, in depth studies of organizations that maintain high reliability have yielded descriptions of five dimensions of collective mindfulness including deference to expertise, commitment to resilience, attention to operations, preoccupation with failure and reluctance to simplify (Weick and Sutcliffe 2001; Weick and Sutcliffe 2007). These five dimensions are described below.

Deference to Expertise. Collectively mindful organizations migrate decision-making authority to individuals with the most experience, demonstrating deference to expertise. Although an individual may hold a particular hierarchical position placing her in charge, she may not be the one with the most relevant experience related to an unanticipated problem. A certain level of flexibility is required to deal most effectively and efficiently with the unexpected (Weick and Sutcliffe 2007). This is supported by work with teams in emergent settings. Faraj and Xiao (2006) found that expertise coordination practices, such as reliance on protocols and knowledge sharing, are necessary for achieving the efficient application of necessary expertise,

particularly when the expertise is distributed across the team. However, additional coordination practices, termed “dialogic coordination practices”, such as joint sense-making and protocol breaking aid in realizing error-free operation to time-critical, novel events (Faraj and Xiao 2006). Predefined processes and structure, while necessary, are not sufficient for achieving reliability in circumstances involving knowledge work and rapid response (Faraj and Xiao 2006).

Commitment to Resilience. Mindful organizations also invest in training and personnel development in order to improve their ability to respond to the unexpected and maintain resilience. No matter how hard an organization tries to prevent problems, failures are bound to happen in complex, tightly coupled environments (Perrow 1984). By staffing the organization with experienced individuals and providing continual development opportunities, the organization positions itself to react to inevitable failures. Resilient organizations demonstrate a determination to solve problems effectively and efficiently (Weick and Sutcliffe 2007).

Attention to Operations. Mindful organizations recognize the importance of monitoring the current state of operations. It can be dangerous to assume that systems are operating as intended. A high level of communication between individuals, teams and departments is necessary to maintain awareness of the “big picture”. Ideally, employees understand how their actions may impact other functional areas which requires a familiarity with the roles other people and functions play in the overall “health” of the system (Weick and Sutcliffe 2007). Such a familiarity enables appropriate adjustments to be made to avoid failure as well as facilitate response in the event of failure.

Preoccupation with Failure. Mindful organizations exhibit a preoccupation with failure by treating every mistake made or failure encountered as an opportunity to learn and be better prepared for the future. This is similar to “double-loop learning” in that the organization does not simply fix the problem and move on with “business as usual”, but instead questions how existing processes may need to be modified in order to avoid additional problems in the future (Argyris 1976; Guide to Management Ideas 2003). Such organizations attend to warning signs promptly, before they escalate into larger problems with greater impact (Weick and Sutcliffe 2007). A culture is fostered in which employees feel comfortable raising concerns.

Reluctance to Simplify. Organizations with mindful cultures demonstrate an unwillingness to adhere to known, familiar categorizations but to adopt new perspectives (Weick and Sutcliffe 2007). Employees are receptive to input from others and are hesitant to take things for granted.

Not only has collective mindfulness been described as consisting of five dimensions, but these dimensions have been classified into two distinct processes: mindful containment and mindful anticipation (Weick and Sutcliffe 2001; Weick and Sutcliffe 2007). Mindful anticipation consists of attention to operations, preoccupation with failure and reluctance to simplify. These aspects of mindfulness are suggested as particularly relevant in avoiding failures. Mindful containment, on the other hand, is more important for dealing with unexpected failures once they have already occurred. Mindful containment is comprised of deference to expertise and commitment to resilience. These two processes, mindful containment and mindful anticipation, each stressing different aspects of mindfulness, suggest that varying

circumstances may require differential emphases on the different aspects of mindfulness.

Although a significant proportion of prior work has investigated collective mindfulness in the context of High Reliability Organizations (HROs) such as hospitals (Kohn et al. 1999), nuclear power plants (Weick and Sutcliffe 2007), and aircraft carriers (Weick and Roberts 1993), scholars have recently suggested that reliability in other less life-threatening organizations can also be improved with collective mindfulness (Baker 2007; Butler and Gray 2006; Valorinta 2009; Vogus and Welbourne 2003; Weick and Sutcliffe 2007). Organizations operating in environments that are complex and tightly coupled seek reliability because small failures can escalate to threaten firm survival (Baker 2007; Vogus and Welbourne 2003). As noted, many organizations depend on the availability of their IT infrastructure to support critical business operations. The IT infrastructure is often complex and tightly coupled in these organizations because of the volume and variety of different software and hardware components. This study examines mindfulness typically found in HROs in a variety of organizations to determine the influence of mindfulness on the organization's response to IT infrastructure failure.

Existing research on collective mindfulness falls into one of two broad streams. One stream, focused on understanding the role of collective mindfulness in failures has largely deployed qualitative methods due, in part, to the difficulty in designing studies to measure failure (e.g. Bigley and Roberts 2001; Weick and Roberts 1993; Weick and Sutcliffe 2007). A second stream of research uses quantitative field data to examine the positive influence of collective mindfulness on

outcomes such as overall perceived safety (Knight 2004; Vogus and Sutcliffe 2007a), ERP assimilation (Mu 2007) and competitive advantage in new product development (Pavlou and El Sawy 2006). Table 2.1 summarizes extant empirical CM research. The majority of quantitative collective mindfulness research treats collective mindfulness as an omnibus measure (e.g. Baker 2007; Pavlou and El Sawy 2006; Vogus 2004; Vogus and Sutcliffe 2007a/2007b). In addition, these studies typically assess mindfulness and its effects during “business as usual” on group level outcome measures such as overall level of innovation (Vogus and Welbourne 2003), competitive advantage as measured by process efficiency and product effectiveness (Pavlou and El Sawy 2006), and medication errors and patient falls (Vogus 2004; Vogus and Sutcliffe 2007a/2007b). To our knowledge, there is no empirical research that examines the influence of collective mindfulness on an organization’s response to distinct instances of failure. Furthermore, no research has examined the potential influence of collective mindfulness dimensions on different types of failure to understand potential moderating effects.

Two prior studies attempt to measure the specific dimensions of mindfulness (Knight 2004; Mu and Butler 2009), and report the development and validation of scales for measuring dimensions of collective mindfulness. In both instances, factor analysis results yielded only 4 factors and not the 5 dimensions suggested by qualitative collective mindfulness research (Weick and Sutcliffe 2001; Weick and Sutcliffe 2007). The deference to expertise and commitment to resilience dimensions loaded together on one factor. Knight (2004) found collective mindfulness (the omnibus measure) to be positively associated with customer satisfaction and it

approached significance in predicting perceptions of customer safety in the context of community swimming pools. While the Knight (2004) study provides a helpful starting point for further development of scales to assess collective mindfulness dimensions, it was conducted on a very small sample size (51 pools). The Mu and Butler (2009) study obtained data for a wide range of organizations representing varied functional areas and industries; however, it was conducted with undergraduate students acting as key informants. Neither study examined the influence of the separate dimensions on key outcomes.

Although we could find no empirical studies explicitly examining the distinct dimensions of collective mindfulness and their potential incremental influence on organizational outcomes, several studies nevertheless suggest the importance of understanding the dimensions and their unique relationships with other variables. First, in a study of individual mindfulness, Baer et al. (2006) found that individual mindfulness consists of four dimensions, of which only three were found to positively predict psychological symptoms. Each dimension accounted for a significant portion of the variance in psychological symptom level, suggesting that each facet has incremental validity in predicting symptoms (Baer et al. 2006). While individual mindfulness and collective mindfulness are not identical constructs, both are characterized by alertness and distinction and are described as consisting of numerous subdimensions. Furthermore, the individual mindfulness of small business owners was found to contribute to organizational mindfulness in small businesses, suggesting an association between the two levels of analysis. Second, in the context of organizational mindfulness, Mu (2007) found two distinct factors of collective

mindfulness, one reflecting the organization's level of alertness and the other reflecting the organization's awareness of unprecedented changes. While the omnibus measure of collective mindfulness was hypothesized to moderate the relationship between ERP scanning and ERP assimilation, only the alertness/attention dimension was significant. Finally, in another study in which HR practices were theorized as proxies for three of the CM dimensions, each HR practice positively influenced innovation, but their relative effects varied (Vogus and Welbourne 2003). For example, organizations exhibiting a commitment to resilience through an emphasis on training increase their anticipated number of patents by a factor of twom while organizations with excellent employee relations, which contributes to a supportive climate and fosters communication, increase their expected number of patents by a factor of eleven. Collectively, this research points to the importance of examining collective mindfulness at the dimension level to disentangle the effects of the different dimensions and improve understanding of how collective mindfulness processes influence failure performance.

2.3 DIMENSIONALITY OF COLLECTIVE MINDFULNESS

Prior to introducing the key relationships in the model and related hypotheses, we address the question of how best to model collective mindfulness: as an omnibus measure or as a related set of dimensions grouped into processes. In the largely qualitative research on collective mindfulness, it is evident that the construct has been conceived of as multidimensional because it is a single theoretical concept that is often referred to as consisting of several distinct but related dimensions (Edwards 2001). There is debate, however, over the utility of multidimensional constructs and

how best to operationalize them (Edwards 2001). Edwards (2001) compared models which treat the construct as either: a composite of the dimensions (aggregate model); being manifested by its dimensions (superordinate model); or as a related set of dimensions in a multivariate model. The results suggest that the constraints imposed by the superordinate and aggregate models on the loadings of the dimensions on the construct can overestimate some relationships while underestimating other relationships between dimensions and outcomes of interest (Edwards 2001). Collectively, these studies imply that multivariate models may be more beneficial to advancing theory. As a result, it has been recommended that the merits of multidimensional constructs and their dimensions should be compared on a study-by-study basis (Edwards 2001). Due to the scant quantitative research examining collective mindfulness and its dimensions simultaneously, we are faced with no accepted precedence for use in this study. Therefore, we seek to determine the most effective method for modeling collective mindfulness and its dimensions grouped together as processes as part of this research.

Collective mindfulness, as it has been defined in the literature, is most similar to a superordinate construct in that it is “a general concept that is manifested by its dimensions” (Edwards 2001, p. 146). In this way, it is analogous to a reflective measure. As advocated by Edwards (2001), we approach the question of how best to model collective mindfulness as an empirical question and compare the extent to which the omnibus measure of collective mindfulness captures variance in the duration of organizational response to failure to the degree of variance explained by its dimensions grouped as two distinct processes. We also make the assumption as

just described that the direction of the relationships between the dimensions and the construct is superordinate (i.e. similar to reflective) which is consistent with Knight (2004).

Due to the increased interest in quantitatively examining collective mindfulness, such an examination is critical as incorrectly specifying a model can lead to issues of validity and theoretical utility. For example, modeling CM as an omnibus measure and testing its influence on group level variables may be at the appropriate level of abstraction. But, to do so when examining the contextual factors of a specific failure may obscure the impact of CM on the duration of failure response (Edwards 2001; Johns 1998). We argue that the construct of collective mindfulness encompasses too many different behaviors to be theoretically precise and practically valuable when examining its influence on distinct failures (Edwards 2001; Johns 1998; Paunonen et al. 1999). Given that we expect to find that relationships with the duration of failure response varies across the collective mindfulness dimensions grouped as processes, we anticipate that a multivariate model which treats the processes of mindfulness as a set will yield the highest explained variance and a better understanding of the relationships between the processes and duration (Edwards 2001; Johns 1998; Paunonen et al. 1999).

H1: Collective mindfulness modeled as a set of related dimensions grouped as processes will yield a higher explained variance than a model including an omnibus measure of collective mindfulness

2.4 CONCEPTUAL MODEL AND HYPOTHESES

Our core theoretical proposition is that IT infrastructure failures arise due to a combination of factors that include breakdowns in routine and an element of novelty,

and that the negative outcome of these failures is moderated by dimensions of collective mindfulness. Expanding on this core proposition, the conceptual model underlying the study is shown in (Figure 2.1). Next, we present the logic underlying the relationships posited in the model.

The focal outcome of interest is the duration of organizational response to IT infrastructure failure. The duration of an organization's response to failure is indicative of how well the organization performs when faced with an unanticipated incident. IT infrastructures typically consist of a patchwork of hardware and software provided by a variety of vendors which has been customized to varying degrees to meet the specific organization's needs. The complexity of IT infrastructures in organizations today is well documented (Goldberg 2005; Vechio 2001; Wing 2008). Many of the devices and firmware are "legacy" and represent older generations of technology, while others are likely "leading edge" (Vechio 2001). A recent example of this is the increasing desire of organizations to evolve to a "service-oriented architecture" that necessitates significant changes in the underlying infrastructure (Govekar 2007). Incompatible protocols and disparate standards create significant technical challenges that must be managed by IT personnel. In such environments, it is not surprising that both novel and not novel failures will occur. In addition, failures will likely occur whether routines have been defined to handle a particular situation or not.

We distinguish failures based on the extent to which solving the failure requires competencies the organization already possesses. We defined not novel failures as those occurring in contexts where the organization had sufficient

knowledge and experience of the problem domain (e.g. problems occurring during maintenance tasks such as running a backup or applying operating system patches). In contrast, novel failures occur in a context where organizational members lack sufficient knowledge and experience of the problem domain (e.g. problems associated with ProtectCo software bugs, hardware failures, fresh installations of ProtectCo software, or new virus attacks). It is important to underscore the situated nature of novelty: what is novel for one organization may not necessarily be novel for another. In the case of novel failures, the operator or staff likely has very little specific experience on which to draw to help in addressing the failure. For not novel failures, IT personnel may encounter circumstances to which they can apply existing knowledge and resources due to a level of familiarity and experience with similar situations in the past.

In prior research that examined a technical support setting similar to the context of our study, unanticipated problems required significant reasoning and took longer to solve than problems that had previously been encountered or for which a solution could be adapted from a similar context (Das 2003). The innovation literature has also shown that when a firm has less experience with an innovation's technology, the project takes longer to implement (Green et al. 1995). It is also highly likely that a novel problem will require escalation to higher levels within the organization, which involves more resources and can be more expensive (Das 2003). Increased ambiguity is likely to lead to more conflicting ideas and further delays. Thus, one would expect failures that occur in more novel contexts to increase the time required to solve the problem. Given that research exists which has examined the

main effects of novelty on performance outcomes, we do not pose such a hypothesis. Instead, we focus on the interactions novelty may have with dimensions of collective mindfulness to answer the question of how mindfulness enters into the process of solving novel failures.

Failures that occur in a context with which the organization has little experience and knowledge, will likely be dealt with differently than failures that occur in contexts with which the organization has more experience. We expect the dimensions associated with both mindful containment and mindful anticipation will influence the duration of failure resolution differently depending on their novelty for the organization. In novel contexts, some forms of analysis are more effective than others (Gavetti et al. 2005; Spacek 2000). Knowledge of existing configurations, procedures, and abilities may not be as helpful for solving novel problems. An example of a novel problem in an IT setting includes encountering a new strain of software virus. Hackers are getting more and more creative in order to circumvent antivirus technology (Turner 2007), yet most organizations do not have enough expertise to tackle new strains single-handedly. During our qualitative study, an engineer made the following observation about an organization that was involved in a virus attack:

The issue was not failure to use software and procedure to routinely detect or correct the problem, but rather was the fact that this was a variation of a virus that was new and tricky which required the development of custom tools to clean the environment and new antivirus definitions.

Creation of custom tools related to cleaning up after a virus attack and new antivirus definitions are outside the expertise of most organizations that purchase antivirus software from external vendors. In this example, an organization with high

levels of mindful containment will want to defer to its internal experts, but the organization may not have any internal resources upon which to draw for help in making decisions related to novel failures. This could lead to the involvement of too many individuals in the resolution process who are not sure what action to take. To illustrate, in our qualitative study, one engineer who worked on a hardware failure that ultimately required replacement of infrastructure components commented:

Management got involved and threw things out of whack. Management tends to bog the process down by asking irrelevant questions and sending people off in wrong directions.

Resolving the failure may also require the involvement of outside expertise which could increase coordination costs. Lower levels of knowledge have been associated with increased coordination costs in outsourcing arrangements (Cha et al. 2008).

Another aspect of novel failures is that the organization may have to engage in consideration of more options than when faced with a not novel failure. As the number of interactions among choices increase, the demand on cognitive resources can increase to a point beyond the team's ability to process the options. Organizations with high mindfulness may want to engage in deductive reasoning and rational choice in these circumstances which can inhibit effective strategic management processes (Gavetti et al. 2005).

Finally, in terms of mindful containment, an organization with high commitment to resilience will find it easier to draw valuable analogies connecting a not novel failure to familiar experiences than when the failure is novel (Gavetti et al. 2005). In the case of novel failures, the organization's attempts to mindfully contain the failure's impact result in increased coordination costs and *analysis paralysis* due

to their lack of experience as they search for answers (Cha et al. 2008; Gavetti et al. 2005; Spacek 2000).

Analysis paralysis can also manifest itself in the dimensions associated with mindfulness anticipation. High levels of attention to operations may increase the organization's response time due to its increased desire to communicate with all potentially affected departments, which increases coordination costs particularly when the domain is novel as no one really understands the nuances of the failure and its solution. Similarly, a preoccupation with failure may impede response to novel failures as the organization has more difficulty anticipating potential problems. Mindfulness processes within the organization are likely to yield the most benefit in the not novel context as the organization can best leverage its existing knowledge of the problem domain and apply the training and knowledge resources already available. Therefore, we propose:

H2: Mindful anticipation moderates the positive relationship between failure context novelty and duration of failure response such that the relationship is more positive for failure contexts that are novel than for failure contexts that are not novel. (i.e., Mindful anticipation facilitates failure resolution less effectively in novel failure contexts)

H3: Mindful containment moderates the positive relationship between failure context novelty and duration of failure response such that the relationship is more positive for failure contexts that are novel than for failure contexts that are not novel. (i.e., Mindful containment facilitates failure resolution less effectively in novel failure contexts)

In terms of the routine involvement in characterizing failures, our prior qualitative research suggests failures are associated with the extent to which a routine was defined for the circumstances leading up to the failure. Therefore, we examine whether the organization lacked routine to guide employee behavior in the circumstances in which the failure occurred (i.e. were routines defined?). We were

not interested in the escalation and problem-resolution routines followed by the organization once the failure had already occurred but rather were interested in whether or not the organization had been following a routine in the activity preceding the failure. That is, we were more interested in how duration is impacted by problems which arise for situations that have documented routines associated with them and those that do not.

It is important to distinguish between failures that are novel in context and failures that involve no previously defined routine. While most novel failures encountered by the organization will not have any defined routines associated with them, there *are* instances which could be considered novel yet still have routines associated with them. For example, the organization may be performing an upgrade from one version of software to another which requires extensive effort and is novel for the organization (because they may not be familiar with the upgraded software requirements) but for which guidelines and procedures are provided by the vendor as release notes. Lack of routine failures can also arise in not novel contexts. For example, failures may occur during normal maintenance (e.g. updating antivirus software with new virus definitions, adding new tape drives) because the organization may not have invested the time to create a formal routine for a repeatable activity and therefore no standard exists, leaving the organization at higher than necessary risk of failure due to human error. Routines improve efficiency in stable environments; therefore, we would expect routines to improve efficiency when dealing with a related problem. Conversely, when no routine is explicitly defined for specific circumstances and a failure occurs, we would expect that addressing such problems

would take longer because there is less to guide the organization's employees and nothing to look back at during problem resolution to potentially serve as a starting point to help find the problem.

H4: Lack of routine for a failure context is positively associated with the duration of failure response .

Similar to the relationships hypothesized between novelty and the mindful containment dimensions of mindfulness, we expect that each of the dimensions associated with collective mindfulness (Weick and Sutcliffe 2001) will influence an organization's response performance differently depending on the extent of routine involvement. Mindful anticipation as exhibited by reluctance to simplify, attention to operations and preoccupation with failure, improves an organization's ability to avoid failure and become aware of the unexpected earlier to avoid having minor problems escalating into catastrophes (Weick and Sutcliffe 2001). While mindful anticipation is normally associated with avoiding failures, the qualities still exist within the organization when a failure occurs. Consequently, we expect that they will influence the organization's response as the organization wants to avoid creating problems during the response. The mindful capabilities associated with mindful anticipation can lengthen response times when no routine exists because the organization will want to invest more time in assessing how the solution to the problem may affect operations in negative ways. This assessment is likely to take longer in the case of failures associated with a lack of routine because the organization has relatively less concrete information to inform the debugging process and to apply in assessing the potential impact of proposed solutions.

If a routine has not been defined, it implies that the organization may not have seen a need to create a routine. We heard about cases of failure during our qualitative studies that were the result of human error in the execution of repeatable actions for which there were no routines explicitly defined. In such cases, individuals would perform ad-hoc processes. When failures occurred with these ad-hoc processes, customers sometimes had difficulty believing the origin of the problem was in a lack of defined routine and resisted suggestions to formalize the processes. Organizations with high mindful anticipation likely feel as if they have created an environment that is not prone to failure because if they see an opportunity to avoid failure, they take appropriate action. Self-justification theory (SJT) posits that individuals tend to increase their commitment toward a particular course of action to justify prior behavior (Keil et al. 2000). SJT may explain why organizations with high mindful anticipation are not going to want to believe they neglected to create a standardized routine when one may have been warranted (Keil et al. 2000). SJT has been implicated as an explanation for why software projects escalate in spite of negative feedback which indicates the project should be abandoned (Keil et al. 2000). Organizations with high mindful anticipation may experience a period of denial which delays efficient response.

Prospect theory may also inform a delayed response on the part of organizations with high mindful anticipation. While taking action swiftly to limit the duration of outcome may result in gains, organizations with high mindful anticipation may be inclined to focus more on the potential losses involved in implementing a solution before contemplating its full impact on the organization. This would be

consistent with prospect theory which posits that losses loom larger than gains in decision-making under risk (Tversky and Kahneman 1984). The perceived potential for loss is likely to be more pronounced for failures due to lack of routine.

In contrast to the influence of mindful anticipation, the dimensions of deference to expertise and commitment to resilience which comprise mindful containment, may improve an organization's ability to react to failures involving a lack of routine. Just because a routine is not defined, does not mean the organization is unfamiliar with the steps necessary to perform the process. As mentioned previously, it may be that individuals have a general sense what actions to take but none-the-less perform tasks on an ad-hoc basis. In such a case, an organization with high deference to expertise would likely have an awareness of where relevant knowledge is located within the organization. It could then improve performance by migrating decision authority to the appropriate individual during critical incidents. Similarly, organizations with a commitment to resilience tend to be willing to act while analyzing a situation to minimize negative outcomes which is more likely to be beneficial if no routine is already specified (Weick and Sutcliffe 2001). These factors may facilitate easier identification of the source of the problem and an appropriate solution, thus reducing the time required to address the failure.

The preceding discussion leads us to propose the following:

H5: Mindful anticipation moderates the positive relationship between lack of routine and duration of failure response such that the relationship is more positive for failure contexts that involve a lack of routine than for failure contexts for which routines exist. (i.e., Mindful anticipation facilitates failure resolution less effectively when the failure context involves a lack of routine)

H6: Mindful containment moderates the positive relationship between lack of routine and duration of failure response such that the relationship is more

negative for failure contexts that involve a lack of routine than for failure contexts for which routines exist. (i.e., Mindful containment facilitates failure resolution more effectively when the failure context involves a lack of routine)

The empirical study conducted to test these hypotheses is described next.

2.5 METHODS

2.5.1 Research Site and Data Collection

The source of our data is a leading software and services vendor, Protecto, that markets enterprise software targeted toward security, availability and compliance and provides services including technical and business expertise and proprietary insight into IT risk management. The focus in this study is on problems that manifest themselves during the process of utilizing this vendor's software (e.g. problems encountered during backup and recovery processes, security breaches and storage redundancy). The nature of the software provided by this particular vendor makes associated problems critical as they potentially threaten the availability of an organization's systems.

ProtectCo offers various levels of service contracts for its products. We focus on failures encountered by customers who have contracted for the highest level of service with the quickest response times and access to a single point-of-contact, called the account liaison (hereafter referred to as critical customers). When critical customers suspect a problem related to one of the products covered under the service contract, they call the support center, at which time the case is assigned a code indicating the severity level of the problem. For this study, we examine the most severe cases which are such that the condition impacts a critical business function or severely impedes major functionality. High severity cases indicate that reliability of

essential information systems has been compromised, and thus provide an appropriate context for a test of the research hypotheses.

Our empirical strategy involved matched surveys completed by key informants from ProtectCo. The unit of analysis is an “incident” in which the reliability of the customer’s system is compromised. We administered two surveys, one for ProtectCo account liaisons to complete regarding the customer mindfulness and control information, and one for ProtectCo technical engineers regarding incident failure characteristics, including the novelty and routine-based characteristics of the problem as well as duration of the outage. Account liaisons are assigned to only two to three critical customers and, as a result, develop an in-depth familiarity with the customer’s environment and key contact personnel. This close customer contact affords them a deep understanding of the customer’s organizational and cultural context and, as a result, the knowledge necessary to provide responses to customer level questions. In addition, collective mindfulness is considered part of an organization’s culture which tends to be consistent over time (Weick and Sutcliffe 2001) making it unnecessary to assess for each failure. Technical engineers work closely “in the trenches” with the customers’ employees to identify the source of the problem and to craft a resolution strategy, enabling them to provide detailed information regarding the failure and its outcomes.

ProtectCo representatives serve as key informants in providing information regarding the infrastructure breakdowns and classifying the mindfulness levels of the customers (Seidler 1974; Kumar et al. 1993). During the survey process, they are not asked to provide personal feelings and opinions as respondents typically describe, but

to focus more on structural patterns and organizational criteria (e.g. “Please answer the following questions about the complexity of the customer’s environment *relative to other customers*”) (Seidler 1974). A question phrased in such a manner requires, at least implicitly, a calculation be performed (Seidler 1974). The informant must consider the environment of all clients, calculate a mean level of complexity and compare this client to that mean level to formulate a response to the question. Similarly, the questions related to the failure context ask the informant to provide their “knowledge and impressions of the customer’s routines related to the incident and its potential root cause” which demands an inventory of all contributing factors followed by a professional determination of the primary cause. The processes required of respondents are usually much more straightforward. Thus, when using an informant approach, informant perceptions and expertise are essential (Kumar et al. 1993).

Organizations choose external service providers for their technical expertise (Koh et al. 2004; Levina and Ross 2003). On average, our ProtectCo informants have more than 13 years of experience in IT and 4 years of experience working specifically at ProtectCo. The customers involved in our study have all entered into long-term, high level service contracts with ProtectCo. These business critical customers receive not only support during failures but also consulting services such as planning for product upgrades and implementation of maintenance patches. ProtectCo business critical account managers and engineers are assigned to work with only two or three customers at a time. Thus, not only do our ProtectCo representatives have the technical expertise necessary to form the impressions and make the judgments

necessary for our study but they also have developed a level of familiarity with the client/customer organizations which is essential of an informant (Kumar et al. 1993). Providing further support for the relevance of an informant strategy in our study of collective mind is provided by Cooren's (2004) study which found that evidence of collective mind can be drawn from analyzing patterns present in conversation between individuals in groups. This suggests that ProtectCo employees can assess the collective mindfulness of customer organizations by participating in teleconferences, conducting site visits to directly interact with customer employees, and one-on-one conversations with customer employees.

The sampling strategy enables a broad view of reliability concerns across industries and size of organization. While we acknowledge that our data is from the perspective of the vendor and not the customer, the vendor's liaisons and engineers are in a unique position to provide responses to our questionnaires because they have significant experience across a wide range of problems and customers and have obtained broad insights into our phenomenon of interest. Obtaining information from both account liaisons and engineers enables information to be gathered from the most appropriate key informant and increases confidence in the quality of the data. Furthermore, obtaining dependent and independent variables from different sources helps alleviate common methods variance concerns (Podsakoff et al. 2003). Data from these two sources was combined for analysis.

The surveys were administered online in two waves, for 8 weeks each in spring and fall 2007. Due to the time required to complete the surveys, especially for the engineers working on high profile incidents of a critical nature, it was not possible

to survey all incidents occurring during the data collection period. To minimize selection bias, emails were randomly sent at varied times of the day and days of the week to alert respondents that they needed to complete a survey. Upon receipt of an email, the engineer would designate the current case as one for the study effort and complete a survey for it upon closing the case. The team lead then requested each account liaison to complete customer information surveys for each customer included in the case selection effort.

2.5.2 Operationalization of Variables

Independent Variables: Based on our definition of novelty, we adapted scales from Gatignon et al. (2002). The items assessed whether or not the customer possessed the skills necessary, or would have had to acquire fundamentally new concepts or principles to successfully solve the problem (see Appendix B). Although the conceptualization of routines as a duality consisting of an ostensive and performative aspect has been considered in organizational research (Edmondson et al. 2001; Howard-Grenville 2005; Zellmer-Bruhn 2003), we are unaware of the existence of scales to measure the existence of routine for particular circumstances. Therefore, we created new items to measure the extent to which a routine existed to handle the circumstances preceding the failure following the methodology described by Moore and Benbasat (1991) beginning with item creation. To very briefly summarize the process, a search of the existing literature for the definitions and descriptions of the construct aided in item creation, the goal of which is to ensure content validity. We originally began with four items that were all 7 point Likert scales anchored with strongly agree and strongly disagree. These items were

intended to determine if the failure was the result of problem with the way in which a routine was defined. Feldman and Pentland (2003) describe how routines are not defined until a recognizable pattern can be observed. This suggests the potential presence or absence of a defined routine, which we used in creating items to reflect an ostensive routine breakdown. In the next stage, we refined the scale using experts to eliminate ambiguous wording. Finally, we tested the instrument during a pilot phase. Based on the pilot, we narrowed our items down to two for routine definition failures.

For the collective mindfulness dimensions, we adapted items used in previous studies (Knight 2004; Mu 2007; Pavlou and El Sawy 2006; Vogus and Sutcliffe 2007a/2007b). Due to the necessity to keep the incident surveys as short as possible given the time pressure under which engineers work, we selected items across studies that we felt would be most relevant in our context. Again, these measures first went through two rounds of sorting and were tested successfully in the pilot for reliability and validity. The items are all 7 point likert scales anchored with strongly agree and strongly disagree.

Dependent Variable: We operationalized the duration of failure response as the number of elapsed days from problem identification to resolution, which is not limited to business days. Critical account customers have contracted for service that can include 24/7 support due to the nature and potential severity of the problems. Therefore, the duration variable represents the number of calendar days from the opening of the case to its closing upon resolution.

Controls: The duration of failure response can be influenced by a variety of factors that are not of theoretical interest in this study. We included a robust set of

controls to account for any variance explained by such factors. We included two measures of complexity: technical environment complexity, and incident complexity. Drawing upon two core aspects of the definition of task complexity including component complexity (number of acts and information cues involved) and coordinative complexity (type and number of relationships among acts and cues), we used two measures to gauge technical environment complexity (Wood 1986). One reflects the volume of different vendors and products present in the customer's IT environment and the other reflects the variety of ages (i.e. legacy versus state-of-the-art) in software and hardware present in the environment. Incident complexity was assessed using the ProtectCo internal severity level code and the number of vendors involved in the problem resolution process since the having to coordinate the efforts of more people from different organizations could increase duration.

Industry is included to control for any possible differences across industry since it is likely that some industries are more vulnerable to significant losses due to infrastructure failure and, thus, have invested more heavily in crafting effective failure responses (Chiasson and Davidson 2005; Turner 2007). Because Protecto's products address different areas of data center management (e.g. data protection such as backup and recovery and availability such as storage redundancy and server failover capabilities), we control for any influence of product type on failure response performance. Finally, organization size is not included as a control since all of ProtectCo's business critical companies are Fortune 500/Global 2000 firms with similar access to resources to achieve performance gains.

2.6 RESULTS

2.6.1 Scale Development

Since there was only one empirical study available which included all dimensions of mindfulness on which to base our item selection and many of those items were quite specific to that study's context, we conducted a rigorous item validation process. We began by adapting Knight's (2004) items to our context where possible. We added items based on Weick and Sutcliffe's (2001, 2007) conceptual definition of each dimension. We then conducted two rounds of sorting which required judges to sort definitions according to conceptual definitions of collective mindfulness and each of the previously defined dimensions of collective mindfulness. A description of our sorting process and its results are included in Appendix C.

2.6.2 Pilot Study

We initially conducted a pilot study to test survey items. We obtained 16 customer information surveys from ProtectCo account liaisons and 13 incident surveys from ProtectCo engineers during a two week period. In general, reliability was high for the study scales and pairwise factor analysis indicated satisfactory convergent and discriminant validity. We added several items and made minor wording changes to improve likelihood of strong psychometric properties during the full launch.

2.6.3 Full Launch Results

We obtained matched pairs for 153 incidents on 70 critical customers with primary locations in the United States, Europe, the United Kingdom, South Africa and Canada. Forty-four account liaisons and forty-six engineers participated from ProtectCo's global support team. Table 2.2 displays the industries represented in the sample. As these data suggest, the random selection of cases yielded responses from a broad range of industries.

Due to the limited number of empirical studies examining the dimensions of collective mindfulness and because the two other studies found fewer than five dimensions during their analyses, we conducted factor analyses to determine the number of meaningful factors underlying our set of variables. An exploratory factor analysis conducted in SPSS using direct oblimin rotation, suggested a four factor structure instead of five. Each dimension of mindfulness loaded on its own factor with the exception of deference to expertise and reluctance to simplify which loaded together. As we have operationalized reluctance to simplify, the items reflect a willingness to question the opinions' of others yet also be receptive to conflicting viewpoints. It is not surprising that these load with the deference to expertise items which indicate a willingness to seek opinion from the appropriate source. These two dimensions combined reflect a capacity to conduct appropriate "search" activities to find solutions or arrive at a decision. We then examined discriminant validity amongst all the study variables using principal components factor analysis with oblimin rotation. This analysis included the 4 items intended to reflect the collective mindfulness omnibus measure. Two of the items cross loaded with the "search"

dimension (CM3 and CM4). After reviewing the item, we decided to drop these items in favor of a clean distinction between the omnibus measure and its dimensions. The two remaining items for collective mindfulness (CM1 and CM2) capture the alertness and attention typically used to characterize collective mindfulness (Weick and Sutcliffe 2007). Finally, after removing the 2 cross loading collective mindfulness measures, another factor analysis was conducted and the results are reported in Appendix D. Each item loads adequately on its appropriate factor with no cross loadings suggesting the study constructs demonstrate convergent and discriminant validity.

Cronbach's alpha for the dimensions of collective mindfulness, novelty and lack of routine all are .7 or above suggesting that the measures possess adequate reliability (see table 2.3) according to generally accepted standards (Nunnally 1967). We then created indices for each of the study constructs. We use the mean of the "search" and commitment to resilience dimensions to create the mindful containment variable and used the mean of the attention to operations and preoccupation with failure dimensions to create the mindful anticipation variable.

Correlations among the constructs are also provided in table 2.3. The four dimensions of mindfulness are significantly correlated at a moderate level (ranging from $r=.33, p<.01$ between the search dimension and commitment to resilience and $r=.41, p<.01$ between the search dimension and preoccupation with failure). These intercorrelations suggest the dimensions tend to covary. In addition, each of the dimensions was positively and significantly correlated with the collective mindfulness omnibus measure with the search dimension exhibiting the highest

correlation ($r=.74, p <.01$) and the attention to operations dimension exhibiting the lowest ($r=.39, p <.01$).

Novelty and lack of routine are correlated at a small level ($r=.18, p<.05$). As expected, some novel failures are not associated with pre-defined routines. The more novel a failure, the less likely it is to have a pre-defined routine associated with it; however, the correlation is low enough to suggest sufficient distinction between the two variables.

To test hypothesis 1 addressing whether collective mindfulness modeled as an omnibus measure yields more explanatory value than modeling the dimensions separately as a related set, we conducted a series of regressions. All variables were mean-centered prior to creation of the interaction terms (Jaccard et al. 1990). First, we explored the relationship between the dimensions and the omnibus measure. The overall model was significant ($F=50.69, p <.001$). The search dimension accounted for the majority of prediction ($\beta =.59, p <.001$). Commitment to resilience and attention to operations were also significant ($\beta =.14, p <.01$ and $\beta =.12, p <.05$ respectively). Preoccupation with failure approached significance ($\beta =.11, p <.10$). Combined, the dimensions explained 58% of the variance in collective mindfulness suggesting that they explain more than half of the variance in collective mindfulness. We also ran a model to explore the relationship between the mindful processes of containment and anticipation on collective mindfulness. This model was also significant ($F=34.57, p <.001$). Both mindful containment ($\beta =.77, p <.001$) and mindful anticipation ($\beta =.33, p <.001$) were positive and significant.

Next, we ran two regressions, one using the omnibus measure as a predictor interacting with novelty and lack of routine and the other using the mindful processes separately. In each regression, we first ran the model with controls only, followed by adding the main effects of failure type first and the main effects of CM next, before finally running the full model including interactions (Cohen et al. 2003). Results for the omnibus measure are presented in table 2.4 and results for the dimensions are presented in table 2.5. Collective mindfulness approaches significance in both the model with its main effect and interactions (models 3 and 4 of table 2.4). Both models suggest that collective mindfulness has a negative relationship with duration meaning that organizations with higher levels of collective mindfulness respond to failures more quickly than organizations with lower levels of collective mindfulness. In the model with only the main effects of mindful containment and mindful anticipation included (model 3, table 2.5), mindful containment is positive and significant ($\beta = -.52, p < .01$). High levels of mindful containment reduce the time it takes to solve failures. While mindful anticipation is not significant as a main effect, its interaction with lack of process is positive and significant in model 4 ($\beta = .29, p < .05$). In addition, the interactions between mindful containment and lack of process ($\beta = -.29, p < .05$) and between mindful containment and novelty ($\beta = .29, p < .05$) are also significant. However, the directions of influence for the two mindful containment interactions are in opposite directions. High levels of mindful containment reduce the time it takes to solve failures associated with a lack of routine while it increases the time it takes to solve novel failures.

The omnibus main effects and interaction models both explain 10% of the variance in duration while the equivalent models for the dimensions modeled as a set explain 16% and 21%, respectively. Examining the mindful processes as a related set yields an improvement in the amount of variation explained of 6% for the main effects model and 11% for the full model. Moreover, the findings suggest that the processes influence duration in different directions when failure characteristics are considered which suggests that the level of abstraction captured in the omnibus collective mindfulness construct is too broad (Edwards 2001). Collectively, our findings support hypothesis 1 and suggest that organizational mindfulness as a factor influencing failure response performance is better viewed as a set of related processes than as a superordinate construct (Edwards 2001).

We use moderated multiple regression for our statistical analysis. This method supports the inspection of main effects and moderations. The relatively small sample size precludes the use of most structural equation modeling techniques where $N > 200$ is desirable (Marsh and Hau 1999, p. 252; Gefen et al. 2000); however, standard multiple moderated regression techniques yield results that are substantively identical to those produced by structural modeling techniques when there are no mediating variables in the conceptual model (Frazier et al. 2004; Iacobucci et al. 2007). We log transformed the duration variable to more closely approximate a normal distribution. Table 2.5 presents the results of the regression analyses which are also depicted in figure 2.2. Again, we initially ran a model with controls only, followed by a model with controls and main effects of failure type first and then collective mindfulness processes, before entering the interactions (Cohen et al. 2003).

We dropped industry, product and incident severity level controls from the model as they were insignificant and did not influence results.

Hypotheses 2 addresses the interactive influence of mindful containment on the relationship between novelty and duration of failure response. Although not formally hypothesized, based on prior research our a priori expectation was that novelty would have a positive relationship with duration. Indeed models 2, 3 and 4 support this relationship as novelty approaches significance in both models suggesting that the more novel the context of the failure is to the organization, the longer it takes the organization to respond ($\beta = .162, p < .10$; model 3).

The interaction between mindful anticipation and novelty is not significant in model 4. This suggests that there is no difference between how organizations respond to novel or not novel failures based on their levels of mindful anticipation. Thus, hypothesis 2 is not supported. However, the results for the interaction between mindful containment and novelty is positive and significant. The interaction suggests that organizations exhibiting high levels of mindful containment respond faster to failures (significant, negative main effect), but not when the failure is novel (significant, positive interaction effect). This result provides support for hypothesis 3, which states that mindful containment will facilitate the duration of response less effectively for novel failures. This interaction is depicted in panel A of figure 3. Intriguingly, the graph shows that for not novel failures, levels of mindful containment do not seem to influence the organization's duration of response.

The remaining hypotheses involve the relationship between lack of routine and failure response performance. The main effect model, model 2, shows a

significant, positive main effect of lack of routine on the duration of response ($\beta = .22, p < .05$). This finding suggests that the amount of time it takes to respond to a failure increases with the extent to which the organization has no routine defined for the circumstances leading up to the failure. It takes relatively less time to respond to failures for which routines are well defined. The relationship is also positive and significant in the full interaction model ($\beta = .21, p < .05$). These findings provide support for hypothesis 4.

Hypothesis 5 posits that the dimensions associated with mindful anticipation (preoccupation with failure, attention to operations and reluctance to simplify) would be less effective at facilitating response to failures for which there was lack of pre-defined routine. The interaction between mindful anticipation and lack of routine is positive and significant ($\beta = .27, p < .05$) suggesting that higher levels of mindful anticipation can impede the resolution process particularly in the case of failures related to a lack of routine. This finding provides support for hypothesis 5. The relationship between mindful anticipation and lack of routine is depicted in panel B of figure 3. The graph shows that high mindful anticipation increases the time to respond to both failures attributed to a lack of routine or failures having a routine already defined, but the effect is more enhanced for failures due to a lack of routine.

Finally, hypothesis 6 posits that the mindful dimensions associated with mindful containment (deference to expertise and commitment to resilience) will facilitate failure resolution more effectively when the failure involves a lack of routine. Note that in our case, reluctance to simplify loaded with deference to expertise and is, thus, subsumed within mindful containment. Model 4 incorporates

the interaction between the mindful containment and lack of routine. The interaction term is negative and significant ($\beta = -.28, p < .05$) suggesting that high levels of mindful containment decrease the time it takes to respond to failures for which no routine was defined. This relationship is depicted in panel B of figure 3. As predicted, the graph shows that high mindful containment decreases the time to respond to both failures attributed to a lack of routine or failures having a routine already defined, but the effect is more enhanced for failures due to a lack of routine. Hypothesis 6 is supported.

Overall, the results are consistent with the assertion that it is important to examine the effects of collective mindfulness at the level of its dimensions grouped as processes rather than as an omnibus measure. We include a summary of the results for each hypothesis in Table 2.6.

2.7 LIMITATIONS

Prior to discussing the implications of our study, we acknowledge that there exist some limitations which present additional opportunities for future research. First, our data is from the perspective of the vendor and could therefore, be subject to bias. However, utilizing two separate sources for our independent variables reduces the potential for bias (Podsakoff et al. 2003). Moreover, it has often been noted that the true incidence of business continuity problems caused by IT breakdowns is understated because, understandably, organizations are reluctant to reveal their vulnerabilities because of the fear of reputational loss (Campbell et al. 2003). Using organizational members as the source of data for a study of organizational failure may reduce the level of objectivity in the response simply because employees do not wish

to reveal the company's weaknesses. Nevertheless a study enabling the comparison of perspectives from both the customer and vender could provide further insight into the factors contributing to reliability in this context.

This study was conducted in the context of a specific domain, the information systems function, and therefore results are limited to that setting and generalizations must be made with care. However, we note that the findings are likely to have broader organizational implications for other business functions in which an element of routine and collective mindfulness play a role, such as customer relationship management, order fulfillment, and manufacturing. These other business functions require consistently conducting repeatable processes yet also being prepared to respond to unexpected actions taken, for example, by competitors, suppliers or customers. ProtectCo allows unique access to customers representing a wide range of industries and failure types providing results to be generalized with caution. Studies should be conducted in other contexts to confirm findings.

Two of our study constructs were measured using two items (collective mindfulness and lack of routine) due to difficulties with cross loadings during factor analysis. While this is an improvement over single item measures, future studies should seek to find additional items to ensure the content validity of the constructs.

2.8 DISCUSSION AND CONCLUSION

This study was motivated by the fact that the business processes of today's enterprises are so inextricably linked with information technology that any breakdowns or failures in the IT infrastructure can result in substantial economic losses. We drew upon prior research in organizational failure to suggest that mindful

behaviors (i.e., the quality of “collective mindfulness”) can help organizations recover from failure more rapidly and improve organizational reliability. However, prior research on CM has examined the effects of the omnibus measure and not the effects of its separate processes which can lead to over- or underestimation of relationships between processes and outcomes. While more mindfulness has been described as better for reliability, it comes at a cost and should be fostered judiciously (Swanson and Ramiller 2004). Our first research question addressed how best to model CM to explain the most variance in the duration of response to individual failures. Our findings suggest that examining the processes separately yields significantly higher explanatory power, particularly when interactions with failure characteristics are incorporated in the model. Furthermore, examining the processes and their individual effects provides increased insight into the mechanisms at play in failure response.

Our second research question involved determining if each of the mindfulness processes of containment and anticipation were more or less helpful at improving organizational response to failures based on their type as characterized by novelty or lack of routine. Indeed, our findings support an interactive influence of the collective mindfulness processes on the relationship between characteristics of failure and the duration of the organization’s subsequent response. First, we find that high levels of mindful containment impede the organization’s response to novel failures. All of the failures encountered by the companies in our study are unexpected and, therefore, novel to a degree. However, novel failures as we define them this study occur in contexts in which the organization has little knowledge and experience which may

result in more mindful organizations spending too much time coordinating the efforts of individuals who do not possess the appropriate knowledge. Organizations become mired in attempting to understand what occurred and why and evaluating the alternative solutions. Less mindful organizations may not be as thorough in their analysis and, thus, do not encounter *analysis paralysis*. Surprisingly, high mindful containment did not appear to make a significant difference in how quickly organizations respond to not novel failures which is counter to past theorizing and case study results (Weick and Sutcliffe 2007). One explanation for this might be that organizations become naturally more mindful when failures occur. We measured collective mindfulness by asking ProtectCo account managers to provide their professional opinions as to the customer's overall mindfulness levels. Although collective mindfulness is associated with organizational culture which is relatively static and difficult to change, perhaps levels of mindfulness do change during times of crisis. Future research could explore whether CM levels change substantially during a crisis event from the organization's levels during "steady-state" operations.

Second, we find opposing influences of CM based on the lack of routine associated with the failure. Specifically, while high levels of mindful containment reduced the duration of failures associated with a lack of routine, mindful anticipation increased it. Our operationalization of lack of routine involved asking whether or not the customer was following a defined routine when the failure occurred. Even though the customer may not have invested the time in defining a routine, they may have a solid understanding of the effort involved and the context in which the failure occurred. This knowledge can be leveraged if the customer has high levels of mindful

containment by appropriately questioning potential options posed and migrating the decision to the correct individuals. Our findings associated with mindful containment and failures for which routines were defined are consistent with Vogus and Sutcliffe's (2007a) findings in the health context. They found that when collective mindfulness is combined with routine, medication errors were reduced. We find that duration of response to a failure is also improved when routines are combined with mindful containment. Although mindful containment is more helpful at responding to failures associated with no defined routine, our findings suggest that such failures take longer to solve as compared to failures associated with a defined routine. This outcome echoes prior research which indicates routines can improve efficiency, in general, by providing evidence suggesting pre-defined routines also help when responding to related failures (Cyert and March 1963; Miner 2002).

We did not find a significant interactive relationship between mindful anticipation and novelty nor did it have a main effect on duration of failure response. However, we did find that mindful anticipation influences duration of response differently depending on the presence or absence of routine associated with the problem. One possible explanation for this is that mindful anticipation processes are probably more attuned to issues of routine than novelty because the nature of the process is one of avoiding failure and recognizing warning signs. To accomplish this, organizations likely make use of routine to improve the predictability of outcomes (Cyert and March 1963) and provide a guideline for "normal" behavior from the systems. There may even be routines to help improve anticipation (Levinthal and Rerup 2006). For example, routines requiring operators to periodically scan system

messages or the requirement that regularly scheduled meetings are held for the purposes of sharing information. As a result, mindful anticipation is more relevant to an examination of its influence on the lack of routine associated with failure.

Organizations with high levels of mindful anticipation may resist the possibility that something may not have been done correctly (such as their failure to define a routine) which could particularly impede response to failures associated with a lack of routine. In addition, mindful anticipation is substantively about being prepared for the unexpected by focusing on avoiding failure and paying attention to current status. It may be that mindful anticipation, while helpful for minimizing the number of failures encountered, gets in the way of swift response when a failure occurs because the organization may be too focused on determining if various potential solutions will lead to further failures and what the impact may be on operations. Weick and Sutcliffe (2007) suggest that mindful anticipation is most helpful at avoiding failures and do not address how mindful anticipation may influence duration of failure response. Our findings indicate that mindful anticipation can be detrimental during failure response which may suggest the value to an organization of knowing when to appropriately suppress anticipation processes. Building anticipation into the organization's culture may be helpful at reducing the overall number of failures, but might not be helpful in the "heat of the moment".

Our findings suggest a contingency approach to the development and application of mindful processes based on the characteristics of the context in which failures occur. High mindfulness is not always better at improving the duration of failure response. While the focus of this study was on understanding the influence of

collective mindful processes on responses to failures once they occur, future research could examine the influence of the different mindful dimensions on reducing the number of different types of errors over time.

2.8.1 Theoretical Implications

From a theoretical perspective, our study proposes a model in which collective mindfulness processes moderate the relationship between two dimensions of failure context, novelty and lack of routine, and failure outcomes as measured by duration. We were able to test the model with a rich dataset representing 153 failures from 70 global customers across more than 9 different industries. Our context, IT infrastructure failures, is critically important to organizations today yet provides an opportunity to examine the underlying processes at work that previous research focusing on catastrophic failures in which human life is at stake cannot provide.

While our findings may appear to contradict prior research conducted with the omnibus measure of CM, these prior studies examined group level, perceptual outcomes. We conduct a more fine-grained examination of the influence of dimensions of CM on more objective outcome as reflected in the duration of a single failure. While Weick and Sutcliffe (2001, 2007) suggest that mindful containment is more helpful at addressing failures that have already occurred and that mindful anticipation is more helpful at avoiding failures, more mindfulness is described as beneficial to the organization. We find that high levels of anticipation actually impede response to individual failures. Our study did not examine how well organizations avoid failure, only their response to failure. Our findings suggest that organizations should “tone down” their mindful anticipation levels during failure

response. Future research could examine the influence of mindful containment and mindful anticipation on overall failure counts over time (e.g. a quarter, or year) and compare that to how the two processes influenced response to a single failure.

In addition, our study represents a first step toward empirically examining the interplay between routine and collective mindfulness. Elements of each type of behavior, routine- and collective mindfulness-based, have recently been theorized as important for the dynamic environments in which organizations must operate and survive today (Butler and Gray 2006; Levinthal and Rerup 2006; Weick and Sutcliffe 2007). However, beyond acknowledging that both routine and mindful behavior are important, the literature provides limited guidance on which approach to managing reliability is efficacious under what circumstances. We find that documenting repeatable activities in routines improves failure response duration but that mindfulness containment can be very helpful in quickly solving failures for which no routine has yet been defined. Unfortunately, mindful anticipation increases the duration of the same failures.

2.8.2 Practical Implications

For practice, our results related to hypotheses 3 and 5 suggest the importance of defining routines. Overall, organizations respond more quickly to problems for which routines are defined and high levels of mindful containment appear to improve such responses. Furthermore, the findings associated with hypothesis 3 suggest that mindfulness is not as helpful as prior literature would have us believe for solving problems in entirely novel contexts. Organizations might look toward other sources of reliability such as partnering with other organizations that may complement their

strengths and can be called on quickly to help address novel failures. Our qualitative data suggests that organizations that had better relationships with ProtectCo were more receptive to their suggestions to address failure. Collectively, our findings suggest that really only the mindfulness captured in our mindful containment process is helpful for solving IT infrastructure failures. Thus, organizations should focus efforts on ensuring employees are aware of who in the organization has what expertise and that there is sufficient flexibility allowed during failure response for decisions to be migrated to the appropriate individuals. In addition, keeping IT employee skills current will improve resilience and, thus, failure response.

With regard to mindful anticipation, we find it can inhibit an organization's response to failures associated with a lack of routine. Thus, as organizations conduct training or efforts to foster collective mindfulness, perhaps the message should be that while mindful anticipation plays an important role in organizational reliability, it has its time and place. These skills should, perhaps be fostered within specific employees who are not as involved in failure response but rather who focus on identifying potential problems and avoiding them.

This study underscores the importance of both routine-based and mindful behavior. Our findings suggest that documenting repeatable activities improve response to failures. In addition, while higher levels of mindful containment can be helpful in solving IT infrastructure failures, mindful anticipation appears not to be as helpful at decreasing duration of outages. Thus, additional research is required to empirically determine the potential value of mindfulness at avoiding IT infrastructure failures.

CHAPTER 3: THE DIGITIZATION OF HEALTHCARE: BOUNDARY RISKS, EMOTION, AND CONSUMER WILLINGNESS TO DISCLOSE PERSONAL HEALTH INFORMATION

ABSTRACT

As healthcare becomes increasingly digitized, the promise of improved healthcare enabled by technological advances must inevitably be traded off against any unintended negative consequences. There is little else that is as consequential to an individual as his or her health. In this context, the privacy of one's personal health information has escalated as a matter of significant concern for the public. The value of drug discovery, medical research, and public health policy can be realized only if consumers are willing to allow their health information to be electronically stored and manipulated. We pose the question: under what circumstances will individuals be willing to disclose identified personal health information and permit it to be digitized? Using privacy boundary theory and recent developments in the literature related to *risk-as-feelings* as the core conceptual foundation, and synthesizing research from information systems, communication, and psychology, we propose and test a model explicating the role played by type of information requested (general health, mental health, genetic), the purpose for which it is to be used (patient care, research, marketing) and the requesting stakeholder (doctors/hospitals, the government, pharmaceutical companies) in an individual's willingness to disclose personal health information. Further, we explore the impact of emotion linked to one's health

condition on willingness to disclose. Results from a nationally representative sample of over 1,000 adults underscore the complexity of the health information disclosure decision and show that emotion plays a significant role, highlighting the need for re-examining the timing of consent. Theoretically, the study extends privacy boundary and *risk-as-feelings* theories to a new context. On a practical level, this study may be used to improve understanding of consumer concerns and influence policy related to the electronic storage of health information.

3.1 INTRODUCTION

Privacy Issue Complicates Push to Link Medical Data: "...Barack Obama's plan to link up doctors and hospitals with new information technology ...is imperiled by a bitter, seemingly intractable dispute over how to protect the privacy of electronic medical records."

*New York Times, January
17, 2009*

Today's discourse on the digitization of healthcare has moved beyond the potential transformational effects of artifacts such as electronic health records to a vision of the future where IT enables the practice and delivery of medicine to be increasingly personalized (Glaser et al. 2008), in much the same way as products and services are customized to the needs and preferences of consumers in commercial domains (Awad and Krishnan 2006). Simultaneously it has ignited unprecedented concerns regarding the protection of large quantities of personal information that must be captured in electronic health records, the foundational technology platform necessary for interoperability and the realization of promised benefits (HHS 2007; Lohr 2006; Shortliffe 1999). Indeed, the volume and scope of personal health information (PHI) being captured and stored in digital form by both healthcare institutions such as hospitals (Kush et al. 2008) and non-health entities such as

Google and Microsoft (Liedtke 2008; Mandl and Kohane 2008) is increasing every day. While the highly publicized forays by Google and Microsoft into the personal health record space are purportedly intended to empower consumers so that they electronically manage their own health information, these organizations are not officially covered under the Health Insurance Portability and Accountability Act (HIPAA) (Mandle and Kohane 2008). Thus, a consumer's electronic PHI is not guaranteed the same privacy protection it is when the consumer provides it to a doctor or pharmacist working for a healthcare organization (Liedtke 2008). As the volume of information which is potentially vulnerable increases exponentially (Kohlmeier 2007), so does the urgency of finding appropriate policies to protect consumer privacy while reaping the benefits of digitization.

The specter of PHI being compromised is alarming: a nationwide Harris poll conducted in 2006 confirms that approximately one quarter of U.S. adults have significant concerns about the use of their health information and fifty percent believe they have lost control of how their medical records are used by insurance companies, employers and governmental agencies (Harris 2007). Since digitally stored health information represents a considerably faster, cheaper method of access than traditional paper records (Nakashima 2008), these risks are compounded. Yet, the benefits to be realized by the digitization of health information are compelling: they include reduced medical errors, improved patient care, and reduced healthcare costs (Glaser et al. 2008; HHS 2007; Mowry and Constantinou 2007). Less frequently cited benefits include improved tracking of drug safety, facilitated research and development of new drug treatments, contribution to public health research, and

increased consumer control over healthcare. Indeed, the social and individual benefits of collecting granular medical data in electronic form are so considerable that it is important to more fully understand consumer concerns related to health information privacy.

On the surface, it may appear that the healthcare context is similar to other privacy dilemmas in which individuals evaluate the costs and benefits of disclosing personal information (Dinev and Hart 2006; Malhotra et al 2005; Gefen 2000; Pavlou and Gefen 2004; McKnight et al 2002). However, the healthcare context is unique in many respects because of the variety of risks raised with the potential loss of sensitive health information (Kohlmeier 2007; Beckerman et al. 2008) as well as the emotion linked to one's medical state (Trumbo et al. 2007; Loewenstein 2005). For instance, prior research has found that people tend to be more emotional and exhibit more risk-seeking behavior when faced with a life-death choice than with problems in other life domains such as personal finances or public property (Druckman and McDermott 2008; McDermott et al. 2008).

The decision to allow PHI to be digitized is not a simple one. It is likely that individuals differ in their perceptions of the privacy risks and benefits related to sharing their electronic health information depending on the specific *context* in which they are asked to disclose the information. For example, prior research has noted that individuals have different privacy concerns over their financial information compared to their demographic profile or lifestyle interests (Phelps, Nowak and Ferrell 2000; Culnan 1993) because the loss associated with a compromise of the former is more consequential than the latter, suggesting that the type of information being requested influences disclosure decisions. The healthcare setting is characterized by multiple

types of health information (e.g. mental health, HIV/AIDS status) which are afforded different levels of protection due to their sensitive nature (Beckerman et al. 2008). Further, the healthcare value chain has multiple players with a need to access and use PHI, and the individual has varied degrees and methods of interaction with these organizations. Finally, a key contextual consideration is the purpose for which information will be used. How do individuals make choices in such a complex contextual milieu? To answer this question we draw from Communication Privacy Management (CPM) theory, which has implicated the notion of multiple privacy boundaries as the driver of such individual behaviors (Petronio 2002; Stanton 2003). Privacy boundary theories in conjunction with the healthcare context provide insight into potential risk factors which influence an individual's level of concern and trust (i.e. the privacy calculus).

A second element of complexity in healthcare decisions is the emotion associated with them. Most theories, including those underlying extant privacy research, conclude that a choice made when uncertain is cognitive and consequentialist (e.g. Schoemaker 1982; Tversky and Kahnemann 1984; Ajzen and Fishbein 1980, Dinev and Hart 2006, Malhotra et al. 2004), yet other studies show that emotions also have a profound influence on decisions (e.g. Ariely and Loewenstein 2006; Damasio 1994; Loewenstein 2005). Surprisingly privacy research has yet to incorporate emotion in its theorizing. In terms of health status, medical condition (e.g. pain, addiction, fear) has been shown to alter preferences and behavior (Trumbo et al. 2007; Lowenstein 2005). Previous studies have also suggested that individuals mis-predict their response in situations where emotions play a significant

role. While other types of personal information may elicit an emotional reaction, PHI provides an extreme case because of its highly sensitive nature that elicits a visceral reaction (Druckman and McDermott 2008; Kuhberger et al. 1999; Wang 1996).

Using CPM and recent developments in the literature related to *risk-as-feelings* as the core conceptual foundations while synthesizing research from information systems, communication, and psychology, we theorize in this paper what type of personal health information an individual is willing to disclose about herself, to whom, and for what purposes. We further examine the role of emotion in health information disclosure decisions, and the extent to which individuals are able to accurately predict the effect of emotion on their response. We contribute to theory by expanding the dimensions of risk introduced by contextual variables in the electronic health information privacy context and considering emotion in order to determine the circumstances under which people are willingness to provide access to health information. We test our theory with data from 1,089 respondents from a nationally representative sample using a quasi-experimental, survey methodology. The practical ramifications of our findings include policy implications regarding the timing of consent.

The rest of this paper is organized as follows. We begin with the theoretical foundations, reviewing prior work on the privacy calculus, the notion of boundaries, and the importance of emotion. This is followed by a discussion of the research model and eight research hypotheses. We next present the results of empirical tests of the model. The paper concludes with a discussion of the theoretical and practical implications of our findings.

3.2 THEORETICAL BACKGROUND

The central thesis of this study is built on the argument that to understand privacy concerns in the digital healthcare context, we must consider risk at a more granular level than has been done in past privacy studies, and that emotion is a central determinant of one's privacy concerns. We begin by describing recent research on the privacy calculus performed by individuals when determining whether or not to disclose personal information. We then argue that many of the elements of risk an individual must consider when performing a privacy calculus in the healthcare context can be informed by Communications Privacy Management theory and its research into the boundaries individuals erect around their personal information. Finally, we briefly summarize recent literature on the role of emotion on decision making.

3.2.1 Privacy Calculus

As argued in expectancy theory, individuals tradeoff costs and benefits when deciding whether or not to disclose private information (Culnan and Armstrong 1999; Dinev and Hart 2006; Phelps et al 2000), i.e., they engage in a privacy calculus. Expectancy theory broadly supports the idea that a person considers the sum of the valences of all possible outcomes and seeks to maximize positive outcomes and minimize negative outcomes in her motivation to act or not act (Vroom 1964). In information privacy contexts, risks often comprise the cost side of the equation while trust, or the willingness to assume the risks associated with disclosure to achieve some outcome, reflects the benefit side (Culnan and Bies 2003; Malhotra et al. 2005; Mayer et al. 1995). Dinev and Hart (2006) found personal Internet privacy concerns,

Internet trust and personal Internet interest to be strongly related to willingness to provide personal information. They also found that a higher level of general perceived Internet risk was related to higher levels of personal Internet privacy concerns and lower levels of willingness to provide personal information (Dinev and Hart 2006). The Dinev and Hart (2006) study provides interesting insight into how Internet users' perceptions of the artifact (i.e. the Internet) influence their behavior. However, it fails to illuminate the determinants of information disclosure to particular vendors or of particular types of information.

Trust is especially important in offsetting perceptions of risks in conditions of information asymmetry such as when consumers are unable to accurately determine if a service has been provided correctly either due to lack of expertise or knowledge (Culnan and Armstrong 1999). Research has shown individuals can be encouraged to disclose to an organization when higher levels of benevolent trust (trustee caring and motivation to act in consumer's best interest) and integrity (trustee honesty) exist (McKnight et al. 2002), as well as when the individual is aware of the organization's use of fair procedures for managing personal information (Culnan and Armstrong 1999). Procedural fairness acts as an intermediary to building trust when relationships are characterized by significant social distance (Culnan and Armstrong 1999). While these findings provide valuable insight into factors that increase the likelihood of disclosure, they do not simultaneously examine a variety of potential risk factors in disclosure.

With an experimental design manipulating the type of information requested (financial and purchase preferences), Malhotra et al. (2005) found that more sensitive

information increases risk beliefs and decreases trusting beliefs and intentions to disclose. Phelps et al (2000) found that consumers were most willing to provide demographic and lifestyle information, less willing to provide purchase-related information and least willing to provide financial information or personally identifiable information. In the same study, consumers indicated a willingness to provide information in exchange for shopping benefits such as time savings suggesting that personal interest factors can override privacy concerns (Phelps et al 2000), reinforced later by the work of Dinev and Hart (2006). Culnan (1993) found that although many people hold positive attitudes toward direct marketing in general, they have negative attitudes toward targeted uses of their personal financial information or shopping preferences, which suggests a need to design studies to examine specific characteristics of information practices.

In summary, individuals engage in a decision process to weigh the costs and benefits associated with disclosing information. Although studies have found that trust and concern vary with particular vendors or artifacts or types of information, no single study has combined the potential influence of all factors that can influence risk when disclosing information. As we argued previously, the complexity of the healthcare context in terms of the plurality of stakeholders coupled with the highly personal and sensitive nature of the information suggest that investigations of privacy must pay attention to a broad range of elements of risk. We next describe literature associated with CPM to help characterize a setting in which all factors are likely to play a role, such as in healthcare.

3.2.2 Boundary Management

Communication Privacy Management (CPM) theory presumes people make choices regarding disclosure of personal information based on criteria they perceive as salient at the time the decision must be made (Petronio 2002). CPM uses the metaphor of boundaries to illustrate borders marking the ownership line over which private information flows to aid in understanding control issues (Petronio 2002). When the boundary is open, information flows freely and when it is closed the information flow is restricted. Much of the research on which this theory is based was conducted in interpersonal situations such as marital and parent-child relationships. However, the mental calculus performed when determining whether to disclose private information to a friend or loved one is arguably similar to the weighing of costs and benefits that must be performed when deciding whether or not to disclose electronic information to an entity in the healthcare value chain.

CPM elaborates rules to aid in decisions about how the boundaries in dyadic relationships are maintained. Two of these rules shed light on the risk factors that must be considered in the PHI privacy calculus: contextual factors and risk-benefit ratio criteria. First, relevant contextual factors include traumatic events and life circumstances. In the healthcare context, one's medical history may make requests for certain types of information (e.g. mental health or substance abuse) particularly sensitive. Second, the risk-benefit ratio criteria of CPM suggests that an individual accounts for the different types and levels of risk that must be considered when deciding whether or not to disclose information. Types of risk include relational, stigma, face, and security (Petronio 2002). In our healthcare setting, requests for

information to be used for a particular purpose such as research versus patient care may make different risks salient, thereby influencing the rules applied by the individual when making the disclosure decision.

Stanton (2003) adapted CPM to the workplace setting to understand the conditions under which employees would or would not reveal information to their organizations. His extension of the theory incorporated computer-mediated communication with organizational representatives such as managers and supervisors. Through incorporation of organizational justice concepts, Stanton (2002) found that the opening and closing of boundaries appears to be influenced by the mission-relatedness of the request for information. In other words, the extent to which requests made by stakeholders are perceived as fair and relevant influences the individual's willingness to disclose. While Stanton's findings clarify the factors influencing an employee's decision to disclose information in the workplace, additional research is required to disentangle the potential influence of the interpersonal relationship the employee has with the organizational representative. In addition, an employee generally has a relationship with the organization he works for and is familiar with its mission and goals. In the healthcare context, there is often a weaker relationship between the consumer and the stakeholder requesting access to PHI, which increases risk. Further, requests for information are not typically associated with an individual but rather an organization as a whole (e.g. a pharmaceutical company or a hospital). Therefore, the individual will not have an interpersonal relationship to be confounded with the dyadic relationship (individual-organization). We extend the study by removing the interpersonal confound and by

varying the degree of familiarity/dependence the individual has with the requesting organization.

Acknowledging in 2005 the degree of variability in stakeholders and their relationships with consumers of healthcare, the federal government's department of Health and Human Services (HHS) created the Health Information Security and Privacy Collaboration (HISPC), a multi-disciplinary team of experts working to accelerate the adoption of health information technology and the secure portability of health information across the U.S. (HHS 2005). As part of the movement to address privacy and security policy questions, HISPC created scenarios designed to cover various types of information as well as the intended use of the information by a wide variety of stakeholders to ensure coverage of all procedures/policies (Dimitropoulos 2007). These HISPC scenarios reinforce the importance of numerous contextual factors influencing privacy in the healthcare setting.

To summarize, we have argued that the determinants of PHI disclosure decisions are significantly more complex than a simple consideration of concern and trust. To the extent that an individual's perception of risk varies based on situational factors present in the request (including the type of information, the purpose for which that information will be used, and the requesting stakeholder), these three situational factors will alter the salience of the type and level of risk and resulting rules applied to the individual's privacy boundaries. Thus, they are likely to interact with concern and trust in the privacy calculus.

3.2.3 Emotion

Much of the privacy research to-date (Dinev and Hart 2006; Malhotra et al 2004; Son and Kim 2008) is based on the tradition that when making decisions under risk and uncertainty, people assess the severity and probability of possible outcomes of choice alternatives to arrive at a decision (e.g. Schoemaker 1982; Tversky and Kahnemann 1984; Ajzen and Fishbein 1980). However, it is also well documented that emotion has the capacity to alter perceptions, physiology and abilities (Cosmides and Tooby 2000). As suggested in recent influential work by behavioral economists and psychologists, the transformation that can be brought on by emotion can also influence decision making (Ariely and Loewenstein 2006; Damasio 1994; Loewenstein 2005; Raghunathan and Pham 1999).

The *risk-as-feelings* perspective (Loewenstein et al 2001) offers an alternative lens for understanding decision making under risk that incorporates allowances for affective states that do not enter into cognitive evaluations. Such affective states respond to factors that are not typically considered in a rational cognition framework (Loewenstein 2001); emotional reactions are influenced by contextual variables that play only a minor role in cognitive evaluations. For example, emotions are affected by an individual's personal experiences (Weinstein 1989), the vividness of mental images (Damasio 1994), and the timing between the decision and possible outcome (Van Boven et al. 2004); all factors that are likely to be important in the context of healthcare. To illustrate, if the individual is anxious or fearful about her medical condition, she may easily be able to visualize a further decline in her health and want

to avoid that at all costs. This feeling may dominate any potential privacy concerns she may have.

In addition to having different determinants than cognitive evaluations, emotional reactions are insensitive to probability variations as compared to cognitive evaluations (Lowenstein et al. 2001). For example, people tend to buy insurance more for emotional reasons such as peace of mind than they do based on probabilities (Lowenstein et al 2001). If an individual is sick, he may disclose information in the hopes that it may somehow improve his health regardless of what the actual probability of improvement may be.

In exploring the role of emotion, Lowenstein (2005) documents what he terms an “empathy gap” in medical decision making. He finds that people have difficulty predicting how they will feel or what they will want if asked to do so for an affective state that is different from their current state (see e.g. Loewenstein 1999; Van Boven and Loewenstein 2003)³. These gaps take two forms. First, when people are in a “cold” state (i.e. not affectively aroused), they are unable to fully appreciate what their own feelings and behavior will be in a “hot” or affectively aroused state. For instance, people have trouble imagining the motivational forces of hunger, pain, or fear and, therefore, underestimate their influence on their feelings and behavior. The reverse is also true. People in a “hot” or affectively aroused state do not realize the extent to which their feelings and behavior are influenced by affect. They tend to believe they are acting more dispassionately than they actually are. Empathy gaps

³ This is analogous to the *hypothetical bias* described in economics literature in which it is generally found that respondents report higher willingness-to-pay in a hypothetical payment situation than in an actual situation (Champ et al. 2009).

can further be classified as to whether they occur when a person is asked to predict his own behavior in the future (prospective), recall his past behavior (retrospective), or predict the behavior of another (interpersonal).

The existence of empathy gaps is documented in the context of addiction, thirst, pain and fear (Giordano et al 2004; Van Boven and Lowenstein 2003; Read and Lowenstein 1999; Van Boven et al 2004). In the addiction study, heroin-addicted individuals receiving a methadone-like treatment drug chose between getting a dose of the treatment drug versus different money amounts. They were told that they would receive their choice when they came in for their next treatment five days later. Subjects made their choice either before receiving their drug treatment (currently deprived) for the day or after. In support of the empathy gap, subjects who were currently deprived better appreciated the force of their future craving and valued the drug treatment more highly than the participants who had already received their treatment and were no longer experiencing a craving. Thus, it is highly plausible that health information privacy decisions are influenced by emotion (i.e., the individual's emotional state related specifically to current health) and that there exists an empathy gap as well.

3.3 CONCEPTUAL MODEL

Drawing from the literature summarized above, Figure 3.1 depicts our conceptualization of the drivers of individuals' willingness to share PHI. The relationships in the model are based on past privacy research (Malhotra et al, 2004; Dinev and Hart 2006; Phelps et al 2000, Petronio 2002), a synthesis of the relevant

factors embedded across the HISPC scenarios (Dimitropoulos 2007) and the *risk-as-feelings* perspective (Lowenstein et al 2001).

The focal dependent variable is individuals' willingness to provide access to a specific type of PHI in electronic format to a particular stakeholder for a specified purpose. Types of PHI can include mental health, general health or genetic information. Healthcare stakeholders are represented by hospitals, pharmacies or governmental/public health agencies each of whom have their own interests in obtaining access to consumer PHI. PHI may be required in the provision of patient care or be beneficial in facilitating research and marketing products and services. Willingness to disclose information as a condition for transacting is an outcome variable which is consistent with prior privacy research (Dinev and Hart 2006; Malhotra et al. 2004; McKnight et al. 2002). However, our dependent variable refers to a much more specific outcome, reflecting the focus of the theoretical model to understand the influence of privacy boundary considerations on willingness to disclose information in the unique healthcare context.

As suggested by theory and empirical tests described in past privacy research in online contexts, we expect to find a negative relationship between an individual's level of privacy concerns regarding the electronic storage of their personal health information and their willingness to provide access to PHI (Culnan and Armstrong 1999; Dinev and Hart 2006; Son and Kim 2008). Prior research has documented this relationship between concern and willingness to disclose extensively; however, as depicted in Figure 3.1, we assert that this relationship is more complex than what has

been previously conceptualized. In particular, we expect key risk scenario factors to interact with concern in their effects on willingness to disclose health information.

Following a similar logic and consistent with past privacy research which focused on the Internet artifact, we expect to find a positive relationship between an individual's level of trust in the storage of PHI in an electronic format, which is a reflection of the individual's willingness to assume the risks associated with the environment to achieve an outcome, and provide access to PHI (Dinev and Hart 2006). We focus on conceptualizations of trust similar to those used by Dinev and Hart (2006) in their study to assess trust in the Internet as a medium, as our focus here is on trust in electronic storage as a medium. We view trust as a multi-dimensional construct comprised of competence, reliability and safety beliefs; i.e., the individual's belief that electronic storage provides a reliable and safe environment in which to store health information, and her belief that electronic storage format provides the necessary components to facilitate electronic storage of health information will be positively related to disclosure. As in the case of concern, the positive relationship between trust in the electronic medium and willingness to disclose information is intuitively appealing, and has been empirically verified in prior work. We suggest, however, that this relationship is not as straightforward as has been previously posited: we expect it to be moderated by the same risk scenario factors that moderate the relationship between concern and willingness to disclose.

Concern and trust represent two key variables individuals weigh when attempting to balance the costs and benefits involved in privacy disclosure (Dinev and Hart 2006; Malhotra et al. 2005; McKnight et al. 2002; Gefen 2000). Each is

influenced by the boundary management mechanisms individuals employ based on the varied risks made salient by the type of PHI requested, the intended purpose of use, and the requesting stakeholder. Previous studies have examined risk and its influence on consumer online behavior in a number of ways including economic loss as an antecedent to intentions to conduct ecommerce transactions with a particular organization (Jarvenpaa et al 2000; Jarvenpaa et al 1999; Pavlou and Gefen 2004), and personal information loss as an antecedent to willingness to disclose to Internet websites in general (Dinev and Hart 2006) and specific vendors (McKnight et al 2002; Gefen 2000). Collectively, these studies suggest that different types of risk may be more influential than others in dissuading individuals from conducting e-commerce transactions (Dinev and Hart 2006). Other research notes that an individual's choice behavior and persuasive propensity differ depending on the domain of risk (Rettinger and Hastie 2001; Mandel 2003). Factors found to influence decision processes across different risk domains such as legal, academic, and financial include the personal importance of the outcome, the familiarity with the decision context, and moral relevance (Rettinger and Hastie 2001). To the degree that each individual's health status is unique, so is the type of loss perceived as most salient. Thus, all three risk scenario factors may invoke different risk types and levels for the individual, influencing the relationships between concern and disclosure and between trust and disclosure.

A handful of prior studies have examined the main effect that type of information -- such as financial versus purchase preferences (Malhotra et al 2004) and demographic versus lifestyle (Phelps et al 2000) -- exerts on willingness to disclose,

but the more nuanced interaction effect has not been proposed. The notion that some health information is more sensitive than others is supported by the existence of greater legal protection for certain types of health information records (Beckerman et al. 2008; Dimitropoulos 2007). Disclosure of information related to mental illness, substance abuse, and even genetic traits can result in negative consequences including: social stigma, discrimination, criminal prosecution, and job loss (Beckerman et al. 2008). To apply concepts from CPM, individuals likely erect different boundaries around different types of PHI and apply varied rules accordingly. It follows then, that the degree of influence an individual's privacy concerns regarding the electronic storage of health information has on willingness to provide access could vary based on the type of information requested. For example, if the request involves general health information such as height, weight, blood pressure, cholesterol level, and chronic illnesses, unauthorized disclosure of that information could jeopardize one's financial future in terms of employability and insurability, while social risks associated with a privacy compromise may not be particularly salient. In contrast, if the request involves information about substance abuse history, this could have financial, legal and social risks if the information becomes available to unauthorized individuals or organizations. The social stigma may be more enhanced when the request involves information such as HIV status, for example. We expect the increasing sensitivity of the information to increase the domains of risk that become salient to the individual, thus enhancing the negative influence of concern on willingness to provide access:

H1: The type of personal health information (PHI) requested moderates the relationship between concern regarding the electronic storage of PHI and willingness to provide access to digital PHI such that the more sensitive the information is perceived to be, the more negative the relationship between concern and willingness to provide access.

Dinev and Hart (2006) found perceived Internet privacy risk negatively influenced Internet trust which suggests a direct relationship between risks and trust in the privacy context. Our risk factors are not directly about the electronic medium but rather they influence the risks made salient to the individual which, in turn, alter the importance of the relationship between trust in the electronic medium and willingness to provide access to information. As the domains of risks made salient to the individual increases with the sensitivity of the type of PHI, so does the importance of trust in the electronic medium:

H2: The type of PHI requested moderates the relationship between trust in the electronic medium and willingness to provide access to digital PHI such that the more sensitive the information is perceived to be, the more positive the relationship between trust and willingness to provide access to personal health information.

A distinctive characteristic of the healthcare context is the multiplicity of stakeholders in the system, each with different domains of activity, organizational goals, and performance criteria. Physicians, hospitals, insurance companies, pharmaceutical companies all stand to benefit from access to electronic health information for a variety of purposes, including new drug research, trend analysis, marketing, disease outbreak control, and patient care. Thus, in a theory aimed at understanding the influence of an individual's health information privacy concerns, it is necessary to consider each of these potential uses of the information to determine if concerns and trust in the electronic medium vary based on the intended use to which the information will be applied. Past privacy research has examined a consumer's

concerns related to disclosing information for conducting a business transaction (e.g. Dinev and Hart 2006), obtaining information (Dinev and Hart 2006), or using personalized service or advertising (Awad and Krishnan 2006).

In much the same way as the perception of the type of risk varies based on the type of information involved in the risk, the perception of risk type likely varies with the purpose for which the information is to be used. For example, if the request for information is in the context of medical care or disease management, the individual may believe that her health is at risk if the information is not provided. This would have to be weighed against any financial and social risks associated with potential unauthorized disclosure of PHI which may also apply to the situation. In this scenario, the perceived risks to one's health associated with not disclosing may offset any potential financial or social risks associated with a loss of privacy. In other words, a desire to improve one's health and avoid any potential health risk will undermine concerns related to the electronic storage of health information.

Individuals tend to be more risk-seeking in situations involving human lives compared to money/property (Kuhberger et al. 1999; Wang 1996). One potential explanation for this is based on optimal foraging theory which suggests that risk seeking behavior increases as the threat to survival increases (McDermott et al. 2008).

Likewise, trust in the electronic medium may become less important in a decision about disclosing information when one is battling for one's health. On the other hand, if the purpose of the request is to use the information for marketing activities, the health benefits are less obvious. In this situation, the potential financial and social risks may become more salient, enhancing the negative influence of

concern on willingness to provide access and increasing the positive influence of trust on willingness to provide access.

The positive moderating influence of intended purpose on the concern/willingness and trust/willingness relationships is supported by the work of Awad and Krishnan (2006). They find consumers more willing to share information for personalized service over personalized advertising (Awad and Krishnan 2006). In addition, a person who is ill and in need of care is likely to be focused on avoiding further loss of health, at whatever cost to privacy. The logic underlying this assertion is embedded in prospect theory in that losses loom larger than gains (Tversky and Kahneman 1984). An individual needing care may view a request to provide health information in a “loss frame” and be more willing to take risks. While an otherwise healthy individual who is asked to make her information available for research may view this more as a potential “gain” and may be more risk averse (i.e. less willing to risk privacy) in this situation. Thus, the extent to which the information is intended for use in improving one’s health should to weaken the influence of concern about the electronic storage of health information and the willingness to disclose health information:

H3: The intended purpose for which PHI will be used moderates the relationship between concern regarding the electronic storage of PHI and willingness to provide access to digital PHI such that the more apparent the potential health benefits are to the individual, the negative relationship between concern and willingness to provide access will be attenuated.

Following a similar logic, the positive relationship between trust in the electronic medium and willingness to provide access to PHI will be attenuated when the purpose of use is more closely related to the provision of healthcare:

H4: The intended purpose for which PHI will be used moderates the relationship between trust in the electronic medium and willingness to provide access to digital PHI such that the more apparent the potential health benefits are to the individual, the positive relationship between trust and willingness to provide access will be attenuated.

The third contextual variable relevant to PHI disclosure decisions is the requesting stakeholder. Individuals have varied levels of interaction with and beliefs about the numerous stakeholders involved in the healthcare arena that influence the risks that are made salient when a particular stakeholder requests PHI. First, while many individuals may see their primary care physician frequently, they likely visit the hospital less often and even less frequently correspond directly with pharmaceutical companies or public health agencies. This variation in interaction yields different levels of familiarity with each stakeholder. Familiarity has been associated with trust (McKnight et al. 2002). If an individual's primary care physician asks for access to PHI for the purposes of conducting research, this may appear less risky than if a pharmaceutical company makes a similar request because of the level of trust one has for their physician based on a history of interactions. As part of the HISPC initiative, the state of West Virginia conducted a survey of over 500 citizens and validated findings by conducting focus groups (Global Strategy Group 2007). The findings suggest consumers trust doctors and hospitals the most to own electronically stored health information and trust for-profit companies (e.g. insurance companies) the least. If an individual has more first-hand knowledge about a stakeholder, his level of confidence in the stakeholder's expertise and ability to perform as expected should lower the importance of the role of trust in the electronic medium.

Second, individuals likely have different beliefs about the role different stakeholders should play in the healthcare value chain. The more consistent the

request seems with the organization's overall perceived mission, the less risky it may appear to be to the individual. As noted, because of procedural fairness expectations, individuals are more receptive to requests that appear consistent with the requesting organization's mission (Culnan and Armstrong 1999; Son and Kim 2008; Stanton 2003). Based on trust levels and perceived roles, consumers erect boundaries between themselves and different stakeholders in the healthcare value chain which influence the relationships between concern and trust and willingness to disclose.

H5: The requesting stakeholder moderates the relationship between concern regarding the electronic storage of PHI and willingness to provide access to digital PHI such that the more trust the individual has in the stakeholder, the negative relationship between concern and willingness to provide access will be attenuated.

H6: The requesting stakeholder moderates the relationship between trust in the electronic medium and willingness to provide access to digital PHI such that the more trust the individual has in the stakeholder, the positive relationship between trust in the medium and willingness to provide access will be attenuated.

As noted previously, the benefit side of the privacy calculus normally consists of an assessment of the individual's trusting beliefs which can balance or offset risks and concerns associated with disclosure (Dinev and Hart 2006; Malhotra et al. 2004). Dinev and Hart (2006) were the first to add a measure for personal interest in obtaining access to content, gauging its influence on willingness to disclose personal information over the Internet. Their findings suggest that personal interest in Internet content can override concerns related to providing information in that context (Dinev and Hart 2006). However, they also point out that research is necessary to further explore the influence of interest in more specific contexts. To the degree that an individual's health status emotion reflects their own personal need for health-related

information, we expect an influence from the individual's health status emotion on willingness to provide access.

An individual's health is closely tied to emotions, particularly when one is diagnosed with an illness such as cancer or lung disease (Koyalli 2005; Trumbo et al. 2007). These types of medical outcomes can result in depression (Koyalli 2005) and increased anxiety (Trumbo et al. 2007). While much of the work on decision making under risk and uncertainty involves cognitive evaluation of the severity and likelihood of available alternatives, the influence of emotion in this context has also been documented (e.g. Loewenstein et al. 2001; Loewenstein 2005). People make choices in "the heat of the moment" that they might not have made if they had "counted to 10" which suggests the often dominant influence of emotion over cognitive evaluation. The *risk-as-feelings* perspective provides an explanation for individual behaviors that allows for emotional influences such as worry, fear, dread, or anxiety (Loewenstein et al. 2001).

Loewenstein et al. (2001) propose a distinction between *anticipated* emotions and *anticipatory* emotions. *Anticipatory* emotions are visceral reactions to risks (e.g. fear, anxiety) while *anticipated* emotions are not currently experienced but are expected to be at some point in the future (Loewenstein et al. 2001). The emotion construct in Figure 3.1 represents the *anticipatory* emotions individuals have involving their health status, as these types of emotions have determinants that are different from those of *anticipated* emotions which tend to be more cognitive in nature (Loewenstein et al. 2001), and are reflected in the concern construct.

Individuals suffering from a serious medical condition often experience visceral, negative emotions related to their health condition (Koyalli 2005; Trumbo et al. 2007; Lowenstein et al. 2001). They have more vivid mental images of the illness and its effects on their day-to-day functioning, which may disproportionately weigh on decisions related to their health (Damasio 1994; Lowenstein et al. 2001).

Emotions can induce a state of insensitivity to probability variations, which can lead individuals to focus more on the desire to improve their health and feel better when choosing to disclose information, even though the probability of realizing a health improvement is actually lower than the potential privacy risk in disclosing health information (Lowenstein et al. 2001). In other words, in a state of illness, the overriding emotion one experiences is to get better, and everything else becomes less salient in decision making. Finally, people tend to experience increased fear when an outcome is closer to realization and behaviors can change as a result (Lowenstein et al. 2001). People in a negative mood often make judgments that tend to continue the negativity (Raghunathan and Pham 1999). In the context of one's health, if an individual is sick it is likely that she will believe she may become sicker and soon need increased care or benefit from research. An otherwise healthy person sees these outcomes (i.e. the necessity for healthcare or research) as far off in the future. Therefore, the healthy person is less likely to be influenced by emotion related to his health condition. This relationship between emotion associated with one's health condition and willingness to provide access to PHI is summarized in the following hypothesis:

H7: An individual's emotions regarding his/her current medical state negatively influences willingness to provide access to digital PHI. Specifically, the more negative (i.e. sad) an individual feels about his health, the more willing he is to provide access.

If emotion is indeed an important factor in the health information privacy context as we have argued, it is also important to determine if individuals are able to accurately predict the extent to which the emotion may influence their willingness to provide access. Studies have shown that individuals are often unable to accurately assess the full impact of emotion on their decision making ability (Giordano et al 2004; Van Boven and Lowenstein 2003; Read and Lowenstein 1999; Van Boven et al 2004). In the health setting, the cold-to-hot empathy gap has been suggested as responsible for non-adherence to drug regimens because people who begin to feel better (i.e. are in a “cold” state) do not understand that they may still be sick (e.g. require medication for bipolar disorder) and are unlikely to fully appreciate how bad their condition could get without the medication (i.e. the “hot” state) (Loewenstein 2001). The ramifications of this gap for policy regarding PHI privacy protection in terms of the timing of consent are significant. For example, if an individual is asked to make the decision about whether or not to make his information available for potential research purposes (e.g. clinical trial research) when he is in a healthy condition (i.e. a “cold” state), his over-riding concerns may be for loss of privacy and he may refuse to disclose information. Whereas if the individual was fighting terminal cancer (i.e. in a “hot” affective state) when asked if he was willing to disclose PHI for potential research purposes, he may choose to disclose his information in hopes of finding a cure or prolonging his life. A prospective empathy gap is one that occurs when individuals try to imagine themselves in an emotional

state different from their current one and then predict their future behavior. If an individual is asked to predict his willingness to disclose under a different emotional state and underestimates the extent to which his decision will be influenced by emotion, this would illustrate the existence of a prospective cold-to-hot empathy gap in the context of health information privacy (Lowenstein 2005):

H8: Individuals mis-predict the extent to which their emotional state regarding their medical condition influences willingness to provide access to digital PHI. Specifically, individuals currently diagnosed with cancer will report a significantly higher willingness to provide access to a hypothetical “cancer diagnosis” scenario than will individuals without cancer.

We have theorized that individuals’ privacy calculus when deciding whether or not to disclose health information in an electronic storage format is influenced by situational risk factors including the type of information requested, the intended purpose and requesting stakeholder. In addition, due to the highly sensitive nature of one’s health, the decision to disclose health information is influenced by emotion which is difficult for people to accurately predict. The empirical study conducted to test these assertions is described next.

3.4 METHODS

3.4.1 Sample and Data Collection

Our empirical strategy involved a scenario-based, repeated measures, quasi experiment where subjects are presented with hypothetical scenarios and asked to indicate how they would respond (Rosenthal and Rosnow 1984). This approach is commonly used in the marketing literature (e.g. Brady et al. 2005, Rick et al. 2008). The sample for the study is drawn from the target population of the general adult

public⁴ and constructed to be representative of the general US population. In addition, to appropriately test Hypothesis 8, a proportion of the sample is purposively selected to include a subset of respondents who were diagnosed with cancer. We collected data using an electronic survey administered by a third party organization based on the demographic characteristics of the sample we requested.

The survey provided contextual information on what the digital health exchange of information could look like to ensure that each respondent completed the survey with a common understanding of the core issue. Through a variety of scenarios, each respondent indicated his/her willingness to disclose PHI for three types of information (general, genetic, and mental health), three purposes (marketing, research, and patient care) and three requesting stakeholders (hospital, pharmaceutical company and government/public health agency), resulting in a total of 27 scenarios (see Appendix F). To eliminate ambiguity, the survey provided explicit definitions and examples of each type of information, purpose of use and requesting stakeholder. To infuse realism, we adapted scenarios from the HISPC documentation which has been validated across 33 states and 1 territory (Dimitropoulos 2007).

To test for the existence of an empathy gap in the health privacy context, we developed a hypothetical scenario similar to the ones used in prior empathy gap studies (Giordano et al 2004; Van Boven and Lowenstein 2003; Read and Lowenstein 1999; Van Boven et al 2004) (see Appendix F). Unlike the previous scenarios in which only the type of information, requesting stakeholder and intended purpose were

⁴ The adult population includes everyone 18 years and older. The provision of health information about minors requires parental consent (OCR 2003)

manipulated, the individual in this scenario is asked to imagine that s/he has been diagnosed with cancer. The respondent is then asked to indicate his/her willingness to provide health information for the purpose of research using the same scale as in the other scenarios.

3.4.2 Operationalization of Variables

Measures were adapted from prior studies and multi-item scales were used to improve reliability and validity of measurement. Willingness to disclose is measured using three items on a 7 point semantic scale anchored with unlikely/likely, not probable/probable, and unwilling/willing. We adapted items from Dinev and Hart (2006) to measure trust in electronic storage as a medium for personal health information and electronic health information privacy concern. Each item involves a statement that is either positive or negative and the respondent utilizes a 7-point Likert scale to indicate his/her level of agreement with the statement. We utilized 15 items from the Health Emotion Scale (Bowman et al. 2006) to measure anger, disgust, fear, sadness, and joy related to an individual's current health status. This scale, developed to assess primary emotion expressed by physically ill patients taps into the anticipatory, visceral emotions described by the *risk-as-feelings* literature as opposed to a more thoughtful, reasoned response. The instrument asks the respondent to think about how s/he is currently affected by her/his health and then to indicate how each item expresses her/his feelings. The instructions ask the respondent not to dwell on the statement and that it is best to respond immediately.

The survey also appropriates demographic variables including age, gender, race/ethnicity, income and education level. To exclude variance explained by

potential confounding factors, we gathered information related to exposure to media coverage of privacy, and prior experience with privacy violations (Malhotra et al. 2004). An individual's altruistic tendencies have been associated with organ donation (Morgan and Miller 2002); therefore, we control for the influence of helping and giving behavior as it could influence information disclosure decisions for research purposes. As trust in electronic storage as a medium is a central study variable, we also control for an individual's trust propensity (McKnight et al. 2002). We also included a list of common chronic illnesses and asked the respondents to indicate if they suffered from each one (e.g. diabetes, back pain, asthma, cancer). Finally, we control for the potential influence of the respondent's current medical history by using the number of doctor appointments as a proxy for general overall state of health. See Appendix E for all measurement scales. Due to the complex nature of the survey content and its length, we conducted a pilot with 28 respondents to ensure the instructions were adequate and to determine any potential items for elimination. We made minor adjustments to the survey instructions as a result.

3.5 RESULTS

As with all self report data, there is the potential for common method bias. Thus, we implemented the procedural remedies recommended by Podsakoff et al. (2003) including assuring respondent anonymity, providing contextual information and definitions to reduce ambiguity, and informing respondents that there were no "right or wrong answers." We also varied the item scale endpoints and formats between the predictor and criterion measures. In addition, we conducted an exploratory factor analysis as suggested by Podsakoff et al. (2003) which yielded 6

separate factors (consistent with the number of constructs and controls in the model). No single factor explains the majority of covariance among the measures indicating that common method biases do not present a significant problem with the data.

We obtained data from 1,089 respondents. The third party service organization assures an average 20% response rate and does not provide specifics on how many individuals received invitations to participate in the survey. However, because we acquired numerous samples in our efforts to achieve national representativeness and to obtain responses from individuals with cancer and were aware of the timing of email reminder notifications, we were able to do sub-sample comparisons and early/late responder comparisons as recommended by Rogelberg and Stanton (2007). No significant differences were found between the summated scales for the sub-samples or early versus late responders, reducing the possibility of non-response bias (Armstrong and Overton 1977; Rogelberg and Stanton 2007).

The demographics of our sample closely resemble that of the U.S. population (U.S. Census 2006) in terms of age, education, race/ethnicity, gender, and income distribution (Table 3.2). Almost half (46.9 percent) of respondents rate their computer skills as quite extensive or very extensive which indicates a familiarity with technology. In addition, the average number of years of computer experience is 14.64. Almost one third of respondents rate their own health as very good or excellent, another third rates it good, while the remaining third rates their own health as fair or poor which suggests a broad range of perceived health status. Finally, 313 (28.7%) respondents report having cancer.

Descriptive statistics for the research constructs are shown in Table 3.2. Cronbach's alpha for the study scales are .80 or above indicating that the measures are reliable. A confirmatory factor analysis performed in SPSS supports the convergent and discriminant validity of the scales (see Appendix G). We created indices for the study variables to be used in the remaining analysis.

3.5.1 Boundary/Contextual Considerations

We use a repeated measures ANCOVA analysis to test the influence of type of information, purpose and requesting stakeholder. This is an appropriate test for assessing differences in judgments of the same individuals over a variety of conditions (Potter and Balthazard 2004; Thatcher and De La Cour 2003). A repeated measures analysis reduces the unsystematic variability in the design by controlling for individual differences, thereby providing greater power to detect effects (Grabe and Westley 2003; Rencher 2002). Thus, we compare an individual's within subject willingness to provide access to the three types of PHI (general, genetic and mental health) for three purposes (marketing, research and patient care) to three different stakeholders (hospitals, pharmaceutical companies and government/public health agencies). We include electronic health information privacy concern and trust in the electronic storage medium as between subjects factors in the empirical model. To do so, we divide respondents into groups based on their scores on the concern and trust indices. Individuals above the mean on the concern index are placed into the high concern group. Similarly, individuals above the mean on the trust index are placed into the high trust group.

In addition, we include negative and positive emotion, gender, age, race/ethnicity, income, education, experience with past privacy violations, media exposure, trust propensity and altruism as covariates in the model. We test for violations of sphericity with Mauchly's test of sphericity. With repeated measures ANCOVA it is important to make adjustments if the variance-covariance matrix of the dependent variables indicates significant differences in variances between conditions (Field 2000). We utilized the Greenhouse and Geisser (1959) estimates to obtain a correction factor that assesses the observed F-ratio. Results are reported in Table 3.3⁵.

The data supports two way interactions between purpose and concern regarding the electronic storage of PHI ($F_{1.82,1842}=9.398$; $p=.000$) and purpose and trust in the electronic storage medium ($F_{1.82,1842}=5.825$; $p=.004$). These interactions are depicted in Figure 3.2. Contrasts indicate that the differences in means between the research and marketing purposes at high and low levels of concern are not significantly different ($F=3.391$; $p=.066$). However, the mean levels for the patient care purpose are significantly different from both the research purpose ($F_{1.82,1842}=12.774$; $p=.000$) and the marketing purpose ($F_{1.82,1842}=14.521$; $p=.000$). The negative relationship between concern and willingness to provide access is attenuated for patient care purposes. Thus, hypothesis 3 is supported. When requests are made for marketing or research purposes, the negative relationship between concern and willingness to disclose is enhanced.

⁵ A fixed effects regression with clustered standard errors to correct for intercorrelations due to multiple observations from the same individual yields results that are consistent with the ANCOVA

Contrasts related to the interaction between purpose and trust in the medium indicate that the differences in means between the research and patient care purposes ($F_{1.82,1842}=11.306;p=.001$) and the research and marketing purposes ($F_{1.82,1842}=5.764;p=.017$) at high and low levels of concern are significantly different. The means between the patient care purpose and marketing are not significantly different ($F_{1.82,1842}=1.450;p=.229$). If the request for PHI is made for the purpose of research, individuals with higher levels of trust in the medium are more willing to provide access and those with lower levels of trust in the medium are less willing to provide access than when the request is made for patient care or marketing purposes. The findings seem to suggest that trust in the electronic medium might be most important in encouraging individuals to disclose information for research purposes. Although the contrasts do not indicate significant differences in the mean levels of willingness to provide access between patient care and marketing at high and low levels of concern, individuals are less willing to provide access for marketing purposes. Due to the decreased significance of the positive relationship between trust in the electronic medium and willingness to disclose for the patient care purpose compared to the research purpose, hypothesis 4 is supported.

In addition, the data supports two way interactions between stakeholder and electronic health information privacy concern ($F_{1.97,1993}=7.606; p=.001$) and stakeholder and trust in the medium ($F_{1.97,1993}=3.301; p=.038$). These interactions are depicted in Figure 3.3. Contrasts indicate that the mean levels for government/public health agencies are significantly different from both hospitals

($F_{1.97,1993}=11.469;p=.001$) and pharmaceutical companies ($F_{1.97,1993}=14.164;p=.000$) at low and high levels of concern. If the request for PHI comes from a government/public health agency, individuals with higher levels of concern reduce their willingness to disclose compared to individuals with low concern significantly more than individuals do when the request comes from a hospital or pharmaceutical company. The mean levels of willingness to provide access are not significantly different when the request is made by a hospital or pharmaceutical company ($F_{1.97,1993};p=.620$). Consumers indicate hospitals are among the most trusted stakeholders when it comes to owning and operating electronic health systems while the government and for profit organizations are less trusted to take such a role (Global Strategy Group 2007). Due to the enhanced negative relationship between concern and willingness for requests coming from government/public health agencies as compared to hospitals, the data suggests support for hypothesis 5. The fact that no significant difference exists between the levels of willingness and concern between hospitals and pharmaceutical companies may suggest that consumer decisions regarding willingness to provide access to PHI is determined not solely based on trust but that other factors related to the perceived role of the stakeholder in the healthcare value chain may also be important.

Contrasts related to the interaction between stakeholder and trust in the electronic medium indicate that the differences in means between hospital and pharmaceutical companies ($F_{1.97,1993}=4.766;p=.029$) and hospitals and government/public health agencies ($F_{1.97,1993}=4.775;p=.029$) at high and low levels of concern are significantly different. The means between pharmaceutical companies

and government/public health agencies are not significantly different ($F_{1,97,1993}=1.997;p=.158$). If the request for PHI comes from a government/public health agency or pharmaceutical company, individuals with lower levels of trust in the medium reduce their willingness to disclose compared to individuals with high trust significantly more than when the request comes from a hospital. The positive relationship between trust in the medium and willingness to provide access is attenuated for requests from hospitals, which is consistent with hypothesis 6.

The interactions between type and electronic health information privacy concern ($p=.277$) and type and trust in the electronic medium ($p=.166$) are not significant. Thus, hypothesis 1 and 2 are not supported.

3.5.2 Emotion

To determine if there is an influence of emotion on willingness to provide access to PHI, we examine the results of the between-subjects portion of the ANCOVA (see table 3.3). As hypothesized, negative emotions are significant ($F_{1,1012}=42.218;p=.000$) in the model. Individuals who are feeling more negative about their current health status are more willing to provide access to PHI than those who are feeling less negative. Positive emotions do not significantly influence willingness ($F_{1,1012}=2.243;p=.135$). These findings support hypothesis 7. Of the controls included in the model, altruism and trust propensity significantly increase an individual's willingness to provide access, while higher levels of education and exposure to media reports about use and potential misuse of health information decrease willingness.

Our final analysis related to the role of emotion in PHI disclosure relates to evidence for the existence of an empathy gap in the context of privacy. Following past empathy gap research, we asked each respondent to read a hypothetical scenario requiring the respondents to imagine themselves in a state evoking emotion and then respond to related questions (Read and Lowenstein 1999; Van Boven and Lowenstein 2003; Van Boven et al. 2004). The hypothetical scenario is administered to two sets of respondents: one set that is in a state emotionally similar to the hypothetical scenario and one that is not. Comparison of the two groups provides evidence of the empathy gap. For our purposes, we compare responses to three items measuring willingness to provide access to PHI in a hypothetical “cancer-diagnosis” scenario (see Appendix F for the complete question) between respondents in our sample who currently have cancer and those who are cancer-free.

Although the third party organization we used to obtain our sample maintains information on a variety of health-related factors for their panel members and could identify panel members with cancer, we did not rely on the self-reported information because cancer can be effectively “cured” or in remission at any given time. Therefore, we used the respondents’ answer to the set of chronic conditions provided at the end of our survey, which included cancer, to place them in either the cancer or cancer-free group.

A cancer diagnosis is associated with a variety of negative emotions including anxiety and depression (Trumbo et al. 2007), and is considered a “hot state”. These two groups in our sample vary significantly in their levels of positive and negative emotions. The cancer group has significantly higher levels ($F_{1,1018}=16.975;p=.000$) of

negative emotion ($M=2.520$) as compared to the cancer-free group ($M=2.225$) and significantly lower ($F_{1,1018}=6.041;p=.014$) positive levels ($M=3.061$) of emotion as compared to the cancer-free group ($M=3.232$) which supports the notion that the cancer group is in a “hot state”.

An ANCOVA comparing responses between the two groups indicates people who have cancer indicate a significantly higher ($F_{1,1015}=7.171;p=.008$) willingness to provide access to PHI (Mean=5.370) to pharmaceutical companies for clinical trial research if they were hypothetically diagnosed with cancer than people who do not currently have cancer (Mean= 5.060). This suggests that people are unable to accurately predict how the emotion associated with a cancer diagnosis may influence their privacy decisions since people who do not have cancer indicate a significantly lower willingness when compared to those who do. We controlled for individual level factors such as gender, age, education, income, race/ethnicity, media exposure, prior privacy violations, altruism, trust propensity, electronic health information privacy concern and trust in the electronic medium. Hypothesis 8 is supported.

3.5.3 Discussion

Overall, empirical results support six of the eight hypotheses and collectively suggest that contextual factors related to the requesting stakeholder and the purpose for which the information is being requested play an important role in moderating the relationships of the privacy calculus, i.e., the effects of electronic health information privacy concern and trust in the electronic medium on willingness to provide access to digital PHI. As theorized, individuals erect boundaries around their electronic PHI and apply different rules to determine whether or not to disclose their electronic PHI

depending on the risk domains made salient by the contextual factors. Further, we find evidence that emotion plays a pivotal role in PHI disclosure: individuals with negative emotions involving their current health status are more willing to disclose PHI. Individuals are also unable to fully comprehend the extent to which a negative diagnosis and the associated emotion may influence their privacy decisions.

Our predictions related to the moderating effect of type of information requested in the privacy calculus were not supported. Not only does type of information not moderate the relationships, we find that type of information does not have a significant main effect on willingness to provide access to PHI. Our expectation for moderation was based on the argument that different types of health information are differentially sensitive and may result in varied levels of loss, hence, risk. Although counter-intuitive at first glance, and inconsistent with prior work that has found differences across, for example, financial and purchase information (Malhotra et al, 2004), a plausible explanation for this is that *all* types of health information are sensitive. It may be the case that individuals do not distinguish between different types of health information and believe that the entire set represents the same level of privacy risk, thereby rendering the main effect of type of information insignificant. This explanation merits further investigation by examining, for example, health information and financial information in the same study.

3.6 LIMITATIONS

Prior to discussing the implications of our findings, several limitations of the study deserve consideration. Although our sample closely matched the U.S. census

demographics which improves the ability to generalize our findings to the U.S. population, the survey was administered online and therefore, respondents represent individuals who have access to the Internet. Future studies should include hardcopy survey and/or telephone interview methods to reach individuals who may not have access to computers as their concerns, trust and willingness to disclose in a digital environment may be different from individuals with more experience with such environments.

Another limitation relates to our measurement of intentions as opposed to actual behavior. Intentions have been shown to be a strong predictor of actual behavior (Sheeran 2002; Venkatesh et al. 2003; Webb and Sheeran 2006) and have also been commonly used as a proxy for actual behavior in information privacy studies (Dinev and Hart 2006; Malhotra et al. 2004; Son and Kim 2008). Nonetheless, a fruitful avenue for future study is to pursue methods that enable examination of consumer privacy behavior in healthcare settings. However, at this point in time, it would not have been possible for us to have realistically designed a study to accurately assess the actual behavior of interest to our research questions. As mentioned in our introduction, the current healthcare landscape is such that physicians and payers largely control PHI. Once consumers become more empowered and legislation evolves, the full benefits of digitization will be realized. Our study was intended as an initial step toward gauging consumer concerns and the factors influencing disclosure in a reality where the consumer has expanded control over the access and use of their own PHI. As such, our scenarios involved an element of forward-thinking.

While we endeavored to examine risk specific variables such as type of information and purpose of use to gain a more granular understanding of privacy concerns, our stakeholder manipulation remained at a general level (e.g. non-specific hospital, pharmaceutical company). This was consistent with our goal of detecting individual differences between disclosing PHI to different categories of stakeholder (i.e. care provider, for-profit company, government agency). It does not enable us to address concerns individuals may have related to specific entities such as the Veterans Administration, Pfizer or the Mayo Clinic. Other studies have examined the role of vendor reputation (McKnight et al. 2002) or familiarity (Gefen 2000) as they relate to intentions to perform Internet transactions which were not the focus of our study. By focusing on the stakeholder in general, our research design eliminated the potential influence of particular entities thus emphasizing the category of the stakeholder. We would argue that both the category of the stakeholder in general and perceptions related to the specific stakeholder (e.g. YXX Memorial Hospital) are important for understanding user behavior and more research is necessary to understand the mutual influence of these factors.

As is a potential concern with any repeated measures design, our results may reflect the influence of order effects. To gain responses to each of the three types of information, three intended purposes and three stakeholders of interest to our research questions, respondents had to complete 27 questions regarding their willingness to provide access. Although respondents may have been subject to effects related to the ordering of the questions, they were consistently administered to all respondents. Counterbalancing the ordering of questions is one technique for avoiding systematic

order effects with a small number of conditions but quickly gets difficult to manage as the number of possible combinations increases and was, therefore, infeasible in our case. Indeed, counterbalancing and randomizing conditions do not always control for order effects and should be utilized in cases where there is reason to believe the effects are significant enough to subsume or inflate the treatment effects (Cohen 1995; Reese 1997). Moreover, we do not have reason to believe that any group of interest in our study (e.g. low/high concern or low/high trust) is any more sensitive than any other to carryover effects (e.g. practice, fatigue, contrast or assimilation) which suggests our approach of administering the scenarios consistently to all respondents is reasonable (Cohen 1995).

Finally, our analysis comparing the answers to the hypothetical cancer scenario between respondents with and without cancer assumes that respondents answered the question related to chronic illnesses honestly. We have no way to independently verify their physical state/diagnosis. Respondents completed the surveys anonymously which effectively eliminates the possibility that an individual's chronic medical condition would inadvertently be disclosed. The comparisons of positive and negative emotions across these two groups are consistent with cancer patients experiencing more negative emotions (Trumbo et al. 2007) which support a suitable grouping of respondents on this factor. While we find evidence of an empathy gap between these two groups, it is likely that similar bias exists between patients with other chronic diseases such as diabetes. Further research could test the boundaries of our findings as they relate to other illnesses.

3.7 IMPLICATIONS AND CONCLUSION

There is little else that is as consequential to an individual as his or her own health. As healthcare becomes increasingly digitized, the promise of improvements enabled by technological advances must be weighed against any unintended negative consequences. There is much value, then, to be realized in drug discovery, medical research, and public health policy if consumers are willing to allow their health information to be electronically stored and manipulated. We asked the question: Under what circumstances will individuals be willing to disclose PHI and allow it to be digitized? It is a question that must be answered in order to craft appropriate policy and encourage usage of HIT in the future.

In this study we noted that healthcare affords an optimal setting to study privacy concerns for multiple reasons, including the highly sensitive nature of health information and the number of stakeholders with a vested interest in gaining access to consumer health information for a variety of purposes. The risks faced by the discloser of health information are diverse (Beckerman et al. 2008). In addition, unlike in retail or financial settings in which much prior privacy research has been conducted (e.g., Dinev and Hart 2006), an individual's health status involves strong emotion (Trumbo et al. 2007) which can influence decision making (Loewenstein 2005). We discuss the theoretical and practical implications of our findings.

3.7.1 Theoretical Implications

The study contributes to theory in two key ways. First, we introduce and reason about the moderating influence of two situational risk factors -- intended purpose and requesting stakeholder -- on the relationships between electronic health

information privacy concern and willingness to disclose PHI and trust in the electronic medium and willingness to disclose. Second, we explicitly incorporate emotion into the privacy calculus.

Previous privacy research has focused on either one of the two situational risk factors at a time, such as willingness to disclose information for the purposes of personalization (Awad and Krishnan 2006) or to disclose in order to obtain a service (Dinev and Hart 2006) or to disclose to a particular fictitious vendor (Malhotra et al. 2004), or has focused on the main effects of vendor reputations or familiarity (Gefen 2000; McKnight et al. 2002). We examine the nuanced interactive influences of the relationships simultaneously in one study. Our model provides a framework for understanding which factors influence individual beliefs about the use of a general technical format (i.e. electronic storage) in a specific context (i.e. healthcare). While the healthcare context with its multiplicity of stakeholders and their distinct objectives provided a fertile setting in which to perform initial tests of these relationships, future investigations could explore whether or not these relationships hold in financial or purchase history contexts.

Although the majority of research on judgment and decision making is cognitive and consequentialist in nature (Harless and Camerer 1994; Tversky and Kahnemann 1984; Vroom 1964), the role of emotion is beginning to be acknowledged in domains outside of information privacy (Ariely and Loewenstein 2006; Loewenstein et al. 2001). To our knowledge, this study is the first to incorporate emotion into the privacy calculus. We focused on anticipatory emotions which are immediate visceral reactions because they tend to have different

determinants than those that drive cognitive evaluations (Loewenstein et al. 2001) and it was our belief that the healthcare context provided an extreme case in which to observe the relationship between emotion and willingness to provide access to information (Druckman and McDermott 2008; McDermott et al. 2008). Future studies could explore this relationship in other privacy settings such as the financial context. In addition, since emotion is linked with physiology, future studies could attempt to measure privacy concerns in clinical settings and, perhaps, obtain physiological measurements from the clinician in addition to the patient self-reported emotions.

Given that emotion is a factor in an individual's willingness to disclose PHI, interesting avenues for future research include determining the boundary conditions for this relationship. For example, does the health status of a close loved one (e.g. a child, parent or spouse) and the subsequent related emotion influence an individual's willingness to provide access to PHI for clinical trial research? Similarly, it seems plausible that altruism may play a stronger role in influencing the willingness to disclose for the purpose of research than for the purpose of one's own care which represents an interesting question to explore. Other areas for future exploration involve the role of financial and social incentives, which might be viewed as extensions to the privacy calculus. In addition to the potential benefits the individual perceives as inherent in requests for access to PHI for patient care, research or marketing, organizations could increase the benefits by providing individuals with monetary rewards in exchange for access to their information. However, studies have suggested that individuals are somewhat unwilling to sell their information to websites (Hoffman et al. 1999; Ward et al. 2005). It may be that a combination of

monetary incentives and interactions that form a social exchange contract (e.g. newsletters sharing research findings) are most effective at increasing individual willingness to provide access to PHI (Ward et al. 2005).

3.7.2 Practical Implications

As we move forward toward a goal of electronic health records for all U.S. citizens by 2014, it is essential to understand what roadblocks stand in the way of progress and to understand the ramifications of such progress. The practical implications of the study include an improved understanding of consumer concerns regarding the electronic storage of health information. A particularly striking result is the finding related to the influence of negative emotion on individual willingness to disclose PHI. Individuals who feel sad, angry and anxious about their current health status are more willing to provide access to their PHI and are, thus, more vulnerable to opportunistic requests for their information. However, people in an unemotional state may feel strongly that they don't want to be a "lab rat" or "guinea pig" until it is their own life at stake in which case the emotion involved with facing their own death influences their decision in a direction that may benefit that individual. At a societal level, the findings related to emotion and the empathy gap in the health information privacy context create difficult questions about the timing of consent – questions that must be resolved before policy can be made. If people's judgments vary with their emotions related to their health at a given point in time, should consent be sought at every interaction with a healthcare professional? If an individual is unduly influenced by emotion, they may make a decision which they may regret at a later point in time, when the private information already been disclosed to an unintended entity

(Loewenstein 2005). Thus, at the individual level, acknowledging the emotion in the privacy calculus may help individuals become aware of and minimize its influence on their behavior.

It is unsurprising that our findings indicate consumers are most willing to share information with hospitals and for the purpose of patient care. However, significant benefits stand to be gained from the digitization of health information for research and it is unlikely that all of that research can be conducted by hospitals. Our findings suggest that there may need to be more assurance of privacy and trust built in governmental agencies and pharmaceutical companies before consumers become comfortable with sharing information with such stakeholders. More research may be required to understand why consumers seem particularly concerned about sharing information with the government/public health agencies as opposed to hospitals and pharmaceutical companies. Consumers stand to gain from appropriate research efforts and marketing campaigns if conducted in a way that is sensitive to their needs. Relatedly, a striking finding revealed that trust in the electronic medium is more important when a request is made for research purposes than when a request is made for marketing or patient care purposes. Perhaps this reflects an underlying negative bias individuals have regarding participation in research, a supposition that warrants more study.

3.7.3 Conclusion

The objective of this study was to shed light on a vexing problem facing the healthcare industry with respect to digitization: rising privacy concerns about personal health information. Drawing upon privacy boundary theory and the risk-as-

feelings perspective we sought to gain a broad-based understanding of individuals' privacy calculus in the healthcare context. Our theoretical model simultaneously examined a broad range of contextual variables that may influence the risks that become salient to an individual. It further incorporated a hitherto overlooked determinant of information disclosure decisions that is arguably of especial significance in healthcare, viz., emotion. We proposed the existence of an empathy gap in PHI disclosure decisions, suggesting that individuals cannot accurately predict how their privacy decisions will change over time. Data from a nationally representative sample of over 1,000 adults support our core assertions and provide evidence for the complex nature of consumer health information privacy concerns. The results have both theoretical and practical implications. Policy makers can use this information to craft policies tailored to meet consumer needs. In addition, consumers can be segmented into groups for targeted marketing campaigns designed to, for example, either recruit consumers who are particularly open to sharing information for potential participation in clinical trials or educate particularly resistant consumers on the benefits and safety of electronic health records.

CHAPTER 4: THE INFLUENCE OF MESSAGE CUES ON COMPUTER USER SECURITY-RELATED OPTIMISTIC BIAS AND INTENTIONS

ABSTRACT

Contracting a computer virus can pose significant financial and social risks for consumers. Although many of the risks associated with online activity can be mitigated if users practice safe online behavior, surprisingly large numbers still do not take basic precautionary steps on a consistent basis. Studies consistently show the existence of an optimistic bias that leads individuals to believe they are less vulnerable to a security violation than the average other person. As a result, they are more likely to ignore the risks associated with unsafe online behavior. Using an experimental methodology, this study examines how appropriate message cues can be used to minimize user optimistic bias and increase security intentions. Building on prior research study 1 examines the interactive influence of situationally primed self-view and risk domain frame (stressing either financial risks associated with recovering from viruses such as costs related to paying for technical support and reduced productivity, or social risks such as embarrassment or disapproval related to unwittingly spreading viruses to friends) on security-related optimistic bias and intentions. Study 2 examines the interactive influence of self view and goal frame on the optimistic bias and related intentions. We find security intentions influenced in study 1 but not optimistic bias while in study 2 we find the opposite (i.e. optimistic bias influenced but not intentions). The implications of the findings are discussed.

4.1 INTRODUCTION

The message that popped into Laurie Gale's Facebook inbox last month seemed harmless enough — a friend had seen a video of Ms. Gale and had sent a link so Ms. Gale could view it. The link led to a video site that prompted her to update her video software, which she did. "Within seconds, everything started shutting itself down," says Ms. Gale. It took a trip to the local computer repair shop and several phone calls to Dell customer-service representatives for her to restore the computer to its factory settings. (De Avila 2009)

Winny, a popular peer-to-peer application in Japan, is prone to malware infestations that can cause serious data leaks. Unlike in most countries, malware authors in Japan are not motivated by money - - instead authors seek to expose or delete sensitive data on machines. (PR Newswire 2008).

The negative impacts of computer viruses on consumers are wide ranging and include, for example, social risks if embarrassing information is leaked to inappropriate sources and financial risks if the resulting damage requires recovery of hardware and software. The risks of home computer users contracting viruses are manifold and extend beyond the individual to impact organizations in a number of ways. For instance, individually owned computers can become bot-infected and used to launch denial of service attacks against organizations, rendering the organization's website inaccessible and causing detrimental financial consequences (Krebs 2005; Garg 2003). Indeed, a leading security vendor reported over 6 million bot-infected computers during the last half of 2006 (Turner 2007). Furthermore, violations such as identity theft can lead to a loss of confidence in consumers' overall willingness to transact business online (Borrus 2005). Collectively, the magnitude of risks for both individuals and organizations make the minimization of the spread of computer viruses a priority. Indeed, cybersecurity is now a priority of the Obama administration as reflected in the creation of a new office at the White House to

integrate policies and coordinate responses for the government (Cyberspace 2009; Krebs 2009).

Despite the considerable effort on the part of software vendors to create technology to improve security, individual users have an equally if not more significant role to play in creating and maintaining a secure environment (Sasse et al. 2001; Stanton et al. 2005). Many of the risks associated with online activity can be mitigated if users take actions such as consistently updating their antivirus software, installing and running effective firewalls and exercising care when opening emails and attachments. Disturbingly large numbers of users still do not take these basic steps on a consistent basis (Roberts 2004; Turner 2007). Although home users were the target of ninety-three percent of targeted attacks in the last six months of 2006 (Turner 2007), paradoxically, many still believe they are less vulnerable to a security violation than the average other person (Campbell et al. 2007; Loch et al. 1992; Rhee et al 2005; West 2008). These findings support the notion that computer users exhibit an optimistic, or self-positivity, bias when assessing their level of personal vulnerability. Optimistic bias is a systematic tendency to view others as more susceptible to risks than the self. This bias is fundamentally a defensive distortion that could undermine appropriate preventive action (Scharzer 1994). Research in other contexts reveals that such bias is manifest in diverse settings and can lead to behaviors that are potentially harmful for the self (Kahn and Luce 2006; Menon et al. 2002). In the context of online security, it is easy to see how such an optimistic bias can limit the ability to mitigate risk and fully leverage the benefits of technology.

In the current study, we investigate ways to minimize computer user optimistic bias and increase security intentions via message appeals. The marketing literature is rich with research that explores the factors influencing consumer decision making and choice behavior using message cues (e.g. Aaker and Lee 2001; Lee et al. 2000; Menon et al. 2002). In the specific context of information systems security, there is evidence to suggest that individuals respond to trade press messages. For instance, Campbell et al. (2003) show that the market reacts with a significant negative response to major newspaper announcements of information security breaches involving confidential data, suggesting the existence of a relationship between trade press messages and the investing community. It is possible then, that computer users will be responsive to targeted persuasive message cues. We focus on identifying specific combinations of message manipulations designed to minimize optimistic bias and increase security intentions

What factors are likely to influence security optimistic bias? Research suggests that self-view, a perception of oneself that is either independent or interdependent, exerts influence on optimistic bias (Heine and Lehman 1997; Kitayama et al. 1997). Individuals with a dominant interdependent self-view focus more on their membership in a group context and as part of a collective, whereas individuals with a dominant independent self-view tend to place an emphasis on themselves as unique and distinct from others. Self-view can be either chronic, as when nurtured by a culture, or situationally activated, as when primed by a message (Aaker and Lee 2001), and is fundamentally a reflection of how the individual views herself in a social context. To the degree that there is an inherent social component to

the online context, it is possible that an individual may be influenced by whether she is primed to think of herself as independent or interdependent when thinking about her security behavior.

In addition, individuals tend to interpret more threatening statements with a higher level of optimistic bias (i.e., they believe themselves to be at lower risk than others) than they do less threatening statements (Kunda 1990; Lench et al. 2006; Smits and Hoorens 2005). Since individuals are more motivated to avoid a threatening event, the manner in which a message is framed may be highly influential.

In this paper, we report the results of two experiments which were conducted to determine if security-related optimistic bias and intentions can be influenced by message cue manipulations. Study 1 investigates the interactive influence of self-view and risk domain frame on security optimistic bias and related intentions. Risk domain frame involves varying the type of risk outcomes stressed in the message (e.g., financial versus social risks). Prior work has suggested that situationally primed self-view interacts with risk domain frame to influence choices (Mandel 2003). For example, interdependent-primed consumers were more risk-seeking in financial choices and less risk-seeking in social choices than were their independent-primed counterparts. However, the influence of these relationships on optimistic bias has yet to be explored. Study 2 investigates the interactive influence of self-view and goal frame on the dependent variables. Goal framing is a type of manipulation that involves emphasizing either the positive aspects of a behavior (i.e., a positive frame), or the negative aspects of not performing the behavior (i.e., a negative frame).

The majority of prior research on the reduction of optimistic bias has examined main effects, while the current study focuses on the more nuanced influence of interaction effects. In addition, prior research focuses primarily on understanding the persuasive influence of goal framing in health-related communications (e.g. Chandran and Menon 2004; Menon et al. 2002; Maheswaran and Meyers-Levy 1990). Given that an individual's choice behavior and persuasive propensity differs depending on the domain of risk including legal, financial and social (Rettinger and Hastie 2001), it is important to examine the potential influence of message cues on optimistic bias in the security context.

The study makes three key contributions. From a theoretical perspective, it elaborates on the relationship between goal frame and self-view to include its influence on optimistic bias which has not previously been demonstrated. Second, it establishes the interactive influence of risk domain frame and self-view on security behavioral intentions which isolates the influence of risk domain frame from context. Third, it extends marketing concepts to the information systems context thus providing insight on the boundaries and generalizability of message cue concepts. Finally, the findings from this study have practical implications for decisions related to social marketing efforts targeted toward increasing user security behavior.

The remainder of this paper includes a brief review of the relevant literature. Study 1 is then described in detail with its hypotheses, methods and results followed by Study 2. The paper concludes with a discussion of the implications of the combined study results.

4.2 THEORETICAL BACKGROUND

Optimistic bias exists in self-evaluations related to a variety of uncertain circumstances with negative outcomes such as susceptibility to health risk (Hoorens and Buunk 1993), crime (Perloff and Fetzer 1986) and car accidents (McKenna 1993). While optimistic bias is widespread, research shows the degree of bias can be influenced by chronic self-view (Heine and Lehman 1997; Kitayama et al. 1997) and a variety of factors related to the outcome under consideration (e.g. Gold and Martyn 2003; Klein and Helweg-Larsen 2002; Menon et al. 2002). The bias can be reduced with message cues including manipulations of the number and frequency of risk factors presented (Menon and Block 2002) and the timing of potential outcomes (Chandran and Menon 2004). In this study, we focus on the influence of situationally primed self-view and two forms of message frames: goal frame and risk domain frame. Prior to briefly describing the relevant literature in these areas, we present the specific context for the study.

As indicated in the introduction, individuals exhibit an optimistic bias when it comes to assessing their personal information security risks (Campbell et al. 2008; Loch et al. 1992; Rhee et al. 2005). This form of bias leads to an inclination toward interpreting uncertain or ambiguous situations in a self-serving manner. In the online context, individuals with an optimistic bias believe that the average other is more vulnerable to security risks than they are themselves. This is problematic as it likely contributes to how people choose to behave online. An individual who perceives himself to be at low risk of contracting a virus or falling victim to identity theft is less inclined to take the time and effort necessary to ensure that he is taking appropriate

precautions in his online behavior. Furthermore, his online behavior potentially has implications for all interconnected users of the Internet (Weaver et al. 2003).

4.2.1 The Influence of Self-View on Optimistic Bias

An individual possesses a chronic self-view that is nurtured by culture. Individuals with a dominant chronic interdependent self-view focus more on the individual's membership in a group context and as part of a collective whereas individuals with a dominant chronic independent self-view tend to place an emphasis on themselves as unique and distinct from others. Thus, self-enhancing biases born out of a desire to maintain a positive sense of uniqueness and self-esteem are more typical in North America and Western Europe where independence is stressed as part of the culture, and much less pronounced in Japan where feelings of belonging and even self-criticism are stressed (Heine and Lehman 1995). Prior research found optimistic bias attenuated or even reversed in cultures with dominant chronic interdependent self-views as compared to cultures with dominant chronic independent self-views (Heine and Lehman 1997; Kitayama et al. 1997).

Kitayama et al. (1997) provide support for a collectivist constructionist theory to explain the cross-cultural differences in self evaluations. They suggest that the Japanese tend to be more self-critical because of a focus on standards of excellence in relationships which highlight deficiencies and problems in meeting those standards. In contrast, American culture supports an autonomous view of the self which tends to motivate individuals to express and confirm unique and distinct attributes. This theory is based on situational definitions made available by the respective cultures which are then essentially habitualized by individuals (Kitayama et al. 1997).

Prior studies on the influence of self-view on optimistic bias involved *measuring* individual traits (i.e. chronic self-view). In our studies, we manipulate self-view via message cues. While we know of no studies specifically manipulating self-view to assess its impact on the optimistic bias, research shows that self-view can be situationally manipulated to produce effects similar to chronic self-view (Aaker and Lee 2001; Lee et al. 2000). In a series of experiments designed to determine if self-view and message framing interact to influence perceptions, Lee et al. (2000) found evidence of systematic differences in groups based on cultural chronic self-views. They then found that they could reverse these effects by situationally inducing a self-view which was opposite to the dominant chronic self-view. These results support the argument that the extent to which the interdependent or independent self is more dominant varies not only across cultures but also within an individual person depending on the specific view of the self that is temporarily activated (Lee et al. 2000).

Building on their findings, other researchers have successfully manipulated self-view to achieve effects on brand and website attitudes (Aaker and Lee 2001) and choice behavior (Hamilton and Biehal 2005). Drawing upon this work, in the current study, we examine the influence of self-view manipulation on the optimistic bias in the online security context.

4.2.2 The Influence of Message Framing on Optimistic Bias

Another explanation provided for the optimistic bias is based on the premise that people engage in motivated reasoning (Kunda 1990). Individuals are simply more motivated to avoid a threatening event and tend to interpret threatening

statements in a more self-serving way than they do less threatening ones (Lench et al. 2006; Smits and Hoorens 2005). This is consistent with loss aversion and the value function used in prospect theory which indicates that a response to losses that is more extreme than the response to gains (Tversky and Kahneman 1984). Numerous studies, frequently based on prospect theory, find that individuals respond differently to messages depending on whether they are positively or negatively worded (e.g. Block and Keller 1995; Maheswaran and Meyers-Levy 1990; Shiv et al. 1997). Decision outcomes are influenced by an individual's desire to avoid a loss more than the desire to realize an identical gain (Tversky and Kahneman 1984).

For a variety of positive (e.g. win the lottery) and negative valence (e.g. be robbed) outcomes, individuals interpret the likelihood of the event in a self-serving manner more for the negative valence outcomes than for the positive ones (Smits and Hoorens 2005). Lench et al (2006) found that unrealistic optimism and motivated reasoning extends to an individual's children. In particular, parents who display stronger levels of involvement and attachments to their children were more optimistic about their child experiencing positive outcomes, providing further supports the notion of motivated reasoning (Lench et al. 2006).

Given that evidence suggests the extent of the optimistic bias is sensitive to the outcome and how it is presented, it is logical to examine persuasive methods available to manipulate how the outcome is presented. We focus on two such message cues that have previously been examined in conjunction with self-view, though the influence of their combined effect on optimistic bias has not been examined to our knowledge. In study 1, we examine the interaction of self-view with

risk domain frame. In study 2, we examine the interaction of self-view with goal frame.

4.3 STUDY 1 – SELF-VIEW AND RISK DOMAIN FRAME

A significant amount of research examining how to minimize optimistic bias involves physical risk to the self (e.g. Chandran and Menon 2004; Menon et al. 2002; Maheswaran and Meyers-Levy 1990). For example, Menon et al. 2002 examined ways to decrease individual bias toward hepatitis risk and increase intentions to get tested for hepatitis. This is limiting, however, because there are many different types of risks individuals face, including financial, social, legal and psychological risks (Mandel 2003; Peter and Tarpey 1975; Rettinger and Hastie 2001). The decision making process varies depending on the domain of risk based on the importance, moral relevance and familiarity of the available choices (Rettinger and Hastie 2001). Studies also suggest that individuals differ in their mental representations of decisions based on content domain. Since memory and recall is different across domains of risk, it is possible that the decision strategy and type of information processing employed by the individual is also influenced (Rettinger and Hastie 2001).

Building on this stream of research, Mandel (2003) found subjects primed on interdependence were less likely to take social risks than financial risks. Subjects primed on interdependence identified more friends and family members who could help them in a financial crisis yet this heightened awareness of significant others simultaneously added pressure to avoid potential social embarrassment (Mandel 2003). The heterogeneity among individuals' responses to different types of risks has been formalized in the form of the *cushion* hypothesis (Weber and Hsee 1998, 1999)

which suggests that individuals with a larger social network can afford to take greater financial risks (Mandel 2003), and the *floodlight* effect that explains the reduced willingness to incur social risk when the presence of close others is made salient (Mandel 2003).

Mandel's (2003) study provides evidence of a relationship between situationally primed self-view and risk domain. However, in her study, context was varied along with risk domain. For example, she compared winning a lottery ticket (financial gain) to choosing a shirt to wear to a family gathering (social gain) and paying a parking ticket (financial loss) to playing truth or dare (social loss). While the financial and social ramifications of these pairs are quite distinct, the contexts and associated decisions to be made are also quite different across all four scenarios. Thus, it is difficult to isolate the effects of context from the effects of risk domain. Since certain behaviors in the online security context can pose both social and financial risks, this context offers the potential to isolate the risk domain effects from the contextual effects that could influence an individual's choice behavior. For example, while an individual is likely to incur lost productivity in the time required to recover his machine and/or incur costs to pay someone to recover data on a hard drive, it is also possible for the individual to experience social losses in the form of embarrassment or disapproval if the individual spreads a virus to a friend via the files on a thumb drive or if a virus sends spam to all the people in his address book. Messages can be tailored to stress either the financial risks associated with contracting a computer virus due to poor judgment in downloading files from the Internet or the social risks. In this study, we hold the context constant and manipulate

risk domain. In this way, we are able to isolate the effects of risk domain, and examine the interaction of risk domain and self-view in their effects on optimistic bias and security intentions.

Prior research has demonstrated that interdependent primed individuals indicate a larger number of individuals who can help in times of financial need than do independent primed individuals (Mandel 2003). These same individuals are more willing to risk financial loss than independent primed individuals. Since financial losses are fungible, the larger social network likely serves to provide interdependent primed individuals with a greater sense of control over the outcome of a potential loss as they feel they can share the burden with others. Consistent with the floodlight effect, individuals whose interdependent selves are activated are expected to take fewer social risks than those whose independent selves have been activated (Mandel 2003). This may be due in part to a lack of control over the number of potential observers to the negative social outcome leading to embarrassment or disapproval among one's family or peers. In addition, as a result of the salience of social norms, an interdependent primed subject is likely to feel more pressure to conform than an independent primed subject (Ybarra and Trafimow 1998). These factors which influence control, lead to changes in perceived vulnerability. The more an individual feels in control of a risk or event, the lower her perceived vulnerability which serves to increase the bias (Hoorens and Smits 2001; Klein and Helweg-Larsen 2002; Rhee et al 2005). The cushion hypothesis and the floodlight effect may serve to shift the degree of control the individual feels over the extent to which the potential loss will be experienced as described above.

Finally, since an interdependent self-view serves to focus an individual on herself as part of a collective, she is likely to feel more involved in a subject focusing on social outcomes. Increased involvement tends to lead to central processing (Aaker and Lee 2001; Petty and Cacioppo 1983). We anticipate individuals to exhibit increased memory, elaboration and persuasion in conditions in which central processing occurs (Petty and Wegener 1998; Petty and Cacioppo 1986). This more “thoughtful” processing should result in a lowered bias. Given that interdependent primed individuals will feel more control over the outcome of a financial loss, their sense of vulnerability will decrease, which serves to increase the optimistic bias. These same individuals will experience lower control over the outcome of a social loss and more involved in a message focused on social outcomes which increases their central processing of the message. Ultimately, their sense of vulnerability increases which will decrease their optimistic bias. Thus, under an interdependent self-view prime, a message is more persuasive in attenuating optimistic bias when it highlights the existence of a social as opposed to a financial risk. This reasoning yields the following hypothesis:

H1: Individuals primed with an interdependent (independent) self-view will report a lower optimistic bias when receiving a social risk-focused (financial risk-focused) frame than those primed with a financial risk-focused (social risk-focused) frame.

Prior research in contexts outside security has demonstrated a link between perceptions of self risk, optimistic bias and behavioral intentions. For example, by manipulating the types of behaviors listed in a message to make an individual feel more or less susceptible to an illness can increase or decrease their intentions to be

tested for the illness (Menon et al. 2002). In addition, making the possible negative outcome seem more proximal can decrease the bias and increase intentions to perform the appropriate behavior to mitigate risk. Kahn and Luce (2006) find that when individuals are expected to take repeated preventive actions such as wearing a bike helmet to avoid head injury in a potential accident, the false sense of security one gets from not having accidents over time and the hassle of taking the preventive measure can degrade intentions. These personal experiences influence one's perceptions of risk relative to others and can influence behavior. Collectively, these findings support a relationship between shifts in optimistic bias and corresponding changes in intentions. Therefore, we expect security intentions to be increased as the optimistic bias is lowered:

H2: Individuals primed with an interdependent (independent) self-view will report a higher level of intentions to perform security-related behaviors when receiving a social risk-focused (financial risk-focused) frame than those primed with a financial risk-focused (social-focused) frame.

4.3.1 Method

Ninety-nine students participated in an experiment in a laboratory setting. The target population is any user of an Internet-enabled computer and the sample consisted of undergraduate students from a large university enrolled in an introductory information systems course. Approximately half of the subjects were male (56%). To ensure subject involvement in the experimental task, student participants received partial course credit or extra credit for participation in the experiment in a lab setting. Participants were isolated from each other, and completed the experiment independently in an environment free from distraction.

A 2 (risk domain frame: social risk vs. financial risk) x 2 (self-view: independent vs. interdependent) factorial design was employed to test the research hypotheses. Subjects participated in computer labs equipped with computers that enabled them to access the experimental scenarios, which were assigned at random, and responded to the post-questionnaire electronically. We manipulated both self-view and risk domain frame via website content.

Risk Domain Frame Manipulation. The manipulations were conducted via asking the subjects to review a website (see Appendix H for the manipulations). The results of recent studies of online behaviors aided in determining the content of the website manipulations (CISCO Systems 2006; Russell Research 2006). We chose to focus the message on the risks associated with contracting a virus based on file downloading behaviors. Eighty-three percent of adults who engage in online social networking admit to downloading questionable files from other people's profiles (Russell Research 2006) while 6% of employees indicated they continue to open attachments received in emails from unknown sources (CISCO Systems 2006). These statistics suggest users still have much to learn with regard to caution when downloading files from the Internet, and these behaviors are ones over which they have control making this a attractive target behavior for our message. We measure intentions due to the difficulty associated with measuring actual behavior in the security context (Vroom and Von Solms 2004).

Self-View Manipulation. The self-view manipulation is accomplished using both text and graphics on the website (Aaker and Lee 2001). Text in the independent conditions focuses on the individual through the use of "you" and "personal" impacts

of viruses versus the individual and friends and family through the use of “us”, “our” and “you, your friends and family”. Graphics in the independent conditions depict single computer users while graphics in the interdependent condition depict networks of computer users (see Appendix H).

We conducted a pre-test on the self-view manipulation. Participants were randomly assigned to either the independent or interdependent condition⁶. After reviewing the website, participants completed manipulation checks which asked them to describe the extent to which the website: (1) made me think about the impact of security issues on just myself, (2) focused my thoughts about the message on just myself, (3) made me think about the impact of security issues on myself and other inter-connected users of the Internet, and (4) focused my thoughts about the message on myself and the Internet community of users. The wording of these questions is consistent with the manipulation checks used to assess the success of the self-view prime used by Aaker and Lee (2001). A total of 28 subjects participated in this test. Repeated measures ANOVA results show the anticipated effect of self-view on thoughts about the self versus thoughts about the self and other users of the Internet ($F=11.225, p<.001$). Participants receiving the independent condition thought more about just the self ($M= 5.063$) than the self with other Internet users ($M=3.813$) while participants receiving the interdependent condition thought more about themselves with other Internet users ($M=4.708$) than they thought about just themselves ($M=3.792$).

⁶ Procedures and subject recruitment for the pre-test were similar to those used for the main study.

Measures. The participants were asked to take their time reviewing the website and then proceeded to the questionnaire portion of the study. After each participant read the website, s/he completed an online questionnaire including multi-item scales to conduct manipulation checks, measure the dependent variables and capture demographic/control information (see Appendix I for the measures). We adapted scales for the two dependent variables which include perceived risk (self and comparison groups adapted from Rhee et al. 2005) and security intentions (Taylor and Todd 1995). The intention measures specifically relate to the user's intentions to exercise care when downloading files by checking the source. We utilize an indirect method of assessing bias using a 7 point Likert scale. This involves assessing risk for the self and the targets separately versus requiring the participant to provide a single estimate for likelihood of experiencing an event relative to a target. The former, indirect method produces less bias in measurement (Klein and Helweg-Larsen 2002). Thus, the participants complete a series of questions estimating their own risk, the risk to "a friend" and the risk to "an average other".

To assess the success of the self-view manipulations, we used measures consistent with Aaker and Lee (2001). Respondents answered questions related to the extent to which the website stressed personal risks versus risks to oneself as well as friends and family members. Following Menon et al. (2002), we included a manipulation check asking participants to rate how similar they think they are to a friend and to an average other. In addition, as a check for the financial and social domain manipulation, we created two items asking the participant to indicate the

extent to which the website focused their thoughts on the financial/social consequences and financial/social risks associated with computer viruses.

We included several questions intended to rule out potential confounds. Respondents indicated their perceptions of the message on seven-point scales anchored by not at all credible/very credible, difficult to comprehend/easy to comprehend, contained little information/contained a lot of information, not at all personally relevant, very personally relevant, and involving, not involving. Where necessary, terms such as computer virus and downloading files were explicitly defined so that each respondent had a common understanding of each term.

Since this study involves individual-level perceptions, we collected demographic information such as gender and age. In addition, to assess any influence of prior experience, subjects were asked to indicate their personal exposure to prior computer viruses as well as how much they heard or read about computer viruses recently.

4.3.2 Analysis

Prior to executing the analyses, we examined the reliability and validity of the constructs. Reliability indicators for all study measures exceeded the minimum Cronbach's alpha value of .7 suggesting that each set of items was consistent in measuring what was intended (Nunnally and Bernstein 1994). We assessed construct discriminant validity through principal component factor analysis with direct oblimin rotation. All items load on the appropriate factor with no cross loadings above the commonly specified minimum value of .4 on unintended constructs (Hair et al. 1998).

Results of the reliability and factor analysis are reported in Appendix J. Summated scales were used in the remaining analysis.

Manipulation Checks. We first conducted a series of manipulation checks. Although the self-view manipulation had been pre-tested, we created an Other Thoughts index based on the two manipulation check items. A 2 (self-view: independent vs. interdependent) x 2 (risk domain frame: social vs. financial) ANOVA revealed the anticipated main effect of self-view ($F(1,95)=4.93; p<.05$). Participants in the interdependent self-view condition reported more thoughts related to themselves, their friends and family ($M=5.07$) than did participants in the independent self-view condition ($M=4.46$). No other effects were significant.

To determine if the risk domain frame manipulation was successful, we created a financial social risk thought index based on the two manipulation check items. A (self-view: independent vs. interdependent) x 2 (risk domain frame: social vs. financial) ANOVA on financial social risk thoughts, revealed the anticipated main effect of risk domain frame ($F(1,95)=5.12, p<.05$). Participants in the social domain frame indicated more thoughts related to social concerns and risks ($M=1.01$) while participants in the financial risk domain frame indicated more thoughts related to financial concerns and risks ($M=-2.62$).

We conducted a 2 (self-view: independent vs. interdependent) x 2 (risk domain frame: social vs. financial) x 2 (target person) repeated measures ANOVA on person similarity ratings. The results confirm a main effect of target person such that participants perceive their best friend to be more similar to them ($M=4.92$) than the average undergraduate ($M=3.85$; $F(1,95)=62.03, p<.001$).

Optimistic Bias. Although evidence of optimistic bias has previously been found in the security context (Campbell et al. 2008; Rhee et al. 2005), we first checked for evidence of the bias in our sample. We used the likelihood of security risk estimates for the three targets (self, friend and average undergraduate) as the dependent measures and expected judgments of risk to be lower for oneself than others. We ran a repeated measures ANOVA using target risk perceptions as a within subject factor and goal frame as a between subject factor.

Results yielded a significant main effect of target person ($F(2,190)=36.33$; $p<.001$). Risk estimates are significantly lower for oneself than for a friend ($M=3.76$ vs. 4.18 , contrast $F(1,95)=10.00$; $p<.05$), and both self and friend's risk is lower than that for the average undergraduate ($M=4.86$, contrast $F(1,95)=65.17$, $p<.001$). Thus, consistent with Campbell et al. (2008) and Rhee et al. (2005), our data confirm that perceived risk increases as perceived similarity decreases, and that individuals exhibit an optimistic bias in the online security context. Means are depicted for each condition in table 4.1.

To test hypothesis 1, we calculated a vulnerability difference score since we were most interested in comparing subjects' perceptions of their own and average others' vulnerability to computer viruses (Perloff and Fetzer 1986). We computed this score by subtracting each subject's estimate of their own vulnerability from the estimate provided for an average other's vulnerability. These difference scores could range from 7 to -7 as vulnerability was assessed on a 7 point Likert scale. Higher scores indicate perceptions of relative invulnerability while lower scores indicate perceptions of relative vulnerability.

A 2 (risk domain frame) x 2 (self-view) ANOVA showed no significant interaction effect of self-view and risk domain frame on the self/other difference score⁷. In an attempt to further analyze the data at a more granular level, we conducted a 2 (self-view: independent vs. interdependent) x 2 (risk domain frame: financial vs. social) x 3 (target person: self/friend/average other) mixed-design ANOVA, treating the message cues as between-subject variables and the target person as the within-subject variable. The interaction effect between self-view and risk domain frame was again not significant. However, there was a marginal main effect of risk domain frame on the optimistic bias ($F(2,182)=2.85, p<.10$). Contrasts indicate that participants perceived the risks to friends and average others to be more similar when receiving the financial risk domain frame than when receiving the social risk domain frame ($F(1,91)=7.89, p<.01$). This effect is depicted in panel A of figure 4.1. Contrasts conducted on self-view indicate a marginal influence on the optimistic bias ($F(1,91)=3.68, p<.10$). In other words, the difference between risk estimates for oneself and a friend was lower when participant's received the interdependent condition versus the independent condition. This effect on the optimistic bias is depicted in panel B of figure 4.1. Hypothesis 1 is not supported.

Intentions. To test hypothesis 2, we conducted a 2 (self-view: independent vs. interdependent) x 2 (risk domain frame: financial vs. social) ANOVA. The analysis revealed the anticipated interaction between the self-view and risk domain frame ($F(1,92)=4.01, p<.05$). Participants receiving the interdependent self-view reported

⁷ Due to the insignificant results, we examined observed power and found it to be .05. The insignificant results combined with the low power make it difficult to draw conclusions related to hypothesis 1.

higher intentions when it was combined with the social risk domain frame ($M=5.64$) as opposed to the financial risk domain frame ($M=5.01$). Participants receiving the independent self-view reported higher intentions when receiving the financial risk frame ($M=5.71$) as opposed to the social risk frame ($M=5.35$). Follow up contrasts show that the differences are significantly different for the interdependent self-view group ($t=-2.16$, $p<.05$), but not the independent self-view group ($t=.89$, $p=.38$). This interaction is depicted in figure 4.2. These findings provide support for hypothesis 2.

We controlled for the effects of gender, media exposure and prior personal experiences with security violations in the ANOVA. None of the controls has significant effects.

4.3.3 Study 1 Discussion

The findings of study 1 suggest that although security-related optimistic bias was not influenced by an interaction of self-view and risk domain frame message cues, security-related intentions were significantly influenced as hypothesized. Specifically, individuals in the interdependent condition indicated significantly higher intentions to exercise care when downloading files from the Internet when receiving messages stressing the social costs associated with contracting a virus as opposed to messages stressing the financial costs. We found evidence of an optimistic bias in the online security context but were unable to significantly reduce the bias using the combination of self-view and risk domain message cues. Thus, study 1 supports hypothesis 2 but not hypothesis 1.

While our findings related to optimistic bias do not support hypothesis 1, the marginal influence of message cues on the optimistic bias suggest that perhaps a

different combination of cues or stronger manipulations might yield significant findings. Therefore, in study 2 we shift the message framing focus and use a different, stronger prime for self-view. Our use of financial and social costs in study 1 essentially constitute negative frames since they both focus on consequences and potential losses associated with not performing a behavior (in this case exercising care when downloading files from the Internet). In effect, this constitutes a fear appeal which may evoke a stronger reaction among participants (Kunda 1990; Lench et al. 2006; Smits and Hoorens 2005). Some studies have shown that negative frames are more successful at inducing behavior, while positive frames are more effective at influencing attitudes and beliefs (Davis 1995; Lord 1994). Therefore, in study 2, we apply the concept of goal framing and include both a positive and negative frame to attempt to influence both optimistic bias and intentions. In addition, we prime self-view in a separate study prior to the main study.

4.4 STUDY 2 – SELF-VIEW AND GOAL FRAME

The manner in which a message is framed can influence choice behavior even when the message conveys essentially the same information (Levin et al. 1998). Goal framing is a type of manipulation that involves two frames, a positive and negative. Both frames are assumed to be good because benefits are implied in each. With goal framing, the positive frame emphasizes the positive aspects of a behavior, and the negative frame emphasizes the negative aspects of not performing the behavior. In the context of this study, goal framing of a message serves to focus the individual either on the consequences associated with not exercising good judgment when downloading files from the Internet which could lead to contracting a computer virus

(negative or prevention frame), or on the benefits associated with exercising good judgment when downloading files from the Internet to enjoy consistent access to resources (positive or promotion frame).

Negative message appeals focus individuals' cognition and subsequent elaboration processes on potential harmful consequences, similar to fear appeals, and tend to require extensive resources to process (Keller and Block 1996; Loro 2007). In contrast, positive frames are likely to generate less emotion and may require fewer resources to process (Loro 2007). In a study of prosocial persuasive appeals, this level of elaboration associated with goal frame was found to interact with self-view to influence attitudes and intentions related to environmental issues (e.g., recycling). Loro (2007) argued that self-referencing messages are more involving than self-other referencing messages due to the larger volume of associations individuals possess to the self as compared to others. Mental representations of the self are more accessible in memory than those of others and serve to, once activated, increase involvement in the persuasion attempt. When the more cognitively demanding negative frame was paired with a self-referencing message or the less cognitively demanding positive frame was paired with a self-other referencing message, individuals reported more favorable attitudes toward recycling. These conditions represent cases in which persuasion is maximized because individuals apply available resources to process message advocacy without having surplus resources available for use in generating counterarguments. For example, individuals receiving a self-referencing message are highly involved in processing the message. When they encounter a positive frame, it requires fewer resources to process which leaves

surplus resources available for the individual to generate undermining counterarguments. Similarly, the self-other referencing message triggers fewer associations in memory resulting in fewer cognitive resources to process a negatively framed message which similarly undermines persuasion.

When the information in a message is presented in a way that optimizes the cognitive resources available for processing the message, we expect the individual's optimistic bias to be reduced. Specifically, when an independent self-view is combined with a negative frame or an interdependent self-view is combined with a positive frame, the message is most persuasive leading to a reduction in the security behavioral bias and related intentions.

H3: Individuals primed with an interdependent (independent) self-view will report a lower optimistic bias when receiving a positive (negative) goal frame than those primed with a negative (positive) goal frame.

H4: Individuals primed with an interdependent (independent) self-view will report a higher level of intentions to perform security-related behaviors when receiving a positive (negative) goal frame than those primed with a negative (positive) goal frame.

4.4.1 Method

To test the research hypotheses, we conducted an experiment in a laboratory setting employing a 2 X 2 (self-view: independent or interdependent by message framing: positive or negative) between subjects factorial design. As explained below, self-view was manipulated by having the subjects read a story prior to the main study while the message framing was manipulated via asking the subjects to review a website that differentially emphasized positive or negative themes.

Our sample consisted of undergraduate students from a large university enrolled in a required marketing course. A total of 84 subjects participated in the

experiment. Thirty-six of the subjects were male (43%). Random assignment of subjects to conditions resulted in between 11 and 17 subjects in each condition (see table 4.2). Participants completed our study as part of a one hour block of experiments completed by undergraduates for partial course credit in an introductory marketing course. This enabled the self-view prime to be administered as if it was separate and unrelated to our main study. The self-view prime was administered as a paper-and-pencil study while the main study was conducted by asking the participants to review a website and complete a questionnaire electronically. The entire block of experiments was conducted with the participants isolated from each other, completing the experiments independently. The laboratory setting ensures an environment that is consistent across all participants and free of distraction.

Self-View Manipulation. For study 2, we chose to manipulate self-view via having subjects read the Sumerian warrior story which has been successfully used to measure interdependent versus independent self-cognitions (e.g. Brewer and Gardner 1996; Gardner et al. 1999) and manipulate self-view (Mandel 2003; Trafimow et al. 1991) in prior research. Subjects are asked to read a story about Sostaras who must select a general to lead troops into battle. In the interdependent version, Sostaras selects a family member which is described as benefiting Sostaras's family. In the independent version of the story, Sostaras chooses a talented general which benefits Sostaras personally. After reading the story, subjects completed 10 statements beginning with "I am –". (Kuhn and McPartland 1954). When the manipulation is successful, the percentage of idiocentric (i.e., self-centered, egocentric) responses

following the interdependent condition is significantly lower than following the independent condition (Trafimow et al. 1991).

Goal Frame Manipulation. After completing the Sumerian warrior story and related questions, the subjects proceeded to the main study and were asked to review a website (see Appendix H). The website again focused on the potential for contracting a virus based on file downloading behaviors similar to the focus of the website used for study 1. However, participants randomly assigned to the positive goal frame condition, read about benefits associated with exercising good judgment when downloading files from the internet including uninterrupted access to files, the ability to remain in contact with other people and reliable access to the Internet. In contrast, participants assigned to the negative goal frame condition read about the consequences of not exercising good judgment when downloading files including loss of files, fraud, and costs associated with restoring a computer after a virus attack.

Measures. Similar to study 1, the main study's online questionnaire included multi-item scales to conduct manipulation checks, measure the dependent variables and capture demographic/control information. We reworded the perceived risk items and reduced the scale to 3 items (2 Likert scale items and one item to measure the probability of perceived risk on a 0 to 100 point scale). We also made minor wording changes to the intention items to tailor them to study 2's content (see Appendix K for study 2's unique items).

To assess the success of the goal frame manipulations, we used measures consistent with Aaker and Lee (2001). Respondents were asked to indicate on seven-point scales the extent to which the website stressed the negative implications of not

exercising good judgment when downloading files online and the extent to which the message stressed the positive implications of exercising good judgment when downloading files online.

4.4.2 Analysis

Prior to executing the analyses, we again examined the reliability and validity of the constructs. The study measures demonstrate acceptable psychometric properties (Hair et al. 1998; Nunnally and Bernstein 1994). Results of the reliability and factor analysis are reported in Appendix L. Summated scales were used in the remaining analysis.

Manipulation Checks. Two independent judges unrelated to the study coded the self-cognition “I am” statements from the Sumerian warrior prime as idiocentric (personal qualities, attitudes, or beliefs that do not relate to others such as “I am young”), or as group or allocentric (statements indicating relationships to others or membership in groups, such as “I am Jewish” or “I am a leader”). The Cohen’s Kappa obtained was .78 ($p < .001$) indicating acceptable interrater reliability (Landis & Koch 1977). For the independence-primed subjects, 73% of the self-cognitions were idiocentric compared to 62% of the self-cognitions of the interdependent-primed subjects. A chi-square test indicates that there is a statistically significant relationship between the thoughts generated by the two versions of the Sumerian warrior story (chi-square with one degree of freedom = 3.85, $p < 0.05$) with fewer idiocentric thoughts generated following the interdependent prime.

To check the effectiveness of the goal frame manipulation, we conducted two separate ANOVAs on each of the thought types: consequences and benefits. A 2

(goal frame) x 2 (self-view) ANOVA on thoughts about benefits of exercising good judgment when downloading files from the Internet showed a significant main effect of goal frame ($F(1,78)=5.18, p<.05$) such that thoughts about benefits were higher in the positive condition ($M=4.41$) and lower in the negative condition ($M=3.72$). A similar 2 x 2 ANOVA on thoughts about consequences of not exercising good judgment when downloading files, indicates thoughts about consequences were higher in the negative condition ($M=4.84$) and lower in the positive condition ($M=4.23, F(1,76) = 3.55, p<.10$).

We conducted a 2 (self-view) x 2 (goal frame) x 2 (target person) repeated measures ANOVA on person similarity ratings. The results confirm a main effect of target person such that participants perceive their best friend to be more similar to them ($M=4.93$) than the average undergraduate ($M=4.24; F(1,78)=26.93, p<.001$).

Optimistic Bias. To test hypothesis 3, we calculated vulnerability difference scores similar to study 1 for both the Likert scale and the probability item response (Perloff and Fetzer 1986). We computed this score by subtracting each subject's estimate of their own vulnerability from the estimate provided for an average other's vulnerability. These difference scores could range from 7 to -7 for the Likert scale responses and from 100 to -100 as vulnerability was assessed on a 100 point probability scale. Higher scores indicate perceptions of relative invulnerability while lower scores indicate perceptions of relative vulnerability.

A 2 (goal frame) x 2 (self-view) ANOVA shows a significant interaction effect of self-view and goal frame ($F(1,45)=6.64, p<.05$) on the probability self/other difference score (for the means see table 4.2). No other effect was significant.

Specifically, subjects primed with the independent self-view and negative goal frame report a significantly lower optimistic bias ($M=14.82$) when compared to subject's primed with the independent self-view and positive goal frame ($M=30.82$). Subjects primed with the interdependent self-view in combination with a positive focused message report a lower optimistic bias ($M=18.30$) than when receiving a negative focused message ($M=34.39$). This interaction is depicted in figure 4.3. Contrasts indicate this difference is significant in the independent condition ($t(23)=-2.21$; $p<.05$) but not in the interdependent condition. The interaction between self-view and goal frame was not significant in the ANOVA using the difference score calculated with the Likert scale responses as a dependent variable.

We controlled for the effects of gender, media exposure and prior personal experience with viruses. Only prior personal experience with viruses was significant ($F(1,45)=20.18$, $p<.001$). Hypothesis 3 is supported.

Intentions. The results of a 2 (goal frame) x 2 (self-view) ANOVA on security behavioral intentions show no significant interaction between self-view and goal frame⁸. Thus, hypothesis 4 is not supported.

4.4.3 Study 2 Discussion

The findings of study 2 suggest that security-related optimistic bias can be influenced by an interaction of self-view and goal frame message cues when individual perceptions are assessed using a 0 to 100 probability scale but not when the risk perceptions are captured on a 7 point Likert scale. A plausible explanation for the

⁸ Due to the insignificant results, we examined observed power and found it to be .06. The insignificant results combined with the low power make it difficult to draw conclusions related to hypothesis 4.

latter insignificant effect is that perhaps the discrete 7 point scale does not allow sufficient variation in perceptions to be captured as compared to the continuous probability scale (Russell and Bobko 1992). Russell and Bobko (1992) found that the information lost when capturing relatively fine latent responses using coarse Likert response scales resulted in a substantial reduction in moderated regression effect size. They suggest the use of a coarse scale may be one reason for mixed findings with regard to moderator effects over the years (Cohen 1983; Russell et al. 1991; Russell and Bobko 1992). For the results based on the probability scale, individuals indicated lower levels of optimistic bias when primed with an interdependent self-view in combination with a positive goal frame or when primed with an independent self-view in combination with a negative goal frame. No such interaction was observed on intentions to perform security-related behaviors which suggests that the influence of message cues on risk perceptions did not result in a corresponding change in intentions. Thus, study 2 supports hypothesis 3 but not hypothesis 4.

4.5 LIMITATIONS

Prior to discussing the implications of the study findings, a few limitations must be acknowledged. First, the sample consisted of undergraduate students. As a result, care should be taken when generalizing beyond this population to other demographic segments as it is possible that different groups may find different messages more persuasive than others. However, young people represent a significant portion of Internet users (Day et al. 2003; Jones and Fox 2009) and, thus, are an important demographic group to study, particularly as they tend to engage in risky behavior. Further, due to the difficulty in measuring realized secure behavior,

as has been noted in literature addressing security compliance in the workplace (Vroom and Von Solms 2004), we measure intentions to perform security-related behaviors and not the actual behavior itself. While the link between intentions and behavior is well established both theoretically and empirically (Fishbein and Ajzen 1975; Ajzen 1991; Sheeran 2002; Venkatesh et al. 2003), a fruitful avenue for future research would be to conduct field studies in which behavior could be compared perhaps before and after a promotional campaign based on the findings reported here.

Finally, it is possible that the risk domain manipulations (financial and social risks) used for Study 1 could make both social and financial risks salient. For example, as an individual considers financial costs of contracting a virus such as paying for technical support or having to redo work that had already been completed, she may also think about the social implications (e.g. embarrassment or disapproval) if others become aware of her having to take such efforts to recover from an attack. Similarly, an individual considering embarrassment if others receive spam from his email address may also think of how to avoid this in the future which could require time and money. However, our manipulations are designed to focus the individual on the primarily financial or social risks associated with contracting a virus and our manipulation check found that participants in the social domain frame indicated more thoughts related to social risks while participants in the financial risk domain frame indicated more thoughts related to financial risks.

4.6 DISCUSSION AND CONCLUSION

With the accelerating use of information technology in both personal and organizational spheres of activity, ensuring the safety and fidelity of the computing

foundation is a critical imperative. The Obama administration acknowledges the importance of safeguarding the cyber infrastructure through public education and awareness campaigns to promote cybersecurity (Cyberspace 2009; Krebs 2009). Increasing secure behavior of online users is important because the Internet enables individuals to be more connected through electronic linkages than ever before. In such a highly interdependent and tightly coupled network, individual behaviors can have far-reaching consequences that transcend borders between people, organizations and nations (Turner 2007; Weaver et al. 2003). The objective of this research was to examine how to minimize optimistic bias in the online security context and increase intentions to perform security-related behaviors through message cues. We explored two mechanisms for influencing optimistic bias and intentions, the way in which the individual views herself in relation to others, and the manner in which the message is framed, through cues in an experimental setting.

While neither study resulted in the chosen message cues influencing both security-related optimistic bias and behavioral intentions, study 1 resulted in the hypothesized increases in behavioral intentions and study 2 resulted in the hypothesized decreases in the optimistic bias. Both these findings are positive outcomes from a practical perspective. Study 1's results suggest that individuals exposed to messages with an interdependent self-view coupled with messages stressing the social costs associated with contracting a virus as opposed to messages emphasizing the financial costs indicated significantly higher intentions to exercise care when downloading files from the Internet. Participants receiving the independent self-view reported higher intentions when receiving the financial risk

frame. As reported in study 2, an independent self-view was particularly effective at lowering optimistic bias when combined with a negative goal frame. Study 1's findings more directly indicate an influence on individual file download behaviors while study 2's findings likely suggest more subtle benefits as a result of a decrease in optimistic bias which were not measured in our study, such as an overall increase in cautious online behavior in general. More research is required to determine the behavioral outcomes of optimistic bias in the online security context. In addition, it is possible that no interaction effect on optimistic bias was detected in study 1 due to the coarse Likert scale response mechanism used to capture perceived risk since an interaction effect on the optimistic bias was only detected in study 2 by using the more granular 100 point probability scale. While Likert scales appear to be sufficient for determining the existence of optimistic bias, less coarse scales may be necessary in studies aimed at identifying potential changes in optimistic bias particularly when moderation is theorized in order to detect effects (Cohen 1983; Russell et al. 1991; Russell and Bobko 1992).

Although other optimistic bias studies in different settings (e.g. health contexts) have illustrated that similar mechanisms influence optimistic bias and intentions, the results of this study appear to suggest that there may be a difference between the mechanisms that influences security-related optimistic bias and security-related intentions. Further research is required to explore potential context-related differences. One possibility may be that the message cues we chose have a cultural component which could be tied to optimistic bias. Self-enhancing biases have been shown to differ culturally (Heine and Lehman 1997; Kitayama et al. 1997) and, in this

study, we chose to attempt to manipulate optimistic bias by situationally altering self-view. While this has been successfully achieved in prior studies, to our knowledge it has not been done with optimistic bias. Further, perceptions associated with financial and social risks may differ based on culture (Markus and Kitayama 1991; Shea and Yeh 2008).

From a theoretical perspective, this study makes a number of contributions. First, we extend the research on risk domain and context effects on choice behavior by demonstrating that a manipulation of risk domain influences security intentions when combined with self-view. The results also suggest that optimistic bias is influenced by risk domain frame. We have also demonstrated that security-related optimistic bias is influenced by an interaction of goal frame and self-view.

From a practical perspective, the study findings provide insight for crafting persuasive social marketing campaigns targeted broadly at the public or more specifically at smaller groups such as employees within a firm. For example, print media (e.g. informational posters) for display or messages delivered to employees could stress potential embarrassment or stigma (i.e. social costs) due to security violations to the team or division/group (i.e. an interdependent focus) in an effort to increase security behavioral intentions. Another example could be public service announcements targeting the individual (i.e. an independent view) while stressing the consequences of poor online behavior (i.e. a negative focus) which should minimize security optimistic bias. In addition, the findings might prove useful for vendors in creating effective advertising for security-related software.

CHAPTER 5: EPILOGUE

Due to technological breakthroughs, the current environment in which we live and work is swiftly changing in terms of how we communicate, conduct business, and interact with the healthcare system. In the case of healthcare, these changes are being fueled by policy. Recent policy also recognizes the need to increase the stability and security of the infrastructure that provides much of the support for social and economic functions. While the benefits of these breakthroughs are relatively obvious, the risks to individuals and organizations are less apparent. Indeed, the risks often take a back seat to the rewards associated with technological advancements. However, the risks are significant and varied, making it important to understand how individuals and organizations respond to their increased reliance on technology. This dissertation examines three areas of vulnerability: IT infrastructure failures at the organizational level, and health information privacy and online security at the individual level. Investigation of these points of vulnerability and how individuals and organizations respond will facilitate further research and enable practitioners to develop appropriate training, craft relevant policy, and design targeted marketing messages.

The first essay draws on the organizational reliability literature to classify IT infrastructure failures and theorize how collective mindfulness can change the way organizations respond to each type of failure. The results validate the research hypothesis that the omnibus measure of collective mindfulness explains less variance in the duration of failure response and is less informative about the influence of collective mindfulness on response than an examination of the two collective

mindfulness processes of containment and anticipation. Collective mindfulness processes influence an organization's response to failure in different directions depending on the failure type. Mindful containment facilitates response to failure, but is more efficacious at reducing duration when the failure is associated with no pre-defined routine. Furthermore, mindful containment can lengthen the organization's response to novel failures. Mindful anticipation, which is described in the literature as helpful at avoiding failure, impedes the response to failures associated with no pre-defined routine. This essay contributes to the organizational reliability literature by demonstrating the importance of disaggregating collective mindfulness and it at the level of the underlying processes processes. In addition, the implications for practitioners include: reinforcement of the value of investing in development of routines; the importance of searching for new ways to deal with novel failures such as vendor alliances; and the necessity for understanding when mindful anticipation processes are appropriate and when they are not.

The second essay synthesizes research from information systems, communication, and psychology to construct a conceptual model explicating the role played by type of information requested (general health, mental health, genetic), the purpose for which it is to be used (patient care, research, marketing) and the requesting stakeholder (doctors/hospitals, the government, pharmaceutical companies) in an individual's willingness to disclose personal health information (PHI). Further, the model incorporates the impact of emotion linked to one's health condition on willingness to disclose. Results from a nationally representative sample of over 1,000 adults show that emotion plays a significant role in the disclosure

decision. Individuals are also unable to fully comprehend the extent to which a negative health-related diagnosis and the associated emotion may influence their privacy decisions, highlighting the need for re-examining the timing of consent. Finally, the findings also suggest that contextual factors related to the requesting stakeholder and the purpose for which the information is being requested play an important role in moderating the relationships between concern and trust on willingness to disclose personal health information. This essay contributes to the privacy literature by introducing the moderating influence of two situational risk factors -- intended purpose and requesting stakeholder -- on the relationships between concern and willingness to disclose PHI and trust and willingness to disclose. A second contribution is the explicit incorporation of emotion into the privacy calculus. The practical implications of the study include an improved understanding of consumer concerns regarding the electronic storage of health information which can be used to craft policy and targeted marketing campaigns.

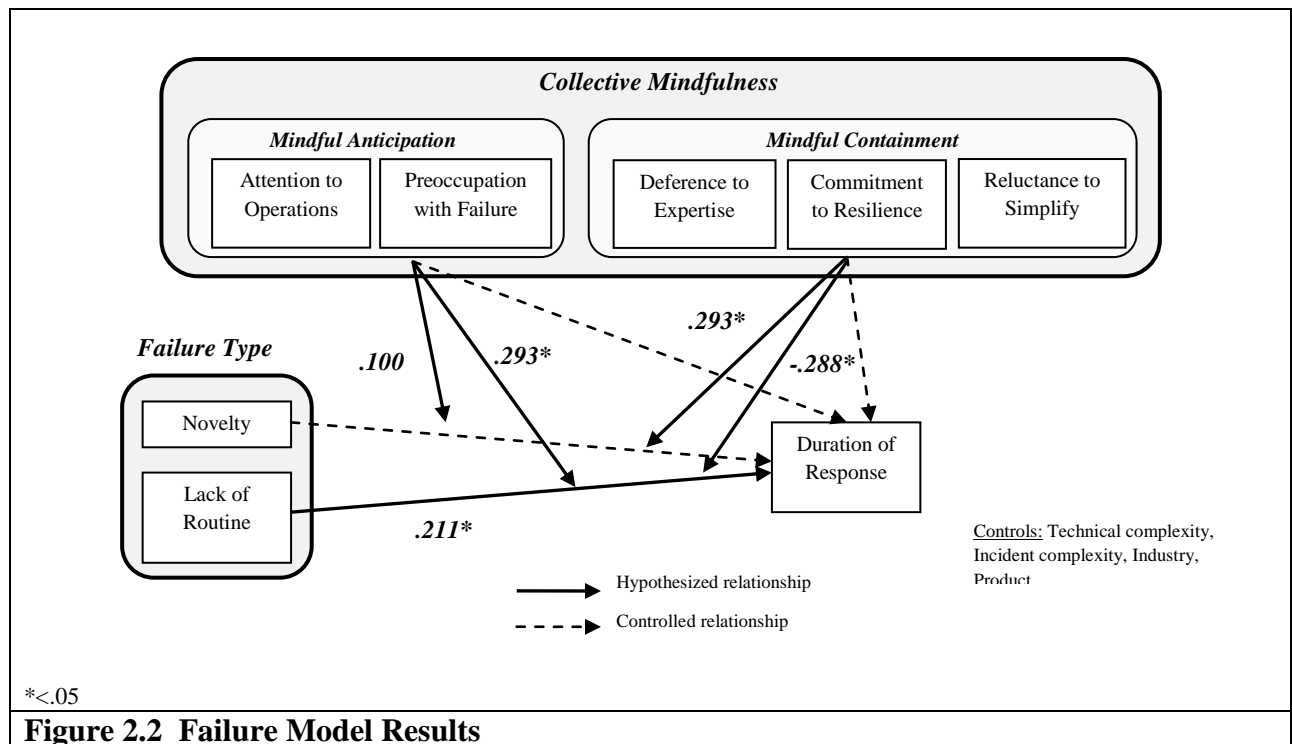
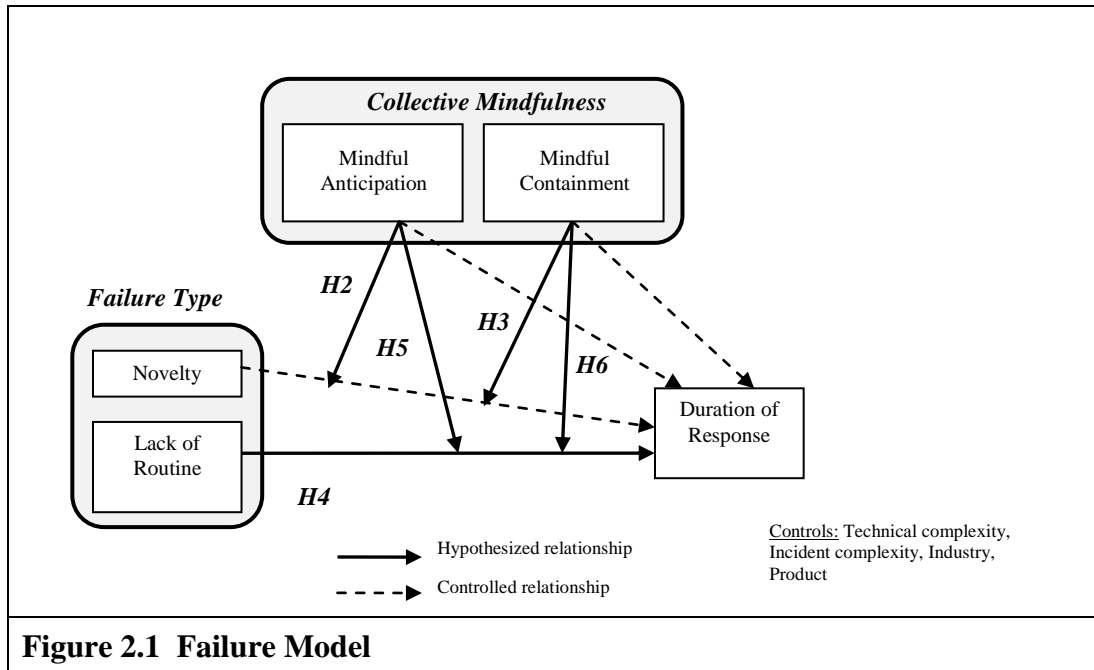
Finally, the third essay examines the influence of self-view and message framing on security-related optimistic bias and intentions. To the degree that individuals' security-related behaviors have widespread ramifications for the security of organizational and national computing infrastructure, understanding the drivers of such behaviors is important. The study draws on literature from marketing and psychology to design two experiments. Results from the first study confirm an interactive influence of self-view and risk domain frame (social or financial) on security-related intentions. An interesting and somewhat surprising finding was that optimistic bias was not significantly influenced by this combination of manipulations.

Nonetheless, the findings suggest that individuals exposed to messages with an interdependent self-view coupled with messages stressing the social costs associated with contracting a virus as opposed to messages emphasizing the financial costs indicated significantly higher intentions to exercise care when downloading files from the Internet. Participants receiving the independent self-view reported higher intentions when receiving the financial risk frame. Study 2 suggests an interactive relationship between self-view and goal frame on optimistic bias but that influence did not translate into similar changes to intentions. An independent self-view was particularly effective at lowering optimistic bias when combined with a negative goal frame. This study extends the research on risk domain and context effects on choice behavior by demonstrating that a manipulation of risk domain influences security intentions when combined with self-view. It also shows that security-related optimistic bias is influenced by an interaction of goal frame and self-view. Practical implications of this essay include insight into the crafting of persuasive social marketing campaigns targeted broadly at the public or more specifically at smaller groups such as employees within a firm.

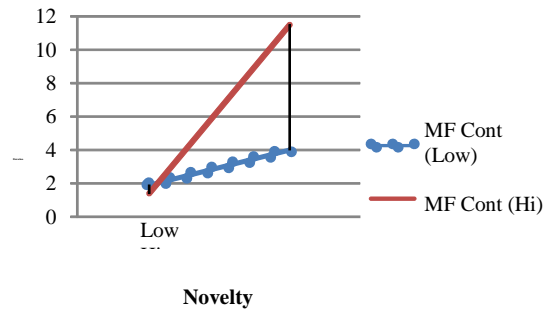
Collectively, the findings of this dissertation have important practical and policy implications for appropriate action in a society that is increasingly connected through technology. Essays 1 and 3 provide insights which could potentially improve cybersecurity. Findings from essay 1 can help organizations to efficiently allocate resources to improve their response to infrastructure failures. A quicker response to failure translates into less downtime which benefits not only the organization, but its employees, customers, suppliers, and potentially the economy as a whole. Essay 3

informs organizations as to which message appeals may be more effective at encouraging consumers to take precautions online. The efforts of each individual can contribute to a safer online environment. Finally, essay 2 has implications for both policy makers and consumers as it suggests how policy may need to change to address consumer concerns regarding the digitization of personal health information. It also enables marketing campaigns to be tailored for specific groups for purposes such as clinical trial recruitment or education of consumers on the benefits of electronic records. It is possible to leverage the benefits of technology without sacrificing privacy and security through actions driven by theory-based, rigorous research.

FIGURES

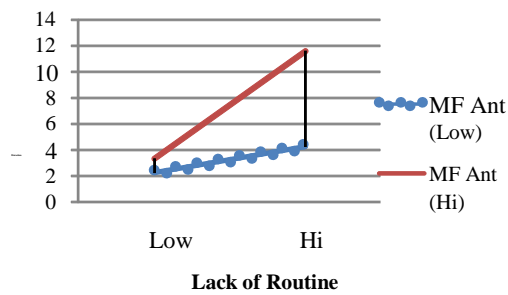


Interaction between Mindful Containment and Novelty

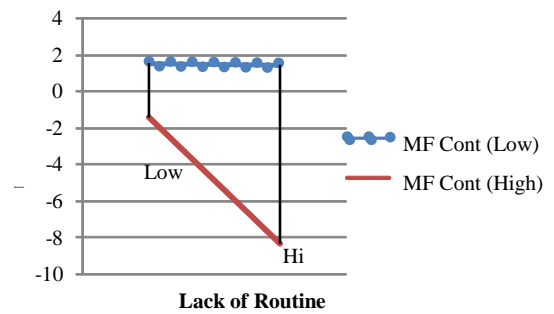


Panel A – Interactive Influence of Mindful Containment and Novelty on Duration

Interaction of Mindful Anticipation and Lack of Routine



Interaction of Mindful Containment and Lack of Routine



Panel B –Interactive Influence of CM Processes and Lack of Routine on Duration

Figure 2.3 Interaction Graphs for Duration

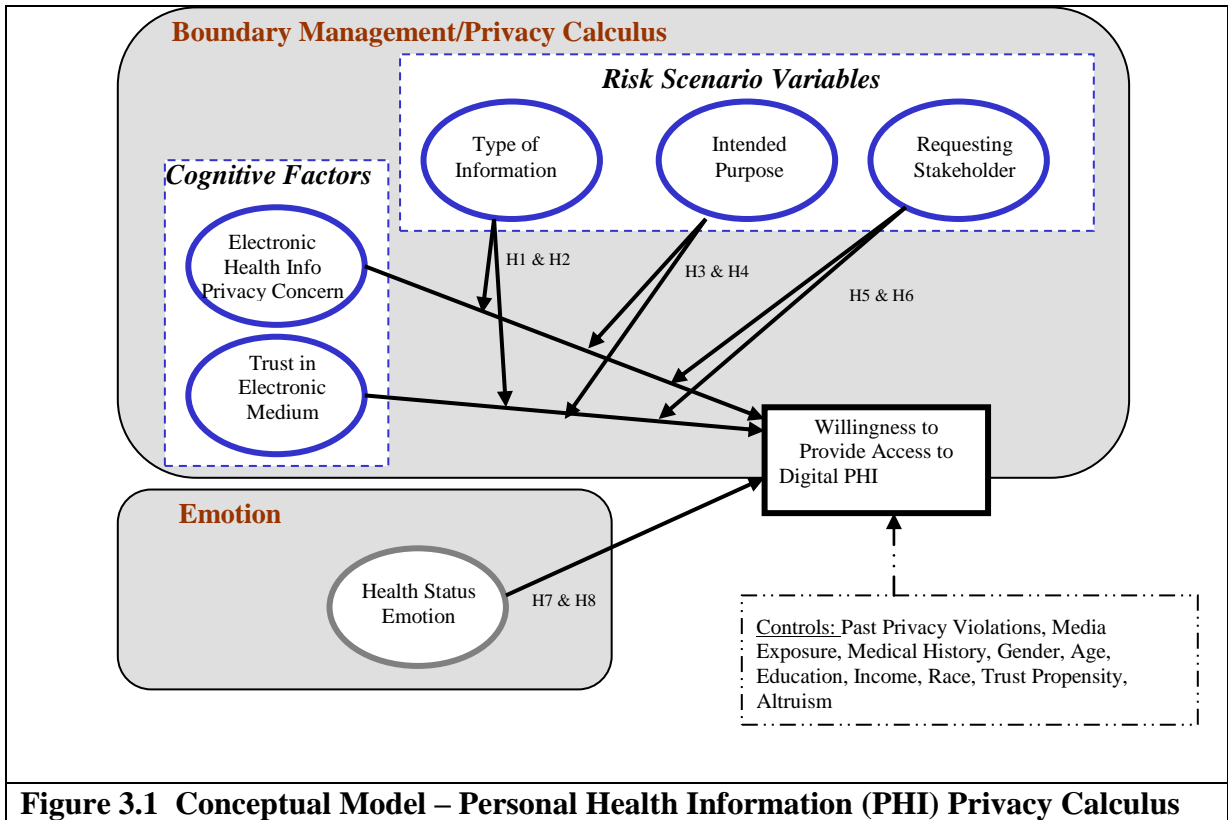
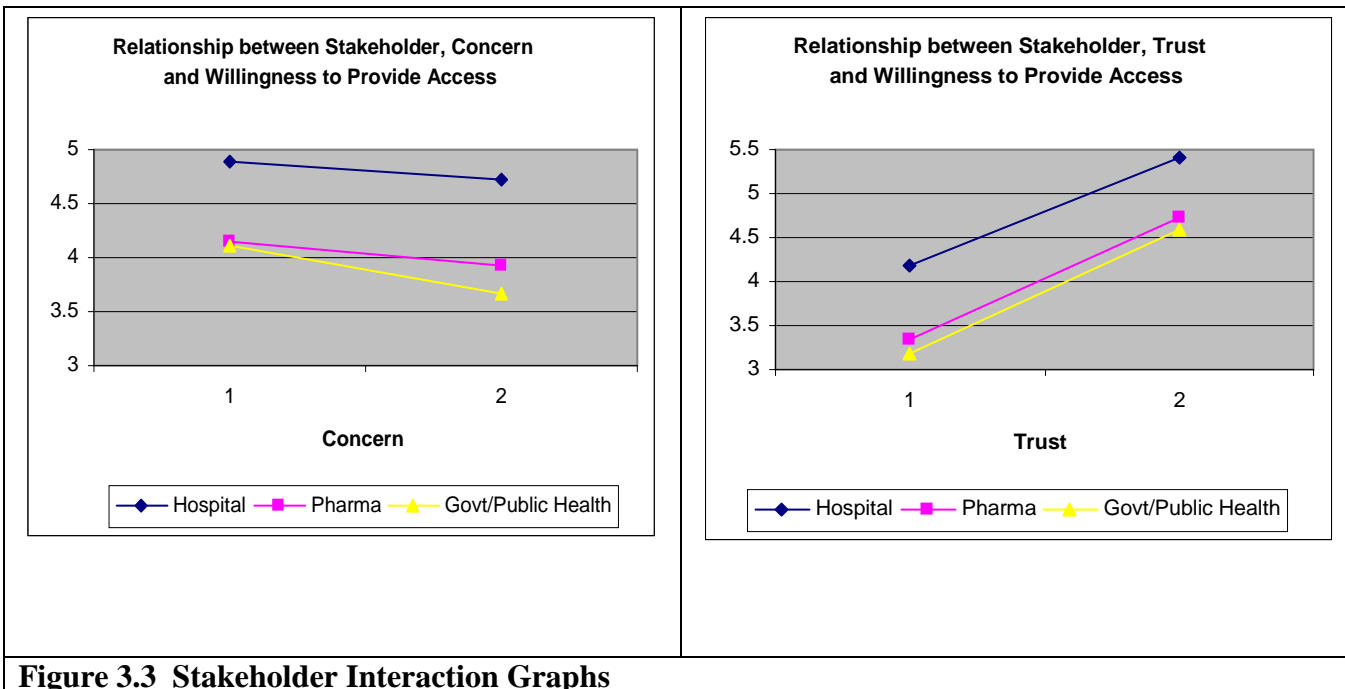
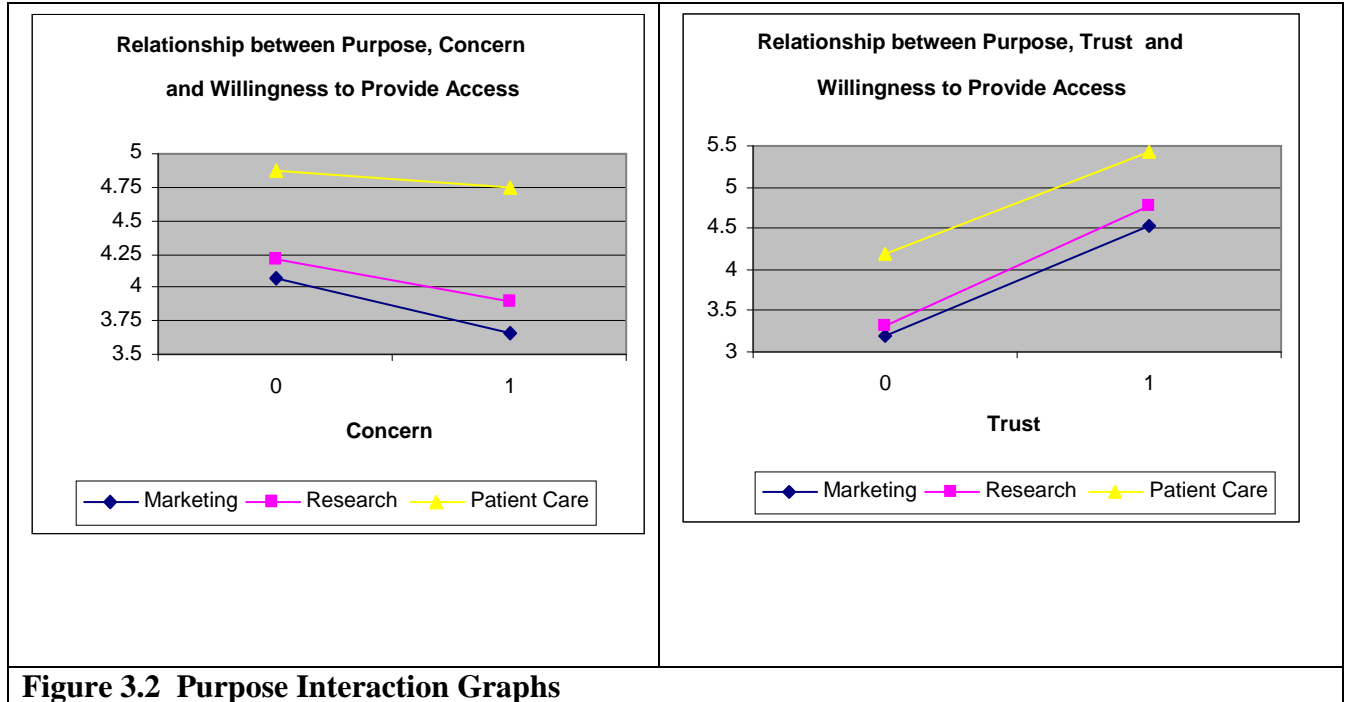
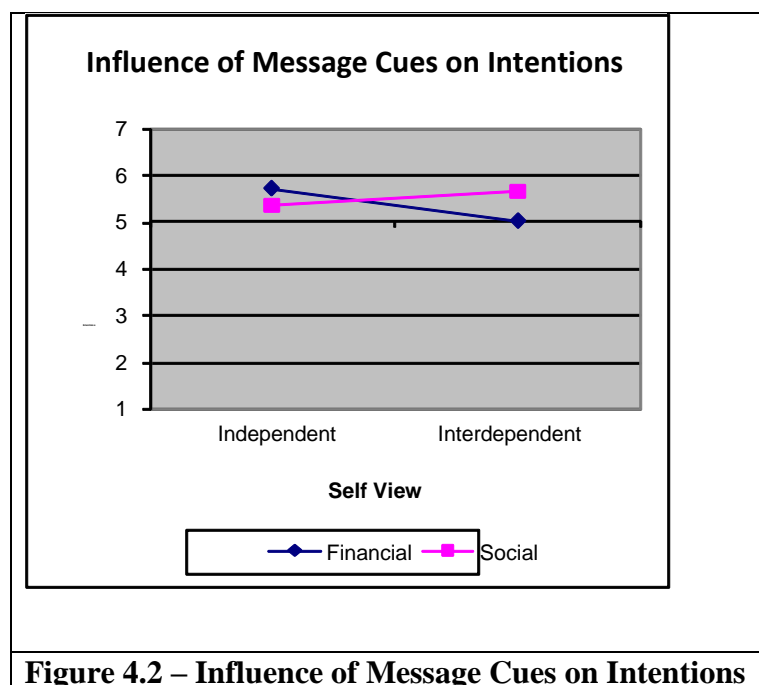
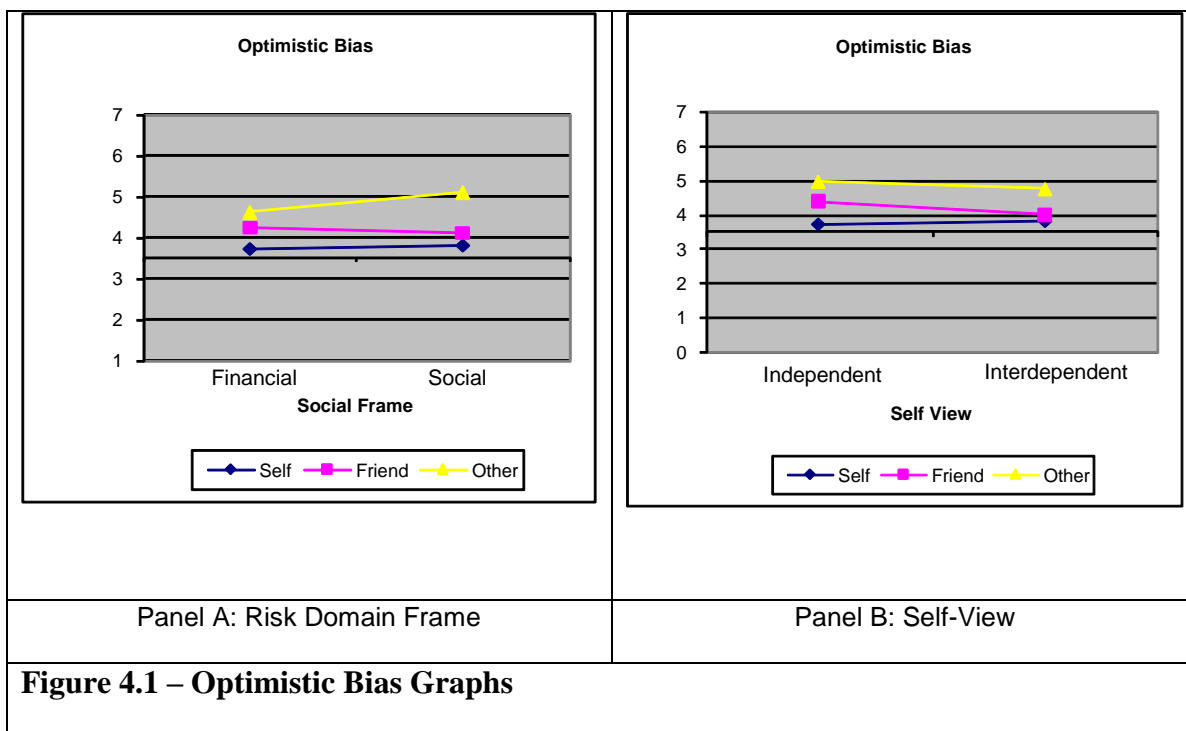


Figure 3.1 Conceptual Model – Personal Health Information (PHI) Privacy Calculus





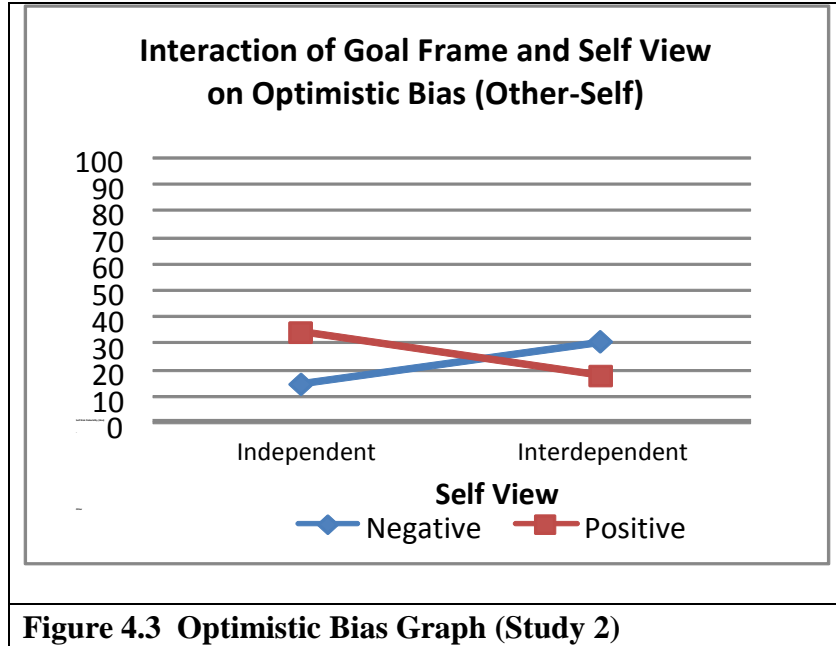


Figure 4.3 Optimistic Bias Graph (Study 2)

TABLES

Table 2.1 Summary of Empirical Collective Mindfulness Research (Reverse Chronological Order)				
Author (Date)	User Base/Context	Methodology	Dimension (s) Used	Description
Mu and Butler (2009)	194 employed or previously employed undergraduate students	Field study: data collected via surveys	Attention to Operations, Reluctance to Simplify, Preoccupation with Failure, Deference to Expertise, Commitment to Resilience	Developed, refined and validated a set of scales for measuring organizational mindfulness. Items created for 5 dimensions but only 4 factors emerged (commitment to resilience and deference to expertise loaded on a single factor). Created a framework and assessment tool for practitioners using an Analytic Hierarchical Process.
Valorinto, M. (2009)	North European retail companies	Case study (observation and archival data)	Collective Mind	IT found to both increase and decrease levels of mindfulness.
Baker, L. T. (2007)	245 respondents representing 199 small businesses	Field study: data collected via surveys and secondary data sources	Organizational Mindfulness	Demonstrates that individual owner mindfulness contributes to organizational mindfulness. Findings suggest the quality of strategic decision process mediates the relationship between organizational mindfulness and performance. Scale for mindfulness includes aspects of reluctance to simplify, respectful interactions and deference to expertise.
Mu (2007)	113 firms	Field study: data collected via surveys	Ombibus Measure with 2 factors: alertness/attention and change/situation	Proposed that IS mindfulness moderates the relationship between ERP scanning and assimilation. Yielded two dimensions of collective mindfulness: alertness/attention and change/situation. Only the alertness/attention dimension moderated the relationship between scanning and assimilation.
Vogus and Sutcliffe (2007)	1685 registered nurses from 125 nursing units in 13 hospitals	Field study: data collected via surveys	Omnibus measure (Safety Organizing)	Developed and tested a self-report measure of <i>safety organizing</i> that captures the behaviors theorized to underlie a <i>safety culture</i> . Safety organizing was negatively associated with number of reported medication errors and patient falls.
Vogus and Sutcliffe (2007)	1033 registered nurses and 78 nurse managers in 78 various nursing units in 10 acute-care hospitals	Field study: data collected via surveys combined with secondary data	Omnibus measure (Safety Organizing)	Findings suggest that benefits of safety organizing on reported medication errors were amplified when paired with high levels of trust in manager or the use of care pathways.
Weick and Sutcliffe (2001, 2007)	Varied	Multiple	Collective Mindfulness	Posit mindfulness assures high performance under complex environments. Define 5 dimensions of mindfulness: commitment to resilience, deference to expertise, reluctance to simplify, preoccupation with failure and sensitivity to operations
Barrett, M., Novak, J. M., Venette, S. J. and Shumate, M.	84 fire department employees	Field study: data collected via surveys	HRO Perception Scale (consisted of a self-efficacy subscale and an organizational risk response subscale)	Study finds satisfactory reliability and validity for a 2-factor HRO Perception scale consisting of a self-efficacy subscale and an organizational risk response subscale. HRO Perception Scale exhibited satisfactory discriminant validity when examined simultaneously with organizational

Table 2.1 Summary of Empirical Collective Mindfulness Research (Reverse Chronological Order)				
Author (Date)	User Base/Context	Methodology	Dimension (s) Used	Description
(2006)				commitment.
Pavlou and El Sawy (2006)	180 individuals employed in firms involved with new product development	Field study: data collected via surveys	Omnibus measure (Collective Mind)	The relationship between IT leveraging competence in new product development (NPD) and competitive advantage is mediated by NPD capabilities. NPD capabilities include dynamic capabilities of which collective mind is a component.
Cooren, F. (2004)	Board meeting in drug rehabilitation center	Case study (observation and archival data)	Collective Mind	Findings suggest that evidence of collective mind can be found by analyzing patterns of conversational behavior. Individual managers contribute textual blocks that represent the overall heedfulness of the group.
Knight (2004)	182 employees (lifeguards) of community swimming pools	Field study: data collected via surveys	Attention to Operations, Reluctance to Simplify, Preoccupation with Failure, Deference to Expertise, Commitment to Resilience	Quantitatively assessed collective mindfulness (CM) and its antecedents, outcomes and correlates. Created items to measure all 5 dimensions of mindfulness and determine influence on safety and customer service quality. Factor analysis yielded only 4 factors (not 5): commitment to resilience and deference to expertise items loaded on the same factor yielding a problem-solving factor. Four factors best predict collective mindfulness. CM predicted customer satisfaction and approached significance in predicting perceptions of customer safety.
Vogus (2004)	134 nursing units	Field study: data collected via surveys combined with archival data	Omnibus measure (Mindful Organizing)	Explores relationship between HR practices and organizational outcomes. HR practices influence respectful interaction and heedful interrelating which, in turn, influence mindful organizing (MO). Mindful organizing has strong, negative relationship to medication errors and patient falls.
Vogus and Welbourne (2003)	184 software firms	Field study: data collected via surveys	HR practices used as proxies for 3 of the CM dimensions (reluctance to simplify, commitment to resilience and sensitivity to operations)	HR management practices, described as proxies for CM dimensions, found to be associated with innovation and higher stock prices over time in software firms recently involved in initial public offerings. Provides support for the importance of individual mindfulness processes.
Bigley and Roberts (2001)	Fire Department	Case Study	High Reliability Organizing	Bigley & Roberts (2001) examine a distinctly bureaucratic system which produces reliable organizations in volatile environments and identifies three main factors enabling this unique combination: structuring mechanisms, constrained improvisation and cognition management methods
Yoo and Kanawattanachai (2001)	146 MBA students assigned to 40 4-person teams	Combination of survey questionnaires, archival data and objective team performance scores	Omnibus measure (Collective Mind)	Collective mind mediates the influence of transactive memory systems on team performance.

Table 2.1 Summary of Empirical Collective Mindfulness Research (Reverse Chronological Order)				
Author (Date)	User Base/Context	Methodology	Dimension (s) Used	Description
Weick & Roberts (1993)	Aircraft carrier personnel	Case study	Collective Mind	Introduces the concept of collective mind which arises from heedful interrelating and improves comprehension to decrease errors

Table 2.2 Industry Breakdown of Incidents		
Industry	N	Percent
Electricity Provider/Utility	8	5.2
Financial	58	37.9
Government	8	5.2
High Tech Services	13	8.5
Insurance	3	2.0
Pharmaceuticals	7	4.6
Telecommunications	32	20.9
Retail	2	1.3
Transportation	8	5.2
Other	14	9.2
Total	153	100

Table 2.3 Descriptive Statistics														
Variable	Reliability (No. of Items)	Min	Max	Mean	St. Dev.	Def / Rel to Sim	Comm to Resil	Att to Ops	Pre w/ Fail	CM	Nov	Rtn Bdown Type	Duration	MFant
Def to Expertise/ Reluctance to Simplify (Search)	.86 (6)	2.83	6.83	4.97	.80	1								
Commitment to Resilience	.81(2)	2.50	7.00	5.42	1.16	.33**	1							
Attention to Operations	.80(2)	1.50	6.50	4.59	1.06	.35**	.22**	1						
Preoccupation with Failure	.82(3)	2.00	7.00	5.09	1.02	.41**	.30**	.19*	1					
Collective Mindfulness	.74(3)	2.67	6.67	4.95	.91	.74**	.40**	.39**	.42**	1				
Novelty	.84(3)	1.00	7.00	3.98	1.53	-0.01	0.03	-0.03	-0.07	-0.02	1			
Lack of Routine	.78(2)	1.00	7.00	4.04	1.64	0.05	-0.01	0	-0.07	0.02	.18*	1		
Duration	n/a	0	176	24.49	32.33	-.31**	-.17*	-0.01	-.18*	-.25**	0.11	.17	1	
Mindful Anticipation	n/a	1.75	6.25	4.84	.82	.49**	.34**	.35**	.77**	.77**	.52**	-.07	-.066	-.044
Mindful Containment	n/a	2.92	6.67	5.19	.87	.81**	.81**	.35**	.44**	.70**	.02	.03	-.35**	.51**

** Correlation is significant at the .01 level (2-tailed); * Correlation is significant at the .05 level (2-tailed)

1

Table 2.4 CM Regression Results (Omnibus Measure)								
	Collective Mindfulness							
	Model 1		Model 2		Model 3		Model 4	
	Controls Only		Controls & Main Effects of Failure Type		Controls & Main Effects of Failure Type & CM		Controls, Main Effects & Interactions	
Variables	B	Std. Error	B	Std. Error	B	Std. Error	B	Std. Error
(Constant)	1.846**	.609	1.895**	.600	2.120**	.606	2.185**	.612
<i>Control Variables</i>								
Number of Vendors and Products	-.054	.103	-.086	.103	-.069	.102	-.073	.104
Variety of Software Ages (e.g. Legacy vs. State-of-the-Art)	.156†	.086	.176*	.085	.122	.089	.114	.090
Number of Vendors Involved in Incident Resolution	.364**	.141	.352**	.139	.305*	.140	.297*	.140
<i>"Failure Type" Factors</i>								
Novelty			.138†	.110	.140	.109	.144	.110
Lack of Routine			.220	.114	.244*	.113	.217†	.117
<i>Collective Mindfulness</i>								
Collective Mindfulness					-.212†	.118	-.199†	.119
<i>Mindfulness / Failure Type Interactions</i>								
CM X Novelty							.145	.106
CM X Lack of Routine							-.003	.116
Number of Observations	153		153		153		153	
Degrees of Freedom	3		5		6		8	
Adjusted r squared	.06		.08		.10		.10	
Change in r squared			.02*		.02*		.00	

*** $p < .001$.01 level; ** $p < .01$ level; * $p < .05$; † $p < .10$

Table 2.5 CM Process Regression Results								
	Model 1		Model 2		Model 3		Model 4	
	Controls Only		Controls & Main Effects of Failure Type		Controls, Main Effects of Failure Type & CM Proc		Controls, Main Effects and Interactions	
Variables	B	Std. Err	B	Std. Err	B	Std. Err	B	Std. Err
(Constant)	1.846*	0.609	1.895**	.600	1.944*	.580	1.887*	.574
<i>Control Variables</i>								
Number of Vendors and Products	-0.054	0.103	-.086	.103	.028	.109	.057	.113
Variety of Software Ages (e.g. Legacy vs. State-of-the-Art)	0.156†	0.086	.176*	.085	.059	.098	.049	.097
Number of Vendors Involved in Incident Resolution	0.364*	0.141	.352 *	.139	.269*	.136	.201	.136
<i>"Failure Type" Factors</i>								
Novelty			.138†	.110	.150†	.106	.162†	.103
Lack of Routine			.220*	.114	.243*	.110	.211*	.108
<i>Mindful Processes</i>								
Containment					-.515**	.166	-.434**	.164
Anticipation					.098	.186	.002	.183
<i>Mindfulness / Failure Type Interactions</i>								
Anticipation X Novelty							.100	.193
Containment X Novelty							.293*	.156
Anticipation X Lack of Routine							.293*	.162
Containment X Lack of Routine							-.288*	.150
Number of Observations	153		153		153		153	
Degrees of Freedom	3		5		7		10	
Adjusted r squared	0.06		.08		0.16		0.21	
Change in r squared			.03†		.08**		.05**	

*** $p < .001$.01 level; ** $p < .01$ level; * $p < .05$; † $p < .10$

Table 2.6 Summary Study Results by Hypothesis	
Hypothesis	Result
H1: CM modeled as a set of related dimensions grouped as processes will yield a higher explained variance than the CM omnibus measure	Supported
H2: Mindful anticipation facilitates failure resolution less effectively in novel failure contexts	Not Supported
H3: Mindful containment facilitates failure resolution less effectively in novel failure contexts	Supported
H4: Lack of routine for a failure context is positively associated with the duration of failure response	Supported
H5: Mindful anticipation facilitates failure resolution less effectively when the failure context involves a lack of routine	Supported
H6: Mindful containment facilitates failure resolution more effectively when the failure context involves a lack of routine)	Supported

Table 3.1 Demographics for Sample and U.S. Population		
Demographic Characteristic	Sample	U.S. Population*
Age		
18-24	6.7%	Approx. 11%†
25-34	13.2%	17.5%
35-44	17.0%	18.9%
45-54	21.5%	18.8%
55-64	18.0%	13.7%
65-74	14.6%	8.2%
75 and over	8.4%	8.0%
Education		
8 th grade or less	.6	6.5%
Some school, no degree	1.6	9.4%
High school graduate or equivalent	21.2	30.0%
Some college, no degree	30.5	19.5%
Associate's degree	10.7	7.4%
Bachelor's degree	22.1	17.1%
Master's degree	8.8	9.9%
Doctorate	4.1	
Gender		
Female	56.7%	51%
Income		
Less than \$10,000	6.8%	8.0%
\$10,000 to \$14,999	6.6%	5.9%
\$15,000 to \$24,999	13.6%	11.4%
\$25,000 to \$34,999	16.1%	11.2%
\$35,000 to \$49,999	16.5%	14.8%
\$50,000 to \$74,999	18.9%	19.0%
\$75,000 to \$99,999	9.0%	11.8%
\$100,000 to \$149,999	7.0%	10.9%
\$150,000 to \$199,999	2.5%	3.6%
\$200,000 or more	2.3%	3.4%
Race		
White	78.8%	73.9
Asian	1.8%	4%
Black or African American	13.8%	12.4%
Native Hawaiian or Other Pacific Islander	.6%	.001%
Other, Please Specify	4.3%	6%
Hispanic	11.8%	14.8%

†The Census reports age breakdowns for 15-19 and 20-25 year olds (i.e. not an 18-24 age range) both of which were 9.2% of the adult population in 2006.

Table 3.2 Descriptive Statistics																			
Variable	Reliability (No. of Items)	Min	Max	Mean	St. Dev	Conc	Trust	Neg Emo	Pos Emo	Trust Prop	Altr	Will	Past Priv Vio	Media Exp	Gend er	Age	Hisp	Race	Inc
Concern	.88 (3)	1.00	7.00	5.42	1.43														
Trust	.93 (3)	1.00	7.00	4.57	1.51	-.06													
Negative Emotion	.95 (12)	1.00	5.00	2.31	1.04	.14	.11												
Positive Emotion	.80 (3)	1.00	5.00	3.18	1.01	.13	.19	-.18											
Trust Propensity	.91 (3)	1.00	7.00	5.17	1.46	.19	.47	.04	.21										
Altruism	.89 (4)	1.00	7.00	5.67	1/05	.29	.20	.03	.26	.32									
Willingnes s to Provide Access	.95 (3)	1.00	7.00	4.22	2.07	-.06	.45	.15	.09	.28	.14								
Past Privacy Violations	n/a	1.00	7.00	3.45	1.73	.29	-.11	.43	-.04	-.07	.04	-.02							
Media Exposure	n/a	1.00	7.00	4.18	1.83	.27	-.09	.21	.08	-.03	.16	-.07	.37						
Gender	n/a	0	1.00	.43	.50	.04	.01†	-.00†	.08	.00†	-.09	-.00†	-.00†	.06					
Age	n/a	1.00	7.00	4.09	1.68	.15	-.02*	-.12	.02	.17	.20	.02	-.18	.04	.17				
Hispanic	n/a	0	1.00	.12	.322	-.04	-.00†	.03	.04	-.03	-.08	-.02	.01*	.01†	.02	-.24			
Race	n/a	1.00	6.00	1.43	1.14	.00†	-.03	.04	.03	-.05	-.05	-.05	.06	.02	.04	-.21	.31		
Income	n/a	1.00	10.00	4.89	2.13	-.03	.01†	-.18	.16	.05	.13	-.02	-.05	.08	.12	.06	-.01*	-.05	
Education	n/a	1.00	8.00	4.72	1.50	-.02	-.06	-.15	.02	-.04	.03	-.07	-.06	.09	.15	.12	-.02	.03*	.37

Table 3.3 Repeated-Measures ANCOVA Table for Willingness to Provide Access to PHI				
Source of Variance	Degrees of Freedom *	Mean Square	F-Statistic *	P-Value
Within-Subjects Factors				
Type	1.59	.473	.145	.816
Type * Concern	1.59	4.134	1.270	.277
Type * Trust	1.59	6.031	1.852	.166
Purpose	1.82	51.538	9.916	.000
Purpose * Concern	1.82	48.845	9.398	.000
Purpose * Trust	1.82	30.277	5.825	.004
Stakeholder	1.97	28.869	5.337	.005
Stakeholder * Concern	1.97	41.142	7.606	.001
Stakeholder * Trust	1.97	17.857	3.301	.038
Between-Subject Factors				
Concern	1	460.887	10.862	.001
Trust	1	11401.753	238.702	.000
Covariates				
Negative Emotion	1	1791.431	42.218	.000
Positive Emotion	1	95.180	2.243	.135
Altruism	1	320.235	7.547	.006
Trust Propensity	1	1358.409	32.013	.000
Medical History	1	6.006	.142	.707
Prior Privacy Violations	1	.234	.006	.941
Media Exposure	1	374.234	8.819	.003
Male	1	15.802	.372	.542
Age	1	72.652	1.712	.191
Hispanic	1	4.786	.113	.737
Race	1	105.161	2.478	.116
Income	1	2.055	.048	.826
Education	1	263.058	6.199	.013
Error(Type)	1012	42.433		
Total N			1089	
Number of observations per subject			27	
R-Squared Within			.20	
R-Squared Between			.32	

* The F-statistic violated the sphericity assumption ($p < .001$) for each of the within-subject factors. The Greenhouse and Geisser (1959) estimates were applied to make conservative corrections to the F-ratio which is reported here.

Table 4.1 Study 1 Table of Risk Estimate Means by Message Cue Condition					
Message Cues		Likelihood (1-7)			DV
Self-View	Risk Domain Frame	Self	Friend	Average Undergrad	Intentions
Independent	Financial (N=23)	3.75 (1.50)	4.49 (.92)	4.86 (1.01)	5.65 (.99)
	Social (N=27)	3.80 (1.48)	4.27 (1.04)	5.18 (1.04)	5.32 (1.32)
Interdependent	Financial (N=23)	3.66 (1.26)	3.93 (.99)	4.49 (1.46)	5.02 (1.07)
	Social (N=26)	3.82 (1.16)	4.02 (1.19)	4.90 (1.15)	5.71 (1.11)

Table 4.2 Study 2 Table of Risk Estimate Means by Message Cue Condition					
Message Cues		Probability (0-100)			DV
Self-View	Goal Frame	Self	Friend	Average Undergrad	Intentions
Control	Negative (N=17)	31.94 (22.19)	50.71 (26.02)	46.71 (26.30)	4.01 (1.57)
	Positive (N=15)	47.73 (26.66)	51 (22.35)	73 (20.64)	3.87 (1.31)
Independent	Negative (N=11)	43.82 (34.69)	48.36 (36.57)	51.55 (36.40)	3.50 (.95)
	Positive (N=14)	38.29 (30.07)	48.93 (25.81)	69.86 (19.06)	3.80 (1.61)
Interdependent	Negative (N=14)	27.64 (23.39)	45.86 (28.77)	61.86 (28.98)	3.80 (1.42)
	Positive (N=13)	54.69 (26.89)	58.85 (22.28)	78.38 (14.36)	4.48 (1.42)

APPENDIX A – FAILURE EXAMPLE

To illustrate the influence of mindfulness in failure response, we provide an example from our qualitative study. IT staff at Customer A perform common maintenance tasks via ad-hoc processes by entering commands directly into the operations terminal instead of requiring the creation of standard pre-written and tested scripts to perform these repeatable processes. “Command line” interfaces such as these are prone to human error as they require the operator to enter complex sequences of instructions, they frequently include default settings that are assumed if the operator does not make modifications, and they lack formal validation checks. An engineer commented on one such circumstance:

They did a “remove” command in a file system and deleted some files in production. [The operator] thought he was running in a test environment but he wasn’t. This was not a user but an operator with [direct system] access. He tried to abort a couple of seconds later after he realized the problem. No one knows how much was deleted. Best practice would indicate no one should log in with [direct access]. Freeware tools are available that require longer commands be issued and prompt with “are you sure you want to do this?” as a safeguard. I was surprised that they don’t use [the freeware].

This is an example of a failure occurring in a not novel context for the organization. The organization is familiar with the actions taken leading up to the failure and knows what must be done to correct it (i.e. recover files) but calls on ProtectCo to help with the resolution process. This failure also illustrates what can happen when no routine is defined for repeatable processes. Collective mindfulness involves high levels of alertness and an appreciation for context (Weick and Sutcliffe 2007). A highly mindful organization will seek to contain this failure by involving individuals with the appropriate expertise and allowing them to make decisions. Additionally, a more mindful organization understands that their technical environment is unique and may be more forthcoming with potentially relevant information and receptive to suggestions from ProtectCo during the resolution process. A less mindful organization encountering the problem may not have a firm handle on “who knows what” in the organization making it difficult to determine which individuals to involve in the failure response. Such organizations also likely have lower skill levels due to a lack of commitment to resilience through training and appropriate hiring and retention strategies. Less experienced individuals are less

able to determine what information is relevant to solving the problem and what is not relevant, which can lead to delays while these individual, who do not understand the failure very well, “come up to speed”.

APPENDIX B – MEASURES AND ITEMS

Preoccupation with Failure (Adapted from Knight 2004)

- Fail1: The customer's IT employees appear to take even the smallest of failures seriously
- Fail2: The customer's IT employees appear to regard close calls and near misses as a kind of failure **
- Fail3: The customer's IT employees generally report work-related failures that could have serious consequences, even if nobody else notices the failure
- Fail4: When failures occur, the customer's IT employees seem to discuss how they could have been prevented *
- Fail5: The customer's IT employees talk about failures and ways to learn from them *

Attention to Operations (Adapted from Knight 2004)

- Ops1: The customer's IT employees appear to be familiar with tasks beyond their own immediate jobs
- Ops2: The customer's IT employees seem to interact often enough with one another to understand what is currently going on within the IT department
- Ops3: The customer's IT employees seem to listen carefully to one another when talking about what is going on in IT operations

Reluctance to Simplify (Adapted from Knight 2004)

- Rel1: Within this customer's IT organization, employees seem to be encouraged to question the status quo **
- Rel2: Within this customer's IT organizations, it appears to be rare that anyone's view is dismissed *
- Rel3: The customer's IT employees appear comfortable expressing differing viewpoints on how work should be done **, *
- Rel4: The customer's IT employees appear to take nothing for granted
- Rel5: The customer's IT employees generally seem to prolong their analysis to better grasp the nature of problems that come up *
- Rel6: The customer's IT employees appear to question the way things are usually done

Commitment to Resilience (Adapted from Knight 2004)

- Comm1: The customer's IT employees appear to be committed to solving any problem that arises
- Comm2: The customer's IT employees do not give up on solving a problem
- Comm3: The customer's IT employees appear to be well trained for the kind of work they do

Deference to Expertise (Adapted from Knight 2004)

- DefExp1: The customer's IT employees appear to be comfortable asking others with more experience within their IT organization for help
- DefExp2: When the customer's IT employees cannot solve a problem, they generally seek someone with more experience within their IT organization to solve it
- DefExp3: At this customer, knowledge appears to be more important than hierarchical position within their IT organization

Collective Mindfulness (Adapted from Knight 2004)

CM1: The customer's employees appear to feel the need to be alert at all times

CM2: The customer employees seem to pay great attention to changes that arise while doing their work

CM3: The customer's employees appear to have a thoughtful, reflective way of tackling tasks†

CM4: When attempting to resolve a problem, the customer's employees take advantage of the unique skills of all employees†

Failure Novelty (Adapted from Gatignon et al. 2002)

Novel1: In order to solve this problem on their own, the customer would have had to learn from completely new or different knowledge bases

Novel2: Responding to this incident required new skills which the customer did not possess

Novel 3: Fundamentally new concepts or principles would have been required for the customer to have solved this problem on their own

Lack of Process (New items)

The following questions address the **processes**⁹, if any, the customer may have used just prior to the incident (and prior to contacting Symantec) that may have contributed to the outage. We are interested in the customer's processes related to this incident and its potential **root cause**. Please indicate the extent of your agreement with the following statements:

Ostensive

DefProc1: The circumstances encountered by the customer did not appear to fit any of the customer's standard processes

DefProc2: No process existed for the customer to follow in the specific situation that led to this failure

Duration

How long was this case open (indicate number of days in digits - e.g. 2 and not "two" or fraction of a day - e.g. .50 for half a day)?

Controls

- Please indicate the number of additional vendors involved (i.e. not including ProtectCo and the customer itself) in the case:
- This customer appears to have a large number of vendors and products as part of its IT configuration
- This customer appears to support a wide range of ages in its products (e.g. legacy systems, different versions of software, etc).
- What product (or products) was (were) involved in this case (select all that apply)?
- What is the customer's industry sector?

* Dropped after the pilot; ** Added after the pilot; † Dropped after factor analysis

⁹ Note that during our qualitative research, participants used the term "process" more often than "routine" to describe pre-defined steps to be taken for repeatable actions. Respondents involved in the pilot testing also noted that the term "routine" was less familiar to them. Therefore, we used "process" throughout the instrument.

APPENDIX C – SORT RESULTS

The first sort was conducted with 10 sorters, recruited from among the PhD business students in a large university, on 15 items across 6 constructs (5 dimensions and CM). The results of the initial sort yielded an overall placement ratio of items within the target construct of 69%, meaning that the judges placed the item in the appropriate target category only 69% of the time. The attention to operations dimension was particularly problematic with almost half of the items placed on the collective mindfulness target. In addition, the collective mindfulness construct received a low placement ratio of items on the target (55%) because many of its items cross loaded with deference to expertise and reluctance to simplify. We then carefully scrutinized our conceptual definitions for clarity, added some items and modified a few others. For example, the use of the word “scrutiny” in the collective mindfulness definition and “skepticism” in reluctance to simplify definition were too similar (considered to be a source of confounding). So, we modified the definition of collective mindfulness to be broader and more encompassing. Finally, several of the attention to operations items cross loaded with collective mindfulness, so two items were reworded to be more specific about the current state of the system.

We then conducted another round of sorting with new judges. This second sort showed improvement over the first with an overall placement ratio of items within the target construct of 77%. Several items from reluctance to simplify, attention to operations and commitment to resilience continue to cross load on the collective mindfulness target. This is to be expected due to the multi-dimensional nature of the construct. Therefore, we removed collective mindfulness from the sort analysis to examine the conceptual clarity across the 5 dimensions of mindfulness. This analysis revealed an overall placement ratio of 87%. Given the nature of the

collective mindfulness construct and its dimensions, this ratio of placement of items within the target constructs demonstrates acceptable construct validity and potential reliability.

Round 1 Sort Results

	Actual Categories							
Target Category	Def to Expertise	Preoc w/Failure	Rel to Simpl	Atten to Ops	Commit to Resil.	CM	Total	Target %
Def to Expertise	17		1			2	20	85%
Preoc w/Failure		22			3	3	28	79%
Reluctance to Simplify	1		15	2		2	20	75%
Atten to Operations	1		1	14		13	29	45%
Commit to Resil		1	1	3	15		20	75%
CM	5		2	1	1	11	20	55%
Item Placements: 137			Hits: 94			Overall Hit Ratio: 69%		

Round 2 Sort Results (including Collective Mindfulness)

	Actual Categories							
Target Category	Def to Expertise	Preoc w/Failure	Rel to Simpl	Atten to Ops	Commit to Resil.	CM	Total	Target %
Def to Expertise	25					1	26	96%
Preoc w/Failure		22		1	4		27	81%
Reluctance to Simplify	2		13	1		2	18	72%
Atten to Operations			2	17		6	25	68%
Commit to Resil				4	20	2	26	75%
CM		3	1	5	1	17	27	63%
Item Placements: 149			Hits: 114			Overall Hit Ratio: 77%		

Round 2 Sort Results (excluding Collective Mindfulness)

	Actual Categories						
Target Category	Def to Expertise	Preoc w/Failure	Rel to Simpl	Atten to Ops	Commit to Resil.	Total	Target %
Def to Expertise	25				1	26	96%
Preoc w/Failure		22		1	4	27	81%
Reluctance to Simplify	2		13	1		16	81%
Atten to Operations			2	17		19	89%
Commit to Resil				4	20	24	83%
Item Placements: 112			Hits: 97		Overall Hit Ratio: 87%		

APPENDIX D – FACTOR ANALYSIS

	Component						
	1	2	3	4	5	6	7
Fail1			.684				
Fail2			.874				
Fail3			.630				
Ops1					.553		
Ops2					.857		
Ops3					.905		
Rel1	.591						
Rel4	.714						
Rel6	.770						
Comm1						.925	
Comm2						.698	
Comm3						.772	
DefExp1	.650						
DefExp2	.784						
DefExp3	.712						
ProcDef1				.912			
ProcDef2				.895			
Novel1		.857					
Novel2		.905					
Novel3		.834					
CM1							-.809
CM2							-.644

Extraction Method: Principal Component Analysis.

Rotation Method: Oblimin with Kaiser Normalization.

- a. Rotation converged in 19 iterations.
- b. Loadings below .40 suppressed

APPENDIX E – ESSAY 2 MEASUREMENT ITEMS

Construct	Measure
WILLING1 ¹⁰	Unlikely/Likely
WILLING2	Not Probable/Probably
WILLING3	Unwilling/Willing
TRUST1	The electronic/digital storage format of health information is a safe environment in which to exchange health information with others
TRUST2	The digital storage format is a reliable environment in which to conduct health related transactions
TRUST3	Organizations handle personal health information submitted by patients in an electronic format in a competent fashion
CONCERN1	Compared with other subjects on my mind, the privacy of my electronic personal health information is very important
CONCERN2	I am concerned about threats to the privacy of my electronically stored personal health information today
CONCERN3	All things considered, I believe the privacy of my electronic personal health information is seriously threatened
NEGEMOT1	Right now I feel sad about something that has happened to my health
NEGEMOT2	I feel disgust for my current state of health
NEGEMOT3	I have an intense loathing for my present state of health
NEGEMOT4	I feel furious at my present state of health
NEGEMOT5	I feel very deep sorrow because of my health
NEGEMOT6	Right now other things in my life will have to wait
NEGEMOT7	My current health state is a real inconvenience
NEGEMOT8	I am extremely displeased with my present health state
NEGEMOT9	Health problems are tiresome to me
NEGEMO10	My present health problems fill me with dread
NEGEMO11	Recent experience has warned me to be more cautious about my health
NEGEMO12	I feel everything needs to be approached with caution right now
JOY1	My spirits are high today
JOY2	I feel ecstatic about life right now
JOY3	I am happy about my health right now
ALT1	Helping others is one of the most important aspects of life.
ALT2	I enjoy working for the welfare of others

¹⁰ More detail regarding the measurement of Willingness to Disclose digital PHI is provided in Appendix F because the wording changed for each of the 27 combinations of type of information (3), requesting stakeholder (3) and purpose of use (3) for which willingness was captured.

- ALT3 My family tends to do what we can to help those less fortunate than ourselves.
- ALT4 I agree with the old saying, "It is better to give than to receive."
- TP1 I usually trust people until they give me a reason not to trust them
- TP2 I usually give people the benefit of the doubt
- TP3 My general approach is to trust new acquaintances until they prove I should not trust them

Controls

Past privacy violations: How frequently have you personally been the victim of what you felt was an improper invasion of privacy? (1=very infrequently; 7=very frequently)

Very infrequently 1 --- 2 --- 3 --- 4 --- 5 --- 6 --- 7 Very frequently

Media exposure: How much have you heard or read during the last year about the use and potential misuse of health information collected electronically? (1=not at all; 7=very much)

Not at all 1 --- 2 --- 3 --- 4 --- 5 --- 6 --- 7 Very much

Computer experience: How many years of experience do you have using computers?

How would you rate your computer skills?

- ☐ 1 None
- ☐ 2 Very little
- ☐ 3 Average
- ☐ 4 Quite extensive
- ☐ 5 Very extensive

How frequently do you schedule doctor appointments for yourself?

- ☐ More than once a month
- ☐ Every 1 to 2 months
- ☐ Every 3 to 6 months
- ☐ Every 7 to 12 months
- ☐ Less than once a year

Do you have a chronic illness? (check all that apply)

- ☐ No, I don't
- ☐ Heart Disease/Congestive Heart Failure (CHF)
- ☐ Diabetes (Sugar)
- ☐ Asthma
- ☐ Cancer (any type)
- ☐ High Blood Pressure/Hypertension
- ☐ AIDS/HIV
- ☐ Arthritis
- ☐ Hypothyroidism
- ☐ Back problems/surgery
- ☐ High cholesterol
- ☐ Depression
- ☐ Known genetic disorder (any type)
- ☐ Other, Please Specify

What is your gender?

- ☐ Male
- ☐ Female

What is your age?

- ☐ 18-24
- ☐ 25-34
- ☐ 35-44
- ☐ 45-54
- ☐ 55-64
- ☐ 65-74
- ☐ over 75

Are you Spanish/Hispanic/Latino? Yes/No?

What is your race (select the one race you most consider yourself to be):

- ☐ 1 White
- ☐ 2 Black or African American
- ☐ 3 Asian
- ☐ 4 Native Hawaiian or Other Pacific Islander
- ☐ 5 Other, please specify

Which category represents the total combined income of your household during the past 12 months?

- ☐ Less than \$10,000
- ☐ \$10,000 to \$14,999
- ☐ \$15,000 to \$24,999
- ☐ \$25,000 to \$34,999
- ☐ \$35,000 to \$49,999
- ☐ \$50,000 to \$74,999
- ☐ \$75,000 to \$99,999
- ☐ \$100,000 to \$149,999
- ☐ \$150,000 to \$199,999
- ☐ \$200,000 or more

What is the highest level of school you have completed or the highest degree you have received?

- ☐ 8th grade or less
- ☐ Some high school, no diploma
- ☐ High School Graduate or equivalent (For example: GED)
- ☐ Some college but no degree
- ☐ Associate degree in college
- ☐ Bachelors degree (For example: BA, AB, BS)
- ☐ Master's degree (For example: MA, MS, MEng, MEd, MSW, MBA)
- ☐ Professional/Doctorate Degree (For example: MD, DDS, JD, PhD, EdD)

APPENDIX F – INSTRUMENT USED FOR DATA COLLECTION

Note the following:

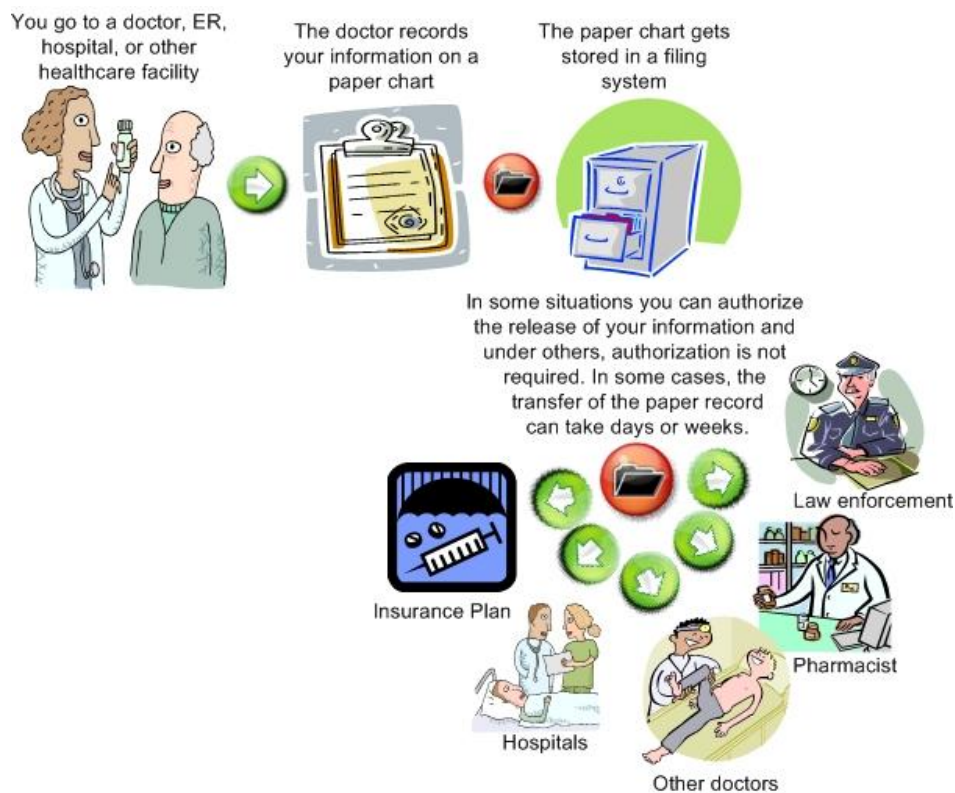
1. Respondents were administered the instrument provided on the following pages for collecting the data used in this study. This is not the complete instrument, which also contained items for constructs such as concern, trust, etc. The items for those were included in Appendix E.
2. At various places in the instrument we have placed text in parentheses labeled [Note:...]. This is purely for explanatory purposes and was not part of the survey.

INTRODUCTION

Thank you for agreeing to participate in this important study! This is an interactive survey in which you will be presented with various scenarios in which your personal health information may be made available for use by different entities involved in providing you with care. You will be asked to respond to questions about its use in different situations. Prior to beginning this survey, we provide some basic explanations.

In all likelihood, your health information is currently stored in multiple locations and in a variety of formats. Your primary care physicians and hospitals have health records for you; the pharmacy has information on your prescriptions and insurance benefits; the labs have information about tests performed on you; and your insurance company collects data on the payments made on your behalf (an illustration of this is shown below in the Current Scenario). Some of this information is shared and common (as between the doctor and insurance company, for example) but much is not. There is work involved to keep all of this information consistent as you may have noticed, for example, if you move and need to change your address on file with the doctor's office, pharmacy, hospital and others.

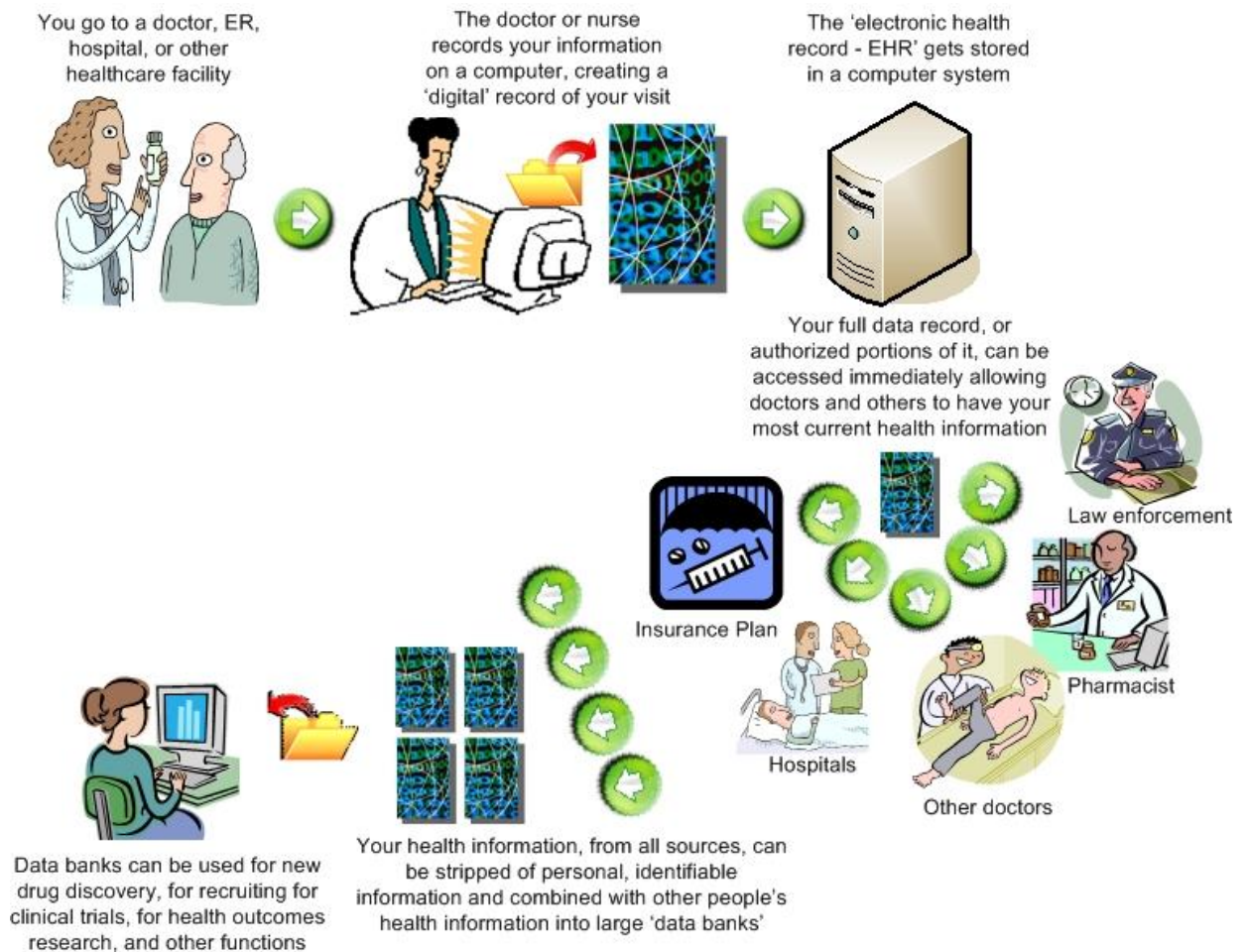
Current Scenario



The situation described above is in the process of changing. Recently you may have read, or seen on TV, that there are efforts underway at the state and federal level to create an electronic health record (EHR) for every person in the USA¹¹. Some states are well on their way to reaching this goal. In the illustration below, we describe a 'Digital Scenario' in which your health information is put into a computer system. A system like this allows your records to be accessed in a 'digital' or electronic format that is more accessible to those involved in your care. It also makes your information available to doctors if you are traveling out of state and need medical care. Finally, it could also improve information available for research on health trends and new drugs.

In summary, if your personally identifiable health information is digitized (i.e. stored electronically), it can conceivably be shared much more easily with a number of entities for a variety of purposes.

Digital Scenario



¹¹ Transforming Health Care for Americans with Health Information Technology, <http://www.whitehouse.gov/news/releases/2004/05/print/20040527-5.html>

All of the questions below relate to the “Digital Scenario” presented above. Therefore we ask you to respond to each question with the understanding that your health information will be entered into a computerized system. There are no right or wrong answers and we are only interested in your opinion. We ask that you do not skip any questions.

SECTION 1 Access to Identifiable Data

The following questions address your willingness to share specific types of digitally stored *personally identifiable* health information with different stakeholders for various purposes. In other words, the recipient of the information will know that it refers to you.

[Note: This section refers to general health information (type of information) for the purposes of marketing. Within each subsection like this one, the respondent is asked questions about each of the 3 stakeholders (hospital, pharmaceutical company, government). This label heading not included in the actual survey.]

For the following series of questions, please think of *general health* information as potentially including such information as cholesterol level, blood pressure, fitness, weight, and overall medical condition.

Please note that after each question is posed, there are 3 items to which you must respond in order for us to accurately get a good impression of your intentions for this research. Thank you in advance for your patience.

A hospital may be interested in contacting you regarding a new clinic being constructed which may be relevant to your health. Specify the extent to which you would be willing to grant a <u>hospital</u> access to your personal <i>general health</i> information for such purposes:									
<i>Unlikely</i>	1	2	3	4	5	6	7	<i>Likely</i>	
<i>Not Probable</i>	1	2	3	4	5	6	7	<i>Probably</i>	
<i>Unwilling</i>	1	2	3	4	5	6	7	<i>Willing</i>	
A pharmaceutical company (e.g. Pfizer, Merck, Johnson and Johnson) may be interested in distributing brochures describing the medications they manufacture that may be useful in treating certain health related problems. Specify the extent to which you would be willing to grant a <u>pharmaceutical company</u> access to your personal <i>general health</i> information for such purposes:									
<i>Unlikely</i>	1	2	3	4	5	6	7	<i>Likely</i>	
<i>Not Probable</i>	1	2	3	4	5	6	7	<i>Probably</i>	
<i>Unwilling</i>	1	2	3	4	5	6	7	<i>Willing</i>	
A governmental/public health agency may be interested in distributing brochures describing current health trends or publicizing the availability of specific health resources in your area. Specify the extent to which you would be willing to grant a <u>governmental/ public health agency</u> access to your personal <i>general health information</i> for such purposes:									
<i>Unlikely</i>	1	2	3	4	5	6	7	<i>Likely</i>	
<i>Not Probable</i>	1	2	3	4	5	6	7	<i>Probably</i>	
<i>Unwilling</i>	1	2	3	4	5	6	7	<i>Willing</i>	

[Note: This section refers to genetic health information (type of information) for the purposes of marketing. This label heading not included in the actual survey.]

For the following questions, please think of genetic health information as potentially including such information as the results of testing conducted for disease prediction and diagnosis (e.g. Huntington’s disease or inherited forms of the breast cancer gene) or results of testing conducted for the purposes of finding interactions between diet and genes to maximize quality of life and avoid disease (e.g. an increased need for vitamin D which could be linked to osteoporosis, cancer and other health conditions).

A hospital may be interested in contacting you regarding a new service being offered or the hospital may want to sell your information to a third party to market products to you relevant to your health. Specify the extent to which you would be willing to grant a hospital access to your personal *genetic* information for such purposes:

<i>Unlikely</i>	1	2	3	4	5	6	7	<i>Likely</i>
<i>Not Probable</i>	1	2	3	4	5	6	7	<i>Probably</i>
<i>Unwilling</i>	1	2	3	4	5	6	7	<i>Willing</i>

A pharmaceutical company may be interested in distributing brochures describing the medications they manufacture that may be useful in treating certain health related problems. Specify the extent to which you would be willing to grant a pharmaceutical company access to your personal *genetic* information for such purposes:

<i>Unlikely</i>	1	2	3	4	5	6	7	<i>Likely</i>
<i>Not Probable</i>	1	2	3	4	5	6	7	<i>Probably</i>
<i>Unwilling</i>	1	2	3	4	5	6	7	<i>Willing</i>

A governmental/public health agency may be interested in distributing brochures describing current health trends or publicizing the availability of specific health resources in your area. Specify the extent to which you would be willing to grant a governmental/ public health agency access to your personal *genetic* information for such purposes:

<i>Unlikely</i>	1	2	3	4	5	6	7	<i>Likely</i>
<i>Not Probable</i>	1	2	3	4	5	6	7	<i>Probably</i>
<i>Unwilling</i>	1	2	3	4	5	6	7	<i>Willing</i>

[Note: This section refers to mental health information (type of information) for the purposes of marketing. This label heading not included in the actual survey.]

For the following questions, please think of *mental health* information as potentially including information about treatment at a mental hospital, medications taken for depression or anxiety, therapy or counseling.

A hospital may be interested in contacting you regarding a new mental health clinic being constructed or the hospital may want to sell your information to a third party to market products to you relevant to your mental health condition. Specify the extent to which you would be willing to grant a hospital access to your personal *mental health* information for such purposes:

<i>Unlikely</i>	1	2	3	4	5	6	7	<i>Likely</i>
<i>Not Probable</i>	1	2	3	4	5	6	7	<i>Probably</i>
<i>Unwilling</i>	1	2	3	4	5	6	7	<i>Willing</i>

A pharmaceutical company may be interested in distributing brochures describing the medications they manufacture that may be useful in treating mental health related problems. Specify the extent to which you would be willing to grant a pharmaceutical company access to your personal *mental health* information for such purposes:

<i>Unlikely</i>	1	2	3	4	5	6	7	<i>Likely</i>
<i>Not Probable</i>	1	2	3	4	5	6	7	<i>Probably</i>
<i>Unwilling</i>	1	2	3	4	5	6	7	<i>Willing</i>

A governmental/public health agency may be interested in distributing brochures describing current mental health trends or the availability of mental health resources in your area. Specify the extent to which you would be willing to grant a governmental/ public health agency access to your personal *mental health* information for such purposes:

<i>Unlikely</i>	1	2	3	4	5	6	7	<i>Likely</i>
<i>Not Probable</i>	1	2	3	4	5	6	7	<i>Probably</i>
<i>Unwilling</i>	1	2	3	4	5	6	7	<i>Willing</i>

[Note: This section refers to general health information (type of information) for the purposes of research. This label heading not included in the actual survey.]

As a reminder, please think of *general health* information as potentially including such information as cholesterol level, blood pressure, fitness, weight, chronic illness, family history, etc.

A university teaching hospital may be interested in conducting research on patients with specific conditions and may be interested in contacting you for participation in related health studies. Specify the extent to which you would be willing to grant a <u>hospital</u> access to your personal <i>general health</i> information for such purposes:								
<i>Unlikely</i>	1	2	3	4	5	6	7	<i>Likely</i>
<i>Not Probable</i>	1	2	3	4	5	6	7	<i>Probably</i>
<i>Unwilling</i>	1	2	3	4	5	6	7	<i>Willing</i>
A pharmaceutical company may be interested in recruiting patients for participation in clinical trials being conducted to test new drug treatments for certain health conditions. Specify the extent to which you would be willing to grant a <u>pharmaceutical company</u> access to your personal <i>general health</i> information for such purposes:								
<i>Unlikely</i>	1	2	3	4	5	6	7	<i>Likely</i>
<i>Not Probable</i>	1	2	3	4	5	6	7	<i>Probably</i>
<i>Unwilling</i>	1	2	3	4	5	6	7	<i>Willing</i>
A governmental/public health agency may be interested in recruiting patients for participation in clinical trials being conducted to test new drug treatments for certain health conditions. Specify the extent to which you would be willing to grant a <u>governmental/ public health agency</u> access to your personal <i>general health</i> information for such purposes:								
<i>Unlikely</i>	1	2	3	4	5	6	7	<i>Likely</i>
<i>Not Probable</i>	1	2	3	4	5	6	7	<i>Probably</i>
<i>Unwilling</i>	1	2	3	4	5	6	7	<i>Willing</i>

[Note: This section refers to genetic health information (type of information) for the purposes of research. This label heading not included in the actual survey.]

As a reminder, please think of *genetic health* information as potentially including such information as the results of testing conducted for disease prediction and diagnosis (e.g. Huntington's disease or inherited forms of the breast cancer gene) or results of testing conducted for the purposes of finding interactions between diet and genes to maximize quality of life and avoid disease (e.g. an increased need for vitamin D which could be linked to osteoporosis, cancer and other health conditions).

A university teaching hospital may be interested in conducting research on patients with specific genetic conditions and may be interested in contacting you for participation in related health studies. Specify the extent to which you would be willing to grant a <u>hospital</u> access to your personal <i>genetic</i> information for such purposes:								
<i>Unlikely</i>	1	2	3	4	5	6	7	<i>Likely</i>
<i>Not Probable</i>	1	2	3	4	5	6	7	<i>Probably</i>
<i>Unwilling</i>	1	2	3	4	5	6	7	<i>Willing</i>
A pharmaceutical company may be interested in recruiting patients for participation in clinical trials being conducted to test new drug treatments or therapies for certain genetic conditions. Specify the extent to which you would be willing to grant a <u>pharmaceutical company</u> access to your personal <i>genetic</i> information for such purposes:								
<i>Unlikely</i>	1	2	3	4	5	6	7	<i>Likely</i>
<i>Not Probable</i>	1	2	3	4	5	6	7	<i>Probably</i>
<i>Unwilling</i>	1	2	3	4	5	6	7	<i>Willing</i>

A governmental/public health agency may be interested in recruiting patients for participation in clinical trials being conducted to test new drug treatments or therapies for certain genetic conditions. Specify the extent to which you would be willing to grant a <u>governmental/ public health agency</u> access to your personal <i>genetic</i> information for such purposes:								
<i>Unlikely</i>	1	2	3	4	5	6	7	<i>Likely</i>
<i>Not Probable</i>	1	2	3	4	5	6	7	<i>Probably</i>
<i>Unwilling</i>	1	2	3	4	5	6	7	<i>Willing</i>

[Note: This section refers to mental health information (type of information) for the purposes of research. This label heading not included in the actual survey.]

As a reminder, please think of *mental health* information as potentially including information about treatment at a mental hospital, medications taken for depression or anxiety, therapy or counseling.

A hospital may be interested in conducting research on patients with specific conditions and may be interested in contacting you for participation in mental health related studies. Specify the extent to which you would be willing to grant a <u>hospital</u> access to your personal <i>mental health</i> information for such purposes:								
<i>Unlikely</i>	1	2	3	4	5	6	7	<i>Likely</i>
<i>Not Probable</i>	1	2	3	4	5	6	7	<i>Probably</i>
<i>Unwilling</i>	1	2	3	4	5	6	7	<i>Willing</i>

A pharmaceutical company may be interested in recruiting patients for participation in clinical trials being conducted to test new drug treatments for mental health conditions. Specify the extent to which you would be willing to grant a pharmaceutical company access to your personal *mental health* information for such purposes:

<i>Unlikely</i>	1	2	3	4	5	6	7	<i>Likely</i>
<i>Not Probable</i>	1	2	3	4	5	6	7	<i>Probably</i>
<i>Unwilling</i>	1	2	3	4	5	6	7	<i>Willing</i>

A governmental/public health agency may be interested in recruiting patients for participation in clinical trials being conducted to test new drug treatments for certain mental health conditions. Specify the extent to which you would be willing to grant a governmental/ public health agency access to your personal *mental health* information for such purposes:

<i>Unlikely</i>	1	2	3	4	5	6	7	<i>Likely</i>
<i>Not Probable</i>	1	2	3	4	5	6	7	<i>Probably</i>
<i>Unwilling</i>	1	2	3	4	5	6	7	<i>Willing</i>

[Note: This section refers to general health information (type of information) for the purposes of patient care. This label heading not included in the actual survey.]

As a reminder, please think of *general health* information as potentially including such information as cholesterol level, blood pressure, fitness, weight, chronic illness, family history, etc.

You are in an accident and are taken to a local hospital emergency room. The hospital physicians request access to your digital health records in order to treat you effectively. Specify the extent to which you would be willing to grant a <u>hospital (and its physicians)</u> access to your personal <i>general health</i> information for such purposes:								
<i>Unlikely</i>	1	2	3	4	5	6	7	<i>Likely</i>
<i>Not Probable</i>	1	2	3	4	5	6	7	<i>Probably</i>
<i>Unwilling</i>	1	2	3	4	5	6	7	<i>Willing</i>

Your physician informs you that you may benefit (i.e. your health may improve) from participating in a clinical trial. Specify the extent to which you would be willing to grant a pharmaceutical company access to your personal *general health* information for the purpose of recruitment and participation in a clinical trial to receive healthcare:

<i>Unlikely</i>	1	2	3	4	5	6	7	<i>Likely</i>
<i>Not Probable</i>	1	2	3	4	5	6	7	<i>Probably</i>
<i>Unwilling</i>	1	2	3	4	5	6	7	<i>Willing</i>

A governmental/public health agency may be administering free immunizations or other services and request access to check your medical record to check for allergies or other relevant history. Specify the extent to which you would be willing to grant a governmental/ public health agency access to your personal *general health* information for such purposes:

<i>Unlikely</i>	1	2	3	4	5	6	7	<i>Likely</i>
<i>Not Probable</i>	1	2	3	4	5	6	7	<i>Probably</i>
<i>Unwilling</i>	1	2	3	4	5	6	7	<i>Willing</i>

[Note: This section refers to genetic health information (type of information) for the purposes of patient care. This label heading not included in the actual survey.]

As a reminder, please think of *genetic health* information as potentially including such information as the results of testing conducted for disease prediction and diagnosis (e.g. Huntington's disease or inherited forms of the breast cancer gene) or results of testing conducted for the purposes of finding interactions between diet and genes to maximize quality of life and avoid disease (e.g. an increased need for vitamin D which could be linked to osteoporosis, cancer and other health conditions).

You are in an accident and are taken to a local hospital emergency room. The hospital physician believes you may have a genetic condition and requests access to your genetic information records in order to treat you effectively. Specify the extent to which you would be willing to grant a hospital access to your personal *genetic* information for such purposes:

<i>Unlikely</i>	1	2	3	4	5	6	7	<i>Likely</i>
<i>Not Probable</i>	1	2	3	4	5	6	7	<i>Probably</i>
<i>Unwilling</i>	1	2	3	4	5	6	7	<i>Willing</i>

Your physician informs you that you may benefit (i.e. your health related to your genetic condition may improve) from participating in a clinical trial. Specify the extent to which you would be willing to grant a pharmaceutical company access to your personal *genetic* information for the purpose of recruitment and participation in a clinical trial to receive genetic condition-related care:

<i>Unlikely</i>	1	2	3	4	5	6	7	<i>Likely</i>
<i>Not Probable</i>	1	2	3	4	5	6	7	<i>Probably</i>
<i>Unwilling</i>	1	2	3	4	5	6	7	<i>Willing</i>

A governmental/public health agency may be administering free genetic counseling services and request access to check your genetic information for relevant history. Specify the extent to which you would be willing to grant a governmental/ public health agency access to your personal *genetic* information for such purposes:

<i>Unlikely</i>	1	2	3	4	5	6	7	<i>Likely</i>
<i>Not Probable</i>	1	2	3	4	5	6	7	<i>Probably</i>
<i>Unwilling</i>	1	2	3	4	5	6	7	<i>Willing</i>

[Note: This section refers to mental health information (type of information) for the purposes of patient care. This label heading not included in the actual survey.]

As a reminder, please think of *mental health* information as potentially including information about treatment at a mental hospital, medications taken for depression or anxiety, therapy or counseling.

You are in an accident and are taken to a local hospital emergency room. The hospital physician believes you may have a history of mental health problems and requests access to your mental health records in order to treat you effectively. Specify the extent to which you would be willing to grant a <u>hospital</u> access to your personal <i>mental health</i> information for such purposes:									
<i>Unlikely</i>	1	2	3	4	5	6	7	<i>Likely</i>	
<i>Not Probable</i>	1	2	3	4	5	6	7	<i>Probably</i>	
<i>Unwilling</i>	1	2	3	4	5	6	7	<i>Willing</i>	
Your physician informs you that you may benefit (i.e. your mental health may improve) from participating in a clinical trial. Specify the extent to which you would be willing to grant a <u>pharmaceutical company</u> access to your personal <i>mental health</i> information for the purpose of participating in a clinical trial to receive mental health-related care:									
<i>Unlikely</i>	1	2	3	4	5	6	7	<i>Likely</i>	
<i>Not Probable</i>	1	2	3	4	5	6	7	<i>Probably</i>	
<i>Unwilling</i>	1	2	3	4	5	6	7	<i>Willing</i>	
A governmental/public health agency may be administering free mental health services and request access to check your medical record for relevant history. Specify the extent to which you would be willing to grant a <u>governmental/ public health agency</u> access to your personal <i>mental health</i> information for such purposes:									
<i>Unlikely</i>	1	2	3	4	5	6	7	<i>Likely</i>	
<i>Not Probable</i>	1	2	3	4	5	6	7	<i>Probably</i>	
<i>Unwilling</i>	1	2	3	4	5	6	7	<i>Willing</i>	

SECTION 3 – Hypothetical health scenario

[Note: This question was used to assess the existence of an empathy gap. This label heading not included in the actual survey.]

Imagine that you have been recently diagnosed with an advanced stage of colon cancer. During a visit to your oncologist to discuss treatment options for your cancer, the doctor asks you if you would be willing to have your personal health information shared with a pharmaceutical company for the purposes of clinical trial research. If you agree to grant the pharmaceutical company access to your health information, the company would have access to your health information until such time as you chose to revoke this access and could contact you regarding clinical trials you may be eligible to participate in for the purposes of testing new drug treatments. You would be under no obligation to participate in any trial. Given this situation, specify the extent to which you would grant access to your personal health information to a pharmaceutical company?									
<i>Unlikely</i>	1	2	3	4	5	6	7	<i>Likely</i>	
<i>Not Probable</i>	1	2	3	4	5	6	7	<i>Probably</i>	
<i>Unwilling</i>	1	2	3	4	5	6	7	<i>Willing</i>	

APPENDIX G – PRINCIPAL COMPONENT ANALYSIS

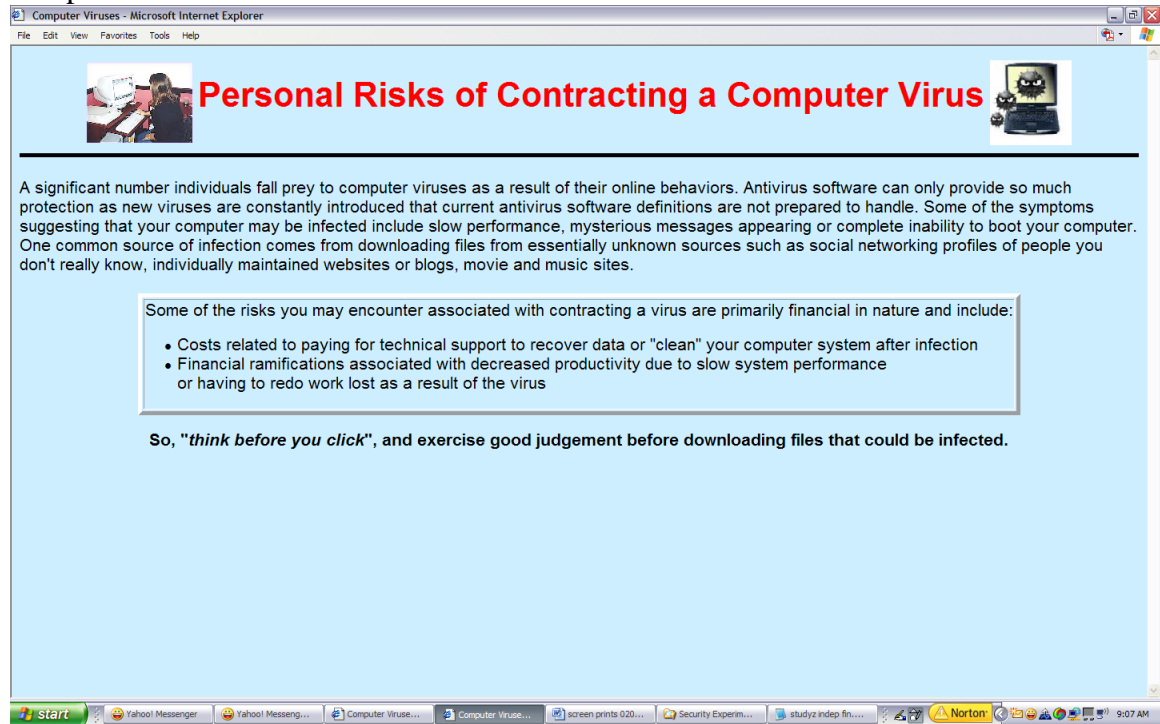
	COMPONENT					
	NEGATIVE EMOTION	ALTRUISM	TRUST	TRUST PROPENSITY	CONCERN	POSITIVE EMOTION
CONCERN1					.862	
CONCERN2					.925	
CONCERN3					.847	
TP1				.880		
TP2				.879		
TP3				.861		
TRUST1			.912			
TRUST2			.918			
TRUST3			.861			
NEGEMOT1	.750					
NEGEMOT2	.792					
NEGEMOT3	.773					
NEGEMOT4	.633					
NEGEMOT5	.849					
NEGEMOT6	.653					
NEGEMOT7	.856					
NEGEMOT8	.890					
NEGEMOT9	.883					
NEGEMO10	.888					
NEGEMO11	.686					
NEGEMO12	.888					
JOY1						.801
JOY2						.846
JOY3						.743
ALT1		.847				
ALT2		.872				
ALT3		.800				
ALT4		.844				

Extraction Method: Principal Component Analysis; Rotation Method: Varimax with Kaiser Normalization
Scores below .4 have been suppressed

APPENDIX H – STUDY MANIPULATIONS

Study 1

Independent/Financial Risk



The screenshot shows a Microsoft Internet Explorer window titled 'Computer Viruses - Microsoft Internet Explorer'. The page has a light blue background and a red title 'Personal Risks of Contracting a Computer Virus'. It features two small images: one of a person at a computer and another of a computer monitor with a virus icon. The text on the page discusses the risks of contracting a computer virus, mentioning symptoms like slow performance and the inability to boot the computer. It also lists financial risks such as costs for technical support and decreased productivity. A box highlights these financial risks, and a concluding sentence advises users to 'think before you click'.

Personal Risks of Contracting a Computer Virus

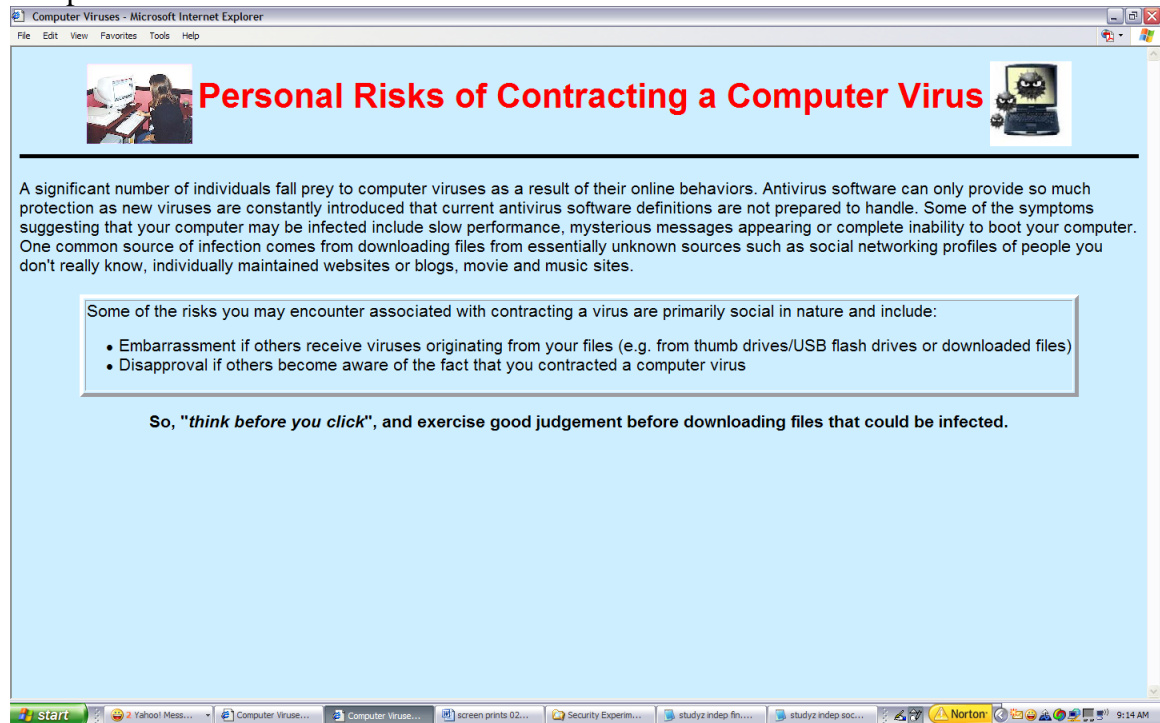
A significant number of individuals fall prey to computer viruses as a result of their online behaviors. Antivirus software can only provide so much protection as new viruses are constantly introduced that current antivirus software definitions are not prepared to handle. Some of the symptoms suggesting that your computer may be infected include slow performance, mysterious messages appearing or complete inability to boot your computer. One common source of infection comes from downloading files from essentially unknown sources such as social networking profiles of people you don't really know, individually maintained websites or blogs, movie and music sites.

Some of the risks you may encounter associated with contracting a virus are primarily financial in nature and include:

- Costs related to paying for technical support to recover data or "clean" your computer system after infection
- Financial ramifications associated with decreased productivity due to slow system performance or having to redo work lost as a result of the virus

So, "*think before you click*", and exercise good judgement before downloading files that could be infected.

Independent/Social Risk



The screenshot shows a Microsoft Internet Explorer window titled 'Computer Viruses - Microsoft Internet Explorer'. The page has a light blue background and a red title 'Personal Risks of Contracting a Computer Virus'. It features two small images: one of a person at a computer and another of a computer monitor with a virus icon. The text on the page discusses the risks of contracting a computer virus, mentioning symptoms like slow performance and the inability to boot the computer. It also lists social risks such as embarrassment and disapproval. A box highlights these social risks, and a concluding sentence advises users to 'think before you click'.

Personal Risks of Contracting a Computer Virus

A significant number of individuals fall prey to computer viruses as a result of their online behaviors. Antivirus software can only provide so much protection as new viruses are constantly introduced that current antivirus software definitions are not prepared to handle. Some of the symptoms suggesting that your computer may be infected include slow performance, mysterious messages appearing or complete inability to boot your computer. One common source of infection comes from downloading files from essentially unknown sources such as social networking profiles of people you don't really know, individually maintained websites or blogs, movie and music sites.

Some of the risks you may encounter associated with contracting a virus are primarily social in nature and include:

- Embarrassment if others receive viruses originating from your files (e.g. from thumb drives/USB flash drives or downloaded files)
- Disapproval if others become aware of the fact that you contracted a computer virus

So, "*think before you click*", and exercise good judgement before downloading files that could be infected.

Study 1

Interdependent/Financial Risk



The screenshot shows a Microsoft Internet Explorer window titled 'Computer Viruses - Microsoft Internet Explorer'. The address bar is empty. The page has a light blue background. At the top, there is a header with a network diagram icon on the left and a computer with a virus icon on the right. The title 'Our Risks of Contracting a Computer Virus' is centered in red. Below the header, there is a paragraph of text. A box contains a list of financial risks. At the bottom of the box, there is a concluding sentence. The taskbar at the bottom shows the Start button, several open applications (Yahoo! Messenger, Computer Viruses, screen prints, Security Explorer, and three instances of 'studyz inter...'), and the system clock showing 9:18 AM.

Our Risks of Contracting a Computer Virus

A significant number of your friends and family members will fall prey to computer viruses as a result of their online behaviors. Antivirus software can only provide so much protection as new viruses are constantly introduced that current antivirus software definitions are not prepared to handle. Some of the symptoms suggesting that your computer may be infected include slow performance, mysterious messages appearing or complete inability to boot your computer. One common source of infection comes from downloading files from essentially unknown sources such as social networking profiles of people you don't really know, individually maintained websites or blogs, movie and music sites.

Some of the risks you, your friends and family members may encounter associated with contracting a virus are primarily financial in nature and include:

- Costs related to paying for technical support to recover data or "clean" computer systems after infection
- Financial ramifications associated with decreased productivity due to slow system performance or having to redo work lost as a result of the virus

So, each of us should "think before we click", and exercise good judgement before downloading files that could be infected.

Interdependent/Social Risk



The screenshot shows a Microsoft Internet Explorer window titled 'Computer Viruses - Microsoft Internet Explorer'. The address bar is empty. The page has a light blue background. At the top, there is a header with a network diagram icon on the left and a computer with a virus icon on the right. The title 'Our Risks of Contracting a Computer Virus' is centered in red. Below the header, there is a paragraph of text. A box contains a list of social risks. At the bottom of the box, there is a concluding sentence. The taskbar at the bottom shows the Start button, several open applications (Yahoo! Messenger, Internet Explorer, screen prints, Security Explorer, and four instances of 'studyz inter...'), and the system clock showing 9:20 AM.

Our Risks of Contracting a Computer Virus

A significant number of your friends and family members will fall prey to computer viruses as a result of their online behaviors. Antivirus software can only provide so much protection as new viruses are constantly introduced that current antivirus software definitions are not prepared to handle. Some of the symptoms suggesting that your computer may be infected include slow performance, mysterious messages appearing or complete inability to boot your computer. One common source of infection comes from downloading files from essentially unknown sources such as social networking profiles of people you don't really know, individually maintained websites or blogs, movie and music sites.

Some of the risks you, your friends and family members may encounter associated with contracting a virus are primarily social in nature and include:

- Embarrassment if others receive viruses originating from your files (e.g. from thumb drives or downloaded files)
- Disapproval if others become aware of the fact that you contracted a computer virus

So, each of us should "think before we click", and exercise good judgement before downloading files that could be infected.

Study 2

Negative Goal Frame Manipulation

Computer Viruses - Mozilla Firefox

File Edit View History Bookmarks Tools Help

file:///C:/Users/Cathy/Documents/spring 2009/security experiment/websites/neuprev2.htm

Official Site - Free Weight Loss Plan x Computer Viruses x

CONSEQUENCES OF CARELESS FILE DOWNLOAD BEHAVIOR

A significant number of computer users fall prey to computer viruses as a result of online behaviors. Antivirus software can only provide so much protection as new viruses are constantly introduced that current antivirus software definitions are not prepared to handle. Some of the symptoms suggesting that a computer may be infected include slow performance, mysterious messages appearing or complete inability to boot the computer. One common source of infection comes from downloading files from essentially unknown sources such as social networking profiles, individually maintained websites or blogs, movie and music sites.

By *not* exercising good judgment before downloading a file, the following consequences may result:

- Loss of the files stored on the computer (e.g. photos, music, games, homework or business files) if the computer become infected with a virus
- Having someone access information to send fraudulent emails to people in stored in address books or social networking friend lists
- The inconvenience of having to potentially invest time and money in restoring the computer to a usable state if it gets infected with a virus

So, to avoid these consequences, "*think before clicking*", and protect access to resources.

Study 2

Positive Goal Frame Manipulation

Computer Viruses - Mozilla Firefox

File Edit View History Bookmarks Tools Help

file:///C:/Users/Cathy/Documents/spring 2009/security experiment/websites/neupromo2.htm

Official Site - Free Weight Loss Plan Computer Viruses

 **BENEFITS OF CAREFUL FILE DOWNLOAD BEHAVIOR** 

A significant number of computer users fall prey to computer viruses as a result of online behaviors. Antivirus software can only provide so much protection as new viruses are constantly introduced that current antivirus software definitions are not prepared to handle. Some of the symptoms suggesting that a computer may be infected include slow performance, mysterious messages appearing or complete inability to boot the computer. One common source of infection comes from downloading files from essentially unknown sources such as social networking profiles, individually maintained websites or blogs, movie and music sites.



By exercising good judgment before downloading a file, the following benefits may result:

- Uninterrupted access to the files on the computer (e.g. photos, music, videos, games, homework, business files)
- The ability to keep in close contact with other people via email and social networking sites
- Reliable access to the Internet from the computers to download music, use maps, do research, shop, etc.



So, to enjoy these benefits, "*think before clicking*", and take action to sustain access to resources.

gadgets 4:44 PM

Study 2

Neutral/Control Condition



APPENDIX I – ESSAY 3, STUDY 1 MEASURES

Dependent Variables

Perceived Risk (7-point Likert scales anchored by Very Low and Very High) Source: Rhee et al. 2005

Self-Risk

- SELFRISK1 The risk from computer viruses to **my** computer is
- SELFRISK2 The likelihood that **my** computer will be disrupted due to a computer virus in the next 12 months is
- SELFRISK3 The chance that **my** computer will fall victim to a computer virus is
- SELFRISK4 The vulnerability of **my** computer to computer viruses is

Friend-Risk

For the following set of questions, “a friend” is someone with whom you have a degree of electronic interaction such as sending and receiving e-mail and/or file sharing activities.

- FRISK1 The risk from computer viruses to **a friend’s** computer is
- FRISK 2 The likelihood that **a friend’s** computer will be disrupted due to a computer virus in the next 12 months is
- FRISK3 The chance that **a friend’s** computer will fall victim to a computer virus is
- FRISK4 The vulnerability of **a friend’s** computer to computer viruses is

Other-Risk

For the following set of questions, “a typical undergraduate student” is someone attending a U.S. university other than this one with whom you have no direct interaction.

- OTHRISK1 The risk from computer viruses to **a typical undergraduate student’s** computer is
- OTHRISK2 The likelihood that a **typical undergraduate student’s** computer will be disrupted due to a computer virus in the next 12 months is
- OTHRISK3 The chance that **a typical undergraduate student’s** computer will fall victim to a computer virus is
- OTHRISK4 The vulnerability of **a typical undergraduate student’s** computer to computer viruses is

Security Behavioral Intentions – (7-point Likert scales agreement scales) Source: Taylor and Todd 1995)

- INT1 I plan to check the source when downloading files to a computer to avoid computer viruses
- INT2 I intend to exercise good judgment when downloading files to a computer to protect it from computer viruses
- INT3 I intend to be careful when downloading files to protect a computer from viruses

Manipulation Checks

Self-View (7-point Likert scale anchored by Not at all and A lot) Source: Aaker and Lee 2001

While you were reviewing the website about the risks of contracting a computer virus, please use the scale provided to describe the extent to which:

OTHTHO1 The website focused my thoughts on myself and my friends and family members

OTHTHO2 The website made me think about the impact of computer viruses on myself and my friends and family members

Risk Domain Frame (7-point semantic differential scales with the following anchors) Newly created

While you were reviewing the website about risks of contracting a computer virus, please use the scale provided to describe the extent to which:

Regarding contracting a computer virus, the website made me think primarily about:

FSRISK1 Financial Risks/Social Risks

Regarding contracting a computer virus, the website focused my thoughts on:

FSRISK2 Financial Consequences/Social Consequences

Similarity to friend and average other (7-point semantic differential scale anchored with Not at all Similar and Very Similar) Source: Menon et al. 2002

How similar do you think you are to your friends?

How similar do you think you are to the average other typical undergraduate student at another university?

APPENDIX J – ESSAY 3, STUDY 1 FACTOR ANALYSIS

Construct	Cronbach's alpha	Item	Factor					
			1	2	3	4	5	6
Perceived Risk to Self	.91	SELFRISK1	.85					
		SELFRISK 2	.91					
		SELFRISK 3	.87					
		SELFRISK 4	.89					
Perceived Risk to Friend	.85	FRISK1		-.77				
		FRISK2		-.80				
		FRISK3		-.77				
		FRISK4		-.81				
Perceived Risk to Other	.95	OTHRISK1			.85			
		OTHRISK2			.94			
		OTHRISK3			.92			
		OTHRISK4			.87			
Financial / Social Consequences	.90	FSRISK1				.96		
		FSRISK2				.94		
Thoughts about Others	.89	OTHTHO1					-.95	
		OTHTHO2					-.93	
Intentions	.84	INT1						.85
		INT2						.90
		INT3						.88

Extraction Method: Principal Component Analysis.

Rotation Method: Oblimin with Kaiser Normalization.

a Rotation converged in 7 iterations.

Loadings below .400 have been suppressed.

APPENDIX K – ESSAY 3, STUDY 2 MEASURES

Dependent Variables

Perceived Risk (7-point Likert scales anchored by Very Low and Very High)

Source: Rhee et al. 2005

Self-Risk

SELF RISK1 What is the likelihood that YOUR computer will be infected with a virus in the near future?

SELF RISK2 How likely are YOU to get infected with a computer virus in the next 12 months?

On a scale of 1-100, what is the probability that YOU will get infected with a computer virus in the next 12 months? _____ (1 – 100) *Source: Menon et al. 2002*

Friend-Risk

FRISK1 What is the likelihood that your BEST FRIEND'S computer will be infected with a virus in the near future?

FRISK2 How likely is it that your BEST FRIEND will get infected with a computer virus in the next 12 months?

On a scale of 1-100, what is the probability that your BEST FRIEND will get infected with a computer virus in the next 12 months? _____ (1-100) *Source: Menon et al. 2002*

Other-Risk

OTHRISK1 What is the likelihood that an AVERAGE UNDERGRADUATE STUDENT'S computer will be infected with a virus in the near future?

OTHRISK2 How likely is it that an AVERAGE UNDERGRADUATE STUDENT will get infected with a computer virus in the next 12 months?

On a scale of 1-100, what is the probability that an AVERAGE UNDERGRADUATE STUDENT will get infected with a computer virus in the next 12 months? _____ (1-100) *Source: Menon et al. 2002*

Security Behavioral Intentions – (7-point Likert scales agreement scales) Source: Taylor and Todd 1995)

INT1 From now on, how likely is it that you will check the source every time when downloading files to your computer to avoid getting infected with computer viruses?

INT2 How likely is it that you will be more vigilant in downloading files to your computer?

INT3 How likely is it that you will be more careful in your downloading activities to try and protect your computer from viruses?

Manipulation Checks

Goal Frame (7-point Likert scale anchored by Not at all and A lot) Source: Aaker and Lee JCR 2001

- CONS1 The website made me think about losing the files (e.g. photos, music, games, homework, etc.) I have stored on my computer
- CONS2 The website made me think about the inconvenience of being unable to use my computer for some period of time while recovering from a computer virus
- CONS3 The website made me think about having someone access my personal information and using it for fraudulent purposes
- BENS1 The website made me think about having reliable access to the Internet to download music, shop, do research, etc.
- BENS2 The website made me think about uninterrupted access to the files on my computer (e.g. photos, music, games, homework, etc.)
- BENS3 The website made me think about being able to use my computer to keep in touch with people through email and social networking sites

APPENDIX L – ESSAY 3, STUDY 2 FACTOR ANALYSIS

Construct	Cronbach's Alpha	Item	Factor					
			1	2	3	4	5	6
Perceived Risk to Self	.82	SELF RISK 1	.95					
		SELF RISK 2	.81					
Perceived Risk to Fried	.93	FRISK1		.91				
		FRISK2		.89				
Perceived Risk to Other	.79	OTHRISK1			.71			
		OTHRISK2			.77			
Thoughts about Benefits	.80	BENS1				.82		
		BENS2				.81		
		BENS3				.83		
Thoughts about Consequences	.75	CONS1					.81	
		CONS2					.77	
		CONS3					.78	
Intentions	.84	INT1						-.89
		INT2						-.86
		INT3						-.81

Extraction Method: Principal Component Analysis.

Rotation Method: Oblimin with Kaiser Normalization.

a Rotation converged in 15 iterations.

Loadings below .400 have been suppressed.

REFERENCES

- Aaker, J. L. and Lee, A. Y. 2001. "'I' Seek Pleasures and 'We' Avoid Pains: The role of self-regulatory goals in Information Processing and Persuasion," *Journal of Consumer Research* (28: 33), pp.33-49.
- Ajzen, I. 1991. "Theory of Planned Behavior," *Organizational Behavior and Human Decision Processes*, pp 179-211.
- Ajzen, I., M. Fishbein. 1980. *Understanding Attitudes and Predicting Social Behavior*, Englewood Cliffs, NJ: Prentice-Hall.
- Argyris, C. 1976. "Single-Loop and Double-Loop Models in Research on Decision Making," *Administrative Science Quarterly* (21:3), pp. 363-375.
- Ariely, D., G. Loewenstein. 2006. "The heat of the moment: The effect of sexual arousal on sexual decision making," *Journal of Behavioral Decision Making* (19), pp. 87-98.
- Armstrong, J. S., T. S. Overton. 1977. "Estimating non-response bias in mail surveys," *Journal Marketing Research* (14:3), pp. 396-402.
- Armstrong, C., and Sambamurthy, V. 1999. "Information Technology Assimilation in Firms: The Influence of Senior Leadership and IT Infrastructure," *Information Systems Research* (10), pp. 304-327.
- ARRA. 2009. "American Recovery and Reinvestment Act." Available online at <http://www.whitehouse.gov/recovery/about/>, accessed on August 18, 2009.
- Awad, N. F., M. S. and Krishnan. 2006. "The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to be Profiled Online for Personalization," *MIS Quarterly* (30:1), pp. 13-28.
- Baer, R. A., Smith, G. T., Hopkins, J., Krietemeyer, J. and Toney, L. 2006. "Using Self-Report Assessment Methods to Explore Facets of Mindfulness," *Assessment* (13:1), pp. 27-45.
- Baker, L. T. 2007. "The Relationship Between Mindfulness, Strategic Decision Process and Small Business Performance," Dissertation, University of Texas at San Antonio.
- Barrett, M. S., Novak, J. M., Venette, S. J., and Shumate, M. 2006. "Validating the High Reliability Organization Perception Scale," *Communication Research Reports* (23:2), pp. 111-118.
- Beckerman, J. Z., J. Pritts, E. Goplerud, J. C. Leifer, P. A. Borzi, S. Rosenbaum, D. R. Anderson. 2008. A delicate balance: Behavioral health, patient privacy, and the need to know. *California Healthcare Foundation: Issue Brief*.
- Bernstein, W. S., J. V. Murchinson, M. J. Dutton, T. D. Keville, R. D. Belfort. 2008. "Whose data is it anyway? Expanding consumer control over personal health information," *California Healthcare Foundation: Issue Brief*.
- Bertalanffy, Ludwig Von, 1968. *General System Theory*, New York; George Braziller.
- Bigley, G. A., and Roberts, K. H. 2001. "The Incident Command System: High-reliability organizing for complex and volatile task environments," *Academy of Management Journal* (44), pp. 1281-1299.
- Block, L. G. and Keller, P. A. 1995. "When to Accentuate the Negative: The effects of perceived efficacy and message framing on intentions to perform health-related behavior," *Journal of Marketing Research* (32:2), pp. 192-203.
- Borrus, A. 2005. Invasion of the Stock Hackers. *Business Week*. November 14, 2005.

- Brady, M.K., B. L. Bourdeau, J. Heskell. 2005. "The Importance of Brand Cues in Intangible Service Industries: An Application to Investment Services," *Journal of Services Marketing* (19:6), pp. 401-410.
- Brewer, M. B. and Gardner, W. 1996. "Who Is This 'We'? Levels of Collective Identity and Self Representations," *Journal of Personality and Social Psychology* (71), pp. 83-93.
- Butler, B.S., and Gray, P. H. 2006. "Reliability, Mindfulness, and Information Systems," *MIS Quarterly* (30:2), pp. 211-224.
- Byun, S., Ruffini, C, Mills, J. E., Douglas, A. C. Niang, M., Stepchenkova, S., Lee, S. K. Loutfi, J., Lee, J., Atallah, M., and Blanton, M. 2009. "Internet Addiction: Metasynthesis of 1996-2006 Quantitative Research," *CyberPsychology and Behavior* (12:2), pp. 203-207.
- Campbell, J., Greenauer, N., Macaluso, K. and End, C. 2007. "Unrealistic Optimism in Internet Events," *Computers in Human Behavior* (23), pp. 1273-1284.
- Campbell, K., Gordon, L. S., Loeb, M. P., and Zhou, L. 2003. "The Economic Cost of Publicly Announced Information Security Breaches: Empirical evidence from the stock market," *Journal of Computer Security* (11:3), pp. 431-448.
- Cha, H. S., Pingry, D. E., and Thatcher, M. S. 2008. "Managing the Knowledge Supply Chain: An Organizational Learning Model of Information Technology Offshore Outsourcing," *MIS Quarterly* (32:2), pp. 281-306.
- Champ, P. A., Moore, R., and Bishop, R. C. 2009. "A Comparison of Approaches to Mitigate Hypothetical Bias," *Agricultural and Resource Economics Review* (38:2), pp. 166-180.
- Chandran, S. and Menon, G. 2004. "When a Day Means More than a Year: Effects of Temporal Framing on Judgments of Health Risk," *Journal of Consumer Research* (31:2), pp. 375-389.
- Chiasson, M. W. & Davidson, E. 2005. "Taking Industry Seriously in Information Systems Research," *MIS Quarterly* (29), pp. 591-605.
- CISCO Systems. 2006. "Understanding Remote Worker Security: A Survey of User Awareness vs. Behavior." White paper accessed online at http://newsroom.cisco.com/dlls/2006/prod_100906.html?print=true on March 2, 2009.
- Clarke, L. 1999. *Mission Improbable: Using Fantasy Documents to Tame Disaster*. University of Chicago Press, Chicago.
- Clemmons, D. 2008. "Risk Factoring More in Decision-Making," *Internal Auditor* (65:1), pp. 13-14.
- Cohen, J. 1983. The Cost of Dichotomization," *Applied Psychological Measurement* (7), pp. 249-253.
- Cohen, P.R. 1995. *Experimental Methods for artificial intelligence*. Cambridge, Mass: The MIT Press.
- Cohen, J., Cohen, P., West, S. G., and Aiken, L. S. 2003. *Applied Multiple Regression/Correlation Analysis for the Behavioral Sciences* (3rd Edition). Mahwah, New Jersey: Erlbaum.
- Cooren, F. 2004. "The Communicative Achievement of Collective Minding: Analysis of Board Meeting Excerpts," *Management Communication Quarterly* (17:4), pp. 517-551.
- Cosmides, L, J. Tooby. 2000. Evolutionary psychology and the emotions. In M. Lewis and J. M. Haviland-Jones (Eds.), *Handbook of Emotions* (2nd Ed., 91-115). New York: Guilford Press.

- Culnan, M. 1993. "How Did They Get My Name? An Exploratory Investigation of Consumer Attitudes Toward Secondary Information Use." *MIS Quarterly* (17:3), pp. 341-364.
- Culnan, M., R. J. Bies. 2003. "Consumer Privacy: Balancing Economic and Justice Considerations." *Journal of Societal Issues* (59:2), pp. 323-342.
- Culnan, M., P. Armstrong. 1999. "Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation," *Organization Science* (10:1), pp. 104-115.
- Cyberspace Policy Review. 2009. Available online at http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf. Accessed on June 30, 2009.
- Cyert, R.M., J.G. March. 1963. *A Behavioral Theory of the Firm*. Prentice Hall, Englewood Cliffs, NJ.
- Damasio, A.R. 1994. *Descartes' error: Emotion, reason, and the human brain*. New York: Putnam.
- Das, A. 2003. "Knowledge and Productivity in Technical Support Work," *Management Science* (49), pp. 416-431.
- Davis, J.J. 1995. "The Effects of Message Framing on Response to Environmental Communications," *Journalism and Mass Communication Quarterly* (72), pp. 285-299.
- Day, J.C., Janus, A., and Davis, J. 2003. "Computer and Internet Use in the United States: October," U.S. Department of Commerce, Economics and Statistics Administration, U.S. Census Bureau, <http://purl.access.gpo.gov/GPO/LPS3637>.
- De Avila, J. 2009. "The Menace in the Machines - - Beware of Facebook 'Friends' Who May Trash Your Laptop," *The Wall Street Journal*, January 29, 2009.
- DeMaria, M. J. 2002. "Home Smart Home," *Network Computing* (13:1), pp. 55-60.
- Dennis, A. R. and Wixom, B. H. 2003. *Systems Analysis and Design* (2nd Edition), John Wiley & Sons, New York.
- Dimitropoulos, L. 2007. "Privacy and security solutions for interoperable health information exchange." Available online at <http://www.rti.org/page.cfm?objectid=09E8D494-C491-42FC-BA13EAD1217245C0>, Accessed on April 21, 2008.
- Dinev, T. and Hart, P. 2006. "An Extended Privacy Calculus Model for E-Commerce Transactions," *Information Systems Research* (17:1), pp. 61-80.
- Dong, S., Xu, S. X., and Zhu, K. X. 2009. "Information Technology in Supply Chains: The Value of It-Enabled Resources Under Competition," *Information Systems Research* (20:1), pp. 18-32.
- Druckman, J. N., and McDermott, R. 2008. "Emotion and the Framing of Risky Choice," *Political Behavior* (30:3), pp. 297-321.
- Edmondson, A.C., R.M. Bohmer, G.P. Pisano. 2001. "Disrupted Routines: Team Learning and New Technology Implementation in Hospitals," *Administrative Science Quarterly* (46), pp. 685-716.
- Edwards, J.R. 2001. "Multidimensional Constructs in Organizational Behavior Research: An Integrative Analytical Framework," *Organizational Research Methods* (4:2), pp. 144-192.
- Faraj, S. and Xiao, Y. 2006. "Coordination in Fast-Response Organizations," *Management Science* (52:8), pp. 1153-1169.
- Feldman, M.S., & Pentland, B.T. 2003. "Reconceptualizing Organizational Routines as a Source of Flexibility and Change," *Administrative Science Quarterly* (48), pp. 94-118.

- Fishbein, M., and Ajzen, I. 1975. *Belief, attitude, intention and behavior: An introduction to theory and research*. Reading, MA: Addison Wesley.
- Frazier, P. A., Tix, A. P., and Barron, K. E. 2004. "Testing Moderator and Mediator Effects in Counseling Psychology Research," *Journal of Counseling Psychology* (51:1), pp. 115-134.
- Gardner, W. L., Gabriel, S. and Lee, A. 1999. "'I' Value Freedom, but 'We' Value Relationships: Self-Construal Priming Mimics Cultural Differences in Judgment," *Psychological Science*, 10, pp. 321-326.
- Garg, A. 2003. "What Does an Information Security Breach Really Cost? Evidence and Implications," *Information Strategy: The Executive's Journal* (19), pp. 21-25.
- Economist (390:8614). 2009. "Here We Go Again," January 17, 2009, pp. 61-62.
- Gatignon, H., Tushman, M.L., Smith, W. & Anderson, P. 2002. "A Structural Approach to Assessing Innovation: Construct Development of Innovation Locus, Type and Characteristics," *Management Science* (48), pp. 1103-1122.
- Gavetti, G., Levinthal, D. A., and Rivkin, J. W. 2005. "Strategy Making in Novel and Complex Worlds: The Power of Analogy," *Strategic Management Journal* (26:8), pp. 691-712.
- Gefen, D. 2000. "Electronic Commerce: The Role of Familiarity and Trust," *Omega* (28:5), pp. 1-19.
- Gefen, D., Straub, D. W., and Boudreau, M. C. 2000. "Structural Equation Modeling Techniques and Regression: Guidelines for Research Practice," *Communications of the AIS* (7), pp. 1-78.
- Giddens, A. 1984. *The Constitution of Society*. University of California Press, Berkeley, CA.
- Gilbert, C.G. 2005. "Unbundling the Structure of Inertia: Resource Versus Routine Rigidity," *Academy of Management Journal* (48), pp. 741-763.
- Giordano, L. A., W. K. Bickel, G. Loewenstein, E. A. Jacobs, G. J. Badger, L. A. and Marsch. 2004. "Mild opioid deprivation and delay to consequences affect how opioid-dependent outpatients value an extra maintenance dose of buprenorphine." Pittsburgh, PA: Carnegie Mellon University, Department of Social and Decision Sciences.
- Glaser, J., D. E. Henley, G. Downing, K. M. 2008. "Brinner. and the Personalized Health Care Workgroup of the American Health Information Community. Advancing personalized health care through health information technology: An update from the american health information community's personalized health care workgroup," *Journal of the American Medical Informatics Association* (Preprinted accepted article) 1-21.
- Global Strategy Group. 2007. *West Virginia Statewide Survey*.
- Gold, R. A. and Martyn, K. 2003. "Event Valence and Unrealistic Optimism," *Psychological Reports* (92:3), pp. 1105-1110.
- Goldberg, A. 2005. "Simpler IT, Better IT," *eWeek* (22), pp. 33.
- Govekar, M. 2007. "Use full-life cycle Management to reduce SOA Downtime," Gartner G00144572.
- Grabe, M., B. H. Westley. 2003. "The controlled experiment." *In Mass Communication Research and Theory*, Guido H. Stempel, David H. Weaver and G. Cleveland Wilhoit, eds., Boston: Allyn and Bacon, 267-298.
- Green, S.G., Gavin, M.B., & Aiman-Smith, L. 1995. "Assessing a MultiDimensional Measure of Radical Technical Innovation," *IEEE Transactions on Engineering Management* (42), pp. 203-214.

- Greenhouse, S. W., S. Geisser. 1959. "Relation of Sample Size to the Stability of Component Patterns," *Psychometrika* (24), pp. 95-112.
- Guide to Management Ideas*. 2003. Pp. 73-74.
- Hair, J. F., Anderson, R. E., Tatham, R. L. and Black, W. C. 1998. *Multivariate Data Analysis* (5th Ed.) Englewood Cliffs, NJ: Prentice Hall.
- Hamilton, R. W. and Biehal, G. 2005. "Achieving Your Goals or Protecting Your Future? The Effects of Self-View on Goals and Choices," *Journal of Consumer Research* (35:2), pp. 277-283.
- Harless, D. W., C. F. Camerer. 1994. "The Predictive Utility of Generalized Expected Utility Theories," *Econometrica* (62), pp. 1251-1289.
- Harris-Ferrante, K. 2009. "The Shift to Packaged Solutions Among North American Life and P&C Insurers." Gartner G00166332.
- Harris Poll, March 26, 2007. Many U.S. adults are satisfied with use of their personal health information. Available online at http://www.harrisinteractive.com/harris_poll/index.asp?PID=743, Accessed on April 25, 2008.
- Heine, S. J. and Lehman, D. R. 1995. "Cultural Variation in Unrealistic Optimism: Does the West Feel More Invulnerable Than the East?" *Journal of Personality and Social Psychology* (68:4), pp. 595-607.
- Heine, S. J. and Lehman, D. R. 1997. "The Cultural Construction of Self-Enhancement: An Examination of Group-Serving Biases," *Journal of Personality and Social Psychology* (72:6), pp. 1268-1283.
- Hewlett, S. A. Sherbin, L. and Sumberg, K. 2009. "Let Gen Y Teach You Tech," *Business Week Online*. Available online at http://www.businessweek.com/managing/content/jun2009/ca20090630_327649.htm, accessed on August 18, 2009.
- HHS, 2007. Personalized healthcare: Opportunities, pathways and resources. United States Department of Health and Human Services. Available online at <http://www.hhs.gov/myhealthcare/news/presonalized-healthcare-9-2007.html>, Accessed on May 4, 2008.
- HHS. October 6, 2005. HHS awards contracts to advance nationwide interoperable health information technology. Available online at <http://www.hhs.gov/news/press/2005pres/20051006a.html>. Accessed online on April 21, 2008.
- Hitt, L. M. and Brynjolfsson, E. 1996. "Productivity, Business Profitability, and Consumer Surplus: Three Different Measures of Information Technology Value," *MIS Quarterly* (20:2), pp. 121-142.
- Hoffman, D.L., T. Novak. M. Peralta. 1999. "Building Consumer Trust Online," *Communications of the ACM* (42:4), pp. 80-85.
- Hoorens, V. and Buunk, B.P. 1993. "Social Comparison of Health Risks: Locus of Control, the Person-Positivity Bias and Unrealistic Optimism," *Journal of Applied Social Psychology* (23:4), pp. 291-302.
- Howard-Grenville, J. A. 2005. "The Persistence of Flexible Organizational Routines: The Role of Agency and Organizational Context," *Organization Science* (16), pp. 618-636.

- Huang, R. L., Lu, Z., Liu, J. J., You, Y. M., Pan, Z. Q., Wei, Z., He, Q. and Wang, Z. Z. 2009. "Features and Predictors of Problematic Internet Use in Chinese College Students," *Behaviour and Information Technology* (28:5), pp. 485-490.
- Iacobucci, D., Saldanha, N., and Deng, X. 2007. "A Meditation on Mediation: Evidence That Structural Equations Models Perform Better Than Regressions," *Journal of Consumer Psychology* (17:2), pp. 139-153.
- IBISWorld, 2009. "51421- IT Support, CRM and Data Processing Services in the U.S. – Industry Report."
- Igou, B. 2007. "User Survey Analysis: Software Support Services, North America," Gartner G00149409.
- Institute of Medicine. "To Err Is Human: Building a Safer Health System," *Institute of Medicine*, National Academy Press, 2000.
- Jaccard, J., Turrissi, R., & Wan, C.K. 1990. *Interaction Effects in Multiple Regression*, SAGE Publications, Inc., Newbury Park, CA.
- Jarvenpaa, S. L., N. Tractinsky, M. Vitale. 2000. "Consumer Trust in an Internet Store," *Information Technology Management* (1), pp. 45-71.
- Jarvenpaa, S. L., N. Tractinsky, L. Saarinen, M. Vitale. 1999. "Consumer Trust in an Internet Store: A Cross-Cultural Validation," *Journal of Computer-Mediated Communication* (5:2), pp. 44-71.
- Johns, G. 1998. "Aggregation or Aggravation? The Relative Merits of a Broad Withdrawal Construct," *Journal of Organizational Behavior* (19), pp. 453-462.
- Jones, S. and Fox. S. 2009. "Generations Online in 2009," *Pew Internet and American Life Project*, available online at <http://www.pewinternet.org/topics/Generations.aspx>, accessed on March 17, 2009.
- Kahn, B. E. and Luce, M. F. 2006. "Repeated-Adherence Protection Model: "I'm Ok, and It's a Hassle," *Journal of Public Policy and Marketing* (25:1), pp. 79-89.
- Kanawattanachai, P. and Yoo, Y. 2007. "The Impact of Knowledge Coordination on Virtual Team Performance Over Time," *MIS Quarterly* (31:4), pp. 783-808.
- Keller, P. A., and Block, L. G. 1996. "Increasing the Persuasiveness of Fear Appeals: The Effect of Arousal and Elaboration," *Journal of Consumer Research* (22), pp. 448-459.
- Klein, C. T. F. and Helweg-Larson, M. 2002. "Perceived Control and the Optimistic Bias: A Meta-Analytic Review," *Psychology and Health* (17:4), pp. 437-446.
- Keil, M. Mann, J., and Rai, A. 2000. "Why Software Projects Escalate: An Empirical Analysis and Test of Four Theoretical Models," *MIS Quarterly* (24:4), pp. 631-664.
- Kitayama, S., Matsumoto, H., Markus, H. R. and Norasakkunkit, V. 1997. "Individual and Collective Processes in the Construction of the Self: Self-Enhancement in the United States and Self-Criticism in Japan," *Journal of Personality and Social Psychology* (72:6), pp. 1245-1267.
- Knight, A.P. 2004. "Measuring Collective Mindfulness and Exploring its Nomological Network," unpublished Master of Arts Thesis, University of Maryland, College Park.
- Koch, C. 2004. "Project Management: AT&T Wireless self-destructs," CIO.com, Available online at http://www.cio.com/article/32228/Project_Management_AT_T_Wireless_Self_Destructs, Accessed on January 23, 2008.
- Koh, C., Ang, S., & Straub, D. 2004. "IT Outsourcing Success: A Psychological Contract Perspective," *Information Systems Research* (15), pp. 356-373.

- Kohlmeier, G. 2007 (forthcoming) "The Risky Business of Lifestyle Genetic Testing: Protecting Against Harmful Disclosure of Genetic Information." SSRN, UCLA.
- Kohn, L.T., Corrigan, J.M., & Donaldson, M.S. (eds). 1999. *To Err is Human: Building a Safer Health System*, National Academy Press, Washington, D.C.
- Koyalli, A. 2005. "Medical Diagnosis Can Induce Depressive Symptoms," *American Journal of Nursing* (105:11), pp. 72J-75J.
- Krebs, B. 2005. "Hacking Home PCs Fueling Rapid Growth in Online Fraud," *Washington Post*. Washington, DC.
- Krebs, B. 2009. "Obama: Cyber Security is a National Security Priority," *Washington Post*. Washington, DC. Available online at http://voices.washingtonpost.com/securityfix/2009/05/obama_cybersecurity_is_a_natio.html. Accessed on June 30, 2009.
- Krebs, B. August 17, 2009. "Three Alleged Hackers Indicted in Large Identity-Theft Case," *Washington Post*, A-Section, pg. A11.
- Kuhberger, A., Schulte-Mecklenbeck, M. and Perner, J.. 1999. "The Effects of Framing, Reflection, Probability, and Payoff on Risk Preference in Choice Tasks," *Organizational Behavior and Human Decision Processes* (78), pp. 204-231.
- Kuhn, M. H., and McPartland, T. S. 1954. "An Empirical Investigation of Self-Attitudes," *American Sociological Review*, 19, pp. 58-66.
- Kumar, N., Stern, L. W., and Anderson, J. C. 1993. "Conducting Interorganizational Research with Key Informants," *Academy of Management Journal* (36:6), pp. 1633-1651.
- Kunda, Z. 1990. "The Case for Motivated Reasoning," *Psychological Bulletin* (108), pp. 480-498.
- Kush, E.D., E. Helton, F. W. Rockhold, C. D. Hardison. 2008. "Electronic Health Records, Medical Research and the Tower of Babel," *New England Journal of Medicine* (358:16), pp. 1738-1741.
- Landis, J. R., Koch, G. G. (1977). "The Measurement of Observer Agreement for Categorical Data," *Biometrics* (33), pp. 159-174.
- Langer, E.J. 1989. *Mindfulness*. Perseus Publishing, Cambridge, MA.
- Langer, E.J., and Piper, A. I. 1987. "The Prevention of Mindlessness," *Journal of Personality and Social Psychology*, (53), pp. 280-287.
- Lee, A. Y., Aaker, J. L. and Gardner, W. L. 2000. "The Pleasures and Pains of Distinct Self-Construals: The Role of Interdependence in Regulatory Focus," *Journal of Personality and Social Psychology* (78:6), pp. 1122-1134.
- Lench, H. C., Quas, J. A., and Edelman, R. S. 2006. "My Child is Better Than Average: An Extension and Restriction of Unrealistic Optimism," *Journal of Applied Social Psychology* (36:12), pp. 2963-2979.
- Levin, I. P., Schneider, S. L. and Gaeth, G. J. 1998. "All Frames are not Created Equal: A Typology and Critical Analysis of Framing Effects," *Organizational Behavior and Human Decision Processes* 76(2), pp. 149-188.
- Levy, S. 2008. "Hazardous to Your Privacy," *Washingtonpost.com*, February 27, available online at <http://www.washingtonpost.com/wp-dyn/content/article/2008/02/26/AR2008022602993.html>, accessed on March 26, 2008.
- Levina, N., and Ross, J.W. 2003. "From the Vendor's Perspective: Exploring the Value Proposition in Information Technology Outsourcing," *MIS Quarterly* (27), pp. 331- 364.

- Levinthal, D., and Rerup, C. 2006. "Crossing an Apparent Chasm: Bridging Mindful and Less-Mindful Perspectives on Organizational Learning," *Organization Science* (17), pp. 502-513.
- Liedtke, M. February 22, 2008. "Google to test medical-record service." WashingtonPost.com, Available online at <http://www.washingtonpost.com/wp-dyn/content/article/2008/02/21/AR2008022100004.html?hpid=sec-health>. Accessed on April 14, 2008.
- Loch, K. D., Carr, H. H., and Warkentin, M. 1992. "Threats to Information Systems: Today's Reality, Yesterday's Understanding," *MIS Quarterly* (16:2), pp. 173-186.
- Loewenstein, G. 2005. "Hot-Cold Empathy Gaps and Medical Decision Making," *Health Psychology* (24:4), pp. S49-S56.
- Loewenstein, G., E. U. Weber, C. K. Hsee, N. Welch. 2001. "Risk as Feelings," *Psychological Bulletin* (127:2), pp. 267-286.
- Lohr, S. 2006. "Smart Care via a Mouse, but What Will It Cost?" *The New York Times Online*, August 20, 2006,
- Lohr, S. 2008. "Belt-Tightening, but No Collapse, Is Forecast in Technology Spending," *The New York Times*, Saturday Section C, p. 1.
- Lord, K. R. 1994. "Motivating Recycling Behavior: A Quasi-Experimental Investigation of Message and Source Strategies," *Psychology and Marketing* (11), pp. 341-358.
- Loroz, P. S. 2007. "The Interaction of Message Frames and Reference Points in Prosocial Persuasive Appeals," *Psychology and Marketing* (24:11), pp. 1001-1023.
- Lucas Jr., H. C. and Grover, V. 2008. "The Transformation Age: Surviving a Technology Revolution with Robert X. Cringely," *Communications of the AIS* (22), pp. 339-350.
- Lucas, Jr., H. C., Swanson, B., and Zmud, R. W. 2007. "Implementation, Innovation, and Related Themes Over the Years in Information Systems Research," *Journal of the Association for Information Systems* (8:4), pp. 206-210.
- Luftman, J. and Kempaiah, R. 2007. "An Update on Business-IT Alignment: "A Line" Has Been Drawn," *MIS Quarterly Executive* (6), pp. 165-177.
- Lyytinen, D. and Rose, G. M. 2003. "Disruptive Information System Innovation: The Case of Internet Computing," *Information Systems Journal* (13:4), pp. 301-331.
- Maheswaran, D. and Meyers-Levy, J. 1990. "The Influence of Message Framing and Issue Involvement," *Journal of Marketing Research* (27:3), pp. 361-367.
- Malhotra, N.K., Kim, S.S., and Agarwal, J. 2004. "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model," *Information Systems Research* (15:4), pp. 336-355.
- Mandel, N. 2003 "Shifting Selves and Decision Making: The effects of Self-construal priming on consumer risk-taking," *Journal of Consumer Research*, (30:1), pp. 30-40.
- Mandle, K. D., I. S. Kohane. 2008. "Tectonic Shifts in the Health Information Economy," *New England Journal of Medicine* (358:16), pp. 1732-1737.
- March, J.G., and Simon. H. A. 1958. *Organizations*. Wiley, New York.
- Markus, H. R., and Kitayama, S. 1991. "Culture and the Self: Implications for Cognition, Emotion, and Motivation," *Psychological Review* (98:2), pp. 224-253.
- Marsh, H. W. and Hau, K. T. 1999. "Confirmatory Factor Analysis: Strategies for Small Sample Sizes," *Statistical Strategies for Small Sample Research*. R. H. Hoyle. Thousand Oaks, CA, SAGE Publications.

- Mayer, R. C., J. H. Davis, F. D. Schoorman. 1995. "An Integrative Model of Organizational Trust," *Academy of Management Review* (20), pp. 709-734.
- McDermott, R., Fowler, J., and Smirnov, O. 2008. "On the Evolutionary Origin of Prospect Theory Preferences," *Journal of Politics*.
- McDonald, M. P. 2008. "Special Report: First Quarter 2008 Global IT Budget Update," Gartner G00160811.
- McKenna, F. P. 1993. "It Won't Happen to Me: Unrealistic optimism or illusion of control?" *British Journal of Psychology* (84:1), pp. 39-50.
- McKnight, D.H., V. Choudhury, V, C. Kacmar. 2002. "Developing and Validating Trust Measures for e-Commerce: An Integrative Topology," *Information Systems Research* (13:3), pp. 334-359.
- Medical News Today. 2009. "Senate Holds Hearing on Health Information Technology Funding in Economic Stimulus Bill." Accessed online at <http://www.medicalnewstoday.com/articles/136229.php>. Accessed on February 2, 2009.
- Meingast, M., Roosta, T., and Sastry, S. 2006. "Security and Privacy Issues with Health Care Information Technology," Proceedings of the 28th IEEE EMBS Annual International Conference, New York City.
- Melville, N., Kraemer, K., and Gurbaxani, V. 2004. "Information Technology and Organizational Performance: An Integrative Model of IT Business Value," *MIS Quarterly* (28:2), pp. 283-322.
- Menon, G., Block, L.G. and Ramanathan, S. 2002. "We're at as Much Risk as We Are Led to Believe: Effects of Message Cues on Judgments of Health Risk." *Journal of Consumer Research* (28:4), pp. 533-549.
- Miller, R.H., West, C., Brown, T.M., Sim, I., and Ganchoff, C. "The Value of Electronic Health Records in Solo or Small Group Practices," *Health Affairs* (24:5), 2005, pp. 1127-1137.
- Miner, J.B. 2002. *Organizational Behavior: Foundations, Theories and Analyses*, Oxford University Press, New York.
- Mishra, A. N., Konana, P., and Barua, A. 2007. "Antecedents and Consequences of Internet Use in Procurement: An Empirical Investigation of U.S. Manufacturing Firms," *Information Systems Research* (18:1), pp. 103-120.
- Mithas, S., Tafti, A., Bardhan, I. and Goh, J. M. 2009. "Information Technology and Firm Profitability: Mechanisms and Empirical Evidence," Working Paper.
- Moore, G. C. and Benbasat, I. 1991. "Development of an Instrument to Measure the Perceptions of Adopting an Information Technology Innovation," *Information Systems Research* (2:3), pp. 192-222.
- Morgan, S. E., J. K. Miller. 2002. "Communicating About the Gift of Life – Altruism and Organ Donation," *Journal of Applied Communications Research* (30:2), pp. 163-179.
- Mowry, M., D. Constantinou. 2007. "Electronic Health Records: A Magic Pill? Applied Clinical Trials," Accessed on Feb. 1, 2007. Available online at <http://www.actmagazine.com/appliedclinicaltrials/article/articleDetail.jsp?id=401622>
- Mu, E. 2007. "The Role of Scanning, Evaluation, and Mindfulness in the Assimilation of Information Technology: The Case of Enterprise Resource Planning (ERP) Systems," Unpublished PhD Dissertation, University of Pittsburgh. Pittsburgh, PA.
- Mu, E. and Butler, B. S. 2009. "The Assessment of Organizational Mindful Processes for the Effective Assimilation of IT Innovations," *Journal of Decision Systems* (18:1), pp. 1-30.

- Nakashima, E. 2008. Prescription data used to assess consumers. Washington Post, August 4, 2008. A Section, A01.
- New York Times*. March 26, 2008. "Safeguarding Private Medical Data," Section A, Editorial, Pg. 22.
- Nunnally, J. C., 1967. *Psychometric Theory*, McGraw Hill, New York.
- Nunnally, J. C., and Bernstein, I. H. 1994. *Psychometric Theory*, New York: McGraw-Hill.
- NSHS. 2007. "National Strategy for Homeland Security," Available online at http://www.dhs.gov/xlibrary/assets/nat_strat_homelandsecurity_2007.pdf, Accessed on May 25, 2008.
- NSSC. 2003. "National Strategy to Secure Cyberspace," Available online at <http://www.whitehouse.gov/pcipb/>, accessed on May 25, 2008.
- OCR. 2003. "Office for Civil Rights Guidance Explaining Significant Aspects of the Privacy Rule – Personal Representatives." Available online at <http://www.hhs.gov/ocr/hipaa/guidelines/personalrepresentatives.pdf>. Accessed on May 4, 2008.
- Paunonen, S. V., Rothstein, M. G., and Jackson, D. N. 1999. "Narrow Reasoning About the Use of Broad Measures for Personnel Selection," *Journal of Organizational Behavior* (20:3), pp. 389-40.7
- Pavlou, P. A., and El Sawy, O. A. 2006. "From IT Leveraging Competence to Competitive Advantage in Turbulent Environments: The Case of New Product Development," *Information Systems Research* (17), pp. 198-227
- Pavlou, P. A., D. Geffen. 2004. "Building Effective Online Marketplaces with Institution-Based Trust," *Information Systems Research* (15:1), pp. 37-59.
- Pear, R. 2009. "Privacy Issue Complicates Push to Link Medical Data," *New York Times*, January 18, 2009, Section A, 16.
- Pentland, B. T. and Feldman, M. S. 2005. "Organizational Routines as a Unit of Analysis," *Industrial and Corporate Change* (14:5), pp. 793-815.
- Perrow, C. 1984. *Normal Accidents: Living with High-Risk Technologies*. Basic Books, New York.
- Peter, J. P. and Tarpey, L. X., Sr. 1975. "A Comparative Analysis of Three Consumer Decision Strategies," *Journal of Consumer Research*, (2) pp. 29-37.
- Petronio, S. 2002. "Boundaries of Privacy: Dialectics of Disclosure," SUNY Press, Albany.
- Petty, R. E. and Cacioppo, J. T. 1983. "Central and Peripheral Routes to Persuasion: Application to Adversising," in *Advertising and Consumer Psychology*, Larry Percy and Arch Woodside, eds. Lexington, MA: Lexington Books, pp. 3-23.
- Petty, R. E. and Cacioppo, J. T. 1986. "The Elaboration Likelihood Model of Persuasion," in *Advances in Experimental Social Psychology*, Vol. 19, ed. Leonard Berkowitz, New York, NY: Academic Press, pp. 123-205.
- Petty, R. E. and Wegener, D. T. 1998. "Matching versus Mismatching Attitude Functions: Implications for Scrutiny of Persuasive Messages," *Personality and Social Psychology Bulletin* (24), pp. 227-240.
- Perloff, L. S. and Fetzer, B. K. 1986. "Self-Other Judgments and Perceived Vulnerability to Victimization," *Journal of Personality and Social Psychology* (50:3), pp. 502-510.
- Pew Internet Research and American Life Project. 2009. "Online Activities - 2000-2009." Available online at <http://www.pewinternet.org/Static-Pages/Trend-Data/Online-Activities-20002009.aspx>, accessed on August 18, 2009.

- Phelps, J., G. Nowak, E. Ferrell. 2000. "Privacy Concerns and Consumer Willingness to Provide Personal Information," *Journal of Public Policy and Marketing* (19:1), pp. 27-41.
- Pisello, T. and Quirk, B. January 5, 2004. "How to quantify downtime," *Network World*.
- Podsakoff, P. M., MacKenzie, S.B., Leong-Yeon, L., and Podsakoff, N.P. 2003. "Common Method Biases in Behavioral Research: A Critical Review of the Literature and Recommended Remedies," *Journal of Applied Psychology* (88), pp. 879-903.
- Potter, R.E., and Balthazard, P. 2004. "The Role of Individual Memory and Attention Processes During Electronic Brainstorming," *MIS Quarterly* (28:4), pp. 621-643.
- PR Newswire, 2008. "McAfee, Inc.: Localized Malware Takes Root; New McAfee Research Shows Regionalized Malware Rising; More Attacks Tailored to Different Cultures and Technologies." February 21, 2008.
- Pultz, J.E., Hafner, B., Orans, L., Neil, D., & Frey, N., 2002. "High Availability Networking Toward Zero Downtime," Gartner Group R-18-0344.
- Raghunathan, R., M. T. Pham, 1999. "All Negative Moods are Not Equal: Motivational Influences of Anxiety and Sadness on Decision Making," *Organization Behavior and Human Decision Processes* 79(1) 56-77.
- Ransbotham, S. and Mitra, S. 2009. "Choice and Chance: A Conceptual Model of Paths to Information Security Compromise," *Information Systems Research* (20:1), pp. 121-139.
- Read, D., G. Loewenstein. 1999. "Enduring Pain for Money: Decisions Based on the Perception of Memory of Pain," *Journal of Behavioral Decision Making* (12), pp. 1-17.
- Rencher, A.C. 2002. *Methods of multivariate analysis*. 2nd ed. John Wiley and Sons, Hoboken, 204-207.
- Reese, H.W. 1997. "Counterbalancing and Other Uses of Repeated-Measures Latin-Square Designs: Analyses and Interpretations," *Journal of Experimental Child Psychology* (64), pp. 137-158.
- Rettinger, D.A. and Hastie, R. 2001 "Content Effects on Decision Making," *Organizational Behavior and Human Decision Processes* (85), pp. 336-359
- Rhee, H., Rhu, Y., and Kim, C. 2005. "I Am Fine But You Are Not: Optimistic Bias and Illusion of Control on Information Security," International Conference on Information Systems, Las Vegas, NV.
- Rhodes, K. A. and Willemsen, J. 2004. "Technology Assessment: Cybersecurity for Critical Infrastructure Protection," *GAO Reports*. United States General Accounting Office. pp. 1-223.
- Rick, S. I., C. E. Cryder, and Loewenstein, G. 2008. "Tightwads and spendthrifts," *Journal of Consumer Research* (34:6), pp. 767-782.
- Rivers, A. T. 1999. "Challenges and Solutions for 24/7 System Availability," Proceedings of the 10th International Symposium on Software Reliability Engineering, p. 2.
- Roberts, P. 2004. "AOL Survey Finds Rampant Online Threats, Clueless Users," *ComputerWorld*.
- Rogelberg, S. G., and Stanton, J. M. 2007. "Introduction: Understanding and Dealing with Organizational Survey Nonresponse," *Organizational Research Methods* (10:2), pp. 195-209.
- Rosenthal, R., R. L. Rosnow. 1984. *Essentials of Behavioral Research: Methods and Data Analysis*. Boston: McGraw-Hill, 141-148.

- Russell, C. R. and Bobko, P. 1992. "Moderated Regression Analysis and Likert Scales: Too Coarse for Comfort," *Journal of Applied Psychology* (77:3), pp. 336-342.
- Russell, C. R., Pinto, J. K., and Bobko, P. 1991. "Appropriate Moderated Regression and Inappropriate Research Strategy: A Demonstration of Information Loss Due to Scale Coarseness," *Applied Psychological Measurement* (15), pp. 125-135.
- Russell Research 2006. *CA/NCSA Social Networking Study Report*.
- Sasse, M.A., Brostoff, S., and Weirich, D. 2001. "Transforming the 'Weakest Link' - A Human/Computer Interaction Approach to Usable and Effective Security," *BT Technology Journal* (19:3), pp. 122-131.
- Scharzer, R. 1994. "Optimism, Vulnerability, and Self-Beliefs as Health-Related Cognitions: A Systematic Overview," *Psychology and Health* (21), pp. 280-304.
- Schoemaker, P. J. H. 1982. "The Expected Utility Model: Its Variants, Purposes, Evidence and Limitations," *Journal of Economic Literature* (20:2), pp. 529-563.
- Seidler, J. 1974. "On Using Informants: A Technique for Collecting Quantitative Data and Controlling Measurement in Organization Analysis," *American Sociological Review* (39:6), pp. 816-831.
- Shea, M. and Yeh, C. J. 2008. "Asian American Students' Cultural Values, Stigma and Relational Self-Constraint: Correlates of Attitudes Toward Professional Help Seeking," *Journal of Mental Health Counseling* (30:2), pp. 157-122.
- Sheeran, P. 2002. "Intention-Behaviour Relations: A Conceptual and Empirical Review," In W. Stroebe & M. Hewstone (Eds.), *European Review of Social Psychology*, (Vol. 12, (pp. 1-36). London: Wiley.
- Shiv, B., Edell, J. A., and Payne, J. W. 1997. "Factors Affecting the Impact of Negatively and Positively Framed Ad Messages," *Journal of Consumer Research* (24:3), pp. 285-294.
- Shortliffe, E.H. 1999. "The Evolution of Electronic Medical Records," *Academic Medicine* (74:4), pp. 414-419.
- Smits, T. and Hoorens, V. 2005. "How Probable is Probably? It Depends on Whom You're Talking About," *Journal of Behavioral Decision Making* (18:2), pp. 83-96.
- Son, J., S. S. Kim. 2008. "Internet Users' Information Privacy-Protective Responses: A Taxonomy and a Nomological Model," *MIS Quarterly* (32:3), pp. 503-529.
- Sorensen, C., & Wang, T. February 12, 2008. "Blackberry Blackout Snarls Users: Concerns Raised Over Reliability of Email Service Following RIM's Second Outage In Less Than a Year," *The Toronto Star*, News Section: A04.
- Spacek, M. 2000. "Is Your IT Project Stuck in the Analysis/Paralysis Mode," *Strategic Finance* (81:7), pp. 24-28.
- Stanton, J. 2003. "Information Technology and Privacy: A Boundary Management Perspective," in *Socio-Technical and Human Cognition Elements of Information Systems*, Travers, J. Ed., Information Science Publishing, London.
- Stanton, J.M., Stam, K.R., Mastrangelo, P.M., and Jolton, J.A. 2005. "Analysis of End User Security Behaviors," *Computers & Security* (24), pp. 124-133.
- Swanson, E. 1994. "Information Systems Innovation Among Organizations," *Management Science* (40:9), pp. 1069-1092.
- Swanson, E.B., and Ramiller, N.C. 2004. "Innovating Mindfully With Information Technology," *MIS Quarterly* (28), pp. 553-583.

- Thatcher, A., and De La Cour, A. 2003. "Small Group Decision-Making in Face-to-Face and Computer-Mediated Environments: The Role of Personality," *Behaviour and Information Technology* (22:3), pp. 203-218.
- Trafimow, D., Triandis, H. and Goto, S. 1991. "Some Tests of the Distinction between the Private Self and the Collective Self," *Journal of Personality and Social Psychology* 60, pp. 649-655.
- Trumbo, C. W., K. A. McComas, and Kannaovakun, P. 2007. "Cancer Anxiety and Perception of Risk in Alarmed Communities," *Risk Analysis* (27:2), pp. 337- 350.
- Turner, D. (Ed), 2007. "Symantec Internet Security Threat Report (Volume XII)," White Paper.
- Tversky, A., and Kahneman, D. 1984. "Choice, Values and Frames," *American Psychologist* (39:4), pp. 341-350.
- Valorinta, M. 2009. "Information Technology and Mindfulness in Organizations," *Industrial and Corporate Change*, pp. 1-35.
- Van Boven, L., and Loewenstein, G. 2003. "Social Projection of Transient Visceral Feelings," *Personality and Social Psychology Bulletin* (29), pp. 1159-1168.
- Van Boven, L., G. Loewenstein, N. Welch, and Dunning, D. 2004. "The Illusion of Courage: Underestimating the Impact of Fear of Embarrassment on the Self." Pittsburgh, PA: Carnegie Mellon University, Department of Social and Decision Sciences.
- Vechio, D. May 7, 2001. "Legacy Software – Tolerate, Eliminate or Integrate?" Gartner Group ID Number SOFT-WW-PR-0028.
- Venkatesh, V., Morris, M.G., Davis, G.B., and Davis, F.D. 2003. "User Acceptance of Information Technology: Toward a Unified View," *MIS Quarterly* (27:3), pp. 425-278.
- Vogus, T. J. 2004. "In Search of Mechanisms: How do HR Practices Affect Organizational Performance?" Dissertation University of Michigan, 248 pages.
- Vogus, T. J. and Sutcliffe, K. M. 2007a. "The Impact of Safety Organizing, Trusted Leadership, and Care Pathways on Reported Medication Errors in Hospital Nursing Units," *Medical Care* (45:10), pp. 997-1002.
- Vogus, T. J. and Sutcliffe, K. M. 2007b. "The Safety Organizing Scale: Development and Validation of a Behavioral Measure of Safety Culture in Hospital Nursing Units," *Medical Care* (45:1), pp. 46-54.
- Vogus, T. J., & Welbourne, T. M. 2003. "Structuring for High-Reliability: HR Practices and Mindful Processes in Reliability-Seeking Organizations," *Journal of Organizational Behavior* (24), pp. 877-903.
- Vroom, V.H. 1964. *Work and Motivation*. Wiley, New York.
- Vroom, C. and R. Von Solms 2004. "Towards Information Security Behavioral Compliance," *Computers & Security* (23), pp. 191-198.
- Walker, T. 2008. "Report Calls for More EHR Privacy," *Managed Healthcare Executive* (18:3), p. 9.
- Wang, X. T. 1996. "Framing Effects: Dynamics and Task Domains," *Organizational Behavior and Human Decision Processes* (68) pp. 145–157.
- Ward, S., K. Bridges, B. Chitty. 2005. Do incentives matter? An examination of online privacy concerns and willingness to provide personal and financial information. *J. Marketing Comm.* 11(1) 21-40.

- Weaver, N., Paxson, V., Staniford, S. and Cunningham, R. 2003. "A Taxonomy of Computer Worms," Proceedings of the 2003 ACM Workshop on Rapid Malcode, ACM Press, New York, pp. 11-18.
- Webb, T. L., P. Sheeran. 2006. "Does Changing Behavioral Intentions Engender Behavior Change? A Meta-Analysis of the Experimental Evidence," *Psychological Bulletin* (132:2), pp. 249-268.
- Weber, E. U. and Hsee, C. K. 1998. "Cross-Cultural Differences in Risk Perception, but Cross-Cultural Similarities in Attitudes Towards Perceived Risk," *Management Science* (44), pp. 1205-1217.
- Weber, E. U., Hsee, C. K. and Sokolowska, J. 1998. "What Folklore Tells Us about Risk and Risk Taking: Cross-Cultural Comparisons of American, German, and Chinese Proverbs," *Organizational Behavior and Human Decision Processes* (75:2), pp. 170-186.
- Weber, E. U. and Hsee, C. K. 1999. "Models and Mosaics: Investigating Cross-Cultural Differences in Risk Perception and Risk Preference," *Psychonomic Bulletin and Review* (6), pp. 611-617.
- Weick, K.E., and Roberts, K.H. 1993. "Collective Mind in Organizations: Heedful Interrelating on Flight Decks," *Administrative Science Quarterly* (38), pp. 357-381.
- Weick, K.E., K.M. Sutcliffe. 2001. *Managing the Unexpected: Assuring High Performance in an Age of Complexity*. Jossey-Bass, San Francisco.
- Weick, K.E., K.M. Sutcliffe. 2006. "Mindfulness and the Quality of Organizational Attention," *Organization Science* (17), pp. 514-524.
- Weinstein, N.D. 1989. "Effects of Personal Experience on Self-Protective Behavior," *Psychological Bulletin* (105), pp. 31-50.
- West, R. 2008. "The Psychology of Security: Why Do Good Users Make Bad Decisions?," *Communications of the ACM* (51:4), pp. 34-40.
- Westerman, G. and Hunter, R. 2007. *IT Risk: Turning Business Threats into Competitive Advantage*. Harvard Business School Press: Boston, Massachusetts.
- Whiting, R. 2006. "Get Free of the Yearly Fee; IT managers seek options to escape high software maintenance costs," *InformationWeek* (45).
- Wing, J. 2008. "Five Deep Questions in Computing," *Communications of the ACM* (51), pp. 58-60.
- Wisniewski, P. K. and Lu, Y. 2009. "Operationalizing Technology Overload and Exploring Its Impact on Knowledge Worker Productivity," *Academy of Management Conference*. Chicago, Illinois.
- Wood, R. E. 1986. "Task Complexity: Definition of the Construct," *Organizational Behavior and Human Decision Processes* (37), pp. 60-82.
- Woods, D. D. 2006. "How to Design a Safety Organization: Test Case for Resilience Engineering," In Hollnagel, E., Woods, D.D., and Leveson, N. (Eds), *Resilience Engineering: Concepts and Precepts*. Burlington, VT: Ashgate.
- Ybarra, O. and Trafimow, D. 1998. "How Priming the Private Self or Collective Self Affect the Relative Weights of Attitudes and Subjective Norms," *Personality and Social Psychology Bulletin* (24) pp. 362-370
- Yoo, Y. and Kanawattanachai, P. 2001. "Developments of Transactive Memory Systems and Collective Mind in Virtual Teams," *International Journal of Organizational Analysis* (9:2), pp. 187-208.

- Zellmer-Bruhn, M.E. 2003. "Interruptive Events and Team Knowledge Acquisition," *Management Science* (49), pp. 514-528.
- Zhu, K., Kraemer, K. and Xu, S. 2006. "The Process of Innovation Assimilation by Firms in Different Countries: A Technology Diffusion Perspective on E-Business," *Management Science* (52:10), pp. 1557-1776.
- Zuboff, S. 1988. *In the Age of the Smart Machine: The Future of Work and Power*, Basic Books, New York.