2010

Essays on Information Assurance: Examination of Detrimental Consequences of Information Security, Privacy, and Extreme Event Concerns on Individual and Organizational Use of Systems

Insu Park
University of New York at Buffalo

Essays on Information Assurance: Examination of Detrimental Consequences of Information Security, Privacy, and Extreme Event Concerns on Individual and Organizational Use of Systems

By

Insu Park

April 30, 2010

A dissertation submitted to the Faculty of the Graduate School of the State University of New York at Buffalo
In Partial fulfillment of the requirements for the degree of

Doctor of Philosophy
Department of Management Science and Systems
School of Management

ProQuest LLC
789 East Eisenhower Parkway
P.O. Box 1346
Ann Arbor, MI 48106-1346

Acknowledgements

I wish to thank everyone for their help, recognizing that my research would have been much more difficult without you. And, for that, I am endlessly grateful to all those who have made this project what it is and enabled it to be completed. I would like to express my deepest gratitude and love to the two most precious people in my life, my wife, Jeewon Cho and my daughter, Sydney Sejin Park. Jeewon, my wife as well as the most important colleague, thanks for sharing every moment of this work with me. Sydney Sejin, my lovely daughter, very special thanks for your existence *per se*. You were my biggest motivator as I moved forward toward the destination of my journey. I love you more than I can do best. My advisors Professor, H. Raghav, Rao. Without your direction, support, and countless patience, I would have never finished. I am particularly thanks to have worked with Professor Raj Sharman for discussion and supports. I would also like to thank Professor Shambhu Upadhyaya for helpful comments and support.

Table of Contents

COPYRIGHT……..……..ii
ACKNOWLEDGEMENTS……..……iii
LIST OF FIGURES...……..……..…...vi
LIST OF TABLES...……..……..……vii
LIST OF APPENDICES.……...……..……vii
ABSTRACT viii
PROLOGUE.....ix

Essay1: Short Term and Total Life Impact Analysis of Email Worms in Computer Systems..... 1
1. Introduction 1
2. Background 3
3. Technique of Measuring Impact of Worms 5
   3.1 The Classification Process 7
   3.2 The Frameworks for Measuring the Impact of Worms 8
      3.2.1 The Dimensions of Total Life Impact (TLI) Framework 9
      3.2.2 The Dimensions of Short Term Impact (STI) Framework 12
4. Data Collection..... 16
5. Independence Test of the STI and TLI frameworks..... 18
6. Results of Comparing Frameworks..... 20
   6.1 Two-Dimensional Categorization..... 21
   6.2 Three-Dimensional categorization with damage potency..... 22
7. Validity and Reliability test..... 24
   7.1 Similarity Index 24
8. Discussion and Conclusion 30

Essay 2: The Effect of Spam and Privacy Concerns on Email Users' Behavior..... 33
1. Introduction 33
2. Background 35
   2.1. Spam and Privacy 35
   2.2. Defense Mechanisms 37
   2.3. User's Behaviors..... 39
3. Hypothesis..... 43
4. Methodology 46
   4.1. Data Collection and Research Method 46
   4.2. Constructs 47
      4.2.1. Spam Experience 47
      4.2.2. Perceived Privacy Concern on spam..... 47
      4.2.3. Usage-Oriented Behavior..... 48
      4.2.4. Protection-Oriented Behavior 48
5. Analysis and Results 49
   5.1. The Relationship between a Spam Experience and Privacy Concerns..... 49
   5.2. Effect of Privacy on Two Defense Behaviors..... 50

5.2.1. Effect of privacy concern on usage-oriented behavior 50
5.2.2. Effect of privacy concern on protection-oriented behavior 52
5.2.3. Effect of Privacy Concern and Dual Behavior 53
6. Discussion 56
6.1. Implications for Research 57
7. Conclusion 58

Essay3: Perceived Information Assurance, Risk, Resilience, and Information Systems Effectiveness in the Context of Disasters 60
1. Introduction 60
2. Background and Literature Review 63
2.1 Background of Disaster 63
2.2 Theoretical Background 64
2.3 Information Systems Effectiveness 65
2.4 Hospital Information Systems (HIS) Effectiveness 69
2.5 Resilience 71
2.6 Perceived Risk 73
2.7 Information Assurance 75
3. Hypothesis Development 76
3.1 The Effect of Perceived Risk 76
3.2 The Effect of Information Assurance 78
3.3 The Effect of Organizational Resilience 79
3.4 The Effect of Disasters 81
4. Methods 84
4.1 Research Context 84
4.2 Item Development and Pilot Test 85
4.3 Participants 86
4.4 Procedure 87
4.5 Measures 89
4.6 Common Method Bias and Organizational Scale for Organization Level 91
4.7 Data Analyses 93
5. Results 94
5.1 Stimulus Check 94
5.2 Measurement Model Estimation 95
5.3 Testing the Structural Model 98
5.3.1 Testing the Significance of Path Coefficients 98
5.3.2 Testing the Hypothesis of the Effect of Disaster 100
5.4 Post Hoc Analysis 102
6. Discussion 104
6.1 Theoretical Implications 106
6.2 Practical Implications 108
6.3 Implications for Practitioners 110
6.4 Limitations and Future Research 112
EPILOGUE 113
REFERENCE 115

LIST OF FIGURES

Essay1: Short Term and Total Life Impact Analysis of Email Worms in Computer Systems

Figure 1. The Classification Process……..…..8
Figure 2. The first month hit number of worms ……..…..……..…13
Figure 3. Two-Dimensional Frameworks for categorization……..…..…….……..…..22
Figure 4. Three-Dimensional Frameworks for Categorization…….……..…..…..…22
Figure 5. Weekly Trend of GSI…….……..…29

Essay 2: The Effect of Spam and Privacy Concerns on Email Users' Behavior

Figure 1. Conceptual Model for Hypothesis 1 to 3……..…….……..…….43
Figure 2. Conceptual Model for Hypothesis 3…….....……...…..45
Figure 3. Data Gathering for Dual Behavior……..…..…..……..…..54

Essay3: Perceived Information Assurance, Risk, Resilience, and Information Systems Effectiveness in the Context of Disasters

Figure 1. Information Systems Success Model……..…..……67
Figure 2. The Theoretical Model……..…..……80
Figure 3. The Effect of a Disaster……...….83
Figure 4. Disaster Recall Stimulus……..…….……..…..88
Figure 5. Results of Data Analysis: Pre and Post……..……..….98

LIST OF TABLES

Essay1: Short Term and Total Life Impact Analysis of Email Worms in Computer Systems

Table 1: Damage Potency Rating.……..……..……..….10
Table 2. The factors for the frameworks……..……..…..……..….16
Table 3. The different payloads between parent worm and a variant……..……..17
Table 4. Result of Chi-square test for STI framework…….……..18
Table 5. Result of Chi-square test for TLI framework……..……..…19
Table 6. Result of Chi-square test for DP and other dimensions…..……..…..…19
Table 7. Correlation matrix among the 4 dimensions……..……..20
Table 8. The number of email worms which have same factor in Cell 4 in Third week…..…….26
Table 9. Weekly GSI……..……..……..….26
Table 10. Clustering using a month of GSI……..…….29

Essay 2: The Effect of Spam and Privacy Concerns on Email Users' Behavior

Table 1. Correlation Matrix…….…….…….50
Table 2. Result of Logistic Regression……..……..……..……..50
Table 3. Testing mediator effects using Logistic Regression……..…..…..…….51
Table 4. Logistic Regression…….…….53
Table 5. Testing mediator effects using Logistic Regression…….…..…..…….55

Essay3: Perceived Information Assurance, Risk, Resilience, and Information Systems Effectiveness in the Context of Disasters

Table 1. Descriptive Statistics (N = 104)…….…….……...…..86
Table 2. Construct Characteristics and K-S Test Results by Subgroup…….……...….93
Table 3. The Result of *T*-Test (N = 104)…..…….…….94
Table 4. Inter-Construct Correlations by Groups.……..…….……..……94
Table 5. PLS Component-Based Analysis: Cross-Loadings …….……95
Table 6. Difference Between Before And After the Disaster …….…….…….…96
Table 7. Difference between main and support users for before disaster…….……..102
Table 8. Difference between main and support users for after disaster……..……102
Table 9. Summary of Hypothesis Testing Results …….……103

LIST OF APPENDICES

Essay3: Perceived Information Assurance, Risk, Resilience, and Information Systems Effectiveness in the Context of Disasters

APPENDIX: SURVEY INSTRUMENT.....124

Abstract

The purpose of this study is to explore systems users' behavior on IS under the various circumstances (e.g., email usage and malware threats, online communication at the individual level, and IS usage in organizations). Specifically, the first essay develops a method for analyzing and predicting the impact category of malicious code, particularly email worms. The current study creates two frameworks classifying email worms based on their detrimental impact. The first is the Total Life Impact (TLI) framework, a classifier to categorize worms in terms of their impact. The other is the Short Term Impact (STI) framework which allows for prediction of the impact of the worm utilizing the data available during the early stages in the life of a worm. Given the classification, this study identifies how well the STI framework allows for prediction of the worm into its final impact category.

The second essay aims to examine the effects of both spam and the resulting lack of privacy on users' behavior with respect to e-mail usage. This study reveals that spam e-mail triggers users' privacy concerns and, in turn, such concerns influence the way that the users cope with spam or junk mails. Upon receiving spam e-mail, the users predominantly exhibit two different behavioral patterns: usage-oriented (passive) and protection-oriented (proactive) behavior.

The third essay examines the impact of perceived information assurance, risk, and resilience on IS effectiveness in the context of extreme events. Resilience in organizations is the positive capacity to cope with negative extreme events. Also, this is critical to ensuring business continuity. While the subject of resilience has been investigated from an engineering perspective, from an IS context, it remains an understudied area. The present study develops a model that is tested with data collected from three of the hospitals in Western New York that were affected by a major snowstorm (labeled a federal disaster).

Prologue

Consistent with development of information systems and technology, security and privacy issues have been widely considered to be explained for effective and secure usage of information systems (IS) and technology (IT) in the various circumstances. The endless war between privacy threats and security in the IS/IT areas has had systems users recognize system vulnerability for individual and organizational purposes in using IS/IT. The users' such perception on privacy may affect their usage performance in individual or organizational contexts.

In this situation, an important overarching issue arises: Whether does information assurance have various impacts on individual behaviors and organizational performance under various IS/IT contexts? This in turn leads to the questions of what roles information security and privacy acts in the relationship between IS and systems users and how the users psychologically deal with the factors affecting their systems usage behaviors. In order to answer the questions, this dissertation, consisting of three essays, focuses on a technical/psychological way to investigate malware and end-user behavior in the context of individual and organizations. These essays shed light on our understanding on human behaviors and their underlying psychological mechanisms in various circumstances focusing on information assurance.

This study is overall to explore systems users' behavior on information systems and explain phenomenon occurring under the various circumstances, such as email usage and malware threats, online communication in individual level, and IS usage in organizations, related to security and privacy issues both technically and psychologically.

This study attempts first to find the effect of email worms on systems and develop a frame to classify email worms based on detrimental impacts of different types of worms. This

study develops two frameworks and compares these two frameworks to categorize those worms. This study show that the there would be categorized with different method from antivirus companies suggests. Second study examines the effects of spam on users' protecting behaviors and how privacy concerns affect users' behavior with respect to email usage. This study explains how users' protecting behaviors come out. This essay explains email users' protecting behaviors are triggered by spam experience but privacy concerns mediate the effect of spam experience on users' behaviors. Therefore, readers can identify that their protecting behaviors arise from not just spam experience but also their privacy concerns.

Third study investigates mediating effect of information security for perceived risk along with organizational resilience in organizations' information systems under the disaster context and its consequence on the usage of the information systems. Used information systems success theory as theoretical framework, this study finds the relationship between critical factors and information systems on integrated model explaining the organizational systems effectiveness. This third study deals with important issues which have been regarded as critical elements in IS research. Theoretically, this study uses psychological process that risk perception affects information system via information assurance and organizational resilience. Methodologically, in order to find the impact of extreme events, this study used multigroup analysis by comparing two contexts: pre- and post-event under the quasi-field experiment design with survey questions. The integrated goal of all there essays is to enhance our understanding about human behavior and psychological mechanisms brought from under different circumstances in terms of information assurance.

Essay1: Short Term and Total Life Impact Analysis of Email Worms in Computer Systems

1. Introduction

Worms, avatars of malicious code, are self-replicating programs that have often almost succeeded in bringing down the whole Internet system.[1] Worms such as SoBig.f and MyDoom, have caused tremendous loss of productivity, time and sales resulting in costs upwards of $1 billion and $250 million, respectively as a result of the tremendous loss of productivity, time and sales (Salkever, 2003; Stein, January 30, 2004). Beyond the major damages stated above, email worms also have influences on intangible assets of companies, such as their prestige and customer loyalty.

The economic damage driven by Internet worms is part of recorded history, once the effective life of the worm is over and the worm has run its course (Sharman, Krishna, Rao, & Upadhyaya, 2006). However, if the effect of the worm could be predicted during the early stages of its life, a more effective and rapid response can be developed. Predicting the impact of the worm in its early stages is beneficial for economic reasons. For example, insurance companies that specialize in cyber policies are interested in knowing the impact of a worm in order to process claims and to determine the payout time based on the expected impact. Payouts on insurance claims for damages are usually made when the extent of the damage has been fully assessed. Further being able to predict the impact of the worm based on early data can become a guiding yardstick in the planning of and monitoring of the application of patches.

[1] http://home.esn.net/support/glossarya.html#I

Although email has become an indispensable communication medium in our life, worms can be almost impossible to eliminate until long after the targets are removed from the internet (Nazario, Anderson, Wash, & Connelly, 2001). For this reason, email worms are increasingly attacking systems with intensity and using more advanced social engineering tricks (C. C. Zou, Oct. 2004). System managers and security officers can decide whether immediate disruption of the business is justifiable based on the potency of the worm in terms of its risk or detrimental impact, such as loss of productivity, lost data, denial of systems, systems crashes and so on. A low impact and low risk worm can perhaps be handled on a bi-weekly or weekly basis as a part of the regular maintenance routine. According to ICSA Labs (ICSA, 2004), 92% of all worms enter the enterprise via email so studying impact of e-mail worms is important. Thus, it is crucial to categorize email worms based on their impact. By doing so, companies would be able to take relevant actions with the predicted information on the potential damages of worms.

There are two main contributions of this paper. First, the current paper develops a descriptive model to categorize email worms based on their impact by using two frameworks, the Total Life Impact (TLI) and Short Term Impact (STI). The Total Life Impact (TLI) Framework is a descriptive model or classifier to categorize worms in terms of their impact, after the worm has run its course. Therefore in a sense the TLI provides a standard reflecting ground truth. The second framework, the Short Term Impact (STI) framework, allows for prediction of the impact of the worm utilizing the data available during the early stages in the life of a worm. These two frameworks help us classify and compare the life of each worm, as well as allow us to determine whether early hit number of worms can represent the total life of their hit and the accuracy of the representation.

Second, the present study develops factors, such as total hit number and hit density to

characterize the impact of e-mail worms. The paper also develops an adaptation of the concept of group similarity index (GSI) to provide insights into the issue of categorization of email worms.

We believe that the frameworks established in this paper can be utilized to enable insurers to make insurance payoffs as well as IT managers to cope with worm damage as early as possible. This is clearly an important need - to provide a way to do early triage of malware that will assist organizations in allocating resources for response.

In exploring these issues, this paper furthers the understanding of the impact of email worms. This paper is structured as follows. In Section 2, we provide a general introduction and background information about worms. The methods of measuring impacts of worms are developed in Section 3. Included in the section are the definitions for factors and descriptions of terms related to the two frameworks, and a detailed technical discussion of these frameworks. Section 4 is devoted to data collection. Independence tests for each factor are presented in Section 5. Section 6 provides a comparison with two frameworks first using two dimensions and then using three dimensions. Validity and reliability tests with group similarity index (GSI) are presented in Section 7 along with the results. Finally in Section 8, forms the conclusion where we discuss the implications of this research on practice as well as limitations of the work.

2. Background

A question often asked is: how vulnerable are the processes, data and systems? To answer such questions we need to have a yardstick for measurement. The presumption here is that “if something can’t be measured, it can’t be managed” (Craft, 2000). While some researchers have started to focus on metrics for vulnerability assessment, there is a lacunae of research for evaluating, classifying, or categorizing damage by worms (Nazario, et al., 2001).

In order to provide a more complete background we provide a brief introduction to worms. The worm is characterized by its activity and independence (Qing & Wen, 2005; Zalewski, 2003) as compared to a virus, which adds itself to other programs, including operating systems. A worm is defined as a piece of malicious code that propagates over a network without human assistance. It can initiate attack independently with the need for the execution of specific programs (D.M. Kienzle & M.C. Elder, 2003) based on malicious code, network propagation, human intervention, and standalone or file-infecting. Worms are grouped into three categories according to their propagation strategies (Qing & Wen, 2005): windows file-sharing worms, traditional worms and e-mail worms. Windows file sharing worms place a copy of themselves in a shared folder under a harmless name[2] and subsequently take on a more malicious role (Darrell M. Kienzle & Matthew C. Elder, 2003). Such worms take advantage of operating systems including Microsoft Windows peer-to-peer service. Traditional worms "attack across the Internet using direct connections over TCP/IP-based protocols, exploit vulnerabilities in operating systems and applications, typically do not require user intervention, and use other propagation vectors besides e-mail and Windows file sharing" (Darrell M. Kienzle & Matthew C. Elder, 2003).

In contrast to these two worms, email worms are malicious codes that propagate through email. According to Zou et al (C. C. Zou, Oct. 2004) a worm can compromise a user's computer and then find all email addresses stored on the computer to send out worm email, when an email user opens a worm program in the attachments of a worm email. Email worms are currently the most common malware type in the world (Hypponen, 2004).

---

[2] http://virusall.com/worms.shtml

Weaver and Paxon (Weaver & Paxson, 2004) have attempted to assess the damage caused by worms to provide a handle on the spending for defense against worms. They combine their estimate of the worst-case worm with a linear damage model, based on lost productivity, repair time, lost data, and damage to systems.

Typically, anti virus companies use three broad attributes to categorize Malware[3]: wild (or wildness), damage (destructiveness), and distribution (or pervasiveness) (e.g. CA, Zonelabs, Symantec). According to Symantec.com[4], category "wild" refers to the extent to which a virus has already spread among computer users. Category "damage" means the amount of damage that a given infection could inflict. "Distribution" is concerned with the matter of how quickly a program spreads itself. Symantec's method divides malware into five severity threat categories from "very low" to "very severe." This categorization is based on the current assessment of a malicious code's severity where severity of malware changes as time goes on. Severity can be changed by filtering, cleaning (Zou, Gong, & Towsley, 2002). However, the different attributes are considered independently and are not grounded statistically. The next section identifies a new metric for classifying worms to determine the impact category of the worm during the course of its life, based on its behavior in its early stage. Our results suggest that this new measurement would serve to classify worms distinctly into several groups.

3. Technique of Measuring Impact of Worms

Sobig, deemed in 2003 as one of the worst e-mail worms ever, sent over 300 million

---

[3] "Malware" is short for malicious software and is typically used as a catch-all term to refer to any software designed to cause damage to a single computer, server, or computer network, whether it's a virus, spyware, et al (http://www.microsoft.com/technet/security/alerts/info/malware.mspx).
[4] http://www.symantec.com/enterprise/security_response/glossary.jsp

infected e-mail messages around the world[5] resulting in unexpected detrimental impact worldwide. As it began spreading through internet, email delivery was delayed by several days, in some cases by weeks. Companies today rely on email to deliver business critical information and the financial implications are serious. This episode served as a warning shot, signaling the importance of e-mail as a communications channel and the vulnerability of our IT-dependant infrastructure.

'SoBig.f' and 'MyDoom' had peak infection dates in the first month after their release. According to Messagelabs, the proportion of the first month infection to total infection for both worms was up to 87.6% and 89.25% respectively. In other words, 'SoBig.f' and 'MyDoom' worms had an early peak infection date and most infections occurred at the beginning stage of their life. W 32 / Yaha.P @mm peaked in terms of the number of hits after about 25 days after release (See Figure 2). From these cases, it is clear that it is important to consider the rapidity of spread for the first month as a crucial factor for evaluating the impact of worms on organizations.

Clearly, the rapidity of spread and the amount of infections increase the probability of an organization being attacked by worms. A worm's damage potency may also have a crucial impact on an organization. Hence detrimental impact should not only include the damage potency of worms but also rapidity of spread and the amounts of infections.

We base the framework development on three fundamental assumptions. The first assumption is that given two active worms with the same type of payload, the worm which has more numbers of hits in the same period has a greater detrimental impact. Second, we assume

---

[5] F-Secure Corporation's Data Security Summary for 2003, The year of the worm, URL: **http://www.f-secure.com/2003/**

that when the time for peak number of hits of a particular worm is earlier than for other worms, that worm has more severe detrimental impact. This second assumption is completely consistent with the first assumption. The reasoning here is that because there is a time lag for organizations to get defenses into place, the early strikers are likely to create more harm than late strikers. (Note this assumption does not always hold, but this is a general statement based on anecdotal information with Symantec executives and has been seen to often hold true). Further, although some worms contain code to stop propagating after a certain date, we focus on worms with one year of more life. Our framework also assumes that a worm can be active for a period greater than a month. Incidentally the data on the 93 worms that we have used in this analysis have activity periods that span more than a month. It is important to point out that the STI framework (to be introduced in Sec. 3.1) is able to provide guidance based on a week's worth of data. It can also be used with three to four days of data with a lower accuracy level.

3.1 The Classification Process

In this subsection we outline the classification process which consists of 4 steps as shown in Figure 1. In the first step, we developed two frameworks: one framework which serves to predict the impact of the using early data and the second framework (considered ground truth) which uses all of the data after the worm has run its course (we consider this to be a year and a half). Each framework has 3 dimensions.

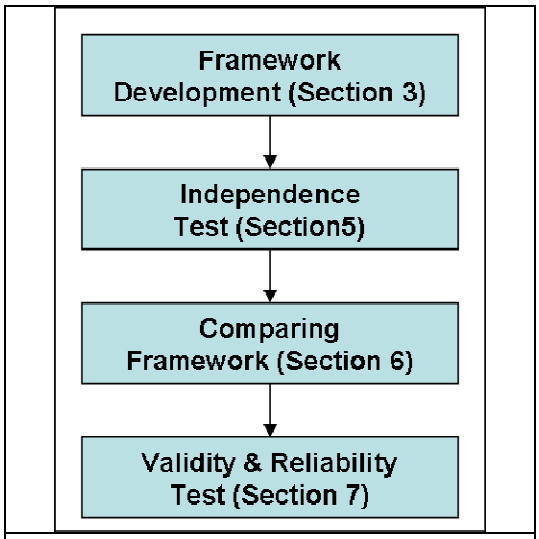


Figure 1. The Classification Process

In the second step, chi-square and correlation analysis are conducted to check independence between dimensions of each framework, and relationship between two frameworks. In third step, we try to find the "goodness" of match, for exploring how the framework can be used to predict the real severity, by comparing two frameworks. In step four we check validity and reliability of the frameworks using the group similarity index (GSI)

3.2 The Frameworks for Measuring the Impact of Worms

In this sub-section, we describe the development of two new frameworks, namely, the Total Life Impact (TLI) and Short Term Impact (STI) frameworks as a first step.

The TLI framework provides a comparison standard as it relates to data after the worm has run its course. The STI framework provides a classification based on data available during the early stages in the life of a worm.

3.2.1 The Dimensions of Total Life Impact (TLI) Framework

Framework TLI uses three dimensions for classification: Total Hit Number (LTH) - the logarithm of the cumulative number of hits over the entire lifespan, Hit density (HT_v), and Damage Potency (DP). We now describe each of these dimensions.

- **Total hit number (LTH)**

In this study, 'total hit number' is defined as the total number of hits, or total number of machines infected by the worm, (as determined Messagelabs and Symantec) for the life of the worm. Hit number is captured by the frequency of emails which contained worms, stopped after the outbreak, by Message Labs6 (www.messagelabs.com). For the purposes of this study, we utilize the log of total hit number (LTH) as one of the dimensions.

- **Hit density (** HT **)**

To measure hit density for the first month, we adapt the concept of 'Hit Density' from (Kim, Sivasailam, & Rao, 2004, 2005) and 'Density Index' (Kim, Song, Baynov, & Rao, 2005). For our purpose we define, Hit density refers to the ratio of the hit number of a worm for the first month to the total hit number during its lifespan. This indicates the extent to which first month hits have an impact on the total impact in terms of the total hit number during worms' lifespan. For example, the hit density of 'JS/Flea.A' worm, which accumulated 2340 hits in the first month out of 3213 (total hits), is 0.72. This value suggests the relative ratio of occurrence of the total hits. (Refer to Figure 2 which shows a plot of hit number versus time in days for the 'JS/Flea.A' and 'w32/Yaha.P@mm' worms). Although most worms show a distinct lifespan that

[6] Message labs had installed servers on the internet to collect the data we are using.

is different from the first month, they fall into the following characteristics with regard to Hit Density:

- The typical range is $0 < HT \leq 1$

- **Damage potency (DP)**

Damage potency (DP) measures the intrinsic attributes of a worm to cause detrimental impact. Damage potency captures the impact of payload and the rapidity of spread. It is also known as "Virulence" which means the degree of spread rapidity of worms that affect resources such as network bandwidth, router CPU/memory, or email server availability (Todd, 2003). The damage potency reflects the magnitude of the damage, which can potentially occur, resulting from an infection. A worm's damage potency may be rated high, medium, or low based on its inherent capacity to cause both direct and indirect damage to systems or networks. Certain worms are designed specifically to delete or corrupt files, causing direct damage. Trendmicro.com[7], classifies damage potency into three categories as worm in Table 1.

Table 1: Damage Potency Rating

LEVEL	CONTENTS	EXAMPLES
High (Unforeseeable & Very Serious Damage)*	・System becomes unusable ・System data or files are unrecoverable ・System cannot be automatically recovered using tools ・Recovery requires restoring from backup ・Causes large amounts of network traffic ・Data/files are compromised and sent to a third party	Flash bios, format HDD Encryption of data Packet flooders, mass-mailers Backdoor capabilities (Silent manipulation of data, Re distribution of confidential data to third parties.)**

[7] http://www.trendmicro.com/en/security/general/glossary/overview.htm#Damage potential

Medium (Serious & Medium Damage)	・System/files can be recovered using Trend Micro products or cleaning tools ・Minor data/file modification ・Malware that write minimal amount of data to the disk ・Malware that kill applications in memory ・Causes medium amount of network traffic ・Automatically executes unknown programs ・Deletes security-related applications	File infectors Slow mailers Antivirus, firewall (Deletion of single files, machine temporarily not available. & Deletion of many files, formatting of hard drives, deletion of Flash BIOS, . . .)
Low (Little Damage)	・No system changes ・Deletion of less significant files in the system ・Changes can be recovered by users without using any tools ・Damage can be reversed just by restarting the system	File deletion (Output of text or sound.)
*Damage from McAfee.com; ** examples from McAfee.com		

Damage potency may result from the payload carried by attack vectors (Lininger & Vines, 2005) i.e. a path or means that a hacker can use to gain access to a computer or network server to deliver a payload or malicious codes[8]. The damages due to the payload are classified in to five types[9] by McAfee (a major anti-virus vendor). The first type referred to as, *Unforeseeable Damage* has the most harmful impact on the systems. This type includes activities like redistributing confidential data to third parties or destroying an entire network. The second type known as *Very Serious Damage* includes activities, such as manipulating data silently. *Serious Damage* is the third type. Its payload includes activities such as deleting files, formatting hard drives, and deleting Flash BIOS. The fourth type is *Medium Damage.* Deleting individual files and rendering the computer temporarily unavailable are the main activities for the type Medium Damage. Finally, the fifth type of payload, *Little Damage* includes activities such as generating bogus text or sounds and is the least virulent.

[8] http://searchsecurity.techtarget.com/sDefinition/0,290660,sid14_gci1005812,00.html
[9] Source: http://us.mcafee.com/VirusInfo/VIL/risk_assessment.asp

It is important to note that damage potency reflects the ability to cause damage and not the actual damages. This is because the actual damage can differ from firm to firm based on quality and speed of response in patch and or anti-virus deployment. In order to measure the magnitude of worms' damage potency, we use the scale from McAfee and Computer Associates[10]. For the purposes of this analysis, the scale was converted to a scale where "high" ranged from 3 to 5 point and "low" ranged from 0 to 2 points in the scale.

3.2.2 The Dimensions of Short Term Impact (STI) Framework

STI framework is a classification based on the data available during the early stages in the life of a worm. STI framework also has three dimensions: the first dimension captures how early the worm has peaked and is a variant of the concept of skewness; the second dimension is the logarithmic measure of the number of hits in the time period from the release date up to the measurement day (three days, 1st week, 2nd week, 3rd week, and 1st month); and the third dimension is Damage Potency (DP). Both the TLI and STI frameworks use this dimension.

The STI framework can be used at any time for example a few days after the release of the worm, a week later, etc. However, for illustrative purposes in this section we describe the STI framework using the first month of data, with no loss of generality. The remainder of this section is devoted to describing the dimensions of this third framework.

ICSA Labs[11] reported that the rapidity of spread is the primary cause for managerial costs driven by worms (ICSA, 2003). To minimize damage arising from rapid spread, organizations often deploy defensive measures within a few hours of the release of worms. Worms vary

---

[10] Source: http://www3.ca.com/securityadvisor/newsinfo/collateral.aspx?cid=59094
[11] http://www.icsalabs.com/icsa/icsahome.php

considerably in terms of their diffusion rate. For example, macro worms, such as Melissa, take at least a few days to diffuse, whereas Code Red took about 12 hours to diffuse. These examples indicate that it is crucial to focus on analyzing information about worms within the early days after worm outbreaks.

- **Tskewness (TSKI)**

We adapt the term, 'Tskewness', from statistics as a way to identify the impact of a worm regarding time. Statistically, skewness refers to the degree of asymmetry of a distribution, or more precisely, the lack of symmetry. A distribution is symmetric when it is placed the same to the left or right of the center point (Milton & Arnold, 1986). The skewness for a normal distribution is zero and all symmetric data should have near zero values for their skewness. Negative values for the skewness imply that data is skewed left, whereas positive values for the skewness indicate that data is skewed to the right. In this paper, we define skewness with a slightly different meaning. Tskewness (*TSKI*) refers to the degree of inclination toward earlier time periods.

Figure 2 shows the number of hits during the first 28 days after the release of the two worms. The data shows that some worms peak earlier while others peak a later. This affects the TSkewness based on when it is measured.

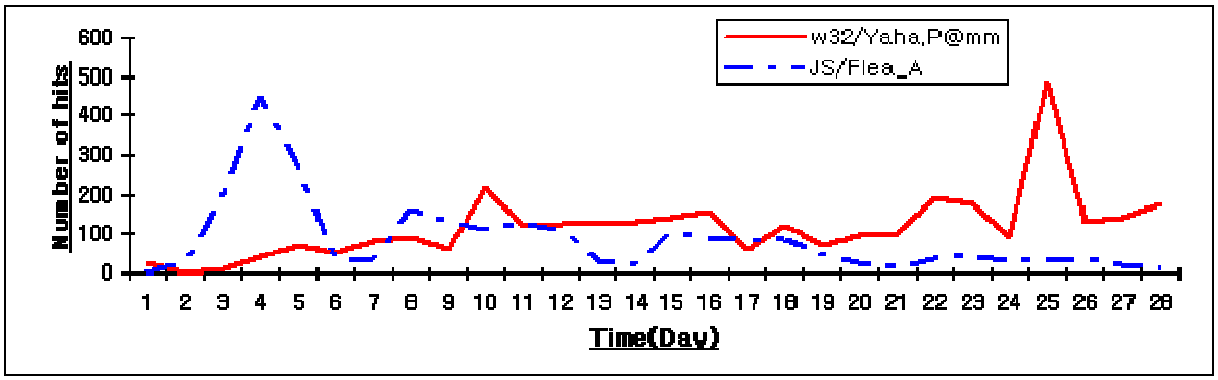


Figure 2. The first month hit number of worms[12]

We now illustrate how Tskewness is computed. At the outset we develop an index by using *the frequency over a specific number of days*. In the example shown below, we demonstrate the computation using 28 days (a month). As a result, we use the equation for the skewness index as,

$$Tskew\_index(V_m) = \frac{3(\bar{Y}_m - Peak_m)}{S_{y_m}} \quad \text{.....(1)}$$

In equation (1),

V_m = index value of date from 1st to 28th for each *m*,
$\bar{Y}_m$ = mean from 1st to 28th, the mean value is fixed with 14.5 point.
$Peak_m$ = specific date of Peak hit from 1st to 28th date,
S_{y_m} =standard deviation from 1st to 28th.

To make *TSKI* 's minimum value zero, we added the absolute minimum value of skewness index.

$$TSKI(V_m) = \frac{3(14.5 - Peak_m)}{S_{y_m}} + |\, Tskew\_index_{minimum} \,| \quad \text{.....(2)}$$

$|\, Tskew\_index_{minimum} \,|$ = absolute minimum value which was computed from equation (1). This absolute minimum value means that the peak hit occurs at the last day (28th day) so that TSKI is greater than or equal to 0.

The mean and median for 28 days are 14.5, and standard deviation (S) is 8.23. Therefore, the range of TSKI is calculated as follow:

[12] Source: http://www.messagelabs.com/viruseye/threats/

$$Tskew\_index_{minimum} = \frac{3(14.5-28)}{8.23} = -4.92, then$$

The range of Tskewness index is

$$(\frac{3(14.5-28)}{8.23} + |-4.92|) \le \text{TSKI} \le (\frac{3(14.5-1)}{8.23} + |-4.92|)$$
$$= 0 \le \text{TSKI} \le 9.8468$$

The closer TSKI is to 9.8468, the larger impact of spread speed the worm has. This is important in that TSKI makes it possible to compare speed of spread, significant to measure the impact among worms. For instance, each TSKI for two worms in Figure 2 is

$$TSKI(JS/fleaA) = \frac{3(14.5-4)}{8.23} + |4.9234| = 8.7527$$
$$TSKI(W32/Yaha.P@mm) = \frac{3(14.5-25)}{8.23} + |4.9234| = 1.0941$$

'7.66' (8.7527-1.0941), the value difference between 'JS/FleaA' and 'w32/yaha.P@mm', implies that JS/Flea A has a greater detrimental impact than w32/Yaha.P@mm.

- **Early time period hit number (LMH)**

Early time period number of hits is defined as the number of hits of a worm from the release date upto the date of measurement which in this illustration is the first month after the worm was released. Since the number of hits varies considerably across the various worms, we use the log value for our computations and for graphing purposes. For the number of hits in first month, we use the acronym Log of Month Hit (LMH)

- **Damage potency (DP)**

The common dimension, "damage potency" also acts as a dimension for STI framework. It is used as common criteria across both frameworks and in Section 7 we demonstrate how it is

used in computing the GSI Index (explained later). The dimensions for two frameworks are summarized in Table 2.

Table 2. The factors for the frameworks

Factors	Initial	Explanation
Total number of hits	*LTH*	The total number of machines infected by worms for the life of the worms
Hit density	*HT*	The ratio of the number of hits of a worm for the first month to the total number of hits during its lifespan
Early time period number of hits	*LMH*	The number of hits of a worm for the first month after the worm was released
Tskewness	*TSKI*	The degree of inclination toward early time periods for the first time period
Damage potency of Worms	*DP*	A rating used to calculate vulnerability, based on the relative damage incurred if a threat should exploit vulnerability[13].

4. Data Collection

The data used in this paper is based on the records of email worms from January 2003 to May 2004 captured by Symantec and Messagelabs on their website[14]. The worms for which data was available had an active life of at least one month to a year and a half. This includes all of the significant worms during that period. All worms that Messagelabs and Symantec deal with were related to email. This data is a relevant sample for this study as the focus of this study is to be able to categorize email worms.

This data includes a variety of variants that refer to the modified version of a worm. These variants are usually developed purposely by a worm author or by someone who modifies the original worm[15]. In case of variants of a worm, it can be argued that organizations may be

[13] Source : Symantec.com
[14] Source: http:// www.Messagelabs.com
[15] Inforsec glossary, http://www.infosec.gov.hk/english/general/glossary_uw.htm#Variant.

able to benefit from the experience of having dealt with the original worm through learning effects. However, it is important to note that the evidence of learning effect *per se* cannot be easily identified for a variety of reasons. First, variants usually spread roughly at the same speed as their parents worms (Lemos, 2003) or may even have more critical effects than parent worms. For example, the Sober.Y variant of the Sober worm has resulted in the worst and largest email worm outbreak in 2005 (Keizer, Nov 23, 2005). Second, variants have become a major stream of creating malicious code. A major trend in the past years has been the seemingly endless number of variants of particular viruses (MessageLabs, 2004). Also, variants show different payloads that result in different damage potency from the original worm. According to antivirus experts (Bruce Hughes, 2003), initial infections from original worm may be only the tip of the iceberg. A payload could for example, include a function to download a modified threat that cannot be detected by current patches. For illustrative purposes, in Table 3, we show the difference with regard to payload (Advisory, January 28, 2004), between *Mydoom.A* worm and *Mydoom.B.*

Table 3. The different payloads between parent worm and a variant

Worm	Payloads
Mydoom.A worm	• Sends emails to users in the infected computer's address book • Leaves a backdoor that can allow the computer to be accessed by a remote attacker. • The backdoor runs on TCP port 3127. • Sends continuous page requests to SCO.com as part of a distributed denial of service attack (DDoS)
MyDoom.B Variant	• Overwrites the local host file to prevent the infected computer from accessing • Microsoft and anti-virus vendor update sites • Opens TCP ports 1080, 3128, 80, 8080, and 10080 for future backdoor access. The backdoor program has the ability to relay TCP packets, which provides IP spoofing • Capabilities and can facilitate future distribution of Spam emails. • Sends continuous page requests to microsoft.com as part of a distributed denial of service attack (DDoS)

Table 3 also shows worm variants may have different mechanisms to facilitate propagation from system to system.

5. Independence Test of the STI and TLI frameworks

In this section, we perform a Chi-square test to identify statistically whether the three dimensions are independent each other in two frameworks.

- **Independence test among dimensions of STI and TLI framework**

To establish that the dimensions of the STI framework are independent, a Chi-square test was performed. A similar process is followed to establish that the dimensions of the TLI framework are independent. Tables 4, 5 and 6 show the results of the Chi-square test based on the fact that each dimension is divided into two (or three) attributes namely high and low which is determined based on wheter the values are lower or higher than the average values. There was no evidence to reject (H_0) the hypothesis that Tskewness has no relationship with Log value of Monthly Hit number (LMH) in STI framework and Hit density has no relationship with total hit number (LTH) in TLI framework, respectively. In other words, Tskewness and LMH, Hit density and LTH have no relationship with one another. Table 4 shows that LMH is not related with TSKI (χ^2=1.879, P>0.1) and that LTH is also not related with Hit Density (χ^2=2.423, P>0.1) as shown in Table 5. Finally, Table 6 shows that damage potency does not have a relationship with the other dimensions.

Table 4: Result of Chi-square test for STI framework

		LMH (Log value of	Total

			monthly hit number)		
			High	Low	
TSkewness	High	Count (Exp.)	20 (16.8)	14 (17.2)	34
	Low	Count (Exp.)	26 (29.2)	33 (29.8)	59
Total		Count	46	47	93
Pearson Chi-Square=1.879(b), *df*=1, Sig. (2-sided) = 0.170					

Table 5: Result of Chi-square test for TLI framework

			LTH (Total hit number)		Total
			High	Low	
HT	High	Count (Exp.)	27 (23.2)	19 (22.8)	47
	Low	Count (Exp.)	20 (23.8)	27 (23.2)	46
Total		Count	46	47	93
Pearson Chi-Square=2.423(b), *df*=1, Sig. (2-sided) = 0.148					

Table 6: Result of Chi-square test for DP and other dimensions

Results of DP and ~	Ch-square	df	Sig (2-sided)
TSKI	.414	1	.642
LMH	.171	1	.824
HD	1.310	1	.179
LTH	.025	1	.874

- **Relationship between the two frameworks**

If the STI Framework is to be utilized as a categorization mechanism, the dimensions of the framework (Tskewness and LMH) should show a relationship with the corresponding dimensions of the TLI Framework (Hit density and LTH respectively). Table 6 describes that correlation between each dimension. The table shows that Tskewness is positively related to Hit density (β=0.412, p<0.001), and LMH is positively related to LTH (β=0.952, p<0.001).

Table 7: Correlation matrix among the 4 dimensions

Dimensions	Tskewness	Hit Density	LMH	LTH
TSkewness	1			
Hit Density	0.412**	1		
LMH[1)]	-0.074	.198	1	
LTH[2)]	-.207	.136	.952**	1
DP	-.030	-.019	.140	.142

**Correlation is significant at the 0.01 level (2-tailed).
1) LMH: log value of 1st month hit number
2) LTH: log value of total hit number

6. Results of Comparing Frameworks

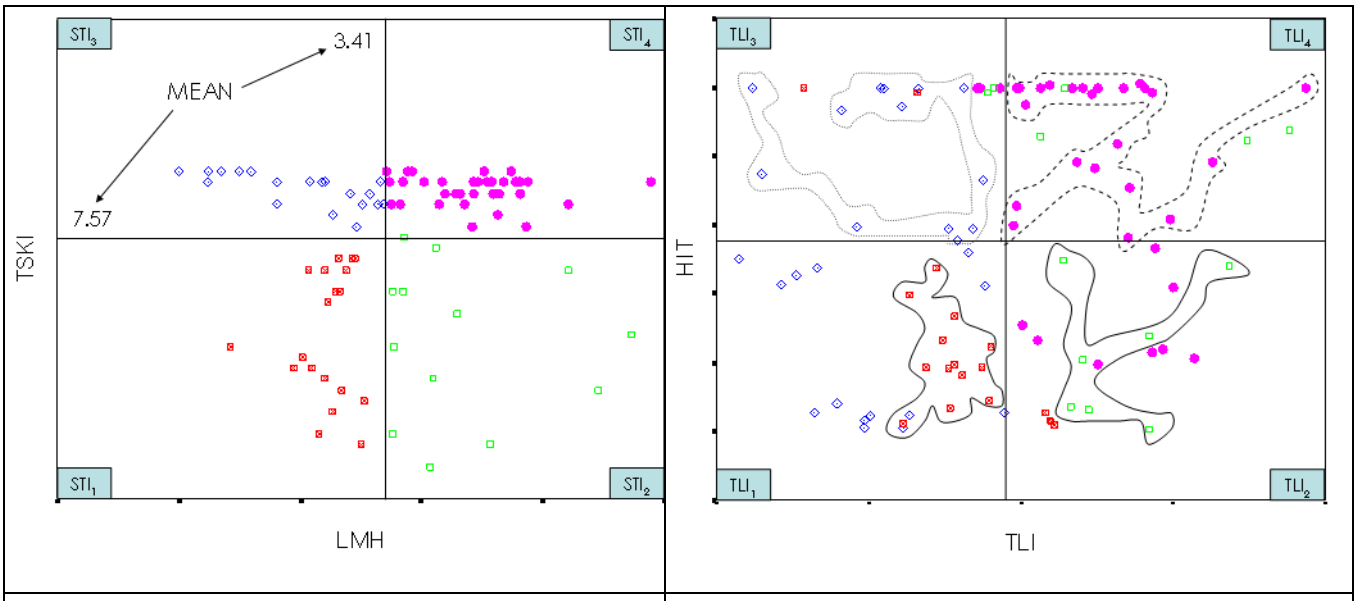
We test correctness and explanatory possibility of the STI framework by comparing it to the TLI Framework by using a *matching ratio*[16]. It stands to reason that if they are well matched, STI can be assumed to be a proper method for the classification of email worms. Please note that the classification using the TLI framework is considered ground truth because the analysis is done after the worm has run its course.

[16] Matching ratio: the ratio between the number of viruses in a cell of STI framework and the number of viruses in corresponding cell of the TLI framework

6.1 Two-Dimensional Categorization

In this subsection we first present the results of the classification based on two dimensions since the third dimension is the same or forms the common criteria. The STI framework analysis was done using the first month of data. The STI framework can be used with early data in the sense that the analysis could have been done using a three days of data, a weeks, data, etc. The process remains the same. Figure 3(a) shows the STI framework using Tskewness and the LMH dimensions. The data for 93 email worms were used in this analysis. Cell 4 (STI_4), to the top right corner is a cell characterized by high number of hits in the first month as well has a high extent of Tskewness. The opposite is true for Cell 1 (STI_1). Clearly, email worms in Cell 4 (STI_4) would be considered to have the highest detrimental impact based on high TSKI and high LMH. In contrast, email worms in cell 1 (STI_1) would have the lowest impact.

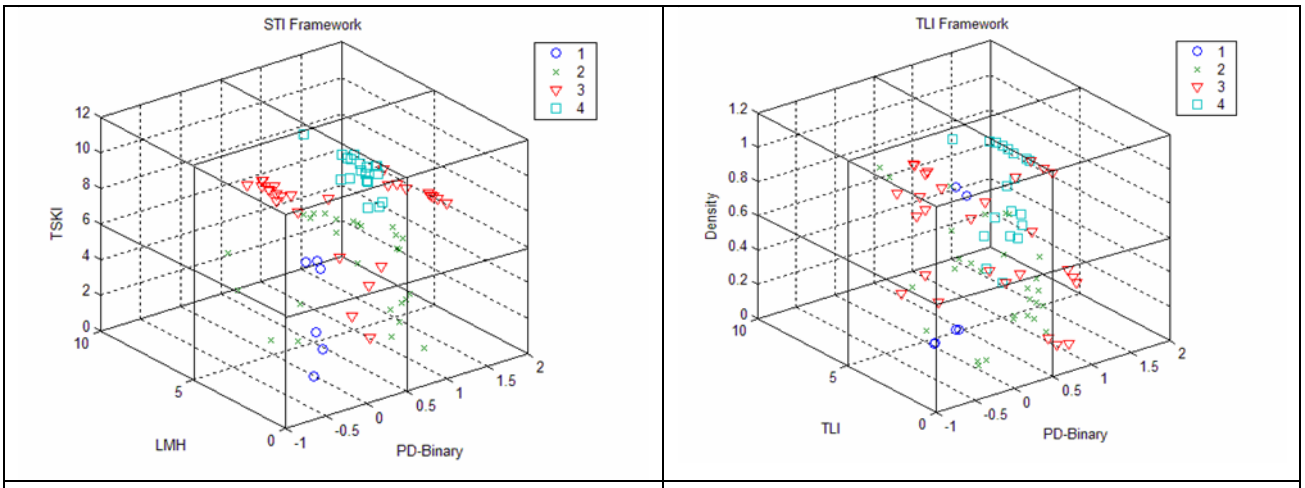
The second picture on the right in Figure 3(b) describes the result using hit density and LTH. Cell 1 ($TLI_{1)}$, to the top right corner is a cell with properties of having high number of total hits as well has a high hit density. The contrary is true for cell 4 ($TLI_{4)}$. The matching email worms in each cell of the respective cells in Figure 3(a) and 3(b) are 13, 7, 9, and 23. The total matched worms for all cells are 52 out of a possible 93. The overall accuracy (matching ratio) is 56% (52/93). The accuracy of each cell is 48.2% (13/27), 36.8% (7/19), 45% (9/20), and 85.2% (23/27), respectively. These values are substantially above similar ratios found in literature (Erlich, Gelbard, & Spiegler, 2002). However, these results are far from desirable so in the next section we discuss the results using three dimensions instead of two.



A) Short Term Impact (STI) Framework	B) Total Life Impact (TLI) Framework

Figure. 3. Two-Dimensional Frameworks for categorization

6.2 Three-Dimensional categorization with damage potency



a) Short Term Impact (STI) Framework	b) Total Life Impact (TLI) Framework

Figure 4. Three-Dimensional Frameworks for Categorization

In order to compare two frameworks with three-dimensions, we categorized the data in the 8 cells into four clusters or levels according to the number of high levels that each group includes. We followed the categorization scale of McAfee and Computer Associates to measure damage potency consistently. For example, if an area has high values in all three dimensions, the area will correspond to level or category 4 as the highest level. On the other hand, if the area has high values in only two or one of the three dimensions, it will correspond to level 3 and 2 respectively. According to this categorization, the highest level (level 4) and lowest level (level 1) include one cell among the 8 cells in the Figure 4, whereas levels 2 and 3 include 3 cells. It is clearly an easy way to classify email worms in the three-dimensional frameworks because the ranking among combinations with three-dimensions is determined explicitly. Therefore, a comparison among those cells can make clear the strength of each level, in contrast to two-dimensional comparisons. Figures 4(a) and 4(b) shows that result of categorization. The result show the number of worms each level in STI framework is 23 (15), 33 (36), 27 (35), and 5 (7) categorized by dimensions in level 4, 3, 2, and 1 respectively. The numbers in parenthesis indicate the number of each level 4, 3, 2, and 1 in TLI framework. The matching ratio of each level indicates the number of worms that the STI framework predicts, divided by the number of true worms that are included in each level. According to the results, the matching number in the TLI framework is 13, 19, 20, and 3. The number of true worms for each level in the TLI framework from Figure 4(b) is 15, 36, 35, and 7. Therefore, the matching ratio is 86.7% (13/15) for level 4, 52.8% (19/36) for level 3, 57.1% (20/35) for level 2, and 42.9% (3/7) for level 1 respectively. Finally, total matching ratio was (55/93) 59.2% and higher value than the result from two-dimensional categorization. The results show a dramatic improvement when all the three dimensions are considered.

7. Validity and Reliability test

To identify the explanatory power for our frameworks, we first used the STI framework and the classification scheme to classify the email worms based on weekly data using 93 email worms. We then compared this with the classification based on complete impact information (TLI framework). We assumed that the TLI framework is the comparison standard reflecting ground truth as it considers data after the worm has run its course (we have assumed this is one and a half years). The results of the comparisons are presented using an adaptation of the Group Similarity Index (GSI) as remain of the section.

7.1 Similarity Index

In order to validate our framework for cluster analysis, we adapt a Group Similarity Index (GSI) from Erlich et al in 2002 (Erlich, et al., 2002). This index provides a simple and easy way of calculating how well the clusters are categorized. According to Erlich et al. (Erlich, et al., 2002), the GSI is defined as "the ratio between the number of similar attribute values, i.e., the number of attributes that entities in a group commonly have and the total number of attribute values for all the entities in the group." The expression for computing the group similarity index is shown as follows:

$$GSI = \frac{sa(G)}{m} \quad \text{.....1}$$

Where,

sa = the number of similar attribute values of a group

G = a group of k entities which is $[i_1, i_2, \ldots, i_k]$

Sa(G) = the number of commonly shared attribute values in group G[17]

m = the number of attributes, which indicates the product of number of attributes and number of entities

GSI has an assumption that all attributes included in the analysis should have a property of mutual exclusivity i.e., an entity must obtain exactly one of the possible values for each attribute (Erlich, et al., 2002). since this study has the same property as previous work, we adapt and the simplified form for the group similarity index is given by the expression:

$$GSI_{ct} = \frac{sa}{A \times G}, \text{and } sa = \sum_{i=1}^{6} D_i \text{.....2 ,}$$

Where,

c= cell level and t = time.

sa = the number of commonly shared attribute in a level

D= the number of commonly shared attribute in i^{th} *dimensions*,

A= the number of attributes, and

G= the number of email worms in each level on TLI framework

The number of commonly shared attribute D_i , which was coded by binary number, is based on the number that email worms in each level are coded identically An email worm in each cell is checked against 6 factors (see Table 1) in two frameworks. For example, Table 8 shows that the number of email worms matched with 6 factors for cell 4 in a month. The number 1 in the table indicates a binary representation matrix value, which means that an email worm

---

[17] In equation,, $sa(G) = \frac{\sum_{j=1}^{m} \sum_{K=1}^{P_j} \sum_{i \in G}, \sum_{xijk \geq rj} |G|^{sijk}}{|G|}$,

Where, *j*=attribute domain, *k*=number of entity, P_j= mutual exclusive possible value, so for each attribute a_j, an entity can attain exactly one of P_j domain values.

has a factor value, and the number 0 indicates the email worm does not have that factor value. For example, if an email worm has high TSKI, the worm has the attribute "TSKI" and then is coded 1 and zero otherwise. Thus, commonly shared attribute means that email worms in a group have same number (1 or 0) on an attribute. Accordingly, Equation 2 has basically the same structure as Equation 1 in estimating GSI for worms in that two equation have same logic and property except that Equation 2 has fixed six attributes. In the summary in Table 8, 16 email worms have matched values of 13, 16, 16, 16, 16, and 16 on each factor respectively. Therefore, the number of commonly shared attribute in a cell *sa* is 93 (13+16+16+16+16+16).

Table 8: The number of email worms which have same factor in Cell 4 in Third week

Attribute / Email worms	STI framework			TLI framework		
	TSKI	LMH	$DP_{initial}$	HT	TLI	DP_{final}
w32/beagle.a@mm	1	1	1	1	1	1
w32/beagle.b@mm	1	1	1	1	1	1
w32/beagle.j@mm	1	1	1	1	1	1
w32/beagle.n@mm	0	1	1	1	1	1
w32/lirva.a@mm	1	1	1	1	1	1
w32/mimail.c@mm	1	1	1	1	1	1
w32/mimail.e@mm	1	1	1	1	1	1
w32/mimail.f@mm	0	1	1	1	1	1
w32/mimail.g@mm	1	1	1	1	1	1
w32/mimail.h-mm	1	1	1	1	1	1
w32/mimail.j@mm	1	1	1	1	1	1
w32/mimail.q@	1	1	1	1	1	1
w32/mimail.s@mm	0	1	1	1	1	1
w32/mydoom.a@mm	1	1	1	1	1	1
w32/mydoom.f@mm	1	1	1	1	1	1
w32/yaha.l-mm	1	1	1	1	1	1
Matched #	13	16	16	16	16	16

Table 9 shows the number of commonly shared attribute of each dimension of classification for each week on a cumulative basis from the first to the fourth week. In Table 5,

we show the GSI values that have been computed using equation 2. The Table shows that the accuracy of the classification improves with time.

Table 9: Weekly GSI

Week	Cell #	Ground Truth (from TLI)	STI dimensions			TLI dimensions			GSI
			TSKI	LMH	$DP_{initial}$	HT	LTH	DP_{final}	
First	$Cell_1$	6	2	6	6	6	6	6	88.9%
	$Cell_2$	42	17	20	28	25	41	41	68.3%
	$Cell_3$	29	15	16	10	15	29	29	65.5%
	$Cell_4$	16	11	10	7	7	16	16	69.8%
Second	$Cell_1$	6	2	6	6	6	6	6	88.9%
	$Cell_2$	42	17	17	26	28	41	41	67.5%
	$Cell_3$	29	16	16	12	21	29	29	70.7%
	$Cell_4$	16	14	15	10	15	16	16	89.6%
Third	$Cell_1$	6	2	6	6	6	6	6	88.9%
	$Cell_2$	42	17	17	26	26	41	41	66.7%
	$Cell_3$	29	18	16	16	22	29	29	75.3%
	$Cell_4$	16	14	15	13	15	16	16	96.9%
A month	$Cell_1$	6	2	6	6	6	6	6	88.9%
	$Cell_2$	42	17	16	25	28	41	41	66.7%
	$Cell_3$	29	19	16	15	23	29	29	75.3%
	$Cell_4$	16	13	16	16	16	16	16	96.9%

The range for group similarity index is between 0 and 1. A GSI value of 1 implies maximum similarity and a value of 0 indicates minimum similarity between email worms.

Based on the adjusted equation, we compute the GSI for all the clusters 4 weeks after the release of the worm using equation 2 as shown in expression 3.

$$GSI_{level,time} = \frac{TSKI + LMH + PD_{initial} + HT + LTH + DP_{final}}{Number\ of\ Attribute \times Ground\ Truth} \quad \ldots\ldots\ldots\ldots 3$$

$$GSI_{1,4} = \frac{(2+6+6+6+6+6)}{6\times 6} = 88.9\%,$$

$$GSI_{2,4} = \frac{(17+16+25+28+41+41)}{6\times 42} = 66.7\%,$$

$$GSI_{3,4} = \frac{(19+16+15+23+29+29)}{6\times 29} = 75.3\% \text{ , and}$$

$$GSI_{4,4} = \frac{(13+16+16+16+16+16)}{6\times 16} = 96.9\%$$

These results suggest that the classification method applying two frameworks which was developed in this study is valid and reliable method to cluster email worms.

Figure 5 indicates the GSI trends of the STI framework during the period from 1 week to 4. The Figure shows that the prediction rate increases for all of the categories except for category two for which we see slightly reduced values. For example, for 6 worms in cell 1, GSI of week 1 reveals that STI framework with 1 week data can predict 88.9% of true worms which are based on TLI framework. The figure shows that the prediction rate increasing but cell 2 which is slightly reduced. This decrese in GSI is caused by migration of the placement of worms into other cells in some particular dimensions. As seen in Table 9, the GSI changes as the number of one of six dimensions is changed. In the case of cell 2, the GIS decreased, as the number of LMH and $DP_{initial}$ are reduced over time. That is, several worms which were placed in cell 2 moved into a higher level such as cell 3 or cell 4.due to increase of hit number over a certain period of time (i.e. weekly base in this case). As a result, the GSI of cell 2 was decreased, while the GSI of other cell to which the cell moved increased correspondingly.

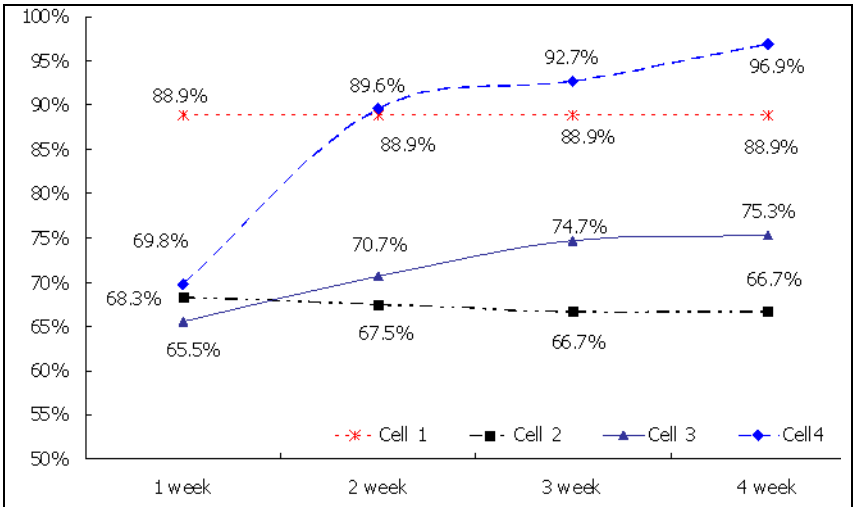


Figure 5. Weekly Trend of GSI

The GSI method further gives support to the categorization that we have employed.

Table 10 shows the overall GSI results for a month unit.

Table 10: Clustering using a month of GSI

Level	N	GSI	Members
1	6	**88.9%**	S/Flea.B; JS/Forten.B-m: W32/Dumaru.F-mm: W32/Dumaru.I-mm; W32/Kindal-mm; W97M/Ethan.d095:
2	42	**66.7%**	2JS/Flea_A; JS/Forten.E-m; VBS/Redlof.E-m; VBS/Soraci ; w32/Gibe.C@mm; w32/Israz@mm; W32/Lovelorn.B-mm; W32/Mapson.A-mm; w32/Mimail.M@mm; w32/Mimail.P@mm; w32/Netsky.F@mm; w32/Nicehello@mm; W97M/Ethan.B; VBS/Lovelorn.dr; w32/Ganda.A@mm; w32/Gibe.B@mm; W32/Lirva.B-mm; W32/Lovelorn.A-mm; w32/Mimail.A@mm; w32/Sober.C@mm; w32/Yaha.P@mm; JS/Netdex-m; VBS/Lubus.A; w32/Dumaru.B@mm; W32/Dumaru.E-mm; W32/Dumaru.G-mm; w32/Dumaru.M@mm; W32/Kriz.3863; w32/Kwbot.E.Worm; w32/Mapson.D.Worm; W32/Mimail.C; W32/Mimail.K-mm; w32/Mydoom.B@mm; W32/Nofear.A-mm; W32/Nofear.B-mm; W32/Tenrobot.B; w32/Yaha.AA@mm; W32/Yaha.P!15bb-mm; w32/Yaha.S@mm; w32/Yaha.T@mm; W32/Yaha.X-mm; W32/Yaha.Y-mm

3	29	**75.3%**	W32/Beagle.K@mm; w32/Bugbear.B@mm; W32/Holar.L-mm; W32/Lovgate.F-m; W32/Lovgate.G-m; w32/Mimail.I@mm; w32/Sobig.A@mm; w32/Swen.A@mm; W32/Swen.B-mm; W32/Torvil.D-mm; w32/Yaha.Q@mm; W32/Yaha.R-mm; w32/Beagle.F@mm; W32/Lovgate.L-m; w32/Mimail.L@mm; w32/Mimail.T@mm; w32/Sober.B@mm; w32/Sobig.D@mm; w32/Beagle.C@mm; w32/Beagle.E@mm; w32/Dumaru.Y@mm; w32/Dumaru.Z@mm; w32/Netsky.B@mm;w32/Netsky.C@mm; w32/Scold@mm; w32/Sobig.B@mm; w32/Sobig.C@mm; w32/Sobig.E@mm; w32/Sobig.F@mm
4	16	**96.9%**	Jw32/Beagle.A@mm; w32/Beagle.B@mm ; w32/Beagle.J@mm; w32/Beagle.N@mm; w32/Lirva.A@mm; w32/Mimail.C@mm; w32/Mimail.E@mm; w32/Mimail.F@mm; w32/Mimail.G@mm; W32/Mimail.H-mm; w32/Mimail.J@mm; w32/Mimail.Q@mm; w32/Mimail.S@mm; w32/Mydoom.A@mm; w32/Mydoom.F@mm; W32/Yaha.L-mm
GSI Avg.	**93**	**81.9%**	

8. Discussion and Conclusion

The purpose of this paper was to develop a new method to classify email worms and to provide a mechanism to compare email worms by employing a visual framework. To this end, we have developed a statistically refined clustering measurement scheme. Our analysis is a first step in clustering email worms according to their detrimental impact. More elaborate efforts are needed to refine the framework in the future. This study contributes to enhancing managerial practice. First, this study identifies factors, which are necessary to categorize email worms into three dimensions of STI framework: Tskewness (TSKI), Monthly Hit number (LMH), and Damage Potency (DP). The STI framework uses early data (3 days, week, two weeks, month, etc) to classify e-mail worms. We have shown that as we get more data the results become much stronger. The accuracy is quite significant validating the methodology. The methodology uses statistical techniques to establish that independence of the dimensions and also the positive correlation between the two frameworks.

Second, this study applies GSI to our framework for clustering of email worms to enhance validation and reliability. The study has identified an important need that is related to provide a way to do early triage of Malware that will assist organizations to allocate resources for response.

This study also has several limitations. First, we did not consider the prevalence patterns of distribution, frequency, and seasonality, because this study was performed under the assumption that worms included in this study are in the equal conditions. As aforementioned, these constraints make it difficult for the frameworks to adapt in exploring changes of worms as time goes on. This could perhaps be overcome in future research with more specific experimental conditions. Second, we used the log value of hit numbers because of the difference (variance) of hit number unit between the email worms. It is possible that 'Log value' shrinks the difference between two email worms which have a huge disparity in the size. We also assumed that the data at the end of one and a half years represents the entire life of an email worm in terms of hits.

The study could be expanded by considering a larger data set. However, an achievable observation is that if we collect more information on email worms as a community; a more accurate prediction may be possible. In this study, we divided the factors into four categories based on high and low values. On the one extreme, we have the option of creating one or two categories. This would not have provided sufficient discrimination for action. The other extreme is the creation of 93 classes, one for each email worm which is clearly unreasonable. We chose to create four categories as these are most actionable from the point of view of the insurance companies and system managers. However, it is possible to draw other tradeoffs in terms of the number of clusters that could conceivably be created. Research in terms of developing an

economics analysis taking into account the detrimental impact of an email worm and the cost relating office-disruption, etc. is a potential area for future exploration. A major limitation in the area of viruses and worms is the availability of data.

Essay 2: The Effect of Spam and Privacy Concerns on Email Users' Behavior

1. Introduction

E-mail has become one of the most popular Internet services providing instant and convenient message delivery. Unfortunately, e-mail also enables the spread of spam mail which is unsolicited, unwanted, and inappropriate bulk e-mail (Neumann & Weinstein, 1997). Spam creates problems such as cost shifting, fraud, resource wastage, and the displacement of legitimate mail (Cournane & Hunt, 2004). Its proliferation is increasing rapidly and it is a potential threat to the credibility of email as a reliable and efficient means of communication over the internet. Further, the effect of spam on the infrastructure and conveniences provided by the internet has augmented *privacy concerns* among email users and has served to reduce users' welfare. According to the Pew Internet Report (Fallows, 2003), 76% of the users who received spam responded that spam compromises their privacy[18].

Spam email evokes both direct and indirect *privacy concerns*[19] in users (Sipior, Ward, & Bonner, 2004). *Privacy concerns* that are derived from spam may be indirect as spam focuses

[18] Privacy is defined as "the ability of the individual to control personally information about one's self (E. F. Stone, Gardner, Gueutal, & McClure, 1983: p. 460)." or "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others (Westin, 1967: p. 7).

[19] Privacy concerns refer to an individual's subjective views of fairness within the context of information privacy(A. J. Campbell, 1997). According to this definition, privacy concerns include individual's personal traits or general disposition to privacy invasion. The concerns for information privacy are affected by external conditions such as industry sectors, cultures, or regulatory laws (Malhotra, Kim, & Agarwal, 2004).

users' attention on privacy when they receive spam mail. In addition, spam email immediately raises concerns about privacy, concerns that are triggered by perceived harm when information is released by the offending party (Wathieu & Friedman, 2005). The foregoing raises the research question: *does the receipt of spam alert the user to privacy concerns*? This issue has not been examined to any extent thus far, although there exists a relationship between spam email and *privacy concerns*. A study of the relationship between spam and privacy can provide benefits to the information security field. It may draw attention to the way in which spam email can affect users' behavior with respect to their email-usage by alerting them to internal concerns regarding their private information.

Users may exhibit different behaviors by invoking defense or coping mechanisms, consciously or unconsciously, to deal with junk e-mail. For example, when they receive spam or junk email, some users may be discouraged from using the internet *itself* or they may harbor negative attitudes towards internet email, while others may solve the problem by finding and eliminating the problem using spam filters, changing e-mail addresses, ensuring that their e-mail address is not available easily on the internet, etc. Although these different behaviors exhibited by users depend largely upon the user's personal characteristics, or his or her preferences, their attitude can be largely affected by cognition, affection, or beliefs (Rosenberg & Hovland, 1960) which may stem from a *spam experience* or because of *privacy concerns*.

This paper attempts to examine the effect of *privacy concerns* on user's behaviors after they have been exposed to spam e-mail. The contributions of this study are twofold: First, this study explains users' coping behavior with regard to spam email as it relates to privacy

protection. By paying attention to the underlying psychological processes and motives, the current study also provides insight on how email users behave while protecting their privacy. Second, this study provides a theoretical scheme for the users' behavior with regard to spam and privacy. In other words, this study explains the effect of spam email and *privacy concerns* on users' behavior by using a psychometric approach.

This paper is organized as follows. The relevant literature on spam and privacy is discussed in Section 2. In Section 3, based on theoretical arguments, four hypotheses are proposed. The methodology for the analysis is contained in Section 4. Results and the summary analysis form the contents of Section 5. Finally, in Section 6, the implications of the findings for management policy and research on spam and privacy are discussed.

2. Background

In this section, at the outset, we provide a general background on the effects of spam along with an overview of the background literature as it relates to the topic of this paper. This section also includes a discussion of defense mechanisms and user behaviors, i.e. usage-oriented and protection-oriented behaviors.

2.1. Spam and Privacy

Spam is unsolicited electronic mail, most often in the form of commercial advertising (Cournane & Hunt, 2004). According to the Federal Trade Commission[20], in the United States two out of three of these messages contain misleading information. Some consumers find unsolicited commercial email - also known as "spam" - annoying and time consuming; others

[20] Federal Trade Commission, *False Claims in Spam*, April 30, 2003. Available from: http://www.ftc.gov/reports/spam/030429spamreport.pdf. [Accessed 25 December 2006].

have lost money to bogus offers that arrived in their email in-box. Companies have reported financial losses due to the costs of unwanted spam traffic. Judge *et al*. (2005) demonstrate in their work how spam detrimentally affects internet use for company business.

In the economic context, spam cost European companies $2.8b in lost productivity alone. US based companies reported a loss of $20bn (Hinde, 2003). This loss includes the time it takes people to delete the messages, the cost of buying larger mail servers and storage systems to cope with inboxes flooded with spam messages, and the cost of having staff unclog networks overloaded by spam. According to a report by MacAfee, entitled "MacAfee Americans and spam survey"[21], spam is the prime technology time waster (49%) as compared to other technical annoyances including automated voice response systems (24%) and slow internet connections (19%). This survey revealed that 49% of Americans spend more than 40 minutes per week deleting spam, while 14% reported that they spend as much as 3.5 hours a week - or 7½ days per annum - on this task.

Hinde (2002) states that spam email has become a potent weapon for targeting unsuspecting consumers and stealing their money and identities. The new trend in spam according Hinde (Hinde, 2002), is its ability to enhance fraudulent schemes and victimize unsuspecting users. Certain traits of spam, particularly the low cost and the ubiquity of email usage, has made spam the best choice for internet fraudsters and identity thieves. Previous research on privacy in this area has focused mainly on economic effects (Huberman, Adar, & Fine, 2005; Odlyzko, 2002) or the privacy trade-offs that individuals are willing to make in order

---

[21] Federal Trade Commission, *False Claims in Spam*, April 30, 2003. Available from: http://www.ftc.gov/reports/spam/030429spamreport.pdf [Accessed 25 December 2006].

to access specific services (Acquisti & Grossklags, 2003, 2005; Hann, Roberts, Slaughter, & Fielding, 2004; Syverson, 2003).

In much of the published literature that addresses the disparities between stated privacy attitudes and actions, the implicit assumption is that people have *privacy concerns*.

There is little research on the relationship between a user's behavior and spam email as well as the mediating effect of *privacy concerns* on the relationship in an email usage context. By understanding whether a user's behavior is affected by spam e-mail alone or if privacy concerns also play a role will allow us to design better systems to ensure a more satisfying experience for the user of e-mail systems. Studying this issue can also provide some understanding about the major reason why email users cope with spam email. Regarding users' behavior, previous research has only shown the privacy paradox which contends that users behave irrationally regarding private information. For example, Syverson (2003) shows that users place a high value on privacy while they paradoxically disregard their privacy in exchange for meager benefits such as a free hamburger or a two dollar discount on groceries. In this paper, we establish that users exhibit both passive and active dual behaviors after a *spam experience* and especially if they have *privacy concerns*.

2.2. Defense Mechanisms

Individuals go through a series of reactions when they are personally confronted with anxiety—they develop a number of internal defense mechanisms to protect themselves from the unpleasant feelings of anxiety (de Board, 1978). Anxiety not only arises from perceived external dangers, but can also be experienced within the individual for no obvious reason (de Board, 1978). This internal resistance called anxiety is often caused by past experiences, fears, or worries the individual has experienced (Wayne & Andrew, 2001).

Defense mechanisms are habitual and unconscious strategies used to deny, distort, or counteract sources of anxiety and to help maintain an idealized self-image (Cramer & Block, 1998). Defense mechanisms lie on the surface of human conduct and can be observed without the help of any explicit or standardized assessment procedure (Hentschel, Juris G. Draguns, Ehlers, & Smith, 2004). In fact, they can be measured by automatic psychological processes that protect the individual from anxiety and from the awareness of internal or external stressors. Email-users, for example, are often unaware of these processes as they operate, even though defense mechanisms mediate the individual's reaction to emotional conflicts and internal and external stressors (p. 751)[22]". According to Holmes (1985) there are three central features of defense mechanisms: avoidance or reduction of negative emotional states, distortion of reality to various degrees, and the lack of conscious awareness in the use of defense mechanisms. Vasiliuk (1992) identifies the following four types of experience as antecedents to the reliance on defense mechanisms: stress, frustration, conflict, and crisis. Several or all of these four conditions can occur together. Even though psychoanalysis has traditionally focused on internal threats and conflicts, the fact that external dangers could trigger defense mechanisms has been recognized (Draguns, 2004).

Due to these characteristics, defense mechanisms have been used to examine individual reactions to organizational change (see Carnall, 1986; Oldham & Kleiner, 1990; Ondrack, 1974; Wayne & Andrew, 2001). However, there is a lack of research on users' reactions to the Internet. Defense mechanisms represent more an effort to confirm, adapt, or adjust to one's surroundings rather than an effort to influence and mould those surroundings to fit one's own desires and ideas.

---

[22] American Psychiatric Association, *Diagnostic and statistical manual of mental disorders*. Washington, DC., The Association, 1994.

Accordingly, users will manifest their behavior on spam or privacy in various avoidant ways such as undoing, repression, denial, and so on. For example, the act of 'undoing' involves nullifying a distressing experience through a reverse action (Clark, 1991). 'Repression' involves removing from one's consciousness painful or shameful experiences (Waldmann, 2000); this process enables an individual to 'conveniently forget' their own undesirable and unethical behavior. On the other hand, 'denial' is a defense mechanism which a person may rely on in an attempt to protect himself of herself from some painful or frightening information related to external reality (Breznitz, 1983). Email users particularly choose avoidance tactics such as undoing or denial when coping with spam in an online context. For instance, users may try to use e-mail less frequently to avoid the annoyance or to protect their privacy.

2.3. User's Behaviors

Bovey and Hede (2001) claim that when users attempt to protect their privacy, their behaviors can be classified as active or passive. Accordingly, we categorize users' behavior as being (a) usage-oriented (passive) or (b) protection-oriented (active). In the remainder of this section, we discuss these two behaviors. Users may have several ways to protect their email accounts from spam or junk mail. They consciously or unconsciously use well-developed and habitual defense mechanisms to protect themselves from spam email and from related anxieties. Users can protect private information by reducing their email usage or by simply avoiding it altogether. On the other hand, by reporting spam or using protection programs and filters, they can aggressively counter spam mail. Post-spam behavior differs depending on the subject's previous *spam experiences* and privacy concerns.

The foregoing two behaviors are different in that usage behavior is a typical defense mechanism, while the second behavior is just defensiveness. According to Cramer (2004), the

term defense mechanism is a theoretical construct that describes a cognitive operation where as defensiveness is a more general term which refers to behaviors that protect the individual from anxiety, loss of self-esteem, or other disrupting emotions. Further, Cramer (2004) argues that a critical distinction between a defense mechanism and defensiveness is that the former is focused on an unconscious or conscious attitude, while the latter may be consciously recognized by the individual.

2.3.1. Usage-Oriented Behavior (UOB)

We use the term "usage-oriented behavior" to describe a behavior that relates to avoiding or reducing email use. This is a typical defense mechanism in the guise of avoidance behavior. Individuals are often unaware of these processes as they operate. Defense mechanisms mediate the individual's reaction to emotional conflicts and internal and external stressors.[23] The matter is, as Kraut (2005) mentions, not so much that dealing with junk email or spam is no longer a mere nuisance, but also one that it leads internet users to have *privacy concerns*. As a result, users may try to avoid using email on the internet as an effective method because the spam or junk mail might be too difficult for them to guard against with protective methods.

2.3.2. Protection-*Oriented Behavior (POB)*

We use the term "protection-oriented behavior" to describe a more active response to spam. Such actions may include reporting spam to the email provider and applying protection filters, or reporting spam to a consumer or government agency. In contrast to usage-oriented behavior in e-mail use, protection-oriented behavior represents the direct impact of spam and

---

[23] American Psychiatric Association, *Diagnostic and statistical manual of mental disorders*. Washington, DC., The Association, 1994.

perceived privacy on users' behavior. Thus, protection-oriented behavior is defined as a "user's positive defense behavior to protect their privacy from particular problems such as spam, hacking, and so on."

The difference between usage-oriented and protection-oriented behavior is not only the degree to which a user's attitude towards privacy impingements are positive or negative but also, in contrast to usage-oriented behavior, protection-oriented behavior actively (rather than passively) protects against spam.

In addition, protection-oriented behavior may depend on perceived privacy rather than spam because users may tend to give priority to protecting private information rather than avoiding spam. A likely reason why spam is perceived to be more threatening than ever is because internet users are beginning to recognize that spam is related to privacy intrusion. This study also assumes that users who know that junk mail or spam resulted from their behavior caused by using the internet will more likely to have *privacy concerns*. As a result, perceived privacy may provide mediating effects on the relationship between spam and protection-oriented behavior. That is, protection-oriented behavior may not be affected by spam directly.

2.3.3. Independence of Two Behaviors

Empirical and theoretical research shows that consumers often lack adequate information to make appropriate privacy-sensitive decisions and, even with sufficient information, they are likely to trade off long-term privacy for short-term benefits (Acquisti & Grossklags, 2005). By contrast, however, users may reveal dual behavior when protecting their privacy, assuming they have enough information about protection. Usage-oriented behavior and protection-oriented behavior are two different and exclusive strategies. If users conduct one of these behaviors, they

do not engage in the other behavior, in general. That is, according to the definitions of the two behaviors as mentioned above, there are probably no intersections between usage and protection oriented behavior.

This dissimilarity is not only because users who discontinue email usage do not have to take care of their email. On the other hand, email users who exhibit protection-oriented behavior use email without considering a reduction in email usage. Since the users acted to prevent their email from attacks, they also would not consider email as an alternative.

The two behaviors (i.e., usage-oriented and protection-oriented behavior) that arise due to the receipt of spam are normally mutually exclusive. The rationale for this is that email users who exhibit protection-oriented (active) behavior are unlikely to engage in usage-oriented (passive) behavior. This relationship between the two behaviors (i.e. usage-oriented and protection-oriented behavior) may be violated because of privacy concerns or the receipt of *spam*. For example, if a user engages in both usage-oriented (passive behavior) and protection-oriented (active) behavior regardless of any other consideration, then we regard this behavior as dual behavior.

In this study, we use term "*dual behavior,"* which refers to an action demonstrating two exclusive behaviors at the same time. When an email user tends to show this dual behavior as a means to cope with spam or privacy rather than to show just either one of two behaviors, we can say that the user is dual behavior. In other words, whenever users are aware of the circumstances surrounding them, or they feel that their privacy is vulnerable, they would manifest their dual behavior, even with perfect information.

3. Hypothesis

This study divides the hypothesis into two different parts. First, Hypothesis 2 and 3 explore the effect of a spam experience and privacy concerns on usage-oriented and protection-oriented behavior. In the second part of this section, we examine email users' behavior by exploring the email user's *dual behavior.*

3.1. The Effect of Spam and Privacy on a Single Behavior

In this section, we present a causal model that affects "Usage-oriented Behavior" and "Protection-oriented Behavior." Figure 1 shows this study's conceptual model for the effect of spam and privacy concerns on a single behavior.

As the first issue of this study, we argue that a spam experience affects users's concerns about the privacy of their information, as mentioned in our research question. Email users believe that spam threatens their privacy. Most users fear that their personal information might fall into the hands of unscrupulous people, such as marketers, who will then intrude upon them with unwanted calls and messages or worse (Fahlman, 2002). Han and Maclauin (2003) found in a survey of attitudes to online privacy that a number of respondents labeled spam as a major privacy issue.

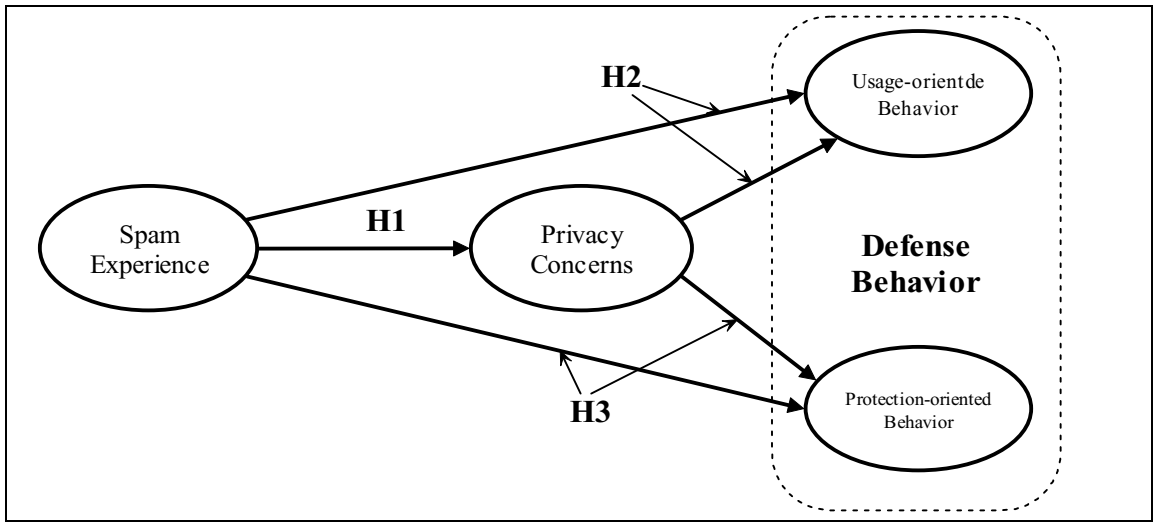


Figure 1. Conceptual Model for Hypothesis 1 to 3

In reality, spam is, indeed, a major privacy issue (Syverson, 2003). While receiving spam can be a consequence of users' negligence in keeping their private information secure, it can also be the result of the illegal distribution of email addresses. Therefore,

Hypothesis 1*: The receipt of spam affects privacy concerns.*

Although the users' experience with spam causes defensive behaviors, the experience can cause different types of behavior. Since usage- and protection-oriented behaviors may be motivated by hierarchically different levels of stimuli, the exhibition of one of those two behaviors depends on the level of stimuli such as spam experience and privacy. Along with the effect of spam experience on usage-oriented behavior, privacy concerns mediate the relationship between spam experience and usage-oriented behavior. Protection-oriented behavior precedes usage-oriented behavior in the degree of intensity. As a result, Hypothesis 2 is as follows:

Hypothesis 2*: spam experience and privacy concerns affect users' usage-oriented behavior.*

Compared to usage-oriented behavior, protection-oriented behavior requires more effort for users to initiate the action because the behavior is more active and conscious. This means that users may not initiate the behavior without stimuli which seriously threatens them such as notification of fraud, warning of abuse of private information, and so on. One of the privacy concerns that can serve as an anxiety trigger is the recognition that private information can be abused by others. For example, without (implicit or explicit) agreements for other uses, privacy

is violated if the merchant later uses that personal information in a manner outside of this primary use (e.g., the merchant sells his customer list) or allows the information to be disclosed to a party not involved in the primary use as secondary use (R. G. a. M. D. Smith, 2005). In summary, protection-oriented behavior will not be conducted because of a *spam experience* but out of concern for privacy

Hypothesis 3*: user's experience with spam does not affect their protection-oriented behavior but privacy concerns do affect their protection-oriented behavior.*

3.2. The Effect of Spam and Privacy on Dual Behavior

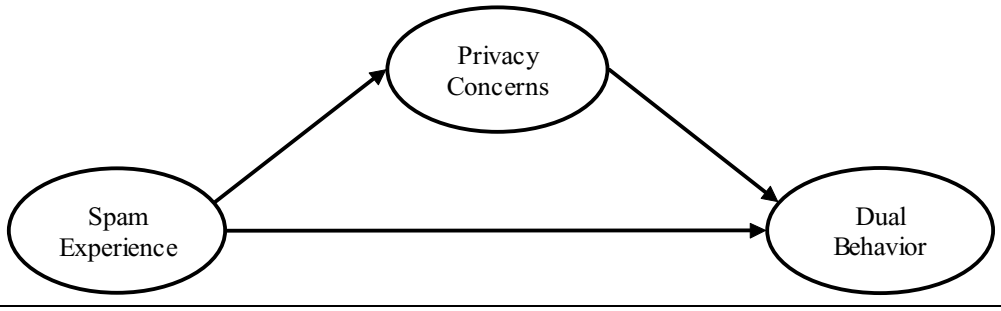


Figure 2. Conceptual Model for Hypothesis 3

When a user engages in both active (protection-oriented) and passive (usage-oriented) behavior at the same time, we term this behavior as *dual behavior*. This behavior is also viewed as the expectation is that he or she engages in one of the two behaviors but not both at the same time. Since usage-oriented behavior is mutually independent with protection- oriented, we assume that rational users would not undertake two behaviors, even though the users have extremely bothersome experiences with spam email. However, when users are annoyed, they are apt to act irrationally. Moreover, spam experience can lead users to undertake dual behaviors

simultaneously. For example, if users consider spam emails as very bothersome, this spam experience could cause users to exhibit usage- and protection- oriented behaviors at the same time.

Furthermore, privacy concerns mediate the relationship between spam and the *dual behavior.* In other words, the users' dual behavior would be caused not only by the impact of the *spam experience* but also by *privacy concerns.* Therefore, we propose,

> ***Hypothesis 4****: Privacy mediates the relationship between the spam experience and a user's dual behavior*

4. Methodology

In this section, we present a methodology in terms of the data collection and the constructs that we have developed for this study.

4.1. Data Collection and Research Method

In order to test these four hypotheses, this study used 'The Pew Internet and American Life Project' data surveyed by the "Pew Internet Research Center" in 2003. The data was surveyed to determine Internet users' attitudes towards spam and the use of email filtering from 6/10/03 to 7/3/03. Individuals who were 18 or older participated in the survey. This Pew survey data contained about 4000 responses that related to all internet users. For this study, we filtered out 2,279 participants because they were e-mail users.

The sample was confined to people who have email accounts and use e-mail every day. Of these 2,279 only 588 users were selected for analysis relating to Hypothesis 1, 2 and 3 as they corresponded to all e-mail users who had a spam experience and then engaged in either protection-oriented or usage-oriented behavior but not both. From the set of 2,279 e-mail users,

1,490 exhibited engaged in either protection-oriented or usage-oriented behavior or both and their responses were used to test Hypothesis 4.

4.2. Constructs

This study uses two different constructs as dependent variables: usage-oriented behavior and protection-oriented behavior.

4.2.1. Spam Experience

Email users experience spam or junk mail each time they log onto the Internet. The experience is measured by the number of spam mails received on a given day or the percentage of spam mail in relation to the total daily mail. In the Pew research questionnaire, *spam experiences* are measured by the following items: "Of all the email you receive in your personal (account/accounts) on a typical day, what percentage are personal messages and what percentage are junk email or spam." This construct was measured as a 7-point scale (1 implying "none" to 7 implying "81 % or more").

4.2.2. Perceived Privacy Concern on spam

Privacy is a uni-dimensional construct (H. J. Smith, Milberg, & Burke, 1996). However, in this study perceived privacy concern was captured in the original Pew research survey via a multiple choice question that asked users to respond to the question "which characteristics of spam affect their email usage". The choices available to responders were: "spam has compromised users' privacy", "Deceptive or dishonest content", "Offensive or obscene content", "the amount of spam online", "the time it takes to deal with spam" and "it is unsolicited or you did not ask for it", and "the damage it can do to your computer". The responses were then

encoded on a dichotomous scale (yes / no) based on whether the respondent chose the answer "spam has compromised users' privacy" or not.

4.2.3. Usage-Oriented Behavior

Usage-oriented behavior is defined by the construct referred to in the original Pew questionnaire as "reducing behavior caused by spam or junk mail". This construct consisted of two items: "Reduced your overall use of email" and "Made you less trusting of email in general".

These items capture intent rather than actual amount of reduction in email usage. The construct 'usage-oriented behavior' is measured on a dichotomous scale based on the responses to the above two items. The construct, therefore, reflected the users' behaviors by measuring their responses on a dichotomous scale (yes/no). If a survey respondent had responded in the affirmative to at least one of the two items, then we encoded the usage-oriented behavior as "yes" (implying that the user engaged in usage-oriented behavior). A "no" was encoded for the usage-oriented construct when the response to both items in the Pew survey was in the negative.

4.2.4. Protection-Oriented Behavior

This construct reflects a user's positive defense behavior to protect their privacy from problems such as spam, hacking, and so on. According to Cramer (2004), protection-oriented behavior may be manifested as other mechanisms, such as acting differently than one feels, or to suppress a disturbing idea. In the original Pew survey participants were asked if they "Requested to be removed from a mailing list", "Reported it to your email provider," and "Reported it to a consumer or government agency" after experiencing spam. The user was deemed to have engaged in protection-oriented behavior (active behavior) if the response one or more of the above questions was in the affirmative. The remaining respondents were considered as not

having engaged in protection-oriented behavior. This provided us data for encoding the variable on a dichotomous scale.

Causality among variables and the mediating effect of privacy was established using logistic regression (for more details on the procedure see Baron and Kenny (1986))

5. Analysis and Results

The results and its analysis are presented in this section. The section is subdivided into four following sections: the relationship between a spam experience and privacy concerns, the effect of privacy on defense behaviors (usage-oriented behavior and protection-oriented), the effect of privacy concerns on dual behavior.

5.1. The Relationship between a Spam Experience and Privacy Concerns

First, to test the relationship between spam experience and privacy concerns, we analyzed this relationship in further study. To examine the relationship between a *spam experience* and *privacy concerns*, we conducted a correlation and logistic regression analysis. Table 1 shows the correlation matrix among four variables. The result indicates that a *spam experience* statistically relates to privacy (0.072, $p<0.01$). Moreover, this relationship is also revealed in Table 2. In this study, the results reveal that a *spam experience* has the possibility of alerting the user to *privacy concerns*. That is, the results show that when users have a *spam experience*, the probability that they are concerned about privacy is higher than users who do not have an experience with spam mail. Therefore, Hypothesis 1 is supported.

Table 1. Correlation Matrix

Variables	Spam	Privacy	Usage	Protect

Spam Experience	1			
Privacy	.072**	1		
Usage	.221**	.348**	1	
Protect	-.012	.081**	.174**	1
** Correlation is significant at the 0.01 level (2-tailed).				

Table 2. Result of Logistic Regression

Independent variables	B	S.E.	Wald	*df*	Sig.	Exp(B)
Spam Experience	-.371	.148	6.316	1	.012	.690
Constant	1.223	.069	312.325	1	.000	3.396
Dependent variable: Privacy concerns Model :Chi-square=6.132, $p<0.05$ $df=1$,						

5.2. Effect of Privacy on Two Defense Behaviors

Given the result that a *spam experience* leads users to have *privacy concerns*, we analyzed the effects of each variable based on two behavior strategies. As a first step, we tested Hypothesis 2 as a means to reveal the presence of a relationship between a spam experience and privacy concerns and usage-oriented behavior. Then, we analyzed the relationship between two variables and protection-oriented behavior. Finally, the relationship between the two behaviors was tested.

5.2.1. Effect of privacy concern on usage-oriented behavior

We initially proposed that both the spam experience and privacy concerns would affect usage-oriented behavior in Hypothesis 2. To test *Hypothesis 2*, we used logistic regression analysis for the effect of *privacy concerns* and *spam experience* on usage-oriented behavior in the first step and the mediator role of privacy concern between a *spam experience* and usage-oriented behavior in the second step. *Spam experience* and privacy variables were coded as a dummy variable. The result is presented in Table 3.

Table 3. Testing mediator effects using Logistic Regression						
Testing steps in mediation model	**B**	**S.E.**	**Wald**	**df**	**Sig.**	**Exp(B)**
Testing step 1						
Outcome: Usage behavior						
Predictor: spam experience	-.818	.161	25.753	1	.000	.441
Testing step 2						
Outcome: Privacy						
Predictor: spam experience	-.371	.148	6.316	1	.012	.690
Testing step 3						
Outcome: Usage behavior						
Mediator: Privacy	-2.009	.181	123.276	1	.000	.134
Predictor: spam experience	.763	.172	19.649	1	.000	2.145
Step 3 Model :Chi-square= 185.53, df=2, $p<0.001$.						

When examining the results for step 3 in Table 3, the regression coefficient for *spam experience* was 0.763, which was significant at the conventional probability level ($p<0.001$). The regression coefficient for privacy was -2.009 ($p<0.001$), meaning that there was a significant relationship with usage-oriented behavior in the sample. Thus, the result supports Hypothesis 2 because *usage-oriented behavior* is related to an unconscious, psychologically-based attitude. Users experience this behavior when they have negative feelings about spam. As mentioned before, *usage-oriented behavior* is a strategy which can easily be used to cope with spam or junk email.

In addition, with regard to the mediation effect, we explored whether a *spam experience per se* affects *usage-oriented behavior*. Table 3 contains the analysis necessary to examine this mediation hypothesis. Following the steps outlined earlier for testing mediation, we first established that a *spam experience* is the predictor and is related to *usage-oriented behavior* by conducting a logistic regression for *usage-oriented behavior* on the *spam experience* in Step 1. The regression coefficient (b =-0.818, $p<0.01$) associated with the effect of a *spam experience* on *usage-oriented behavior* was significant. Thus, the effect of spam experience on usage-oriented

behavior is significant and the requirement for mediation in Step 1 is met (Baron & Kenny, 1986).

To examine the relationship between a *spam experience* and *privacy concerns*, we conduct a logistic regression for *privacy concern* on the *spam experience* in Step 2. The regression coefficient (b=0.371, p<0.05) associated with this relation also was significant. To test whether *privacy concern* was related to *usage-oriented behavior*, we conducted a logistic regression for *usage-oriented behavior* simultaneously on both *privacy concern* and the *spam experience* variable in Step 3. The coefficient associated with the relationship between the *privacy concern* and *usage-oriented behavior* was significant (b=-2.009, p< .0001). This third regression equation also provided an estimate of the effect of spam experience on usage-oriented behavior in step 1, the relation between *spam experience* and *usage-oriented behavior*, controlling for *privacy concern*. The effect of spam experience on usage-oriented behavior in step 3 was -0.763 with statistical significance in p< 0.01. Therefore, Hypothesis 2 was supported.

In summary, Table 3 shows that *spam experience* has its own affect on usage-oriented behavior and *privacy concern*s mediates between *spam experience* and usage behavior.

5.2.2. Effect of privacy concern on protection-oriented behavior

To test H2, a logistic regression analysis was conducted. We expected that *spam experience* does not affect protection-oriented behavior. Results from this model are reported in Table 4. Table 4 shows the result of the effect of a *spam experience* on protection-oriented behavior. The model is significant at the p<0.001 level ($\chi 2$=20.739). The result in Table 4 also shows that *spam experience* does not affect protection-oriented behavior (b=0.175, p>0.1). This result may be because protection-oriented behavior is more positive so that users should consciously consider doing this behavior, in contrast to usage behavior.

We also see from Table 4 that *privacy concern*s affect protection-oriented behavior (b=-0.676, p<0.001). Therefore, the results from Table 4 support Hypothesis 3.

Table 4. Logistic Regression

Testing steps in mediation model	B	S.E.	Wald	df	Sig.	Exp(B)
Spam experience (1)	.175	.151	1.331	1	.249	1.191
Privacy (1)	-.676	.158	18.311	1	.000	.509
Constant	-.979	.073	181.728	1	.000	.376

Chi-square= 20.739, *df*=2, *P*<0 .000.
Refernce: privacy =0, no privacy=1; Spam experience =0, no spam experience=1

5.2.3. Effect of Privacy Concern and Dual Behavior

In this study, we assumed that a rational user would engage in only one type of behavior, either usage or protection-oriented behavior. These two behaviors can be substituted for a defensive attack on each other but, under normal circumstances, users seldom engage in two behaviors as an integrated behavior simultaneously. If a user adopts a protection-oriented approach to block spam from their mail account, they would still use email. On the other hand, if the user adopts usage behavior due to spam, they would not experience protective behavior. These are the two approaches a user adopts while dealing with spam. However, if they have *privacy concerns* from spam, they may start using both approaches.

According to the argument mentioned above, we test Hypothesis 4 by examining whether users selected both defensive behaviors when they perceived an impingement on their private information. In doing this, we created a new dependent variable "dual behavior" by combining usage- and protection-oriented behavior in existing data to fit within this analysis as follows. First, the defensive behaviors were integrated into one variable by being recoded as a binary variable (see Figure 3). If a user engaged in either usage or protection-oriented behavior, they would belong to quadrant Q1 or Q3, which in turn would indicate rational behavior. On the other

hand, if the user conducts dual behavior, they would belong to quadrant Q2 (see Figure 3) which in turn would signify dual (both active and passive at the same time) behavior.

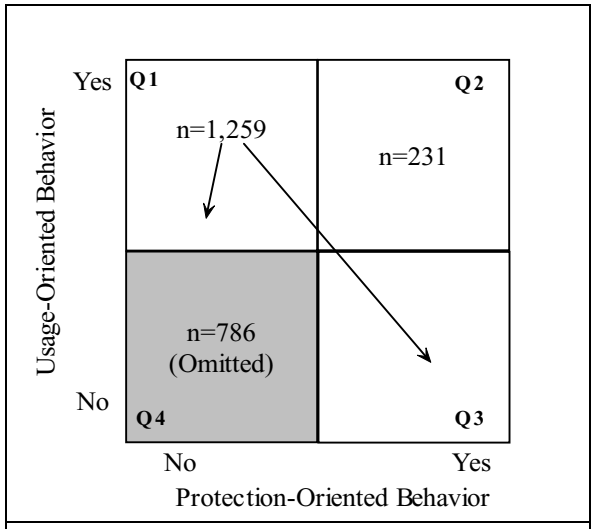


Figure 3: Data Gathering for Dual Behavior

Quadrant Q4 (Figure 3) was omitted in this study because this variable is binary in the analysis. We encode dual behavior as a binary variable. (Users who behave rationally, by either engaging in active (protection-oriented) or passive (usage-oriented) behavior but not both, are encoded with the value 0; and users who engage in both active (protection-oriented) and passive (usage-oriented) behavior at the same time are encoded with the value 1). It may be noted that the new variable (dual behavior) has a statistically different sample from that used for Hypothesis 3.

Using this new variable as a dependent variable, we can find the effects of privacy concerns on the rationality of user behavior. In other words, our hypothesis that privacy can make a user's dual behavior will be supported. We used Equation 1, 2, and 3 for logistic regression.

Step 1: Synchronous Behavior = $\beta_0 + \beta_1 Spam$.....1)

Step 2: Privacy concerns = $\beta_0 + \beta_1 Spam$.....2)

Step 3: Synchronous Behavior = $\beta_0 + \beta_1 Spam + \beta_2 Privacy$.....3)

Results are shown in Table 5. In this Table, for *spam experience* at each step, coefficients are 0.445 ($p< 0.05$), -0.371 ($p< 0.05$), and 0.008 ($p>0.1$) respectively. In addition, *privacy concerns* as mediator was -0.764 ($p<0.01$) in step 3. Results indicate that *privacy concerns* perfectly mediate the relationship between the *spam experience* and combination behavior. In step 3, the effect of *spam experience* on integrated behavior was not significant (b=0.008, $p>0.1$) which means that the effect of a *spam experience* on combination behavior was mediated by *privacy concerns*. In addition, the result of step 3 indicates that *privacy concern* plays a mediating role in the relationship between the *spam experience* and *integrated behavior (b*=-0.764*, p<0.01).*

In sum, users are more likely to conduct both behaviors at the same time when they perceive *privacy concerns* as a result of receiving spam or junk email than when they do not have *privacy concerns*. Although the result shows a low likelihood for conducting both behaviors (*Prob* =18.3%), we can conclude that privacy leads users to enact both behaviors. Therefore, Hypothesis 4 is supported.

Table 5. Testing mediator effects using Logistic Regression

Testing steps in mediation model	B	S.E.	Wald	df	Sig.	Exp(B)
Testing step 1 Outcome: Integrated behavior Predictor: spam experience	.445	.209	4.522	1	.033	1.561
Testing step 2 Outcome: Privacy Predictor: spam experience	-.371	.148	6.316	1	.012	.690
Testing step 3	-.764	.291	6.908	1	.009	.466
Outcome: Integrated behavior	.008	.043	.034	1	.854	1.008

Mediator: Privacy Predictor: spam experience						
Step 3 model: Chi-square= 8.157, *df*=2, *P*<0 .01. Dependent variable: Reference: privacy =0, no privacy=1; Spam experience =0, no spam experience=1						

6. Discussion

In this study, we distinguish between two strategic behaviors that email users can choose to use against spam and junk emails: usage-oriented and protection-oriented behavior. The purpose of this study is to explore mechanisms in relation to how users' experience with spam and *privacy concerns* could function in terms of two behaviors, i.e. the effect of a *spam experience* and privacy. The results revealed several key findings.

Primarily, our results show that a *spam experience* has a relationship with *privacy concerns*. With regard to this relationship, *usage*-oriented *behavior was affected by both *spam experiences* and *privacy concerns*. In addition, privacy has a partly mediating effect on the relationship between a *spam experience* and usage-oriented behavior.

Secondly, for protection-oriented behavior, which was a positive and proactive strategy against spam mail, spam experiences were not significant. However, when users who have such an experience feel that their privacy is being threatened, they adopt protection-oriented behavior.

Thirdly, the effect of a *spam experience* on both behaviors is a result of the mediation effect of *privacy concerns*. Results showed that users' behaviors to protect their mail from junk or spam mails are not because of an experience with spam but instead are due to *privacy concerns*.

We have structured the remainder of this conclusion section into two sub-sections. In the first sub-section we discuss the implication of this research and in the second sub-section we

discuss the limitation of this research. The limitations also represent issues that need further investigation and hence are topics for further research.

6.1. Implications for Research

This study has several implications for research and practice on privacy and spam mail. First and foremost, this study explains the use of defense mechanisms in users' privacy protection behavior. Psychoanalytic theory provides the conceptual framework for understanding unconscious or conscious processes that are simply described as thoughts and desires for the protection of one's privacy. By paying attention to the underlying psychological processes and motives, the current study responds to questions of how email users behave in order to protect their privacy.

Second, this study presents a theoretical initiative for users' behavior with spam and privacy. There has been little research on an email user's behavior for protecting their privacy and preventing spam email. This study explains the role of spam email and *privacy concerns* on users' behavior by using a psychological process.

Third, this study reveals that a *spam experience* has a limited impact on users' protection-oriented behavior. Results show that a *spam experience* might have a significant effect only on passive behavior but not on active behavior. In practice, we assume that a *spam experience* may affect users' behavior, but the preliminary analysis shows that spam has a limited impact on behavior. Privacy has more of an impact on these behaviors by making the users aware of risks from spam.

This study also reveals that an experience with spam has different effects according to users' behaviors. Regardless of the severity of the two behaviors, the *spam experience* affects usage-oriented behavior but does not affect protection-oriented behavior. According to the

characteristics of the two behaviors, a *spam experience* is related to passive behavior, which is easy to choose without any physical efforts. That is, the experience with spam is considered as the factor which brings about *privacy concerns* rather than as a critical factor that causes users to make more efforts to protect their email from spam or privacy attacks.

Finally, this result shows that *privacy concerns* lead users to resort to dual behavior. In practice, the concept of rational action is clearer in the field of economics than in psychology. This clarity is due to the fact that economics views rationality in terms of the choices it produces, whereas psychology views it in terms of the processes it employs (H. A. Simon, 1982; Herbert A. Simon & Thaler, 1986). The two different behaviors (usage-oriented and protection-oriented) are exclusive to each other so that it is enough for users to choose only one behavior to protect their email.

The study shows that privacy is important in explaining users' dual behavior. Although this study does not explicitly reveal that users are dual behavioral decision makers, the study demonstrates why users exhibit both behaviors to prevent spam or junk mails at the same time. If users are more concerned about privacy due to a *spam experience*, the user's behavior is likely to be highly dual behavior. According to the study, dual behavior comes from extreme concerns for protecting private information, whereas *spam experience* is not a determinant which makes users act with dual behavior. However, as users experience more spam they are likely to perceive their private information as vulnerable to attack. Their perception of *privacy concerns* eventually leads them to adopt both approaches.

7. Conclusion

Despite these implications, this study has some limitations. Firstly, although results were statistically significant, this study uses secondary data which was collected by surveys for

general internet use. For this reason, we recoded the data. Secondly, with regard to the secondary data, measuring scales for variables were inconsistent with each other which makes the study's reliability low for a generalization of the results. We cannot say that the analysis is best for measuring dual behavior. This study can be treated as exploratory and as a means to define the need for a future study in this area.

This study sheds light on the effect of *spam experience*, *privacy concerns*, and users' strategies on spam email. The model shows that privacy plays a mediating role in the relationship between the *spam experience* and the users' behavior. Moreover, this study reveals that when users are faced with *privacy concerns*, they demonstrate dual behavior (i.e. both active and passive at the same time). We hope that this study will spur researchers to examine and amplify the potentially influential role of privacy and of users' behavior with in other vulnerable online contexts.

Essay3: Perceived Information Assurance, Risk, Resilience, and Information Systems Effectiveness in the Context of Disasters

1. Introduction

Much of the research on extreme events has focused on the physical, economic, or environmental impacts of mass disasters[24]. Beyond the physical and financial devastation and loss of human life, mass disasters wreak considerable toll on the work life of humans as well (Weems et al. 2007). The toll on worklife may lead to loss of productivity and motivation at a time when, because of the lack of resources experienced during disasters, more is demanded from employees and systems. As a result, employees may come to believe that their organization's information systems cannot effectively support them in accomplishing their tasks during such critical times.

Despite the likelihood of impact on employees, and subsequent impact on organizational performance, resilience (the ability to persevere and thrive despite considerable disadvantages and threats to success) is a characteristic that may have a positive effect on effectiveness. Mallak (1998) argues that resilient organizations have an impact on the resilience of employees. Much of the previous research in resilience has focused mainly on the detrimental physical impact of disaster on critical infrastructure (Barton 2006; Calhoun et al. 2004).

Further, since the risks of business discontinuity increasingly depend on information systems infrastructure (Cerullo et al. 2004), the effectiveness of organizations' information

[24] By disasters, we specifically refer to extreme events. For the purposes of this paper we focus on the Federal Disaster referred to as the October Snow Storm of 2006.

systems should be strongly tied to business continuity (i.e., as the processes that seek to ensure that organizations are capable of withstanding any disruption to normal functioning (Elliott et al. 2002)). The most important aspects of the business continuity plan include protecting organizational assets and restoring critical business functions in order to continue to provision service to members and providers (Devaney 2007).

In the context of hospitals, during a disaster, the ability to keep operating using its information systems is based on its organizational resilience and the ability to identify risks affecting hospital services. In addition, issues critical to maintaining an information system during a disaster relate to threats to cyber-security, which include (but are not limited to) unauthorized access to a system, disruption/denial-of-service, unauthorized use of a system, or unauthorized changes to system hardware or software.

In the case of hospitals, the proper use and functioning of electronic medical records in the provisioning of health is critical: there is dependence on the electronically stored information which needs to be available at all times. Further, patient confidentiality needs to remain upheld at all times. These factors result in an environment that makes perceived risk and resilience critical issues (see, Jensen et al. 2007). Information security and privacy are very important issues in healthcare organizations (Bhatti et al. 2007) and there are several mandates such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules, for the protection of patient data. Therefore, when employees perceive that patient information might be inadvertently vulnerable to compromise or that a system might be disrupted caused by natural disaster, the perception of risk may affect employees' effective use of information systems regarding their works.

The aforementioned issues lead to a reduction in an organization's ability to accomplish its mission effectively (Paton et al. 2000), and also lead to a reduction in resilience. Even though prior research shows that risk and resilience are two interactive factors that have different, overlapping, or common causal mechanisms (Haeffel et al. 2007), it is not clear how perceived risks and resilience operate in conjunction with each other to impact the effectiveness of information systems (IS) in a disaster context. We have yet to understand how the effectiveness of hospital information systems is affected by disasters and extreme events.

In order to bridge this knowledge gap, the current study examines three specific research questions in the context of hospital information systems users: (1) How does perceived risk resulting from extreme events affect the perception of the effectiveness of information systems? (2) How does organizational resilience enhance the perception of individual and organizational performance? and (3) How does a disaster affect the relationships between constructs such as perceived risk, information assurance, organizational resilience, and hospital information systems (HIS) effectiveness? In addition to our main analysis, we also examine the effect of both organizational resilience and information assurance on hospital information systems effectiveness based on the different HIS user groups (i.e. clinical user and administrative user) in a post hoc analysis of the data.

This research attempts to provide a deeper understanding of how perceived information assurance, employees' perceived risk, information assurance, and organizational resilience affect the effectiveness of the information systems in the context of extreme events using data from hospitals. In particular, we argue that perceived risk decreases the information systems effectiveness in the following ways: (a) perceived risks carry negative effects on perceived information assurance and perceived organizational resilience that lead to increase in

effectiveness of information systems that help the organization, and (b) the perceived organizational resilience affected by information assurance perceptions translates mechanism to enact the effective use of information systems. Perceived organizational resilience should act as a viable translating mechanism in this case. Therefore, perceived risk decreases users' attitude toward the information systems by transferring the negative effect of the risk perception to the perceived organizational resilience. The major contribution of this research is that it empirically provides a psychological mechanism on perceived risks, perceived information assurance, and organizational resilience for the usage of information systems under the disaster. According to the information systems literature, such psychological aspects in linking risks and organizational resilience have not been empirically investigated.

This paper is organized as follows. The next section reviews the literature in the area. In the following section, the causal relationships (hypotheses) are examined and explicated. The proposed methodology for the analysis is included in the methods section while results and discussion follow in final section.

2. Background and Literature Review

2.1 Background of Disaster

The ice storm that impacted Buffalo, New York on October 12-13, 2006 has become known as the October Snow Storm. One of the biggest storms in the region's history, the October Snow Storm left behind a legacy of downed trees, lost power, and intense snow and flooding. In the immediate aftermath of the storm, approximately 300,000 residents were without electric power and some residents (100,000) had to endure as many as 10 days without electricity. On Tuesday October 24, 2006, President Bush declared Western New York a major disaster area in the wake

of the off-season snowstorm that decimated and defoliated the area. The Western New York region is well-prepared and well-equipped to effectively deal with typical snow storms and blizzards; there is a well-oiled infrastructure of people, process, and technology in place to respond to snow storms and blizzard. However, the ice and snow storm hit in October which is markedly early for such winter weather; the timing of the storm rendered Buffalo ill-equipped to cope with the October snowstorm. The devastation was extensive and major portions of the region experienced power outages (Waikar et al. 1997). Roads were unusable due to debris and fallen live wires strewn across city streets rendering navigation dangerous if not impossible. Businesses providing survival essentials (e.g. food, gas) were no longer operable not only because of loss of power but also because of travel bans in the area. Several hospitals in the area were affected.

While the influx of patients did not change much (in contrast to other natural disasters), the hospitals had to face severe resource constraints because employees could not drive in and there were no replacements coming in to take over when they were tired. Further, the limited user training of specific parts of the information systems resulted in additional problems because of the mismatch of staff reporting to work and having to perform tasks outside of the realms of normal functions.

2.2 Theoretical Background

Our theoretical framework builds on the information system success model (DeLone and McLean, 1992) and adapts the work of Paton and Johnston on disaster resilience (2001). Our study theorizes that perceived risk affects individual and organizational impact on information systems via organizational resilience and information assurance as well. There is now a growing

body of literature that informs on the importance and impact of perceptual factors as it relates to information systems' effectiveness (W. H. DeLone & McLean, 1992; Rai, Lang, & Welker, 2002). Unlike past research which predominantly focuses on users' perceptions in business context, this study provides insight into employees' perceived risk, organizational resilience, and information assurance - the perceptual factors that are important in a disaster context.
We also theorize that perceived risk and resilience operate in conjunction with each other in impacting information systems effectiveness in a disaster context. This investigation is aligned with work by Paton et al. (2001) who explained how natural hazards affected resilience via perceived risk. Prior research also established a link between employees' perceptions of information assurance and the goals achieved by effectively using information systems (Jean-No Ezingeard, McFadzean, & Birchall, 2005). In this study we propose that information assurance is an important factor that influences information system effectiveness in positive ways.

In the remainder of this section we review literature to develop an understanding of the constructs in the theoretical model. Literature on each of the following constructs is presented: Information Systems Effectiveness, Hospital Information Systems (HIS) Effectiveness (Individual and Organizational impact), Resilience, Perceived Risk (External and Internal), and Information Assurance.

2.3 Information Systems Effectiveness

The concept of information systems success has been widely accepted in IS research as a principal criterion for assessing performance resulting from the usage of information systems (Rai, et al., 2002). Information systems success refers to the extent to which a given information

system actually contributes to achieving organizational goals (i.e., its effect on organizational performance) (Hamilton & Chervany, 1981).

DeLone and McLean (1992) proposed, but did not empirically test, a model of IS success that included six constructs: system quality, information quality, use, user satisfaction, individual impact, and organizational impact (see Figure 1). The DeLone and McLean model for IS success assumes that system quality and information quality affect both user satisfaction and actual use. In addition, it posits that use and user satisfaction are reciprocally interdependent, and presumes these constructs to be direct antecedents of individual impact, which also has an effect on organizational impact.

Although IS researchers have offered a variety of conceptualizations, the core of IS effectiveness remains the degree of organizational goals or performance triggered from the use of an information system (Hamilton & Chervany, 1981; Raymond, 1985). Regarding the measurement of IS effectiveness, it is difficult to identify a precise measure or set of measures of IS effectiveness that is common across all organizations (Thong & Yap, 1996). As Ives et al. [1983] point out, it is difficult to quantify intangible costs and especially the benefits of information systems (Lucas, 1981). Moreover, it is a complex task to objectively assess benefits and information systems for decision support. As a proxy measure, IS effectiveness is easier to operationalize. Therefore, to measure IS effectiveness, IS researchers have used not only diverse constructs, but also multiple measures that they are certain will accurately tap into a given concept (W. H. DeLone & McLean, 1992; Rai, et al., 2002; Seddon, 1997) such as individual impact and organization impact. In addition, because they have been widely accepted as valid and reliable constructs in the IS field for assessing IS effectiveness (See W. H. DeLone & McLean, 1992; Rai, et al., 2002; Thong, Yap, & Raman, 1996), such factors are appropriate to

represent overall IS effectiveness.

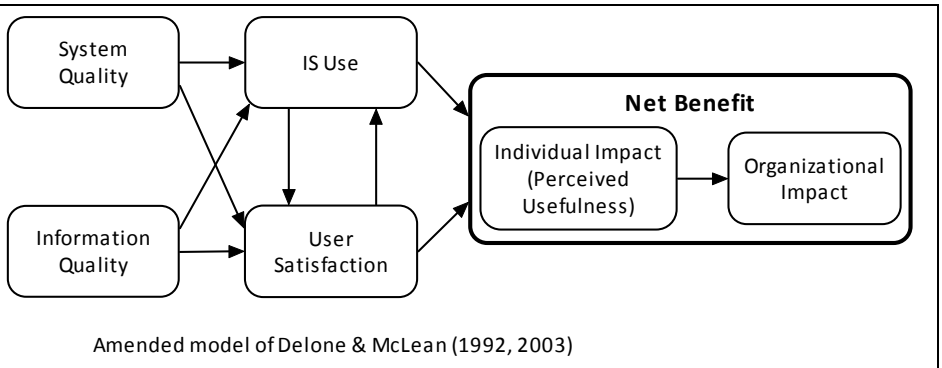


Figure 1. Information Systems Success Model

Information quality refers to measures of IS output—namely, the quality of the information that the system produces (Halawi, McCarthy, & Aronson, 2007). According to Nelson et al. (2005), information quality can be observed either from an intrinsic view, in which the properties of information remain largely isolated from a specific user, task, or application, or from a contextual view, wherein IS output is assessed based on the degree to which it is helpful in completing a particular task. *System quality*, by comparison, refers to measures of the information processing system itself. Past research has shown that elements of system quality often are intermingled with dimensions that are closely related to service quality and ease of use (See Rai, et al., 2002).

Information quality is related most closely to the output of an IS, while system quality reflects the information processing system required to produce that output (Nelson, et al., 2005). Even though two qualities have different dimensions, sometimes confusion arises in differentiating system quality from information quality factors. When considering information and system quality together, it is useful to think of information as the product of a system, and the system as the information processing entity that produces the information (W. H. DeLone &

McLean, 1992). Interaction effects may exist between these two constructs (Nelson, et al., 2005).

According to DeLone and McLean (1992), *individual impact* refers to the positive effect of information on individual behavior. These authors explain that the term "impact" in itself indicates performance or productivity. Several items have been used to evaluate individual impact, such as net benefits, individual job performance, and individual productivity. Seddon (1997) used the label "perceived usefulness" instead of "individual impact." Rai et al. (2002) considered perceived usefulness to be an individual impact because it is based on several of the constructs DeLone and McLean (1992) had linked to individual impacts, such as improved individual productivity. Therefore, consistent with past research (See, Rai, et al., 2002; Sabherwal, Jeyaraj, & Chowa, 2006; Seddon, 1997), this study uses *perceived usefulness* as a construct of individual impact. In line with individual impact, *organizational impact* indicates the effect of information on organizational performance (W. H. DeLone & McLean, 1992; Hamilton & Chervany, 1981).

In this study, the constructs "individual impact" and "organizational impact" are viewed as consequences of information systems usage. This usage reflects both these terms' appropriateness for the study and three additional considerations: What qualifies as a benefit? For whom? And at what level of analysis? (2003p. 22). Specifically, even though DeLone and McLean use the term "net benefit" as the dependent variable, the net benefit concept has not yet been clearly defined so that "collapsing 'individual and organizational impacts' into a single variable, net benefit, does not make the problem go away" (2003, p.23). In addition, DeLone and McLean mentioned that net benefit is not a different concept from the "two impacts," but simply a more parsimonious one.

2.4 Hospital Information Systems (HIS) Effectiveness

A hospital information system defines the socio-technical subsystem of a hospital, which comprises all information processing, as well as the associated human or technical actors in their respective information processing roles (Haux et al. 2004). HIS allows for timely patient health information to those making health related decisions (Katehakis et al. 2002), in addition to facilitating the billing and administrative aspects in a hospital. Users of patient health information include physicians, nurses, lab technicians, administrators such as those involved with billing, records management, etc.

Several studies have attempted to account for effectiveness from a perception perspective, given that attitudes are often affected and behaviors motivated by perceptions. Henry and Stone (1999) examined computer self-efficacy and outcome expectancy with hospital staff members using computer-based medical information systems and concluded that management support, ease-of-use, and computer self-efficacy had a positive influence on satisfaction.

Understanding the role of perception in employees' interactions with HIS, it is important to identify both individual and internal organizational factors that have potential to affect an individuals' perceptions and attitudes, and behaviors as they attempt to most effectively use the information system. Anderson (1997) declares that, in relation to hospital information systems, several decades of experience with computer-based information systems have made it clear that the critical issues in the implementation of these systems are social and organizational, not solely technical. Likewise, since some degree of IS effectiveness is dependent on the users and on organizational factors, this paper argues that such factors may directly and/or indirectly affect hospital information system effectiveness.

In estimating the effectiveness of hospital information systems, at the outset, we consider organizational resilience and perceived risk as factors that affect a part of hospitals' business continuity in a disaster context. Specifically, we explore the mechanism by which perceived risk and resilience facilitates (or obstructs) the impact of information systems on individual or organizational performance as an important part of business continuity. Secondly, perceived information assurance—the degree to which employees perceive that information security and privacy are assured—is proposed to have an effect on information systems effectiveness as articulated below. Sharing or using sensitive patient information in a large, distributed and heterogeneous hospital could bring out security and privacy risks (Braghin et al. 2008) which might be compromised or threatened by attackers. These risks can lead users to carefully consider the system vulnerability in terms of security and privacy as important determinant for information systems effectiveness. It is recognized that security and privacy concerns are critical obstacles in enhancing hospital's improvement of hospital information systems (Goldman 1998), even in a disaster context. Existing regulations, such as HIPAA, regarding health care information shows the important example in terms of security and privacy for patients' records. Given these factors, the present study focuses primarily on the effect of perceived risk, resilience, and information assurance on HIS effectiveness. This will allow us to have a better understanding about the internal driving-forces for IS effectiveness in hospitals.

It is important to note that while we treat *hospital information systems* as an entity, the reality in most hospitals is that there is an administrative and billing system that is distinct from

the electronic health record system (Reddy et al. 2008). Thus, the users of the systems can be viewed as either dealing with support (including administrative functions) or medical and health functions (for the purposes of the discussion in this manuscript we henceforth refer to them as 'medical users'). In addition to considering the hospital information systems as a single entity, we also include analysis that presents perspectives based on usage (support and medical) by way of sub-group analysis.

2.5 Resilience

The term, 'resilience' has been widely used in various fields including ecology, psychology, economics, business, and applied critical infrastructure. Consequently, diverse definitions garnish the literature determined by the research field of context. For instance, psychological resilience is viewed as a relatively stable personality trait characterized by the ability to bounce back from negative experiences and by flexible adaptation to the ever-changing demands of life (Block et al. 1996). It is also used to indicate a characteristic of resistance to future negative events.

In disaster contexts, resilience refers to the capacity of an entity or system to maintain and renew itself particularly in the presence of stressors, or the ability or capacity of a system to absorb or cushion against damage or loss (Rose 2004). In this case, resilience indicates the overall capability of an organization as a whole to respond to external catastrophes for business continuity. The concept of resilience is therefore associated with reduced failure probability, reduced consequences from failure, and reduced time to recovery as suggested by Bruneau et al. (2003).

Past research on *resilience* has been extended to various topics such as business coping behavior and community response (Tierney 1997), nonlinear adaptive response of organizations (Comfort 1999), and systems performance (Petak 2002). However, the concept of organizational resilience still receives little attention in the IS arena.

Resilient organizations have the ability to "maintain positive adjustment under challenging conditions" (Sutcliffe et al. 2003, p. 95). In the face of disaster circumstances, a resilient organization is able to make better sense of what is happening, to take more effective action based on the sense that has been made, and is better able to manage threats as they unfold (Bigley et al. 2001). O'Rourke et al. (2003) found in their study, New York City was able to recover relatively quickly after September 11 not only because of the inherent redundancy of its physical infrastructures but also because of its institutional resilience.

In the context of environments experiencing disaster, resilience extends to organizational success in post-disaster environments. Resilience in post-disaster conditions is distinguished from pre-disaster activities that reduce potential losses through mitigation, The construct of resilience must capture the ability of a system to respond and recover from an extreme incident (Dalziell et al. 2004). In this sense, resilience is not a static attribute that organizations do or do not possess but rather results from processes that help organizations retain their resources in a form sufficiently flexible, storable, convertible, and malleable to avert maladaptive tendencies and cope positively with the unexpected (Sutcliffe et al. 2003). This capability is important both to organizations that deal with critical uncertainty on a regular basis, and to individuals for whom crisis is an unfamiliar yet potentially very real circumstance (Barton et al. 2006).

2.6 Perceived Risk

Risk perceptions is defined as a decision maker's assessment of the risk inherent in a situation (Sitkin et al. 1992). Research has long addressed how people perceive risk and how their decisions are affected by their the perceptions (Slovic et al. 1981). Perceived risk is believed to be a crucial factor in shaping policy, attitudes, and decisions (Sjöberg 2004). In general, the concept of perceived risk is based on heuristics, which are often employed to reduce difficult mental tasks to simpler ones. When asked to evaluate risks, people make inferences based on what they remember hearing or observing about the risk in question using a number of general inferential rules. According to Slovic et al. (1981), people seldom have statistical evidence about the impacts of risk, on hand. Thus, perceived risk refers to a collection of notions that people form, based on risk sources relative to the information available to them, and on common sense (Jaeger et al. 2002). This type of intuitive risk perception is predicated on how the information about the source of a risk is communicated, the psychological mechanisms for processing uncertainty, and earlier experiences of danger. Persons' perceived risk is considered central to their evaluations, choices, and behaviors (e.g., Dowling 1999). The way an individual perceives risk depends on how he or she defines and values the outcome. Individuals perceive risk in relation to their wider beliefs about the risk issues and the more general implications that these have on their lives. For instance, beliefs about a risk issue may include both immediate and far-reaching consequences of accepting or not accepting the risk (Thomas et al. 1981). Researchers have also found perceived risk to be a consequence of higher levels of uncertainty (Mukhopadhyay et al. 2009; Oglethorpe et al. 1987). When people perceive risks, there is an expectation of some loss. It is also important to note that employees' perceived risk is negatively

correlated with intentions and behavior (Stone et al. 1987). In this paper, we study how perceived risks affect hospital information system effectiveness.

Perceived risk in this regard are assessment of the risk inherent stemming as a consequence of risks of disruptions among interrelated external infrastructures (external risk) and disruptions of their information systems (internal risk) in disaster situations.

External risk (ER) is caused by vulnerabilities resulting from interdependencies due to linkages of physical infrastructure with information systems, and external disruptions such as physical disruptions that affect an organization. For example, disruption of the civil transportation infrastructure may cause unavoidable absenteeism; appropriate personnel may be unavailable to operate the information system, thus preventing access to pertinent medical information as a consequence of the disaster (as was the case in the October Storm). When employees believe that infrastructures might physically affect their organization and respective information systems, they intuitively evaluate this risk source based on their subjective perception (Chen et al. 2010).

Internal risk (IR) can be induced by the negative feelings relating to the effect of organizational disruption stemming from information systems related activity or lack thereof. The potential ineffectiveness of IS on provisioning of patient care can result not only because of the technology and its governance, but also from the actions of other infrastructures such as human resource, for example. Consider two infrastructures in an organization: information systems and the medical facility. Each infrastructure faces a certain risk of disruption that could render it non-functional to its primary clients (internal effect) and affecting other dependent infrastructures (external effect). Therefore, perceived risks caused by the internal infrastructure in an organization can have a debilitating impact on the organization's performance (which, is

largely based on the infrastructure). These negative externalities are an important feature of perceived risks (Heal et al. 2006).

2.7 Information Assurance

Ezingeard et al. (2007) describes information assurance as the certainty that the information within an organization is reliable, secure, private, accurate and available. They suggest that information assurance typically defines how these assets (i.e., data and/or information within both the tangible and the virtual bounds of the organization) should be secured to provide maximum benefit. The term, 'information assurance' is growing in acceptance and usage amongst a number of government and international agencies (Wolf 2003).

Information assurance deals with protecting and defending information and information systems by ensuring their availability, integrity, confidentiality, identification and authentication, and non-repudiation (DoD 1998). Information assurance subsumes information security which focuses on the need to protect systems from internal and external attack, environmental threats and accidental damage (Whitman 2004). Information assurance provides a view of information protection that includes defensive measures in all three states of processing, storage, and transmission (Schou et al. 2004). This embodies providing for the restoration of information systems by incorporating protection, detection, and reaction capabilities. It is these capabilities that produce the kind of defense required to comply with legislation such as FERPA and HIPAA.

In this study, we refer to information assurance as the degree to which employees perceive that their information security and privacy is assured. Based on this characterization, this study examines how hospital information systems effectiveness is affected by information assurance, organizational resilience and perceived internal and external risks.

3. Hypothesis Development

3.1 The Effect of Perceived Risk

In a disaster context, people may perceive risk in terms of the disaster itself, the information systems disruptions caused by disasters, or the inter-organizational factors that may affect their activities. Specifically, as the interdependence of infrastructures increases, there is a growing risk that restoration efforts or uncertainties experienced by one sector could adversely affect the operations or restoration efforts of another, thereby contributing to further service disruptions (Saxton 2002). Hospital Information Systems typically encompass several components such as platforms, applications, technologies, and people (both IT support staff and IT users). In a health care organization, the more the employees (both clinical and administrative) perceive external risk caused by a disaster, the more they perceive internal risk about the availability of Electronic Medical Resources, nurse scheduling data, and of information assurance (especially because of the potential misuse of personal health information (PHI) data). For example, the storm of October 12-13, 2006 in the Buffalo area affected stakeholders both physically and mentally and caused a concern that the hospital information systems would not be efficient and effective. This leads to our first set of hypotheses in the context of hospital information systems:

H1a: perception of external risk will positively affect perception of internal risk.

H1b: perception of external risk will negatively affect perception of information assurance.

H2a: perception of internal risk will negatively affect perceived information assurance

Existing literature on risk perception also finds that, perceived risk is negatively associated with perceived ability to combat the threat (Rimal 2001). Other related research shows

the negative relationship between consumer self-efficacy and perceived risk in the e-commerce context of online customers (Dash et al. 2007). People with high-risk perception perceive themselves as not being able to achieve their goals or overcome the situation. Perceived risk also motivates people to evaluate the level of their ability to cope in a given situation. Likewise, this relationship between perceived individual ability and perceived risk can also be viewed from an organizational resilience perspective. The belief is that employees' perception about organizational resilience would diminish depending upon the degree of their perception of internal risk. Internal risks in organizations cause people to worry about their organizational infrastructures (e.g., hospital information systems in this case) as not being operated well or having the ability to cope with negative extreme events (Chen et al. 2008a). Eventually, the more risk employees perceive, the less likely they are to have a positive perception of their organization's resilience. Our next hypothesis is formulated as follows:

H2b: perception of internal risk will negatively affect perceived organizational resilience.

Prior research shows a negative relationship between IT risks and IT project success (Jiang et al. 2001). According to Jiang et al. (2001), behavioral and technology-related risks can negatively affect information systems' success either directly or indirectly. The research suggests that as perceived risk increases, people engage in different types of risk-reduction activities, such as the careful evaluation of alternatives, functionality or organization performance (See, Dowling et al. 1994). In a disaster context, hospital employees who perceive high risk are likely to engage in a conservative evaluation of their individual and organizational performances and, in turn, internal risk will reduce the hospital information systems effectiveness. Proposed hypotheses regarding the relationship between interdependency risks and the hospital information systems effectiveness read as follows:

H2c: perception of internal risk will negatively affect organizational impact.

H2d: perception of internal risk will negatively affect individual impact.

3.2 The Effect of Information Assurance

Information Systems are vulnerable for a wide variety of reasons. Hospital Information Systems are no exception, regardless of the fact that they have to be HIPAA compliant. A fundamental cause of many of the risks derives as a consequence of the variety of ways that individuals and/or groups can utilize digital technologies to engage in mistaken, inappropriate, criminal or other illegal online activities (Vlasti et al. 2004). Security breaches elevate one's awareness of the price for failing to safeguard information systems in terms of reputation damage, loss of business, and valuation loss on stock markets (Dhillon et al. 2001; Ettredge et al. 2002). In the context of hospitals, this awareness is amplified because of the impact on the provisioning of care and the sensitivity of protected health information (PHI) related data. Past research provides some testimony that there is a relationship between organizations' information assurance and their performance, such as reducing stock price (Campbell et al. 2003; Ettredge et al. 2003), prohibitively high cost of a security breach (Sauer et al. 1997), and the effect of poor information assurance compliance on privacy and data protection (Culnan et al. 1999).

Alternatively, information assurance can create positive organizational benefits (Ezingeard et al., (2005). For example, information assurance impacts the organization's ability to deliver goods and services more effectively and also facilitates improvement in the quality, integrity, and availability of information. Past research suggests a link between employees' perceptions of information assurance and goal achievement through effective use of information

systems. That is, the more people perceive an organization's information systems as highly assured, the greater the degree to which employees use the information systems effectively.

In addition, employees who perceive that information assurance is high are more likely to believe that their organization is resilient and become more committed to the organization and their job with the organization. Eventually, the perception of high information assurance will motivate employees to increase their attitude toward using information systems despite problems thus improving organizational resilience. Thus, this study offers the following hypotheses in the context of a hospital environment:

H3a: perceived information assurance will positively affect perceived organizational resilience.

H3b: perceived information assurance will positively affect organization impact.

H3c: perceived information assurance will positively affect individual impact.

3.3 The Effect of Organizational Resilience

At the individual level, employees' perceived organizational resilience is defined as the belief that an organization has a relatively stable trait characterized by the ability to bounce back from negative experiences and by flexible adaptation to the emergency context.

This study posits that, if employees believe that their organization is resilient enough to handle unexpected events, they will effectively use their systems regardless of the disaster and eventually their belief encourages them to enhance their work performance. Ezingeard et al. (2007) argued that resilience enables more consistent operational performance which, in turn, reduces costs and increases the ability to adapt quickly to changing external circumstances. Since organizational resilience becomes a motivational factor that directly mobilizes employees' behaviors, organizational resilience affects individual performance using information systems by

helping people to create feelings of confidence in approaching difficult tasks and activities. Thus, individuals with a high perception of organizational resilience show a positive view of their organization, a sense of control over the organization, and an optimistic outlook on the future—all resources should contribute to better adjustment to a disaster context. Specifically, given the external attribution of negative events described by Seligman (1998), when faced with negative outcomes, optimistic employees will likely attribute the failure to external causes, avoiding any sense of blame that may lead to deviant behavior. The lack of positive belief about an organization's resilience tends to discourage employees, resulting in lower levels of performance on the job and the possibility of being less effective. Based on this reasoning, we hypothesize that organizational resilience is positively related to hospital information systems effectiveness:

H4a: perceived organizational resilience will positively affect organizational impact.

H4b: perceived organizational resilience will positively affect individual impact.

Figure 1 captures the combined theoretical model and hypothesized relationships of this study which we develop. We discuss H5 in the next subsection.

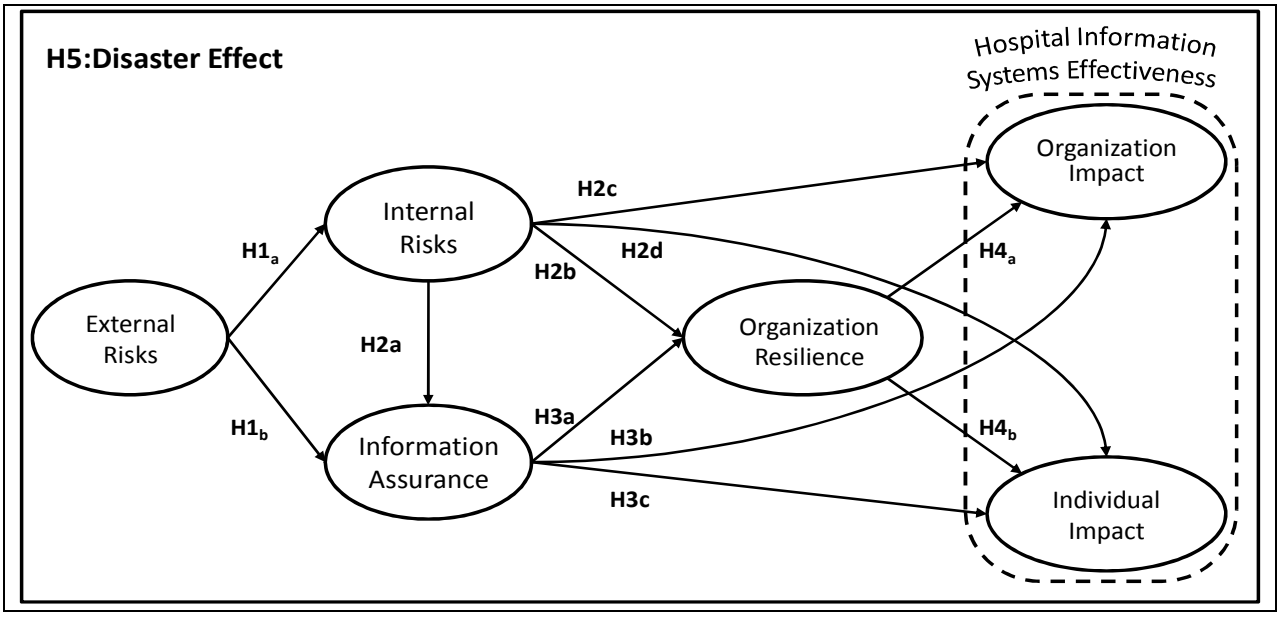


Figure 2. The Theoretical Model

3.4 The Effect of Disasters

People construct their own reality and evaluate risks according to their subjective perceptions. According to the availability heuristic, a cognitive strategy in which people rely upon knowledge that is readily available rather than examine other alternatives or procedures (Tversky & Kahneman, 1982), people use the ease with which examples of a disaster can be recollected as a cue for estimating the probability of a hazard. As a result, experiences with a disaster should change the relationship between perceived risks, organizational resilience, and information assurance and information systems effectiveness from one before a disaster experience. We argue that an employee's evaluation process appears differently depending on the experience of disasters.

Prior studies show that past experience with disasters is an important factor in influencing people's perceptions of hazards (See, Jackson, 1981). Specifically, Jackson (1981) found that experience after damaging earthquakes influenced the adoption of more frequent precautions. Stakeholders, therefore, would consider perceived risks, organizational resilience, and information assurance to make sure that their information systems work well in the disaster context. That is, these perceptions cause employees to become relatively more concerned that their information systems will not properly function and prevent them from completing the tasks that need to be discharged in a disaster context. This impedes employees from evaluating the effects of information assurance, organizational resilience, and perceived risks on information systems in a distinct way. It also deflates employees' confidence in the effectiveness of

information systems with high-risk perception. Ultimately, employees will lean on their perception of risks and information assurance in gauging the hospital information system's effectiveness. Therefore, hypothesis 5a is:

H5a: The relationship between perceived risk and organizational impact will be stronger in the context of a disaster than outside of it.

H5b: The relationship between perceived risk and individual impact will be stronger in the context of a disaster than outside of it.

Paton et al. (2000) showed the relationship between disasters and resilience by exploring the effect of disaster experience on resilience. When employees experience a disaster, they elaborate whether their organization maintains business continuity (Waikar & Nichols, 1997). If employees conclude that their organization is resilient to operate well despite the disaster, compared to a pre-disaster context, these employees will focus more on their business continuity issues and are likely to have positive perceptions of their organizational ability to overcome disaster (Shen & Shaw, 2005). Hence, employees' perceptions based on organization's capability to secure information systems will help employees execute their charge in a better manner.

Personal and organizational responses related to a disaster effect are predicated on consistent findings from protection motivation theory (Rogers, 1975). According to the theory, people can be motivated to engage in desirable behaviors to avoid risks or fears from disasters. That is, when an individual faces a threat, he/she appraises the information available about the perceived severity of the threat and the perceived probability that the threat will occur. e/she

conducts the processes in selecting the perceived ability of a coping behavior to remove the threat and the individual's perceived ability to carry out the coping behavior (Rogers 1983).

In the case of a disaster in an organizational context such as a hospital, the likelihood of employees undertaking psychological threat reduction behaviors can be increased by (1) the belief that their organization can still be secure in protecting their information systems from the disaster (i.e., information assurance), and (2) the belief that the organization would be able to mitigate the effect of the disaster (i.e., organizational resilience). This belief in the resilience of the organization leads the employees to avoid or reduce the psychological impact of the disaster. Employees who have experienced disasters would potentially exhibit greater levels of perceived organizational resilience in comparison to outside of the context of the disaster. This leads to the following hypotheses:

H6a: The relationship between perceived organizational resilience and organizational impact will be stronger in the context of a disaster than otherwise.

H6b: The relationship between perceived organizational resilience and individual impact will be stronger in the context of a disaster than otherwise.

H7a: The relationship between perceived information assurance and organizational impact will be stronger in the context of a disaster than otherwise.

H7b: The relationship between perceived information assurance and individual impact will be stronger in the context of a disaster than otherwise.

Figure 2 shows the aforementioned arguments regarding the effect of a disaster.

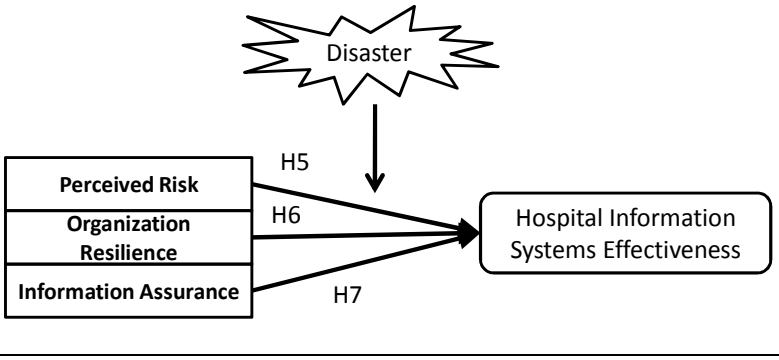


Figure 3. The Effect of a Disaster

4. Methods

4.1 Research Context

This study examines the work-life factors affecting users of hospital information systems (HIS) rather than the technological factors such as information, systems, and service quality as is typically the case. Determining the extent to which a disaster changes the effect of work-life factors on HIS is performed by comparing the effectiveness of the systems before and after a disaster. In order to conduct this study, three hospitals affected by the debilitating October Snow storm of 2006 from the Western New York were selected. These three hospitals have similar hospital information system in terms of the basic functions performed. In addition, even though the three hospitals are different in size and type, the underlying security and privacy issues in using the HIS are similar. The hospitals are mandated to securely store health and administrative information in their HIS. Clinical hospital information systems provide online access to databases containing patients' medical information for authorized main users (such as nurses, physicians, therapists, and lab technicians) to use in highly restricted ways. The system usage is predominantly dictated at the transaction level by the number of patients and the medical

procedures performed on them. This was not affected and therefore, system usage did not change during the storm because the patient inflow did not change.

4.2 Item Development and Pilot Test

While several items for constructs (i.e., organization and individual impact) were operationalized based on prior research, scale items for *perceived risks*, *information assurance,* and *organizational resilience* were newly developed in this study. At the outset, we developed an initial survey based on the literature. We interviewed IT executives from hospitals in the Buffalo area (including the Deputy Commissioner of Emergency Management at the county level, CIO and CSOs of the local hospitals, as well as the Director of Medical Emergency Services) in order to understand how stakeholders perceived their (organizational) ability to recover from disasters and factors that affects their risks and resilience. Since participants' perceptions on those factors defer depending upon the usage of HIS, this study tried to include their various viewpoints by encouraging stakeholders to participate in this survey. This allowed us to deal with face validity for the construct components. Such an approach is consistent with Rousseau's original conceptualization (1989) of psychological contracts.

A pilot study with 50 employees from one of three hospitals was conducted to validate the survey instrument and establish that the survey items portrayed their intended meaning. Feedback was also sought on the survey's length, its overall appearance, and participants' expected reaction to its receipt in the mail. Comments and suggestions from interviewees were used to revise the survey.

4.3 Participants

A quasi-experimental field research, specifically a one-group pretest-posttest design (Cook et al. 1975) using surveys was conducted at three of the hospitals in the Buffalo area that were affected by a disaster referred to as the *October snow storm* of October, 2006. This quasi-experimental design was chosen to meet the criteria that the research should be based on the actual impact of disaster. Two hundred and fifty questionnaires were composed of repeated-measure items and were distributed to the hospital employees. One hundred and eleven completed questionnaires were returned. These included hospital administrators, nurses, physicians, IT support staff, laboratory technicians, etc. These surveys included a treatment design with pretest, treatment presentation, and posttests. Of these, after removing surveys that had relatively high amounts of missing responses and/or surveys in which the same value was circled consecutively for every question, 104 surveys were considered usable, an effective response rate of 40.1%. The sample was relatively small because all participants selected in this experiment were filtered at first step of experimental procedure that will be mentioned below. Since the employees' disaster experience determines the success of the fundamental of this study, had to elaborately collect participants that made sample size small. Table 1 presents descriptive statistics relating to the responses.

Table 1. Descriptive Statistics (N = 104)

Contents		Mean	S.D.	
Total Years of Working		17.4	10.5	
Organization Tenure		11.99	10.23	
Year Using MIS		7.1	7.8	
Profession		Frequency	Sub-totals	
Main user group	M.D. Nurse Therapist	5 39 2	46	44.2%

Support user group	IT Technologist Administrator	25 33	58	55.8%

4.4 Procedure

The users for hospital information systems can be categorized into two types of users: main users (i.e., physicians and nurses) vs. support users (i.e., hospital and IT supporters) depending on their usage of either clinical or administrative and support components of the system. There was no control group in this study. In order to identify the impact of disaster on the relationships among factors in our proposed model, we administered a treatment to the survey participants to facilitate the recall of their experiences during the October storm. The survey questionnaire consisted of three steps. First, participants were asked whether they worked in hospitals when the October storm was brought out. This question was intended to screen right subjects who meet our experiment. Since this study was mainly rely on their experience in terms of disaster and information systems in their organizations, subjects should have experience on working under the disaster context. In conducting a quasi-experimental design, our study was strictly applied to collect sample. This procedure allows us to achieve better research outcome in terms of the purposes of this study. Therefore, this should not be a limitation on this study, although the study was performed with a small sample size,

Second, participants were asked to answer the questions for all constructs without any cue regarding disasters. Second, a picture and news article along with five probing questions to serve as stimulus were presented to the same participants, to facilitate the recall of their experiences of the October storm. Third, after providing the treatment, the participants also were asked to answer the exact same questions. Since participants lived in the Buffalo area, they knew how the storm affected their everyday lives.

Stimulus Message*:* The experiment required each participant to read an enclosed news article (Figure 3) and a set of questions that was part of the survey. The message along with a picture (see Figure 3) was part of *news article from New York Times* story about the October storm. This news article was intended to recall only what happened at Buffalo area with the *October storm.* Thus, employees should clearly draw the memory about how the city was under the disaster. In addition, this message should not recollect employees' memory related to them or their organizations including organizations' information systems, their performance, or perceptions on information systems. Therefore, we believe that the message as a stimulus is not only simple and clear for the goal of the purpose of this study but this also would prevent employees from being directly affected by the message on two factors measuring IS effectiveness.

Stimulus Check: After the disaster recall stimulus, participants were asked to respond to two *stimulus check* questions: "Did the news article help in recalling details about the storm?" and "how much do you remember about the October storm in 2006?" The response for the second question was elicited as a score on a 7-point Likert scale (1 = strongly disagree to 7= strongly agree) and similarly to first question (1= very clearly to 7= no recollection of the event).

Cost of Buffalo Storm Cleanup May Top $30 Million

Electrical service workers in Buffalo, N.Y., on October 17, 2006.
Mike Groll for The New York Times

BUFFALO, Oct. 18 — More than 100,000 homes and businesses remained without power here on Wednesday, nearly a week after a preseason snowstorm dumped almost two feet of snow and wreaked havoc on trees and power lines. (By David Staba, Published: October 19, 2006)

Figure 4. Disaster Recall Stimulus

4.5 Measures

Information Systems Effectiveness: We used two factors to identify the impact of the disaster on information systems effectiveness in a hospital: Individual Impact and Organizational Impact concepts (both derived from DeLone and McLean (1992)). For the 'individual impact factor', we adapted and modified three items developed by DeLone and McLean (1992). We considered various aspects of an individual's job related to their performance based on HIS. Employees in hospitals use HIS for their hospital related work in the provisioning of patient care. The sample list of items included are "The hospital information systems helps me meet patient needs effectively," "The hospital information systems increases my productivity," and "The hospital information systems saves my time." The second measure of IS effectiveness, Organizational Impact, is a perceptual measure of the impact of an information system on the performance of the business. The underlying assumption is that an

information system is effective when it contributes to organizational effectiveness. DeLone and McLean (1992) suggest that organizational impact may be measured in terms of profit, sales revenue, staff productivity, competitive advantage, operations efficiency, and improved decision-making (Thong et al. 1996b). Five items from Thong et al (1996b) were used to measure *organizational impact* in this study. The sample list of items included are "the hospital information systems increase the effectiveness of our hospital's operations and provide us with information to effectively manage medical supplies" and "the hospital information systems provides us with information to effectively manage medical supplies." Measure items for both individual and organizational impacts are detailed as part of the appendix.

Organizational Resilience: This is a new construct defined for the purposes of this study as the ability and capacity to withstand systemic discontinuities and adapt to it (Starr, Newfrock, & Delurey, 2003), as another dimension of information systems effectiveness. This construct was measured using four items. Sample items are: "Our organization has business continuity plans to handle unfamiliar situations" and "Our information systems recover quickly after critical incidents." Respondents were asked to indicate their perception of the degree to which the organization's information systems contributed to the organization's impact in terms of staff productivity, operations efficiency, and improved decision-making using a 7-point Likert scale of agreement.

Perceived Risks: We developed two dependency risk constructs: (a) an external risk construct measured using eight items and (b) an internal risk construct measured using three items. Sample items for external risk include: "Our hospital information systems might not operate, when the electric power system is disrupted", "Our hospital information systems might not operate, when the gas and oil storage system is disrupted" etc. Sample item for internal risk

were: “When network facilities (e.g., network/cable plant) are disrupted the medical information systems are affected.”

Information Assurance: Five items were used as a measure for the construct, perceived information assurance defined for the purposes of this study as the degree of perceived availability, confidentiality, and integrity of information systems. Those items were designed to cover both clinical and general (i.e., non clinical) information systems aspects. Items included were: “Medical information systems are accessible only to those authorized to have access” and “Our primary database system (i.e., medical records) is stable and safe against tampering.”

Control Variable: The subjects of the survey were employees in three hospitals in the Buffalo area that were affected by the October Snow Storm. In order to find whether there were effects across organizations, organization was controlled. The three hospitals, from which data was collected for this study, are different in size and type. However they have similar hospital information system in terms of the basic functions they perform. To control for a possible organization type effect, we used categorical variables to assess consistency of results.

4.6 Common Method Bias and Organizational Scale for Organization Level

In order to address common method bias in our measures, we employed two statistical and procedural methodologies recommended by Podsakoff et al. (2003) using Harman’s single factor test. According to the Harman’s test, common method bias is an issue if results from an exploratory factor analysis reveal that (1) a single factor emerges or (2) the first factor accounts for the majority of the covariance among the variables. Results from the Harman test suggested that common method bias was not a serious issue among these variables as more than one factor emerged from the un-rotated solution. All indicators showed high factor loadings and low cross-

loadings. Each principal component explained almost an equal amount of the 74% total variance, ranging from 3.98% to 30.46%. This indicates that our data do not suffer from common method bias. The first factor accounted for only 30.46% of the variance and the second factor accounted for 14.16%.

In order to further address method bias, another procedural remedy was introduced in the measurement of the variables as suggested by Podsakoff et al. (2003). First, as noted above, we reduced evaluation apprehension by providing respondents with verbal and written assurances of confidentiality by assuring them that there was no right or wrong answers, and requesting that they answer each question as honestly as possible. The latter procedures are known to reduce the likelihood of bias caused by social desirability or respondent acquiescence

Employees provided ratings of both individual and organizational impact of the hospital's information systems. Since the construct 'organization impact' is used as an organizational unit of analysis, there is the potential for common-method variance to inflate the associations between individual and organization impacts evaluated by the same employees. In order to ensure whether both concepts are the same unit of analysis, two tests were performed. First, we conducted *within-group agreement (inter-rater reliability; R_{wg}[25]) indexes*[26] (James et al. 1984) for the organizational impact scale. The r_{wg} value has been employed to justify the appropriateness of aggregating data to higher levels of analysis. For this analysis, all employees of three hospitals were included. Results showed that within-group variances are not

---

[25] $R_{WG(J)}$ = {J[1- (mean of S_x^2 / σ_E^2)]} / {J[1- (mean of S_x^2 / σ_E^2)] + mean of S_x^2 / σ_E^2}, where J is the number of items rated, mean of S_x^2 is the observed item-wise variance across individuals, averaged over items, and σ_E^2 is the expected variance.

[26] An index of the observed variance divided by the expected variance due to random measurement errors, and indicates the extent of within-group agreement as opposed to reliability (Kozlowski et al. 1992). This reflects the perceptual congruence of a group of individuals who are assessing the same behavioral characteristic with respect to the target manager.

homogenous (R_{wg}= 0.35), which indicates that the concept of organization impact should not be aggregated to a higher level. Second, we used a Levene test for equality of variances (Levene 1960) that indicates homogeneity of group variance to compare organizations. Results of this test were consistent with R_{wg} analysis, showing that within-group variances are not homogenous (F= 5.100, $p < 0.05$). In sum, both analyses suggested that the concept, 'organization impact' in this study should be conceptualized at the individual-level. Based on the preceding results, the statistical analyses for hypotheses testing in relation to organization impact were conducted with 104 individuals.

4.7 Data Analyses

Partial Least Squares (PLS), as implemented in PLS Graph version 3.0, was used for data analysis. The PLS approach allows researchers to assess measurement model parameters and structural path coefficients simultaneously (Barclay, Higgins, & Thompson, 1995). It focuses on a prediction-oriented and data-analytic method, seeking to maximize the variances that are explained in constructs (Barclay, et al., 1995). Several reasons motivate our using PLS in this study. First, this study was primarily intended for causal-predictive analysis, a condition for PLS suggested by Chin and Newsted (1999). Second, PLS requires fewer statistical specifications and constraints on the data than the covariance-based strategy of LISREL (e.g., assumptions of normality). Further, PLS was suitable for this study due to the small sample (N=104). Specifically, researchers often argue that PLS only requires a sample size of 10 times the most complex relationships within the research model (Barclay, et al., 1995). Third, PLS is effective for those early-theory testing situations that characterize this study.

Before testing the hypotheses in this study, preliminary analysis examined availability of pooled sample, and construct validity. Since the sample along user-type lines yielded a main (clinical) user group with 46 cases and a support user (administrative) group with 58 cases, the pooled data should be available to test hypothesis regardless of user-type. Table 2 reports the means and standard deviations for the subgroups and the results of Kolmogorov-Smirnov (K-S) tests for differences across the subgroups and the Levene's test for homoscedasticity with SPSS. Both K-S test and Levene's test show that there is no violation of the assumption that the two groups have approximately equal variance on the dependent variable (see Table 2).

Table 2. Construct Characteristics and K-S Test Results by Subgroup

Constructs	Main user group		Support user group		Levene's Test for Equality of Variances		Kolmogorov-Smirnov Test	
	Mean	Std. Dev.	Mean	Std. Dev.	F-Score	Sig.	Z- Score	Sig.
IM_M	4.61	1.48	4.88	1.75	1.81	0.18	0.991	0.279
OM_M	4.13	1.57	4.33	1.64	0.12	0.73	0.752	0.624
BBR_M	4.71	1.24	4.84	1.50	1.51	0.22	0.731	0.659
FBR_M	5.02	1.13	5.12	1.42	1.71	0.19	1.012	0.257
BSP	5.38	1.05	5.73	1.15	0.55	0.46	1.099	0.179
FSP	5.62	0.96	5.80	1.15	1.61	0.21	1.037	0.233

Note: **ER**: external risk, **IR**: internal risk, **IM**: impact on individual, **OM**: impact on organization, **IA**: information assurance, **BBR**: before resilience, **FBR**: after resilience, **BPS**: before information assurance, **FSP**: after information resilience

5. Results

5.1 Stimulus Check

Overall, the results indicated that the stimulus worked as intended. To identify how much the stimulus affected the recall, we conducted the analysis of variance (ANOVA) using two questions: "Did the news article help in recalling details about the storm?" and "How much do you remember about the October storm in 2006?" The results indicated that the stimulus

significantly affected participants' memory of the disaster (F= 5.452, p<0.001). Participants, who responded that the news article helped in recall, answered that they remembered the disaster clearly.

Results of t-tests show the response differences in dependent constructs before- and after-disaster. The results lend credence to the argument that the stimulus was successful (See Table 3). For all of the constructs, responses were scored higher after the disaster context than before: External perceived risk (t-value = 1.928, p < .05), internal perceived risk (t-value = 3.414, p < .001), organizational resilience (t-value = 3.488, p < .001), and information assurance (t-value = 2.614, p < .01).

Table 3. The Result of *T*-Test (N = 104)

Construct	Mean		Mean Difference	*t*-value
	Before	After		
External Perceived Risk	3.65	3.86	-.1993	-1.928*
Internal Perceived Risk	4.64	4.96	-.3168	-3.414***
Resilience	4.83	5.09	-.2500	-3.488***
Information Assurance	5.56	5.71	-.1505	-2.614**

5.2 Measurement Model Estimation

The measurement model in PLS was assessed by examining internal consistency and convergent and discriminant validity (Barclay, et al., 1995; Wynne W. Chin, 1998). An internal consistency reliability of 0.7 or higher is considered adequate (Barclay, et al., 1995). Convergent and discriminant validity is assessed with the average variance extracted (AVE) for each construct from its indicators and item loadings. AVE should be greater than 0.50 to justify using a construct.

Table 4. Inter-Construct Correlations by Contexts

Contexts and Construct	Mean	S.D.	Correlations of Constructs[a]					
Pre treatment			1	2	3	4	5	6
[$]ER (1)	3.65	1.54	**0.78**					
IR (2)	4.64	1.34	0.38**	**0.87**				
Resilience (3)	4.73	1.61	-0.08	-0.13	**0.73**			
IA (4)	4.29	1.58	-0.3**	-0.21*	0.3**	**0.87**		
IM (5)	4.83	1.35	-0.25*	-0.23*	0.29**	0.26*	**0.96**	
OM (6)	5.56	1.09	-0.22*	-0.33**	0.46**	0.36**	0.65**	**0.82**
Post treatment			1	2	3	4	5	6
[$]ER (1)	3.86	1.59	**0.79**					
IR (2)	4.96	1.34	0.53**	**0.86**				
Resilience (3)	4.73	1.61	-0.19*	-0.15	**0.76**			
IA (4)	4.29	1.58	-0.32**	-0.31**	0.23*	**0.87**		
IM (5)	5.09	1.28	-0.26*	-0.3**	0.25*	0.26*	**0.96**	
OM (6)	5.71	1.03	-0.34**	-0.39**	0.39**	0.33**	0.74**	**0.82**

Note: [a] Diagonal elements in the "correlation of constructs" matrix are the square root of the average variance extracted (AVE). For adequate discriminant validity, diagonal elements should be greater than corresponding off-diagonal elements.
[$]**ER**: external risk, **IR**: internal risk, **IM**: impact on individual, **OM**: impact on organization, **IA**: information assurance
[**]*P < 0.01* (2-tailed), [*]*P < 0.05* (2-tailed)

Tables 4 and 5 show the scale means, standard deviations, Pearson's correlations, composite reliability (C.R.), and Average Variance Extracted (AVE) among the measures, in two contexts: before and after the stimulus was administered. The composite scale reliability for each construct, which is similar to Cronbach's alpha, were each above 0.80 (the recommended cut-off of 0.70), indicating that the measures used in this study are adequately reliable. Further, confirmatory factor analysis shows that each construct explains the variance equally. The aforementioned results suggest that the constructs in the study exhibit good psychometric properties. Factor loadings for the indicators associated with each construct are reported in Table 5 and it shows that each of them exceed 0.70, indicating adequate reliability—the only exception being one item for the *organizational impact* construct.

Table 5. PLS Component-Based Analysis: Cross-Loadings

Items	Before Disaster				After Disaster			
	Cross Loadings [27]	Composite Reliability	Cronbach's Alpha	AVE	Cross Loadings	Composite Reliability	Cronbach's Alpha	AVE
ER1	0.750				0.823			
ER2	0.793				0.777			
ER3	0.824				0.788			
ER4	0.706				0.689			
ER5	0.762				0.755			
ER6	0.746				0.743			
ER7	0.872				0.879			
ER8	0.822	0.927	0.912	0.617	0.854	0.930	0.914	0.625
IR1	0.777				0.859			
IR2	0.912				0.890			
IR3	0.850	0.884	0.804	0.718	0.859	0.903	0.839	0.756
IM1	0.974				0.974			
IM2	0.961				0.961			
IM3	0.946	0.972	0.958	0.922	0.947	0.973	0.958	0.923
OM1	0.704				0.843			
OM2	0.689				0.850			
OM3	0.748				0.732			
OM4	0.792				0.899			
OM5	0.970	0.915	0.885	0.683	0.799	0.915	0.885	0.683
RES1	0.914				0.874			
RES2	0.584				0.714			
RES3	0.821				0.724			
RES4	0.765	0.857	0.782	0.607	0.728	0.847	0.760	0.582
IA1	0.896				0.873			
IA2	0.900				0.888			
IA3	0.865				0.865			
IA4	0.808				0.822			
IA5	0.876	0.939	0.919	0.755	0.902	0.940	0.920	0.758

Note: To calculate cross loadings, a factor score for each construct was calculated based on the weighted sum, provided by PLS graph, of that factor's standardized and normalized indicators. Factor scores were correlated with individual items to calculate cross loadings.
Notes: **ER**: external risks, **IR**: internal risk, **IM**: individual impact, **OM**: organization impact, **RES**: Resilience, **IA**: information assurance

[27] We included two items in organizational impact and perceived resilience, even though such items showed slightly lower factor loading scores than the recommended cut-off, .70 in further analyses. As Barclay et al. (1995) mentioned, some of the scales do not show the same psychometric properties when used in different theoretical and research contexts from those in which they were first developed. That is, it is important to retain as many items as possible from the original scale to preserve the integrity of the original research design, as well as the comparability of the results with other studies that used the same scales (Barclay, et al., 1995) , even though some of the factor loadings are slightly below than .70.

In any study, each construct is expected to share more variance with its items than with those of other constructs in the model in order to obtain convergent and discriminant validity. Convergent and discriminant validity is inferred when the square root for each construct's AVE is larger than its correlations with other constructs (Wynne W. Chin, 1998). As shown in Table 4, the square root of AVE for every construct exceeded the suggested criterions of 0.70 for all measures (see the diagonal elements in the matrix; note that the AVE of each construct is higher than its correlations with other constructs). Therefore, adequate convergent and discriminant validity was obtained.

5.3 Testing the Structural Model

5.3.1 Testing the Significance of Path Coefficients

PLS allows for testing of the structural model by evaluating path coefficients between latent constructs. Figure 4 presents the path coefficients for each of the sub-samples: before ($path_b$) and after ($path_a$) the disasters contexts across each of the constructs. First, for the effect of external risk (H1), represented as path coefficients from external risk on internal risk are significant ($path_b = 0.383$; $path_a = 0.529$); for Hypothesis H1a (external risk to information assurance: $path_b = -0.169$; $path_a = -0.221$) and for Hypothesis H1b (internal risk to information assurance: $path_b = -0.194$; $path_a = -0.192$) path coefficients are significant for both before and after the disaster context.

Second, for the effect of internal risk on IS effectiveness ($H2_{a\&b}$), results show statistically significant paths from internal risk to organizational impact ($path_b = -0.217$; $path_a = -0.174$). On the other hand, the effects of internal risk on individual impact ($path_b = -0.149$; $path_a = -0.147$) was not found to be significant. For the hypothesis $H2_b$, i.e., effect of internal risk on

organizational resilience, there was no statistical significant at both contexts ($path_b$ = -0.058; $path_a$ = -0.024).

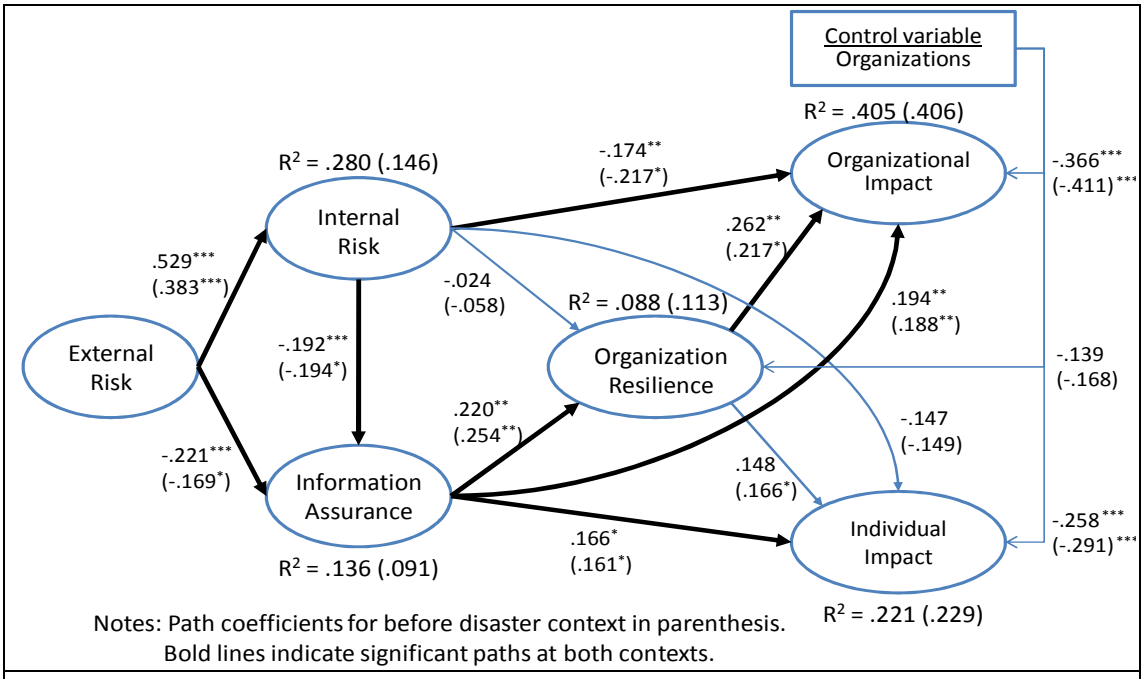


Figure 5. Results of Data Analysis: Pre and Post

Third, the effects of employees' perceptions of information assurance on IS effectiveness (Hypothesis $H3_a$ and $H3_{b)}$, path coefficients from information assurance to resilience ($path_b$ = 0.254; $path_a$ = 0.220) and to organizational impact ($path_b$ = 0.188; $path_a$ = 0.194) and to individual impacts ($path_b$ = 0.161; $path_a$ =0.166) were positive and statistically significant,.

Finally, for the effect of organizational resilience on IS effectiveness ($H4_{a\&b}$), the effect of resilience on organizational impact ($path_b$ = 0.217; $path_a$ = 0.262) was positively and statistically significant but for individual impact ($path_b$ = 0.167; $path_a$ =0.058) did not show significant results. Table 5 shows the indirect effects of external (internal) risks through internal risk (information assurance) on information systems effectiveness. The external risks have

indirect effects on organization and individual impact, while internal risk only affects resilience through information assurance.

5.3.2 Testing the Hypothesis of the Effect of Disaster

Following the model tested, we conducted a multiple group analysis to find the differences in path coefficients for the before- and after- disaster effects. To test the effect of disaster, we estimated two separate models using before and after items in PLS. We then compared two models using the test for differences implemented by Keil et al. (2000) by calculating t-statistics to evaluate the differences in path coefficients across models. Unlike prior research, we used the same subject to compare two different contexts. The t-tests compare responses within participants.

The results shown in Table 6 indicate that the differences between two path coefficients can be divided into two directions[28], either positive or negative, based on the impact of the disaster: 1) the negative effects of external/internal perceived risk, and 2) the positive effects of information assurance and organizational resilience on three dimensions of information systems effectiveness.

First, the negative effect of external risks on internal risks and information assurance were significantly stronger after the disaster than the corresponding effect in the structure model for the pre-disaster context (T-value= -12.739 and -3.200). For the hypothesis 5, the effect of internal perceived risk was statistically significant results for organizational impacts and

---

[28] $Spooled = \sqrt{[(N_1 -1)/(N_1 + N_2 +2)] \times SE_1^2 + [(N_2 -1)/(N_1 + N_2 +2)] \times SE_2^2}$, $t = (PC_1 - PC_2) / [\text{Spooled} \times \sqrt{(1/N_1 + 1/N_2)}]$, where, spooled indicates pooled estimator for the variance, N_i is sample size of dataset of group *i*, SE_i is standard error of path in structural model for group *i*, and PC_i is path coefficient in structural model of group *i. in this study, two group sizes =102.*

organizational resilience (T-value= -3.133 and -1.866) (H5a) but for the information assurance and individual impact, there were no significant differences (H5b).

Second, the positive effects of organizational resilience and information assurance on individual and organization impact were found to be higher after the disaster context than before the disaster context. For the hypothesis 6, organizational resilience was significantly stronger for organization impact after the disaster context as compared to the before disaster context (T-value= 2.869) (H6a) but was not significant for individual impact (H6b).

Finally, the effect of information assurance did not show statistical significance for both organizational (H7a) and individual impact (H7b) but organizational resilience in the before disaster context than in the after disaster context (*T*-value= 2.146). The discussion section will address the implications of the results.

Table 6. Difference Between Before And After the Disaster

Path	Before			After			A vs. B	
Direct Effect	S.D	Path	T	S.D	Path	T	$P. Diff.	T-value
ER → IR	0.089	0.383	4.267	0.074	0.529	7.605	0.146	12.739***
ER → IA	0.119	-0.169	*ns*	0.113	-0.221	2.383	0.052	3.200***
IR → IA	0.106	-0.194	1.656	0.102	-0.192	2.422	-0.002	*ns*
IR → IM	0.115	-0.149	*ns*	0.109	-0.147	*ns*	*ns*	*ns*
RES → IM	0.125	0.166	*ns*	0.099	0.148	*ns*	*ns*	*ns*
IA → IM	0.126	0.161	1.946	0.117	0.166	2.163	*ns*	*ns*
IR → OM	0.098	-0.217	2.030	0.098	-0.174	1.631	-0.043	-3.133***
RES→ OM	0.126	0.217	1.884	0.096	0.262	2.815	0.045	-2.869**
IA → OM	0.165	0.188	2.331	0.118	0.194	2.525	*ns*	*ns*
IR → RES	0.136	-0.058	*ns*	0.124	-0.024	*ns*	*ns*	*ns*
IA → RES	0.107	0.254	2.112	0.119	0.220	1.907	-0.034	2.146*
Indirect Effect	S.E%		Z stat	S.E%		Z stat		
ER→IR→ OM	0.043	-0.090	-2.07	0.059	-0.151	-2.571	0.061	8.397***
ER→IR → IM	0.047	-0.063	*ns*	0.062	-0.122	-1.958	0.059	7.621***
ER→IR → RES	0.053	-0.027	*ns*	0.067	-0.046	*ns*	*ns*	*ns*
IR→IA → OM	0.030	-0.024	*ns*	0.031	-0.033	*ns*	*ns*	*ns*
IR→IA → IM	0.023	-0.018	*ns*	0.047	-0.029	*ns*	*ns*	*ns*
IR→IA → RES	0.030	-0.033	*ns*	0.033	-0.040	*ns*	*ns*	*ns*

Notes: ER: external risks, IR: internal risk, IM: impact on individual, OM: impact on organization, IA: information assurance

% $sqrt\ (b^2s_a^2 + a^2s_b^2 + s_a^2s_b^2)$, where a and b and are the magnitudes of the paths between x, M, and y, and s_a and s_b are the standard deviations of a and b.
$ P. Diff.: Differences of path coefficients between before and after the disaster. Negative sign indicates that the path coefficient of Before the disaster is bigger than one of After the disaster.
$P^* < 0.05$, $P^{**} < 0.01$, $P^{***} < 0.001$

5.4 Post Hoc Analysis

We tested the impact of a possible explanatory factor: usage of different groups. This post-hoc analysis relates to the differential effect of both organizational resilience and information assurance on hospital information systems effectiveness between main (clinical) user and support (administrative) user. We analyzed the different effect on HIS based on user types. As we mentioned in methods section, HIS users can be categorized into two major users: main users who are consumers of the information system, such as physicians and nurses vs. support users who are suppliers, such as hospital and IT supporters and they have different purposes to use the systems. As consumers, main-users are deeply involved in using systems applications (i.e., software applications, database software etc) that typically relate to EMR. On the other hand, support-user focuses more on the technical and system hardware and billing/scheduling systems. Therefore, the effect of disaster on their hospital information system can be different between these two user groups. Specifically, users' position can moderate the effect of two factors on the relationship between risk, resilience, and information assurance and those consequences (IM and OM). Since the purpose of the use for hospital information systems is different between main users who involve in data and information relating to the provisioning of care for patients and supporters who focus on keeping the systems constantly available. For example, comparably stressful perception (i.e., perceived risk) can have more serious influence on main users such as physician and nurse than on administrators such as IT supporters.

Perceived risk has a stronger negative impact on the nurses or physician's use of hospital information systems than administrators do.

The results of differences between two path coefficients across the before- and after-disaster context are shown in Table 7 and 8. First, the tables showed that internal risk affected individual impact (IR IM), which was not significant for the whole model, for main user both before ($b = -.273$, $p < 0.01$) and after disaster ($b = -.266$, $p < 0.01$). However, the table reveals insignificant results not only for the effect of internal risk on information assurance ($b = -.146$ and , $p > 0.05$) and resilience on organizational impact ($b = -.204$, $p > 0.05$) for before disaster but also the effect of external risks on information assurance ($b = .139$ and , $p > 0.05$), resilience on organizational impact ($b = .253$ and , $p > 0.05$), and information assurance on organizational impact ($b = -.149$ and , $p > 0.05$) for after disaster.

Second, for the support user, Table 7 and 8 showed significant results on the effect of external risk on information assurance before disaster ($b = -.300$ and , $p < 0.01$) and the effect of information assurance on individual impact after disaster ($b = -.219$ and , $p < 0.05$) (both results were not significant in whole model).

Finally, for the difference between two users, results showed consistent direction for information assurance and internal risk. Support user has higher impact from the paths in terms of information assurance than main users do (i.e. ER → IA, IA → IM, and IA → OM). Main user, however, has higher impact from the paths in terms of internal risk than support user do (i.e., ER → IR, IR → IM, IR → OM, and IR → RES).

Table 7. Difference between main and support users for before disaster

Path	Main user (n=46)			Support user (n=58)			A vs. B	
Direct Effect	S.D	Path	T	S.D	Path	T	$P. Diff.	T-value
ER → IR	0.143	0.448	1.861*	0.153	0.315	2.067*	0.133	4.531***
ER → IA	0.261	-0.037	*ns*	0.154	-0.300	2.300**	-0.263	6.401***
IR → IA	0.190	-0.146	*ns*	0.133	-0.169	*ns*	*ns*	*ns*
IR → IM	0.116	-0.273	2.627**	0.157	-0.086	*ns*	0.187	6.746***
RES → IM	0.127	0.146	*ns*	0.162	0.134	*ns*	*ns*	*ns*
IA → IM	0.135	0.126	*ns*	0.137	0.190	*ns*	*ns*	*ns*
IR → OM	0.094	-0.430	4.367***	0.152	-0.094	*ns*	0.336	13.126***
RES→ OM	0.102	0.204	*ns*	0.136	0.127	*ns*	*ns*	*ns*
IA → OM	0.106	0.204	2.121*	0.136	0.251	2.023*	-0.047	1.925*
IR → RES	0.163	-0.141	*ns*	0.197	-0.056	*ns*	*ns*	*ns*
IA → RES	0.110	0.465	3.803***	0.215	0.196	*ns*	0.269	7.717***
control → IM	0.101	-0.207	1.784*	0.083	-0.355	4.702***	-0.148	8.203***
control →OM	0.091	-0.265	2.705**	0.069	-0.523	8.107***	-0.258	16.445***
control →RES	0.135	-0.124	*ns*	0.128	-0.253	1.981*	-0.129	4.983**

Table 8. Difference between main and support users for after disaster

Path	Main user (n=46)			Support user (n=58)			A vs. B	
Direct Effect	S.D	Path	T	S.D	Path	T	$P. Diff.	T-value
ER → IR	0.100	0.663	6.612***	0.126	0.423	3.343***	0.24	10.547***
ER → IA	0.130	0.139	*ns*	0.099	-0.428	4.904***	-0.567	25.253***
IR → IA	0.208	-0.368	1.769*	0.106	-0.132	*ns*	0.236	7.505***
IR → IM	0.147	-0.266	2.355**	0.157	-0.033	*ns*	0.233	7.730***
RES → IM	0.188	0.128	*ns*	0.156	0.149	*ns*	*ns*	*ns*
IA → IM	0.144	0.115	*ns*	0.149	0.219	*ns*	*ns*	*ns*
IR → OM	0.136	-0.315	3.263***	0.133	-0.058	*ns*	0.257	9.690***
RES→ OM	0.198	0.253	*ns*	0.120	0.237	1.969*	0.016	*ns*
IA → OM	0.175	0.149	*ns*	0.140	0.267	2.173*	-0.118	3.821*
IR → RES	0.227	-0.177	*ns*	0.199	0.058	*ns*	*ns*	*ns*
IA → RES	0.147	0.328	2.227**	0.179	0.156	*ns*	0.172	5.259***
control → IM	0.164	-0.153	*ns*	0.114	-0.324	3.127***	-0.171	6.262***
control → OM	0.133	-0.223	1.677*	0.084	-0.460	6.128***	-0.237	11.075***
control → RES	0.229	-0.001	*ns*	0.106	-0.227	2.134*	-0.226	6.674***

Notes: $P^* < 0.05$, $P^{**} < 0.01$, $P^{***} < 0.001$

6. Discussion

In this study, we explored how external perceived risks affect information systems' effectiveness through perceived internal risk and information assurance and the impact of disaster on the relationship between the two. The study also addressed the issue of whether

organizational resilience positively affected information systems effectiveness. Table 9 presents a summary of the results and shows that data from the hospitals supported nine of the fourteen proposed hypotheses.

Table 9. Summary of Hypothesis Testing Results

Hypothesis	Descriptions	Support
H1a	External risk is positively related to internal risk.	Yes
H1b	External risk is negatively related to information assurance.	Yes
H2a	Internal risk is negatively related to information assurance.	Yes
H2b	Internal risk is negatively related to organizational resilience.	No
H2c	Internal risk is negatively related to organization impact.	Yes
H2d	Internal risk is negatively related to individual impact.	No
H3a	Information assurance will positively affect organizational resilience.	Yes
H3b	Information assurance will positively affect organization impact.	Yes
H3c	Information assurance will positively affect individual impact.	Yes
H4a	Organizational Resilience will positively affect organization impact.	Yes
H4b	Organizational Resilience will positively affect individual impact.	Yes (only Before context)
H5a	Risks will differently affect organizational impact depending on the presence or absence of a disaster.	Yes
H5b	Risks will differently affect individual impact depending on the presence or absence of a disaster.	No
H6a	Organizational Resilience will affect organizational impact differently depending on the presence or absence of a disaster.	Yes
H6b	Organizational Resilience will affect individual impact differently depending on the presence or absence of a disaster.	No
H7a	Information assurance will affect organizational impact differently depending on the presence or absence of a disaster.	No
H7b	Information assurance will affect individual impact differently depending on the presence or absence of a disaster.	No

Thus, the overarching conclusion is that a disaster experience affects hospital employees' perceptions about information systems in important ways. Specifically, organizational resilience has relatively higher effect on information systems effectiveness in the context of a disaster,

while internal perceived risk has more effect on information systems effectiveness before the disaster. We also conclude that internal perceived risk negatively affects 'organizational impact' both before and after the disaster context. Finally, our results also yielded no support for the hypothesis (H2b) relating internal risk and organizational resilience, a surprising and interesting conclusion.

6.1 Theoretical Implications

This research contributes to the body of literature on extreme events. It informs both research and practice. Our work contributes in several ways. First, the major contribution of this research is that it empirically provides a psychological mechanism on perceived risks, perceived information assurance, and organizational resilience for the usage of information systems under the disaster. According to the information systems literature, such psychological aspects in linking risks and organizational resilience have not been empirically investigated. Distinguishing between external and internal perceived risks caused by disaster enhances our understanding of how people are influenced by external risks. Even though external perceived risk itself does not affect the information systems effectiveness and resilience, it triggered employees in their perceptions regarding internal risk and information assurance in their organization. This finding calls for future research on identifying and integrating additional factors to extend the impacts of resilience and information assurance on information systems effectiveness.

Second, our research sheds light on the way in which a disaster affects the relationship between employees' perceptions and information systems' effectiveness. We show how various individual perceptions differently affect information systems effectiveness in the disaster context by focusing on system users' cognitive elements, such as perceived risks, information assurance,

and organizational resilience. Specifically, this study shows that a disaster could increase the effect of perceived risks, while decreasing the effect of resilience on information systems effectiveness, which in turn indicates negative effects on information systems effectiveness. We explored employees' perceptions about risks and resilience as two major potential factors of enhancing information systems effectiveness, which helps us to answer, in part, how a disaster affects individuals and what factors can explain the way that disaster affects information systems' effectiveness.

Third, this study integrated effects of risks and resilience, which are often described as different sides of the same coin (Haeffel et al. 2007), by considering factors affecting organizational performance (i.e. hospital information systems effectiveness) in the model. Past research shows that risk and resilience are both affected by disasters (see, Paton et al. 2000). To date however, the relationship between perceived risk and resilience and the effect on the organizational performance and information systems effectiveness has not been studied. To our knowledge, this is the first study of its kind and the related issues need further flushing by way of further research in this area. The study informs us that the effect of resilience on information systems effectiveness was higher in the context of the disaster than before the disaster experience, while perceived internal risk more affects hospital information systems effectiveness before the disaster. When individuals deal with extreme events, they tend to lean more heavily on positive beliefs (i.e., resilience) than negative beliefs (perceived risk). In the context of the disaster, however, a disaster experience relieves perceived risk and in turn, the relieved perceived risk reduces the effect of IT on organizational impact. On the other hand, the experience fortifies the perceived resilience to keep their business continuity being stable and thus, the resilience reinforces employees to enhance organizational impact. Drawing on information systems success

theory and resilience theory, we provide an explanation for how the use of perceived risks and resilience correspondingly affect organizational performance. The empirical results suggest that these two factors are critical for the information systems effectiveness in disaster contexts.

6.2 Practical Implications

Many companies encourage their employees to believe that their organization maintains business continuity plans so as to reduce perceptions about their organizational risks and to improve their firms' performance through organizational resilience. Many of them will have plans, but the details of the plans may not be widely known to employees, except to the disaster response teams. Preparing for extreme events and training employees to manage, helps employees cope better with stressors that are a consequence of extreme events, and would positively affect organizations in terms of better business continuity and information system effectiveness. On the other hand, negative extreme events result in physical and psychological impacts that lead to elevated stress levels and higher perceived risk, and this in turn generates a negative image. Proper coping strategies need to be developed and employees should be made to participate in them. The findings suggest that the employees' perceptions of risks and information assurance are important not only to maintaining resilience and hospital information systems effectiveness but also to facilitating employees' work using hospital information systems. Managers should focus on employees' work practices by enhancing their capabilities to handle emergency contexts and to maintain better business continuity during and in the aftermath of extreme events.

In order for hospitals to increase information systems effectiveness, hospitals may pursue two strategies in terms of risk and resilience in a disaster context: (a) increasing organizational

resilience and/or (b) decreasing internal risk perception. Even though internal risk perception is decreased, organizational resilience may not improve. Hospital management should adopt a process to enhance resilience and a separate process to reduce perceived internal risk. Since disasters expose employees to tasks that are physically and psychologically complex, ambiguous and difficult to assimilate(Hahn et al. 2010; Paton et al. 2001), the perception of organizational resilience—the perceptions that systems are powerful, resourceful, and capable of dealing with all the demands employees may face—makes employees more effectively use hospital information systems to enhance their performance and to overcome the disaster.

In order to enhance employees' perception of organizational resilience, hospital managers can increase their organization's information assurance, such as improving security and privacy practices instead of decreasing risk perception. Information assurance in and of itself influences improvement in IS effectiveness. As the results show, information assurance increases organizational resilience which is consistent with Ezingeard et al.'s (2007) suggestion that information assurance is an important function within organizations, a factor as critical to organizational success. Information assurance can also be enhanced by educating and informing employees as it increases the probability of a high degree of security and privacy perceptions among employees.

Finally, the findings suggest that when individuals deal with extreme events, they tend to lean more on a positive belief (i.e., resilience) than a negative belief (perceived risk) in the context of an of organization. The experience of disaster reduces the effects of perceived risk. After an actual disaster, however, the disaster experience decreases perceived risk, and that in turn reduces the effect of it on 'organizational impact'. In addition, a disaster experience may ameliorate the positive effects of information assurance on organizational resilience and the

effect of organizational resilience on IS effectiveness. The experience fortifies the perceived resilience to keep their business continuity being stable and thus, the resilience reinforces them to enhance organizational impact.

6.3 Implications for Practitioners

In keeping their business continuity, Managers may undertake two different strategies for different users of the information systems. *First, pre- and post-disaster strategy*: Managers want to keep their businesses continuing under any given circumstance. However, results revealed that individuals were affected workplace environment under the different context i.e., extreme event. In terms of the work environment, this research has important implications for job design and management of IT enabled work environments in continuing their business. If managers want to alleviate such differences in employees' behavior between different contexts, they need to establish emergency response policies including preparedness and risk management to guide employees on how to deal with extreme events and when continue working on their tasks with effectively using hospital information systems for success. A core objective of emergency response is facilitating the capacity of individuals and communities to maintain or regain prior levels of functioning following significant disruption by extreme event activity (Paton, Kelly, Burgelt, & Doherty, 2006). In addition, organizational preparedness can reduces the risk of damage within a organization and facilitates a capability for coping with the temporary disruption related to extreme event. Therefore, the maintenance of preparedness over time is essential to sustaining individual resilience (Paton, et al., 2000). By doing so, when perceptions of risk or information assurance caused by the extreme events inhibit the employees' resilience and effective utilization of information systems, perhaps employees' disaster preparedness can

be increased and thus, their usage of information systems can be enhanced. Through careful management of the change of work environment, we can influence whether and how employees try to keep their works consistent. While it may appear intuitively clear that these are things a good managers should do anyway, our study provides empirical evidence that should provide a guideline for managers to control information systems.

Second, A strategy for different users: Although exploratory, this study's findings suggest IT-related goals of different user groups may be influenced by different aspects of information systems. In particular, managers need to take into account such different types of users and circumstances when dealing with hospital information systems. Results show that the different effect on HIS based on user types which have different purposes to use the systems. According to results, main users, who are physicians and nurses as consumers using the information system for clinical purpose, are more concerns about the effect of internal risk on their effective use of information systems regardless of disaster, while support users, who are IT technologists and administrators as suppliers to keep the information systems sustaining, tended to focus more on information assurance such as security and privacy concerns and external perceived risk. This is because they use the information systems with different purposes; the main-users are deeply involved in using systems applications (i.e., software applications, database software etc) that typically relate to patients care and these might be detrimentally affected by the inoperable systems caused by extreme events. On the other hand, support-user are more concerned about not only keeping technical/system hardware and billing/scheduling systems safe but also preventing their patients records from threats. To enhance the applicability of main users and IT support users' use of information systems, management should provide employees with information on security and privacy policies with strong system security/privacy protection

programs. In addition, managers need to ensure they behave and structure solid hospital information systems such that employees believe not only that the systems are not vulnerable to physical or technical threats but also that they are capable of controlling information systems for their tasks under any circumstances. Consistent with the institutional efforts for enhancing hospital employees' perceived organizational resilience and reducing information assurance on hospitals' information systems, top management should clearly advertise the point that the organization cares about the robustness of hospital information systems and that this is an important mission of the organization.

6.4 Limitations and Future Research

Future research could strengthen and extend the results of this study by addressing the limitations. First, the research design in this study has limited internal validity due to the lack of a control group (i.e., employees were not randomly assigned to conditions in general).

Second, this study excluded several important factors regarding IS effectiveness, such as information quality, systems quality, and user satisfaction. Even though this study mainly focused on the factors relating to disasters, those measures may help refine the results in the model and allow us to better understand the phenomenon. Despite such limitations, this study represents an initial step in developing a better understanding of perceived risks, resilience, and information assurance regarding information effectiveness, and it provides feasible suggestions for further investigation. To our knowledge, this is the first study of this kind to address such issues.

Acknowledgements:

Third essay has been funded in part by NSF under grant 0705292 and by grants from SUNY Buffalo school of Management Research Grants.
We would like to thank Dean Messing (Deputy Commissioner (Retd) of Emergency Management at Erie County, NY), Joanne Ruh and Mike Mineo (CIO and IT Manager of Roswell Park Cancer Institute, John Herman of Kenmore Mercy Hospital and Francis J. Meyer (Vice President, Kalieda Health) and Davis Ellis (Directory of Emergency Services, Erie Community Medical Center).

Epilogue

The three essays in this dissertation cover important areas of the technical and behavioral aspects of information assurance including security and privacy. Information assurance (IA) is a topic of growing interest to many organizations in terms of their organizational and individual performances using information systems and technology.

The three essays presented in the previous chapters of this dissertation explain various and independent but inter-related aspects regarding the information systems environment surrounding information systems users. Consequently, combined together, the findings of these essays offer more insightful information and provide stronger implications.

The three essays in this dissertation span across themes, dealing with various topics in the contemporary technological and psychological research issues, such as malware protection, privacy concerns in online mail usage, and impact of extreme event on performances in organizations regarding information systems. It is important to note that the three essays presented an important contribution to the information systems research community by shedding light on scientific knowledge in this field and provide practical implications for managers improve effectiveness of information systems in their organizations. This research has implications for practice and has been well received by not only the peers in the field, but also by practitioners. The studies considered in this dissertation present big picture covering not only technical aspect which is able to build systems security but also individual usage of the systems and organizational policy on usage of information systems under the extreme event.

There are quite a few directions along which the research reported in these three essays can be extended. The findings of these studies as well as limitations of these studies provide opportunities for further exploration in information systems area. First essay in this dissertation

considered the categorizing framework with simple criteria as technical method. It is possible to draw other tradeoffs in terms of the number of clusters that could conceivably be created. In categorizing the malware, further research would be valuable to develop an economics analysis taking into account their detrimental impact and the cost relating office-disruption, etc. is a potential area for future exploration. Second essay suggests researchers to examine and amplify the potentially influential role of privacy and of users' behavior with in other vulnerable online contexts.

Third essay used sample collected at specific area: Western New York. Unfortunately, however, Mother Nature does not unfair to take a mercy on earth. Any area and organizations could be target of extreme events. This study was just beginning to scratch their surfaces. This study recommends researchers extend with larger and wider ranges of samples from different countries. In addition, future research should consider a variety of individual and organizational factors in looking for critical impacts on individual and organization performances using information systems.

REFERENCES

Acquisti, A., & Grossklags, J. (2003). *Losses, Gains, and Hyperbolic Discounting: An Experimental Approach to Information Security Attitudes and Behaviors.* Paper presented at the 2nd Annual Workshop on Economics and Information Security Robert H. Smith School of Business, University of Maryland, MD.

Acquisti, A., & Grossklags, J. (2005). Privacy and Rationality in Individual Decision Making. *IEEE Security & Privacy, 3*(1), 26-33.

Advisory, Q. S. (January 28, 2004). *Multiple Variants of the MyDoom Email Worm*: Qualys, Inc.

Anderson, J. (1997). Clearing the way for physicians' use of clinical information systems. *Commun ACM, 40*, 83-90.

Barclay, D. C., Higgins, C., & Thompson, R. (1995). The Partial Least Squares Approach to Causal Modeling: Personal Computer Adoption and Use as an Illustration. *Technology Studies, 2*(2), 285-308.

Baron, R. M., & Kenny, D. A. (1986). The Moderator-Mediator Variable Distinction in Social Psychological Research: Conceptual, Strategic, and Statistical Considerations. *Journal of Personality and Social Psychology, 51*(6), 1173.

Barton, M., Christianson, M., Gittell, J. H., Martin-Rios, C., Powley, E. H., & Sutcliffe, K. (2006). *Organizational resilience: A social mechanisms perspective*. Paper presented at the Academy of Management 2006.

Barton, P. T. (2006). Resilience under military operational stress: Leaders influence hardiness? *Military Psychology, 18*, 131-148.

Bhatti, R., Samuel, A., Eltabakh, M. Y., Amjad, H., & Ghafoor, A. (Writer). (2007). Engineering a Policy-Based System for Federated Healthcare Databases [Article], *IEEE Transactions on Knowledge & Data Engineering*.

Bigley, G. A., & Roberts, K. H. (2001). The incident command system: High-reliability organizing for complex and volatile task environments. *Academy of Management Journal, 44*(6), 1281-1299.

Block, J., & Kremen, A. M. (1996). IQ and ego-resiliency: Conceptual and empirical connections and separateness. *Journal of Personality and Social Psychology, 70*, 349-361.

Bovey, W. H., & Hede, A. (2001). Resistance to organisational change: The role of defence mechanisms. *Journal of Managerial Psychology, 16*(7/8), 534.

Braghin, S., Coen-Porisini, A., Colombo, P., Sicari, S., & Trombetta, A. (2008, May 17-18, 2008). *Introducing Privacy in a Hospital Information System.* Paper presented at the SESS'08, Leipzig, Germany.

Breznitz, S. (1983). *The Denial of Stress*. New York: International Universities Press, Inc.

Bruce Hughes. (2003, Thursday, June 5, 2003. URL: http://infosecuritymag.techtarget.com/2003/jun/digest05.shtml). Sobig.c Dies, Danger Lingers. *information security, 5*.

Bruneau, M., Chang, S., Eguchi, R., Lee, G., O'Rourke, T., Reinhorn, A., Shinozuka, M., Tierney, K., Wallace, W. and, & von Winterfelt, D. (2003). A framework to quantitatively assess and enhance seismic resilience of communities. *Earthquake Spectra, 19*, 733-752.

C. C. Zou, D. T., and W. Gong, . (Oct. 2004). *Email worm modeling and defense*. Paper presented at the 13th International Conference of Computer Communications and Networks (ICCCN'04).

Calhoun, L., G., & Tedeschi, R. G. (2004). Author's response: The foundations of posttraumatic growth: New Considerations. . *Psychological Inquire, 15*, 93-102.

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

Campbell, K., Gordon, L. A., Loeb, M. P., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: empirical evidence from the stock market. *Journal of Computer Security, 11*(3), 431-448.

Carnall, C. A. (1986). Toward a Theory for the Evaluation of Organizational Change. *Human Relations, 39*(8), 745.

Cerullo, V., & Cerullo, M. J. (Writer). (2004). BUSINESS CONTINUITY PLANNING: A COMPREHENSIVE APPROACH [Article], *Information Systems Management*: Taylor & Francis Ltd.

Chen, R., Rao, H. R., Sharma, R., Upadhyaya, S., & Kim, J. (2010). An Empirical Examination of IT-Enabled Emergency Response: The Cases of Hurricane Katrina and Hurricane Rita. *Communications of the Association for Information Systems (CAIS), 26*(8), 141-156.

Chen, R., Sharman, R., Chakravarti, N., Rao, H. R., & Upadhyaya, S. (2008). Emergency Response Information System Interoperability: Development of Chemical Incident Response Data Model. *Journal of the Association for Information Systems (JAIS), 9*(3), 203-232.

Chen, R., Sharman, R., Rao, H. R., & Upadhyaya, S. (2008). An Exploration of Coordination in Emergency Response Management. *Communications of the ACM (CACM), 51*(5), 66-73.

Chin, W. W. (1998). Issues and opinion on structural equation modeling. *MIS Quarterly, 22*(1), VII.

Chin, W. W., & Newsted, P. R. (1999). Structural Equation Modeling analysis with Small Samples Using Partial Least Squares. In R. Hoyle (Ed.), *Statistical Strategies for Small Sample Research* (pp. pp. 307-341): Sage Publications.

Clark, A. J. (1991). The Indentification and Modification of Defense Mechanisms in Counseling. *Journal of Counseling and Development : JCD, 69*(3), 231.

Comfort, L. (1999). *Shared Risk: Complex Seismic Response*. New York, NY.: Pergamon.

Cook, T. D., & Campbell, D. T. (1975). *Quasi-experimentation: Design and analysis issues for field settings*. Chicago: Rand McNally.

Cournane, A., & Hunt, R. (2004). An analysis of the tools used for the generation and prevention of spam. *Computers & Security, 23*(2), 154.

Craft, J. P. (2000). *Metrics and the USAID Model Information Systems Security Program*. Paper presented at the NIST and CSSPAB Workshop. Retrieved from http://csrc.nist.gov/csspab/june13-15/Craft.pdf

Cramer, P. (2004). Stress, Autonomic Nervous System Reactivity, and Defense Mechanisms. In U. Hentschel, G. Smith, J. G. Draguns & W. Ehlers (Eds.), *Defense Mechanisms: Theoretical, Research, and Clinical Perspectives* (Vol. 136). New York: Elsevier.

Cramer, P., & Block, J. (1998). Preschool antecedents of defense mechanism use in young adults: A longitudinal study. *Journal of Personality and Social Psychology, 74*(1), 159.

Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: an empirical investigation. *Organization Science, 10*(1), 104-115.
Dalziell, E. P., & McManus, S. T. (2004). *Resilience, Vulnerability, and Adaptive Capacity: Implications for System Performance*. Paper presented at the International Forum for Engineering Decision Making.
Dash, S., & Saji, K. B. (2007). The Role of Consumer Self-Efficacy and Website Social-Presence in Customers' Adoption of B2C Online Shopping: An Empirical Study in the Indian Context. *Journal of International Consumer Marketing; 2007, Vol. 20 Issue 2, p33-48, 20*(2), 33-48.
de Board, R. (1978). *The Psychoanalysis of Organisations*. London: Tavistock.
DeLone, W. H., & McLean, E. R. (1992). Information Systems Success: The Quest for the Dependent Variable. *Information Systems Research, 3*(1), 60-95.
Delone, W. H., & Mclean, E. R. (2003). The DeLone and McLean Model of Information Systems Success: A Ten-Year Update. *Journal of Management Information Systems, 19*(4), 9–30.
Devaney, E. (2007). Hurricane preparedness: Planning and procedures at Blue Cross Blue Shield of Florida. *Journal of Business Continuity & Emergency Planning 2*(2), 128–137.
Dhillon, G., & Backhouse, J. (2001). Current directions in IS security research: toward socio-organizational perspectives. *Information Systems Journal, 11*(2).
DoD. (1998). *Joint Doctrine for Information Operations*.
Dowling, G. R. (1999). Perceived Risk. In P. E. Earl & S. Kemp (Eds.), *The Elgar Companion to Consumer Research and Economic Psychology* (pp. 419–424). Cheltenham, UK: Edward Elgar.
Dowling, G. R., & Staelin, R. (1994). A Model of Perceived Risk and Intended Risk-Handling Activity. *Journal of Consumer Research, 21*, 119-134.
Draguns, J. G. (2004). Defense Mechanisms in the clinic, the laboratory, and the social world: Toward closing the gaps. In U. Hentschel, G. Smith, J. G. Draguns & W. Ehlers (Eds.), *Defense Mechanisms: Theoretical, Research and Clinical Perspectives* (pp. 3-41). Boston, MA: Elsevier.
Elliott, D., & Swartz, E. (2002). *Business Continuity Management Routlegde*: Taylor & Francis Group
Erlich, Z., Gelbard, R., & Spiegler, I. (2002). Data Mining by Means of Binary Representation: A Model for Similarity and Clustering. *Information Systems Frontiers, 4*(2), 187.
Ettredge, M., & Richardson, V. J. (2002). *Assessing the risk in e-commerce.* Paper presented at the the 35th Annual Hawaii International Conference on System Sciences, Maui, HI.
Ettredge, M., & Richardson, V. J. (2003). Information transfer among internet firms: the case of hacker attacks. *Journal of Information Systems, 17*(2), 71-82.
Ezingeard, J.-N., McFadzean, E., & Birchall, D. (2005). A Model of Information Assurance Benefits. *Information Systems Management, 22*(2), 20.
Ezingeard, J.-N., McFadzean, E., & Birchall, D. (2007). Mastering the art of corroboration. *Journal of Enterprise Information Management, 20*(1), 96.
Fahlman, S. E. (2002). Selling interrupt rights: a way to control unwanted e-mail and telephone calls. *IBM System Journal, 41*(4).
Fallows, D. (2003). *How It Is Hurting Email and Degrading Life on the Internet*: Pew Internet & American Life Project.

Ghanea-Hercock, R. (2003). Authentication with P2P Agents. *BT Technology Journal, 21*(4), 146.

Haeffel, G. J., & Grigorenko, E. L. (2007). Cognitive Vulnerability to Depression: Exploring Risk and Resilience. *Child and Adolescent Psychiatric Clinics of North America, 16* 435-448.

Hahn, D., Block, J., Keith, M., & Vinze, A. (2010). Collaborative Systems for Decision Making for Disaster Preparedness and Response, Department of Information Systems. In N. Bajgoric (Ed.), *Always-On Enterprise Information Systems for Business Continuance: Technologies for Reliable and Scalable Operations Source* (pp. 41-57).

Halawi, L. A., McCarthy, R. V., & Aronson, J. E. (2007). An Empirical Investigation of Knowledge Management Systems' Success. *The Journal of Computer Information Systems, 48*(2), 121.

Hamilton, S., & Chervany, N. L. (1981). Evaluating information system effectiveness part I: comparing evaluation approaches. *MIS Quarterly, 5*(3), 55-69.

Hann, I.-H., Roberts, J., Slaughter, S., & Fielding, R. (2004). *Economic Returns to Open Source Participation: A Panel Data Analysis.* Paper presented at the Third Annual Workshop on Economics of Information Security, University of Minnesota, MS.

Haux, R., Winter, A., Ammenwerth, E., & Brigl, B. (2004). *Strategic Information Management in Hospitals: An Introduction to Hospital Information Systems*: Springer.

Heal, G., & Kunreuther, H. (2006). Modeling Interdependent Risks. Risk Management and Decision Processes Center, University of Pennsylvania

Henry, J. W., & Stone, R. W. (1999). End user perceptions of the impacts of computer self-efficacy and outcome expectancy on job performance and patient care when using a medical information system. *International Journal of Healthcare Technology Management, 1*, 103-124.

Hentschel, U., Juris G. Draguns, Ehlers, W., & Smith, G. (2004). Defense Mechanisms: Current Approaches to research and measurement. In U. Hentschel, G. Smith, J. G. Draguns & W. Ehlers (Eds.), *Defense Mechanisms: Theoretical, Research and Clinical Perspectives* (pp. 3-41). Boston, MA: Elsevier.

Hinde, S. (2002). Spam, scams, chains, hoaxes and other junk mail. *Computers & Security, 21*(7), 592.

Hinde, S. (2003). Spam: The evolution of a nuisance. *Computers & Security, 22*(6), 474.

Holmes, D. S. (1985). Defense mechanisms. In R. J. Corsini (Ed.), *Encyclopedia of psychology* (Vol. 1, pp. 341-350). New York: Wiley.

Huberman, B. A., Adar, E., & Fine, L. R. (2005, 2-3 June 2005). *Valuating Privacy.* Paper presented at the Workshop on Economics and Information Security, Boston, MA.

Hypponen, M. (2004). *Mydoom email worm already bigger than Sobig*: Director, Anti-Virus Research, F-Secure Corporation.

ICSA. (2003). *ICSA Labs 9th Annual Computer Virus Prevalence Survey*: ICSA.

ICSA. (2004). *ICSA Labs 10th Annual Computer Virus Prevalence Survey*: ICSA.

Jackson, E. L. (1981). Response to earthquake hazard. *Environment and Behavior, 13*, 387-416.

Jaeger, C., Renn, O., Rosa, E., & Th., W. (2002). *Risk and Rational Action*. London: Earthscan.

James, L. R., Demaree, R. G., & Wolf, G. (1984). Estimating within-group interrater reliability with and without response bias. *Journal of Applied Psychology, 69*(85-98).

Jensen, T. B., & Aanestad, M. (2007). Hospitality and hostility in hospitals: a case study of an EPR adoption among surgeons. *European Journal of Information Systems, 16*, 672.
Jiang, J. J., Klein, G., & Discenza, R. (2001). Information system success as impacted by risks and development strategies. *IEEE Transactions on Engineering Management, 48*(1), 46.
Judge, P., Alperovitch, D., & Yang, W. (2005, 2-3 June 2005). *Understanding and Reversing the Profit Model of Spam.* Paper presented at the WEIS05: Workshop on Economics and Information Security, Boston, MA.
Katehakis, D., Kostomanolakis, S., Tsiknakis, M., & SC, O. (2002). An open, component-based information infrastructure to support integrated regional healthcare networks. *International Journal of Medical Informatics, 68*, 3-26.
Keil, M., Tan, B. C. Y., Wei, K.-K., & Saarinen, T. (2000). A cross-cultural study on escalation of commitment behavior in software projects. *MIS Quarterly, 24*(2), 299.
Keizer, G. (Nov 23, 2005). Newest Sober Variant: Biggest Worm Attack of The Year. *TechWeb News*. Retrieved from http://informationweek.com/story/showArticle.jhtml;jsessionid=BU4AG1LM4LTU4QSNDBCSKH0CJUMEKJVN?articleID=174401802
Kienzle, D. M., & Elder, M. C. (2003). *Recent Worms: A Survey and Trends*. Paper presented at the the 2003 ACM Workshop on Rapid Malcode (WORM-03).
Kienzle, D. M., & Elder, M. C. (2003). *Recent Worms: A Survey and Trends.* Paper presented at the The Workshop on Rapid Malcode (WORM03), Washington, DC, USA.
Kim, D. J., Sivasailam, N., & Rao, H. R. (2004). Information Assurance in B2C Websites for Information Goods/Services. *Electronic Markets, 14*(4), 344-359.
Kim, D. J., Sivasailam, N., & Rao, H. R. (2005). Information Assurance in B2C Websites for Information Goods/Services. *Electronic Markets, forthcoming*.
Kim, D. J., Song, Y. I., Baynov, S. B., & Rao, H. R. (2005). A multidimensional trust formation model in B-to-C e-commerce: a conceptual framework and content analyses of academia/practitioner perspectives. *Decision Support Systems, 40*(2), 143.
Kozlowski, S. W., & Hattrup, K. (1992). A disagreement about within-group agreement: Disentangling issues of consistency versus consensus. *Journal of Applied Psychology, 77*, 161-167.
Lemos, R. (2003, August 13, 2003, 1:05 PM). Users race against worm, variants. *ZDNet News:*. Retrieved from http://news.zdnet.com/2100-1009_22-5063356.html
Levene, H. (1960). Essays in Honor of Harold Hotelling. In I. O. e. al. (Ed.), *Contributions to Probability and Statistics* (pp. 278-292): Stanford University Press.
Lininger, R., & Vines, R. D. (2005). *Phishing: Cutting the Identity Theft Line*. Indianapolis, IN.: Wiley
Lucas, H. C. (1981). *Imlementation: The Key to Successful Information Systems*. New York: McGraw-Hill.
Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Information Systems Research, 15*(4), 336.
Mallak, L. (1998). Putting organizational resilience to work. *Industrial Management Science, 40*, 8-14.
MessageLabs. (2004). *Intelligence Annual Email Security Report 2004*: MessageLabs.

Milton, J., S., & Arnold, C. J. (1986). *Probability and Statistics in the Engineering and Computing Sciences*. New York: McGraw-Hill Book Company.

Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A., & Sadhukhan, S. K. (2009). E-risk Insurance Product Design: A Copula based Bayesian Belief Network. In M. Gupta & R. Sharman (Eds.), *Handbook of Research on Social and Organizational Liabilities in Information Security*.

Nazario, J., Anderson, J., Wash, R., & Connelly, C. (2001). The Future of Internet Worms. Crimelabs research (http://www.crimelabs.net/).

Nelson, R. R., Peter, A. T., & Barbara, H. W. (2005). Antecedents of Information and System Quality: An Empirical Examination Within the Context of Data Warehousing. *Journal of Management Information Systems, 21*(4), 199.

Neumann, P., & Weinstein, L. (1997). Inside Risks: Spam, Spam, Spam! . *Communications of the ACM, 40*(6), 112.

Odlyzko, A. (2002). *Privacy, Economics, and Price Discrimination on the Internet* Paper presented at the Workshop on Economics and Information Security, University of California, Berkeley, CA.

Oglethorpe, J. E., & Monroe, K. B. (1987). *Risk Perception and Risk Acceptability in Consumer Behavior: Conceptual Issues and an Agenda for Future Research.* Paper presented at the AMA Winter Marketers Educators' Conference, Chicago.

Oldham, M., & Kleiner, B. H. (1990). Understanding the nature and use of defense mechanisms in organisational life. *Journal of Managerial Psychology, 5*(5), 1-15.

Ondrack, D. A. (1974). Defense mechanisms and the Herzberg Theory: An alternate test. *Academy of Management Journal (pre-1986), 17*(000001), 79.

Paton, D., & Johnston, D. (2001). Disasters and communities: vulnerability, resilience and preparedness. *Disaster Prevention and Management, 10*(4), 270-277.

Paton, D., Kelly, G., Burgelt, P. T., & Doherty, M. (2006). Preparing for bushfires: understanding intentions. *Disaster Prevention and Management, 15*(4), 566.

Paton, D., Smith, L., & Violanti, J. (2000). Disaster response: risk, vulnerability and resilience. *Disaster Prevention and Management, 9*(3), 173.

Petak, W. (2002). *Earthquake resilience through mitigation: a system approach*. Paper presented at the The International Institute for Applied Systems Analysis.

Podsakoff, P., MacKenzie, S., & Podsakoff, N. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology, 88*(5), 879-903.

Qing, S., & Wen, W. (2005). A survey and trends on Internet worms. *Computers & Security, 24*(4), 334.

Rai, A., Lang, S. S., & Welker, R. B. (2002). Assessing the validity of IS success models: An empirical test and theoretical analysis. *Information Systems Research, 13*(1), 50.

Raymond, L. (1985). Organizational Characteristics and MIS Success in the Context of Small Business. *MIS Quarterly, 9*(1), 37.

Reddy, M., Purao, S., & Kelly, M. (2008). Developing IT Infrastructure for Rural Hospitals: a case study of benefits and challenges of hospital-to-hospital partnerships. *Journal of the Medical Informatics Association, 15*(4).

Rimal, R. N. (2001). Perceived Risk and Self-Efficacy as Motivators: Understanding Individuals' Long-Term Use of Health Information. *Journal of Communication, 51*(4), 633-654.

Robert E. Kraut, S. S., Rahul Telang, and James Morris. (2005). Pricing Electronic Mail to Solve the Problem of Spam. *Human-Computer Interaction, 20*(1/2), 195-223.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Joiirnal of Psychology, 91*, 93- 114.

Rose, A. (2004). Defining and measuring economic resilience to disasters. *Disaster Prevention and Management, 13*(4), 307.

Rosenberg, M., & Hovland, C. (1960). *Attitude organization and change*. New Haven, CT: Yale University Press

Rousseau, D. M. (1989). Psychological and implied contracts in organizations. *Employee Responsibilities and Rights Journal, 2*, 121-139.

Sabherwal, R., Jeyaraj, A., & Chowa, C. (2006). Information System Success: Individual and Organizational Determinants. *Management Science, 52*(12), 1849-1864.

Salkever, A. (2003). The Ever-Growing Virus Crisis. *BisinessWeek*.

Sauer, C., Dampney, C. N. G., & Southon, G. (1997). *Fit, failure, and the house of horrors: toward a configurational theory of IS project failure.* Paper presented at the Eighteenth International Conference on Information Systems, Atlanta, GA.

Saxton, J. (2002). *Security in the Information Age: New Challenges, New Strategies*. Washington, D.C.: Joint Economic Committee, United States Congress.

Schou, C. D., & Trimmer, K. J. (2004). Information Assurance and Security. *Journal of Organizational and End User Computing, 16*(3), I.

Seddon, P. B. (1997). A respecification and extension of the DeLone and McLean model of IS success. *Information Systems Research, 8*(3), 240.

Seligman, M. E. P. (1998). *Learned optimism: How to change your mind and your life*. New York: : Pocket Books.

Sharman, R., Krishna, K. P., Rao, H. R., & Upadhyaya, S. (2006). Malware and Antivirus Deployment for Enterprise Security. In M. Warkentin & R. Vaughn (Eds.), *Enterprise Information Systems Assurance and Systems Security* (pp. 42-61). Hershey, PA: Idea Group Publishing.

Shen, S. Y., & Shaw, M. J. (2005). *Using Information Technology for Effective Emergency Response*. Paper presented at the International Business Research Forum

Simon, H. A. (1982). *Empirically Grounded Economic Reason* (Vol. 3). Cambridge, MA: MIT Press.

Simon, H. A., & Thaler, R. H. (1986). Rationality in Psychology and Economics/The Psychology and Economics Conference Handbook: Comments on Simon, on Einhorn and Hogarth, and on Tversky and Kahneman. *The Journal of Business, 59*(4), S209.

Sipior, J. C., Ward, B. T., & Bonner, P. G. (2004). Should Spam Be on the Menu? *Association for Computing Machinery. Communications of the ACM, 47*(6), 59.

Sjöberg, L. (2004). Explaining Individual Risk Perception: The Case of Nuclear Waste. *Risk Management, 6*(1), 51-64.

Slovic, P., Fischhoff, B., Lichtenstein, S., & Roe, F. J. C. (1981). *Perceived Risk: Psychological Factors and Social Implications [and Discussion].* Paper presented at the Proceedings of the Royal Society of London. Series A, Mathematical and Physical Sciences,.

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly, 20*(2), 167.

Smith, R. G. a. M. D. (2005, 2-3, June, 2005). *Protecting Personal Information: Obstacles and Directions* Paper presented at the WEIS05: Workshop on Economics and Information Security, Boston, MA.

Starr, R., Newfrock, J., & Delurey, M. (2003). Enterprise Resilience: Managing Risk in the Networked Economy. *Strategy & Business, Spring*

Stein, A. (January 30, 2004). Microsoft offers MyDoom reward. *CnnMoney*. Retrieved from http://www.moneymag.com/2004/01/28/technology/mydoom_costs/

Stone, E. F., Gardner, D. G., Gueutal, H. G., & McClure, S. (1983). A Field Experiment Comparing Information-Privacy Values, Beliefs, and Attitudes Across Several Types of Organizations. *Journal of Applied Psychology, 68*(3), 459.

Stone, R. N., & Winter, F. W. (1987). *Risk: Is it still uncertainty times consequences?* Paper presented at the Proceedings of the American Marketing Association, Winter Educators Conference, Chicago, IL.

Sutcliffe, K. L., & Vogus, T. (2003). Organizing for Resilience. In J. E. D. a. R. E. Q. K. Cameron (Ed.), *Positive Organizational Scholarship*. San Francisco: Berrett-Koehler.

Syverson, P. (2003, May 29-30, 2003). *The Paradoxical Value of Privacy.* Paper presented at the 2nd Annual Workshop on Economics and Information Security Robert H. Smith School of Business, University of Maryland, MD.

T.D O'Rourke, A. J. L., and L.K. Nozick. (2003). Lessons Learned from the World Trade Center Disaster About Critical Utility Systems. In M. F. Myers (Ed.), *Beyond September 11: Ail Account of Posl-Disoster Research* (pp. 269-290). Boulder, CO: Natural Hazards Research and Applications Information Center, University of Colorado.

Thomas, K., Dunster, H. J., & Green, C. (1981). *Comparative Risk Perception: How the Public Perceives the Risks and Benefits of Energy Systems [and Discussion]*. Paper presented at the Proceedings of the Royal Society of London. Series A, Mathematical and Physical Sciences.

Thong, J. Y. L., & Yap, C.-S. (1996). Information systems effectiveness: A user satisfaction approach. *Information Processing & Management, 32*(5), 601.

Thong, J. Y. L., Yap, C.-S., & Raman, K. S. (1996). Top management support, external expertise and information systems implementation in small businesses. *Information Systems Research, 7*(2), 248.

Tierney, K. (1997). Impacts of recent disasters on businesses: the 1993 midwest floods and the 1994 Northridge earthquake. In B. Jones (Ed.), *Economic Consequences of Earthquakes: Preparing for the Unexpected*. Buffalo, NY.: National Center for Earthquake Engineering Research.

Todd, M. (2003). Worms as attack vectors: Theory, Threats, and Defenses. Retrieved Sep 27, 2005, from SANS Institue http://www.sans.org/rr/whitepapers/threats/930.php

Tversky, A., & Kahneman, D. (1982). Availability: A heuristic for judging frequency and probability. In D. Kahneman, P. Slovic & A. Tversky (Eds.), *Judgment Under Uncertainty: Heuristics and Biases* (pp. 163-189). Cambridge: Cambridge University Press.

Vaillant, G. E. (1992). *Ego mechanisms of defense: Aguide for clinicians and researchers*. Washington, DC: American Psychiatric Press.

Vlasti, B., & Paul, T. (2004). Intrusion Detection: Issues and Challenges in Evidence Acquisition. *International Review of Law, Computers & Technology, 18*(2), 149.

Waikar, A., & Nichols, P. (1997). Aviation safety: a quality perspective. *Disaster Prevention and Management: An International Journal, 6*(2).

Waldmann, E. (2000). Incorporating Freud's Theory on Cognitive Processes into Business Ethics Education. *Teaching Business Ethics, 4*(3), 257.

Wathieu, L., & Friedman, A. (2005). *An Empirical Approach to the Valuing Privacy Valuation.* Paper presented at the WEIS05: Workshop on Economics and Information Security, Boston, MA.

Wayne, H. B., & Andrew, H. (2001). Resistance to organisational change: The role of defence mechanisms. *Journal of Managerial Psychology, 16*(7/8), 534.

Weaver, N. C., & Paxson, V. (2004, May 13-14, 2004). *A Worst-Case Worm.* Paper presented at the The Third Annual Workshop for Economics and Information Security (WEIS04), Minnessota.

Weems, C. F., Watts, S. E., Marsee, M. A., Taylor, L. K., Costa, N. M., Cannon, M. F., et al. (2007). The psychosocial impact of Hurricane Katrina: Contextual differences in psychological symptoms, social support, and discrimination. *Behaviour Research and Therapy, 45*, 2295-2306.

Westin, A. F. (1967). *Privacy and freedom*. New York: Atheneum.

Whitman, M. E. (2004). In defense of the realm: understanding the threats to information security. *International Journal of Information Management, 24* (1), 43-57.

Wolf, D. G. (2003). Statement by NSA's Director of Information Assurance before the House Select Committee on Homeland Security, US House of Representatives, available at: www.nsa.gov/ia/Wolf_SFR_22_July_2003.pdf. Retrieved 22 July from available at: www.nsa.gov/ia/Wolf_SFR_22_July_2003.pdf

Zalewski, M. (2003). I don't think I really love you, or writing internet worms for fun and profit.

Zou, C. C., Gong, W., & Towsley, D. (2002). *Code Red Worm Propagation Modeling and Analysis.* Paper presented at the presented at Proceedings of the 9th ACM conference on Computer and communications security, Washington, DC, USA.

Appendix. Survey Instrument

School of Management
University at Buffalo The State University of New York

Hospital Information Infrastructure
Survey Questionnaire

The enclosed survey is part of an information systems research project that examines the risk mitigating factors that influence the effectiveness of the hospital information infrastructure during critical incidents. This study will help us develop a framework for analyzing the effectiveness of hospital information infrastructure in public health systems. This framework could be used by hospitals to help it respond to critical incidents (such as the October storm at Buffalo) in a more effective way.

(Please note that we define hospital information infrastructure as technologies, people and processes working in an organized way to provide services to patients in a hospital.

A critical incident can be defined as any event that is unexpected, acute, stressful and exceeds the normal coping capacities of individuals.)

The information you provide will assist in the development of better hospital information infrastructure systems in the future. At the end of the study, **the results of the survey will be available at:**

http://www.som.buffalo.edu/isinterface/Information%20Infra/infra_1.htm

All information obtained from participants of this survey will be confidential, and will be used for research purposes only. Please note that you may withdraw from the study at any time, and the data you provided will be destroyed. **You will be a candidate for receiving a gift certificate worth five dollars for your participation.**

The School of Management at UB (University at Buffalo) sincerely appreciates your participation in this survey. If you have any questions about this questionnaire, you can reach us at insupark@buffalo.edu or Prof. Sharman at 716-645-2081.

Research Team: Insu Park (Ph.D. Candidate), Dr. H.R Rao, Dr. Raj Sharman, Dr. Shambhu J Upadhyaya
Management Science and Systems, University at Buffalo, NY

General Instructions

For parts I, II, IV, V, and VI, please choose a number **between 1 and 7** to indicate the degree to which you agree or disagree with each statement. The numbers 1 to 7 indicate the level of agreement (1 = Strongly Disagree; 2 = Disagree; 3 = Somewhat Disagree; 4 = Neutral; 5 = Somewhat Agree; 6 = Agree; 7 = Strongly Agree).

For part III, the numbers 1 to 7 indicate the level of excellence (1 = Very Poor; 2 = Poor; 3 = Somewhat Poor; 4 = Neither poor nor good; 5 = Fair; 6 = Good; 7 = Excellent).

If it is not applicable to you, ***please circle "N/A."*** Please circle your choice as shown below:

	Strongly disagree			Neutral			Strongly agree	N/A
1. Smoking should be banned from public places	1	2	3	4	5	6	(7)	0

Part I: INFRASTRUCTURE EFFECTIVENESS

Individual Impact

Individual impact refers to the impact of the hospital information infrastructure on individual job performance.

The hospital information infrastructure…	**Strongly disagree**			**Neutral**			**Strongly agree**	**N/A**
20. . …increases my productivity (requires less effort than would have been required without it).	1	2	3	4	5	6	7	0
21. . …saves my time (i.e. it allows me to accomplish more work than what would have been possible without it).	1	2	3	4	5	6	7	0
22. . … helps me meet patient needs effectively.	1	2	3	4	5	6	7	0

Organizational Impact

The following items refer to the impact of information infrastructure on the organization's performance.

The hospital information infrastructure…	**Strongly Disagree**			**Neutral**			**Strongly agree**	**N/A**
23. . … increases the effectiveness of our hospital's operations.	1	2	3	4	5	6	7	0
24. . … provides us with information to effectively manage medical supplies.	1	2	3	4	5	6	7	0
25. . … supports effective scheduling (nurses, physicians, beds, operating rooms etc)	1	2	3	4	5	6	7	0
26. . … provides us with information to effectively help patients.	1	2	3	4	5	6	7	0
27. . … supports effective billing and insurance activities.	1	2	3	4	5	6	7	0
28. . … will not be restrictive as the organization grows, enters new alliances, or develops new businesses.	1	2	3	4	5	6	7	0

Part II: ENVIRONMENT PERCEPTIONS

Directions: There are two parts for same question: Before and After October Storm.

Before October Storm

External Risk

Our hospital might not operate when… (Please Note * implies extended period, i.e. more than one hour)	**Strongly disagree**			**Neutral**			**Strongly agree**	**N/A**
29. . … the electric power system (e.g. Niagara Mohawk) is disrupted*.	1	2	3	4	5	6	7	0
30. . … the telecommunication system (e.g. Verizon, Sprint) is disrupted*.	1	2	3	4	5	6	7	0
31. . …the gas and oil storage system (e.g. National Fuel Gas Company) is disrupted*.	1	2	3	4	5	6	7	0
32. . …the national financial system (e.g. banks, insurance companies) is disrupted*.	1	2	3	4	5	6	7	0
33. . …the transportation system (e.g. roads, bus) is disrupted*.	1	2	3	4	5	6	7	0
34. . …the law & order (e.g. police) is disrupted*.	1	2	3	4	5	6	7	0
35. . …Food & supply management is disrupted*.	1	2	3	4	5	6	7	0
36. . ...water supply is disrupted*.	1	2	3	4	5	6	7	0

Internal Risk

37. When network facilities (e.g. network/cable plant) are disrupted, the medical information systems are affected.	1	2	3	4	5	6	7	0
38. When the internal telecommunication system is disrupted, the medical information systems are affected.	1	2	3	4	5	6	7	0
39. When the staff does not turn up, it will negatively affect the performance of the medical information systems.	1	2	3	4	5	6	7	0

Security and Privacy

40. Medical information systems are accessible only to those authorized to have access.	1	2	3	4	5	6	7	0

41.	Information is securely shared in our hospital.	1	2	3	4	5	6	7	0
42.	Legitimate users are never denied access to the medical information whenever it is required.	1	2	3	4	5	6	7	0
43.	Our primary database system (i.e. medical records) is stable and safe against tampering.	1	2	3	4	5	6	7	0
44.	Our information infrastructure protects the privacy of the patients (i.e. sensitive patient data are not shared or released without permission).	1	2	3	4	5	6	7	0

PART III: RESILIENCE

Business Resilience

Before October storm

Business resilience refers to the ability of the network to provide and maintain an acceptable level of service in the face of various faults and challenges to normal operation.

		Strongly disagree N/A			Neutral			Strongly agree	
45.	Our information infrastructure can handle many critical incidents at a time.	1	2	3	4	5	6	7	0
46.	People in the organization are well prepared to respond during critical incidents.	1	2	3	4	5	6	7	0
47.	Our organization has business continuity plans to handle unfamiliar situations.	1	2	3	4	5	6	7	0
48.	Our information infrastructure recovers quickly after critical incidents.	1	2	3	4	5	6	7	0

Individual Resilience

Individual resilience refers to the ability of an individual to work normally under any circumstances.

49.	I can perform my hospital duties normally during or after a critical incident, if I have not been affected by it.	1	2	3	4	5	6	7	0
50.	I can perform my hospital duties normally even if I have personally been affected by a critical incident in some way.	1	2	3	4	5	6	7	0
51.	I can perform my hospital duties normally even if my family members have been affected by a critical incident in some way.	1	2	3	4	5	6	7	0
52.	I felt as though I could effectively communicate my needs to my higher ups in the hospital.	1	2	3	4	5	6	7	0
53.	I had many healthy ways to cope with the stress of my job.	1	2	3	4	5	6	7	0
54.	My peers can perform their hospital duties normally during or after a critical incident.	1	2	3	4	5	6	7	0

Notice !!

In the next three pages of the survey, we will request you for responses in the context of "Before the October 2006 snow storm" and "After the October 2006 snow storm."

Immediately following this page is a description of the October storm.

We hope to be able to capture the diversity of the storm's impact in the survey.

General Questions – Please circle your answer			
A.	Was your hospital physically damaged by the October storm?	Yes	No
B.	Did your hospital operate normally during/ immediately after the October storm?	Yes	No
C.	Were you able to use the medical information system (e.g. database, medical records during/ immediately after the October storm?	Yes	No
D.	Was the operation of your hospital affected by any absence of staff members (due to reasons such as a driving ban being imposed) after the October storm?	Yes	No
E.	Were you at the hospital during or immediately after this critical incident?	Yes	No

F. Please list the infrastructures (e.g. electric power, water, telecommunications etc) that were affected by the October storm and specify for how long the disruption lasted.

Infrastructure affected	Duration (in hrs)

Cost of Buffalo Storm Cleanup May Top $30 Million

Electrical service workers in Buffalo, N.Y., on October 17, 2006.
Mike Groll for The New York Times

BUFFALO, Oct. 18 — More than 100,000 homes and businesses remained without power here on Wednesday, nearly a week after a preseason snowstorm dumped almost two feet of snow and wreaked havoc on trees and power lines. (By David Staba, Published: October 19, 2006)

After October Storm

External Risk

Our hospital might not operate when… (Please Note * implies extended period, i.e. more than one hour)	**Strongly disagree**			**Neutral**			**Strongly agree**	**N/A**
55. . … the electric power system (e.g. Niagara Mohawk) was disrupted*.	1	2	3	4	5	6	7	0
56. . … the telecommunication system (e.g. Verizon, Sprint) was disrupted*.	1	2	3	4	5	6	7	0
57. . …the gas and oil storage system (e.g. National Fuel Gas Company) was disrupted*.	1	2	3	4	5	6	7	0
58. . …the national financial system (e.g. banks, insurance companies) was disrupted*.	1	2	3	4	5	6	7	0
59. . …the transportation system (e.g. roads, bus) was disrupted*.	1	2	3	4	5	6	7	0
60. . …the law & order (e.g. police) was disrupted*.	1	2	3	4	5	6	7	0
61. . …Food & supply management was disrupted*.	1	2	3	4	5	6	7	0
62. . …water supply was disrupted*.	1	2	3	4	5	6	7	0
Internal Risk								
63. When network facilities (e.g. network/cable plant) were disrupted, the medical information systems could be affected.	1	2	3	4	5	6	7	0
64. When the internal telecommunication system was disrupted, the medical information systems could be affected.	1	2	3	4	5	6	7	0

65. When the staff did not turn up, it would negatively affect the performance of the medical information systems.	1	2	3	4	5	6	7		0

Security and Privacy

66. Medical information systems are accessible only to those authorized to have access.	1	2	3	4	5	6	7	0
67. Information is securely shared in our hospital.	1	2	3	4	5	6	7	0
68. Legitimate users are never denied access to the medical information whenever it is required.	1	2	3	4	5	6	7	0
69. Our primary database system (i.e. medical records) is stable and safe against tampering.	1	2	3	4	5	6	7	0
70. Our information infrastructure protects the privacy of the patients (i.e. sensitive patient data are not shared or released without permission).	1	2	3	4	5	6	7	0

PART IV: RESILIENCE

Business Resilience

Before October storm

Business resilience refers to the ability of the network to provide and maintain an acceptable level of service in the face of various faults and challenges to normal operation.

	Strongly disagree N/A			Neutral			Strongly agree	
71. Our information infrastructure can handle many critical incidents at a time.	1	2	3	4	5	6	7	0
72. People in the organization are well prepared to respond during critical incidents.	1	2	3	4	5	6	7	0
73. Our organization has business continuity plans to handle unfamiliar situations.	1	2	3	4	5	6	7	0
74. Our information infrastructure recovers quickly after critical incidents.	1	2	3	4	5	6	7	0

Individual Resilience

Individual resilience refers to the ability of an individual to work normally under any circumstances.

75. I can perform my hospital duties normally during or after a critical incident, if I have not been affected by it.	1	2	3	4	5	6	7	0
76. I can perform my hospital duties normally even if I have personally been affected by a critical incident in some way.	1	2	3	4	5	6	7	0
77. I can perform my hospital duties normally even if my family members have been affected by a critical incident in some way.	1	2	3	4	5	6	7	0
78. I felt as though I could effectively communicate my needs to my higher ups in the hospital.	1	2	3	4	5	6	7	0
79. I had many healthy ways to cope with the stress of my job.	1	2	3	4	5	6	7	0
80. My peers can perform their hospital duties normally during or after a critical incident.	1	2	3	4	5	6	7	0

Demographics

Directions: Finally, I would like to have some background information about you for classification purposes only. Please complete the following:

DG1. What is your overall job experience in the health care field? _____ **years** _____ **months**

DG2. For how long have you been in the present organization? _____ **years** _____ **months**

DG3. For how long have you used the medical information systems? _____ **years** _____ **months**

DG4. Job title _____

DG5. Profession _____