

# The Impact of Interdependent Risk on Health Care Information Infrastructure Effectiveness

Insu Park, Raj Sharman, H. R. Rao and Shambhu Upadhyaya  
State University of New York, Buffalo, NY

**Abstract**-This study explores how health care organizations mitigate risks due to infrastructure interdependencies using the information systems success framework. Specifically, this study examines whether interdependent risks affect information infrastructure effectiveness and, if so, what are the critical factors? How are interdependent risks mitigated by those factors across stakeholders? And how does mass disaster affect the stakeholders' perception of interdependent risks? This study makes a contribution to the literature on information infrastructure and risk management. This study will offer empirical support for the proposed framework on risk mitigation for infrastructure interdependent risks by using an information systems success framework. Further, this study will empirically support the theorized link between the way interdependent risks are managed and an organization's information infrastructure.

**Keywords:** *interdependent risks, health care information infrastructure, infrastructure interdependency, information infrastructure effectiveness.*

## I. INTRODUCTION

The worst storm (October 12-13, 2006) in Buffalo's history left behind a heartbreaking legacy of downed trees, lost power and a double whammy of snow and flooding. The unprecedented mix of a warm Lake Erie and rapidly dropping air temperatures created nearly two feet of extremely heavy snow that fell on thousands of trees in full fall foliage. Every hospital serving the Buffalo area was at or near capacity, with patients in beds and more coming through the door from Friday through Sunday in the storm's aftermath. Much of the impact was magnified because of the interdependence of infrastructure in terms of input and output of resources, geographic proximity of power structures to foliage, power lines and roads, foliage to roads, etc. In particular, individuals in the public health sector might have been psychologically affected by the fear that the infrastructure might not work well. Consequently, the potential impact resulting from the physical risks led them to work ineffectively.

This study explores, first, the effect of perceived interdependency risks on the information infrastructure's effectiveness, second, how health care organizations mitigate perceived interdependent risks (i.e., risks resulting from mutual dependency among entities) due to infrastructure interdependencies using the information systems success framework [8], and third, how a mass

disaster affects the individuals' perception of interdependent risks.

This model makes a contribution to the literature on information infrastructure and risk management. First, by providing a detailed description of the nature of interdependency risks and its underlying mitigators, it contributes to our better understanding of perceived risks, which might be considered as psychological effects in infrastructural disasters. Second, it describes the mechanisms by which the information infrastructure can be enhanced by identifying and describing how interdependency risks can be mitigated. This study integrates sociological (e.g., computer self-efficacy), technical (e.g., systems factors), and organizational (e.g., management support) fields using the information systems success framework in order to theoretically explain the impact of perceived interdependency risks on information infrastructure and mitigating roles of the three fields. This opens new avenues for identifying mitigating factors that can overcome interdependency risk perceptions by explaining its proposed antecedents.

This paper is organized as follows. The relevant literature on health care information infrastructure is discussed in Section 2. A conceptual model is presented in Section 3. Four propositions are also presented. The proposed methodology for the analysis is contained in Section 4. Section 5 forms the conclusion.

## II. RELATED RESEARCH

### A. Health Care information infrastructure (HII)

The term *Information infrastructure* has been widely used only during the last couple of decades. According to Hanseth et al. (1998) the notion of *Information infrastructure* consists of an inter-connected collection of computer networks, but with a heterogeneity, size, and complexity extending beyond what exists today. They define information infrastructure as "a shared, evolving, heterogeneous and open system of IT capabilities whose evolution is enabled and constrained by the installed base and the nature and content of its components and connections" [13]. On the other hand Sirkemma (2002) defines IT infrastructure as a combination of technology, hardware and software that provide services to a range of applications and users, and it is usually managed by the IT-group. This definition is based on the fact that IT infrastructure is not just a combination of different devices

and components but it highlights the importance of the human element [29]. In contrast to Information systems/Technology, information infrastructure has no fixed purpose to justify its existence.

On the other hand, a corporate/regional/national healthcare information infrastructure (HII) is about bringing timely health information to, and aiding communication among, those making health decisions for themselves, their families, their patients, and their communities [17]. The Centre for health information infrastructure defines information infrastructure as a series of technologies, products and services that will provide the framework for an interconnected and interoperable network to link hospitals clinics, research institutions, community health centers, other health related institutions, and homes<sup>1</sup>.

HII can be divided into several sub sections depending on the area/section. For example, local or community health information infrastructures (LHII) collect sources of clinical information within a community or region, with many potential economic advantages [20]. The National Healthcare Information Infrastructure (NHII)<sup>2</sup> is an initiative set forth to improve the effectiveness, efficiency, and overall quality of health and health care in the United States. This includes the set of technologies, standards, applications, systems, values, and laws that support all facets of individual health, health care, and public health (NHII, 2004). The Public health care information infrastructure (PHII) comprises of an intricate web of data resources, information systems, epidemiological analysis and investigation, standards, laws, and values. These elements are used by public health agencies at the local, state, and federal levels to prevent illness and promote health<sup>3</sup>.

Information infrastructure's general goal is to offer IT-based shared information services to a community. Their definition highlights two critical features. First, information infrastructure must be open and as a result of this it must rely on shared standards [13]. Infrastructures are open in the sense that there is no limit on how many users, computer systems or other technical components can be linked to it. In addition, an infrastructure emerges as a shared resource between heterogeneous groups of users.

### *B. Infrastructure Interdependency*

Each of the critical infrastructure sectors is increasingly becoming interdependent with the others. Disruptions in one sector are likely to affect the operations of others, adversely. Interdependent effects occur when an infrastructure

disruption spreads beyond itself to cause an appreciable impact on other infrastructures, which in turn causes more disruptive effects on the other infrastructures. When an infrastructure system suffers an outage, it is often possible to estimate the impact of that outage on service delivery. These are the "directly dependent effects" of the outage. For example, loss of telecommunications services can delay financial service transactions and the delivery of electric power. As a relatively new and crucial concept, interdependency is defined as the reliance of one infrastructure upon another or even mutual reliance of infrastructures upon one another [27, 32]. Interdependency effects have been observed numerous times, such as while assessing the US western states power outage in 1996. Rinaldi et al [27] identified six dimensions for understanding infrastructure systems, including infrastructure characteristics, such as spatial and organizational scope, and the legal/regulatory framework.

The interdependency problem is further compounded by the extensive linkage of physical infrastructure with information technology systems. Communication and information technologies (ICT) affect infrastructure system design, construction, maintenance, operations, and control, and more change appears inevitable. Potential applications include coupled sensing, monitoring, and management systems, distributed and remote wireless control devices, internet-based data systems, and multimedia information systems.

Although the coupling of physical infrastructure with information technology promises improved reliability and efficiency at reduced cost, there is surprisingly little knowledge about the behavior of these coupled systems, and thus, their potential for cataclysmic failure is high. Experience has shown that software is fragile by nature, and the software element of control and data acquisition systems is usually the least robust part of an integrated system.

Interdependency is a bidirectional relationship among infrastructures through which the state of each infrastructure is influenced by or correlated with the state of the others. As a simple example, the national electric power grid and natural gas network are interdependent – natural gas fuels many electrical generators, and elements of the natural gas infrastructure (e.g., gas conditioning plants, compressors, and computerized controls) require electricity to operate. A disturbance in the electrical system can cascade to the natural gas system, and loss of natural gas pressure can curtail the generation of electricity. Consequently, the states of these systems are mutually correlated. This simple case illustrates the importance of employing a systems perspective – an operational or security analysis of either infrastructure would be incomplete if it did not consider how the electric grid influenced the state of the natural gas system and vice-versa. There are four primary classes of interdependencies [27]: Physical, geographic, cyber and

---

<sup>1</sup> Centre for Health Information Infrastructure, "HealthScape' 95-Charting Health Information Infrastructure". Dec. 95

<sup>2</sup> <http://aspe.hhs.gov/sp/nhii/>

<sup>3</sup> <http://content.healthaffairs.org/cgi/reprint/21/6/45.pdf>

logical.

Interdependencies have been predominantly physical and geographic in nature. However, several factors have increased the prevalence and importance of cyber and logical interdependencies [24]. These include the proliferation of information technology along with the increased use of automated monitoring and control systems, and the increased reliance on the open marketplace for purchasing and selling infrastructure commodities and services.

### C. Interdependent Risks

The term ‘interdependent risk’ is derived from ‘interdependent security’ in the study of Kunreuther and Heal [19] and Heal and Kunreuther [14]. They recently introduced the concept of interdependent security using game-theoretic models as a way of investigating how interdependency affects individual choices about security expenditures in interdependent systems. Specifically, this framework has been applied to evaluating investments by individuals and firms in the security of infrastructure operations, emphasizing that any firm's risk is strongly dependent on the operational behaviors, priorities, and actions of others through interconnected networks or supply chains.

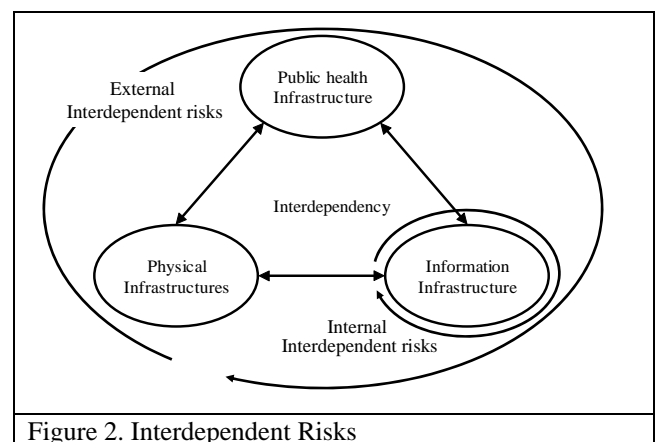
As the infrastructures become more interdependent on each other, there is a growing risk that restoration efforts or uncertainties undertaken by one sector could adversely affect the operations or restoration efforts of another, thereby contributing to further service disruptions [5]. The risk faced by one infrastructure of an organization or society depends on the actions of others because organizations’ information infrastructure is connected to other entities – so its efforts may be undermined by failures elsewhere. According to this, interdependent risks in this study are defined as the risks caused by the activities of one sector (or infrastructure) that produce a negative impact on other interconnected infrastructures.

Interdependent risks with respect to the information infrastructure are closely related to risks among interrelated critical infrastructures (external interdependent risks) or internal components (internal interdependent risks) in an organization. The risk faced by an individual is determined in part by one’s own behavior (direct impacts) as well as the behavior of others (indirect impacts). This characteristic of interdependent risks, gives a unique, and hitherto, unnoticed structure to the incentives for organizations to invest in mitigation. A consequence of interdependent risks is that a part of the cost of a failure is passed on to stakeholders.

In this study, we use two different concepts to explain the risks arising from interdependency of infrastructures. First, the increased interdependency combined with greater operational complexity, has made critical infrastructures

particularly vulnerable to natural hazards, human error and technical problems as well as new forms of cyber crime, terrorism and warfare [23]. Each of these events can result in severe service deterioration or outright infrastructure failure [1]. External interdependent risks (EIR) are caused by the vulnerabilities resulting from interdependency among the extensive linkages of physical infrastructure with information technology systems. For example, the 2001 world trade center attack showed the effect of risks of interdependency among infrastructures [22]. Thus, EIR may increase physical damage and are difficult to be controlled by an organization.

On the other hand, internal interdependent risks (IIR) can be caused by the components building an infrastructure in an organization. For the interdependencies within an organization, each internal infrastructure may suffer from the disruptions of the other infrastructure. Information infrastructure in an organization contains several components such as, platforms, applications, technologies, and humans. Compared to EIR, the conflicts among these components in IIR reduce the effectiveness of an organization’s infrastructure, and may be controlled by the organization that includes those components. The potential consequences of ineffective information systems to a healthcare center depend not only on its own choice of information infrastructure but also on the actions of other infrastructures such as human development. To illustrate this point, consider two infrastructures in an organization; information and medical facility. Each infrastructure faces a certain risk or uncertainty of a disruption that damages itself, and also a probability that such an attack would disrupt the activities of the other infrastructures. Therefore, interdependent risks in an organization can have devastating impacts on all parts of the organization. These negative externalities are an important feature of interdependent risks [15].



### D. Information Infrastructure Effectiveness

Our conceptual framework is based on the information systems success framework from DeLone and McLean [8]. This framework integrates two different viewpoints on

information systems i.e., the organizational and socio-technical viewpoint. Several viewpoints have been shown to explore information systems' effectiveness in previous research. For instance, Garrity and Sanders [10] show two different ways to view IS success; organizational perspective and socio-technical perspective. However, these perspectives focus largely on the IS related factors, such as information quality and systems quality as independent factors. These factors are not related with IS but related with the organizational climate and the individual. The principal focus of the organizational perspective is on the quality of the interface and the information provided by an IS to aid the workers in accomplishing their tasks. This was criticized for ignoring the human element. The socio-technical perspective, however, focuses on individual needs and assumes that the individual employee seeks monetary and other rewards.

DeLone and McLean identify six dimensions from the organizational and socio-technical perspectives of an IS. They are embedded in many common current approaches to evaluate IS effectiveness, which differ only in terms of the dimensions chosen for measurement [2]. The concept of information systems' effectiveness has been widely accepted in IS research as a principal criterion for assessing performance resulting from the usage of information systems [25]. Although a variety of conceptualizations have been offered among IS researchers, a core concept of IS effectiveness indicates that the degree of success in attaining organizational goals or performance is triggered from the usage of an information system [12, 26]. To measure IS effectiveness, IS researchers have not only used diverse constructs but also multiple measures that are able to tap into the concept properly [8, 25, 28]. Based on the review of previous literature, this study assesses IS effectiveness with three factors: individual impact, user satisfaction toward IS, and organizational impact. Such factors have been widely accepted among IS researchers as reliable constructs [8, 25, 31].

According to DeLone and McLean [8], *individual impact* refers to the positive effect of information on individual behavior. They explained that the term, "impact," contains

the indication of performance or productivity. Several items have been used to evaluate individual impact, such as perceived usefulness [25], net benefits [28], individual job performance, individual productivity, ease to do, etc. In line with individual impact, organizational impact indicates the organizational effect of information on organizational performance [8,12]

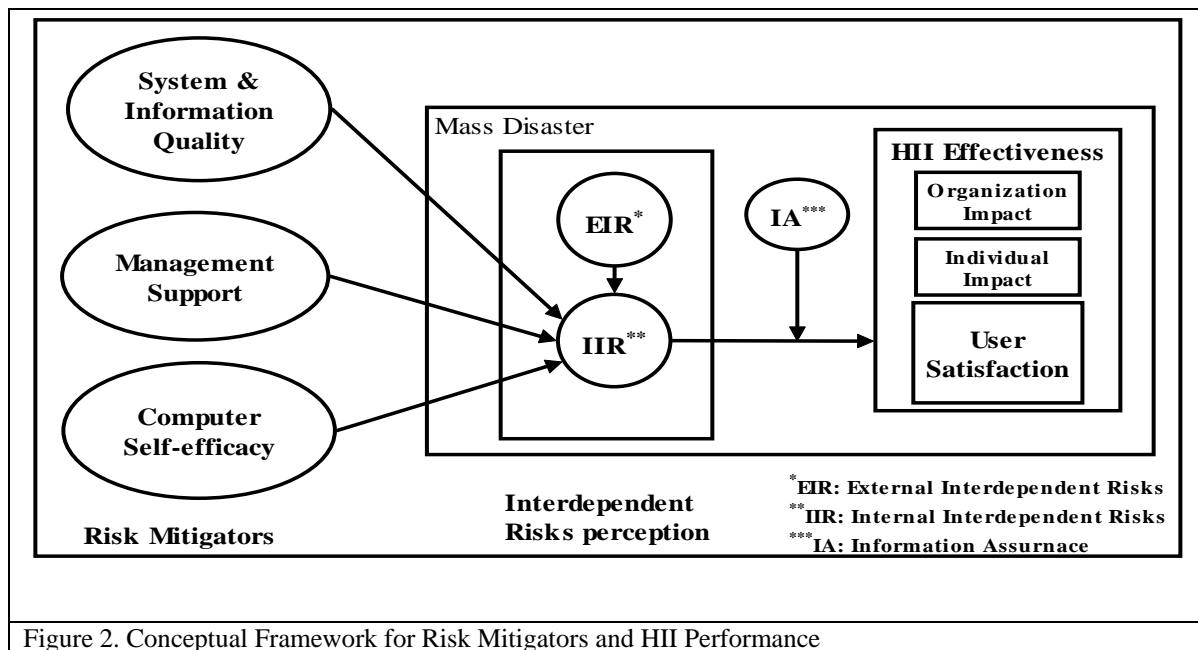
The final construct is user satisfaction, which refers to end-users' overall effective and cognitive evaluation of the level of consumption-related fulfillment experienced with information systems [2]. User satisfaction is the most widely used measure of information systems success. This is not only because it is often used as a surrogate of management information systems effectiveness, but also because it is related to other important variables in systems analysis and design.

### III. PROPOSITION

Following the information systems success framework, we propose three risk-mitigating constructs: systems and information quality, Management support, and computer self-efficacy. This paper focuses on the proposed constructs that mitigate internal interdependency risks rather than specific items that compose each of these factors.

Since the proposed interdependent risk mitigators are hard to develop, it is important to empirically assess their relative effectiveness in mitigating perceived risks. Our results will inform information infrastructure practitioners about interdependent risk mitigators, and they will thus be able to design an information infrastructure that specifically aims to incorporate each of the proposed mitigators.

Based on the preceding statements, a research model is proposed that aims to understand and prescribe how interdependency risks can be mitigated (Figure 2). In this model, infrastructure effectiveness is determined by external/internal interdependency risks. These interdependency risks, are mitigated by systems, organizational, and personal factors.



A. *The Effect of Interdependent Risk (IR) on Information Infrastructure Effectiveness in Public Health sector*

As for any risk, regardless of whether resulting in an injury to an individual or society, or whether causing damage to a system or to any other assets, it needs to be reduced [11]. The external interdependent risks positively affect internal interdependent risks. In a health care organization, the more the stakeholders perceive external interdependent risks from infrastructures, the more they perceive internal interdependent risks. In the real context, for example, the storm (October 12-13, 2006) had affected stakeholders both physically and mentally and had caused a concern that health care information infrastructure had not proved to be efficient and effective in tackling the situation. In addition, external and internal interdependent risks can reduce the information infrastructure’s effectiveness. Previous research shows that information technology or systems have been stimulated by the discovery of a negative relationship between IT risks and IT project success [3,16]. According to the Jiang et al [16], behavioral and technology-related risks can negatively affect information systems’ success directly or indirectly. Thus, our propositions regarding the relationship between interdependency risks and the information infrastructure’s effectiveness are as follows,

- **Proposition 1a:** *External interdependency risks are positively related to internal interdependency risks*
- **Proposition 1b:** *External interdependency risks are negatively related to HII effectiveness*
- **Proposition 1c:** *Internal interdependency risks are negatively related to HII effectiveness*

B. *Internal Interdependent Risk Mitigators*

One aspect of perceived risk is positively associated with demands for risk mitigation and decision-making. Previous

research has found that there are significant correlations between risk perception and precautionary behavior and decisions to implement countermeasures aimed at risk reduction (e.g.[9, 18, 30]). Consequently, risk perception is expected to be positively associated with demands for risk reduction or demands for risk mitigation.

Since perceived interdependent risks are determined by the external and internal interconnection among infrastructures, they can be mitigated not only by controlling the relationship between their information infrastructure and other infrastructures but also by enhancing the internal components of the information infrastructure. However, external interdependent risks are not controlled by an organization, because those risks are caused by bidirectional relationships between infrastructures through which the state of each infrastructure is influenced by or correlated with the state of the other.

To mitigate perceived IIRs, we propose three sets of factors; information infrastructure characteristics (i.e., systems quality, information quality which are largely based on the information systems’ success framework), top management support as organizational characteristics, and computer self-efficacy as individual factor.

Based on the past studies on information and system quality, this study adopts information and systems quality as mitigation factors of interdependent risks. As past research has shown [8], information and system quality can play a role in enhancing information systems success, which is expected to reduce the risks related to the information used. Several studies have focused on the positive effect of top management support on IS effectiveness. Management support creates a positive attitude in employees towards the use of IS [31]. In reality, many disaster recovery service

providers agree that management support is vital for disaster recovery planning to work [21]. Management support is essential to identify operations which are critical for the public sector in several situations and to provide important information concerning significant functions [4]. Prior research on computer self-efficacy (CSE) has suggested that CSE plays an important role in an individual's behavior towards information systems. Compeau et al. [6] examined that CSE is significantly associated with performance expectations, personal expectations, and system usage with a longitudinal context. This logic can be applied to mitigate the interdependent risks caused by information infrastructure. That is, high levels of computer self-efficacy would reduce internal interdependent risks. This becomes a major impetus for people to enhance their confidence levels towards the application of IS, and this can ultimately be linked to better performance beyond their expectations on information infrastructure. The factors mentioned above offer the following propositions of the present study:

- **Proposition 3a:** *Information & system quality reduce internal interdependency risks*
- **Proposition 3b:** *Management support reduces internal interdependency risks*
- **Proposition 3c:** *Computer self-efficacy reduces internal interdependency risks*

#### C. The Moderating Effect of Information Assurance

Interdependent risks from information infrastructure are prone to be vulnerable due to flaws in the network security. A fundamental cause of many of risks is in the variety of ways that individuals and/or groups can utilize digital technologies to engage in inappropriate, criminal or other illegal online activities (Vlasti et al. 2004). Information assurance “protects and defends information and information systems infrastructure by ensuring their availability, integrity, identification and authentication, confidentiality, and non-repudiation.” This includes providing for the restoration of information infrastructure by incorporating protection, detection, and reaction capabilities. In this study, information assurance plays a moderating role for enhancing effectiveness of information infrastructure by reducing the impact of interdependent risks.

- **Proposition 4:** *Information assurance moderates the relationship between interdependent risks and Information infrastructure effectiveness.*

## IV. PROPOSED RESEARCH METHODOLOGY

We propose a research design within the explained proposed framework as a field study. The subjects must be involved in related tasks within an information system with access to organizational data. All the work-scales complying with this requirement should be equally considered. Specific data regarding the subjects' work position and the size of the organization should also be gathered. We anticipate the use

of partial least square (PLS) to analyze the data. PLS is frequently used to test causal model.

#### A. Sample and Procedure

A survey method will be employed in order to test the propositions of the paper. Surveys will be administered to individuals embedded in health care organizations. Since all participants would be related to the health care information system, the authors will administer all the surveys in multiple sites through personal visits, and all participants will be assured of the confidentiality of responses with anonymous participation. With regard to data analysis and validity constraints, we consider the ideal sample size from public health care organizations to be no less than 200 subjects,.

#### B. Measures

The first order risk mitigator factors can be characterized based on the organizations and stakeholders included in the survey. Specifically, *systems factors* should include systems quality, information quality, and systems usefulness. *Management support* would be measured by the items adopted by Thong et al [31]. In addition, *computer self-efficacy* would include used items developed by Compeau and Higgins [7]. Using *information assurance* as a moderator, *interdependency risks* will be measured by each known item that we would develop further. Items should include the degree of perceived availability, confidentiality, and integrity of information infrastructure

The information infrastructure's effectiveness is measured by multi dimensional factors as aforementioned: *organizational impact, individual impact, user satisfaction.* *Organizational impact* and *individual impact* are derived from DeLone and McLean [8]. In this study, we adapt four items developed by DeLone and McLean [8]: tapping into individual productivity, task performance, time saving on the job, and individual effectiveness on the job related to information infrastructure. Six items from Thong et al [31] will be used to measure organizational impact. Since the costs and benefits of information infrastructure attributing to health care organizations' performance are hard to quantify and are not recorded in the form of objective data, these items will be treated as perceptual measures of organizational impact. Respondents were asked with a 7-point scale (1, strongly disagree, to 7, strongly agree) to indicate their perception of the degree to which the organization's information infrastructure systems contributed to the organization's impact in terms of staff productivity, operations efficiency, and improved decision-making. *User satisfaction*, on the other hand, will be measured by the definition, which is the extent of public sector being interdependent with other organizations. Similar to *organizational impact*, public impact will be measured by perceptions of individuals engaging in the public health care sector. Since the effectiveness of information infrastructure largely relies on the data in health

care organizations, the items of organizational impact can identify how individuals are affected by interdependency risks.

## V. CONCLUSION

This paper has proposed a framework for evaluation of mitigators of interdependent risks and the effect of interdependent risks on information infrastructure. This can prove to be an important means for increasing information infrastructure effectiveness, by identifying the potential risk mitigators. This framework provides a basis for future research to develop a comprehensive implementation guide of information infrastructure effectiveness in public healthcare sectors.

## ACKNOWLEDGEMENTS

Many thanks to Deepa Velu and Radhika Raghu for help with the manuscript.

## REFERENCES

- [1] P.S Anderson. "Critical Infrastructure Protection in the Information Age," in: *Networking Knowledge for Information Societies: Institutions & Intervention*, R. Mansell, Samarajiva, Rohan. and Mahan, Amy. (Eds.) (ed.), DUP Science, Delft, 2002.
- [2] N. Au, E.W.T. Ngai, and T.C.E. Cheng. "A critical review of end-user information system satisfaction research and a new research framework," *Omega*, Vol.30, No.6, p. 451, Dec 2002.
- [3] H. Barki., S. Rivard, and J. Talbot. "Toward an assessment of software development risk," *Journal of Management Information Systems*, Vol.10, No.2, p.203, 1993.
- [4] Blake, W.F. "Making Recovery a Priority," *Security Management*, Vol.36, No.4, p.71, 1992.
- [5] Committee, J.E. "SECURITY IN THE INFORMATION AGE: NEW CHALLENGES, NEW STRATEGIES," JOINT ECONOMIC COMMITTEE, UNITED STATES CONGRESS, Washington, D.C., p. Internet Address: <http://www.house.gov/jec>.
- [6] D. Compeau, C.A. Higgins, and S. Huff. "Social cognitive theory and individual reactions to computing technology: A longitudinal study," *MIS Quarterly*, Vol.23, No.2, p.145, 1999.
- [7] D.R. Compeau and C.A. Higgins. "Computer self-efficacy: Development of a measure and initial test," *MIS Quarterly*, Vol.19, No.2, p. 189, 1995.
- [8] W.H. DeLone, and E.R. McLean. "Information Systems Success: The Quest for the Dependent Variable," *Information Systems Research*, Vol.3, No.1, pp. 60-95, 1992.
- [9] W. Frun. "Cognitive components in risk perception," *Journal of Behavioral Decision Making*, Vol.5, No.2, pp.117-132, 1992.
- [10] E.J. Garrity and G.L. Sanders. *Information Systems Success Measurement* Idea Group Pub, Hershey, PA, 1998.
- [11] M. Gerber and R.V. Solms. "Management of risk in the information age," *Computers & Security*, Vol.24, No.1, p.16, 2005.
- [12] S. Hamilton, and N.L. Chervany. "Evaluating information system effectiveness part I: comparing evaluation approaches," *MIS Quarterly*, Vol.5, No.3, pp. 55-69, 1981.
- [13] O. Hanseth and K. Lyytinen. "Design Theory for Managing Dynamic Complexity in Information Infrastructures," 2005.
- [14] G. Heal and H. Kunreuther. "IDS Models of Airline Security," *The Journal of Conflict Resolution*, Vol.49, No.2, p.201, 2005.
- [15] G. Heal, and H. Kunreuther. "Modeling Interdependent Risks," Risk Management and Decision Processes Center, University of Pennsylvania 2006.
- [16] J.J. Jiang, G. Klein and R. Discenza. "Information system success as impacted by risks and development strategies," *IEEE Transactions on Engineering Management*, Vol.48, No.1, p.46, 2001..
- [17] D.G. Katehakis, S. Kostomanolakis, M. Tsiknakis, and S.C. O. "An open, component-based information infrastructure to support integrated regional healthcare networks," *International Journal of Medical Informatics*, Vol.68, pp.3-26, 2002.
- [18] N.N. Kraus and P. Slovic. "Taxonomic analysis of perceived risk: modeling the perceptions of individuals and representing local hazard sets," *Risk Analysis*, Vol.8, No.3, pp. 435-455, 1988.
- [19] H. Kunreuther and G. Heal. "Interdependent security," *Journal of Risk and Uncertainty*, Vol.26, No.2, p.231, 2003.
- [20] J. McDonald, J., J., C., and Marc Overhage, M.B., G. Schadow, L. Blevins, P.R. Dexter, B. Mamlin and the INPC Management Committee "The Indiana Network For Patient Care: A Working Local Health Information Infrastructure," *Health Affairs*, Vol.24, No.5, pp.1213-1220, 2005.
- [21] P. Meade. "Taking the risk out of disaster recovery services," *Risk Management*, Vol.40, No.2, p.20, 1993.
- [22] D. Mendonca, E.E. Lee and W.A. Wallace. "Impact of the 2001 World Trade Center Attack on Critical Interdependent Infrastructures," in: *IEEE International Conference on Systems, Man and Cybernetics*, 2004.
- [23] E. Nickolov "Critical Information Infrastructure Protection: Analysis, Evaluation, and Expectations," *INFORMATION & SECURITY. An International Journal*, Vol.17, pp.105-119, 2005.
- [24] J. Peerenboom, "Infrastructure interdependencies: Overview of concepts and terminology," Infrastructure Assurance Center, Argonne National Laboratory, Argonne, IL, p. [http://www.pnwr.org/pris/peerenboom\\_pdf.pdf](http://www.pnwr.org/pris/peerenboom_pdf.pdf).
- [25] A. Rai, S.S. Lang and R.B. Welker. "Assessing the validity of IS success models: An empirical test and theoretical analysis," *Information Systems Research*. Vol.13, No.1, p.50, 2002.
- [26] L. Raymond "Organizational Characteristics and MIS Success in the Context of Small Business," *MIS Quarterly*, Vol.9, No.1, p.37, 1985.
- [27] S. Rinaldi, J. Peerenboom and T. Kelly. "Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies," in: *IEEE Control Systems Magazine, IEEE*, , pp. 11-25, 2001.
- [28] P.B. Seddon. "A respecification and extension of the DeLone and McLean model of IS success," *Information Systems Research*, Vol.8, No.3, p.240, 1997.
- [29] S. Sirkemaa. "IT Infrastructure Management and Standards," Proceedings of the International Conference on Information Technology: Coding and Computing, IEEE Computer Society Washington, DC, USA, 2002.
- [30] Slovic, P., and Monahan, J. "Probability, danger, and coercion," *Law and Human Behavior* (19:1) 1995, pp 49-65.
- [31] Thong, J.Y.L., Yap, C.-S., and Raman, K.S. "Top management support, external expertise and information systems implementation in small businesses," *Information Systems Research* (7:2) 1996, p 248.
- [32] US Dep. Energy, O.C.I.P. "Critical infrastructure interdependencies: impact of the September 11 terrorist attacks on the World Trade Center (a case study)," Rep. US Dep. Energy, Off. Crit. Infrastruct. Prot., Washington, DC.