Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2008 Proceedings

Americas Conference on Information Systems (AMCIS)

2008

Perceived Risk and Resilience in the Face of Natural Disasters: A Study of Hospital

Insu Park
SUNY - Buffalo, insupark@buffalo.edu

Raj Sharman
SUNY - Buffalo, rsharman@buffalo.edu

H. Raghav Rao
SUNY - Buffalo, mgmtrao@buffalo.edu

Shambhu J. Upadhyaya
SUNY - Buffalo, shambhu@cse.Buffalo.EDU

Perceived Risk and Resilience in the Face of Natural Disasters: A Study of Hospital Information Infrastructure Systems: Research in Progress

Insu Park
State University of New York at Buffalo
Insupark@buffalo.edu

Raj Sharman
State University of New York at Buffalo
rsharman@buffalo.edu

H. Raghav Rao
State University of New York at Buffalo
mgmtrao@buffalo.edu

Shambhu J. Upadhyaya
State University of New York at Buffalo
shambhu@cse.buffalo.edu

ABSTRACT

Though hospital information systems have been extensively studied as a technology and there is now a growing body of literature in the area of infrastructure interdependencies, the dependencies of civil and built infrastructure on the health care information infrastructure (HII) is understudied. In particular, there is no study to our knowledge that addresses the issue of Hospital Information Infrastructure in the context of disasters. This study explores how an organization's information systems infrastructure is affected by disasters and examines the relationship between organizational resilience and information infrastructure effectiveness by using conceptual model.

KEY WORDS

A field quasi-experiment, information infrastructure, disasters, information infrastructure effectiveness, Research in progress

INTRODUCTION

The worst snow storm (October 12-13, 2006) in Buffalo's history had resulted in downed trees, lost power and both snow and flooding. The unprecedented mix of a warm Lake Erie and rapidly dropping air temperatures created nearly two feet of extremely heavy wet snow that fell on thousands of trees in full fall foliage. The sudden snow storm was also the cause of several accidents. Every hospital serving the Western New York area was at or near capacity, with patients in beds and more coming through the doors 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. While the intake rate ratcheted upwards, the surge was also due to the inability of hospital to discharge patients due to concerns stemming from lack of electricity, unplayable roads and the potential loss of a clean water supply as the water pumping stations had lost power. In particular, individuals in the public health sector might have been psychologically affected by the fear that the infrastructure may not function well. Consequently, the potential impact resulting from the physical risks led some of them to work insecurely and ineffectively.

This research explores the effect of perceived risks and perceived resilience on information infrastructure effectiveness and how disasters affect the way people evaluate the information infrastructure effectiveness in hospital contexts. By applying the field quasi-experimental design, we propose a model that attempts to explain people's perception of risks, information assurance and information infrastructure in the context of hospitals.

This study makes a contribution to the literature on information infrastructure and risk management. First, by providing a detailed description of the nature of interdependency risks, it contributes to better understanding of perceived risks in infrastructural disasters. Second, it explores how the information infrastructure effectiveness can be enhanced by identifying and describing perceived dependency risks.

This paper is organized as follows. The relevant literature on health care information infrastructure is discussed in the first section. Next, hypotheses are presented. The proposed methodology for the analysis is contained in the methods section, and the conclusion.

LITERATURE REVIEW

Hospital Information Infrastructure (HII)

The term *Information infrastructure* has been widely used only during the last couple of decades. According to Hanseth et al. (1998), *Information infrastructure* consists of an inter-connected collection of computer networks, but with a heterogeneity, size, and complexity. 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, nature and content of its components and connections" (2005). In addition, Sirkemma (2002) defines an IT infrastructure as a combination of technology, hardware and software that provide services to a range of applications and users, and is usually managed by the IT-group. On the other hand, a corporate/regional/national healthcare information infrastructure (HII) is concerned with bringing timely health information to, and aiding communication among, those making health decisions for themselves, their families, their patients, and their communities (Katehakis DG Kostomanolakis S Tsiknakis M and SC. 2002). 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[1].

Infrastructure Dependent Risks

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 (Saxton 2006). 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 their efforts may be undermined by failures elsewhere. According to this, infrastructure dependent 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.

Infrastructure dependent risks with respect to the information infrastructure are closely related to risks among interrelated critical infrastructures (external dependent risks) or internal components (internal dependent 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).

In this study, we use two different concepts to explain risks arising from the interdependency of infrastructures. External dependent risks (EDR) 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 (Mendonca Lee and Wallace 2004). Thus, EDR may increase physical damage and are difficult to control by an organization.

On the other hand, internal dependent risks (IDR) can be caused by the components used in building an infrastructure in an organization. For the interdependencies within an organization, each internal infrastructure may suffer from the disruptions of the other infrastructures. Information infrastructure in an organization contains several components such as, platforms, applications, technologies, and humans. Compared to EDR, the conflicts among these components in IDR reduce the effectiveness of an organization's infrastructure. 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/ data center and medical facility. Each infrastructure faces a certain risk or uncertainty of a disruption that damages it, and also a probability that such an attack would disrupt the activities of the other infrastructure. Therefore,

[1] Centre for Health Information Infrastructure, "HealthScape' 95-Charting Health Information Infrastructure". Dec. 95

infrastructure dependent risks in an organization can have devastating impacts on all parts of the organization. These negative externalities are an important feature of infrastructure dependent risks (Heal and Kunreuther 2006).

Information Assurance

Information assurance "protects and defends information and information systems infrastructure by ensuring their availability, integrity, identification and authentication, confidentiality, and non-repudiation."(DoD 1998). Information assurance provides a view of information protection that includes defensive measures in all three states-processing, storage, and transmission (Schou and Trimmer 2004). This includes providing for the restoration of information infrastructures by incorporating protection, detection, and reaction capabilities. Therefore, information infrastructure must be defended not only for national security but for legal reasons such as FERPA[2] and HIPPA[3]. Accordingly, the increasing need for Information Assurance (IA) of government, commercial and individual information systems stems from the growing number of threats with their increasing capabilities of inflicting damage upon information systems. *In this study, we define information assurance as the degree to which employees perceive their information security and privacy to be assured.*

Resilience Theory

Research on resilience has been conducted in disaster contexts related to several topics such as business coping behavior and community response (Tierney 1997), nonlinear adaptive response of organizations (Comfort 1999), and systems performance (Petak 2002). Resilience is defined as the capacity of an entity or system to maintain and renew itself particularly in the presence of stressors. Enterprise resilience refers to the ability and capacity to withstand systemic discontinuities and adapt to new risk environments (Starr Newfrock and Delurey 2003), or ability or capacity of a system to absorb or cushion against damage or loss (Rose 2004). This concept is also consistent with three aspects that Bruneau et al. (2003) mentions: Reduced failure probability, reduced consequences from failure, and reduced time to recovery. As 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.

Since resilience also refers to post-disaster conditions, which are distinguished from pre-disaster activities that reduce potential losses through mitigation, key concepts must include the ability of a system to respond and recover from an accident. Further, resilience should allow an organization to adapt to new organizational structures after the disaster event (Dalziell and McManus 2004).

In this study, we define resilience as the perceived capability of the information infrastructure to bounce back over time in the context of an emergency. Since resilience can be enhanced by adopting an approach that facilitates technical and psychological preparedness and by developing an adaptable response capability (Paton Flin and Violanti 1999), it is critical to develop a comprehensive measure of factors mitigating risks from disaster stress, and identity interventions to enhance the degree of organizational resilience and effective performance in organizations in disaster context.

Information Infrastructure Effectiveness

In this study, information infrastructure effectiveness refers to the extent to which the information infrastructure is perceived to contribute to achieving organizational goals. Our conceptual framework is based on the information systems success framework from DeLone and McLean (1992). 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 (Rai Lang and Welker 2002). 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 (Hamilton and Chervany 1981; Raymond 1985) measured by diverse constructs that are able to tap into the concept properly (DeLone et al. 1992; Rai et al. 2002; Seddon 1997). Based on the review of previous literature, this study assesses Information infrastructure effectiveness with three factors: *individual impact*, *organizational impact, and organizational resilience*. Such factors have been widely accepted among IS researchers as reliable constructs (See DeLone et al. 1992; Rai et al. 2002; Thong Yap and Raman 1996).

According to DeLone et al. (1992), 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 (Rai et al. 2002), net benefits (Seddon 1997), 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 (DeLone et al. 1992; Hamilton et al. 1981).

---

[2] The Family Education Rights and Privacy Act
[3] The Health Insurance Portability and Accountability Act

RESEARCH MODEL AND HYPOTHESIS DEVELOPMENT

Based on the preceding statements, a research model is proposed that aims to understand and prescribe how interdependency risks affect the information infrastructure effectiveness (Figure 1). In this model, infrastructure effectiveness is determined by external/internal interdependency risks.

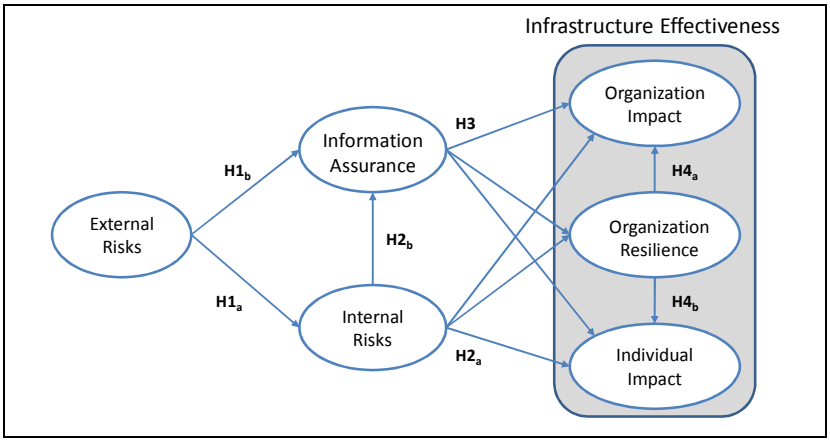

Figure 1. Research Model

The Effect of Perceived Risk

As for any risk, regardless of whether it results 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 (Gerber and Solms 2005). In a health care organization, the more the stakeholders perceive external dependent risks caused by disaster, the more they perceive internal dependent risks and information assurance as well. 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.

Hypothesis 1a*: External interdependency risks are positively related to internal interdependency risks.*
Hypothesis 1b*: External interdependency risks are negatively related to information assurance.*

In addition, internal dependent 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 (Barki Rivard and Talbot 1993; Jiang Klein and Discenza 2001). According to Jiang et al (2001), behavioral and technology-related risks can negatively affect information systems' success directly or indirectly. Thus, our Hypotheses regarding the relationship between interdependency risks and the information infrastructure's effectiveness are as follows,

Hypothesis 2a: *Internal interdependency risks are negatively related to HII effectiveness.*
Hypothesis 2b: *Internal interdependency risks are negatively related to perceived information assurance.*

The Effect of Information Assurance

Infrastructure dependent risks from information infrastructure are prone to be vulnerable due to flaws in the information or network security. A fundamental cause of many of risks is in the variety of ways that unethical individuals and/or groups can utilize digital technologies to engage in inappropriate, criminal or other illegal online activities (Vlasti and Paul 2004). According to Ezingeard et al (2005), information assurance (IA) can create positive benefits. For example, IA can not only impact the organization's ability to deliver goods and services more efficiently or effectively but also facilitate improvement in the quality, integrity, availability of information (see Ezingeard et al. 2005). In this study, information assurance, especially, security and privacy issues play a role for enhancing effectiveness of information infrastructure by reducing the impact of interdependent risks. The Hypotheses related to IA are

Hypothesis 3a: *Information assurance will positively affect Information infrastructure effectiveness.*

The Effect of Resilience

As O'Rourke et al (2003) found in their study, New York City was able to recover relatively quickly after September 11 because of its institutional resilience. According to Dalziell et al. (2004) resilience should allow an organization to adapt to

new organizational structures after the disaster event. According to Stajkovic (2006), when workers have resilience which composes confidence as a higher construct, their performance would be higher and their knowledge regarding tasks would be effectively facilitated by enabling their existing potential by belief that one can handle what needs to be done. Therefore,

> ***Hypothesis 4:*** *Perceive Resilience will positively affect organization (4_a) and individual (4_b) impact on information infrastructure.*

The Effect of Disasters

People construct their own reality and evaluate risks according to their subjective perceptions. According to the availability heuristic (Tversky and 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 increase perceived risks. This type of intuitive risk perception is based on information about the source of a risk, the psychological mechanisms for processing uncertainty, and earlier experience of danger. Studies show that past experience with disasters is an important factor in influencing people's perceptions of hazards (See, Baumann and Sims 1978; Jackson 1981; Weinstein 1989).

In this study, we argue that an employees' evaluation process appears differently depending on the existence of disasters. In disaster context, employees would relatively be more concerned that their information infrastructure would not be operated properly in performing their works. In disaster context, perception of risk in general reduces an employees' confidence toward the information infrastructure, This leads to the hypothesis of the study:

> ***Hypothesis 5****: Hospital information infrastructure will be evaluated differently by employees depending on the presence or absence of a disaster.*

METHODS

Participants and Procedures

Field quasi-experimental research (one-group pretest-posttest design)(Cook and Campbell 1975) using a survey will be conducted at hospitals in buffalo area. Hospitals employees will be asked to complete the survey which is composed of repeated-measure items. The survey contains an alternative treatment design with a pre-test, treatment presentation, and post-tests. There will be no control group in this study in order to keep the consistency of participants' perceptions directed toward a disaster and contexts. In order to identify the impact of a disaster on the relationships among the factors, we will use a simple stimulant treatment to the same subjects to make them recall the experiences surrounding the October storm (see figure 2)[4].

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 2. Treatment

[4] Since October storm (Oct. 18, 2006) occurred one and half years ago, participants might not remember the incident itself or the impact. In order to check how the treatment works, we will ask questions about how much they remember and how much the treatment (i.e., the picture and news) helps them spark recall.

The survey questionnaire consists of two steps: first, participants will be asked to answer the questions on perceived risks and information infrastructure effectiveness without any clue to disasters, second, a picture and news article will be used as a stimulus and will be presented to the participants to recall the October storm which occurred in buffalo. Third, after providing the treatment, the participants also will be asked to answer the exact same questions. Since participants live in the buffalo area, they knew how the storm affected their everyday life.

Measures

Information assurance (5) and external (8)/internal (3) dependent *risks* will be measured by items that we developed as part of our study. In order to identify whether the disaster on infrastructure components in a hospital occurs, we use multidimensional factors: *organizational impact, individual impact, and resilience. Organizational impact* and *individual impact* are derived from DeLone et al (1992). In this study, we adapt four items developed by DeLone et al. (1992). Six items from Thong et al (1996) will be used to measure organizational impact. Finally, we created a new construct, resilience perception which focuses on the ability and capacity to withstand systemic discontinuities and adapt to new risk environments (Starr et al. 2003), as another dimension of information infrastructure. These items are based on (Starr et al. 2003) and are adapted.

Data Analyses

Partial Least Squares (PLS), as implemented in PLS Graph version 3.0, will be used for data analysis. PLS Graph provides the ability to model latent constructs even under conditions of non-normality and small- to medium-size samples (Chin 1998a) and multiple analysis which compare two groups with path coefficients.

RESEARCH PROGRESS AND CONCLUDING REMARKS

In this study, we investigate not only the mechanisms that external perceived risks affect the information infrastructure effectiveness through perceived internal risks and information assurance, but we also examine the impact of a disaster on the relationship that perceived risks affect information infrastructure effectiveness including resilience in a hospital context. The study focuses on the issue of how hospital employees perceive the information infrastructure as effective tools to achieve their performances when they confronted disasters and whether the organizational resilience positively affects information infrastructure effectiveness. By finding the impacts of the disaster on the relationship between perceived risks, information assurance and information infrastructure effectiveness: resilience, organization impact, individual impact, we will find the evidence to support or not support several hypotheses.

To ensure the face and content validity of the measures, we reviewed the instrument with faculty members who are experts in scale development. To understand how stakeholders perceive their ability to recover from disasters and what determines their risks and resilience, after clarifying the concepts and developing initial items in the initial version of the survey, we employed in-depth interviews with IT executive members of hospitals in the Buffalo area.

A pilot study with five IT professionals in hospitals will be conducted to validate that the survey is clear and concise and that the items portray their intended meaning. Feedback will be also sought on the survey's length, its overall appearance, and participants' expected reaction to its receipt in the mail.

Based on the feedback from the pilot study, we will further refine some of the measures. Responses to the final questionnaires will be collected from stakeholders in hospitals in Buffalo area. Participation in this study will voluntary and all data will be gathered in an anonymous manner. Once the validity of the responses will be verified, partial least square (PLS) analysis will be employed to test our research hypotheses on the data collected.

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

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

2. Barki, H., Rivard, S., and Talbot, J. "Toward an assessment of software development risk," *Journal of Management Information Systems* (10:2) 1993, p 203.

3. Baumann, D.D., and Sims, J.H. "Flood insurance: Some determinants of adoption," *Economic Geography* (54) 1978, pp 189-196.

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

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

6. Chin, W.W. "The Partial Least Squares Approach to Structural Equation Modeling," in: *Modern Methods for Business Research,* G.A. Marcoulides (ed.), London, 1998b, pp. pp. 295-336.

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

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

9. 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.

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

11. Dalziell, E.P., and McManus, S.T. "Resilience, Vulnerability, and Adaptive Capacity: Implications for System Performance," in: *International Forum for Engineering Decision Making*, Stoos, Switzerland, 2004.

12. DeLone, W.H., and McLean, E.R. "Information Systems Success: The Quest for the Dependent Variable," *Information Systems Research* (3:1) 1992, pp 60-95.

13. DoD "Joint Doctrine for Information Operations," in: *joint pub 3-13,* D.o. Defense (ed.), 1998.

14. Ezingeard, J.-N., McFadzean, E., and Birchall, D. "A MODEL OF INFORMATION ASSURANCE BENEFITS," *EDPACS* (32:11) 2005, p 1.

15. Gerber, M., and Solms, R.v. "Management of risk in the information age," *Computers & Security* (24:1) 2005, p 16.

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

17. Hanseth, O., and Lyytinen, K. "Design Theory for Managing Dynamic Complexity in Information Infrastructures," 2005.

18. Heal, G., and Kunreuther, H. "Modeling Interdependent Risks," Risk Management and Decision Processes Center, University of Pennsylvania 2006.

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

20. Jiang, J.J., Klein, G., and Discenza, R. "Information system success as impacted by risks and development strategies," *IEEE Transactions on Engineering Management* (48:1) 2001, p 46.

21. Katehakis DG, Kostomanolakis S, Tsiknakis M, and SC., O. "An open, component-based information infrastructure to support integrated regional healthcare networks," *International Journal of Medical Informatics* (68) 2002, pp 3-26.

22. Mendonca, D., Lee, E.E., and Wallace, W.A. "Impact of the 2001 World Trade Center Attack on Critical Interdependent Infrastructures," in: *IEEE International Confi?rence on Systems, Man and Cybernetics*, 2004.

23. Paton, D., Flin, R., and Violanti, J. "Incident response and recovery management," in: *Posttraumatic Stress Intervention: Challenges, Issues and Perspectives,* J.M. Violanti, D. Paton and C. Dunning (eds.), Charles C. Thomas, Springfield, IL., 1999.

24. Petak, W. "Earthquake resilience through mitigation: a system approach," in: *The International Institute for Applied Systems Analysis*, Laxenburg, 2002.

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

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

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

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

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

30. Sirkemaa, S. "IT Infrastructure Management and Standards," Proceedings of the International Conference on Information Technology: Coding and Computing, EEE Computer Society Washington, DC, USA, 2002.

31. Stajkovic, A.D. "Development of a Core Confidence-Higher Order Construct," *Journal of Applied Psychology* (91:6) 2006, p 1208.

32. Starr, R., Newfrock, J., and Delurey, M. "Enterprise Resilience: Managing Risk in the Networked Economy," in: *Strategy & Business*, 2003.

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

34. 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.

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

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

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

38. Weinstein, N.D. "Effects of personal experience on selfprotective behavior," *Psychological Bulletin* (105) 1989, pp 31-50.