Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2009 Proceedings

Americas Conference on Information Systems (AMCIS)

2009

Measuring Effectiveness of Information Systems Security: An Empirical Research

Adolfo S. Coronado
University of Texas at El Paso, adolfoc@miners.utep.edu

M. Adam Mahmood
University of Texas at El Paso, mmahmood@utep.edu

Seppo Pahnila
University of Oulu, seppo.pahnila@oulu.fi

Edimara M. Luciano
Pontifical Catholic University of Rio Grande do Sul, eluciano@pucrs.br

Measuring Effectiveness of Information Systems Security: An Empirical Research

Adolfo S. Coronado
University of Texas at El Paso
adolfoc@miners.utep.edu

M. Adam Mahmood
University of Texas at El Paso
mmahmood@utep.edu

Seppo Pahnila
University of Oulu, Finland
seppo.pahnila@oulu.fi

Edimara M. Luciano
Pontifical Catholic University of Rio Grande do Sul, Brazil
eluciano@pucrs.br

ABSTRACT

The objective of the present research is to put forth a theoretical model that measures information systems security effectiveness in minimizing security breaches. Very few studies were undertaken in this area. The model includes a number of literature-supported constructs. A number of hypotheses based on the influence of these constructs on IS security effectiveness are presented. These hypotheses are grounded using the appropriate literature. In the next phase of the study, we intend to revise and empirically validate the model using a pilot study utilizing a number of practitioners from Brazil, Finland, and the United States. The data obtained from the pilot study will be used to make improvements on the initial instrument designed for the study. In the third stage of the research a large sample of data will be collected from the aforementioned countries and a regression analysis will be conducted on the data to investigate which constructs influence IS security effectiveness.

Keywords

Information systems security; information systems security effectiveness; measures of effectiveness

INTRODUCTION

Information security incidents businesses have confronted with within the last few years have significantly increased. In 1997-1999 surveys, 37-50% of the organizations were victims of information security breaches (Thomson and von Solms, 1998). The same numbers in the years 2001-2003 ranged from 75% to 91% (Gordon and Loeb, 2002; Hinde, 2002). According to 2008 CSI Computer Crime & Security Survey, the average loss per respondent (144 respondents answered) caused by various types of computer security incident was $288,618, down from $345,005 in 2007 but up from the low of $167,713 in 2006 (Richardson, 2008). The most expensive type of breaches was related to financial frauds. Most of the computer criminals are motivated by money more than anything else (Richardson, 2008). CSI respondents estimated that their financial losses were mostly due to attacks from outside the organization being 36% in 2007 and 51% in 2008. They reported that the most common incidents or computer attacks were caused by viruses (50%), insider abuse (44%), laptop theft (42%), and unauthorized access to systems (29%).

The high levels of connectivity, unencrypted Internet communications, and the availability of sophisticated hacking tools have created unprecedented opportunities for hackers to survive and flourish (Hu, Hart and Cooke, 2007). In order to cope with increased IS security threats, businesses are paying more attention to IS security breaches. More and more research studies are also being conducted on several aspects such as technical (Huang, Hu and Behara, 2008), economies (Anderson and Moore, 2006), human (Liginlala, Simb and Khansac, 2009; Ng, Kankanhalli and Xu), and social (Dhillon and Backhouse, 2001; Dourish and Anderson, 2006). Hu et al. (2007) suggested that information systems security defenses created based on an understanding of organizational factors should provide a significant defense against these threats.

Straub (1990) developed a pioneering study on the effectiveness of information security. The author claimed that the “investment in IS security results in more effective control of computer abuse”. Goodhue and Straub (1991) put forth a number of IS security effectiveness measures based on an understanding of “abusive situation”. Kankanhalli, Teo, Tan and

Wei (2003) developed a model of IS security effectiveness based on the influence of organizational size, top management support, and deterrent efforts on information security effectiveness.

The objective of the present research is to put forth a theoretical model that measures information security effectiveness in relation to severity of information security threats a business encounters, its vulnerability to these threats, risks it takes by not securing its information systems, trusts its business partners have on its security apparatus, and privacy afforded to the business partners by this apparatus. The research also provides a number of hypotheses based on this model. The importance of the present research stems from the fact that very few studies on the effectiveness of information systems security using organizational factors have been conducted in the past.

The manuscript is structured in the following manner: the next section provides a literature review that describes the constructs used in the present research and the literature sources for these constructs. This is followed by a description of the research model and the corresponding hypotheses based on the model. The manuscript concludes by providing a description of future research studies and implications for these studies.

LITERATURE REVIEW

It is our contention that a comprehensive and integrated model is needed to measure IS security effectiveness. It is our belief that the model, as stated earlier, should include severity, vulnerability, risks, trust, and privacy constructs (see Figure 1). In what follows, the literature support for each of the constructs and justification for including these in the model are provided. The constructs and references for the constructs are provided in Table 1.

	ISS Effectiveness	Severity of threats	Vulnerability	Risks	Privacy	Trust
Allen (1993)						
Anderson and Moore (2006)			X			
Arora et al. (2004a)			X			
Arora et al. (2004b)			X			
Axelrod and Newton (1991)			X			
Baskerville and Heje (2004)			X			
Cavusoglu et al. (2008)		X	X	X		
Cho (2006)				X		X
De Lone and McLean (1992)						X
Farahmand et al. (2004)		X	X			
Garg et al. (2003)		X				
Goodhue and Straub (1991)	X					
Gordon and Loeb (2002)			X			
Granovetter (1985)						X
Hann et al. (2007)					X	
Hass et al. (1975)		X				
Hui et al. (2007)					X	
Johnson and Goetz (2007)				X		
Jøsang et. al (2007)						X
Kankanhalli et al. (2003)	X					X
Kesh and Ratnasingam (2007)						
Komiak and Benbasat (2005)						X
Kumar et al. (2008)				X		
Liberman and Chaiken (1992)			X			
Pavlou et al. (2007)						X
Rogers and Prentice-Dunn (1997)		X	X			
Rose (2006)					X	
Rousseau et al. (1998)						X
Seydel et al. (1990)		X				
Singh and Sirdeshmunkh (2000)						X
Son and Kim (2008)					X	
Stephan (1990)			X			

Straub (1990)	X					
Sun et al. (2006)				X		
Telang and Wattal (2007)			X			

Table 1. Constructs Literature Review

Information Systems Security Effectiveness

The effectiveness in information systems security refers to the results of the actions taken and the alignment of these actions to the expected outcome. According to Straub (1990) security effectiveness represents the ability of IS security measures to protect against unauthorized or deliberate misuse of IS assets.

In order to understand the effectiveness and importance of IS Security, the managers involved in IS security must be able to recognize information security threats and take the actions that are effective in mitigating these threats. This is a need mentioned by Kankanhalli et al. (2003) because managers may be skeptical about IS security effectiveness due to the difficulty in evaluating the benefits derived from these security measures. Goodhue and Straub (1991) suggest the use of a perceptual measure of IS security effectiveness as an alternative to inaccurate quantitative aspects of IS security abuses.

Straub (1990) conducted a pioneering study on the effectiveness of information security within an economic context. The findings of the research demonstrated that IS security investments result in a more effective control of computer abuse. Kankanhalli et al. (2003) developed an integrative model of IS security effectiveness and empirically tested the model. The model analyzes the influence of organizational size, top management support and industry type, deterrent efforts, deterrent severity, and preventive efforts on information security effectiveness.

Vulnerability and Severity

Perceived vulnerability and perceived severity constructs in the model came from Roger's Protection Motivation Theory (PMT). PMT had originated in health sciences, aimed at motivating people to avoid unhealthy behavior through fear appeals (Rogers, 1975; Rogers, 1983). Perceived vulnerability and perceived severity, in the context of the present research, are used to measure how susceptible an organization is to IS security breaches and potential harms (e.g., legal and financial ramifications) that may be caused by these breaches. A number of research studies have addressed the issue of vulnerability and severity in the context of IS security. Gordon and Loeb (2002), for example, define vulnerability as a "threat that once realized (i.e., an attack) would be successful". Gordon and Loeb (2002) suggest that market often rewards vendors for putting out low quality software with in adequate security mechanisms in order to be the first to market and receive the first mover's advantage. They also claimed that lack of legal liability and high switching costs decrease vendors' real incentives to put resources into high quality and secured information systems.

Telang and Wattal (2007) suggest that vulnerability announcements have a negative and significant effect on vendors' market value. They found that vendors' loss was caused by the stock market's negative reaction to the news of vulnerability announcements (Telang and Wattal, 2007). They also found that losses are correlated with the severity; the more severe vulnerability is the higher stock price losses are. Arora et al. (2004a) found that instant vulnerability disclosure attracts hackers and leaves users defenseless against these attackers. Organizations, therefore, report vulnerability discovers only to vendors and keep their discover secret to rest of the world allowing enough time for vendors to patch their software (Arora et al., 2004b).

Anderson and Moore (2006) pay attention to consequences of the vulnerabilities. They suggest that "systems are particularly prone to failure when the person guarding them is not the person who suffers when they fail.", and that insecure software dominates markets because most users cannot distinguish secured software from unsecured ones. The authors also suggest that vendors are capable of designing more secure software but they have little incentive to do so since first to market is more important. This finding is consistent with the finding of Baskerville and Heje (2004). Baskerville and Heje (2004) suggest that time pressure is one of the most important issues in software development. Companies try to minimize time-to-market. The authors found that in most firms quality was negotiable due to time pressure (Baskerville and Pries-Heje, 2004).

According to Cavusoglu (2004), information security should be perceived as value creator that supports business rather than as a cost of doing business. Assessing the costs of information security breaches is problematic because costs can be both tangible and intangible. Some breaches can be measured in money but some assets, for example the value of information, documented or intellectual, are difficult to assess (Cavusoglu et al., 2004; Farahmand, Navathe, Sharp and Enslow, 2004). On the other hand, although information security breaches can be severe, security is still hard to sell to managers; they want to see evidence that investing in information security is worthwhile (Cavusoglu et al., 2004). When assessing the information systems severity, one should take into consideration the sensitivity of information. Market reaction can be significantly negative when the breach is directed to confidential data but the reaction can be insignificant when the breach is directed to non-confidential data (Farahmand et al., 2004). Thus, the most severe financial losses are involved in unauthorized access to confidential information (Farahmand et al., 2004). Market reactions also differ depending on various types of information security breaches. They react most severely to credit card information theft due to possibility of third-party liability (Garg, Curtis and Halper, 2003).

Risk

Sun, Srivastava and Mock (2006) define risk as the "plausibility of information not being secure". Johnson and Goetz (2007) indicate that risks and businesses are inseparable (Sun et al., 2006). Organizations are dedicating more time and attention to risks management because of the "new generation of threats which are often difficult to detect and nearly impossible to assess their long-term consequences" (Johnson and Goetz, 2007). In information systems, risks are probably more studied because it is one of the basic premises of information security. Information security is getting increasing attention among corporate managers because of increased security breaches.

Companies, seeking to avoid catastrophic consequences, have been developing mechanisms for analysis of risks. Sun et al. (2006) identifies risk analysis as a "critical step for management of Information Systems Security (ISS)". The author proposes a model for risk assessment, providing "a way to assess the cost/benefit of maintaining controls to counterbalance the threats". The evaluation of risks is, however, not a simple activity because threats and vulnerabilities become more complex. Other variables such as trust, vulnerabilities, and privacy will also need to be reviewed. Also involved with risks analysis are disaster recovery, risks countermeasure and plans "to mitigate possible damage due to security attacks" (Kumar, Park and Subramaniam, 2008).

Trust

Trust has long been an important subject in situations that involved uncertainty and authority or caution with opportunism (Cho, 2006). Rousseau et al. (1998) define trust as a psychological state that understands the intention to accept vulnerabilities based on expectations of the intentions or behaviors of other. There are two interpretations in this regards: first, the trust is related to positive expectations about the intentions or behavior (Singh and Sirdeshmukh, 2000). Second trust is related to one's characteristics. Trust is not as easy to conceptualize (Komiak and Benbasat, 2006) and is a little confusing because the term is used with different meanings (Jøsang, Ismail and Boyd, 2007). In ISS, trust represents one's faith in the security policies, rules and procedures and this faith has a significant impact on the attitude towards the data and systems of the company. If a company, for example, trusts the information systems security of another company, it may accept a contract for mutual interchange of information between the two companies.

Granovetter (1985) explains that trust plays an important role in relationships among companies with recognized reputations. This is especially true when businesses are exposed to the risk of an opportunistic behavior especially in the context of uncertainty and incomplete information. Cho (2006) did a study about the roles of trusts and risks in information-oriented online services and online media, identifying the influence of perceived use, perceived usefulness, compatibility, perceived risk with online media, and online services. Their findings confirmed that there is a positive relationship between trust in online services and customers' attitude toward adopting online services. The study of Jøsang et al. (2007) found a positive relationship between trust and reputation of a company.

Privacy

The discussion of privacy started by Aristotle when he differentiated the public life (political activities) and the private life (domestic activities) (Swanson, 1992). Judge Thomas Cooley's work entitled "The Elements of Torts" in 1873 gave a classic definition to the word privacy meaning the right of being in peace and left alone. Many others, after him, began to study privacy in other discipline such as sociology, law, communication, and health sciences.

In IS, privacy is frequently mentioned as the balance between the risks of supplying information by organizations and the benefits received from an end user's access to the organizations' information and services. The concern is if the companies share information with business partners, they take a risk of loosing confidentiality which may result in invasions of privacy. Many advances in IT in general and e-commerce in particular unfortunately facilitate this invasion (Rose, 2006).

Hui, Teo, Lee (2007)studied the value of privacy assurance by investigating the impact of privacy statements and privacy seals on electronic commerce consumers. They found, through a field experiment, "the existence of a privacy statement vis-à-vis a privacy seal induced more subjects to disclose their personal information". Another way of looking at privacy is related to an "individual's concern about losing control over his or her private information"(Rose, 2006). According to Rose (2006) ''privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others''

MODEL

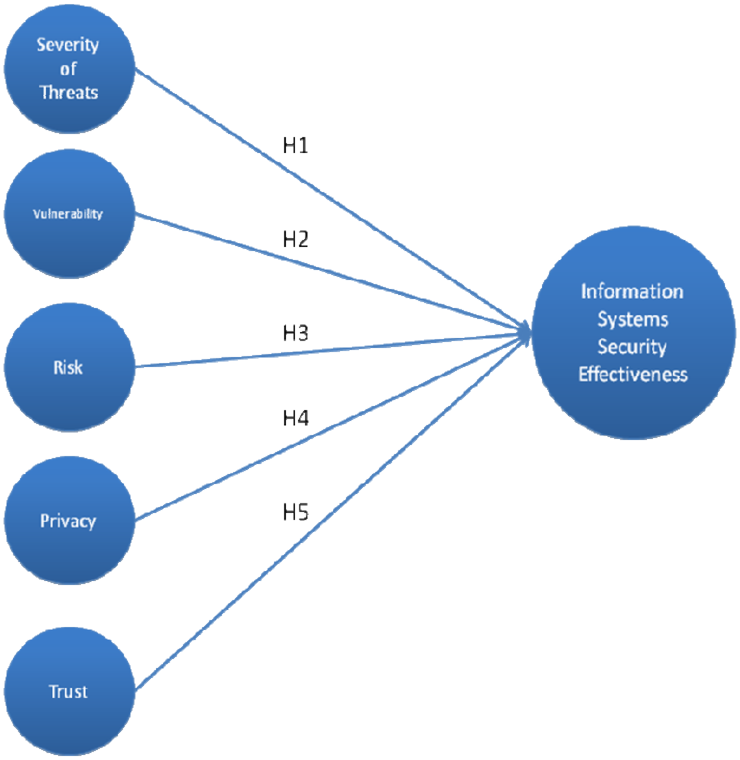

Figure 1: IS Security Effectiveness Model

HYPOTHESES

A Previous research in different areas presents consistent findings that show that decrease in perceived severity leads to lesser intentions to behave in a healthier manner (Rogers and Prentice-Dunn, 1997). More specifically, a number of studies in different areas had shown the importance of perceived severity towards deterring smoking (Hass, Bagley and Rogers, 1975), increasing safe-sex behavior (Ahia, 1990), breast self-examination (Seyde, Taal and Wiegman, 1990), and action against nuclear war (Allen, 1993). We, therefore, put forth the following hypothesis:

H1: Severity of increased potential IS security breaches will negatively impact Information Systems Security Effectiveness

Previous research in different areas also presents consistent findings that show that an increase in perceived vulnerability leads to greater intention to behave in a healthier manner (Rogers and Prentice-Dunn, 1997). More specifically, a number of studies in the past had shown that an increase in vulnerability can lead to increased testicular self-examinations (Stephan, 1990), action against nuclear war (Axelrod and Newton, 1991), and decreased caffeine consumption (Liberman and Chaiken, 1992). We, therefore, put forth the following hypothesis:

H2: Increased vulnerability to IS resources will negatively impact Information Systems Security Effectiveness

Kesh and Ratnasingam (2007) suggested that risk management is the key to controlling and mitigating risks to IT security. Sun et al. (2006) identified risk analysis as a critical step for managing IS security. Kumar et al. (2008) integrated risk analysis, disaster recovery, and counter measures to present a comprehensive model for information security. Wang, Chaudhury and Rao (2008) theorize that IS security investment employing system risk assessment has the potential to reduce the likelihood of security breaches. We, therefore, hypothesize

H3: Increased risks of potential security breaches will negatively impact Information Systems Effectiveness

Cho (2006) suggests, in their study on the role of trusts and risks in adoption of information-oriented online legal services, a lack of security feeling about a specific site may compromise the trust in all of the services offered by an online system. DeLone and McLean (1992) used this argument to study the relationship among user satisfaction, individual impact, and organizational impact in their study of system effectiveness. Pavlou, Liang and Xue (2007) studied the relationship between trust and the buyer's concerns about information security and concluded that trust mitigates the concerns about information security.

The lack of security feeling generates customers' mistrust on a system and this mistrust can compromise the feelings about the effectiveness of the information security. Trust or mistrust is feelings, like a perception, is translated into a point of view on information security. In accordance with this idea, potential users of a system must have faith in the effectiveness of information security before they use the system. We, therefore, put forth the following hypothesis:

H4: Increased mistrust will negatively impact Information Systems Security Effectiveness

According to Hann, Hui, Lee and Png (2007), "violation of privacy occurs when an organization, in its efforts to pursue the organization's objectives, collects, stores, manipulates, or transmits personal information unbeknownst to the individual". Privacy represents the people's right to keep their information secret and decide what information can be shared, when, how and with whom (Rose, 2006) as well as an obligation on the part of the companies to keep their customers' information safe. Because of this, people need privacy assurances from a company to have trust in its systems, web sites, or services (Hui et al., 2007).

The threat of privacy violations for the information security effectiveness is that it will be possible to obtain information that will allow one to access unauthorized information from the system that may be used later for social engineering (Hann et al., 2007; Son and Kim, 2008). In this sense, violation of privacy can contribute negatively to the effectiveness of information security. We put forth, based on this, the following hypothesis:

H5: Increased privacy violations will negatively impact Information Systems Security Effectiveness

FUTURE RESEARCH

In the next phase of the study, we intend to revise and empirically validate the model. In order to do so, a research instrument will be designed using the identified constructs utilizing a 7-point Likert-type scale, where 1 is the least and 7 is the highest. A content validity of the instrument will be done using a pilot study based on exploratory interviews with a number of practitioners from Brazil, Finland, and the United States. According to Straub (1989), concepts introduced independently by several participants can contribute to constructs validity and reliability. The data obtained from in the pilot study will be analyzed and used to make improvements on the questionnaire. The process will be driven by recommendations made by Churchill (1979) and Straub (1989)

In the second stage of the research a large sample of data will be collected again from Brazil, Finland, and the United States. The sample will include medium- and large-size organizations. Participants will be knowledgeable about information security policies, procedures, and breaches. The data will also be collected on respondents and organizations.

In the third stage, regression analysis will be conducted on the data to find out which independent variables affect IS security effectiveness. Realizing that there could be a possible inter-action effect among the various independent constructs, we will also conduct a SEM-type of analysis on the data.

The present research, once fully completed, will contribute in a number of ways: first it will help measure the effectiveness of information security apparatus, policies, and procedures in place in an organization. Our objective is to come up with elaborate measures and methodologies to help understand the effectiveness of the efforts put in securing information resources and help, in the process, prevent future IS security breaches. Second, it will contribute to our knowledge about information security effectiveness. Third, it will help organizations measure IS security effectiveness using the constructs used in the research and by observing interactions among these variables.

REFERENCES

1. Ahia, R.N. (1990) Compliance with safer-sex guidelines among adolescent males: application of the health belief model and protection motivation theory, *Journal of Health Education*, 22, 49-52
2. Allen, B.P. (1993) Frightening Information and Extraneous Arousal: Changing Cognitions and Behavior Regarding Nuclear War, *Journal of Social Psychology*, 133, 4, 459-467
3. Anderson, R., and Moore, T. (2006) The Economics of Information Security, *Science*, 314, 5799, 610-613
4. Arora, A., Krishnan, R., Nandkumar, A., Telang, R., and Yang, Y. "Impact of Vulnerability Disclosure and Patch Availability - An Empirical Analysis," 2004a.
5. Arora, A., Telang, R., and Xu, H. "Optimal Policy for Software Vulnerability Disclosure," 2004b.
6. Axelrod, L.J., and Newton, J.W. (1991) Preventing Nuclear War: Beliefs and Attitudes as Predictors of Disarmist and Deterrentist Behavior1, *Journal of Applied Social Psychology*, 21, 1, 29-40

7. Baskerville, R., and Pries-Heje, J. (2004) Short cycle time systems development, *Information Systems Journal*, 14, 3, 237-264

8. Cavusoglu, H., Cavusoglu, H., and Raghunathan, S. (2004) Economics of it Security Management: Four Improvements to Current Security Practices, *Communications of AIS*, 2004, 14, 65-75

9. Cho, V. (2006) A study of the roles of trusts and risks in information-oriented online legal services using an integrated model, *Information & Management*, 43, 4, 502-520

10. Churchill, G.A. (1979) A Paradigm for Developing Better Measures of Marketing Constructs, *Journal of Marketing Research*, 16, 1, 64-73

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

12. Dhillon, G., and Backhouse, J. (2001) Current directions in IS security research: towards socio-organizational perspectives, *Information Systems Journal*, 11, 2, 127-153

13. Dourish, P., and Anderson, K. (2006) Collective Information Practice: Exploring Privacy and Security as Social and Cultural Phenomena, *Human-Computer Interaction*, 21, 3; 3, 319-342

14. Farahmand, F., Navathe, S., Sharp, G., and Enslow, P. "Evaluating Damages Caused by Information Systems Security Incidents," 2004.

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

16. Goodhue, D.L., and Straub, D.W. (1991) Security concerns of system users: a study of perceptions of the adequacy of security, *Information and Management*, 20, 1, 13-27

17. Gordon, L.A., and Loeb, M.P. (2002) The economics of information security investment, *ACM Trans.Inf.Syst.Secur.*, 5, 4, 438-457

18. Granovetter, M. (1985) Economic action and social structure: The problem of embeddedness, *American Journal of Sociology*, 91, 3, 481-510

19. Hancock, B. (1999) 1999 CSI/FBI survey: Cyberattacks on the rise, *Computers & Security*, 18, 3, 188-189

20. Hann, I.-H., Hui, K.-L., Lee, S.-Y.T., and Png, I.P.L. (2007) Overcoming online information privacy concerns: an information-processing theory approach, *Journal of Management Information Systems*, 24, 2, 13-42

21. Hass, J.W., Bagley, G.S., and Rogers, R.W. (1975) Coping with the energy crisis: Effects of fear appeals upon attitudes toward energy consumption, *Journal of Applied Psychology*, 60, 6, 754-756

22. Hinde, S. (2002) Security surveys spring crop, *Computers & Security*, 21, 4, 310-321

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

24. Huang, C.D., Hu, Q., and Behara, R.S. (2008) An economic analysis of the optimal information security investment in the case of a risk-averse firm, *International Journal of Production Economics*, 114, 2, 793-804

25. Hui, K.-L., Teo, H.H., and Lee, S.-Y.T. (2007) The Value of Privacy Assurance: an Exploratory Field Experiment, *MIS Quarterly*, 31, 1, 19-33

26. Johnson, M.E., and Goetz, E. (2007) Embedding Information Security into the Organization, *Security & Privacy, IEEE*, 5, 3, 16-24

27. Jøsang, A., Ismail, R., and Boyd, C. (2007) A survey of trust and reputation systems for online service provision, *Decision Support Systems*, 43, 2, 618-644

28. Kankanhalli, A., Teo, H.-H., Tan, B.C.Y., and Wei, K.-K. (2003) An integrative study of information systems security effectiveness, *International Journal of Information Management*, 23, 2, 139-139

29. Kesh, S., and Ratnasingam, P. (2007) A Knowledge Architecture for IT Security, *Communications of the ACM*, 50, 7, 103-108

30. Komiak, S.Y.X., and Benbasat, I. (2006) The Effects of Personalization and Familiarity on Trust and Adoption of Recommendation Agents, *MIS Quarterly*, 30, 4, 941-960

31. Kumar, R.L., Park, S., and Subramaniam, C. (2008) Understanding the Value of Countermeasure Portfolios in Information Systems Security, *Journal of Management Information Systems*, 25, 2, 241-279

32. Liberman, A., and Chaiken, S. "Defensive Processing of Personally Relevant Health Messages," 1992.

33. Liginlala, D., Simb, I., and Khansac, L. (2009) How significant is human error as a cause of privacy breaches? An empirical study and a framework for error management, *Computer & Security*, 1-14

34. Ng, B.-Y., Kankanhalli, A., and Xu, Y. Studying users' computer security behavior: A health belief perspective, *Decision Support Systems*, In Press, Corrected Proof,

35. Pavlou, P.A., Liang, H., and Xue, Y. (2007) Understanding and Mitigating Uncertainty in Online Exchange Relationships: a Principal--Agent Perspective, *MIS Quarterly*, 31, 1, 105-136

36. Richardson, R. "Computer Crime & Security Survey (CSI)," pp. 1-30.

37. Rogers, R.W. (1975) A Protection Motivation Theory of Fear Appeals and Attitude Change, *Journal of Psychology*, 91, 1, 93-93

38. Rogers, R.W. "Cognitive and Physiological Processes in Fear Appeals and Attitude Change: A Revised Theory of Protection Motivation Theory," in: *Social Psychophysiology*, Guilford, New York, 1983.

39. Rogers, R.W., and Prentice-Dunn, S. "Protection Motivation Theory," in: *Handbook of Health Behavior Research I: Personal and Social Determinants*, NY: Plenum Press, New York, 1997, pp. 113-113.

40. Rose, E.A. (2006) An examination of the concern for information privacy in the New Zealand regulatory context, *Information & Management*, 43, 3, 322-335

41. Rousseau, D.M., Sitkin, S.B., Burt, R.S., and Camerer, C. (1998) Not so Different After All: a Cross-Discipline View of Trust, *Academy of Management Review*, 23, 3, 393-404

42. Seyde, E., Taal, E., and Wiegman, O. (1990) Risk-appraisal, outcome and self-efficacy expectancies: Cognitive factors in preventive behaviour related to cancer, *Psychology & Health*, 4, 2, 99-109

43. Singh, J., and Sirdeshmukh, D. (2000) Agency and Trust Mechanisms in Consumer Satisfaction and Loyalty Judgments, *Journal of the Academy of Marketing Science*, 28, 1, 150-150

44. Son, J.-Y., and Kim, S.S. (2008) Internet Users' Information Privacy-Protective Responses: a Taxonomy and a Nomological Model, *MIS Quarterly*, 32, 3, 503-529

45. Straub, D.W. (1989) Validating Instruments in MIS Research, *MIS Quarterly*, 13, 2, 147-169

46. Straub, D.W. (1990) Effective IS Security: An Empirical Study, *Information Systems Research*, 1, 3, 255-276

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

48. Swanson, J.A. (1992) The public and the private in Aristotle's political philosophy, Cornell University Press,

49. Telang, R., and Wattal, S. (2007) An Empirical Analysis of the Impact of Software Vulnerability Announcements on Firm Stock Price, *IEEE Transactions on Software Engineering*, 33, 8; 8, 544-557

50. Thomson, M.E., and von Solms, R. (1998) Information security awareness: educating your users effectively, *Information Management & Computer Security*, 6, 4, 167-173

51. Wang, J., Chaudhury, A., and Rao, H.R. (2008) A Value-at-Risk Approach to Information Security Investment, *Information Systems Research*, 19, 1, 106-120