Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2007 Proceedings

Americas Conference on Information Systems (AMCIS)

December 2007

A Meta-Analysis of Security Risk Theory Literature in IS from 2000-2006

April Adams
Mississippi State University

Gary Templeton
Mississippi State University

Natalie Campbell

A META-ANALYSIS OF SECURITY RISK THEORY LITERATURE IN IS FROM 2000 – 2006

April M. Adams
Mississippi State University
ama192@msstate.edu

Gary Templeton
Mississippi State University
gtempleton@cobilan.mstate.edu

Natalie Campbell
Mississippi State University
ncc34@msstate.edu

Abstract

Information Security Risk (ISR) has become an important focus in MIS literature as of late (Hale 1996; Hancock 2000; Jaamour 2005). However, few studies have attempted to analyze the types of articles being published as well as defining the area of research interest in security literature. The purpose of this study demarcates the historical and maturation of ISR research in MIS by a comprehensive appraisal of the published Security Risk articles in MIS journals over the last 6 years (2000-2006).

This paper addresses the following core questions about the material covered in the Security Risk articles: 1) What are the contexts of the research? 2) What are the methodologies used? 3) What types of factors affect the evolution of the topic? It is widely recognized that research that synthesizes existing studies to provide an overview of an emerging field is often scarce but extremely important to advance scholarly understanding of the current state of the field and to suggest future directions (Hovav et al. 2004). A number of areas for future research are presented, as well as a discussion on the findings in trends of evolution of the topic.

Keywords

Security, risk, meta-analysis

Introduction

Background

Research follows a natural progression in terms of topic evolutions. Some disciplines have concepts and ideas dating back to the Roman Empire. Other disciplines are relatively new. Management information systems, as a discipline, is a fairly young field. Consequently there are many research questions to be answered. Also, as a young discipline there are many opportunities for new research.

Security is considered to be a vital area of interest in Management Information Systems (2007; Campbell 2006; Cavusoglu et al. 2005; Straub et al. 1998). Disaster recovery, business continuity, and emergency planning are all exciting new areas available for research. Security has always been an important concern to most all information systems researchers. However recent events such as Hurricane Katrina, 9/11, and Enron scandals have been a catalyst for security interest in information system practitioners.

In order to establish how prepared an organization is for any type of security breach, risk must be determined and calculated. Typically, this determination of risk comes from a "risk analysis"(Erwin 2002). Once an organization has determined the level of risk, the organization moves into a "risk management" stage of planning (Braithwaite 2001). Managing the security risks associated with an organization's growing dependence on information technology is a continuing challenge. In particular, organizations have put forth great efforts to find competent ways to ensure that they fully understand the information security risks affecting their operations, so that they are able to implement appropriate controls to mitigate these risks. Assessing risk is one element of a broader set of risk management activities (Ohanley 2004). As reliance on computer systems and electronic data has grown, information security risk has joined the array of risks that governments and organizations must manage. There are various models and methods for assessing risk, and the extent of an analysis and the resources expended can vary depending on the scope of the assessment and the availability of reliable data on risk factors (Zuccato 2004). Because of this growing need in the practitioner area, academia has begun to study Security Risk.

Many different events have come together to force the issue of security on Information Systems personnel. The digital economy has added to this level of risk (Sambamurthy et al. 2005). Businesses and organizations are storing enormous quantities of data and information in databases for data mining, customer relationship management, enterprise resource management and other types of analysis or forecasting (Yihua Philip et al. 2005). Because of this shift from records and books to a digital era, our information has become a valuable asset.

While security has always been an important part of areas like national defense, events like September 11, the Tsunami in 2005, and Hurricane Katrina have made academics and practitioners alike realize that our information is at risk (Bhaskar 2006). Consequently the process of studying security and risk factors has evolved.

The authors of this paper have developed a framework for conducting Security Risk research. Several high level research questions were developed to allow the authors to decompose these questions further into low level more detailed questions. A multi-component approach was used to assess the data: the contexts of research, the level of analysis, the topics, and methods. We will address the questions and synthesis the results on each of the articles found in MIS journals over the last 6 years (2000 – 2006).

The core research questions the authors utilized are as follows: 1) What are the contexts of the research? 2) What are the methodologies used? 3) What types of factors are affecting the evolution of the topic? These questions were selected because it is possible to drill down and synthesize a richer understanding of the literature with these questions and their sub-questions.

Figure 1 presents an overview of the broad security issues that will be presented in this paper, which is organized as follows. The following section presents a broad overview of security risk topics studied in Management Information Systems, including a framework to structure the Security Risk topics, and research questions for this study. Second will be the methodology section, including the classification schemes and other findings used in the study. Next, we present investigation results to answer the research questions. The final section offers possibilities of future research.

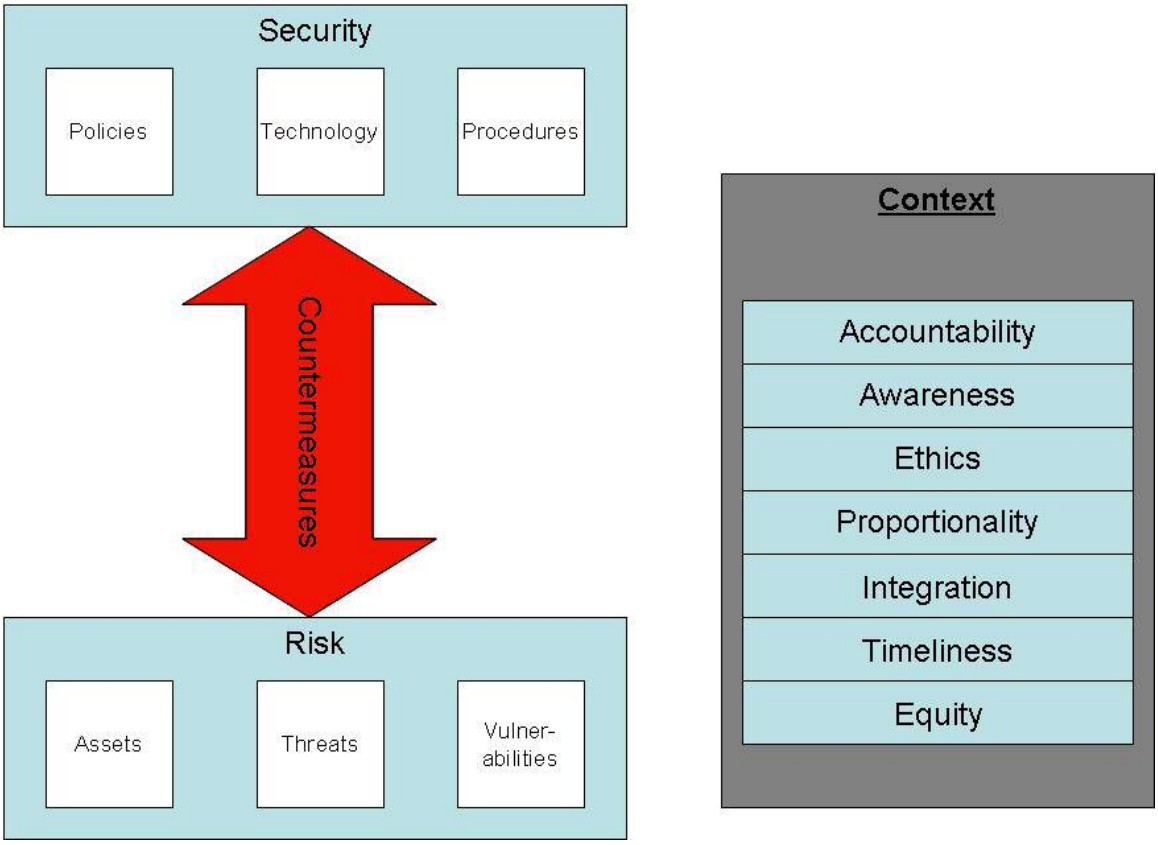

Figure 1. An Overview of Broad Security Issues

Contexts of Security Risk

As Figure 1 indicates, the two major components that we examine are security and risk. Security is typically broken down into three categories: Policies, Technology, and Procedures. For example security policies keep students from accessing illegal materials from a university owned security lab (Doherty et al. 2006). Technology is the artifact that allows us to protect the information system. Examples of technology would be Norton Antivirus software. Finally security procedures are methodologies or guidelines to be followed in order to protect systems (Nyanchama 2005).

Risk is made up of three components: Assets, Threats, and Vulnerabilities. An asset must be evaluated and weighed to determine its worthiness to an organization. Threats can be human or non-human, and if they are human can be internal or external. Human threats can be further broken down by premeditated or opportunistic, benign and malignant threats (2003). Vulnerabilities can be thought of as a door that allows a risk to be introduced. As long as the door remains closed the system has virtually no risk. Once the vulnerability is introduced then risk becomes present in the system (Covert et al. 2005).

Where risk and security interact is the countermeasures (Neal et al. 2006). Countermeasures are superficial barriers that are erected to protect information system assets. Typically the asset is information found in the information system. Countermeasures can be a business continuity plan that is rehearsed or it could be merely installing Operating System patches to close security holes (Boyce 1997).

Business professionals and academics must look at security using context as their magnifying glass. Upon the initial investigation the researchers found these seven contexts to be the most frequently found in the literature. The following are the contexts that could be used:

- Accountability
- Awareness
- Ethics
- Proportionality
- Integration
- Timeliness
- Equity

Accountability describes the ability to inspect the actions of all parties and processes which interact with information or the asset (Ward et al. 2002). Roles and responsibilities are clearly defined, identified, and authorized at a level corresponding with the sensitivity of the information. The relationship among all parties, processes, and information must be clearly defined, documented, and acknowledged by all parties (Masuda 2006).

Awareness applies between and within organizations. Awareness of information security principles, standards, conventions, and mechanisms enhances and enables controls and can help to mitigate threats. Awareness of threats and their significance also increases user acceptance of controls (Malhotra et al. 2004). Without user awareness of the necessity for particular controls, the users can pose a risk to information by ignoring, bypassing, or overcoming existing control mechanisms. The awareness principle applies to unauthorized and authorized parties (Braithwaite 2001).

Information should be used, and the administration of information security should be executed, using an ethical approach. Information systems saturate societies and cultures (Tsiakis et al. 2005). The Information Age and the ubiquitousness of computing makes information readily available. Rules and expectations are evolving with regard to the appropriate provision and use of information systems and the security of information. Use of information and information systems should match the expectations established by social norms, and obligations (Poore 2003).

Information security controls should be proportionate to the risks of modification, denial of use, or disclosure of the information (Furnell et al. 2006). Security controls should be commensurate with the value of the information assets and the vulnerability (Flowerday et al. 2005). Practitioners should consider the value, sensitivity and criticality of the information, and the probability, frequency, and severity of direct and indirect harm or loss.

Principles, standards, conventions, and mechanisms for the security of information should be coordinated and integrated with each other and with the organization's policies and procedures to create and maintain security throughout an information system (Subramani et al. 2004). Many breaches of information security involve the compromise of more than one safeguard. The most effective control measures are components of an integrated system of controls (Kumar et al. 2004). Information security is most efficient when planned, managed, and coordinated throughout the organization's system of controls and the life of the information.

Emergency planning deals with actions that are timely. Acting in a timely, coordinated manner to prevent or respond to breaches of and threats to the security of information and information systems. In order to maximize security an organization should be capable of swift coordination and action to enable threat event prevention or mitigation. This context recognizes the need for the public and private sectors to establish jointly mechanisms and procedures for rapid and effective threat event reporting and handling . Access to threat event history could support effective response to threat events and may help to prevent future incidents (Chang et al. 2005).

Management should respect the rights and dignity of individuals when setting policy and when selecting, implementing, and enforcing security measures. Information security measures implemented by an organization should not infringe upon the obligations, rights, and needs of legitimate users, owners, and others affected by the information when exercised within the legitimate parameters of the mission objectives (Besnard et al. 2004).

Methodology

Although meta-analysis of quantitative research is a well-established technique, the synthesis or aggregation of qualitative studies remains rare and at times controversial. Qualitative meta-analysis begs several questions, for example concerns about feasibility, validity, study selection, mechanism, interpretation, and even ethics are prevalent. Valid qualitative meta-analysis research must conduct a critical assessment and evaluation of research it is not enough to merely summarize that attempts to address a focused clinical question using methods designed to reduce the likelihood of bias. This study will draw on grounded theory as the methodology for research synthesis and meta-analysis. Although grounded theory

was not originally designed to perform meta-analysis or review of published literature, Glaser & Strauss explain that collecting data in libraries is analogous to collecting data through fieldwork or interview:

"There are some striking similarities—sometimes obvious although often overlooked between field work and library research. When someone stands in the library stacks, he is, metaphorically, surrounded by voices begging to be heard. Every book, every magazine article, represents at least one person who is equivalent to the anthropologist's informant or the sociologist's interviewee." (Glaser et al. 1967).

With the advent of quantitative meta-analysis techniques, some qualitative researchers have attempted to use qualitative research methods to perform similar research tasks as in order to reach objectivity and generalize-ability in synthesizing research. Other disciplines describe this technique as a qualitative meta-synthesis approach (Saunders et al. 2003).

Context Classification Coding

When analyzing the candidate papers for this paper the authors used a coding technique to make them aware of the type of security risk where each paper focused. The authors conducted a qualitative meta-analysis by comparing the types of Security Risk articles being published in prolific information systems journals.

A qualitative coding scheme was devised to elucidate paper contexts. Two different coders used the coding scheme independently. The coding schemes had a structure with the following seven categories: Accountability, Awareness, Ethics, Proportionality, Integration, Timeliness, and Equity. Initially, two researchers performed coding decisions to test the coding scheme's reliability. If the two researchers did not agree about the coding then an independent third party was asked to code the paper based on the contexts.

Table 1. Context Classification Coding

A	Accountability
B	Awareness
C	Ethics
D	Proportionality
E	Integration
F	Timeliness
G	Equity

Table 1 demonstrates the coding the authors used to give context to the security risk articles that were examined for the study. These contexts were described in the following classification scheme: accountability, awareness, ethics, proportionality, integration, timeliness, and equity. Each of the articles used in the study was coded according to context. An article could contain any combination from one to seven contexts.

Method Classification Coding

Table 2 demonstrates the types of methodologies that were available to be used in the article. Methodologies were classified as follows: quantitative, qualitative, conceptual, hybrid, or other. These articles were then coded as A – E. The authors examined the articles for the methodology utilized in each publication.

Table 2. Method Classification Coding

A	Quantitative
B	Qualitative
C	Conceptual
D	Hybrid
E	Other

Utilization of Contexts

Table 3 demonstrates the analysis of each context that is utilized per article. The authors interpreted each article and coded them according to the context or contexts they contained. As demonstrated in the table most of the articles were written encapsulating a single context (75/112 or 66.96%). The next largest group was articles which employed the use of two contexts (25/112 or 22.32%). As demonstrated in the table none of the articles used all seven contexts; however, two articles used at least six contexts. As the table shows, only 4% of the articles that were analyzed used more than three contexts.

Table 3. Number of Contexts Utilized per Article

# Contexts	# Articles	Total	Percentage
1 Context	75	112	66.96%
2 Contexts	25	112	22.32%
3 Contexts	7	112	6.25%
4 Contexts	0	112	0.00%
5 Contexts	3	112	2.68%
6 Contexts	2	112	1.79%
7 Contexts	0	112	0.00%

Figure 2 represents the types of contexts available to be utilized by the Security Risk journal articles. These contexts consisted of the following: accountability, awareness, ethics, proportionality, integration, timeliness, and equity. Each of the articles utilized one or more of these contexts. For journals that utilized more than one context, only their primary context was documented by the researchers.

Figure 2 Types of Contexts

Frequency of Context Use

Table 4 represents the frequency of context used. The researchers only demarcated the main context. For example if a paper's context was predominantly about integration, then it was only counted as an integration context even if the paper discussed proportionality.

Table 4. Frequency of Contexts

Context	Type	Number	Total	Percentage
A	Accountability	12	112	10.71%
B	Awareness	20	112	17.86%
C	Ethics	3	112	2.68%
D	Proportionality	28	112	25.00%
E	Integration	40	112	35.71%
F	Timeliness	5	112	4.46%
G	Equity	4	112	3.57%

Table 5 demonstrates the frequency of additional contexts that were developed in the articles. While several of the journals dealt with integration as their main context, many of them discussed proportionality as a secondary context.

Table 5. Frequency of Additional Contexts

Context	Type	Number	Total	Percentage
A	Accountability	0	112	0.00%
B	Awareness	5	112	4.46%
C	Ethics	0	112	0.00%
D	Proportionality	22	112	19.64%
E	Integration	10	112	8.93%
F	Timeliness	0	112	0.00%
G	Equity	0	112	0.00%

Figure 3 exhibits the number of occurrences per year in the academic literature. Only the primary contexts were included in this graph. This graph examines in which publication year the contexts were the most common. For example in 2001 and 2002 there was an increate publication in Awareness, Ethics, Accountability, and Timeliness. One possible explanation for this type of spike would be the events that occurred on September 11, 2001 (Tipton 2002).

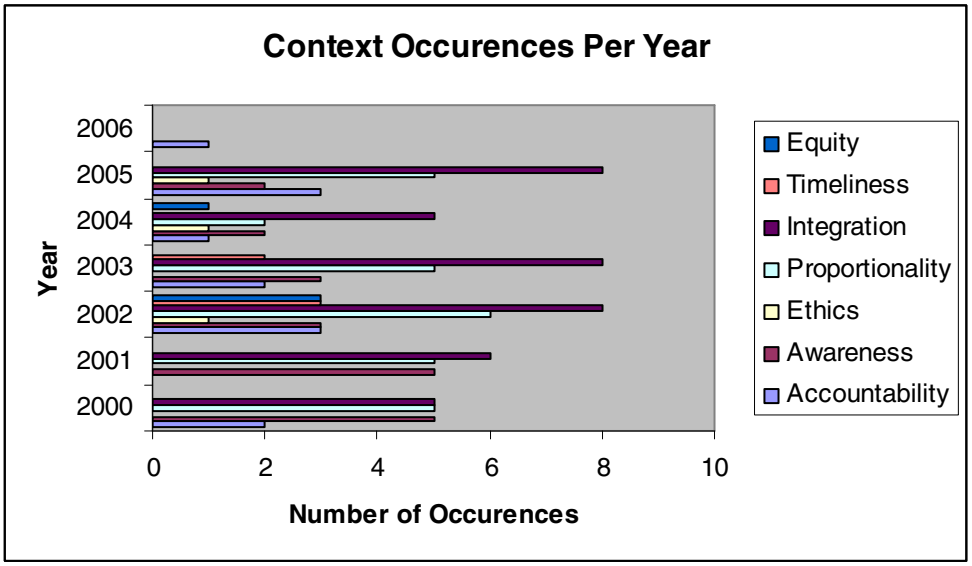

Figure 3. Number of Context Occurrences Per Year

Table 7 expresses the occurrence of methodology found in the data set. Most of the data set used a quantitative methodology; however, there was a large number of qualitative topics, as well as, several theory-based papers.

Table 6. Method Occurrence Frequency

Code	Method	Number	Total	Percentage
A	Quantitative	69	112	61.61%
B	Qualitative	9	112	8.04%
C	Conceptual	21	112	18.75%
D	Hybrid	10	112	8.93%
E	Other	3	112	2.68%

Potential Future Direction for Information Security Risk

It is beyond the scope of this study to analyze where Information Security Risk stands in terms of maturation of the discipline. However because of some of the underutilized contexts that are available for publication areas, Information Systems Security Risk topics will have a plethora of research areas in the coming years.

One notable finding is the advent of security based special interest journals available to the security researcher. It is interesting to note that some of these special interest journals have low acceptance rates that qualify them as top journals in the Management Information Systems field.

Potential areas of future research include a more thorough analysis of the designated data set developed in this paper. For example the authors could drill down and ask more research questions of the data set used in the study.

Latent areas of future research in Information System Security Risk would be to further develop the contexts available for research. For example several of the contexts are under-utilized. Additionally development of new contexts in security is a possibility. Finally researchers might also explore other areas of security risk to develop more fully.

Conclusion

Diversity is an important piece of the MIS discipline (Vessey et al. 2002). Security has become a cornerstone of MIS over the past decade (von Solms et al. 2005). It is imperative that researchers see the importance of studying not just security but the risks that security poses for what is now becoming our most vital asset, our information.

Future research is needed to further address this topic. For example, each of the articles selected could be analyzed using a high level approach of the questions, and a more in depth level. The high level question "What are the contexts of the research?" can be further broken down to analyze other questions like:

- RQ1.a: What are the frameworks of the research?
- RQ1.b: What are the research areas or topics?
- RQ1.c: What topics are most often studied?

The second research question could be broken down as well.

- RQ2.a: What research methods are most often used?
- RQ2.b: What methods are often used to study what topics?
- RQ2.c: What are the levels of analysis?

This study systematically assesses IS literature to synthesize and categorize the research of Information Systems Security. The study is educational in providing the state of research issues and concerns, research emphases and gaps, potential research directions, and publication opportunities for this relatively new area. Thus, it can play an important role in the identification and promotion of this emerging sub-discipline and suggest directions for guiding future efforts in research, collaboration, publication, practice, and education. It can also help interested doctoral students to identify potential research topics for dissertation research. Overall, this study contributes to the literature in a unique way.

References

"Information System Security Risk," *Communications of the ACM* (46:10), Oct2003 2003, pp 136-136.
"Security through uncertainty," *Network Security* (2007:2) 2007, pp 1-1.
Besnard, and Arief, B. "Computer security impaired by legitimate users," *Computers & Security* (23:3), May2004 2004, pp 253-264.
Bhaskar, R. "State and Local Law Enforcement is not Ready for a: CYBER KATRINA," *Communications of the ACM* (49:2), Feb2006 2006, pp 81-83.
Boyce, B. "Cyber extortion--the corporate response," *Computers & Security* (16:1), 1997 1997, p 25.
Braithwaite, T. "Executives Need to Know: The Arguments to Include in a Benefits Justification for Increased Cyber Security Spending," *Information Systems Security* (10:4), Sep 2001, pp 35-48.
Campbell, S. "How to Think About Security Failures," *Communications of the ACM* (49:1), Jan2006 2006, pp 37-39.
Cavusoglu, H., Mishra, B., and Raghunathan, S. "The Value of Intrusion Detection Systems in Information Technology Security Architecture," *Information Systems Research* (16:1), Mar2005 2005, pp 28-46.
Chang, D.B., and Young, C.S. "Infection dynamics on the Internet," *Computers & Security* (24:4), Jun2005 2005, pp 280-286.
Covert, and Nielsen "Measuring Risk Using Existing Frameworks," *Information Systems Security* (14:1), Mar 2005, pp 21-25.
Doherty, N., Fulford, H., and nbsp "Aligning the information security policy with the strategic information systems plan," *Computers & Security* (25:1), Feb2006 2006, pp 55-63.
Erwin, D.G. "Understanding Risk (or the Bombastic Prose and Soapbox Oratory of a 25-Year Veteran of the Computer Security Wars)," *Information Systems Security* (10:6), Jan 2002, p 14.
Flowerday, and von Solms "Real-time information integrity= system integrity + data integrity + continuous assurances," *Computers & Security* (24:8), Nov2005 2005, pp 604-613.
Furnell, Jusoh, A., nbsp, Katsabas, D., and nbsp "The challenges of understanding and using security: A survey of end-users," *Computers & Security* (25:1), Feb2006 2006, pp 27-35.
Glaser, B.G., and Strauss, A.L. *The discovery of grounded theory: Strategies for qualitative research* Aldine Publishing Company, Chicago, 1967.
Hale, R. "End-user computing security guidelines," *Information Systems Security* (4:4), Winter96 1996, p 49.
Hancock, B. "Cellular Security Hazards," *Computers & Security* (19:7), 2000 2000, p 579.
Hovav, A., and D'Arcy "The Impact of Virus Attack Announcements on the Market Value of Firms," *Information Systems Security* (13:3), Jul 2004, pp 32-40.
Jaamour, R. "Securing Web Services," *Information Systems Security* (14:4), Sep 2005, pp 36-44.
Kumar, R.L., and nbsp "A Framework for Assessing the Business Value of Information Technology Infrastructures," *Journal of Management Information Systems* (21:2), Fall2004 2004, pp 11-32.
Malhotra, N.K., Sung S. Kim, and Agarwal, J. "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model," *Information Systems Research* (15:4), Dec2004 2004, pp 336-355.
Masuda, B. "Managing the Risks of Managed Security Services," *Information Systems Security* (15:1), Mar 2006, pp 35-42.
Neal, R., and nbsp "Social Psychological Variables That Contribute to Resistance to Security Assessment Findings," *Information Systems Security* (15:1), Mar 2006, pp 43-52.
Nyanchama, M. "Enterprise Vulnerability Management and Its Role in Information Security Management," *Information Systems Security* (14:3), Jul 2005, pp 29-56.
Ohanley, R. "Maintaining Security and Privacy Requires Getting "Back to Basics"," *Information Systems Security* (13:5), Nov 2004, pp 2-3.
Poore, R.S. "Attractive Hazard: Entrapment or Forensic Tool?," *Information Systems Security* (11:6), Jan 2003, p 10.
Sambamurthy, V., nbsp, Subramani, M., and nbsp "Special Issue on Information Technologies and Knowledge Management," *MIS Quarterly* (29:1), Mar2005 2005, pp 1-7.
Saunders, C.S., Jasperson, J., Butler, B.S., and Carte, T.A. "Lessons Learned from the Trenches of Metatriangulation Research," *Communications of AIS* (2003:11), 2003 2003, pp 245-269.
Straub, D.W., and Welke, R.J. "Coping With Systems Risk: Security Planning Models for Management Decision Making," *MIS Quarterly* (22:4), Dec98 1998, pp 441-469.
Subramani, M., and nbsp "How Do Suppliers Benefit from Information Technology Use in Supply Chain Relationships?[1]," *MIS Quarterly* (28:1), Mar2004 2004, pp 45-73.
Tipton, H.F. "Computers at Risk--Ten Years After," *Information Systems Security* (10:6), Jan 2002, p 37.

Tsiakis, T., and Stephanides, G. "The economic approach of information security," *Computers & Security* (24:2), Mar2005 2005, pp 105-108.

Vessey, I., Ramesh, V., and Glass, R.L. "Research in Information Systems: An Empirical Study of Diversity in the Discipline and Its Journals," *Journal of Management Information Systems* (19:2), Fall2002 2002, pp 129-174.

von Solms, B., and von Solms, R. "From information security to…business security?," *Computers & Security* (24:4), Jun2005 2005, pp 271-273.

Ward, P., and Smith, C.L. "The Development of Access Control Policies for Information Technology Systems," *Computers & Security* (21:4), 2002 2002, p 356.

Yihua Philip, Mykytyn, J.P.P., Litecky, C.R., and Allen, G. "Competitor Analysis and Its Defenses in the E-Marketplace," *Communications of the ACM* (48:8), Aug2005 2005, pp 107-112.

Zuccato, A. "Holistic security requirement engineering for electronic commerce," *Computers & Security* (23:1), Feb2004 2004, p 63.