A Research Framework for Information Systems Security

By: Sherry Cannoy, Prashant C. Palvia, and Richard Schilhavy.

Cannoy, S., Palvia, P., and Schilhavy, R. (2006). "A Research Framework for Information Systems Security." *Journal of Information Privacy & Security*. 2 (2), 3-29.

Abstract:

Securing the IT infrastructure and the data it contains is one of the most critical components of IT that management faces today. Technologies such as the Internet and the wide-spread dissemination of computers to more users has increased the vulnerabilities of IT infrastructures as well as the likelihood of internal and external threats to companies. Managers are able to prevent or mitigate some of the damage caused by these attacks by aligning security policies with IT infrastructures to protect the organization's information capital. The purpose of this study was to examine security articles in top-tier IS journals from 1996 to 2005 to determine what types of security research has been performed, to find out if a comprehensive framework for security in IS exists, and; if not, to develop a framework based upon the current literature and theory. Through the analysis of hypotheses, frameworks, and variables, security research appears to be very narrow and highly fragmented, suggesting security research remains fertile, yet immature. Additionally, no comprehensive framework was present in the analyzed literature; thus a comprehensive research framework is proposed for IS security.

Keywords: security | meta-analysis | framework | privacy

Article:

INTRODUCTION

Information is a vital asset to any company, and needs to be appropriately protected (Hong et a1 2003). It is interesting to note that as early as 1978, Madnick wrote an article for Sloan Management Review in which he stated ". . . much of the literature and research on computer-security related matters has focused either on privacy and its associated social and legislative implications or on technical mechanisms to enforce a specific security objective" (Madnick, 1978). Although a quarter of a century has passed since his article was published, his premise still seems to hold true. Security is a hot topic now, and it seems that we should be inundated with academic research regarding security; however, there are relatively few articles. When

examining the current state of IS security research articles, it seems that what Madnick suggests still exists-the technical and behavioral issues are still a concern. Madnick predicted that managerial security issues would persist even after security legislation was enforced. Even before regulations such as HIPAA, this prediction reinforces the fact that management of security is difficult to implement, enforce, and maintain. Much of this stems from the fact that management of security is a fairly ill-structured problem. In an article proposing a new methodology for handling ill-structured problems, Mitroff and Emshoff (1979) suggest that policies to implement solutions to ill-structured problems ". . . are all-too-often directed towards the surface or structural characteristics of a policy. . ." This is apparent in many companies today that are forced by regulations to write and advertise their security and privacy policies, but the companies do not have the infrastructure and management in place to ensure that the policies are properly enforced. Ideally, the security and privacy policies should be in place and integrated with the IT infrastructure components. A CRA report on Security Risk Management (CRA Reports 2003) cites the logical reasons that security in the IS field is so fragmented:

"Nobody in corporate America denies the strategic imperatives associated with protecting the information infrastructures and data that underpin virtually all commercial activities in today's economy. And yet, despite the documented costs of cyber attacks by hackers, viruses--even trusted employees within organizations-the security posture in most large enterprises is still characterized by a series of largely disconnected measures and countermeasures designed to respond to events after they have occurred. Current security strategies are, in other words, reactive in nature-not proactive. "

Given the paucity of research and apparent lack of coherence in IS security research, the purpose of this article is to conduct a thorough examination of top-tier journals in Information Systems and report on the state of IS security research. Another important goal is to develop a comprehensive research framework which can be instrumental in understanding current efforts and guiding future work.

BACKGROUND AND RESEARCH OBJECTIVES

According to Hong, et al, (2003) there is very little literature regarding security management. Part of the problem is the level of difficulty experienced in conducting security research. For example, Kotulic et al (2004) experienced several problems testing a proposed security risk management model due to the sensitive nature of collecting security information for research. The original methodology was to perform a preliminary field study at two firms which had a security risk management program in place, and surveys would be created based on the information gathered from the field studies. There were five firms who then agreed to participate in the pilot test of the questionnaires. After being provided with the research study proposal and the preliminary questionnaires, these firms were to administer self-report questionnaires. Even though the identity of the individuals and firms would be kept confidential, these five firms declined to participate. Thirty-eight alternative firms were then chosen and asked to participate. Only one firm agreed to participate in the pilot test of the questionnaire. The questionnaire was then sent to 1,500 firms. Only 23 of these firms returned the questionnaires, not all of which were usable. While there were several reasons for these difficulties, the most enlightening one is a company policy not allowing the sharing of information about computer security policies with

those external to the organization. Furthermore, it seems that there is no consensus in the IS field as to how security fits into the organizational structure of management and IS policy and infrastructure. Many of the frameworks proposed in IS security research are extremely specific and task-related. NIST (National Institute of Standards and Technology) is highly involved in developing risk, contingency, and security policies for the government. There are many published articles by NIST regarding the development of security policies in governmental agencies (www.nist.gov) (2000). They have developed a descriptive security framework for their agencies to follow. They suggest that "agencies" should:

1. Assure that systems and applications operate effectively and provide appropriate confidentiality, integrity, and availability.

2. Protect information commensurate with the level of risk and magnitude of harm resulting from loss, misuse, unauthorized access, or modification (NIST 2000) The main goal of their framework is to develop standard documented policy and procedures to be implemented, tested, and reviewed. Development of security policy and infrastructure is core to mitigating risks, threats, and vulnerabilities in an organization.

Given the apparent fragmented state of IS security research, the purpose of this study is to examine the research conducted in the last decade (from 1996 to 2005) in information systems journals regarding security issues. With security being a major concern facing IS management, it seems that academic researchers would be very involved in studying the phenomena of how these threats, vulnerabilities, and risks affect IS management, infrastructure, and employees. Through a meta-analysis, this study will examine the focus of IS research according to the following research objectives and then propose a research framework for IS security. The research questions posed are as follows:

1. What has been the focus of security research in IS from 1996 to 2005?

2. What are the main variables utilized in IS security research during this period?

3. What are some of the hypotheses from the IS security studies?

4. Does a comprehensive research framework for IS security exist?

5. If not, can a comprehensive framework for IS security be developed based on previous works and proposed for future research development?

METHODOLOGY

In an attempt to address the research questions above, the authors performed a meta-analysis of 82 security articles from what are considered to be the top-tier journals in Information Systems. Table 1 shows the journals analyzed and the frequency of security-related articles found for each journal. A list of all the articles examined is included in Appendix A. Chaisson and Davidson (2004) utilized similar journals in their study of information systems in healthcare, although a significantly smaller list was chosen. Meta-analysis has frequently been chosen as a suitable

methodology for studies focusing on codifying a domain of knowledge (Hunter 1990), although meta-analysis research is not without its problems (Hwang 1996). Previous literature has also performed meta-analysis on specific domains of knowledge within Information Systems, particularly in decision support systems and group decision support systems literature (Benbasat Lim 1993, Dennis et al 2001, McLeod Liker 2002). A recent meta-analysis of information systems literature was performed by Palvia, et al. (2004). The initial set of articles was based on their study; later our search was expanded to include all security articles from 1996 to 2005.

Besides many articles which focus primarily on privacy also discuss security as a secondary topic, these articles were also included (see Table 2 below).

Table 1. Journals and the Frequency of Security-Related Articles

Communications of the ACM	*51*
Decision Science	*3*
Information and Management	*10*
Information Systems Research	*7*
Journal of Management Information Systems	*2*
Management Sciences	*5*
MIS Quarterly	*4*
Total	**82**

Table 2: Privacy Related Articles

Personal Information Privacy: Implications for MIS Managers	Henderson, Snyder	*I&M*	Oct 1999 v36:4 pg 213
Software Security and Privacy Risks in Mobile E-Commerce	Ghosh, Swaminatha	*CACM*	Feb 2001 v44:2 pg 51
Information Privacy: Measuring Individuals' Concerns About Organizational Practices	Smith, Milberg, Burke	*MISQ*	June 1996 v20:2 pg 167
Markets and Privacy	Laudon	*CACM*	Sept 1996 v39:9 pg 92
Privacy lost anytime, anywhere	Meeks	*CACM*	Aug 1997 v40:8 pg 11
Privacy, information technology, and healthcare	Rindfleisch	*CACM*	Aug 1997 v40:8 pg 92
Beyond concern: A privacy-trust behavioral intention model of e-Commerce	C Liu; J Marchewka; J Lu; C Yu	*I&M*	2004; 42; 127-142

Because this research is more descriptive in nature, the data collected was written on a predefined form. This provided some structure and a common method of analysis for each of the coders. The following items were recorded from each article:

Items Recorded from each Article

1.	Name of article	6.	Dependent, independent, and intermediate variables
2.	Journal and date of publication	7.	Categories of main variables
3.	Summary of article	8.	Related keywords from articles
4.	Framework (if present)	9.	Hypotheses
5.	Pertinent charts, diagrams, and tables	10.	Findings of hypotheses
		11.	Major findings

To improve inter-rater reliability, the authors coded the initial ten articles independently, comparing the results of the analysis and correcting any discrepancies. Once a common understanding was reached, the remaining articles were divided between two of the authors at random and summarized in the context of the predefined form. Any confusion coding a particular article was resolved through consensus between the two coders. In addition, a common level of knowledge in the security area among coders, aided in mitigating discrepancies between the authors' analysis of the individual articles.

FINDINGS OF THE META RESEARCH

1. What has been the focus of security research in IS from 1996 to 2005?

Table 3 displays the frequency of security articles per year. The research is very fragmented and there is very little on a comprehensive view of how security fits into the organization. The interest in security research declined after the mid-nineties; however it has risen again in the last couple of years.

Table 3: Number of Security Articles in Top-Tier IS Journals per Year

	Number of Articles per Year
1996	12
1997	16
1998	4
1999	6
2000	1
2001	8
2002	6
2003	6
2004	12
2005	11

Table 4 provides a summary of the types of research and representative articles for the past ten years. There have been several articles written on legal issues related to security. Along related lines, there were a few articles regarding computer monitoring and ethics. Vulnerabilities and risks were discussed, as well as threats to systems in several articles. Detection of these risks was also the topic of several articles, as well as specific security technologies, such as data

perturbation, digital watermarking and cryptography. However, the majority of the articles dealt with piracy issues.

Table 4: Sample Articles Based on Topic

Legal Issues	Technical Trials and Legal Tribulations	Craver, Yeo, Yeung	CACM	Jul 1998 v41:7 pg 45
	Copyright Functions and Patentable Speech	Burk	CACM	Feb 2001 v44:2 pg 69
	Watermark-Based Copyright Protection System Security	Kowk	CACM	Oct 2003 v46:10 pg 98
	Regulation of Technologies to Protect Copyrighted Works	Samuelson	CACM	July 1996 v39:7 pg 17
Monitoring and Morality	Computer Monitoring: Benefits and Pitfalls Facing Management	Ariss	I&M	July 2002 v39:7 pg 553
	Morality and Computers: Attitudes and Differences in Moral Judgement	Gattiker, Kelley	ISR	Sept 1999 v10:3 pg 233
	Computer-Based Monitoring: Common Perceptions and Empirical Results	George	MISQ	Dec 1996 v20:4 pg 459
Vulnerabilities and Risks	Coping with Systems Risk	Straub, Welke	MISQ	Dec 1998 v22:4 pg 441
	Enemy at the Gate: Threats to Information Security	Whitman	CACM	Aug 2003 v46:8 pg 91

	Security Threats to Internet: A Korean Multi-Industry Study	Jung, Han, Lee	I&M	Oct 2001 v38:8 pg 487
	Market for Software Vulnerabilities? Think Again	K Kannan; R. Telang	IM	May 2005; 51:5; 726-740
Detection	A Process Control Approach to Cyber Attack Detection	Ye, Giordano, Feldman	CACM	Aug 2001 v44:8 pg 76
	Data Mining for Network Intrusion Detection: A Comparison of Alternative Methods	Zhu, Premkumar, Zhang, Chu	DS	Fall 2001 v32:4 pg 635
	The Value of Intrusion Detection Systems in Information Technology Security Architecture	H. Cavusuglu; B Mishra; S Raghunathan	ISR	March 2005; 16:1; 28-46
	Detection and Prevention of Stack Buffer Overflow Attacks	B A Kuperman; C E Brodleyl H Ozdoganoglu; T N Vijaykumar; A Jalote	CACM	Nov 2005; 48:11; 50-56
Data Pertubation	An Improved Security Requirement for Data Perturbation with Implications for E-commerce	Muralidhar, Sarathy, Parsa	DS	Fall 2001 v32:4 pg 683
	A General Additive Data Perturbation Method for Database Security	Muralidhar, Parsa, Sarathy	MS	Oct 1999 v45:10 p 1399
	Perturbing Nonnormal Confidential Attributes: The Copula Approach	R Sarathy; K Muralidhar; R Parsa	MS	2002; 48:12
	An Enhanced Perturbation Approach for Small Data Sets	K Muralidhar; R Sarathy	DS	Aug 2005; 36:3; 513-529
	The Security of Confidential Numerical Data in	Sarathy, Muralidhar	ISR	Dec 2002 v13:4 pg 389

	Databases			
Digital Watermarking	Digital Watermarking	Yeung	CACM	July 1998 v41:7 pg 30
Cryptography	Cryptography, security and the future	Schneier	CACM	Jan 1997 v40:1 pg 138
Piracy	The MP3 Open Standard and the Music Industry's Response to Internet Piracy	Easley, Michel, Dewaeaj	CACM	Nov 2003 v46:11 pg 90
	Prevention and Deterrent Controls for Software Piracy	Gopal, Sanders	JMIS	Spring 1997 v1:4 pg 29
	Software Piracy and its Legal Implications	Koen Jr, Inn	I&M	Jan 1997 v31:5 pg 265
	A Reversed Context Analysis of Software Piracy Issues in Singapore	T Moores; J Dhaliwal	IM	2004; 41; 1037-1042
	Managing Digital Piracy: Pricing and Protection	A Sundararajan	ISR	Sept 2004; 15:3; 287-308
	Managing Piracy: Pricing and Sampling Strategies for Digital Experience Goods in Vertically Segmented Markets	S Shivendu; R Chellappa	ISR	Dec 2005; 16:4; 400-417

2. What are the main variables utilized in IS security research during this period?

We specifically divided the articles into those that offered formal hypotheses and those that did not. We then examined what dependent, independent, and intermediate variables were used most frequently in the proposed hypotheses. Most of these variables related to security in the realm of management policy, infrastructure, and protection of data. We also examined the keywords in each article (and when keywords were not provided, we utilized the most frequently used concepts from the articles). The keywords most frequently used were in the areas of threats, privacy, security, access control, data integrity and data confidentiality.

3. What are some of the hypotheses9om the IS security studies?

Table 5 below displays the frequency of articles which included formal hypotheses. Articles that focused primarily on generating mathematical models were not considered in the formal hypotheses. A few of the hypotheses did not relate to any of the identified constructs. The hypotheses from Gattiker et a1 (1999) were not included since they are primarily concerned with environmental variables, such as individual characteristics.

Table 5: Frequency of Articles with Formal Hypotheses Stated

Communications of the ACM	3
Decision Science	3
Information and Management	2
Information Systems Research	1
Journal of Management Information Systems	2
Management Science	0
MIS Quarterly	2
Total	**13**

Few relationships across hypotheses were found. The hypotheses were typically narrowly focused. This is not surprising given how few articles actually contained formal hypotheses and how diverse security research has been. Some of the hypotheses tested similar variables or constructs, for example, piracy prevention. However, no connections between articles were found, for example, connecting moral judgments with piracy behaviors. Clearly there is a lack of cumulativeness or theory-building in IS security research. Some examples of hypotheses are shown in Table 6.

Table 6: Some Formal Security Hypotheses

From Straub, et al 1998:

- Managers are aware of only a fraction of the full spectrum of actions that can be taken to reduce systems risk
- Managers exposed to theory-grounded security planning techniques will be inclined to employ these in their planning processes

From Biros et al 2002:

- Warnings about possible deception in computer-based data will be positively associated with detection. Warnings about possible deception in computer-based data will be positively associated with the issuance of false alarms.
- The combination of just-in-time training to find deception in computer-based data and warnings about possible deception will be positively associated with the issuance of false alarms.

From Zviran et al (1999):

- The number of characters in a password is associated with characteristics of data being protected.
- The composition of a password is associated with characteristics of data being protected.
- The frequency with which a password is changed is associated with the characteristics of the data being protected

4. Does a comprehensive research framework for IS security exist?

The analysis of these articles revealed that the security research in this area is fragmented and no comprehensive framework was discovered. It was expected that the current research would involve more frameworks than were actually found. Most articles included diagrams, charts, and tables; however, none of them included major constructs and their relationships, only proposing a model for a narrow topic or clarifying a technical system. Therefore, the next research objective was to develop a comprehensive framework for security, which would enable a broad agenda for future research.

5. If not, can a comprehensive framework for IS security be developed based on previous works and proposed for future research development?

Based on the articles we reviewed, their categories, variables, keywords, and diagrams, a research framework is developed and proposed for security in information systems. This process is described in the next section.

A RESEARCH FRAMEWORK

Based upon our comprehensive examination of 82 articles in top-tier IS journals, the research framework intended to examine IS security issues in an organization is shown in Figure 1. Since there were few hypotheses found in existing research on which to base these relationships and constructs, our approach was based more on the descriptive and qualitative aspects of the articles rather than the quantitative aspects. Nevertheless, we show the number of articles related to each construct and relationship in parentheses next to the construct/relationship.

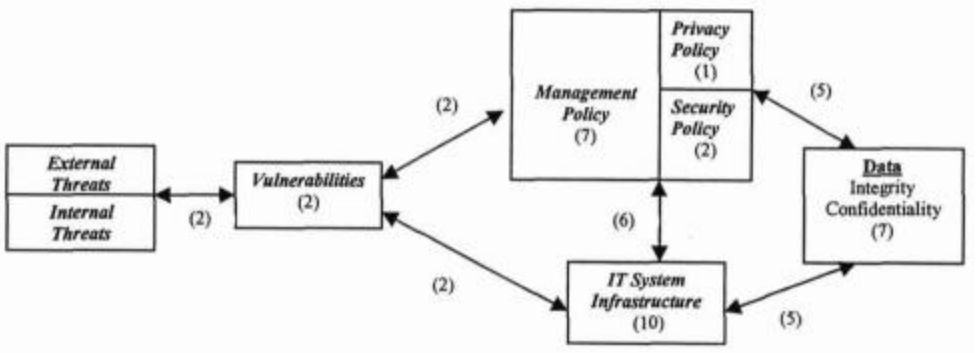

Figure 1: A Research Framework for IS Security

Table 7 lists the descriptions of the above constructs. The categorization of these constructs was grounded from the variables and the keywords, including those generated by the authors when keywords or variables were not available. Such keywords were subjectively chosen by the authors as relevant words or topics after a careful reading of the articles. It was deemed necessary to make up these keywords in order for the analysis to be representative of all of the articles under review.

Table 7: Description of Constructs

CONSTRUCT NAME	DESCRIPTION
External Threats	Any threat or risk outside of the organization which includes intentional or unintentional threats.
Internal Threats	Any threat or risk inside of the organization which includes intentional or unintentional threats.
Vulnerabilities	Any vulnerability inside of the organization, particularly related to the IT infrastructure that would present easier access to the system for external or internal threats. It includes hardware, software, and human threats.
Management Policy	The development of the management policy regarding both managerial and employee issues as well as IS issues. This includes the lifecycle of developing management policies based on management policy theory and government laws and regulations.
Privacy Policy	One aspect of the management policy that deals specifically with privacy of data contained within the system and data about the system infrastructure.
Security Policy	One aspect of the management policy that deals specifically with the security of access to the data and the system itself.
IT System Infrastructure	The system hardware, software, and connections—regulated by the management policy. Includes user interfaces and physical access control.
Data	Data stored in the system, metadata, infrastructure data
Integrity	Accuracy of the data; ensuring that the data has not been tampered with or changed either intentionally or unintentionally.
Confidentiality	Ensuring the privacy of data—through unauthorized internal access and sharing or external access.

Before we discuss the framework constructs, some general comments are in order. Throughout this process, our focus has been on a realistic framework that is based on what is very fragmented research. It is somewhat ironic that the issues faced in supporting the validation of the constructs and relationship choices (i.e., scarce, fragmented and qualitative IS security research) are also the reason that this security research is necessary.. Therefore, the next steps in the process of recommending such a framework would obviously be to validate the relationships and constructs as proposed.

Threats and vulnerabilities seem to have strong relationships with one another, such that threats are, in part, dependent upon the vulnerabilities and vulnerabilities are dependent upon existing threats. Research regarding vulnerability and risk analysis is almost nonexistent in the articles reviewed in our study. However, it is proposed that, in order for a person or an entity to be a threat to the organization's security, there has to be an existing vulnerability in the security structure (e.g., policies, infrastructure, data, etc.). For example, if there is no policy on how to format passwords, many users may utilize their usernames as passwords. This would be considered a vulnerability since a threat would be likely if the passwords were easy to speculate

and did not require both alpha and numeric characters. The relationship is double-sided because the threat will often expose a vulnerability (i.e., by utilizing a brute force approach or algorithm to discover passwords) or the threat may unintentionally find a vulnerability (i.e., stumbling upon confidential information that should be protected by some type of access control mechanism).

The type of threat and vulnerability also determine the types of policies that should be in place as well as what type of infrastructure should be implemented. More serious threats will call for stricter policies and a tightly controlled infrastructure. Policies stem from both general management and IS management, often from governmental directives. Policy can also dictate the type of infrastructure implemented for a specific security application, as well as specific infrastructure technologies which may affect the type of policies generated. The articles we found relating to music piracy are an excellent example of such interdependencies.

The last construct for data is the most fundamental% the framework. The purpose for examining threats, vulnerabilities, policies, and infrastructure is of critical importance so that data integrity and confidentiality can be protected. While the policy and infrastructure determine how the data is protected, the type of data also determines the types of policies and infrastructure in place. An example hypotheses from the meta-analysis further explains this: "Classification accuracy for intrusion detection will differ based upon the format for data representation" (Zhu Zhang 2002).

FRAMEWORK CONSTRUCTS

Note that some variables may overlap into more than one construct. For example, access control can be a part of management policy with regard to general use guidelines outlining who can access particular system components. It may also be contained in the IT infrastructure as a method of controlling access. In some regard, this supports the interrelation between the constructs in the framework, such that, using access control as an example, management policy concerning access control should align with the physical infrastructure and vice versa.

Little difference was found between the variables and keywords for external and internal threats, suggesting that the research has either largely ignored the distinction or, even more interesting, that there is no difference from an organizational perspective. Thus questioning the distinction between the two sub-constructs. In either case, this specific research question would be interesting to address in future research. Generally speaking though, threats as a construct has been given significant attention from the articles analyzed.

With that being said, we would also assume that the vulnerabilities of the organization to such threats would also be given similar attention. This, however, is not the case given the lack of variables and significantly fewer keywords associated with security vulnerabilities. This seems to be a large gap in security research. Present research seems to focus on the threats to the organization, assuming the organization already minimizes their vulnerabilities, which may be far from the case. Thus, future research may focus on what vulnerabilities organizations do manage, which vulnerabilities are not managed, how organizations manage vulnerabilities, and how all of these can be improved.

It is suggested that vulnerabilities are a product of both management and security policies practiced and the IT infrastructure in the organization. Each of these areas has received extensive attention from the literature analyzed in this study. Both had a significant number of formally defined variables in comparison to other areas and had the most unique keywords associated with them. Concerning management policy, it is interesting to note that legal concerns were included in the construct, which consisted of items such as copyrights and patents. The extensive number of instances of this keyword may suggest the possibility of expanding the framework to include environmental variables, in this case, the legal environment. Both security and privacy policies received equal attention. However, relative to general management policies, we would suspect these two sub-constructs to be given greater attention in security research. IT infrastructure is particularly intriguing having an extensive number of unique keywords associated with the construct. This observation is supported by the copious amount of technical and descriptive research found in security research.

The data construct received a moderate amount of attention from the articles coded. While this may be the very thing the policies and infrastructures are designed to protect, the relative lack of research in this area may not be too surprising, since other constructs may be of more concern to IS researchers and their interests. Since data integrity was associated with several keywords, we suspect that this sub-construct may be more complex, requiring additional constructs or factors to describe it. Data confidentiality, on the other hand, was only associated with a single keyword, confidentiality.

As a final observation, most of the hypotheses related to a single construct. However, in general, those which spanned multiple constructs support the relationships shown in the framework.

DISCUSSION

In addition to proposing the framework, through our analysis we have made some conclusions concerning IS security research as a whole. Studies varied greatly in scope and rigor and seemed to cluster into two groups, studies which focused on narrow topics with high rigor, and studies which focused on broad topics with low rigor. Those in the first category, narrow scope with high rigor, tended to be highly technical in nature, often focusing on single technologies or algorithms. As such, the variables and constructs were well-defined, often supported with mathematical models. However, since the scope of these articles was so severely limited, determining which broad constructs the articles refer to becomes a difficult task, much less relating them to a single construct. These studies, however, did not account for the most significant portion, namely those with broad scope and low rigor. Part of this bias toward such articles is due to a vast majority of them appearing in the Communications of the ACM, to be discussed later in this paper. These articles discussed primarily broad topics, such as security concerns for the Internet commerce or management concerns about copyright law. Many of these constructs were simply not well defined, even in the more rigorous journals. Definitions of the constructs were not consistent between studies. It appears that the underlying constructs to these general constructs have not been given careful enough consideration for synthesizing a complete, unified picture.

One exception to this trend was the study by Biros (2002) which examined the effects of training and warnings on detection of deception and false alarms of such detection. This article had well-defined variables which were not so narrow in scope that their value is moot. Since this study appeared more recently, we suspect that we will see great improvements in security research in the future.

Our analysis yields another intriguing trend between the number of dependent, independent and keywords. There were few studies which focused on formally defined variables, either dependent or independent, and even fewer considered intermediary, confounding, or control variables. Additionally, these variables are highly fragmented and narrow in scope, suggesting that security research as a field is relatively immature. However, if the keywords are considered, we have a more complete picture of the security field as a whole. This observation suggests that a greater portion of the security field has been considered in an informal, non-rigorous manner, much more so than with formally defined variables.

The most recent research from 2004 and 2005 focuses in security of areas such as the semantic web (Lee et al2005, Thuraisingharn 2005), malware and spyware (Lee Kozar 2005, McHugh Deck 2005, Shukla Fui-Hoon Nah 2005, Zhang 2005), Internet voting (Jefferson et a1 2004), and investments (Ocavusoglu et al 2004). The area of investments and the economics of security in information systems are evolving, and the future should hold promise for research in return on investment and how to measure the quality of service that security technology provides. Another stream of research that is continuing into the future is that of data perturbation. There has been a prominent group of authors, including Sarathy, Muralidhar, and Parsa, (2002) who are building mathematical models and theory in this area.

One limitation of our study is that we focused only on the recognized top-tier journals. In the past few years, a few niche journals in security research have been initiated, e.g., the Journal of Information Privacy and Security, and the Journal of Information Systems Security. As security issues are more prevalent now, many other IS journals are also publishing security research. Although including articles from these journals will expose a broader range of issues, one must confine the scope of the study. We believe that by including the top-tier journals, we have reviewed the "best practices" in IS security research, and although not exhaustive, our findings are a good representation of current security research.

Another issue is the inclusion of Communications of the ACM (CACM) articles in the analysis and the potential bias it creates in the findings. These articles constituted more than half of the total articles coded. These articles tended toward qualitative and descriptive research, and focused on a wide variety of areas. Chiasson and Davidson (2004) make similar observations during their meta-analysis of the CACM, emphasizing the quality of the non-editorial and non-column articles. However, CACM has long been acclaimed as an important journal in the IS field, although in the past few years, its emphasis is shifting more toward the practitioner audience. In any case, the Communications of the ACM brings an important perspective which cannot be ignored.

The final limitation of our study and also call for research relates to the proposed framework. Although we are confident that the framework encompasses IS security research, we

nevertheless developed the framework from what we found as an evolving and fragmented field consisting of few hypotheses and well-defined variables and constructs. It is quite possible that future studies in security research will provide additional constructs to the framework, or support or refute some of the relationships between constructs that are proposed in our work. In addition, many of these variables and constructs may have to be further refined. Future studies should aim to provide additional validation and completeness to the framework proposed in the article.

CONCLUSION

This study set out to explore recent security research studies in order to synthesize a comprehensive view of security research in the IS field. Our analysis explored over 80 articles from seven top-tier IS journals over ten years. No comprehensive framework was found in the article set, thus one was proposed based upon the variables and topics discussed in these articles. In addition to the framework, some general observations of the research are given. Security research is largely fragmented, focusing on policy and infrastructure issues. Few proposed formal variables and/or hypotheses and even when proposed, they were ill-defined and either too narrow or broad in scope. Therefore, future research potential is rich in security research in IS. Since many of the constructs discussed in the articles lacked formal definitions, research seeking to further refine these constructs in a more rigorous setting would have significant value. Also, studying relationships among constructs instead of minor factors underlying such constructs will add more value to the field.

Perhaps we can learn from Kotulic et al's (2004) suggestion that security research is very intrusive to the organization being studied. Initially, research will be fairly narrowly focused, and most likely will not be the result of extensive surveys of many organizations. The groundwork of research in this area will stem from a few organizations which have a vested interest in the research and who have come to trust the researcher. Ultimately, the metrics for measuring the success of security technology will be developed, and could be a factor that would persuade practitioners to find a benefit from participating.

Gaining the trust of practitioners is necessary for yielding important insights into critical areas of security research.

REFERENCES

Benbasat, I. And L. H. Lim. (1993) The Effects of Group, Task, Context, and Technology Variables on the Usefulness of Group Support Systems: A Meta-Analysis of Experimental Studies. Small Group Research, 1993, 24, 430-462.

Biros, David P., Joey F. George, and Robert W. Zmud. (2002) Inducing Sensitivity to Deception in Order to Improve Decision Making Performance: A Field Study, MIS Quarterly, 26; 2, 119.

Chiasson, Mike W. and Elizabeth Davidson. (2004) Pushing the contextual envelope: developing and diffusing IS theory for health information systems research, Information and Organization, 14, 155 - 188.

Dennis, Alan R., Barbara H. Wixom and, Robert J., Vandenberg, "Understanding Fit and Appropriation Effects in Group Support Systems via Meta-Analysis", MIS Quarterly, 2001, 25:2, 167 - 193.

Gattiker, Kelley. (Sept. 1999) Morality and Computers: Attitudes and Differences in Moral Judgment. Information Systems Research. 10:3, 233.

Hong, Kwo-Shing, Chi, Yen -Ping, Chao, Louis R, and Jih-hsing Tang. (2003) An Integrated System Theory of Information Security Management, Information Management and Computer Security, AB/Inform Global, 1 1:5, 243.

Hunter, J. E. and F. L. Schmidt. Methods of Meta-Analysis, Sage, Newbury Park, 1990.

Hwang, M. I. (1 996) The use of meta-analysis in MIS research: promises and problem. , Data Base, 27:3, 35 – 48.

Jefferson, D.; Rubin, A.; Simons, B.; Wagner, D. (Oct. 2004) Analyzing Internet Voting Security. Communications of the ACM. 47: 10, 59-64.

Kotulic, Andrew and Clark, Jan Guynes. (2004) Why there aren't more information security research studies. Information and Management. 41, 597- 607.

Lee, J; Shambhu, S; Raghav Rao, H.; Sharman, R. (Dec. 2005) Secure Knowledge Management and The Semantic Web. Communications of the ACM. 48:12; 48-54.

Lee, Y and Kozar, K. (Aug. 2005) Investigating Factors Affecting the Adopting of Anti-Spyware Systems. Communications of the ACM. 48:8, 72- 77.

Madnick, Stuart E. (Fall 1978) Management Policies and Procedures Needed for Effective Computer Security. Sloan Management Review, 20: 1, 61.

McHugh, J. and Deck, F. (June 2005) An Incentive System for Reducing Malware Attack. Communications of the ACM. 48:6, 94-99.

McLeod, P. L. and J. K. Liker. (1992) Electronic Meeting Systems: Evidence From a Low Structure Environment. Information Systems Research, 3:3,195- 223.

Mitroff, Ian I., and James R. Emshoff. (1 979) On Strategic Assumption-Making: A Dialectical Approach to Policy and Planning. Academy of Management Review, 4: 1, 1.

NIST. (Nov. 28, 2000) Federal Information Technology Security Assessment Framework Accessed January 2006 at http://www.NIST.gov

Ocavusoglu, H.; Mishra, B.; Raghunathan, S. (July 2004) A Model for Evaluating IT Security and Investments. Communications of the ACM. 47:7, 87-92.

Palvia, P., Leary, T.D., Mao, E., Midha, V., Pinjani, P., and Salarn, A.F. Research Methodologies In MIS: An Update. Communications of the AIS. Vol 14, article 24, November 2004, pp. 526-542.

Sarathy, R.; Muralidhar, K,; Parsa, R. (2002) The Perturbing Non-normal Confidential Attributes. Management Science. 48: 12.

Security Risk and Management: Strategies for Managing Vulnerabilities and Threats to Critical Digital Assets. CRA Reports, 2003. Accessed January 2006 at http://www.foundstone.com/pdf/security risk management.pdf

Shukla, S and Fui-Hoon Nah, F. (Aug. 2005) Web Browsing and Spyware Instruction. Communications of the ACM. 48:8, 85-90.

Straub, Welke. (Dec. 1998) Coping with Systems Risk MIS Quarterly. 22:4, 441.

Thuraisingham, B. (Dec. 2005) Directions for Security and Privacy for Semantic E-Business Applications. Communications of the ACM. 48: 12; 7 1 – 73

Zhang, X. (Sept. 2005) What Do Consumers Really Know about Spyware? Communications of the ACM. 48:9; 44-48.

Zhu, Prernkurnar, and Zhang, Chu (Fall 2001) Data Mining for Network Intrusion Detection: A Comparison of Alternative Methods. Decision Science. 32:4, 635.

Zviran, Haga. (Spring 1999) Password Security. Journal of Management Information Systems. 15: 4, 16 1.