A Nomological Network Analysis of Research on Information Security Management Systems

Fernando Parra
University of Texas at El Paso
parra@utep.edu

Laura L. Hall
University of Texas at El Paso
lhall@utep.edu

Abstract

This study offers a comprehensive examination of hypothetical concepts related to the behaviors, attitudes, outcomes, processes, experiences, manifestations and indicators connected with an organization's design, implementation and management of a coherent set of policies, procedures and systems to manage risks to its information assets. We introduce network analysis tools as a novel approach to highlight the construct relationships found in Information Security Management Systems (ISMS) literature published in the new millennium. Descriptive results display a significant expansion in the research of ISMS-related phenomena. Network analyses showcase the critical influence of certain constructs in scholarly publications as well as the most salient relationships among these constructs. Our study provides a gap analysis that also underscores those constructs that may require further exploration by this stream of research.

1. Introduction

The innovation of revolutionary information systems over the last few decades, combined with a reduction of trade barriers across countries, aggressive worldwide corporate activism and decisive governmental trade action, has sparked a vast ocean of organizational information that mandate the adaptation of security management paradigms in this new Information Age. Given the volatility of digital information, organizations need to ensure that they manage risks effectively by integrating security initiatives in their daily operations as well as their overall governance. This is a particularly serious mandate given the constant and deliberate attempts to disrupt businesses by a myriad of global security breaches that have been motivated by ill-defined ideologies, state-sponsored international conflict or traditional illicit enterprise [39].

As reported in a special congressional report and a subsequent U.S. Senate hearing before the Subcommittee on Crime and Terrorism, we have experienced a significant rise in computer security breaches that are estimated to have caused losses due to virus, worms, and other form of information security breaches ranging from $13 billion to $226 billion [9,33]. These efforts have not subdued; in the U.S. alone, the Privacy Rights Clearinghouse has documented a total of 3,704 security breach incidents affecting at least 600 million records over the last 9 years [33]. The lack of security systems that can deter information breaches not only impact the livelihood of corporations, but as stated by Defense Secretary Leon E. Panetta [8], they represent a national security threat that could "cause physical destruction and the loss of life…and could shock the nation and create a profound new sense of vulnerability." Risk, although sometimes not detected or recognized, is existent in every business. Thus, it is critical that enterprises have an effective risk management system to sustain the viability of commerce as we know it.

Information Security Management Systems (ISMS), as defined by the International Organization for Standardization in its 27001 standard, is a set of policies concerned with information security management that aim to manage risk with the goal of implementing, monitoring, reviewing, maintaining and improving information security [25]. More specifically, an ISMS encompasses an organization's design, implementation and management of a coherent set of policies, processes and systems to manage risks to its information assets, ensuring acceptable levels of information security risk. Basic concepts of security management have focused on setting the minimal security standards that are determined based on a classification level information sensitivity. Such measures are applied to technology, processes and people that have access to information objects.

Risk management is a critical objective of Information Security Management Systems (ISMS) and it encompasses financial and operational

978-1-4799-2504-9/14 $31.00 © 2014 IEEE
DOI 10.1109/HICSS.2014.536

exposure, data integrity and identification of and containment of strategies for risk [36]. Risk defines the possibility that an event will interfere with the achievement of a firm's objectives; as such, its proper mitigation requires risk awareness by top management, appraisal of a firm's tolerance, allowance for regulatory compliance demands, identifying exposure, and establishing responsibilities [44]. The increasing dependence of business performance on information technology requires an impetus for proper ISMSs that can effectively manage the risk that exists from the operation of information technology.

Over the last century, security policy models for accomplishing these goals included the Bell-La Padula model [3] and the lattice model [24], which focused on protecting information confidentiality. Other models such as the Biba model [5] focused on protecting the integrity of information in any organization. Under these basic models, information security policies are set forth by a priori classifications based on the security classification level of information objects. Contemporary approaches to security management expand on this approach and take risk management as a driving factor in setting up policies [26]. As such, its requirements have a dynamic character that is influenced by risk assessment. This emerging concept of information security embodies a broader scope of information security policy that is interdependent with other management domains, such as institutional variables and environments.

While a myriad of relevant information security management driving issues have garnered increasingly important attention as they are streamed into the information systems literature, no specific research has been developed to summarize the trends in this field of research. The prominent security incidents and the rapid technology developments of the last decade have impelled the rise of academic research on information security management systems. This study introduces network analysis tools as a novel approach to describe the most salient key construct relationships found in Information Security Management Systems (ISMS) literature published since the year 2000 in order to effectively analyze such academic contributions. We first provide questions to drive our research; we subsequently ground the benefits of using network analysis tools to analyze research contributions. We detail the methodology used to conduct our analysis followed by results. We finalize this study by offering a discussion regarding the results and suggest future research directions.

2. Development of research questions

Recent drastic economic changes, dramatic institutional stability changes and revolutionary technology innovations, such as the emergence of the cloud, raise important issues that mandate a review of new contributions. While scholars have placed particular attention to several constructs related to the management of information security, the discipline is limited in scope at a minimum because it has not taken a broader approach in operational issues [41]. Most valuable research articles in this field have not described key ISMS construct interactions from a macro-to-micro level of approach; such contributions, like most research articles, concentrate on a set of narrow dynamics within this field. A broader picture of the literature is necessary to further advance any discipline [e.g. 31, 32]; the application of such a broader analysis would offer an alternative methodology that is intended to advance the insight on the direction of this stream of research as well as assist practitioners to easily identify relevant expertise drawn from applied science.

Through the review of the most recent literature in ISMS, focus is placed on the following research questions:

- Has ISMS research garnered increased academic attention in the last decade?
- What are the most salient ISMS construct relationships?
- Which ISMS constructs are most centric and relevant?
- Which referents are used for the top relevant constructs?
- Which ISMS constructs are most isolated and seem to merit further academic attention?

3. Nomological network analysis

As reviews are conducted to summarize contributions in the literature, scholars resort to a variety of techniques to effectively bring answers across diverse disciplines. Researchers normally use meta-analyses to contrast and combine results from different studies by identifying and measuring the weighted average of a measure of the strength of any given phenomenon. However, a meta-analysis is intended to provide a focused assessment of a particular relationship that has already been identified in the literature with the purpose of providing clarification to a conflicting set of results or to provide a robust, validated summary of previous findings [24]. While this is an effective tool to look for a particular research question, it requires the

formulation of such questions before gathering the literature. This approach would narrow the scope of this study by limiting the research questions to only those that can be defined before conducting the literature search. Thematic reviews summarize the literature pinpointing, examining, and recording patterns or themes that are important to the description of a set of phenomena associated with general specific questions [20]. While thematic reviews tend to be useful in capturing the intricacies of meaning within a broad set of articles, most reviews experience a structural fallacy that originates from the coding of relevant manuscripts into "best fit" categorization, ignoring the possibility that manuscripts may be relevant to multiple themes. More importantly, given that certain themes may be interrelated in a complex manner, the non-granular analysis of articles ignores the specific dynamics of the interaction effects of the constructs within the analyzed articles. This approach would not be adequate for this study because it ignores the critical relevance of the interaction among relevant constructs across the literature. Valuable alternative approaches in discovering interesting patterns on text documents have been offered by information systems scholars [17;29], such cataloguing, may be expanded by focusing on the interaction between constructs, rather than individual constructs.

Cronbach and Meehl [14] contributed the idea of a nomological network in order to examine the construct validity of psychological measures. According to the authors, a nomological network consists of observable items, theoretical constructs, and the relationships between the theoretical constructs and the observable items. Most studies use a nomological network in order to test the validity of a construct within new scales; however, certain studies have used this concept to analyze relationships among constructs within specific topics [10; 28; 31; 32]. In essence, by using a nomological network analysis, patterns and trends can be analyzed at the construct level, rather than at a manuscript level. A nomological network can serve as a unique dataset used to "explore construct relationships, their magnitudes and significances, and their positions in the network" [10]. By aggregating a broad scope of literature that focuses on ISMS and using a nomological network analysis, this study navigates the complex interrelations between constructs. Thus, this study introduces an alternative and novel approach that overcomes the shortcomings of traditional methods to analyze such construct interactions through the use of a network analysis tools of such construct relationships, or dyads, across publications, time and journal tiers.

4. Methodology

Given that our analysis is based on dyadic construct relationships, we observe Kenny, Kashy and Cook's [27] guidelines for dyadic data analysis, proposing the Actor-Partner Interdependence Model as the main method to analyze relationships. In this methodology, both members of a dyadic relationship are assumed to have actor and partner effects. It is essential to note that most research articles are derived from cross-sectional data; as such, it is appropriate for the dyads to lack an actor-partner effect direction. In undistinguishable models such as the case of constructs in this study, the partner and actor effects are assumed to be equal. Based on this premise, we propose to explain deeper phenomena patterns in previous literature by analyzing the prevailing relationships in the form of ties (relationships) of nodes (constructs) rather than the individual constructs themselves.

In addition, Short, Broberg, Cogliser and Brigham [38] highlight deficiencies in text-based content analysis studies that lack content validity and recommends that a researcher should use deductive content validity. Among the steps to avoid this issue and validate the use of content-analysis methodology, the authors suggest the following steps to conduct this type of analysis: (1) Researchers should create a working definition of the constructs of interest using a priori theory when possible. (2) An initial assessment of construct dimensionalities to properly relate constructs should be conducted. (3) An exhaustive list of keywords should be developed, considering the proper terminology to relate constructs. (4) Word lists should be validated using content experts to assess rater reliability, suggesting Holsti's (1969) method for assessing inter-rater reliabilities. (5) Commonly used words from narrative texts should be identified as synonyms of constructs using available software packages and the previous steps should be repeated to validate them. (6) Finally, the authors suggest the assessment of the terms' ability to predict theoretically related variables not captured via content analysis using regression or structural equation modeling.

Observing these guidelines and advancing on previous academic studies [31, 32, 10, 27, 37], the following major steps were thus conducted to address our research questions:

(1) the creation of a taxonomy of keywords into conglomerations of information security management systems' constructs using a priori theory and relevant ISMS literature;

(2) a systematic selection of articles that study information security management systems;

(3) an extraction of keywords provided by authors at the time of publication;

(4) identification of inter and intra relationships of the articles' constructs;

(5) highlight of relevant trending patterns through descriptive statistics and network analysis.

4.1 Identification of nomological constructs

Table 1. Excerpt of theory-based constructs

Construct	Theoretical Grounding
Agency Theory [35]	alignment of interests, contracts, efficiency, information asymmetry, moral hazard, risk sharing, successful contracting, trust
Behavioral Decision Theory [38]	biases, choice, cognitive processes, data completeness, decision processes, decision support, individual differences, inputs, judgmental heuristics, processing, risk assessment, strategy, tasks
Information Systems Control and Auditing Theory [43]	audit, controls, data resources, tests, effectiveness, efficiency, inputs, integrity, operations, processing, output, performance, processes, programming, quality assurance, safeguards, security management, systems development, top mgmt.
Risk Management Theory [45]	assessment, assets, awareness, compliance, controls, effectiveness, impacts, policies, risk assessment, risk management, safeguards, standards, threats, vulnerabilities
ISO/IEC 27000-Series[25],	acceptance, access controls, assets, audit, authorities, authorization, awareness, change management, compliance, confidentiality, continuity, coordination, impacts, cryptography, disciplinary, process, forensics, human resources, incident mgt., operations, policies, information classification, risk, redaction, monitoring, orga. measurements, organizational citizenship, physical security, tests, planning, processes, processing, property rights, regulations, training, response, responsibilities, risk assessment, risk factors, risk management, risk preference, safeguards, security failures, segregation of duties, stakeholders, third-parties, vulnerabilities

Based on the recommendations of Short and colleagues [37], an authoritative taxonomy of constructs was created by matching keywords as referrers of specific construct dimensions to define constructs of interest a priori. While no specific unified theory exists for ISMS, the following theories have been used to explain the underlying principles of ISMS [22]: Risk Management Theory [45], Control and Auditing Theory [43]; Contingency Theory [16]. An excerpt of theories that are reported by the Association for Information Systems [34] as having been used in IS research were also included [1; 2; 11; 13; 35; 38; 40; 42]. In addition, relevant constructs were also extracted from relevant literature on ISMS including ISO/IEC's 27000 series [25], COBIT [12] and SSAE 16[40]. Table 1 provides an excerpt of the 230 a-priori nomological constructs offered by theory or relevant literature.

4.2 Systematic selection of sources for articles related to ISMS

Given the interdisciplinary nature of ISMS and the relatively scarce number of publications in the subject, the sources for articles were defined by selecting relevant national and international peer-reviewed journals in business management, information systems and security that were indexed by the major academic databases: Academic Search Complete, Psychology and Behavioral Sciences Collection, Business Source Complete and Inspec. In order to assess a journal's relative importance within its field, the average number of citations to its recent published articles was used as a proxy for relative ranking. SCImago' Journal Rank & Country Rank (SJR indicator) has been established as a reputable measure of scientific influence of scholarly contributions that is based on both the number of citations received by its publications as well as the level of prestige of the citing source.

In alignment with this study, the SJR indicator bases is algorithm on network analysis similar to the widely known algorithm Google PageRank, which establishes different values for citations according to the scientific influence of the journals that generate them. This approach uses a three-year citation window that sufficiently covers both the citation peak of a significant number of journals and reflects the dynamics of the scholarly communication process [19]. A total of 180 journals were ultimately selected as the target source for articles related to ISMS. All journals were ranked based on their SJR indicator for 2011. All journals were subsequently grouped into three tiers: Tier 1 journals had an SJR of 1.0 or above

Table 2. Journal Sources

Journal	SJR
Tier 1	
ACM Computing Surveys	9.93
ACM Transactions on Database Systems	4.20
Administrative Science Quarterly	5.65
IEEE Transactions on Industrial Electronics	3.12
IEEE Transactions on Software Engineering	3.29
Information Systems Research	3.65
Journal of the ACM	5.95
MIS Quarterly	5.14
Organization Science	5.47
Strategic Management Journal	5.22
Tier 2	
Behaviour & Information Technology	0.55
IBM Journal of Research & Development	0.59
Information Management & Computer Security	0.46
Information Technology & People	0.48
Journal of Computer Information Systems	0.52
Journal of Computer Sciences	0.52
Multimedia Tools & Applications	0.58
Technology Analysis & Strategic Management	0.55
Telecommunications Policy	0.59
Total Quality Management & Business Excellence	0.51
Tier 3	
Information Systems Security	-
International Journal of Computer and Network Security	-
Journal of Accountancy	-
Journal of Digital Forensics, Security & Law	-
Journal of Information Privacy and Security	-
Journal of Information Processing	-
Journal of Service Science	-
Journal of Strategic Security	-
Studia Informatica	-
Theoretical & Applied Economics	-

which indicate those journals which have the highest academic status based on the impact of their scholarly contributions; Tier 2 contained those with a lower SJR than 1.0; and, Tier 3 contained all those journals without an SJR indicator. Table 2 provides an excerpt of these selected sources.

Our selection of publication date was motivated by the rise of prominent cyber security incidents beginning with the year 2000, the technology significant technological events of the last decade, and the intent to limit our scope to the most relevant research studies in this era. As such, a search for scholarly manuscripts was conducting ranging from January 2000 to May 2013 based on the following full-text phrases: "information security risk", "information security risk management", "information security management" and "information security management systems". The abstracts from the identified articles were examined to determine whether an ISMS theme was addressed by the study. Journal articles that were not peer-reviewed were excluded; several other articles were excluded on the basis of relevance or duplication across indexing databases. The search query yielded a total of 439 peer-reviewed articles pertaining to ISMS research within the specified range of dates.

4.3 Extraction of keywords and correlation to nomological constructs

Keywords provided by authors were extracted using the EBSCOHost digital librarian tools. These keywords were compared with original text for accuracy. Keywords were imported into a relational database that captured normalized information into different tables, including articles, keywords, constructs, theories, and journals.

Keywords extracted from research articles were analyzed for association with a pre-defined constructs that were previously defined by theory and relevant literature. Specifically, a total of 2,815 keywords were examined to determine whether they matched a dimension of any ISMS construct, defined for purposes of this study as referents related to the behaviors, attitudes, outcomes, processes, experiences, manifestations and indicators connected with an organization's design, implementation and management of a coherent set of policies, processes and systems to manage risks to its information assets.

Holsti's [21] method for assessing inter-rater reliabilities was used to validate the association of keywords and constructs. As different constructs emerged in the analysis of keywords, the list was revised by committee of academic experts on this field of research; for disagreement in coding, a

discussion was held to arrive to a consensus. If a keyword could refer to more than one construct, a group discussion was held and the most relevant construct was used. Table 3 provides a representative sample of extracted keywords and how they were aligned to constructs.

Table 3. Keyword-Construct Correlation

Referents/Keywords (examples)	Construct
adoption, assimil., adoption levels	Adoption
accreditation, assurance services, certification, cert. organisations, certified security professionals	Assurances
confidentiality, data privacy, privacy, sensitive information	Confidentiality
corporate culture, cultural aspects, cultural differences, cultural dimensions, culture	Culture
security investment	IT investment
continuous improvement, six sigma (quality), quality mgmt..	Quality Assurance
risk analysis, risk assessment, risk forecasting, risk perception, risk quantification, risk assessment	Risk Assessment

4.4 Identification of relationships among constructs for each article

Using a relational query that matched each article's keywords with a given construct, we obtained a dataset that resulted in a set of constructs for each article. In essence, upon alignment of keywords, each article was assigned the corresponding constructs. A small representative sample of articles and their respective constructs is shown in Table 4. Hovav and D'Arcy's [23] research examined whether national culture influenced the deterrent capabilities of security policies, security education, computer monitoring, and awareness programs. The article contained several keywords, some of them were aligned to the following specific constructs: culture, international environment, people, policies, security management, training, and value. Similarly, Mookderjee and colleagues' [30] contribution contained keywords that were aligned to security management, security failures, security, policies, people, organizational, behavior, industry, deviant behavior and assessment. Bodin et al.'s [6] contribution, included keywords that were aligned to security management, security, risk management, policies, information system types, industry and access controls. Therefore, a matrix for these articles would display an interconnected association amongst all constructs as displayed in Figure 1. Such matrix, contains crossover construct relationship between security, security management, policies, people, and industry. However, the most relevant relationship across all articles is security management and policies, which was addressed by the three articles. This processes is further detailed in next section.

Table 4. Article Construct Relationships

Article	Construct Relationships
Hovav and D'Arcy [23]	culture, environment-international, people, policies, security management, training, value
Mookerjee, Mookerjee,& Bensoussan [30]	security management, security failures, security, policies, people, organizational behavior, industry, deviant behavior, assessment
Bodin, Gordon, Loeb [6]	security management, security, risk management, policies, information system types, industry, access controls

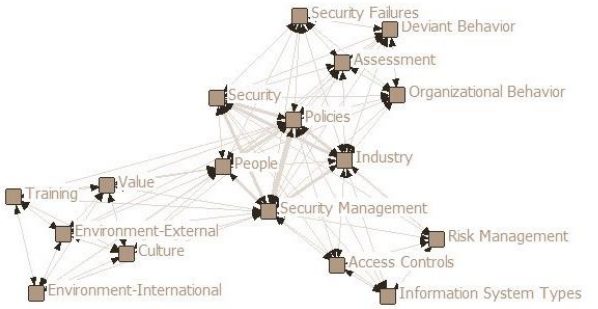

Figure 1. Sample construct matrix

4.5 Highlight of relevant trending patterns through descriptive statistics and network analysis

Various descriptive statistics are given based on the grouping by elements captured in the dataset including construct frequencies, authorship, and constructs. Given the network relationship approach of this study, we borrowed the methodology used by Parra et al [31; 32] and Chen [10], and constructed a matrix of the ISMS construct dyads. This social network is represented by dyad frequency observations. Using UCINET 6.0 software [7], four different types of analysis provided insight on the ISMS literature.

First, centrality measures were utilized to identify those constructs that have the most connections with other nodes. As described by Freeman [18], the degree of centrality provides the sum of the values that a given node holds to its neighbors, a higher degree represents a more powerful influence. Similar to an individual in a social network with many connections or friends would be considered an influential person, a construct with a higher degree of centrality would be considered to affect ISMS phenomena because it has been studied more frequently with other constructs.

Second, a degree of betweeness was assessed to identify those constructs that are more critical in the literature. The degree of betweeness, also a measure of a node's centrality, was offered by Freeman [18] to describe the number of shortest paths from all vertices to all others that pass through that node inside a network. Betweenness is a useful measure of both the load and importance of a node. The higher the degree of betweenness a node displays, the more critical it is in connecting other constructs because it plays a core position in the network [10]. In a network of individuals, a person through which more individuals depend in order to connect from one side of a network to another in the most efficient way, the more important it is. As such, a construct with higher betweenness would namely play a core position in ISMS research.

Finally, our study analyzed structural holes, or those within the network with missing links. This degree of structural deficiency may suggest a gap in the network, which in turn will suggest that particular phenomena relationships might merit further exploration in the literature.

5. Results

To address whether ISMS research has garnered increased academic attention in this millennium, we first conducted a descriptive analysis which confirms a growing trend in the number of research studies conducted per year. Figure 2 summarizes this trend; and, it displays the proportional contribution of articles based on their tier. The trend exhibits a cumulative growth in publications over the last 12 years. While all tiers display a rise in the importance of ISMS phenomena, Tier 2 exhibits a higher linear slope of growth (β_{Tier2} = 1.83) followed by Tier 3 journals (β_{Tier3} = 1.51). Tier 1 Journals exhibit a moderate rise in attention (β_{Tier1} = 0.43).

Network analysis tools were utilized to address all other research questions. A total of 8116 unique construct dyads were incorporated in a network. Figure 3 displays a net diagram highlighting the most relevant construct relationships across the literature with bolder connections, weaker ties (f < 4) are not displayed to provide more visual clarity.

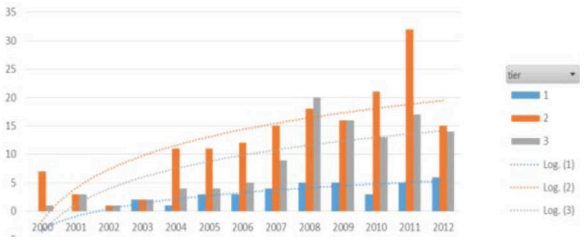

Figure 2. Publication trends by journal tier

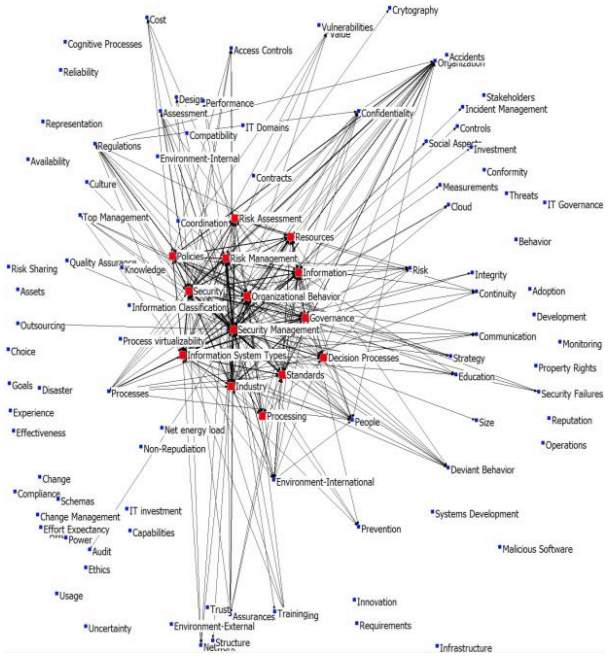

Figure 3. ISMS network diagram

In order to underline the most salient ISMS construct relationships, we reviewed the full nomological matrix with an effect size of at least 23 ties. We find that the most relevant construct relationships are concentrated in the interaction of 14 different constructs highlighted in red (Figure 3). Such constructs have asymmetric interactions across this core network. Table 5 provides the 10 most salient ISMS construct relationships that have dominated the academic research interest in this millennium. Such interactions are further discussed in our next section.

To feature the ISMS constructs that have been more relevant, we utilized network centrality measures. Normalized degree of centrality measures reveal the constructs that are more relevant in ISMS due to the frequency in which they have been researched with other constructs.

Table 5. ISMS most salient relationships

Construct	Construct	Ties
Security Management	Risk Management	91
Security Management	Security	91
Security Management	Information System Types	63
Security Management	Industry	51
Security Management	Organizational Behavior	45
Security Management	Standards	45
Security Management	Information	39
Security Management	Resources	37
Security	Info. System Types	35
Security Management	Policies	32

Table 6. Construct centrality measures

Centrality	Betweeness
Security Management (0.907)	Security Management (0.137)
Security (0.769)	Security (0.073)
Information System Types (0.769)	Information System Types (0.068)
Governance (0.667)	Governance (0.041)
Policies (0.667)	Policies (0.034)
Information (0.667)	Information (0.03)
Industry (0.62)	Risk Management (0.03)
Risk Management (0.611)	Risk Assessment (0.03)
Organizational Behavior (0.611)	Industry (0.028)
Risk Assessment (0.602)	Regulations (0.028)

Betweeness measures reveal the constructs with a suggested core position in ISMS research. Table 6 displays the top 10 most relevant constructs and the top 10 which are suggested to have played a core position in research in this new millennium. In order to explicate these results, Table 7 provides an excerpt of the referents for the top 5 constructs, further expanding on our original research questions.

Finally, this study applied structure holes using effective sizes and efficiencies to explore the missing links in ego networks to identify the ISMS constructs that were most isolated and seem to merit further academic attention. Ego networks with a higher efficiency value suggest there are more missing links.

Table 8 provides the top 6 ISMS constructs which were found to have the most missing links in their structural network.

Table 7. Referents for top constructs

Construct	Referents
Security Management	computer security mgmt., information systems security mgmt., patch mgmt., power system protection, power system security, safety mgmt., security mgmt., security of data, security systems, optimal security mgmt.
Security	data protection, enterprise info. sec., data sec., computer network sec., cyber sec., computer sec., database sec., firewalls, industrial safety, sec., information sec., information systems sec., internal sec., IT sec., network sec., telecom. sec.
Information System Types	applications, communication syst., client-server syst., courseware, decision support syst., document imaging syst., electronic syst., email syst., extranets, expert syst., medical syst., groupware, enterprise syst., intelligent syst., and 65 others.
Governance	I.S. governance, health care org. administration, I.S. management, ISMS, IT Governance, QA admin, organization and administration
Policies	measures, security policies, policy formation guidelines, economic policies, educational policies, incentive schemes, and 12 others

Table 8. Network structural gaps

Construct	Degree	EffSize	Efficiency
Security Mgmt.	98	77.633	0.792
Adoption	23	17.56	0.763
Threats	24	18.117	0.755
Value	42	31.289	0.745
Investment	22	16.338	0.743
People	54	40.002	0.741

6. Discussion

The main purpose of this study was to provide an examination of the relationships prevailing in the Information Security Management Systems literature published in the new millennium. Our findings suggest that there has been a significant expansion in the research of ISMS-related phenomena. Such stream of research has been mainly focused around the interaction of different aspects of security

management with risk management principles in a variety of security domains. Scholars have also explored a variety of security management issues experienced in different industry settings and different types of information systems. Research has also concentrated on organizational aspects and organizational standards as they relate to security management.

Our findings highlight the most relevant constructs of the stream of research suggesting that security management and security issues are naturally the most relevant constructs. Interestingly, a variety of different systems types were used in connection with ISMS studies, suggesting an attempt by scholars to duplicate findings in different application settings. Governance and policies, were also evidenced to be trending constructs in the literature. These findings should serve as a guide for those researchers that aim to provide a comprehensive summary of the literature organized around constructs and their interactions.

Security management issues still merit further discussion which will be evidenced by the future rise of related publications in the next decade. More importantly, our study suggests there is a need to further explore both threats and technology adoptions and their effects on ISMS. We further suggest that scholars should examine the value of ISMS-related investments; for example, the value of obtaining a third party ISMS assurance certifications or the risk mitigation value of implementing an enterprise system. Finally, our study also suggests that more research is needed in the human element of ISMS.

This study is limited by the accuracy of keywords provided by authors as construct referents. As such, it is possible that the keywords listed on each one of the articles might not sufficiently reflect all the constructs discussed in the underlying studies. We would welcome future studies that validate this study's methodology. We propose a future literature review that expands on the most relevant and the most deficient construct relationships that were identified in study.

7. References

[1] Alchian, A., and H. Demsetz, "Production, Information Costs, and Economic Organization", American Economic Review, 1972, 62(5), pp. 777-795.

[2] Bandura, A. "Self-efficacy: Toward a Unifying Theory of Behavioral Change". Psychological Review, 1977, 84(2), pp. 191–215.

[3] Bell, D.E., and L.J. La Padula, "Secure Computer Systems: Mathematical Foundations," MTR-2547, Vol. I, The MITRE Corporation, Bedford, MA, March 1, 1973.

[4] Bertalanffy, L.V., "General system theory - A Critical Review" General Systems, 1962, 7, pp. 1-20.

[5] Biba, K.J. "Integrity Considerations for Secure Computer Systems", MTR-3153, The Mitre Corporation, Bedford, MA, April 1977.

[6] Bodin, L.D., L.A. Gordon, and M.P. Loeb, "Information Security and Risk Management", Communications of the ACM, 2008, 51(4), pp. 64-68.

[7] Borgatti, S.P., M.G. Everett, and L.C. Freeman, Ucinet for Windows: Software for Social Network Analysis. Harvard, MA: Analytic Technologies, 2002.

[8] Bumiller, E., and T. Shanker. "Panetta Warns of Dire Threat of Cyberattack on U.S.", The New York Times, October 12, 2012.

[9] Cashell, B., W.D. Jackson, M. Jickling, and B. Webel, "The Economic Impact of Cyber-Attacks", Congressional Research Service, Government and Finance Division, The Library of Congress, Washington DC, 2004.

[10] Chen, C.C. "Empirical Examination of Sales Research: Meta-Analysis, Social Network and Nomological Network Analyses, Dissertation, University of Texas at Arlington, 2011.

[11] Coase, R.H., "The Nature of the Firm". Economica, 4(16), pp. 386-405.

[12] "COBIT 5", Information Systems Audit and Control Association, Rolling Meadows, IL, 2012.

[13] Compeau, D.R., and C.A. Higgins, "Application of Social Cognitive Theory to Training for Computer Skills", Information Systems Research, 1995, 6(2), pp. 118-143.

[14] Cronbach, L.J., and P.E. Meehl, "Construct validity in psychological tests". Psychological Bulletin, 1955, 52(4), p. 281.

[15] Denning, D.E., and P.J. Denning. "Certification of programs for secure information flow", Communications of the ACM, 1977, 20(7), pp. 504–513.

[16] Drazin, R., and A.H. Van de Ven, "Alternative Forms of fit in Contingency Theory", Administrative Science Quarterly, 1985, 30 (4), pp. 514-539.

[17] Feldman, R., and I. Dagan, "Knowledge Discovery in Textual Databases (KDT)", Proceedings of the 1st International Conference on Knowledge Discovery in Databases and Data Mining, 1995.

[18] Freeman, L.C., "Centrality in Social Networks: Conceptual Clarification," Social Networks, 1979, 1(3), pp. 215-239.

[19] González-Pereiraa,B., V.P. Guerrero-Boteb, and F. Moya-Anegónc, “The SJR Indicator: A New Indicator of Journal' Scientific Prestige”, 2009, arxiv.org/abs/0912.4141

[20] Guest, G., Applied Thematic Analysis, Sage, Thousand Oaks, California, 2012, p.11.

[21] Holsti, O., “Content Analysis for The Social Sciences and Humanities”, Addison-Wesley, Don Mills, ON, 1969.

[22] Hong, K.W., Y.P. Chi, L.R. Chao, and J.H. Tang, “An Integrated System Theory of Information Security Management”, Information Management & Computer Security, 2003, 11(5) pp. 243-248.

[23] Hovav, A., & J. D'Arcy, “Applying an Extended Model of Deterrence Across Cultures: An Investigation of Information Systems Misuse in the U.S. and South Korea”, Information and Management, 2012, 49(2), pp. 99-110, doi:DOI: 10.1016/j.im.2011.12.005.

[24] Hunter, J.E. and F.L. Schmidt (2000), “Fixed Effects vs. Random Effects Meta-Analysis Models: Implications for Cumulative Research Knowledge, International Journal of Selection and Assessment, 2000, 8(4), pp. 275-292.

[25] ISO and IEC, “ISO/IEC 27001:2005 Standard”, International Organization for Standardization and the International Electrotechnical Commission, October 2005.

[26] Jaquith, A., Security Metrics, Addison-Wesley, 2007.

[27] Kenny, D.A., D.A. Kashy, and W.L. Cook, Dyadic Data Analysis; Methodology in the Social Sciences, The Gilford Press, New York, NY, 2006.

[28] Le, H., F.L. Schmidt, J.K. Harter, and K.J. Lauver, “The Problem of Empirical Redundancy of Constructs in Organizational Research: An Empirical Investigation,” Organizational Behavior and Human Decision Processes, 2010, 112(2), pp. 112-125.

[29] Lent, B., R. Agrawal, and R. Srikant, “Discovering trends in text databases”. Proceedings of the 3rd International Conference on Knowledge Discovery in Databases and Data Mining, 1997.

[30] Mookerjee, V., R. Mookerjee, and A. Bensoussan, “When Hackers Talk: Managing Information Security under Variable Attack Rates and Knowledge Dissemination”, Information Systems Research, 2011, 22(3), pp. 606-623, doi:10.1287/isre.1100.0341

[31] Parra, F., P. Kirs, and G. Udo, “A Trend Analysis of Information Systems Sourcing”, Decision Science Institute 43rd Annual Meeting, San Francisco, CA, 2012.

[32] Parra, F., T. Han, A, Peters, and P. Vidyarthi, “A Thematic Trend Analysis of Relationships Among Organizational Behavior Constructs”, Academy of Management and Business Conference: Boston, MA, 2012.

[33] PrivacyRights.org. “Chronology of Data Breaches”, www.privacyrights.org/data-breach, Retrieved May 1, 2013.

[34] Schneberger, S. and M. Wade, “Theories Used in IS Research”, Association for Information Systems, home.aisnet.org/displaycommon.cfm?an=1&subarticlenbr=209, Retrieved May 1, 2013.

[35] Selznick, P., “Foundations of the Theory of Organizations”, American Sociological Review, 1948, 13, pp. 25-35.

[36] Sherwood, J., A. Clark, and D. Lynas, Enterprise Security Architecture: A Business-Driven Approach, 1st Edition, CMP Books, Gilroy, CA, 2005.

[37] Short, J.C., J.C. Broberg, C.C. Cogliser, and K. Brigham, “Construct validation using computer-aided text analysis (CATA): An illustration using entrepreneurial orientation”, Organizational Research Methods, 2009, 13(2), pp. 320-347.

[38] Simon, H.A., "Theories of Decision Making in Economics and Behavioral Science." American Economic Review, 1959, 49(1), pp. 253-283.

[39] Snow, G.M., “Statement before the senate judiciary committee Subcommittee on Crime and Terrorism”, U.S. Senate, www.fbi.gov/news/testimony/cybersecurity-responding-to-the-threat-of-cyber-crime-and-terrorism. (April 12, 2011)

[40] “Statement on Standards for Attestation Engagements 16”, American Institute of CPAs, Washington, DC, 2010.

[41] Steinbart, P. J., R. L. Raschke, G. Gal, and W. N. Dilla, “Information Security Professionals' Perceptions about the Relationship between the Information Security and Internal Audit Functions”, Journal of Information Systems, In-Press, 2013.

[42] Stoneburner, G. “Underlying Technical Models for rmation Technology Security”, NIST Special Publication 800-33, National Institute of Standards and Technology, Washington, DC, December 2001.

[43] Weber, R., Information System Control and Audit, Prentice-Hall, Englewood Cliffs, NJ, 1999.

[44] Wilkin, C.L., and R.H. Chenhall, “A Review of IT Governance: A Taxonomy to Inform Accounting Information Systems, Journal of Information Systems, 2010, 24(2), pp. 107-146.

[45] Wright, M., “Third Generation Risk Management Practices”, Computer Fraud & Security, 1999, 2, pp. 9-12.