African Journal of Business Management Vol. 6(1), pp. 213-221, 11 January, 2012
Available online at http://www.academicjournals.org/AJBM
DOI: 10.5897/AJBM11.1764
ISSN 1993-8233 ©2012 Academic Journals

Full Length Research Paper

A knowledge network production: Ten years of information security research

Chuan-Yuh Wang

Center for General Education, National Quemoy University, Kinmen, Taiwan, 710, R. O. C.
E-mail: def1234@ms9.hinet.net. Tel: +886-921290123. Fax: +886-6-6221719.

Accepted 19 September, 2011

This study explores and maps the intellectual structure of information security studies from 1998 to 2007, by analyzing 3059 cited references of 223 articles from information security in ssci and sci databases, bibliometric, multivariate analysis and social network analysis techniques used to map the important publications and most influential scholars, as well as the correlations between publications through analysis of citations and co-citations. A systematic and objective evaluative tool is introduced to determine the relative importance of different knowledge nodes in the development of information security research. Five factors emerged: (1) Information security management and assessment, (2) information security investment, (3) information security techniques, (4) information systems security monitoring and development (5) cryptographic technology design.

Key words: Information security, intellectual structure, bibliometric technique, social network analysis.

INTRODUCTION

The end of the 20th century and the beginning of the 21st were marked by rapid advancements in telecommunications, computing hardware and software, and data encrypttion. The widespread use of electronic data processing and electronic business through the Internet, in addition to increased occurrences of international terrorism, fueled the need for improved data protection. The academic disciplines of computer security, information security and information assurance developed in tandem with numerous professional organizations in the interest of ensuring the security and reliability of information systems.

Information security entails the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction (Allen, 2001). The terms information security, computer security and information assurance are often and erroneously, used interchangeably. Despite sharing the common goals of protecting the confidentiality, integrity and availability of information, there are some subtle differences in their respective approaches to the subject, the methodologies used and the areas of concentration. Information security pertains to the confidentiality, integrity and availability of data, irrespective of the form data takes: electronic, print or other forms. Researchers have produced articles in this field over the last decade. When these findings are disseminated to scholars and managers in journal articles, and other documents, readers find they have no means at their disposal to map the field. Although, many studies have explored this issue (Axelsson, 2000; Denning, 2000; Dhillon, 2007; Gordon and Loeb, 2002; Power, 2001), they are limited by their dependence on the subjective assessment of different professionals. Such an approach is unable to account for the lack of consensus in the field.

The present study employs a theory-based citation and co-citation analysis. Citation analysis uncovers the interlinked nodes. From these sources, the most influential publications and scholars in the information security field are identified. Co-citation analysis investigates the

Abbreviations: NA, Network analysis; **SRM,** security risk management; **IS,** information security; **ROSI,** return on security investment; **3D,** three-dimensional.

intellectual structure of information security between 1998 and 2007. Profile analysis and bibliometric techniques were used to create maps of the relationships among authors as perceived by scholars citing their paper over the stipulated periods. Documents were counted from a chosen field – paired or co-cited documents.

This study provides a tool for evaluating information security publications and to provide a systematic and objective means of determining the relative importance of different knowledge nodes in the development of information security research. The purpose of this study is to explore and map the intellectual structure of information security studies from 1998 to 2007. This paper also attempts to help researchers identify the important publications and the influential scholars as well as the correlations among these publications by analyzing citations and co-citations.

LITERATURE REVIEW

A knowledge network in the information security field is comprised of a sufficiently large number of published articles, the active researchers and citations appearing in various media relating to electronic commerce and other fields (Ngai and Wat, 2002; Shaw et al., 1997; Wareham et al., 2005). This knowledge network can depict the developmental patterns of information security. During the accumulation of cross-field knowledge, key nodes are the most important bridges used to connect separate domains. They attain their status during the process of cross-fertilization, which facilitates communication.

Acedo and Casillas (2005) considered two approaches. The first is a subjective approach based on a qualitative analysis of the literature, starting from the researcher's interpretation. The second approach is objective, based on bibliographical analysis that is quantitative in nature. Each has its own pros and cons, so they should be construed as complementary to understand the structure of any field of study. Our paper used an objective measure to identify the primary criterions within the field of information security. Based on bibliometric analyses, this is a method widely used to map epistemological fields (Acedo et al., 2001; Culnan, 1986; Knight et al., 2000; Pilkington and Liston-Heyes, 1999).

Bibliometrics is a research method that originated in library and information science. It uses quantitative analysis and statistics to describe patterns of publication within a given field or body of literature. Researchers can use bibliometric techniques to determine the influence of a single author, or to describe the relationships with other authors. Citation analysis is based on the hypothesis that authors cite papers they consider important to their research. Chandy and Williams (1994) pointed out that citations are viewed as the explicit linkages between articles with commonalities. Many researchers have studied citations, the “raw data” of citation analysis.

Cronin (1984) described the citation process as a detailed theoretical scrutiny that includes a review of the role and the content of citations. Co-citation analysis records the number of papers that have cited any particular pair of documents. It is interpreted as a measure of the degree of similarity between the content of documents. Co-citation analysis is a bibliometric technique used by information scientists to “map” the topical relatedness of clusters of authors, journals, or articles that is the intellectual structure of a research field. Co-citation studies compile co-citation counts in a matrix form and statistically scale them to capture “a snapshot at a distinct point in time of what is actually a changing and evolving structure of knowledge” (Small, 1993).

Several studies have used bibliometric techniques to study management research. For example, Pilkington and Teichert (2006) investigated the intellectual pillars of the management of technology literature and explored whether these are distinct from those commonly associated with its rival fields; Acedo and Casillas (2005) explored the research paradigms of international management research by applying factor analysis techniques in an author co-citation study; Ramos-Rodriguez and Ruiz-Navarro (2004) examined the intellectual structure change of strategic management research by conducting a bibliometric study of the strategic management journal; Ponzi (2002) focused on the intellectual structure and interdisciplinary breadth of knowledge management in its early stage of development, using principle component analysis on an author co-citation frequency matrix.

Two major methodological approaches can be distinguished (Chandy and Gopalakrishna, 1992). The first is based on subjective and qualitative analyses. It includes the most recent contributions of Buckley (2002) and Lu (2003). The second employs objective tools of analysis, usually based on bibliometric analysis. The study proposes an objective criterion to identify the main paradigms of information security. The present work can be included within the sub-group, as it complements the outlook provided by the first approach. No study has treated the field of information security; therefore, this study aims to fill a gap in information security literature by applying bibliometric, multivariate analysis and social network analysis techniques to a representative collection of research articles to map the structure of this field.

METHODOLOGY

The research methods used for this study are bibliometric and social network analysis. Bibliometrics is a theory-based citation and co-citation analysis. Using citation analysis, the interlinked invisible nodes are discovered from which the most influential publications and scholars in the information security field are identified. Further, co-citation analysis is conducted using social network analysis to explore the intellectual structure of the information security studies. The knowledge nodes that have contributed most to information security studies are to be explicated, along with their evolutionary patterns.

The general methods of data gathering and analysis in author co-

citation analysis have been described by various scholars (McCain, 1983, 1984, 1990; White and Griffith, 1981; White, 1983). Detailed discussions of retrieval strategies and techniques of data manipulation are available in these publications. Based on this, the purpose of this study is to explore and map the intellectual structure of modern information security studies from 1998 to 2007.

Co-citation counts of all author pairings over the period in question are organized into a matrix. The values in the diagonal cells are scaled to fit the range of co-citation values in the corresponding column (White, 1983). Citation networks are like social networks in which the actors are journals, articles, or authors. The valued resources are ideas and knowledge, and the interactions are actors' mutual citations. We used the graphing program NetDraw (Borgatti et al., 2002) to examine co-citation matrixes. In addition, a companion software package for NetDraw, Ucinet, was utilized to develop measures of degree, closeness and betweenness. Nodes high on closeness have the shortest paths to all others and they monitor what is happening in the network. Finally, betweenness is a calculation of influence. A node with high betweenness has great influence over what flows in the network. With bibliometric, multivariate and social network analysis, this study has assumed three phases, each of which required different approaches to examine the evolution of information security studies.

Selection

The databases of SSCI and SCI from 1998 to 2007 serve as the base for our analysis owing to their reputations and their extensive collection of 8,292 (SSCI-1866, SCI-6426) refereed journals (JCR Social Sciences Edition, 2007). SSCI and SCI provide the most comprehensive and widely accepted databases of information security publications. We used "key words" search of the journal title fields and the subject categories in the SSCI and SCI databases to choose sample articles.

Data collection and analysis

Citation data was collected by counting the number of articles published in the references these articles cited between 1998 and 2007, resulting in a total of 223 published articles and 3,059 cited publications. Citation was tabulated for each of the 223 source documents. These data were then imported to Microsoft Excel for analysis. Approximately 116 highly-cited documents were identified, of which 30 were selected for inclusion. Following a series of operations, key nodes in the knowledge network of the information security studies were identified. From this point, a structure started to become discernible.

Data mapping

The key-nodes from 1998 to 2007 were identified (a co-citation matrix). This data was imported to Ucinet software (Borgatti et al., 2002) for social network analysis and factor analysis (Pilkington and Teichert, 2006). The intellectual structure of information security was mapped to describe the knowledge distribution process in the information security area.

We used r-Pearson as a measure of similarity between author pairs, because it registers the likeness in shape of their co-citation count profiles over all other authors in the set (White and Griffith, 1981). The co-citation correlation matrix was analyzed using varimax rotation, a commonly used procedure, which attempts to fit (or load) the maximum number of authors on the minimum number of factors.

The factor analysis divides the authors according to the similarities of their article contents into several groups. Each individual group represents a different subfield or research issue within information security. Factor analysis permits us to derive subfields from the co-citation matrix. Subfields correspond to the extracted factors, and each subfield represents an intellectual theme defined by the works of authors who load highly on that subfield/factor. The amount of variance explained by a factor can be construed as its contribution to the conceptual foundation of the field. Subfields that exhibit a high cumulative tradition in research are likely to account for a larger percentage of the total variance. We have considered that a work should be included in a trend when its loading is equal to or greater than 0.4, and if the loading is greater than 0.7 the work is a contribution of great relevance within the corresponding paradigm (Acedo and Casillas, 2005).

Network analysis (NA) is an analytical tool that reveals the number of interactions and consequently, the closeness of the relationships between nodes within a network. It produces diagrammatical representations of the relative distance between nodes, and illustrates structural patterns and differing positions within the network (Wasserman and Faust, 1997). The graphing program NetDraw was used to examine the co-citation matrixes (Borgatti et al., 2002). Social network analysis tools may be used to graph the relations in the co-citation matrix and identify the strongest links and the core areas of interest in information security (Pilkington and Teichert, 2006).

RESULTS AND DISCUSSION

Citation analysis

The preliminary phase of data analysis produced the frequency of journal citations, which are presented in statistical form in Table 1. The subject category scope includes: computer science, information systems, optics, hardware and architecture, software engineering, theory and methods, interdisciplinary applications, engineering, industrial, electrical and electronic, business and management, alongside the specific information security journals.

Among all the cited journal articles, the most cited information security article titles between 1998 and 2007 are: Gordon and Loeb (2002) "The economics of information security investment," followed by Straub and Welke (1998) "coping with systems risk: Security planning models for management decision making," and Kotulic and Clark (2004) "Why there are not more information security research studies" (Table 2).

These articles are highly influential in information security research and collectively define this field. Although, it does not exclude the bias against recent articles, it still represents the focus of the primary articles and provides an indication of the popularity of some information security topics between 1998 and 2007.

Co-citation analysis

Data mapping was conducted and the intellectual structure of information security studies revealed by using co-citation analysis. Co-citations were tabulated for each of the 223 source documents using Microsoft Excel. Many of the authors had very low co-citations and were either

Table 1. Highly cited journals in information security studies.

No.	Journal name	Fq.
1	Computers and security	43
2	MIS Quarterly	19
3	Optics letters	19
4	Information and management	19
5	Communications of the ACM	17
6	Industrial Management and Data Systems	13
7	Applied Optics	10
8	Lecture Notes in Computer Science	10
9	Optical Engineering	10
10	ACM Transactions on Information Systems	9
11	Information Management and Computer Security	7
12	IEEE Transactions on Information Theory	6
13	Optics Communications	6
14	Harvard Business Review	5
15	IEEE Security and Privacy	5

either unlikely to have had a significant impact on the development of the field, or their publications were too recent to have had any significant impact. Following the recommended procedures of White and Griffith (1981), the total numbers of citations in the selected journal articles were used to identify the top 20 scholars, and then a co-citation matrix (20×20) was created to represent the correlations among different publications.

Multivariate methods such as factor analysis and social network analysis effectively highlight author relationships. Factor analysis attempts to explain the interrelationships among the variables through the creation of a much smaller number of derived variables of factors (McCain, 1990); it is, in effect, a data reduction method. Authors in specialized areas typically build on each other's ideas, and are likely to be co-cited by other researchers in the field (McCain, 1990). Such authors are loaded onto the same factor. The factor loading is an indication of the degree to which an author belongs to or loads on a factor. A factor is thus deemed to be a subfield whose theoretical underpinnings can be gleaned by examining the published output of those who load highly on it. The eigenvalue refers to the variance accounted for by a factor (Hair and Anderson et al., 1998), or the squared loadings on the factor. The result from the factor analysis gives five main groups. The general concepts and research interests of these five groups are relatively independent of each other. In our study, factor groups were ranked from 1 to 5, indicating decreasing effectiveness to represent the entire field of information security research. Authors were classified by each factor group according to their relatedness in terms of research issues to other authors created in the same factor group (Table 3 and 4).

Clearly, Gordon, Straub and Kotulic (Table 2) authored the three most influential articles in information security research over the last decade. From Table 4 we can see Kotulic loaded in factor 1, Gordon loaded in factor 2 and Straub loaded in factor 3 respectively. Gordon was not classified as part of the first factor group. This increases the problem as to why these highly cited authors were classified by the Ucinet procedure into the second factor group. We attribute this to the fact that many of them hold senior status in the field, and therefore, they are cited in most articles relating to information security research. The most cited articles and often the most influential written by these three authors, were early works and therefore might not be representative of the main research issues in information security.

Social network analysis tools can be used to graph the relations in the co-citation matrix and identify the strongest links and the core areas of interest (Pilkington and Teichert, 2006) in information security. Figure 1 shows the core of the co-citation in journal articles with links of co-citations shown in the network and using the "Eigenvalue$<$1" rule for stopping extraction of factors. Ucinet software (Borgatti et al., 2002) shows in graphic form the core areas of interest. The different shapes of the nodes result from performing a faction study of these authors. This method seeks to group elements in a network based on the reciprocal sharing of common links. These factions can be interpreted as concentrating on the interaction between information security management and assessment, information security investment, information security techniques, information systems security monitoring and development, and cryptographic technology design. Figure 1 shows a clear picture. Its focus is only on the most core area. Co-citation matrix and grouping the authors (using factor analysis of the correlation between the entries) determine who is grouped together because of shared interests. The closeness of author points on such maps is algorithmically

Table 2. Highly cited journal articles in information security.

No.	Full citation index for journal articles	Fq.
1	GORDON LA, 2002, ACM T INFORM SYST, V5, P438	9
2	STRAUB DW, 1998, MIS QUART, V22, P441	8
3	KOTULIC AG, 2004, INFORM MANAGE-AMSTER, V41, P597	6
4	DHILLON G, 2000, COMMUN ACM, V43, P125	5
5	JAVIDI B, 2000, OPT LETT, V25, P28	5
6	REFREGIER P, 1995, OPT LETT, V20, P767	5
7	VONSOLMS B, 2004, COMPUT SECUR, V23, P371	5
8	BASKERVILLE R, 1993, ACM COMPUT SURV, V25, P375	4
9	CAMPBELL K, 2003, J COMPUTER SECURITY, V11, P431	4
10	DIFFIE W, 1976, IEEE T INFORM THEORY, V22, P644	4
11	DUTTA A, 2002, CALIF MANAGE REV, V45, P67	4
12	HOFFER JA, 1989, SLOAN MANAGE REV, V30, P35	4
13	TAJAHUERCE E, 2000, APPL OPTICS, V39, P6595	4
14	AUSTIN RD, 2003, HARVARD BUS REV, V81, P120	3
15	BACKHOUSE J, 1996, EUR J INFORM SYST, V5, P2	3
16	BISHOP M, 2003, IEEE SECUR PRIV, V1, P67	3
17	BRANCHEAU JC, 1996, MIS QUART, V20, P225	3
18	DENNING DE, 1987, IEEE T SOFTWARE ENG, V13, P222	3
19	ELOFF JHP, 1993, COMPUT SECUR, V12, P597	3
20	ELOFF MM, 2000, COMPUT SECUR, V19, P698	3
21	FOLTZ CB, 2005, IND MANAGE DATA SYST, V105, P137	3
22	FORREST S, 1997, COMMUN ACM, V40, P88	3
23	FULFORD H, 2003, INFORM MANAGEMENT CO, V11, P106	3
24	GERBER M, 2001, COMPUT SECUR, V20, P577	3
25	HIGGINGS HN, 1999, INFORMATION MANAGEME, V7, P217	3
26	MATOBA O, 1999, OPT LETT, V24, P762	3
27	STANTON JM, 2005, COMPUT SECUR, V24, P124	3
28	VONSOLMS B, 2000, COMPUT SECUR, V19, P615	3
29	VROOM C, 2004, COMPUT SECUR, V23, P191	3
30	WHITMAN ME, 2003, COMMUN ACM, V46, P91	3

Table 3. Eigenvalues of the top five factors.

Factor	Eigen value	Pct. of var.	Cum. Pct.
1	7.614	37.1	37.1
2	3.744	18.2	55.8
3	2.593	12.6	68.0
4	1.568	7.6	75.6
5	1.216	5.9	81.5

related to their similarity as perceived by citers.

The most influential scholars in information security studies between 1998 and 2007 are grouped together in this study. Five factors were extracted from the data and together they explain over 81% of the variance in the correlation matrix (Table 3). Table 4 lists the five most important factors along with the authors that had a factor loading of at least 0.4. We tentatively assigned names to the factors based on our own interpretation of the authors with high associated loadings. Our interpretation of the analysis results is that the information security field comprises five basic but different sub-fields: (1) information security management and assessment, (2) information security investment, (3) information security techniques (4) information systems security monitoring and development, and (5) cryptographic technology de-sign. We did not attempt to interpret the remaining factors because of their relatively small eigenvalues (<1.216). They have therefore been excluded from Table 4.

Figure 1 and Table 4 feature six authors with a factor loading over 0.6 in factor 1. Factor 1 can explain the variance of 37.1% in the information security field. Evidently, the main research focused on information security management and assessment; including Kotulic, Dutta and Eloff et al. Kotulic and Clark (2004) proposed a conceptual model based on the study of security risk management (SRM) at the firm level. They provided a

Table 4. Authors factor loadings (varimax rotation) at 0.4 or higher.

Factor	Variance
F1: Information security management and assessment	**37.1 %**
KOTULIC	0.907
DUTTA	0.841
ELOFF	0.818
VONSOLMS, B	0.801
DHILLON	0.676
RASMUSSEN	0.635
F2: Information security investment	**18.2 %**
CAVUSOGLU	0.937
GORDON	0.913
CAMPBELL	0.813
F3: Information security techniques	**12.6 %**
REFREGIER	0.998
TAJAHUERCE	0.981
JAVIDI	0.912
POON	0.791
DIFFIE	0.533
F4: Information systems security monitoring and development	**7.6 %**
HOFFER	0.930
BASKERVILLE	0.860
STRAUB	0.741
WHITMAN	0.608
VONSOLMS R	0.465
F5: Cryptographic technology design	**5.9 %**
WANG	0.884

description of their model, the methodology designed to test that model, the problems faced during testing, and their suggestions on how to work in highly sensitive areas. Dutta and McCrohan (2002) addressed information security tests on three foundational points: critical infrastructures, organization and technology. While critical infrastructures are beyond the organization's direct control, balancing them is critical to corporate governance. Total security is neither technically feasible nor operationally practicable. They presented an organizational security approach that senior managers can use as a roadmap to initiate and audit the implementation of security plans and policies. Eloff and VonSolms (2000) proposed that information security (IS) is the key to the effective management of any organization. IS management is not always a quantifiable entity and its evaluation is complicated by how it can be viewed from an electronic or procedural and managerial perspective. They aimed to provide a consolidated approach to the evaluation of IS management that was fully cognizant of both perspectives

There are three authors with a factor loading over 0.8 in factor 2. Factor 2 explains the variance of 18.2% in the information security field, and represents the information security investment; including Cavusoglu, Gordon and Campbell. Cavusoglu et al. (2004) argue that, as per the IT productivity paradox, the return on security investment (ROSI) has become a controversial topic because of the immense growth of e-businesses. Defining the value of security investments is challenging. However, it is clear that "security consumers will need to understand the variables that define ROSI and endure the discomfort of assigning dollar values to quantities that currently are extremely ill-defined". Gordon and Loeb (2002) presented an economic model that determines the optimal amount to invest to protect a given set of information. The model takes into account the vulnerability of the information to a security breach and the potential loss should such a breach occur. It is shown that for a given potential loss, a firm should not necessarily focus its investments on information sets with the highest vulnerability. Campbell et al. (2003) examined the economic effect of information security breaches reported in newspapers on publicly traded U.S. corporations. They found limited evidence of an overall negative stock market reaction to public announcements of information security breaches and a highly significant negative market reaction for information security breaches involving unauthorized access to confidential data, but no significant reaction when the breach does not involve confidential information. These findings are consistent with the argument that the economic consequences of information security breaches vary according to the nature of the underlying assets affected by the breach.

Five authors have a factor loading over 0.5 in factor 3. Factor 3 can explains the 12.6% variance of the information security field, and revealed the information security techniques; the relevant authors here are Refregier et al. (1995) proposed a new optical encoding method of images for security applications. The encoded image is obtained by random-phase encoding in both the input and the Fourier planes. They analyzed the statistical properties of this technique and show that the encoding converts the input signal to stationary white noise. Moreover, the reconstruction method is robust. Tajahuerce and Javidi (2000) presented a method for the optical encryption of three-dimensional (3D) information by use of digital holography. A phase-shifting interferometer records the phase and amplitude information generated by a 3D object at a plane located in the Fresnel diffraction region with an intensity-recording device.

Encryption is performed optically by use of the Fresnel diffraction pattern of a random phase code. Images of the 3D object with different perspectives and focused at different planes can be generated digitally or optically after decryption with the proper key. Javidi and Nomura (2000) demonstrated an information security method that uses a digital holographic technique. An encrypted image is stored as a digital hologram. The decryption key is also

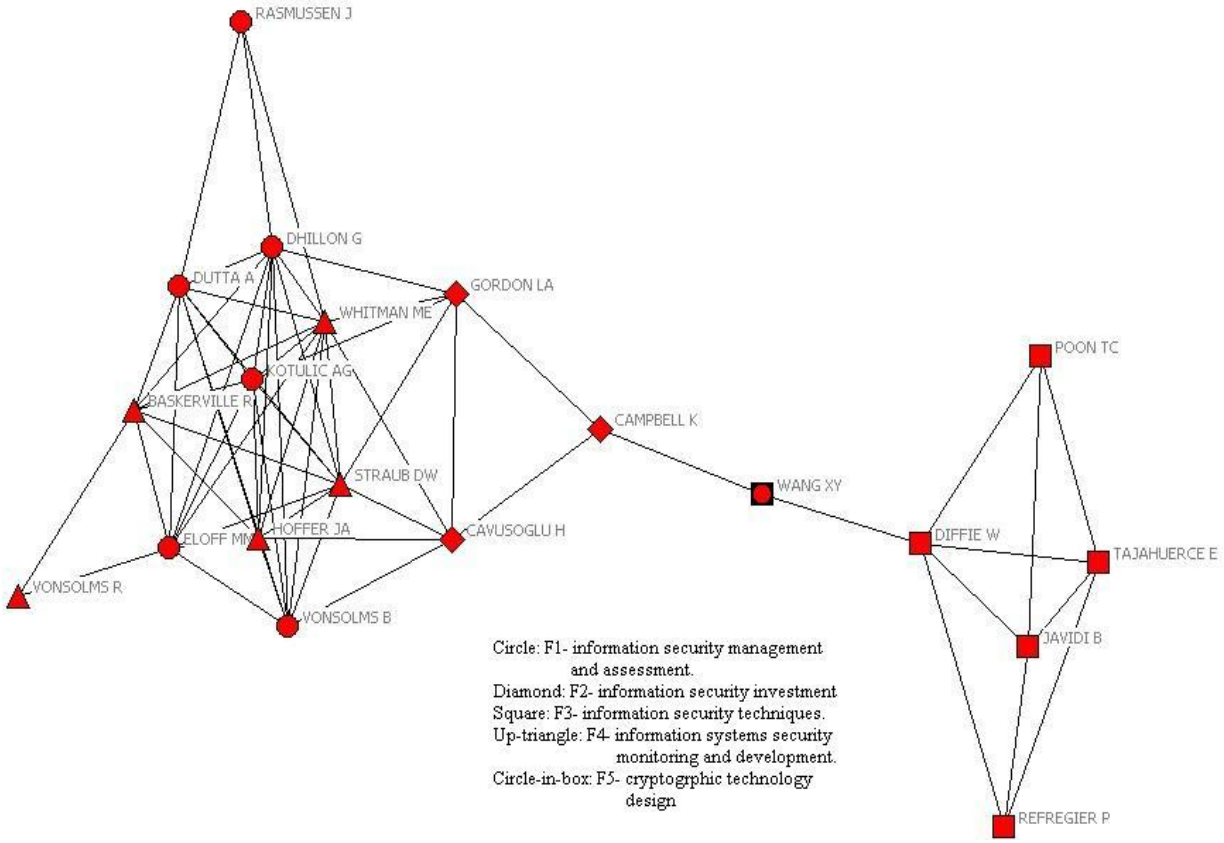

Figure 1. Co-citation network of information security studies.

stored as a digital hologram. The encrypted image can be electrically decrypted by use of the digital hologram of the key. This technique provides security for both storage and data transmission.

There are five authors with a factor loading over 0.6 in factor 4. Factor 4 can explain the 7.6% variance of the information security field. The topic of interest in this respect was the monitoring and development of information systems security; the notable authors included Hoffer et al. The annual financial losses attributable to computer systems are incalculable. Hoffer and Straub (1989) indicated they could be substantial—many of them could be avoided if firms were more serious about deterrence and prevention. Their article calls for proactive computer security administration: It outlines the most common forms of abuse, the most effective countermeasures and the steps to effective security management. Baskerville (1993) revealed that systems analysts and designers develop expertise in methods for specifying information systems security. The characteristics found in three generations of general information system design methods provide a framework for comparing and understanding current security design methods. These methods include approaches that use checklists of controls, divide functional requirements into engineering partitions, and create abstract models of both the problem and the solution. Straub and Welke (1998) addressed one viable explanation for why losses from computer misuse and malfunctions today are uncomfortably large and still so potentially devastating after many years of attempting to deal with the problem. The results of comparative qualitative studies in two information services Fortune 500 firms identify an effective approach to the problem. This theory-based security program includes (1) use of a security risk planning model, (2) education/training in security awareness and (3) Countermeasure Matrix analysis.

One author has a factor loading over 0.8 in factor 5. Factor 5 can explain the 5.9% variance of the information security field, which is associated with cryptographic technology design. SHA-1 is the best established of the existing SHA hash functions and is employed in several widely used security applications and protocols. Its hashing is also used in distributed revision control systems such as Git, Mercurial and Monotone to identify revisions and detect data corruption or tampering. SHA-1 is the secure hash algorithm required by law for use in certain U. S. Government applications, including use within other cryptographic algorithms and protocols, for the protection of sensitive unclassified information. SHA

hash functions have been used as the basis for the SHACAL block ciphers. Wang et al. (2005) presented new collision search attacks on the hash function SHA-1. They showed that collisions of SHA-1 could be found with complexity less than 269 hash operations. This is the first attack on the full 80-step SHA-1 with complexity less than the 280 theoretical bound.

Conclusions

This study has explored and mapped the intellectual structure of information security studies from 1998 to 2007 by analyzing 3,059 cited references of 223 articles in the SSCI and SCI databases. We identified the important publications (high impact) and the influential scholars, as well as the correlations among these publications, by analyzing citation and co-citation, and conducting social network analysis. Researchers can also use these methods to explore the intellectual structure of their own fields.

Social network analysis tools can be used to graph the relations in the co-citation matrix and to identify the strongest links and the core areas of interest (Pilkington and Teichert, 2006) in information security. Co-citation matrix and the grouping of authors (using factor analysis of the correlation between the entries) determined the clusters of authors. According to this, the closeness of author-points on such maps is algorithmically related to their similarity as perceived by citers. A factor analysis of the co-citations proposed that the field includes five different concentrations of interest within the ten years: (1) Information security management and assessment, (2) information security investment, (3) information security techniques, (4) information systems security monitoring and development and (5) cryptographic technology design. The intellectual structure of information security and the development path discussed above can help researchers as well as professionals by recognizing the influential publications and scholars of this field. This method also provides researchers with a wide spectrum of inter-connected (web-like) nodes laden with ideas, concepts and theories, from which scholars and thinkers can embark on their own explorations. In other words, future researchers stand to gain from the directions offered here. Particularly valuable is the provision of an objective and systematic means of determining the relative importance of different knowledge nodes in the development of the information security field.

Even though this research has these merits, it also has some limitations: our data collection criteria excluded some journals that may publish information security articles, and the research method of this study could not exclude the phenomenon of self-citation. To surmount the limitations associated with citation analysis, future researchers are encouraged to combine citation analysis with content analysis; such a research tool will more ably determine the presence of certain words or concepts within texts or sets of texts.

All methodologies have their intrinsic limitations, and co-citation analysis is no exception. In our study, many recent articles did not register as highly cited in our co-citation network, because of the time lag. Our study offers more of a historical review of the development of the information security field, rather than any definitive judgment of the importance of the respective authors or articles. The exception of the recent papers is not owing to their lack of importance, but simply our methodological limitations. Fortunately, these limitations do not detract from the results of the research.

ACKNOWLEDGEMENTS

The authors would like to thank the National Science Council, the Republic of China, Taiwan, for the financial support for this research.

REFERENCES

Acedo FJ, Barroso C, Casillas JC, Galán JL (2001). Dominant approach in the field of management. Int. J. Organ. Anal., 9: 327-353.
Acedo FJ, Casillas JC (2005). Current paradigms in the international management field: An author co-citation analysis. Int. Bus. Rev., 14: 619-639.
Allen JH (2001) The CERT guide to system and network security practices. Addison-Wesley, Boston.
Axelsson S (2000). The base-rate fallacy and the difficulty of intrusion detection. ACM Trans. Inf. Syst. Secur., 3: 186-205.
Baskerville R (1993). Information systems security design methods: Implications for information systems development. Comput. Surv., 25: 375-414.
Borgatti SP, Everett MG, Freeman LC (2002). Ucinet for Windows: software for social network analysis, Analytic Technologies. Harvard.
Buckley PJ (2002). Is the international business research agenda running out of steam? J. Int. Bus. Stud., 33: 365-373.
Campbell K, Gordon LA, Loeb MP, Zhou L (2003). The economic cost of publicly announced information security breaches: empirical evidence from the stock market. Comput. Secur., 11: 431-448.
Cavusoglu H, Mishra B, Raghunathan S (2004). A model for evaluating IT security investments. Commun. ACM 47: 87-92.
Chandy PR, Gopalakrishna P (1992). A content analysis of contributions to the MIR journal. Manage. Int. Rev., 32: 273-283.
Chandy PR, Williams TG (1994). The impact of journals and authors on international business research: A citation analyses. J. Int. Bus. Stud., 25: 715-728.
Cronin B (1984). The citation process: The role and significance of citations in scientific communication. Taylor Graham, London.
Culnan M (1986). The intellectual development of management information systems. Manage. Sci., 32: 156-172.
Denning D (2000). Reflections on cyberweapons controls. Comput. Secur., 16: 43-53.
Dhillon G (2007). Principles of information systems security: text and cases. John Wiley & Sons, NY.
Dutta A, McCrohan K (2002). Management's role in information security in a cyber economy. Calif. Manage. Rev., 45: 67.
Eloff MM, VonSolms SH (2000). Information security management: an approach to combine process certification and product evaluation. Comput. Secur., 19: 698-709.
Gordon LA, Loeb MP (2002). The economics of information security investment. ACM Trans. Inf. Syst. Secur., 5: 438.
Hair J, Anderson R, Tatham R (1998). Black W Multivariate Data

Analysis. Simon and Schuster, Upper Saddle River.
Hoffer JA, Straub DW (1989). The 9-to-5 underground: Are you policing computer crimes. MIT Sloan Manage. Rev., 30: 35-43.
Javidi B, Nomura T (2000). Securing information by use of digital holography. Opt. Lett., 25: 28-30.
Knight GA, Hult GTM, Bashaw RE (2000). Research productivity in the journal of business research: 1985–1999. J. Bus. Res., 49: 303-314.
Kotulic AG, Clark JG (2004). Why there aren't more information security research studies. Inf. Manage., 41: 597-607.
Lu JW (2003). The evolving contributions in international strategic management research. J. Int. Manag., 9: 193-213.
McCain KW (1983). The author co-citation structure of macroeconomics. Scientomerics. 5: 277-289.
McCain KW (1984). Longitudinal author co-citation mapping: The changing structure of macroeconomics. J. Am. Soc. Inf. Sci. Technol., 35: 351-359.
McCain KW (1990). Mapping authors in intellectual space: A technical overview. J. Am. Soc. Inf. Sci. Technol., 41: 433- 443.
Ngai EWT, Wat FKT (2002). A literature review and classification of electronic commerce research. Inf. Manage., 39: 415-429.
Pilkington A, Liston-Heyes C (1999). Is production and operations management a discipline? A citation/ co-citation study. Int. J. Oper. Prod. Manage., 19: 7-20.
Pilkington A, Teichert T (2006). Management of technology: themes, concepts and relationships. Technovation. 26: 288-299.
Ponzi LJ (2002). The intellectual structure and interdisciplinary breadth of knowledge management: A bibliometric study of its early stage of development. Scientometrics. 55: 259-272.
Poon TC, Qi Y (2003). Novel real-time joint-transform correlation by use of acousto-optic heterodyning. Appl. Optics, 42: 4663-4669.
Power R (2001). CSI/FBI computer crime and security survey. Comput. Secur., 17: 29-51.
Ramos-Rodriguez AR, Ruiz-Navarro J (2004). Changes in the intellectual structure of strategic management research: A bibliometrics study of the strategic management journal, 1980-2000. Strateg. Manage. J., 25: 981-1004.
Rasmussen J (1997). Risk management in a dynamic society: A modelling problem. Safe. Sci., 27: 183-213.
Refregier P, Javidi B (1995). Optical image encryption based on input plane and Fourier plane random encoding. Opt. Lett., 20: 767-769.
Shaw MJ Gardner DM, Thomas H (1997). Research opportunities in electronic commerce. Decis. Support Syst., 21: 149-156.
Small HG (1993). Macro-level Changes in the Structure of Co-citation Clusters: 1983-1989. Scientometrics. 26: 5-20.
Straub DW, Welke RJ (1998). Coping with systems risk: Security planning models for management decision making. MIS Q., 22: 441-469.
Tajahuerce E, Javidi B (2000). Encrypting three-dimensional information with digital holography. Appl. Optics, 39: 6595-6601.
VonSolms R (1997). Driving safely on the Information Superhighway. Inform. Manage. Comput. Secur., 5: 20-22.
Wang XY, Yin YL, Yu HB (2005). Finding collisions in the full SHA-1 Advances in cryptology-CRYPTO 2005. Proceedings book series: Lecture Notes in Computer Science. 3621: 17-36.
Wareham J, Zheng JG, Straub D (2005). Critical themes in electronic commerce research: A meta-analysis. J. Inf. Technol., 20: 1-19.
Wasserman S, Faust K (1997). Social network analysis: Methods and applications. Cambridge University Press, Cambridge, MA.
White H, Griffith B (1981). Author co-citation: A literature measure of intellectual structure. J. Am. Soc. Inf. Sci. Technol., 32: 163-171.
White HD (1983). A co-citation map of the social indicators movement. J. Am. Soc. Inf. Sci. Technol., 34: 307-312.