Empirical vs. Non-Empirical Work in Information Systems Security: A Review and Analysis of Published Articles 1995-2005

J.M. Stanton

Syracuse University School of Information Studies
jmstanto@syr.edu

Abstract

Information Systems Security is generally recognized as a small subfield of the larger field of Information Systems. A literature analysis of articles published in the field of Information Systems Security in the years 1995-2005 is presented. Results from the analysis suggested showed that the mix of article content in this subfield favored articles without data. This finding, along with other related findings suggests that the field is in a relatively early state with respect to scientific maturity. Comprehensive literature review articles published in high impact Information Systems journals and a journal dedicated to the subfield may help ISS to progress into a more scientifically mature phase.

Keywords

Information systems security, Empirical research, Literature review.

1. Introduction

Empirical research provides the substantive basis for advances in social science. In the field of Information Systems (IS), a variety of authors have reviewed the state of empirical literature in the field with an eye towards identifying paradigms, trends, and patterns that help to understand the direction and future needs for research. Benbasat and Zmud (Benbasat and Zmud, 1999) commented that the field's "continuing emphasis on performing rigorous research has paid off," with respect to the quality of published research. Claver, Gonzalez, and Llopis (2000) reviewed 16 years of research in Information Systems and found that as the field matured there was an "increase in the number of empirical articles over theoretical ones," and that "the most frequent of the empirical studies is the field study, followed by the case study." Interestingly, their data also showed a gradual decline in the amount of research on information security between 1981 (5.5% of articles in IS) and 1989 (0.4% of articles in IS), after which the percentage began to climb. Vessey (2002) reviewed the diversity of IS research between 1995 and 1999. She found that most studies used a hypothetico-deductive approach, although the reference disciplines used by the researchers were highly variable. Looking across the past two or three decades, then, the IS field has adopted a range of the available methodological approaches from the social sciences and employed them in the service of conducting and publishing more and more rigorous research.

What is true for the field as a whole, however, is not necessarily true of every subfield. In the subfield of Information Systems Security (ISS), which began to flourish only with the onset of the widespread use of the Internet in the early 1990s, the use of empirical methods to explore security-related phenomena may not reflect the same trends as in the larger field of IS. In particular Kotulic and Clark (2004) have commented that conducting security research, particularly in organizational contexts provides unique challenges because of the sensitivity of the subject matter. To use an analogy, organized studies of public health occurred no later than the early 1800s (e.g., John Snow's studies of drinking water and cholera in London), but the first large scale public health studies of sexuality did not begin until at least a century later (e.g., the infamous Tuskeegee syphilis study). Information security breaches are a matter that most organizations are highly reluctant to discuss, particularly with outsiders such as academic researchers whose primary intention is to publish their findings. Nonetheless, as the analogy shows, difficult, sensitive, and private behaviors are subject to scientific study, given sufficient creativity and persistence by researchers.

Thus, the purpose of this paper is to examine the extent to which researchers in Information Systems Security (ISS) have begun to conduct the rigorous empirical research that marks a more mature field or subfield. Alternatively, if a majority of the research is non-empirical – theory and conceptual development, or editorial expressions of opinion and analysis – then it may be possible to conclude that the ISS subfield is still in a relatively immature state. This paper does not attempt to make a value judgment on the significance or contribution of particular pieces of research – whether conceptual or empirical – but rather tries to ascertain the state of literature in ISS to provide an informative picture that can guide future research.

2. Background

In the *Structure of Scientific Revolutions*, Kuhn (1970) describes three phases of development in which research activity occurs. The pre-scientific phase is marked by a lack of consensus on theory and methods, the normal phase includes the production of a substantial amount of research under conditions of consensus about theories and methods, and the transition phase includes various crises in which the theories and methods of the current paradigms of normal science are shown to produce results incommensurable with current assumptions. Physics has passed through several such periods including the shift from Newtonian physics to the ideas of relativity introduced by Einstein. Psychology has also witnessed several paradigm shifts including the rise and fall of Skinnerian behaviorism.

Of primary relevance to this paper, the pre-scientific period in a field includes multiple divergent attempts to develop conceptual frameworks that will serve as the basis of future empirical research and theory development. Note that Kuhn did not intend the term pre-scientific as pejorative toward the skills and knowledge of researchers and academics active in a newly emerging field, but rather as a gross categorization of the level of consensus in the community about what to study and how to study it. While empirical research does occur during the pre-scientific period, its prevalence relative to non-empirical work is likely to be low. Likewise, among the non-empirical work, there is likely to be a wide variety of writings, including material intended to advance a particular theoretical perspective, material that editorializes for or against the importance of a particular problem, and material that seeks to persuade researchers of the superiority of a particular viewpoint or perspective.

The goal of the literature analysis presented below was to examine whether the patterns of publication in the subfield of ISS over the last decade (1995-2005) fit Kuhn's notion of a field in its pre-scientific phase. These patterns would primarily appear on the basis of examining the topic matter of the literature over time and most importantly the evidentiary mix appearing in the literature. Literature may contain the author's opinions, analysis of previously published literature or archival materials, evidence from simulations or generated data, evidence from laboratory settings, or evidence from in vivo (field) settings. Some articles may contain more than one type of evidence. A preponderance of articles containing archival, simulated, laboratory, or field data, collected and analyzed in the context of a particular theoretical paradigm, would be indicative of a normal science phase. A preponderance of articles containing authorial opinions and/or analysis of previous literature, suggesting pre-consensus attempts at conceptual and theoretical development, would be indicative of a pre-scientific phase. To this end, a rough hierarchy of article types appears in Table 1.

In addition to examining the types of articles over time, it may be fruitful to check a few other sources of information. For example, citation rates of articles can help to indicate the extent to which a research area is consolidating itself around a particular perspective or framework. In addition, to assess the notion that information security research was difficult at first because of the sensitivity issues, but has become easier over time, it may be useful to examine the evolution of sample sizes over time. A pattern of increasing sample sizes may indicate a move from conceptual articles toward empirical articles.

Type	Mix of Evidence
Editorial	Primarily authorial opinion, possibly supplemented by basic discussion of previous literature or anecdotal practitioner material. Example article: Darragh and Darragh (2001).
Developmental	Systematic analysis of previous literature focused on development of conceptual or theoretical frameworks. Possible limited use of small-N techniques such as case studies to support development. Example article: Gonzalez and Sawicka (2002).
Pragmatic	Studies involving the use of small-N techniques, simulations, design exercises, and other evidence collected and analyzed without use of an orthodox theoretical and measurement context. Example article: Schwartz and Zalewski (1999).
Empirical	Data-based studies that collect and analyze data within the context of an accepted conceptual or theoretical framework. Laboratory, field, or archival data studies that try to confirm, modify, or extend existing frameworks. Example: Straub and Welke (1998).

Table 1: Research Articles and Evidence Types

3. Method

3.1 Article Selection

Publications from peer reviewed journal articles and archival, published conference proceedings (e.g., by the Association for Computing Machinery) were included in the data set. Publications were located through searches in major databases containing Information Systems (IS) research, such as ABI Inform, Google Scholar, EBSCO Business Source Elite, and Emerald Fulltext. In all searches, the quoted phrase “information security” was used to separate articles on this topic from articles on related topics such as privacy. Because “information security” also provides results from engineering and computer science – including articles on primarily technical topics such as cryptographic algorithms – a variety of additional search terms were used to qualify these searches. Additional search terms included user, organization, organizational, behavior, and human.

Articles were rejected from inclusion if they were not peer reviewed, if they did not contain at least one reference, if the topic matter was technical and did not contain an organizational or human component, or if the topic matter pertained to teaching or curriculum development for the college classroom (as opposed to organizational training and development topics, which were included). Because the analysis for this paper also included consideration of citation rates, it was necessary not to choose articles published very recently. A minimum publication delay of one year allowed inclusion of articles from 2005 and earlier. An arbitrarily chosen study period of eleven years included the middle and late 1990s – a period of major growth in research and publication on ISS topics. Thus, articles were included only if their publication date was between 1995-2005.

3.2 Article Coding

Article characteristics were coded by the author through the application of a coding rubric. A code was assigned designating each article as editorial, developmental, pragmatic, or empirical. Differentiating between editorial/developmental versus pragmatic/empirical was straightforward as the collection of data was evident or absent in each article. The distinction between editorial and developmental was made on the basis of whether the author presented a framework or other theoretical structure, as well as on whether the stated purpose of the article was to guide future research. The distinction between pragmatic and empirical was made on the basis of the presence or absence of theoretical discussion, statement of hypotheses, and/or use of established or systematically developed measures or research protocols. In the great majority of cases the code designations were not controversial.

Number of years since publication was coded as 2007 minus publication year. For convenience, citation counts were collected from Google Scholar and were not corrected for self citation[1]. Number of citations was corrected to take into account years since publication in order to avoid an unfair advantage for older articles. For developmental, pragmatic, or empirical articles containing data, the sample size was coded based on reading the method sections of the articles and summing all of the “cases” reported across all data collections in the article at the finest level of analysis. Thus a case study in which a company was analyzed at a general level from unstructured observations was counted as N=1, whereas another study in which 10 individuals were separately interviewed within a single company was counted as N=10. Articles without data were coded as N=0. Because sample size was very highly positively skewed, we used the base 10 log of sample size in our analyses. We also recoded sample size as a binary indicator of whether the article had data or not.

4. Results

Using the article selection criteria described above, we located 496 articles that qualified as peer reviewed literature on Information Systems Security (ISS). From this large set we randomly sampled n=98 articles for coding by choosing every fifth article from the compiled list. Some articles appeared both in the form of a conference proceedings paper and a journal article, and in these cases we only considered the latter of these. The mean time of publication was 2002 and the modal year was 2005, suggesting that a greater amount of literature was published later half of the study period.

[1] Google Scholar citation figures are known to contain inaccuracies, including self citations, but nonetheless provide information over a much broader set of publication outlets than ISI Web of Science

The modal article type was a developmental article that focused on reviewing existing literature and/or developing a theoretical or conceptual framework for later use; 36.7% of articles were of this type. The next most common type of article was an editorial article; 29.5% of articles consisted of an author's opinion and/or analysis of an issue in ISS. Pragmatic articles with small-N data collection and no reference to theory accounted for 9.2% of the articles. Empirical articles containing more substantial data sets and using theoretical or conceptual frameworks accounted for 24.5% of the articles. Using these percentages the most important contrast to notice is that empirical articles comprised about one third of the literature whereas non-empirical articles comprised the remaining two thirds. The average sample size across all articles was N=50, but this is a somewhat deceptive figure: The average sample size counting only articles that had data collections was N=145.

On average, articles in the data set were cited 9.3 times. This measure was highly skewed, however, as the modal number of citations was zero. About 18% of the articles had no citations at all, whereas an additional 17% had just one citation).The most highly cited article was Straub and Welke (1998) – an empirical article – which had 95 citations. The time-corrected citations measure was somewhat less skewed: about 1.8 citations per year. Note that citations were counted up to the present and corrected for the span of time from publication year to the present. Thus an article published in 2005 that had a total of two citations would have a time-corrected value of one citation per year.

A small set of correlations highlights key patterns in these data. The point-biserial correlation between years since publication and whether or not the article was data-based was not statistically significant, suggesting no evidence of a trend toward more empirical articles as the research advanced through time. Likewise the correlation between years since publication and article type was also not significant, an absence of evidence that more empirical and pragmatic articles might be appearing more frequently in recent years. The correlation between years since publication and the (base 10 log) sample size was not statistically significant, indicating no evidence of researchers collecting more data for recent articles as opposed to older articles. The correlation between citation rate and (base 10 log) sample size was also not statistically significant, indicating a lack of evidence that researchers cited articles with more data more frequently. The correlation between citation rate and article type was r=.36, p<.001, indicating that articles that contained data were substantially more highly cited than articles that did not. Further clarification of this evidence came from comparing the citation rates of articles with data versus those without: Articles with data were cited at a rate of 2.1 citations per year, whereas those without data were cited at 1.64 per year.

5. Discussion

The preponderance of editorial/opinion and conceptual review type articles in the Information Systems Security (ISS) literature – relative to the occurrence of articles with data – suggests that ISS is still in the earliest stages of development as a subfield of Information Systems. Articles with data constituted slightly less than one third of all published studies in ISS, whereas the remaining two thirds were non-data-based. Contrast this with Claver et al.'s (2000) review of research in the Information Systems field, which showed 68.7% of articles as empirical while only 31.3% were theoretical. The proportions are essentially reversed in ISS. Additionally, over the 11 year study period there was no indication that empirical articles were becoming more common over time. Likewise, there was no indication that sample sizes were increasing over time, lending continuing support to Kotulic and Clark's (2004) proposition that collecting organizational data on a sensitive topic such as information security continues to provide an important barrier to the conduct of empirical ISS research.

Kuhn (1970) characterizes this earliest stage of scientific development as a period in which researchers struggle to find common ground on matters of theory and method. With this perspective, it is comforting to note that theoretical and conceptual development articles far outnumbered those of the editorial variety, at least by a small margin. It is likely that because of the very large practitioner population in the information security world, editorial and opinion articles will remain popular as they provide a conduit for researchers and others to express ideas in non-academic language that can be considered by practitioners. Nonetheless, it is the developmental and empirical articles that will ultimately advance the research area, so the preponderance of developmental articles at this stage is an encouraging indication that researchers are trying to create a dialog about theories and methods within the community.

The citation analysis provides additional evidence concerning this issue. The pattern of citations was highly positively skewed, with an average of 9.3 citations per article but fully 36% of the articles with one or zero citations. No comparative benchmark is needed to know that an article with no citations is not particularly influential on subsequent research, but comparisons with top information systems journals show that the mean citations per year of 1.8 is comparable with the citation rates for articles in information systems journals (e.g., MISQ: 1.96 citations per article per year, see Katerattanakul et al., 2003).

This evidence suggests a possible paradox in ISS research. On the one hand the proportion of empirical articles is low: Researchers are productively generating constructs, frameworks, and models, but the number of data-based articles testing out all of these ideas is small. On the other hand, the most influential articles in ISS (e.g., Straub and Welke) are cited at rates comparable with other areas of information systems, suggesting accumulation of research results over time that is similar to the mainstream. One possible resolution of this paradox lies in comparing citation rates of articles with and without data. Those ISS articles with data are cited comparably to other areas of information systems, whereas those without are cited at much lower rates. Another way of saying this is that ISS researchers are paying substantial attention to each others' data, but less attention to proposed constructs, frameworks, and models. This finding suggests an important need for a journal whose editorial policies will support the production of articles addressing the development of scholarly consensus on appropriate models and theories to guide future ISS research. A special issue of an existing high impact journal would provide one fruitful venue for such articles.

All of the issues described above suggest the need for one or more journals dedicated to the subfield of ISS. Although a multitude of journals currently exist with "computer security" or "information security" in the title, few among these focus exclusively on theories, methods, and empirical research for ISS. As the data from this study show, a journal whose editorial policies encourage the publications of ISS studies containing data, and that help the ISS scholarly community reach consensus on appropriate models and theories will push the subfield of ISS forward into the next phase of scientific maturity.

References

Acquisti, A. & Grossklags, J. (2003) Losses, gains, and hyperbolic discounting: An experimental approach to information security attitudes and behavior. *2nd Annual Workshop on Economics and Information Security-WEIS,* 3.

Adams, A. (1999) The Implications of Users' Multimedia Privacy Perceptions on Communication and Information Privacy Policies. *Proceedings of Telecommunications Policy Research Conference.*

Alner, M. (2001) The effects of outsourcing on information security. *Information systems security,* 10**,** 35-43.

Atkinson, W. (2005) Integrating Risk Management & Security. *Risk Management,* 52**,** 32.

Backhouse, J., Hsu, C., Tseng, J. C. & Baptista, J. (2005) A question of trust. *Association for Computing Machinery. Communications of the ACM,* 48**,** 87.

Belsis, P., Kokolakis, S. & Kiountouzis, E. (2005) Information systems security from a knowledge management perspective. *Information Management & Computer Security,* 13**,** 189.

Benbasat, I. & Zmud, R. W. (1999) Empirical Research in Information Systems: The Practice of Relevance. *MIS Quarterly,* 23**,** 3-16.

Beulen, E. & Streng, R. J. (2002) The Impact of Online Mobile Office Applications on the Effectiveness and Efficiency of Mobile Workers' Behavior: A Field Experiment in the IT Services Sector. *Proceedings of ICIS***,** 629–640.

Blatchford, C. (1998) Information security, business, and the Internet. *Information systems security,* 7**,** 44-53.

Boukhonine, S., Krotov, V. & Rupert, B. (2005) Future Security Approaches and Biometrics. *Communications of the Association for Information Systems,* 16**,** 1.

Braithwaite, T. (2001) Executives need to know: The arguments to include in a benefits justification for increased cyber security spending. *Information systems security,* 10**,** 35-48.

Brostoff, S. & Sasse, M. A. (2001) Safe and sound: a safety-critical approach to security. *Proceedings of the New Security Paradigms Workshop, Cloudcroft, NM*, 41-50.

Brusil, P. & Hale, J. (2005) The Shifting Sands of Security Management. *Journal of Network and Systems Management,* 13**,** 241.

Campbell, K. (2003) The economic cost of publicly announced information security breaches: empirical evidence from the stock market. *Journal of Computer Security,* 11**,** 431-448.

Chellappa, R. K. & Pavlou, P. A. (2002) Perceived information security, financial liability and consumer trust in electronic commerce transactions. *Logistics Information Management,* 15**,** 358-68.

Chen, Y. S., Chong, P. P. & Zhang, B. (2004) Cyber security management and e-government. *Electronic Government, an International Journal,* 1**,** 316-327.

Claver, E., Gonzalez, R. & Llopis, J. (2000) An analysis of research in information systems (1981-1997). *Information & Management,* 37**,** 181-195.

Darragh, D. M. & Darragh, S. M. (2001) On the 6 th day: A nonprofessional's view of information systems security. *Information systems security,* 10.

Dhillon, G. (2001) Challenges in Managing Information Security in the New Millennium. *Information Security Management: Global Challenges in the New Millennium.*

Dhillon, G. & Backhouse, J. (2000) Technical opinion: Information system security management in the new millennium. *Communications of the ACM,* 43**,** 125-128.

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

Doherty, N. F. & Fulford, H. (2005) Do Information Security Policies Reduce the Incidence of Security Breaches: An Exploratory Analysis. *Information Resources Management Journal,* 18**,** 21.

Dynes, S., Brechbuhl, H. & Johnson, M. E. (2005) Information Security in the Extended Enterprise: Some Initial Results From a Field Study of an Industrial Firm. *Workshop on the Economics of Information Security.*

Ezingeard, J.-N., McFadzean, E. & Birchall, D. (2005) A MODEL OF INFORMATION ASSURANCE BENEFITS. *Information Systems Management,* 22**,** 20.

Foote, P. & Neudenberger, T. (2005) Beyond Sarbanes--Oxley compliance. *Computers & Security,* 24**,** 516.

Furnell, S. M., Gaunt, P. N., Holben, R. F., Sanders, P. W., Stockel, C. T. & Warren, M. J. (1996) Assessing staff attitudes towards information security in a European healthcare establishment. *Med Inform (Lond),* 21**,** 105-12.

Furnell, S. M., Gennatou, M. & Dowland, P. S. (2002) A prototype tool for information security awareness and training. *Logistics Information Management,* 15**,** 352-357.

Gallor, E. & Ghose, A. (2003) The Economic Consequences of Sharing Security Information. *2nd Workshop on Economics and Information Security*, 29-30.

Gonzalez, J. J. & Sawicka, A. (2002) A Framework for Human Factors in Information Security. *WSEAS International Conference on Information Security, Rio de Janeiro*.

Gonzalez, J. J. & Sawicka, A. (2003) The Role of Learning and Risk Perception in Compliance. *Proceedings of the 21st International Conference of the System Dynamics Society, New York.*

Gordon, L. A., Loeb, M. P. & Lucyshyn, W. (2002) An economics perspective on the sharing of information related to security breaches: Concepts and empirical evidence. *The First Workshop on Economics and Information Security*.

Gupta, A. & Hammond, R. (2005) Information systems security issues and decisions for small businesses: An empirical examination. *Information Management & Computer Security,* 13**,** 297.

Hansche, S. (2001a) Designing a security awareness program: Part I. *Information systems security,* 9**,** 14-22.

Hansche, S. (2001b) Information system security training: Making it happen, part 2. *Information systems security,* 10**,** 51-70.

Hazari, S. (2005) Perceptions of End-Users on the Requirements in Personal Firewall Software: An Exploratory Study. *Journal of Organizational and End User Computing,* 17**,** 47.

Holzinger, A. (2000) Information security management and assurance a call to action for corporate governance. *Information systems security,* 9**,** 32-39.

Hone, K. & Eloff, J. H. P. (2002) Information security policy-what do international information security standards say? *Computers and Security,* 21**,** 402-409.

James, H. L. (1996) Managing information systems security: a soft approach. *Proceedings of the Information Systems Conference of New Zealand***,** 10-20.

Kankanhalli, A., Teo, H. H., Tan, B. C. Y. & Wei, K. K. (2003) An Integrative Study of Information Systems Security Effectiveness. *International Journal of Information Management,* 23**,** 139-154.

Karart, C. M., Karat, J. & Brodie, C. (2005a) Why HCI research in privacy and security is critical now. *International Journal of Human-Computer Studies,* 63**,** 1-4.

Karat, J., Karat, C. M., Brodie, C. & Feng, J. (2005b) Privacy in information technology: Designing to enable privacy policy management in organizations. *International Journal of Human-Computer Studies,* 63**,** 153-174.

Katerattankakul, P., Han, B. & Hong, S. (2003) Objective quality ranking of computing journals. *Communications of the ACM* 46**,** 111-114.

Keller, S., Powell, A., Horstmann, B., Predmore, C. & Crawford, M. (2005). Information Securirty Threats and Practices in Small Businesses. *Information Systems Management,* 22**,** 7.

Khalfan, A. M. (2004) Information security considerations in IS/IT outsourcing projects: a descriptive case study of two sectors. *International Journal of Information Management,* 24**,** 29-42.

Kim, E. B. (2005) Information Security Awareness Status of Full Time Employees. *The Business Review, Cambridge,* 3**,** 219.

Kokolakis, S. A. (2000) The use of business process modelling in information systems security analysis and design SA Kokolakis, AJ Demopoulos, EA Kiountouzis The Authors. *Information Management & Computer Security,* 8**,** 107-116.

Kotulic, A. G. & Clark, J. G. (2004) Why there aren't more information security research studies. *Information and Management,* 41**,** 597-607.

Krause, M. & Brown, L. (1996) Information security in the healthcare industry. *Information Systems Security,* 5**,** 32-40.

Krishnan, R., Peters, J., Padman, R. & Kaplan, D. (2005) On Data Reliability Assessment in Accounting Information Systems. *Information Systems Research,* 16**,** 307.

Kuhn, T. S. (1970) *The Structure of Scientific Revolutions,* Chicago, University of Chicago Press.

Kunreuther, H. & Heal, G. (2003) Interdependent Security. *Journal of Risk and Uncertainty,* 26**,** 231-249.

Leach, J. (2003) Improving user security behaviour. *Computers and Security,* 22**,** 685-692.

Lee, S. M., Lee, S. G. & Yoo, S. (2004) An integrative model of computer abuse based on social control and general deterrence theories. *Information and Management,* 41**,** 707-718.

Liu, L., Yu, E. & Mylopoulos, J. (2003) Security and Privacy Requirements Analysis within a Social Setting. *Proc. of RE'03*, 151–161.

Ma, Q. & Pearson, J. M. (2005) ISO 17799: "Best Practices" in Information Security Management? *Communications of the Association for Information Systems,* 15**,** 1.

Miyazaki, A. D. & Fernandez, A. (2000) Internet Privacy and Security: An Examination of Online Retailer Disclosures. *Journal of Public Policy & Marketing,* 19**,** 54-61.

Murray, W. H. (1998) Enterprise security architecture. *Information systems security,* 6**,** 43-54.

Nagaratnam, N., Nadalin, A., Hondo, M., McIntosh, M. & Austel, P. (2005) Business-driven application security: From modeling to managing secure applications. *IBM Systems Journal,* 44**,** 847.

Nyanchama, M. (2005) Information Security Management Enterprise Vulnerability Management and Its Role in Information Security Management. *INFORMATION SYSTEMS SECURITY,* 14**,** 29.

O'Rourke, M. (2005) Data Secured? Taking on Cyber-Thievery. *Risk Management,* 52**,** 18.

O'Brien, D. G. & Yasnoff, W. A. (1999) Privacy, confidentiality, and security in information systems of state health agencies. *American Journal of Preventive Medicine,* 16, 351-358.

Paliotta, A. R. (2001) Beyond the Maginot-line mentality: A total-process view of information security risk management. Based on COSO principles and supplemented by other control models and the author's experience. *Information systems security,* 10, 21-50.

Palmer, M. E., Robinson, C., Patilla, J. C. & Moser, E. P. (2001) Information security policy framework: Best practices for security policy in the E-commerce age. *Information systems security,* 10, 13-27.

Peltier, T. R. (1998) Information classification. *Information systems security,* 7, 31-43.

Pernul, G. (1995) Information Systems Security: Scope, State-of-the-art, and Evaluation of Techniques. *International Journal of Information Management,* 15, 165-180.

Pollitt, D. (2005) Energis trains employees and customers in IT security. *Human Resource Management International Digest,* 13, 25.

Poore, R. (2000) Valuing information assets for security risk management. *Information systems security,* 9, 17-23.

Riley, R. A. J. & Kleist, V. F. (2005) The biometric technologies business case: a systematic approach. *Information Management & Computer Security,* 13, 89.

Rindfleisch, T. C. (1997) Privacy, information technology, and health care. *Communications of the ACM,* 40, 92-100.

Ryan, J. J. C. H. & Ryan, D. J. (2005) Proportional Hazards in Information Security. *Risk Analysis,* 25, 141.

Saffady, W. (2005) Risk Analysis and Control: Vital to Records Protection. *Information Management Journal,* 39, 62.

Saint-Germain, R. (2005) Information Security Management Best Practice Based on ISO/IEC 17799. *Information Management Journal,* 39, 60.

Schlarman, S. (2002) The case for a security information system. *Information systems security,* 11, 44-50.

Schultz, E. E. (2002) A framework for understanding and predicting insider attacks. *Computers & Security,* 21, 526-531.

Schwartz, A. P. & Zalewski, M. A. (1999) Assuring data security integrity at ford motor company. *Information systems security,* 8, 18-26.

Shaw, E. D., Ruby, K. G. & Post, J. M. (1998) *Insider Threats to Critical Information Systems. Technical Report #2; ,* Washington. DC, Political Psychology Associates.

Siponen, M. T. (2001) On the Role of Human Mortality in Information System Security: From the Problems of Descriptivism to Non-Descriptive Foundations. *Information Resources Management Journal.*

Siponen, M. T. (2005) An analysis of the traditional IS security approaches: implications for research and practice. *European Journal of Information Systems,* 14**,** 303.

Spurling, P. (1995) Promoting security awareness and commitment. *Information Management & Computer Security,* 3**,** 20-26.

Stacey, T. R. (1996) Information security program maturity grid. *Information Systems Security,* 5**,** 22-33.

Stanton, J. M., Stam, K. R., Guzman, I. & Caledra, C. (2003) Examining the linkage between organizational commitment and information security. *Systems, Man and Cybernetics, 2003. IEEE International Conference on,* 3.

Stanton, J. M., Stam, K. R., Mastrangelo, P. & Jolton, J. (2005) Analysis of end user security behaviors. *Computers and Security,* 24**,** 124-33.

Stewart, A. (2005) Information security technologies as a commodity input. *Information Management & Computer Security,* 13**,** 5.

Straub, D. W. & Welke, R. J. (1998) Coping with Systems Risk: Security Planning Models for Management Decision Making. *MIS Quarterly,* 22**,** 441-469.

Sullivan, W. E. & Ngwenyama, O.K. (2005) How are Public Sector Organisations Managing IS Outsourcing Risks? An Analysis of Outsourcing Guidelines from Three Jurisdictions. *The Journal of Computer Information Systems,* 45**,** 73.

Summers, W. C. & Bosworth, E. (2004) Password policy: the good, the bad, and the ugly. *Proceedings of the winter international synposium on Information and communication technologies***,** 1-6.

Tassabehji, R. & Vakola, M. (2005) Business email. *Association for Computing Machinery. Communications of the ACM,* 48**,** 64.

Thompson, E. D. & Kaarst-Brown, M. L. (2005) Sensitive information: A review and research agenda. *Journal of the American Society for Information Science and Technology,* 56**,** 245.

Thomson, K.-L. & Von Solms, R. (2005) Information security obedience: a definition. *Computers & Security,* 24**,** 69.

Toval, A., Nicolas, J., Moros, B. & Garcia, F. (2002) Requirements Reuse for Improving Information Systems Security: A Practitioner's Approach. *Requirements Engineering,* 6**,** 205-219.

Trim, P. R. J. (2005) Managing computer security issues: preventing and limiting future threats and disasters. *Disaster Prevention and Management,* 14**,** 493.

Trompeter, C. M. & Eloff, J. H. P. (2001) A Framework for the Implementation of Socio-ethical Controls in Information Security. *Computers and Security,* 20**,** 384-391.

Tryfonas, T. (2001) Embedding security practices in contemporary information systems development approaches T. Tryfonas, E. Kiountouzis, A. Poulymenakou The Authors. *Information Management & Computer Security,* 9**,** 183-197.

Turner, C. W., Zavod, M. & Yurcik, W. (2001) Factors that Affect the Perception of Security and Privacy of E-Commerce Web Sites. *Intl. Conf. on E-Commerce Research (ICECR,* 2, 628-636.

Vera-Munoz, S. C. (2005) Corporate Governance Reforms: Redefined Expectations of Audit Committee Responsibilities and Effectiveness. *Journal of Business Ethics,* 62, 115.

Vessey, I. (2002) Research in Information Systems: An Empirical Study of Diversity in the Discipline and Its Journals. *Journal of Management Information Systems,* 19, 129-174.

Von Solms, B. (2001) Corporate Governance and Information Security. *Computers and Security,* 20, 215-218.

Von Solms, B. & Von Solms, R. (2005) From information security to...business security? *Computers & Security,* 24, 271.

Von Solms, S. H. (2005) Information Security Governance - Compliance management vs. operational management. *Computers & Security,* 24, 443.

Vroom, C. & Von Solms, R. (2004) Towards information security behavioural compliance. *Computers & Security,* 23, 191-198.

Wen, H. J. & Tarn, J. M. (2001) Privacy and security in E-healthcare information management. *Information systems security,* 10, 19-34.

Winkler, I. S. & Dealy, B. (1995) Information Security Technology?… Don't Rely on It: A Case Study in Social Engineering. *5 thUNIX Security Symposium, June*, 5-7.

Yan, J. (2000) *The Memorability and Security of Passwords: Some Empirical Results*, University of Cambridge, Computer Laboratory.

Appendix A: Articles Included in Data Analysis

(Acquisti and Grossklags, 2003)
(Adams, 1999)
(Alner, 2001)
(Atkinson, 2005)
(Backhouse et al., 2005)
(Belsis et al., 2005)
(Beulen and Streng, 2002)
(Blatchford, 1998)
(Braithwaite, 2001)
(Brostoff and Sasse, 2001)
(Brusil and Hale, 2005)
(Campbell, 2003)
(Chellappa and Pavlou, 2002)
(Chen et al., 2004)
(Darragh and Darragh, 2001)
(Dhillon, 2001)
(Dhillon and Backhouse, 2000)
(Dhillon and Backhouse, 2001)
(Doherty and Fulford, 2005)
(Dynes et al., 2005)
(Miyazaki and Fernandez, 2000)
(Murray, 1998)
(Nagaratnam et al., 2005)
(Nyanchama, 2005)
(O'Brien and Yasnoff, 1999)
(O'Rourke, 2005)
(Paliotta, 2001)
(Palmer et al., 2001)
(Peltier, 1998)
(Pernul, 1995)
(Pollitt, 2005)
(Poore, 2000)
(Riley and Kleist, 2005)
(Rindfleisch, 1997)
(Ryan and Ryan, 2005)
(Saffady, 2005)
(Saint-Germain, 2005)
(Schlarman, 2002)
(Schultz, 2002)
(Schwartz and Zalewski, 1999)

(Ezingeard et al., 2005)
(Foote and Neudenberger, 2005)
(Furnell et al., 1996)
(Furnell et al., 2002)
(Gal-Or and Ghose, 2003)
(Gonzalez and Sawicka, 2002)
(Gonzalez and Sawicka, 2003)
(Gordon et al., 2002)
(Gupta and Hammond, 2005)
(Hansche, 2001a)
(Hansche, 2001b)
(Hazari, 2005)
(Holzinger, 2000)
(Hone and Eloff, 2002)
(James, 1996)
(Khalfan, 2004)
(Kankanhalli et al., 2003)
(Karat et al., 2005a)
(Karat et al., 2005b)
(Keller et al., 2005)
(Kim, 2005)
(Kokolakis, 2000)
(Kotulic and Clark, 2004)
(Krause and Brown, 1996)
(Krishnan et al., 2005)
(Kunreuther and Heal, 2003)
(Leach, 2003)
(Lee et al., 2004)
(Liu et al., 2003)
(Ma and Pearson, 2005)
(Boukhonine et al., 2005)
(Shaw et al., 1998)
(Siponen, 2001)
(Siponen, 2005)
(Spurling, 1995)
(Stacey, 1996)
(Stanton et al., 2003)
(Stanton et al., 2005)
(Stewart, 2005)
(Straub and Welke, 1998)
(Sullivan and Ngwenyama, 2005)
(Summers and Bosworth, 2004)
(Tassabehji and Vakola, 2005)
(Thompson and Kaarst-Brown, 2005)
(Thomson and von Solms, 2005)
(Toval et al., 2002)
(Trim, 2005)
(Trompeter and Eloff, 2001)
(Tryfonas, 2001)
(Turner et al., 2001)
(Vera-Muñoz, 2005)
(von Solms, 2001)
(von Solms, 2005)
(von Solms and von Solms, 2005)
(Vroom and von Solms, 2004)
(Wen and Tarn, 2001)
(Winkler and Dealy, 1995)
(Yan, 2000)