A Critical assesment of IS Security Research Between 1990-2004

Willison, Robert Andrew; Siponen, Mikko

Copenhagen
Business School
HANDELSHØJSKOLEN

A Critical assesment if IS Security Research Between 1990-2004

by

Robert Willison & Mikko Siponen

Department of Informatics
Howitzvej 60
DK - 2000 Frederiksberg

WORKING PAPER NO. 01-2007

Professor Mikko Siponen* and Dr. Robert Willison rw.inf@cbs.dk

* Corresponding author
Professor Mikko Siponen
Department of Information Processing Science
University of Oulu
PL 3000
90014 University of Oulu
Finland
Tel, 00 358 8553 1900
Fax, 00 358 8553 1890
msiponen@tols16.oulu.fi

A CRITICAL ASSESSMENT OF IS SECURITY RESEARCH BETWEEN 1990-2004

Abstract

This paper reviews the IS security literature for the period 1990-2004. More specifically three security journals and the top twenty IS journals were examined. In total 1280 papers were analysed in terms of theories, research methods and research topics. Our research found that 1043 of the papers contained no theory. In addition, almost 1000 of the papers were categorized as 'subjective-argumentative' in terms of methodology, with field experiments, surveys, case studies and action research accounting for less that 10% (8.10%) of all the papers. Fifty nine research topics were identified with fourteen of these topics totaling 71.05% of the articles.

This papers offers implications for future research directions on IS security, scholars to publish IS security research, tenure practice, and IS security classification schemas.

1 INTRODUCTION

In recent years organisations have paid increasing attention to IS security. This is understandable given the sheer amount of information now in digital form. The desire to secure such information has been fuelled by concerns over the rising number of corporate security breaches. One security survey, for example, noted how in 1997, 37% of respondents reported a breach (Thompson, 1997). However, more recent surveys have reported a figure averaging 90% (Bagchi and Udo., 2003, p. 684; Hinde 2002 p. 310).

Given the need for effective IS security, what has been the academic response? Has the discipline, in a bid to support the security efforts of practitioners, developed intellectually? What topics are being addressed? What methodologies are being deployed and what theories are being adopted? The purpose of this paper is to answer these research questions. To do so, we have analysed three main IS security journals and the top twenty IS journals for the period 1990-2004. In total 1280 papers were assessed.

The next section of the paper describes those existing IS security studies which have analysed the field. This is coupled with a description of the research framework used in this study and the related research strategy. The results and discussion sections then follow, with the final part of the text presenting the conclusions.

2 EXISTING RESEARCH, RESEARCH FRAMEWORK AND RESEARCH STRATEGY

2.1 Existing research

Previous literature reviews in IS security have focused on the methods for the development of secure systems (Baskerville, 1992; Siponen, 2005a,b; Villarroel, Fernández-Medina et al., 2005). In addition, the IS security literature has been analyzed using sociological paradigms by Burrell and Morgan to illustrate the need for understanding the social as well as technical aspects of a control environment (Dhillon et al., 2000) – see Table 1.

Article	Area	No. of articles analysed
Baskerville (1992)	Methods for the development of	19

	secure systems.	
Dhillon and Backhouse (2001)	IS security literature.	11
Siponen (2005a)	Methods for the development of secure systems.	17
Siponen (2005b)	Methods for security management and the development of secure systems.	17
Villarroel, Fernandez-Medina and Piattini (2005)	Methods for the development of secure systems.	11

Table 1. Existing IS Security Literature Reviews

While there is no doubt that these studies have provided a number of important insights for IS security research and practice, they have certain limitations. First, the number of IS security articles covered by these studies are relatively small (Table 1). Second, none of these studies apply inter-rater reliability criteria. The latter refers to a method whereby the literature is reviewed separately by two or more individuals, known as coders or raters. To the best of our knowledge, this is the first attempt to review the literature in this manner.

2.2 Selection of research framework

The cornerstone of a sound literature review is the use of a conceptual framework which not only helps to map out the existing research, but also helps in identifying directions for future research. For this purpose, different frameworks have been used by IS scholars. Hirschheim et al. (1995; 1996) and Iivari et al. (2001) used Burrell and Morgan's sociological paradigms to review methods for the IS development. Iivari et al. (1998) have analyzed IS development methods in the terms of research methods, the organizational role of IS, and research objectives. Kuhn's work on paradigms has influenced Iivari's (1991) research, while Farhoomand (1987) applies Popper's view of science.

While these philosophical views have produced interesting findings, there are deficiencies. Both Burrell and Morgan (1979) and Kuhn (1970) take a relativist position with regard to 'paradigms'. This means that different paradigms are always incommensurable. A scholar belonging to one paradigm, say a "positivist" cannot understand and criticize research within other paradigm, say "interpretivist", according to Burrell and Morgan (1979) and Kuhn (1970). For Kuhn, the incommensurability occurs as a result of the fact that different paradigms define their own fundamental assumptions regarding research methods, validation and even language. Since scholars within different paradigm "practice their trades in different worlds", their findings are not comparable in any way across different paradigms. As a consequence, because scientific revolutions represent an "all-or-nothing" form of change, there is no progress in science, according to Kuhn (1970, 150)[1]. Similarly, Burrell and Morgan (1979) argue that research within different paradigms is not comparable, and hence meaningful conversations between different paradigms are not possible. In addition they insist that different paradigms must not be reconciled.

Following Chua (1986), Iivari (1991) and Landry and Banville (1992), we argue that such incommensurable views – (1. impossible to measure and compare research across paradigms; 2. any discussions across paradigms are meaningless, 3. paradigms should not be integrated) - are difficult to accept. If inter-paradigmatic research is incommensurable, research within a paradigm would be immune to external criticism. This then leads to the position where research quality would be difficult to measure, since everything would be accepted simply by appealing to the

[1] Kuhn sees that scientific revolutions are "non-cumulative developmental episodes in which an older paradigm is replaced in whole or in part by an incompatible new one." (Kuhn, 1970 p. 92).

incommensurability of a paradigm. Yet, such a position would not be welcome. To avoid these problems, Laudan (1984) advances a reticulated model of science (see also Landry & Banville, 1992). This model is used to underpin the research framework.

2.3 Research framework

Laudan proposes the Reticulated Model of Science which consists of theories, methods, and aims (goals, ends, values). In his view, changes in theories, methods, and aims are piecemeal and happen one at a time, rather than the all-or-nothing position as proposed by Kuhn[2]. In addition, aims, methods and theories are rationally negotiable. In opposition to Kuhn (1970), conceptual dialogue across paradigms is a potential source of progress in science (Batts & Crawford, 1991 p. 348). For Laudan, there is no one aim (e.g., "truth") in science. Finally, science is progressive, since scientific progress is nothing more than progress towards our goals. If the goal changes, then the criterion on what constitutes progress changes. Therefore, progress in science, though relative to fixed goals, can be rationally evaluated.

In summary, there are three elements of Laudan’s Reticulated Model of Science: Theories, methods and aims. Next we describe how we use these elements in our analysis, and also point out their importance in IS literature.

2.3.1 Theories and research methods.

As discussed below, the application of theory and the use of appropriate research methods are seen as essential and elementary features of any research. In the IS field, this view is also shared by natural science (often referred to as positivists) and social science orientated (often referred to as interpretivists) scholars (Culnan, 1987; Landry et al., 1992). The importance of theory and research methods, is further recognized by supporters of “IS-as-a-design-science” view, which asserts that IS research does not easily fit into the models of the social or natural sciences (Walls et al., 1992, Walls et al., 2004).

In an attempt to assess the quality of the theories applied in IS security, and the manner in which they are used, we refer back to Laudan’s “reticulated model of science”. Laudan argues that a theory must be in accordance with the research method used and the goals of the research. To adapt a simple interpretation of this view: a theory has to be used in a way that it contributes something to the study/topic that would most likely be lacking without this theory. That is, studies only referring to theory as skin deep do not meet this criterion. To illustrate such a use of a theory, in their article on the use of design theory, Walls et al. (2004 p. 55) describe four levels of the use of design theory. At the first level, design theory is referred to at a superficial level, as a "cloak of theoretical legitimacy", without indicating how exactly the design theory guides the research. In our analysis, we would not classify such studies as based on design theory.

The research method classification was adopted from Galliers (1992), which includes: laboratory experiment, field experiments, surveys, case studies, theorem proof, subjective/argumentative, case studies, forecasting and future research, simulation and, finally, action research. ‘Laboratory experiments’ refer to tests carried out in such an environment, while ’field experiments’ utilize natural science methods to study phenomena in the field rather than in the context of a laboratory. While ‘surveys’ are used to collect quantitative information (Straub, 1989), ‘case studies’ focus on in-depth studies of a single event, hence the name, ‘case’ (Yin, 2002). ‘Theorem proof’ refers to non-empirical research containing theorems and their proofs, typically used in field of Computer Science (Lending et al., 1992 p. 5). ‘Subjective/argumentative’ refers to conceptual-

[2] Kuhn sees that theories, methods and aims in science form an inseparable package: scholars cannot modify one without modifying the others.

theoretical research research. ‘Simulation’ refers to quantitative modeling of systems in order to understand their functioning. ‘Action research’ takes a similar form to case studies, with a notable difference being the iterative action research cycle (Baskerville and Wood-Harper, 1998).

We also added a research method called 'secondary data' to Gallier’s classification (1992). During the analysis the authors identified papers, which used such data as a basis for their methodology, hence it was decided that the category should be created.

2.3.2 Research topics (aims)

Within IS, the examination of the research topics, which constitute a specific field is considered to be highly relevant. Such examination helps to throw light on the type of research, and ultimately the very nature of the subject area itself (Bacon et al., 2001). There are two ways of forming a research topic classification. One method is to “let the published works speak themselves”, i.e., analyze the literature while avoiding the use of a predefined classification systems (Bacon et al., 2001). In other words, produce a classification based on a theory creating or ‘grounded theory’ type of method. An alternative approach is to use *a priori* theory or classification systems such as the ISRL categories or the ACM classification system (as used by Vessey et al., 2002). The former method was chosen for the purposes of this study for the following reasons. First, the authors wanted to offer a genuine and comprehensive picture of IS security research. It can be argued that existing classification schemas (for example the ACM categorization), reflect a limited computer science perception of security research. Furthermore, a classification of the literature, "starting with a clean slate", offers the potential for an updated view of the field, as opposed to the use of a predefined classification system. In addition, when using predefined classification systems (like the ACM), no insight is offered into how such typologies are created. Predefined classifications may also not reflect the actual research in the field. For instance, Zhang and Li (2005 p. 272) noted this difficulty when using predefined classification schema for analyzing HCI research. In fact, using a strategy based on ‘let the published works speak for themselves’, may even contribute to such classification schemas as advanced by the ACM.

2.4 Methodological considerations

To classify research within a specific IS field, scholars have analyzed key words, abstracts or full texts (Vessey et al., 2002). This study is based on the analysis of full texts, as it was considered the most reliable method of reviewing the literature and developing a research topic classification.

To increase the reliability of the analysis, we applied the inter-rater reliability criteria as follows. The first stage of analysis involved the authors separately reviewing the relevant literature, and identifying tentative categories of classification. The authors then critically discussed their initial analyses and through this process reached a consensus with regard to the most suitable forms of classification.

2.5 The scope of the research

The scope of the research covered three IS security journals and the top 20 IS journals. The security journals included Computers & Security, Information Management & Computer Security and Information Systems Security. These were chosen as they act as the three major publications in the field. Other publications including the Journal of computer security and ACM Transaction on Information and Systems Security were omitted from the research. These well known security forums were classified as computer science forums based on their editorial policy and the type of papers published in them. In addition, the top 20 IS journals were analyzed. There are other well known ranking lists, the most notable being the combination of six ranking studies (see http://www.isworld.org/csaunders/rankings.htm). This list, however, contain journals within related disciplines that do not really contain IS papers (Chua, Cao, Cousins et al., 2002), not to mention IS security papers. And yet, the list may not fully reflect the status of the journals in the field. For example, JAIS is often, (as per the Saunders ranking), ranked below CAIS (Lyytinen, 2006). For these reasons, we selected a list that primarily ranks IS journals (Peffers and Tang, 2003). The IS journals in the list are: CAIS, JACM, ISF, IT&P, EJIS, ISR, JSIS, ISJ, JCIS, IRMJ, I&M, JMIS, JAIS, MISQ, JofDM, DSS, JGinfMgt and IJofECom.

The period of analysis covers 15 years (from 1990 to 2004) and compares well with similar IS research projects. Indeed, Zhang and Li (2005), whose review of the HCI literatures covers 13 years note how their study 'is more than double the period that is normally used in this type of research'. As a consequence we feel that our period of analysis is more than justified. The number of IS security papers analysed amounted to 1280. Once again, this figure can be viewed in a favourable light when compared with similar IS research (Culnan, 1987; Zhang et al., 2005; Iivari, 2004).

3 RESULTS

3.1 Theories Used In IS Security Research

In total 38 theories, listed in Table 2 (see appendix), were identified through our analysis. Of the 1280 papers we analysed, 237 (18.51%) included one or more of these theories. By far the largest category identified was 'mathematics' accounting for 189 papers, which represents nearly 80% (79.74%) of all the articles containing theory. Hence the other 37 theories accounted for just over twenty percent of the remaining (48) papers. This means that 30 of the 37 theories were cited once. The remaining seven theories included six which were cited twice, leaving General Deterence Theory which was referenced in six papers.

3.1.1 Methods Used In IS Security research

Table 3 (see appendix) summarises our findings with regard to the research methods used in the articles. The 'subjective-argumentative' category, accounted for 996 (77.81%) papers. The remaining nine categories, therefore, covered the other 284 papers. Of this total, 146 (11.40%) were categorised as 'theorem proof' texts. If we combine the 'subjective-argumentative' and 'theorem proof' total, the figure comes to 1,142 (89.21%) papers. Hence, the remaining categories (field experiment, survey, action research, case research, forecast, simulation, laboratory experiments and secondary data) accounted for 138 (10.79%) papers.

3.1.2 Topics in IS security research

Table 4 (see appendix) summarises our research findings for the topics studied in the articles. As can be seen, fifty-nine categories were identified using the inter-rater method, discussed earlier. Despite this large number, 14 categories constitute 71.95% of all the papers. These categories (with over 30 papers or more) include 'legal aspects of IS security' (43 = 3.35%), 'general IS security' (85 = 6.64%) 'business continuity planning' (41 = 3.20%), 'IS security management and planning' (113 = 8.82%), 'OS security' (32 = 2.50%), 'risk management' (38 = 2.96%), 'viruses and malware' (61 = 4.76%), 'computer-crime' (32 = 2.50%), 'database security' (80 = 6.25%), 'intrusion detection systems' (38 = 2.96%), 'network and communication security' (139 = 10.85%), 'secure systems design' (33 = 2.57%), 'identification and authentication' (46 = 3.59%) and cryptography (140 = 10.93%).

Of the remaining 45 categories, the most notable include 'security and privacy' (28 = 2.18%), 'copyright and piracy issues' (17 = 1.32%), 'security behaviour' (15 = 1.17%), 'hackers and hacking' (16 = 1.25%), 'security polices' (21 = 1.64%), 'Public Key Infrastructures' (17 = 1.32%) and 'computer forensics' (29 = 2.26%). This means, therefore, that the remaining 38 categories constitute 216 (16.88%) papers. While the remaining number of 38 additional categories may appear high, an additional category of 'general IS security' was introduced (see above), owing to the fact that a number of papers (85) proved difficult to place in the other categories. Hence these papers were assigned to this 'general' category.

From another perspective, it is interesting to note the distribution of the 1280 papers in the journals. The three specialized security journals accounted for 1,166 (91.09%) of the papers. Hence the top twenty IS journals contained 114 IS security articles for the period 1990-2004. In fact it should be noted that two of the top twenty IS journals (Database, MISQ Discovery) contained no security papers in this period.

4 DISCUSSION

4.1.1 Research methods and theories

In total only 18.51 % of the articles cited one or more theories. Hence over 1000 articles contained no theory whatsoever. As noted, of the 18.51%, nearly 80% cited 'mathematical' theory, which leads to the position where the other 37 theories accounted for only 48 papers. Indeed, thirty of the theories identified were only cited once. This indicates that while theories may be cited, intellectual development fails to occur as other researchers do not adopt and explore such theories. Hence these figures generally indicate that IS security research is chronically underdeveloped in terms of theory. This is worrying as with science in general (Laudan 1984), the use of proper theories are seen as a fundamental element of IS research (Walls et al., 1992).

Overall, 79 % of the IS papers were subjective argumentative in terms of their research method. While there is nothing wrong with descriptive and conceptual papers, these results suggest a worrying picture regarding the status of IS security research. While the field needs to advance intellectually, this is hampered by the lack of empirical research which has taken place. The percentage of papers in the study which use field experiments (0.07%), surveys (5.31%), case studies (2.65%) and action research (0.07%) illustrate how such intellectual development is hamstrung by the paucity of empirical research into the problems posed in the field. This in itself is problematic, but the lack of empirical research also fails to provide directions for, and a firm basis on which, future research can be based. These problems are compounded further when coupled with the dearth of theory used in the IS security field. Finally, the low number of use of theories and empirical research methods in Information Systems Security, Computers & Security and Information Management and Computer Security and raise serious doubts on whether these forums can be on the target journal list for tenure-track faculty.

4.1.2 Research topics

It is perhaps worrying that just 14 topics account for nearly 72% (71.95%) of all the papers reviewed. IS security is supposedly a broad church covering numerous areas of research and yet relatively few categories account for such a high percentage of the papers. Of the 71.95%, those categories with an overtly technical focus (OS security, viruses and malware, database security, intrusion detection systems, network and communication security, secure systems design, identification and authentication, and cryptography), account for nearly 45% (44.45%) of all the papers. When this analysis is broadened to include other technical topics identified in our analysis (technical certification, digital signatures, wireless security, mobile application security, technical standards, DOS and PC security, firewalls, biometrics, hackers and hacking, Public Key

Infrastructures, spam, code security, and computer forensics) the figure rises to 54.45% (697 papers). Hence only nineteen topics account for this number.

In relation to the above, it has long been recognised that it is important to understand the social as well as technical elements of IS security. Yet the more ‘social’ topics in comparison with their technical counterparts have received relatively little attention. For example, our analysis found that just 2 (0.15%) and 7 (0.54%) papers have been written about ‘security education’ and ‘security awareness’, respectively. Another category which covers the ‘security behaviour’ of those involved in maintaining security accounted for 15 (1.17%) of all the papers. Given that people play a central role in enforcing IS security, it is perhaps alarming that so little research has addressed these three areas.

4.1.3 Implications for key words and research topics classifications

The findings have implications for keyword classifications, as provided by ACM, IEEE, ISR and MISQ (to our knowledge, JAIS and JMIS do not include predefined keyword categories). The ISR keyword classifications schema does not contain any items related to IS security. Of these classifications systems, ACM’s is the broadest in terms of topics covered. As one might expect, the IEEE keywords system is CS oriented. The "Abuse and crime involving computers" is the only IS security, or non-computer science category. Interestingly, while the MISQ classification system (Barki & Rivald, 1993) contains items such as "Abuse and crime, Piracy, Fraud and Ethics", it also has a strong technical or computer science flavour, as indicated by the keywords such as data security, data encryption, access control, authentication, authorization, passwords, and computer viruses. This interpretation is based on the idea that concepts like "data encryption" refer to the study of the technology itself rather than user interaction or organizational implications of "data encryption". Comparing the findings of our study with these classifications systems, we find several IS security topics missing. These include security economics, security management standards, users security behaviour, security management and planning, social engineering, IS security risk management, IS security education, IS security awareness, secure systems design, computer forensics, information warfare, and finally, password creation and memorization. We suggest that the keyword classification systems of leading IS journals should be updated in the light of our findings.

5 CONCLUSION

As the importance of IS security has increased in practice - what has been the academic response? Has the discipline, to support the security efforts of practitioners, developed intellectually? What research topics are being addressed? What methodologies are being deployed and what theories are being adopted? To explore these questions, we analyzed IS security journals and the top 20 IS journals over a period of 15 years (1990-2004). As a result, 1280 security articles were identified and analyzed in terms of their (1) research topics, (2) theories and (3) research methods used. The results suggest that most of the studies were subjective argumentative in terms of their research methodology. Furthermore, our analysis suggests that IS security research is theoretically underdeveloped. As a result, we argue the need for theoretically grounded research that uses empirical research methods including, for example, surveys, case studies and actions research.

Interestingly, while the number of IS security articles in Information Systems Security, Computers & Security and Information Management and Computer Security has increased and the number of IS incidents have increased, one would expect that the number of IS security articles in top IS journals would increase. However, historical figures regarding the most leading IS journals, MISQ and ISR, show that the number of IS security articles has remained slow, or even decreased. For example, the only IS security article in ISR is published in 1990. Between 1999-2004, there are no IS security articles in MISQ, while between 1990-1998 there are 4. In JMIS, there is IS security articles between 2001-2004, while between 1991 and 2000, there is 5 IS security articles. These considerations raise several questions. Are IS security papers difficult to publish in top-tier IS journal, or is the low quality of submission the reason explaining the low number of security articles in top-tier IS journals.

6 REFERENCES

Bagchi, K. and Udo, G., “An analysis of the growth of computer and Internet security breaches”, Communications of AIS 12, 2003, 684–700.

Baskerville, R. (1993) “Information systems security design methods: Implications for information systems development,” ACM Computing Surveys (25) 4, pp. 375–414.

Baskerville, R. and Wood-Harper, T. (1998) “Diversity in information systems action research methods,” European Journal of Information Systems 7, pp. 90–107.

Baskerville, R., & Myers, M. (2002). Information Systems as a Reference Discipline. MIS Quarterly, 26(1), pp. 1-14.

Banville, C. and Landry, M. "Can the Field of MIS be Disciplined"?. Communications of the ACM, January 1989, Vol. 32, Number 1, pp. 48-60.

Burrell, G. and Morgan, G. Sociological Paradigms and Organisational Analysis, Heinemann, London, 1979.

Batts, B & Crawford, L.L. (1992) Problematic progress: A review of Laudan’s progress and its problems and science and values. Journal of the experimental analysis of behaviour, issue 55, no 3, pp. 337-349.

Dhillon, G. and Backhouse, J., “Current directions in information security research: toward socio-organizational perspectives”, Information Systems Journal. 11, 2, 2001.

Farhoomand, A.F., (1987), Scientific Progress of Management Information Systems. Database, pp. 48-56.

Culnan, M.J. Mapping the Intellectual Structure of MIS,1980-1985: A co-citation Analysis. MIS Quarterly, 11 (3):341-354, September 1987.

Chua, C, Cao, L., Cousins, K and Straub, D (2002) Measuring Research-Production in Information Systems. JAIS 3, pp. 145-215.

Galliers, R. (ed.). Information systems research: Issues, methods, and practical guidelines, Blackwell Scientific Publications, Oxford, 1992.

Hinde, S., “Security surveys spring crop”, Computers & Security, 21, 4, 2002, 310-321.

Hirschheim, R., Klein, H. K., & Lyytinen, K. (1995). Information Systems Development and Data Modelling: Conceptual and Philosophical Foundations. Cambridge University Press, UK.

Hirschheim, R., Klein, H. K., & Lyytinen, K, (1996), Exploring the intellectual structures of information systems development: a social action theoretic analysis, Accounting, Management and Information Technologies 6 (1-2), pp. 1-64.

Iivari, J, Hirschheim, R., Klein, H. K. (1998), A Paradigmatic Analysis Contrasting Information Systems Development Approaches and Methodologies. Information Systems Research, vol. 9, no. 2, pp. 164-193.

Iivari, J. and Hirschheim, R., Klein, H. K. (2001), A Dynamic Framework for Classifying Information Systems Development Methodologies and Approaches. Journal of Management Information Systems. Vol. 17 No. 3, pp. 179 – 218.

Iivari, J, Hirschheim, R., Klein, H.K., Towards a distinctive body of knowledge for Information Systems experts: coding ISD process knowledge in two IS journals. ISJ, 14: 313–342, 2004.

Kuhn, T.S., 1970. The Structure of Scientific Revolutions. (2nd. edition enlarged) Chicago: University of Chicago Press.

Lakatos, I., Musgrave ed. (1970). Criticism and the Growth of Knowledge. Cambridge: Cambridge University Press.

Landry, M and Banville, C (1992), A Disciplined Methodological Pluralism for MIS Research. Accounting, Management and Information Technologies, vol. 2, no. 2, pp. 77-97.

Laudan, L., 1984, Science and Values. Berkeley: University of California Press, CA, USA.

Lending, D. & Wetherbe J.C (1992): Update on MIS Research: A Profile of Leading Journals and U. S. Universities. DATA BASE 23(3): 5-11.

Peffers, K., & Tang, Y. (2003). Identifying and evaluating the universe of outlets for information systems research: Ranking the journals, The Journal of Information Technology Theory and Application (JITTA), 5:1, 63-84.

Siponen, M.T. (2005a) “Analysis of modern IS security development approaches: towards the next generation of social and adaptable ISS methods,“ Information and Organization (15) 4, pp. 339–375.

Siponen, M.T. (2005b) “An analysis of the traditional is security approaches: implications for research and practice,” European Journal of Information Systems (14) 3, pp. 303–315.

Straub, D. W., “Validating Instruments in MIS Research", MIS Quarterly, 13, 2, 1989, 147-169.

Thompson, D., “1997 Computer crime and security survey”, Information Management & Computer Security, 6, 2, 1998, 78–101.

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

Villarroel, R., Fernández-Medina, E. and Piattini, M., “Secure information systems development – a survey and comparison”, Computers & Security, 24, 4, 2005, 308-321.

Walls, J.G., Wildmeyer, G.R. and El Sawy, O.A. (1992) “Building an information systems design theory for vigilant EIS,” Information Systems Research (3) 1, pp. 36–59.

Walls, J. G., Widmeyer, G. R., and El Sawy, O. A. (2004). Assessing information system design theory in perspective: How useful was our 1992 initial rendition? JITTA: Journal of Information Technology Theory and Application, (6)2, pp. 43-58.

Yin, R.K. Case Study Research. Design and Methods. Third Edition. Applied social research method series Volume 5. Sage Publications. California, 2002.

Zhang, P and Li, N., (2005), The intellectual development of Human-Computer Interaction Research: A critical Assessment of the MIS literature (1990-2002). The Journal of the Association for Information Systems. Vol. 6, no. 11, pp. 227-292.

7 APPENDIX

Table 2: Analysis of Theories Used in IS Security Research

Journal	C&S	ISS	IM&CS	JACM	ISF	IT&P	EJIS	CAIS	ISR	JSIS	ISJ	JCIS	IRMJ	I&M	JMIS	JAIS	MISQ	JofDM	DSS	IJofECom	Total
Theory																					
Mathematics	152	3	9	23										1					1		189
Agricultural sciences	1																				1
Schank's theory of conceptual dependency	1																				1
Theory of planned behavior			1												1						2
Theory of reasoned action			1																		1
Emotivism			1																		1
Universal Prescriptivism			1										1								2
General deterrence theory			1						1					1	1		2				6
Social bond theory			1																		1
Social learning theory			1																		1
Possibility theory																		1			1
Burrell and Morgan's sociological paradigms											1										1
Porter's value chain	2																				2
Modern portfolio theory	1																				1
The theory of stock market efficiency	1																				1
Game theory	1							1													2
Transaction cost theory	1																				1

Risk compensation theory	1																1
Immunology	1																1
Cell theory						1											1
Information theory	2																2
Falsificationism	1				1												2
Schein's theory of org. culture	1																1
Fuzzy logic			1														1
Viable systems theory			1														1
Theory of satisfactoriness											1						1
Theory of the search for associative memory											1						1
Social control theory											1						1
The Compertz survival time model						1											1
Expected utility theory												1					1
Ethics							1										1
Theory of justice										1							1
Cultural relativism										1							1
Bayesian theory									1								1
Goodhue's theory of IS success											1						1
Differential Association Theory																1	1
Rational Choice Theory																1	1
Routine Activity theory																1	1
Total	166	3	18	23	1	3	2	1	1	3	6	3	2	1	1	3	237

Table 3: Analysis of Methods Used in IS Security Research

Journal	C&S	ISS	IM&CS	JACM	ISF	IT&P	EJIS	CAIS	ISR	JSIS	ISJ	JCIS	IRMJ	I&M	JMIS	JAIS	MISQ	JofDM	DSS	JGinfMgt	IJofECom	**Total**
Methods																						
Sub/Argumentative	501	273	176	1	7		2	6			2	13	2	5	1			2	2	1	2	996
Field experiment			1																			1
Surveys	27	1	13				1		1	1		11		7	2	1	3					68
Action research																	1					1
Case research	13	2	12		2	1	1						1	1	1							34
Forecast																						0
Simulation	7																					7
Lab experiment	16	1	4		1									1				1				24
Theorem proof	111	3	5	23					1			1						1	1			146
Secondary data								2				1										3
Total	676	280	211	24	10	1	4	8	2	1	2	26	3	14	4	1	4	4	3	1	2	1280

Table 4: Analysis of Topics Used in IS Security Research

Journal	C&S	ISS	IM&CS	JACM	ISF	IT&P	EJIS	CAIS	ISR	JSIS	ISJ	JCIS	IRMJ	I&M	JMIS	JAIS	MISQ	JofDM	DSS	JGinfMgt	IJofECom	Total
Topic																						
Industrial espionage	5	1																				6
Technical certification	3																					3
Digital signatures	6	1	2	1																		10
Audit of IS	5	1	2																			8
Legal aspects of IS	19	12	7		2	1	1													1		43
Wireless security	2	6	3					1														12
Outsourcing & sec	1	3	1																			5
E-com and Dig pay	3	5	1		1					1											1	12
Mobile application sec	3	1	2																			6
The Inform society	1		1																			2
Info sec expenditure	4	2						1														7
Review articles	1										1											2
Security economics	2		1																			3
Physical security	2		2																			4
Technical standards	3	1																				4
Sec mgt standards	6	2	5																			13
EDI security	7	2	4																			13
Security and ethics	1		2																			3
DOS and PC sec	2											1										3
General IS sec	47	20	17									1										85
Bus cont plan	11	8	19		1			1					1									41
Types of sec attacks	4	3	1					1						1								10

Sec and privacy	4	12	9	2	1													28
Cryptography	108	12	4	16														140
Home working	1		1															2
Copy & piracy issues	3	3	2					1	6		1	1						17
Security behaviour	10		1					1			2		1					15
Sec mgt and plan Plan	48	27	24			1			4	1	3	1		2	1	1		113
Secure voting issues	4																	4
Information warfare	9	3	1															13
Firewalls	6	3	2															11
Biometrics	5	1	2															8
National info sec	6	1																7
OS security	18	13	1															32
Hackers & Hacking	7	5	2				1		1									16
Social engineering	1	3																4
Security taxonomies	3																	3
Security education	2																	2
Risk management	18	9	6			1			1	1	1	1						38
Viruses and malware	37	13	3				1		5		2							61
Security policies	9	5	5			1			1									21
Computer crime	14	5	6		2				2		1			1			1	32
Password creation & memorization	4		2									1						7
Database sec and access control	57	10	7								3				3			80

Workstation sec	1																					1
Intrusion detection systems	23	7	8																			38
Security awareness		4	3																			7
PKI	5	3	8																1			17
Code security	5		1																			6
Spam	2	1																				3
Security threats	2																1					3
Network and com sec	60	38	29	4	2			2				4										139
Trust			4																1			5
Secure systems design	20	7	5								1											33
Password systems	4																					4
Computer forensics	13	15			1																	29
Identification & authentication	29	12	4											1								46
Total	676	280	210	23	10	1	4	8	2	1	2	26	3	15	4	1	4	4	3	1	2	1280