RESEARCH IN INFORMATION SECURITY: A LITERATURE REVIEW USING A MULTIDIMENSIONAL FRAMEWORK

Yan Chen, Lubar School of Business, University of Wisconsin-Milwaukee, 3202 North Maryland Avenue, Milwaukee WI 53211, 414-229-1122, yanchen@uwm.edu
Derek Nazareth, Lubar School of Business, University of Wisconsin-Milwaukee, 3202 North Maryland Avenue, Milwaukee WI 53211, 414-229-1122, derek@uwm.edu
Kuang-Wei Wen, College of Business Administration, University of Wisconsin-la Crosse, 1725 State Street, La Crosse, WI 54636, 608-785-6658, wen.kuan@uwlax.edu

ABSTRACT

To better understand the current status of information security research, this study developed a multidimensional classification framework that includes four key research characteristics as well as the NSTISSC dimension, and surveyed 240 information security related articles in ten academic journals published in 2000-2007. Our analyses revealed the disproportionate concentration of studies in the four socio-organizational paradigms, the dominant research methods, the relationship between information security and other established fields, the prevalent levels of study and relationship between information security research and industrial practices. These findings led to our identification of promising directions for future research.

Keywords: Information Security, Security Literature Survey, Socio-organizational Perspective

INTRODUCTION

While information security has been studied by the academia for decades (e.g. [27][30][32]), the majority of research works have disproportionally focused on the technical aspect alone. This bias could be due to the lack of awareness of the complex and multidisciplinary nature of information security or caused by the disparate views on information security problems from different disciplines' perspectives ([2][10][29]). On the practice side, businesses found that their information security problems also call for managerial, social, ethical, and legal solutions ([23][31]). As compared to other types of IS research, information security research is also hard and scant because security information is critical and sensitive to organizations and they are normally not inclined to give out such information. As a result, some commonly used research methods such as survey, case study, and action study may not work well in information security research [17].

Having been subject to these difficulties, what is the current status of information security research? To answer this question, we conduct an analysis on the published works of information security and security management along multiple dimensions. We try to construct a "whole" picture about what research has been done in the field recently, what trends exist in current research, and what kind of potential research need to be done in the future.

RESEARCH FRAMEWORK

Due to the paucity of frameworks for classifying information security literature we developed a multidimensional framework that also borrows frameworks for analyzing IS literature.

Socio-organizational Paradigms

From philosophical and social perspectives, Orlikowski and Baroudi [24] and Chen and Hirschheim [6] examined IS literature and classified IS research methodologies into positivist, interpretive, and critical paradigms. This classification of research epistemologies borrowed the theories from "school of thought" (e.g. Burrell and Morgan [4]). In a similar approach, Dhillon and Backhouse [10] reviewed both IS and information security literatures before 2000. Using two dimensions, subjective-objective and regulation-radical change, they argued that IS and information security literature fell into four paradigms: functionalist, interpretive, radical humanist, and radical structuralist paradigms. Iivari et al. developed a three-dimensioned framework ([12]: paradigms, approaches, and methodologies) and then enhanced it to a four-tiered framework ([13]: paradigms, approaches, methodologies, and techniques) to classify IS development approaches and methodologies**.**

In order to allow room for researches investigating the dynamics of designing and implementing effective information security systems as well as their impacts on various aspects of the organization, we need to employ a sound classification framework that is sufficiently inclusive with a higher level of abstraction (see, for example, [29]). In addition, as the second criterion, the adopted framework must be able to accommodate any discernible trends in the historical and emerging literatures. With these two tests we evaluated the reviewed classification frameworks for IS and information security related literatures, and adopted Dhillion and Backhouse's framework for its ability to allow for emerging trends in exploring radical changes and conflicts brought by security management from both structured and unstructured perspectives.

Research Methods

IS researchers have shown great interest in research methods when conducting literature survey research. Vessey et al. **[**33] considered research method as one of the most important characteristics when studying the current state of IS research diversity. Extensive work on finding IS research methods have been done by Alavi and Carlson [1] and Palvia et al. [25][26]. Comparisons of and criticisms on various methods can be found in Lyytinen [20], Markus and Lee [21], and Walsham **[**34]. Following the existing IS methodological taxonomies (e.g. [1][24][25][26]), we identified nine essential methodology categories: 1) conceptual analysis, 2) mathematical analysis/analytical modeling, 3) literature review, 4) speculation/commentary, 5) system implementation/evaluation, 6) experimentation, 7) survey, 8) instrument development, and 9) case study for the current research.

Reference Discipline

Reference discipline is a dimension we can use to analyze core theories and foundations of a discipline or research field. Some scholars point out that IS is multi-disciplined in nature and rooted in social sciences, and that IS research needs to focus on broad organizational and social issues. Therefore we tend to use a broad range of reference disciplines as our source of core theories **(**[15][28]). Vessey et al. [33] studied the key characteristics of diversity in IS and found that the reference discipline dimension had the highest index of diversity among five key characteristics. Siponen and Oinas-Kukkonen [29] also found that information security research borrowed theories and methods from a broad range of reference disciplines such as mathematics, philosophy, criminology and biosciences.

For the reference discipline dimension in this study, we basically adopted the categories developed by Vessey and Glass [33]. Following their classification scheme we indentified one core reference discipline for each article by looking at the theories the authors used to develop their model or hypothesis. Our categories are: 1) cognitive psychology, 2) social and behavior science, 3) computer

science, 4) economics, 5) information systems, 6) management, 7) management science, 8) mathematics, 9) others, and 10) not applicable.

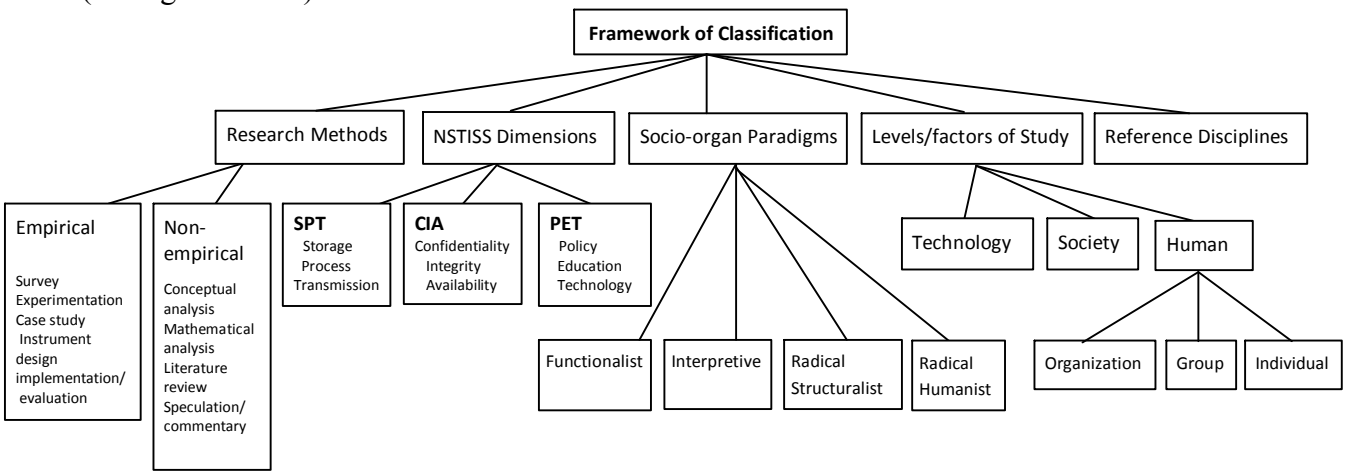
Level of Study

The main theme of IS research is to provide IS technology solutions to individual, group, organizational and social issues and to find out the impacts of these solutions on individuals, groups, organizations and societies. Many IS researchers have recognized the need for studying different levels of IS behaviors ([16][29][33][35]). Both Vessey et al. [33] and Siponen and Oinas-Kukkonen [29] included the dimension of level of study in their survey frameworks. In a theme paper, using keywords queries, Beznosov and Beznosova [3] conducted blanket searches of Google News Archives, Web of Science, and Engineering Village. They surveyed activities of information security on the basis of technological, human, and social factors.
We followed the existing literature to define three main levels of study: technology, society, and human. The human level was further broken down to three sub-levels: individual, group, and organization.

NSTISS Dimension

In answering Chiasson and Davidson's [7] call for IS researcher to "take industry seriously" we introduced the NSTISS (National Security Telecommunications and Information Systems Security) security model into our framework. This security model was developed by NSTISSC (National Security Telecommunications and Information Systems Security Committee) to provide "the minimum course content for the training of information systems security professionals in the disciplines of telecommunications security and automated information systems security" ([22]). By including this practical security model into our survey framework we could deepen our understanding of how academic research on information security is aligning with industry's interest.

In sum, our survey framework comprises four key research characteristics (socio-organizational paradigm, research method, reference discipline and level of study) as well as the NSTISS security model (see figure below).



JOURNAL SELECTION AND PAPER CLASSIFICATION

Traditionally, meta-analysis and literature survey studies in MIS area have focused on the "main stream" IS journals (e.g., [6][10]). In particular, the top IS journals are always included in such researches. To be more inclusive of a wider scope of information security research, the current study identified eight main

stream IS journals and two exclusive security journals for review. The IS journals include *MIS Quarterly* (MISQ), *Information Systems Research* (ISR), *Journal of Management Information Systems* (JMIS), *European Journal of Information Systems* (EJIS), *Information Systems Journal* (ISJ), *Information and Management* (I&M), *International Journal of Electronic Commerce* (IJEC), and *Journal of the Association for Information Systems* (JAIS), whereas the two Information security journals are *ACM Transactions on Information and System Security* (ACM-ISS) and *Information Management and Computer Security* (IM&CS).

As to the period of our review we argue that works published from the new millennium until now would be most relevant. Because it takes at least two years to complete and publish a quality research, papers which were in print in 2000 addressed issues and analyzed data collected in or before 1998 – the beginning of the climax of the dotcom surge and the panic of the Y2K crisis, which was accompanied by heightened security awareness. A review period starting from 2000 would suffice to cover a drastic IT market cycle from its peak to trough and the initial rise of the importance of information security. Yet, due to the availability of papers in several online databases at the time of this research, we had to restrict our review period to the eight years from 2000 to 2007.

RESULTS OF LITERATURE REVIEW AND CLASSIFICATION

A total of 240 papers from ten selected journals were reviewed and classified by three Ph.D.-level IS researchers for this study. Necessary reconciliations were performed whenever disagreement in classification occurred. Detail results from investigating different publication outlets: all the surveyed outlets, the three top-tiered IS outlets, the IS "main stream" outlets, and the two exclusive security outlets have been complied into a set of 23 tables. However, due to space limitation, we could not present them here. Instead, we reference and interpret significant and aggregate statistics in our review results in the discussion section next. (All tables are available upon request from the authors.)

DISCUSSION AND CONCLUSION

When excluding the two security journals, the remaining 8 IS outlets published only 27 articles in eight years. On the volume side, given the paramount importance of the subject area, the IS academia has been seriously falling behind its fair share of intellectual contributions. Although information security research had not attracted much interest on the IS side before the advent of e-commerce, one would logically expect it to gain traction in the dotcom era and the recently emerged digital economy. But according to our survey results, this expectation did not materialize, at least in the review period of eight years. There might be many factors leading to this paucity of intellectual works, but a plausible one has been revealed in our study – the traditional dominance of technology in the security field. Below, the findings of our work are organized and interpreted along the dimensions of our framework.

Socio-organizational Paradigms

Before the recent recognition of humans being the weakest link in any information security system, academicians and practitioners all looked to technology for answers to security problems. This technological bias has been indentified and explained in previous literature surveys and meta-analyses (e.g. [6][10][24]). The same trend also existed in our study in that the majority of information security publications in the IS journals have taken a functionalist approach that is technical in nature. And not surprisingly, almost all papers in the security-focused outlets are highly technical. As technical security issues tend to be specific and often require computer science or engineering solutions, the traditional discipline of MIS staffed mainly by behavioral researchers has a difficult time to attend to them.

However, technical and analytical researches only occupy one quadrant of Dhillon and Backhouse's framework. What happened to the remaining three quadrants? What could explain the near non-existence of security articles under these paradigms? One possible explanation would be methodological constraints facing traditional IS researchers. In their paper titled "Why there aren't more information security research studies?" Kotuli and Clark [17] attributed their failed data collection scheme to companies' reluctance to providing security data. They argued that this is an intrinsic security problem specific to information security research because giving out security data to external researchers is deemed an insecure or undesirable practice on the part of organizations. Should this fallacy persist, it would be next to impossible to perform any empirical studies on information security based on large samples. And even if a few institutions can be convinced to lend themselves to in-depth case studies, it would take enormous effort to gain full support and trust from them so that robust qualitative studies can be conducted (see, e.g. [32]). This conjecture helps to explain the almost empty quadrant that houses the interpretive paradigm.

By the same token we offered above, we can also partially explain why there has not been any paper falling under the radical humanism paradigm. However, the anti-technology and anti-organization views characterizing this paradigm tend to contradict with the core concept of company, thereby also inhibiting IS researchers' interest.

The most puzzling finding of our survey is the empty quadrant of radical structuralist paradigm. As information security heavily involves corporate governance and risk management on the human side, conflicts of various natures between organizational units and employees will be unavoidable. So far, in the IS literature, only specific topics pertaining to studying internal conflicts such as employee privacy, workplace monitoring, and ethics have appeared in publications (see, e.g., [8][11][14]), and they in general are not directly associated with information security. It is our view that innovative researches employing analytical or empirical tools are desperately needed to generate new theories of or insights into the human factors that critically impact the success of information security.

Research Methods

Many information security issues such as access control, key management, digital signature, security protocols and security systems development are technical in nature. Not surprisingly, researchers heavily use mathematical analysis to develop algorithms, conduct experiments to validate the algorithms, and implement the algorithms into security systems. These technical research occupy two third of the surveyed articles. What are the research methods used by the remaining one third of the articles? About 26% of the reviewed articles use non-technical research methods such as conceptual analysis, speculation/commentary and literature review research. These articles provide conceptual works,

literature reviews, and practical advices and guidelines, but are marginally significant to adding new knowledge to the field. This observation also implies that information security research is still in its embryonic state.

A good sign in our work is that we found some survey-based empirical studies. Our findings suggest that with proper precaution in designs, survey-based empirical study in the information security field still could be done. Some useful suggestions include designing less intrusive questionnaires, using social networks, using secondary data , and carrying out necessary follow-ups (see e.g., [27]).

One surprising finding of our survey is the near-empty research category, instrument development. Developing novel instrument or significantly improving existing instrument could have great impacts on fundamental aspects of a field. This is especially true for the new discipline of information security because many crucial constructs such as effectiveness of security programs and return on security investment still desperately need measurement tools. At a general level, research focusing on proof-of-concept development for an entirely novel instrument could significantly advance a field. As a classic example, technology acceptance model (TAM) serves a broad research need in the information systems community and intensive research has been done after the TAM instruments were developed (see, e.g. [5][9][18]). In sum, our findings indicate that we seriously lack novel instruments and constructs to serve our needs in information security research.

Reference Disciplines

While the surveyed articles cover all reference discipline categories, three particular disciplines have been intensively referenced: computer science, mathematics, and system implementation/evaluation. This finding provides two important implications. First and the obvious one, information security literature heavily focuses on technological solutions for security issues. Second and the more encouraging one, a sign of diversity in reference disciplines is appearing. This sign of diversity indicates that information security research is undertaking a migration effort to borrow models, theories and instruments from many established fields. And we believe that the initial use of existing models, theories and instruments from other fields is inevitable when a field is establishing. However, we are deeply concerned with, though not surprised by, the extreme shortage of articles referencing the information systems discipline. As it stands now, the IS academia has been seriously falling behind its fair share of intellectual contributions that are indispensible to forming a robust basis for information security research.

Level of Study

From the viewpoint of level of study, information security research is clearly focused on technological issues. The extreme example is the ACM Transactions on Information and System Security (ACM-ISS) in which all published articles are positioned in the technical level. This technical orientation is consistent with findings in the previous dimensions. However, while we cannot deny the technical nature of security research, neither can we deny the danger and importance of humans to any information security system.

Although there also exist a few articles (16.8%) focusing on human factors, the majority of them (73%) focus on the organizational level. This could be the extension of the traditional bias on organizational level by the main IS journals ([33]). But unfortunately, this tradition does not serve the field of study well; without better understanding of the impacts of information security at all levels we could hardly reach desirable goals of studying information security ([30][37]).

We believe that there are several possible explanations for the shortage of security research concerning human and social factors. One possible explanation is that the traditional empirical/grounded theory

approach for studying IS behaviors might not be suitable for studying information security behaviors. Another explanation is that human behaviors and social factors are hard to capture and measure. For example, if we consider information security behaviors as avoidance behaviors ([19]), such behaviors involve at least three linked processes: from threat appraisal to coping appraisal and then to actual coping behaviors. Each process is dynamic, therefore hard to capture. Our last explanation is that we have very limited access to data on the attack side. If we consider information security as a defense and attack game, the academia still has no clear idea about the attackers' behaviors.

NSTISSC Dimensions

The findings in the NSTISSC security model indicate that academic research in information security has been misaligning with industry focus: very few researches were found in the information states dimension. Since the dimensions in the NSTISSC model are not independent of each other, and together, they define all the essential issues of information security, the absence of research in the information states dimension tends to flatten the model, thereby reducing the specificity of research topics. While this shortcoming by itself is not a fatal weakness, it could lead to missing opportunities in addressing appropriate issues that are of concern to the industry. For example in the background of the intersection of education and integrity, there are three distinct areas of concerns: storage, processing, and transmission, each requiring different attention. If we only broad-brush the topic of how to educate employees on maintaining the integrity of information, the subtle needs of different user groups that are involved in various state of company information would be ignored. And such research will not be of great value to the organization, because the recommended security education will not be pertinent to all the user groups.

Our work here only takes a high level look at the current status of information security literature. Many of the reasons we offered to explain the observed trends are plausible, but they still need further empirical validation. With this paper, we have just answered the question of what have been done with the academic research. Our findings do reveal a serious vacuum of intellectual works spanning all dimensions of the research field, except the technical domain. Since there is no shortage of computer scientists, mathematicians, statisticians and the like to create more knowledge on the technical side (functionalism), future IS researches should be targeting the other three paradigms of the socio-organizational dimension. Furthermore, future research also can explore new theories and methodologies focusing on social and human factors of information security. And as a final note, we urge the academia to pay close attention to the needs of the industry and address information security issues more specifically.

REFERENCES

A set of references are available from the authors upon request.