INFOSEC in a Basket, 2004-2013

Completed Research Paper

Mark-David McLaughlin
Bentley University/Cisco Systems
mclaugh_mark@bentley.edu

Janis Gogan
Bentley University
jgogan@bentley.edu

Abstract

Topical and methodological diversity are key strengths of Information Systems (IS) research. To the extent that an IS sub-field such as IS security (hereafter, InfoSec) employs varied methods to examine various topics, the sub-field can claim strength through diversity. We conducted a systematic review of ten years of 85 InfoSec studies published in the IS Senior Scholars Basket of eight journals. We find that InfoSec researchers have employed a variety of quantitative and qualitative methods to study a variety of topics; that some journals published papers based on some methods and InfoSec topics more than others; that many methods are underutilized as applied to some topics; and that topics addressing the organizational/managerial and inter-organizational levels of analysis are understudied. We conclude that InfoSec research is maturing, yet abundant opportunities still exist to conduct further research aimed at building stronger theories and offering stronger implications for InfoSec practice.

Keywords

information security, literature review, future research, computer abuse

Introduction

IS researchers publish in many outlets; however, the eight journals comprising the Association for Information Systems (AIS) Senior Scholars Basket (ECIS, JAIS, JIT, JMIS, JSIS, ISJ, ISR, MISQ) are regarded as the most influential IS publications. We assume that IS scholars read these journals on a regular basis, along with relevant specialty journals (such as *Computers & Security*, *Decision Support Systems*, or *International Journal of Electronic Commerce*). In addition, IS scholars follow citation trails back to seminal works published in other outlets, skim papers presented at IS conferences like AMCIS, ECIS, PACIS, and ICIS, and stay abreast of relevant work in reference disciplines such as computer science, management or sociology. Given that keeping up with papers in the Senior Scholars' Basket is a shared norm, it follows that IS scholars' awareness of published studies outside their own specializations is likely to be heavily influenced by papers in the Basket. One cannot claim that the Basket contains all the important work produced in any IS sub-field, but it seems reasonable to claim that many scholars become aware of major findings in sub-fields outside their specialty areas by perusing papers in the Basket.

Some prior information systems reviews have aimed to identify a set of core topics and research questions that define the IS field (Benbasat and Zmud 2003); other reviews celebrate topical and methodological diversity as a key strength of the field (Bernroider et al. 2013; Venkatesh et al. 2013). If diversity is valued and expected, then it is important to consider whether each separate IS sub-field is diverse in terms of sub-topics, methods, theories, and other aspects. We thus propose that to the extent that information systems security (hereafter, InfoSec) researchers employ varied methods to examine various topics, they can claim to support methodological diversity in this sub-field. Methodological diversity is one important indicator of the maturity of a field or sub-field (Bernroider et al. 2013).

This review focuses on the IS sub-field of InfoSec—a research topic of great importance in light of the many high-profile security breaches in recent years. For instance, personally identifiable information of over 70M Target customers was illegally accessed by an attacker in December 2013; on-line account information for 152M Adobe Systems customers was published by hackers in fall 2013; confidential United States government files were accessed and released by Edward Snowden in summer 2013; and countless other

attacks violating the confidentiality, integrity, and availability of information systems serve as constant reminders of the importance of InfoSec technologies and management practices.

We reviewed 85 InfoSec studies published in the eight Basket journals over a ten year period – 2004 through 2013 -- and also briefly reviewed 20 studies in which InfoSec constructs played a secondary role as an independent, mediating, moderating or control variable. Our review aimed to answer the following research questions regarding InfoSec papers published in the eight Basket journals from 2004-2013:

- RQ1. What InfoSec topics were addressed?
- RQ2. What methods (quantitative, qualitative, or mixed methods) did the studies use?
- RQ3. To what extent do Basket journals vary in terms of InfoSec topics and methods?

The paper is organized as follows. We discuss prior reviews of InfoSec research and explain why our systematic review of the past ten years' InfoSec studies published in the Basket is needed. We describe our literature review method and present our findings. After answering the three research questions noted above, we discuss the implications of our findings for InfoSec research and for other IS sub-fields. We acknowledge limitations of the current study and in the final section we offer suggestions for further research addressing understudied InfoSec topics and making use of underutilized empirical methods.

Prior InfoSec Literature Reviews

Since our review was restricted to the IS Scholars Basket, our first step was to identify prior InfoSec literature reviews published in Basket journals since 2000. We identified four reviews; no review restricted its scope to the eight Scholars Basket journals. Because no review specified a detailed method, readers cannot readily ascertain the intended boundaries of the reviews or whether they were complete in their coverage. Two reviews (Dhillon and Backhouse 2001; Siponen 2005) concluded with calls for interpretive field studies examining InfoSec issues. Dhillon and Backhouse (2001) focused on methodologies employed by InfoSec studies, classified according to a framework proposed by Burrell and Morgan (1979) which pitted a "subjective-objective" axis versus a "regulation-radical change" axis. This yields four research approaches: functionalist ("concerned with the regulation and control of all organizational affairs"), interpretive (considering "social reality as a network of assumptions and inter-subjectively shared meanings"), radical humanist (exploring "structural conflicts and modes of domination") and radical structuralist (focused on "transformation of structures"). Based on papers written mostly in the 1990s, this review reported that InfoSec research had thus far emphasized functionalist studies, followed by interpretive studies. Two functionalist and three interpretive InfoSec studies were in the IS Senior Scholars Basket of journals, and no studies in the Basket followed the radical humanist or radical structuralist forms. The studies identified in the Basket publications were:

- Functional:
    1. a structured risk analysis paper in *JIT* by Birch and McEvoy (1992).
    2. a paper reporting on IS executives' views about InfoSec threats, published in *MISQ* by Loch, Carr, and Warkentin (1992).
- Interpretive:
    1. Baskerville (1991) in *EJIS*, which found that risk assessment tools were best used as interpretive devices to stimulate conversation and raise awareness.
    2. Backhouse and Dhillon (1996), in *EJIS*, considered InfoSec management through a semiotics lens.
    3. A mixed-methods *MISQ* paper by Straub and Welke (1998) combined interpretive interviews and action research to explore managers' InfoSec awareness and attitudes.

Dhillon and Backhouse (2001) concluded that prior InfoSec studies (as far back as 1976) were overly focused on "formalized rule structures in designing security." Meanwhile, the broader IS community had come to realize "that computer-based systems dynamically interact with the formal and informal environments in which they are used. Hence an understanding of human interactions, patterns of behavior

and meanings associated with the actions of individuals becomes important." They concluded that "risk analysis, rooted in the functionalist paradigm, is extremely useful for evaluating security but it cannot form the basis of an entire security strategy."

> "Likewise traditional evaluation methods can be useful in assessing the extent of security, but a corporate strategy to prevent the occurrence of negative events cannot be based on the highly structured security evaluation criteria. ... A socio-organizational perspective is the way forward if security of information systems is to be achieved" (p. 147).

Siponen (2005) asserted that there was insufficient evidence from the extant body of InfoSec research to verify the efficacy of traditional information systems security methods such as checklists, standards, maturity criteria, risk management and formal methods. Siponen concluded that "there is a need for rigorous qualitative and quantitative empirical studies, which explore the usability and relevance of the traditional ISS methods in practice." (p. 313). We note that just two IS Scholars Basket papers focusing on InfoSec were cited in Siponen's review paper: Baskerville (1991) and Dhillon and Backhouse (2001).

Two more recent reviews focused on an InfoSec sub-topic: employee InfoSec attitudes and behavior. A review by D'Arcy and Herath (2011), in *EJIS*, offered several explanations for why, despite many studies, deterrence theory had received mixed support. Eight papers in this review had appeared in three IS Scholars Basket journals: in *EJIS*: Myyry et al. (2009); Herath and Rao (2009); Warkentin and Willison (2009); in *ISR*: D'arcy et al. (2009); Straub (1990); in *MISQ*: Bulgurcu et al. (2010); Harrington (1996); Siponen and Vance (2010). Eleven papers on this subject, published in journals outside the Scholars Basket were also reviewed: *Communications of the ACM* (two papers), *Computers & Security*, *Decision Support Systems* (two papers), *IEEE Security & Privacy*, *Information and Management*, *International Journal of Information Management*, *Journal of the American Society for Information Science and Technology*, *Journal of Business Ethics*, and *Journal of Computer Information Systems*. D'Arcy and Herath concluded that five potential moderating variables needed further investigation; that methodological consistency would be helpful; and that researchers relying on deterrence theory needed to consider employee perceptions of beneficial aspects of security violations (e.g., convenience or efficiency).

A recent paper by Willison and Warkentin (2013) also focused on individual behavior in light of deterrence theory. This review included 16 papers from four IS Scholars Basket journals: EJIS (7 papers), ISR (2 papers) JMIS, and MISQ (6 papers). Nine other IS papers addressing employee information security attitudes, intentions and behavior were reviewed: 3 in *Communications of the ACM*, and one each in *Computers & Security*, *Computers in Human Behavior*, *Ethics and Information Technology*, *Information and Management*, *Information Management and Computer Security*, and *Journal of the American Society for Information Science and Technology*. Also drawing heavily on studies in management and social psychology journals, this review concluded that "we need to consider the thought processes of the potential offender and how these are influenced by the organizational context prior to deterrence" (p. 14). Willison and Warkentin argued that future studies should focus on intentional or malicious employee computer abuse using theories of organizational justice and neutralization.

We note that prior literature reviews published in the Basket did not include review method sections that verify review completeness or scope. To summarize their findings: Dhillon and Backhouse (2001) reported that positivist research taking a functional perspective predominated; that early interpretive studies showed promise and should continue to be pursued; and that no InfoSec studies had clearly pursued the radical humanist or radical structuralist approaches. (D'Arcy and Herath 2011; Willison and Warkentin 2013) each limited their scope to employee InfoSec non-compliance and gave roughly equal weight to InfoSec papers published in IS journals outside the Basket as those in the Basket. Thus far, no published InfoSec review has claimed thorough coverage of the IS Senior Scholars Basket of eight journals. We conclude that while general deterrence theory and its offshoots have been reviewed at a reasonable level of completeness, other aspects of information security have not yet been thoroughly reviewed. There is a need for a thorough and recent InfoSec review. We partially answer this need here, with a review of 85 InfoSec papers published between 2004 and 2013 in the Basket.

Review Method

It is important to use an explicit process to conduct a literature review (Webster and Watson 2002), but not necessary to claim that *all* extant studies have been found (Levy and Ellis 2006). Our objective was to fully capture studies across the full domain of information security/computer security research published in the Basket in the past ten years (between 2004 and 2013). We further limited our scope to the research topics and methods used in the 85 InfoSec papers (with brief comments on 20 papers in which InfoSec attitudes, behavior, or outcomes were not conceptualized as a dependent variable. These studies had a different purpose, such as exploring determinants of eCommerce adoption or opportunities (Khalifa and Liu 2007), user trust in website privacy policies (Wakefield 2013), and risks associated with supply chain technologies like RFID (Kapoor et al. 2009)).

Our review identified papers via both manual and automated searches. We read the abstracts of every paper published in the Scholars Basket since 2004, identifying 95 papers to review. We then conducted an automated search for the word fragments "secur", "attack", "hack", "vulnerabilit", "insider", "threat", "protection", and "abuse"—resulting in 121 additional papers. We read the abstracts of these papers to ensure that the manual search had found all InfoSec papers. This led us to decide that 111 papers reported on studies of "social security", "financial security exchanges", "insider trading", or other aspects that were obviously not InfoSec related; these papers were eliminated. The literature reviews that have already been discussed in our introduction were not included in the count, nor were editorials or commentaries. The two authors separately assessed the remaining 105 papers and recorded their findings for subsequent reconciliation and discussion. A candidate paper was not eliminated from the review database unless both authors marked it independently for deletion or came to a consensus when one author thought it should be removed. In this way false positives were identified and removed. For example, a paper by August and Tunca (ISR, 2013) included the word "security" in a footnote explaining support services but did not otherwise directly address an InfoSec topic. Dinev et al. (JSIS, 2008) used the word "security" to mean "safety" and in the context of "Homeland Security", but did not otherwise directly address InfoSec topics.

20 candidate papers mentioned InfoSec topics in the context of other topics such as online trust or privacy concerns. Again both authors independently judged these and went through a process to reach consensus that was similar to that for removing papers. In reaching our decisions about these papers, we applied the criterion that when an InfoSec construct is one of many independent variables or treated as a mediator, moderator, or control variable, we classified the paper as treating InfoSec as a "secondary" topic. We further checked the author-supplied keywords for these papers. Of the 20 papers classified in this category, three (Kim, JMIS 2008 ; Pavlou et al. MISQ 2007 and Wakefield JSIS 2013) did include "security" in the list of keywords. After extensive discussion of these three, we reached consensus that InfoSec was a secondary topic in these papers. We provide citations to the 20 papers classified as "InfoSec is Secondary" in Table 1, so readers can judge whether we classified them appropriately.

Author/s	Journal and Citation Details	"secur" in keyword list?
Kapoor, et al.	EJIS 18(6): 526-533. Dec 2009	No
Khalifa and Liu	EJIS 16(6): 780-792. Dec 2007	No
Yao and Murphy	EJIS 16(2): 106-120. Apr 2007	No
Zhu et al.	EJIS 15(6): 601-616. Dec 2006	No
Carter and Belanger	ISJ 15(1): 5-25. Jan 2005.	No
Lee and Rao	ISJ 22(4): 313-341. Jul 2012	No
Ramesh et al.	ISJ 20(5): 449-480. Sep 2010.	No
Tsai et al.	ISR 22(2), June 2011	No
Xu et al.,	ISR 23(4), Dec 2012	No
Sutton et al.	JAIS 9(3-4): 151-174. 2008	No
Kim and Ahn	JIT 22(2): 119-132. Jun 2007	No
Arora and Forman	JMIS 24(2): 73-102. Fall 2007	No
Benlian et al.	JMIS 28(3): 85-126. Win 2011.	No
Fang et al.	JMIS 22(3): 123-157. Win 2005.	Perceived Security
Kim	JMIS 24(4): 13-45. Spr 2008	No
Wakefield	JSIS 22(2): 157-174, June 2013	Internet Security
Hahn et al.	MISQ 33(3): 597-616. Sep 2009	No
Iivari and Huisman	MISQ 31(1): 35-58. Mar 2007	No
Li et al.	MISQ 36(1): 179-203. Mar 2012	No
Pavlou, et al.	MISQ 31(1):105-136,Mar 2007	Information security
N=20		

Table 1 InfoSec is a secondary topic in these Scholars Basket papers

The 85 remaining papers (see Appendix) focused exclusively on InfoSec issues and/or treated InfoSec constructs as dependent variables. Each paper was classified according to its primary research topic, using the following categories:

- *Individual*: Papers primarily focused on individual InfoSec attitudes, intentions, or behavior. We further subdivided this category into "Inside" (similar to Willison (2006) and D'Arcy, Hovav, and Galletta (2009) who define an "insider" as an employee, contractor or other party who has authorized access to an organization's systems and data), and "User" (this category represents all other studies focused on individual attitudes, intentions or behavior, including consumers shopping online or "users" not further defined).
- *Organization*: Papers primarily focused on managerial issues such as InfoSec policies or tactics and security incident response.
- *Inter-organizational*: Papers addressing topics such as industry-wide security standards setting processes, inter-organizational coordination/collaboration during incident response, security issues related to inter-organizational information sharing.
- *Economic*: Papers that self-identified as being in the information economics stream of research, or that focused on quantitative data more heavily than on managerial behavior when addressing questions such as optimal InfoSec investment levels for a firm or market reactions to events such as security breaches or vulnerability disclosures.
- *Technical*: Papers that examined the design of or factors related to the effectiveness of security tools such as firewalls and intrusion detection systems, or which explored technical issues related to the incorporation of security features in other software applications.
- *Other*: Papers addressing InfoSec issues at a societal, philosophic, ontological or other perspective that could not otherwise be classified into the prior categories.

The two authors independently coded the papers per the above criteria. Some studies focused on multiple levels of analysis; however, it was usually possible to identify a primary focus according to the criteria identified above, particularly by locating the dependent variables in the study. Many *Introduction* sections discussed why InfoSec is an important topic for organizations and their leaders, but we did not use the "so what?" research justification as a guide to the focal topic. Similarly, the *Conclusions* section might also tie a study to broader security concerns, but we agreed that this was also not a reliable indicator of a paper's primary focus. With those considerations in mind, our independent reviews reached identical conclusions for 75 of the 85 papers. We discussed the remaining 10 papers until we reached agreement. For the benefit of the reader, the Appendix flags those 10 topics on which we did not initially agree (with ★).

Next, we classified the papers according to the study methods employed, using a coding scheme adapted from Galliers (1991), as follows:

- Subjective Argument: Per Galliers (1991), these papers offer propositions based on a critical literature review, but stop short of providing either a mathematical model or empirical data.
- Design Science: studies reporting on the design of a prototype InfoSec system.
- Action Research: studies in which the researcher was a participant.
- Case: critical, ethnographic, interpretive or positivist case study (single case, embedded cases, or multiple cases).
- Qual: other qualitative methods, such as field interviews not associated with case studies, discourse analysis, critical incident technique, or textual classification.
- Survey: attitude surveys administered to employees, IS professionals, managers, or computer users in general.
- Model: theorem proofs, simulations using synthetic data, models using synthetic or real data.
- Experiment: lab, field, or natural experiment.
- Quant: other quantitative method (e.g. event studies, analysis of field data, etc.).
- Mixed Methods: While some authors argue that a study should not be considered mixed methods unless it combines both quantitative and qualitative approaches, we took a more liberal view and included any combination of the above-listed research methods in a single study.

Findings

Table 2 summarizes the methods used in 85 InfoSec studies identified in the eight Basket journals between 2004 and 2013. We include in our findings papers classified as Subjective Argument, which is a non-empirical technique. Our discussion, however, emphasizes the empirical methods. Our findings reveal that the top three empirical methods were mixed methods (21 papers), quantitative models (19 papers) and attitude surveys (15 papers). Some journals have emphasized some methods over others, as shown in Table 2. For example, *ISR* and *JMIS* heavily feature papers based on quantitative models, and ISR published the greatest number of mixed methods InfoSec papers.

Topic	Total	Design Science	Survey	Model	Experiment	Other Quantitative	Action Research	Case	Other Qualitative	Mixed Methods	Subjective Argument
EJIS	10	1	4		1			2		1	1
ISJ	5		2					1	1	1	
ISR	16		1	6		1				8	
JAIS	8		2		1	1				2	2
JIT	3					1	1			1	
JMIS	19		2	9	2	4				2	
JSIS	7		1	1				3		1	1
MISQ	17		3	3	1	2		2		5	1
Total	85	1	15	19	5	9	1	8	1	21	5

Table 2. InfoSec in IS Scholars Basket Journals, 2004-2013: Methods Employed

Likewise, some topics have been examined more extensively with particular methods. For example, InfoSec economics were most commonly examined with quantitative models, and technical papers tended to heavily rely on mixed methods. Our findings also show that some methods were heavily utilized to study particular InfoSec research topics. For instance, experiments were exclusively used in studies that focused on individuals. While specific topics lend themselves more readily to particular research methodologies, alternative methodologies do exist and senior scholars have argued they are needed to provide a deeper understanding of IS issues (Galliers and Markus 2007). Table 3 summarizes the findings regarding methodologies used to study various InfoSec topics.

Topic	Total	Design Science	Survey	Model	Experiment	Other Quantitative	Action Research	Case	Other Qualitative	Mixed Methods	Subjective Argument
InfoSec Economics	22			13		7				2	
Individual: Insider	16		7		1	1		3		2	2
Individual: User	13		6		4					2	1
Technical	12	1		2						9	
Organizational	16		2	2		1	1	4	1	4	1
Inter-organizatinal	5			2				1		2	
other	1										1
Total	85	1	15	19	5	9	1	8	1	21	5

Table 3. InfoSec Topics in the Basket, 2004-2013 by Methods Employed

Tables 2 and 3 further imply that design science, action research and qualitative methods other than case studies (such as studies based on critical incident technique or discourse analysis) are under-represented in the last ten years' worth of InfoSec papers in the Basket. These methods are represented to some extent in the 21 mixed methods papers, as shown in Table 4.

Table 4 reveals that design science is a featured method in 9 of 21 mixed methods papers; that quantitative models are included in 8 of these papers and surveys in 9 papers. Of the qualitative techniques, we find in the mixed methods papers 2 action research, 4 case studies and 9 studies using other qualitative methods. Considered this way, action research is the least utilized empirical strategy, and models and surveys are dominant methods overall when mixed-methods studies are taken into account (yielding 27 studies using a quantitative modeling method and 24 using attitude surveys).

Author/s	Journal and Citation Details	Topic	Methods Used							
D'aubeterre,	EJIS 17(5): 2008.	Technical	Design		Model					
Wong et al.	ISJ 22(1): 2012	Technical	Design		Model	Experiment				
Garfinkel and Gopal	ISR 18(1): 2007	Technical	Design		Model					
Hsu et al.	ISR 23(3): 2012	Organization		Survey						Qual
Li and Sarkar	ISR 17(3): 2006	Technical	Design		Model					
Li and Sarkar	ISR 22(4): 2011	Technical	Design		Model					
Melville and McQuaid	ISR 23(2): 2012	Technical	Design		Model					
Ransbotham and Mitra	ISR 20(1): 2009	Organization					Quant			Qual
Wang et al.	ISR 19(1): 2008	Economic			Model					Qual
Wang et al.	ISR 24(2): 2013	Economic				Experiment				Qual
D'Aubeterre et al.	JAIS 9(3): 2008	Technical	Design						Case	
Siponen et al.	JAIS 7(11): 2006	Technical	Design					Action		
Tow et al.	JIT 25(2): 2010	Individual		Survey						Qual
Majchrzak and Jarvenpaa	JMIS 27(2): 2010	Inter-Org		Survey						Qual
Sun et al.	JMIS 22(4): 2006	Organization		Survey					Case	
Goel and Chengalur-Smith	JSIS 19(4): 2010	Individual		Survey						Qual
Abbasi et al.	MISQ 34(3): 2010	Technical	Design		Model	Experiment				
Posey et al.	MISQ 37(4): 2013	Individual		Survey						Qual
Puhakainen and Siponen	MISQ 34(4): 2010	Individual		Survey				Action		
Smith et al.	MISQ 34(3): 2010	Inter-Org		Survey					Case	
Spears and Barki	MISQ 34(3): 2010	Organization		Survey					Case	Qual
Total			9	9	8	3	1	2	4	9

Table 4. InfoSec in the IS Scholars Basket, 2004-2013: The Mixed-Methods Papers

Finally, we consider the topics that InfoSec researchers have addressed in the eight Basket journals for the past ten years. Table 5 reveals that research continues to be heavily weighted toward understanding user behavior, with 29 studies (16 + 13) examining factors that influence user attitude, intention or behavior. Papers from the InfoSec economics stream are also heavily represented (22), and only five papers have addressed inter-organizational InfoSec issues.

Journal	Total	InfoSec Economics	Individual: Insider	Individual: User	Technical	Organizational	Inter-organizational	other
EJIS	10		6	1	2	1		
ISJ	5			2	1	2		
ISR	16	7	1		5	2	1	
JAIS	8	1	1	3	2			1
JIT	3	1		1		1		
JMIS	19	8	2	1	1	5	2	
JSIS	7	1	2	2		2		
MISQ	17	4	4	3	1	3	2	
Total	85	22	16	13	12	16	5	1

Table 5. InfoSec in the IS Scholars Basket, 204-2013, Topics Addressed

Discussion: Contributions, Limitations, Conclusions

This literature review of ten years' worth of InfoSec studies published in the IS Senior Scholars Basket of journals reveals a vibrant and diverse set of studies. The findings reveal evidence that InfoSec researchers have answered Siponen's (2005) call for more empirical studies using qualitative or quantitative methods. However, the findings also offer initial evidence that methods used in InfoSec studies are not uniformly distributed among either the topics or journals. Assuming that journals in the Basket do not have policies explicitly favoring particular methods or topics, there are many opportunities to contribute to the InfoSec literature and to strengthen applicable theories by making use of underutilized quantitative methods such as lab or field experiments and underutilized qualitative methods such as action research, critical incident technique, discourse analysis and other approaches.

Our findings on methods employed in InfoSec studies during the past decade suggest that the field is indeed becoming somewhat more diverse in terms of methods employed; this answers calls for methodological diversity by Bernroider et al. (2013) and Venkatesh et al. (2013). However, researchers examining some specific topics seem to strongly favor specific methods. For example, studies addressing user attitudes, intentions or behavior tend to rely on attitude surveys. This is a strong sub-stream addressing Dhillon and Backhouses's (2001) call for a focus on individual user intentions and behaviors. Another strong sub-stream addresses InfoSec challenges through an economic lens. Still, our findings lead us to ask: why does the InfoSec field continue to rely heavily on a few quantitative methods (such as economic modeling and attitudinal surveys)? This finding is cause for some concern because studies in the econometric and survey-research traditions tend to rely on proxy variables rather than measuring the variables of greatest interest. For example, many studies that take the individual as the unit of analysis ultimately aim to understand user behavior, yet rely heavily on measures of attitudes and behavioral intentions. In other words, some heavily used dependent variable measures are one or more steps removed from actual user behavior "in the wild." To be clear: the survey studies in the Individual InfoSec streams are well designed, but we are arguing for additional complementary studies using other methods—such as observation, ethnography, diaries, screen capture and other ways to measure actual behavior.

Some journals—particularly *ISR* and *MISQ*—attracted and published mixed-methods papers. Of the 21 papers classified as mixed-methods, 12 papers paired a quantitative method with a qualitative method (action research, case study or other qualitative). However, the findings also give rise to some concerns. Considering some journals, it appears that the way to get qualitative research published is to include it in a mixed-methods study. We observe that *ISR* published no papers based solely on a qualitative method, and *MISQ* included just two qualitative papers (cases) in the 17 InfoSec papers they published 2014-2013. While we applaud mixed methods studies as offering a helpful way of triangulating and increasing readers' confidence in findings, we hope that journals are not enacting policies that view qualitative research as a weak step-sister, not sufficiently strong to stand on its own merits.

This paper has contributed to the body of work on information security by using a systematic literature review method which explicitly aimed to discover all InfoSec papers in the IS Senior Scholar's Basket for a defined period (2004-2013), and with a clear focus on delineating the InfoSec sub-topics examined and the methods used to study them. The benefit of our approach is that others can readily verify whether our findings are valid. One limitation is that this review does not include papers published before 2004 or after 2013. Also, we have not told a full story about the *content* of the InfoSec literature in the Basket (answering questions such as: What has been learned about InfoSec thus far? What theories have been tested or proposed? What questions about InfoSec remain unanswered?) There is need for such a review, because recent reviews (discussed in the Introduction) focused primarily on studies directed at the individual unit of analysis and using or extending general deterrence theory.

While our focus on papers published in the Basket is justified, we readily acknowledge that InfoSec researchers participate in non-AIS conferences and publish important work in other journals. Clearly, a literature review focused outside the Basket is also warranted, and comparison of a sample of Non-Basket studies published in the same time period with the current sample might reveal some interesting similarities and differences and shed further light on the development of the InfoSec research stream. Other avenues for further work include a study which would closely examine authorship data to identify clusters of collaborators and co-citation patterns to shed light on how InfoSec findings propagate and why some InfoSec studies have not (as yet) spawned further work.

To the extent that IS study findings translate into improved system and information security practices and tools, IS researchers can claim to have a valuable impact on practice. InfoSec economic studies have called attention to contextual influences surrounding security concerns, impacts of breaches and other InfoSec events, and optimal investments in security resources. Studies aimed at the individual level have shed light on factors that shape users' attitudes toward InfoSec practices and policies. Studies directed at the organizational level have begun to provide managerial guidance on effective policies, tactics, and security incident response. Yet, cyber-attacks and other security breaches are increasing in size, frequency, impact, and cost. Thus, more research aiming at both the organizational level and at inter-organizational issues is sorely needed. Therefore, we echo Siponen's earlier call that "there is a need for rigorous qualitative and quantitative empirical studies, which explore the usability and relevance of ... ISS methods in practice"—with the added clarification that more studies need to aim to understand InfoSec management at the organizational and inter-organizational levels.

REFERENCES

Backhouse, J., and Dhillon, G. 1996. "Structures of Responsibility and Security of Information Systems," *European Journal of Information Systems* (5:1), Mar, pp. 2-9.

Baskerville, R. 1991. "Risk Analysis: An Interpretive Feasibility Tool in Justifying Information Systems Security," *European Journal of Information Systems* (1:2), pp. 121-130.

Benbasat, I., and Zmud, R.W. 2003. "The Identity Crisis within the Is Discipline: Defining and Communicating the Discipline's Core Properties," *MIS quarterly*), pp. 183-194.

Bernroider, E.W., Pilkington, A., and Cordoba, J.-R. 2013. "Research in Information Systems: A Study of Diversity and Inter-Disciplinary Discourse in the Ais Basket Journals between 1995 and 2011," *Journal of Information Technology* (28:1), pp. 74-89.

Birch, D.G., and McEvoy, N.A. 1992. "Risk Analysis for Information Systems," *Journal of Information Technology* (7:1), pp. 44-53.

Burrell, G.M., Gareth. 1979. *Sociological Paradigms and Organizational Analysis*. Farnham, Surrey, United Kingdom: Ashgate Publishing.

D'Arcy, J., and Herath, T. 2011. "A Review and Analysis of Deterrence Theory in the Is Security Literature: Making Sense of the Disparate Findings," *European Journal of Information Systems* (20:6), Nov, pp. 643-658.

D'Arcy, J., Hovav, A., and Galletta, D. 2009. "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach," *Information Systems Research* (20:1), Mar, pp. 79-98.

Dhillon, G., and Backhouse, J. 2001. "Current Directions in Is Security Research: Towards Socio-Organizational Perspectives," *Information Systems Journal* (11:2), pp. 127-153.

Galliers, R., and Markus, M.L. 2007. *Exploring Information Systems Research Approaches: Readings and Reflections*. Routledge.

Galliers, R.D. 1991. "Choosing Appropriate Information Systems Research Approaches: A Revised Taxonomy," in *Information Systems Research: Contemporary Approaches & Emergent Tradition*, H.-E. Nissen, H.K. Klein and R. Hirschheim (eds.). Amsterdam: North Holland, pp. 327-345.

Kapoor, G., Zhou, W., and Piramuthu, S. 2009. "Challenges Associated with Rfid Tag Implementations in Supply Chains," *European Journal of Information Systems* (18:6), Dec, pp. 526-533.

Khalifa, M., and Liu, V. 2007. "Online Consumer Retention: Contingent Effects of Online Shopping Habit and Online Shopping Experience," *European Journal of Information Systems* (16:6), Dec, pp. 780-792.

Levy, Y., and Ellis, T.J. 2006. "A Systems Approach to Conduct an Effective Literature Review in Support of Information Systems Research," *Informing Science* (9), pp. 181-212.

Loch, K.D., Carr, H.H., and Warkentin, M.E. 1992. "Threats to Information Systems: Today's Reality, Yesterday's Understanding," *Mis Quarterly* (16:2), Jun, pp. 173-186.

Siponen, M.T. 2005. "An Analysis of the Traditional Is Security Approaches: Implications for Research and Practice," *European Journal of Information Systems* (14:3), Sep, pp. 303-315.

Straub, D.W., and Welke, R.J. 1998. "Coping with Systems Risk: Security Planning Models for Management Decision Making," *Management Information Systems Quarterly* (22), pp. 441-470.

Venkatesh, V., Brown, S.A., and Bala, H. 2013. "Bridging the Qualitative-Quantitative Divide: Guidelines for Conducting Mixed Methods Research in Information Systems," *MIS Quarterly* (37:1), pp. 21-54.

Wakefield, R. 2013. "The Influence of User Affect in Online Information Disclosure," *Journal of Strategic Information Systems* (22:2), Jun, pp. 157-174.

Webster, J., and Watson, R.T. 2002. "Analyzing the Past to Prepare for the Future: Writing a Literature Review," *Mis Quarterly* (26:2), Jun, pp. XIII-XXIII.

Willison, R., and Backhouse, J. 2006. "Opportunities for Computer Crime: Considering Systems Risk from a Criminological Perspective," *European Journal of Information Systems* (15:4), Aug, pp. 403-414.

Willison, R., and Warkentin, M. 2013. "Beyond Deterrence: An Expanded View of Employee Computer Abuse," *MIS Quarterly* (37:1), pp. 1-20.

Notes:

1. *Papers which were the subject of this review are noted with partial citations in the Appendix; full citations available from the authors.*

APPENDIX

Items denoted with ★ are those papers on which authors initially disagreed regarding the topical focus.

Author/s	Partial Citation	Primary Topic	Method
Boss et al.	EJIS 18(2): 2009	Individual (inside)	Surv
D'aubeterre,	EJIS 17(5): 2008	Technical	mixed (DS, model)
Fernandez-Medina, et al.	EJIS 16(4): 2007	Technical	DS
Herath and Rao	EJIS 18(2): 2009	Individual (inside)	Surv
Hsu	EJIS 18(2): 2009	Individual (inside)	Case
Myyry et al.	EJIS 18(2): 2009	Individual (inside)	Surv
Njenga and Brown	EJIS 21(6): 2012	Organization	Case
Warkentin et al.	EJIS 20(3): 2011	Individual (inside)	Surv
Willison and Backhouse	EJIS 15(4): 2006	Individual (inside)	SA
Zhang et al.	EJIS 18(2): 2009	Individual (user)	Exp
Dhillon and Torkzadeh	ISJ 16(3): 2006	Organization	QL other
Dinev et al.	ISJ 19(4): 2009	Individual (user)	Surv
Herath et al.	ISJ 24(1): 2012	Individual (user)	Surv
Stahl et al.	ISJ 22(1): 2012	Organization	Case
Wong et al.	ISJ 22(1): 2012	Technical	Mixed (DS, Model, Exp)
Arora et al.	ISR 21(1): 2010	Economic	Quant
August and Tunca	ISR 19(1): 2008	Economic	Mod
Cavusoglu et al.	ISR 16(1): 2005	Economic	Mod
Cavusoglu et al.	ISR 20(2): 2009	Technical	Mod
D'Arcy et al.	ISR 20(1): 2009	Individual (inside)	Surv
Gal-Or and Ghose	ISR 16(2): 2005	Inter-org'l	Mod
Garfinkel and Gopal	ISR 18(1): 2007	Technical	Mixed (DS, model)
Hsu et al.	ISR 23(3): 2012	Organization	Mixed (Qual, Surv)
Lee et al.	ISR 24(2): 2013	Economic	Mod
Li and Sarkar	ISR 17(3): 2006	Technical	Mixed (DS, model)
Li and Sarkar	ISR 22(4): 2011	Technical	Mixed (DS, model)
Melville and McQuaid	ISR 23(2): 2012	Technical	Mixed (DS, model)
Mookerjee et al.	ISR 22(3): 2011	Economic ★	Mod
Ransbotham and Mitra	ISR 20(1): 2009	Organization	Mixed (Qual, Quant)
Wang et al.	ISR 19(1): 2008	Economic	Mixed (Qual, model)
Wang et al.	ISR 24(2): 2013	Economic	Mixed (Exp, Qual)
D'Aubeterre et al.	JAIS 9(3): 2008	Technical ★	Mixed (DS, QL case)
Dinev and Hu	JAIS 8(7): 2007.	Individual (user)	QT (survey)
Goldstein et al.	JAIS 12(9): 2011	Economic	QT (event data)
Karjalainen and Siponen	JAIS 12(8): 2011	Individual (inside) ★	SA
Keith et al.	JAIS 10(2): 2009	Individual (user)	Exp
Liang and Xue	JAIS 11(7): 2010	Individual (user)	QT (survey)
Siponen et al.	JAIS 7(11): 2006	Technical	Mixed (DS, action research)
Vuorinen and Tetri	JAIS 13(9): 2012	(other)	SA
Salmela	JIT 23(3): 2008	Organization ★	AR
Tow et al.	JIT 25(2): 2010	Individual (user)	Mixed (Qual, Surv)
Yayla and Hu	JIT 26(1): 2011	Economic	Quant

Author/s	Partial Citation	Primary Topic	Method
Cavusoglu et al.	JMIS 25(2): 2008	Economic	Mod
Chen et al.	JMIS 29(3): 2012	Individual (inside)	Exp
Cremonini and Nizovtsev	JMIS 26(3): 2009	Economic	Mod
Dey et al.	JMIS 29(2), 2012	Economic	Mod
Guo et al.	JMIS 28(2): 2011	Organization ★	Surv
Herath and Herath	JMIS 25(3): 2008	Economic	Quant
Hui et al	JMIS 29(3), 2013	Economic	Mod
Johnson	JMIS 25(2): 2008	Organization	Quant
Kumar et al.	JMIS 25(2): 2008	Organization	Mod
Kwon and Johnson	JMIS 30(2): 2013	Organization	Surv
Majchrzak and Jarvenpaa	JMIS 27(2): 2010	Inter-Org	Mixed (Qual, Surv)
Png et al.	JMIS 25(2): 2008	Economic	Quant
Png and Wang	JMIS 26(2): 2009	Economic ★	model
Sun et al.	JMIS 22(4): 2006	Organization	Mixed (Case, Surv)
Temizkan et al.	JMIS 28(4): 2012	Inter-Org ★	Quant
Vance et al.	JMIS 29(4), 2013	Individual (inside)	Surv
Wright and Marrett	JMIS 27(1): 2010	Individual (user)	Exp
Yue and Cakanyildirim	JMIS 24(1): 2007	Technical ★	Mod
Zhao et al.	JMIS 30(1): 2013	Economic	Model
Djekic and Loebbecke	JSIS 16(2): 2007	Individual (user) ★	QT Surv
Goel and Chengalur-Smith	JSIS 19(4): 2010	Individual (user)	Mixed (Qual, Surv)
Hedstrom et al.	JSIS 20(4): 2011	Individual (inside) ★	Case
Hua and Bapna	JSIS 22 (2): 2013	Economic	Mod
Hu et al.	JSIS 16(2): 2007	Organization	Case
Katos and Adams	JSIS 14(3): 2005	Organization	SA
Vaast	JSIS 16(2): 2007	Individual (inside)	Case
Abbasi et al.	MISQ 34(3): 2010	Technical	Mixed (DS, Model, Exp)
Anderson and Agarwal	MISQ 34(3): 2010	Individual (user)	QT (Surv, Exp)
Backhouse et al.	MISQ 30(3): 2006	Inter-Org	Case
Bulgurcu et al.	MISQ 34(3): 2010	Individual (inside)	Surv
Chen, et al.	MISQ 35(2): 2011	Economic	Mod
Culnan and Williams	MISQ 33(4): 2009	Organization	Case
Galbreth and Shor	MISQ 34(3): 2010	Economic	Mod
Gordon et al.	MISQ 34(3): 2010	Economic	Quant
Gupta and Zhdanov	MISQ 36(4) 2012	Organization	Mod
Johnston and Warkentin	MISQ 34(3): 2010	Individual (user)	Exp
Liang and Xue	MISQ 33(1): 2009	Individual (user)	SA
Posey et al.	MISQ 37(4): 2013	Users (inside)	Mixed (Qual, Surv)
Puhakainen and Siponen	MISQ 34(4): 2010	Individual (inside)	Mixed (AR, Surv)
Ransbotham et al.	MISQ 36(1): 2012	Economic	Quant
Siponen and Vance	MISQ 34(3): 2010	Individual (inside)	Surv
Smith et al.	MISQ 34(3): 2010	Inter-Org	Mixed (Case, Surv)
Spears and Barki	MISQ 34(3): 2010	Organization	Mixed (Qual, Surv)
Djekic and Loebbecke	JSIS 16(2): 2007	Individual (user) ★	QT Surv
Goel and Chengalur-Smith	JSIS 19(4): 2010	Individual (user)	Mixed (Qual, Surv)
Hedstrom et al.	JSIS 20(4): 2011	Individual (inside) ★	Case
Hua and Bapna	JSIS 22 (2): 2013	Economic	Mod
Hu et al.	JSIS 16(2): 2007	Organization	Case
Katos and Adams	JSIS 14(3): 2005	Organization	SA
Vaast	JSIS 16(2): 2007	Individual (inside)	Case
Abbasi et al.	MISQ 34(3): 2010	Technical	Mixed (DS, Model, Exp)
Anderson and Agarwal	MISQ 34(3): 2010	Individual (user)	QT (Surv, Exp)
Backhouse et al.	MISQ 30(3): 2006	Inter-Org	Case
Bulgurcu et al.	MISQ 34(3): 2010	Individual (inside)	Surv
Chen, et al.	MISQ 35(2): 2011	Economic	Mod
Culnan and Williams	MISQ 33(4): 2009	Organization	Case
Galbreth and Shor	MISQ 34(3): 2010	Economic	Mod
Gordon et al.	MISQ 34(3): 2010	Economic	Quant
Gupta and Zhdanov	MISQ 36(4) 2012	Organization	Mod
Johnston and Warkentin	MISQ 34(3): 2010	Individual (user)	Exp
Liang and Xue	MISQ 33(1): 2009	Individual (user)	SA
Posey et al.	MISQ 37(4): 2013	Users (inside)	Mixed (Qual, Surv)
Puhakainen and Siponen	MISQ 34(4): 2010	Individual (inside)	Mixed (AR, Surv)
Ransbotham et al.	MISQ 36(1): 2012	Economic	Quant
Siponen and Vance	MISQ 34(3): 2010	Individual (inside)	Surv
Smith et al.	MISQ 34(3): 2010	Inter-Org	Mixed (Case, Surv)
Spears and Barki	MISQ 34(3): 2010	Organization	Mixed (Qual, Surv)