The Journal of the Southern Association for Information Systems

Volume 8 | Issue 1 Article 4

July 2021

A Decade in Review: An Exploration of the Level of Analysis and the Subjects for Information Systems Security (ISS) Research

Christopher Kreider
Christopher Newport University, chris.kreider@cnu.edu

Recommended Citation
Kreider, C. (2021). A Decade in Review: An Exploration of the Level of Analysis and the Subjects for Information Systems Security (ISS) Research. The Journal of the Southern Association for Information Systems, 8, 69-79. https://doi.org/10.17705/3JSIS.00018

A Decade in Review: An Exploration of the Level of Analysis and the Subjects for Information Systems Security (ISS) Research

Cover Page Footnote
doi:10.17705/3JSIS.00018

ABSTRACT

Research into information systems security (ISS) showed a significant increase in scholarly output in the 2000's after nearly thirty years of slow growth. Increases in a research stream can represent either a persistent contribution to the identity of the discipline, or may be better categorized as a fashion wave, a short term increase in interest, followed by a steep decline. Within ISS research, additionally, there are concerns about relevance, with much of our research failing to do better than experienced professionals. This paper assesses ten years of ISS scholarly output across a selection of top IS journals. This research is assessed to determine whether ISS research is an increasing trend, or an example of a fashion wave. Additionally, the level of analysis, subjects and nature of the artifacts explored in this area of research are assessed to provide initial insight into the relevance problem. We find that with a nearly 200% increase in ISS articles over the prior decade, with a strong focus on individuals and the firm/organization, that ISS research is an increasing and thriving area of IS research.

INTRODUCTION

Modern organizations rely on effective use of their information systems to be successful (Cram, D'Arcy, & Proudfoot, 2019). One challenge to effective use of information systems within organizations are information security related incidents, which can have serious negative impacts with current global cybersecurity costs estimated at $575 billion (Huigang, Yajiong, Pinsonneault, & Yu, 2019). As a result, cybersecurity research, or information systems security (ISS) research, is an area that information systems (IS) researchers can and should contribute to (Zafar & Clark, 2009). It has been, however, a relatively recent area to be incorporated into the IS literature, with significant increase in research in this arena in the 2000's.

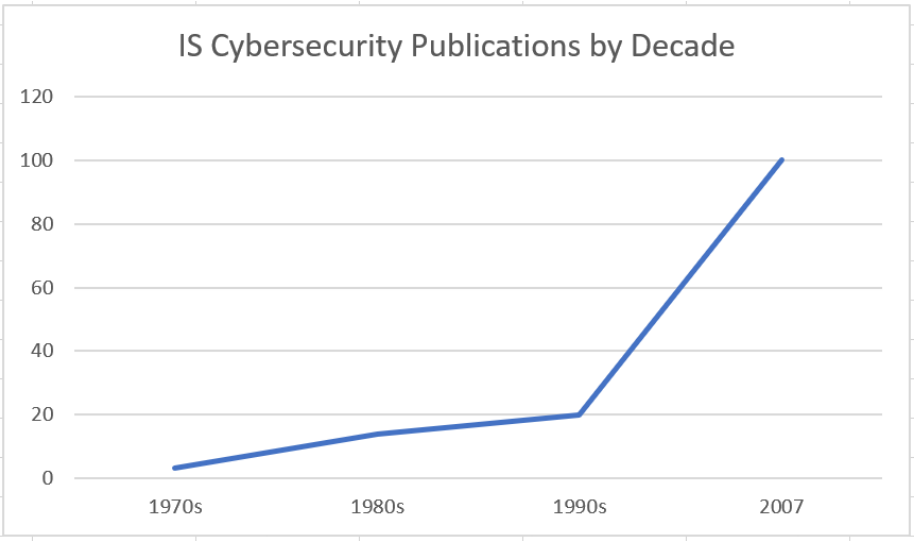

Figure 1: IS Cybersecurity Publications by Decade according to Zafar and Clark (2009)

During this time period, IS research has both increased in frequency, and breadth of topics covered. No studies identified in the 1970's explored governance or threat mitigation. However, in the 2000's, there were 22 and 18 studies respectively accounting for 40% of the research identified in that decade. Despite this increase in articles across the explored period, it is still possible that this increased trend may represent a fashion wave in IS research, a peak in interest around a research topic within the academic community that is short lived (Baskerville & Myers, 2009). With fashion waves in IS research, the time it takes to reach a peak can vary, followed by a downswing. This downswing can occur relatively shortly after the peak, or be drawn out 10 or more years. While the results of

Zafar and Clark (2009), on the surface, show a longer trend in ISS research than most fashion waves, it is possible that the research "trickled" in from the 1970's to the 2000's, finally becoming vogue and reaching a peak between 2000 and 2009, nearly within the 5-8 year window identified by Baskerville and Myers (2009). As this period from 2000-2009 clearly shows a marked increase, with 100 articles in the decade, compared to 37 articles identified in the 3 decades prior, if ISS research did in fact represent a fashion wave starting in the early 2000's, investigating the decade since then should provide insight into the status of this topic in terms of its place overall in IS research.

Additionally, as research in this area has become a significant and recognizable component of IS research, it has struggled with some of the challenges that other areas of IS research have had to tackle, namely rigor versus relevance (Lee & Hubona, 2009; Siponen & Baskerville, 2018; Straub & Ang, 2011). Siponen and Baskerville (2018) go as far as to say "…we have not demonstrated that our best research, or new theoretical contributions, can beat industry best practices or practitioners' intuitive approaches (Siponen & Baskerville, 2018, pg. 247)." One possible explanation for this shortcoming of ISS research may be due to a lack of empirical samples that exhibit ideal properties in terms of representativeness and generalizability. Specifically, samples consisting of students may not reflect a population of interest, resulting in challenges to the internal validity, external validity, and construct validity. This problem may be compounded when larger samples of these subjects may be preferred over smaller samples that better reflect reality (Lebek, Uffen, Neumann, Hohler, & Breitner, 2014). While this practice is frequently used, there is significant discussion from authors who either provide rationalization for this decision, or explicitly list it as a limitation of the study (Chatterjee, Sarker, & Valacich, 2015; Steinbart, Keith, & Babb, 2016). A second area of focus that IS researchers have engaged in active discourse is the idea of the artifact (Orlikowski & Lacono, 2001). While this conversation has been generally applied to IS research, specifically calling for researchers to better understand and theorize about the role the artifact plays, this expectation should be considered important for ISS research as well.

The rest of this paper will be structured as follows. We will first provide a brief literature review, then identify our research questions, followed by a description of our methodology. We will then present our findings with respect to our research questions, and draw implications for ISS researchers. Finally, we will provide a conclusion, discussing the limitations of this work, as well as future directions.

LITERATURE REVIEW

Zafar and Clark (2009) provide an in-depth exploration of information system security (ISS) research across a selection of top journals. They utilize a broad definition of information security which incorporates the people, processes, and technology into protection of an information system. This is broken down into several components including understanding threats and risks, establishing policies and procedures for protection and mitigation, implementing monitoring technology, continuous assessment, governance and education. They perform their review primarily over a selection of top ranked IS journals, and those from the senior scholars basket including CAIS, EJIS, I&M, ISJ, ISR, JAIS, JMIS and MISQ. They structure their review around the IBM reference model which identifies 8 broad security themes including governance, privacy, threat mitigation, transaction and data integrity, identity and access management, application security, physical security and personnel security. Additionally, they add an emergent category related to the economics of security.

Decade	# of ISS Publications
1970s	3
1980s	14
1990s	20
2000s	100

Table 1: IS Cybersecurity Publications by Decade according to Zafar and Clark (2009)

https://aisel.aisnet.org/jsais/vol8/iss1/4
DOI: 10.17705/3JSIS.00018

They break their review down by decade, summarized in Table 1, categorizing each article according to the broad themes and decade of publication. They find slow growth from the 1970s through 1990s, with an initial spike in the 2000s. Given the slow growth from 1970s through 1990s, one may wonder whether the increase in the 2000s was the result of a fashion wave or the start of a persistent trend in IS scholarly output.

Baskerville and Myers (2009) pull from neo-institutional theory, innovation and diffusion theory and Abrahamson's management fashion theory to explore fashion waves in the context of IS research. They define a fashion in the IS research context as, *"…a relatively transitory collective belief in IS research and practice, disseminated by fashion setters, that a technique or technology leads to rational IS innovation*. (pg. 649)." Using bibliographic research methods, they explore four fashions including office automation, computer-aided software engineering, business process re-engineering and e-commerce. They identify key phases, including the fashion upswing, and the fashion downswing. They found that the upswing of an IS fashion wave is rapid, often occurring within a maximum of 8 years. On the other hand, the downswings showed less consistent trends, with some topics lingering for some time, and others ending abruptly. They use this evidence to provide an explanation why IS academic literature may be considered outdated when compared with practitioner IS literature. Within the realm of information systems security (ISS) research, one might ask is ISS a persistent trend in IS scholarly output? Is it currently on an upswing, to be followed by a downswing. Additionally, this delay in IS scholarly output is specifically concerning in the context of ISS research, whose topics are rapidly evolving. Another concern for IS research streams is ensuring the artifact is appropriately represented. Orlikowski and Lacono (2001) provide a conceptualization of the IT artifact into categories including the tool view of technology, proxy view of technology, ensemble view of technology, computational view of technology and the nominal view. They found that nominal view, viewing the technology as absent, represented the greatest percentage of the 188 ISR articles they investigated, accounting for 24.8 %. As ISS research seeks to increase relevance, and given the inherent role technology artifacts play in ISS, understanding how the artifact is explored should be an important step towards better understanding of the contributions to practice within this area.

METHODOLOGY

We follow procedures specified by Templier and Paré (2015) for guiding and evaluating literature reviews within IS. Their framework includes key steps including formulating the problem, searching the literature, screening for inclusion, assessing the quality, extracting data and analyzing/synthesizing the data. Given that the selection of journals represents the top scholarly output within the discipline, the assessing for quality step is omitted, as acceptance into these journals generally represents the highest quality work published within the IS discipline. Additionally, the analyzing and synthesizing data step is reported in the results section. The remainder of the steps are discussed below.

Formulating the Problem

The first research question we seek to explore will identify whether the role of information systems security (ISS) research represents a continuing trend of relevant research within the discipline. The second research question seeks to better understand how researchers in the past decade have utilized various levels of analysis, and subjects, with a specific focus the role students and other sampling frames are utilized in the research. Finally, we seek to better understand the role of the IT artifact in ISS research. Specifically, we want to identify which studies clearly focus on an artifact as part of the study, and what that artifact is. The research questions are summarized below in table 2.

RQ#	Question
1	Does (ISS) research show a continued trend of it's overall importance in IS research, or better classified as a "fashion wave" after peaking in the 2000's?
2	What are the trends in terms of subjects and level of analysis of ISS research in the past decade (with a specific focus on the role of students)
3	What role does the artifact play in ISS research in the most recent decade, and what artifacts are explored?

Table 2: Summary of Research Questions

Searching the Literature

Using the prior work of Zafar and Clark (2009) as a starting point to answer our research questions, we have decided to bound our literature review to a similar basket of journals. By focusing on these journals, we will gain the following benefits with respect to the questions we seek to answer. First, we will be able to draw comparisons between decades, when compared to the work of Zafar and Clark (2009), which included a selection of the top ranked IS journals, as well as those included in the senior scholars basket. These included CAIS, EJIS, I&M, ISJ, ISR, JAIS, JISSEC, JMIS and MISQ. Secondly, quality related factors such as sampling frame and focus on the, these journals represent the highest quality work, representative of the core of the IS research output. Given the large number of articles that have emerged from the other journals in the field, and our goals of exploring the role of information security research within the IS discipline, we have decided to omit the Journal of Information System Security (JISSEC), as every article within the time frame would automatically meet our search criteria. As such, we have chosen to perform our review across the journals listed in Table 3 below.

Journal	Date Range Selected	Date Range Zafar and Clark (2009)
CAIS	January 2009 – December 2019	March 1999 – December 2007
EJIS	January 2009 – December 2019	January 1993 – December 2007
I&M	January 2009 – December 2019	March 1977 – December 2007
ISJ	January 2009 – December 2019	January 1991 – December 2007
ISR	January 2009 – December 2019	March 1990 – December 2007
JAIS	January 2009 – December 2019	March 2000 – December 2007
JMIS	January 2009 – December 2019	May 1984 – December 2007
MISQ	January 2009 – December 2019	March 1977-December 2007

Table 3: Journals and Date Ranges Selected

When searching through these journals, we used a keyword search with the term "security", specifically focusing on the abstract as well as performed a manual review of each journal in the date range specified to identify relevant articles that the search term may have missed. All articles listed in the specified journal that met the search criteria were included, regardless of the type of publication such as research paper or an editorial.

Screening for Inclusion

After completing our review, we first identified the total number of articles in each journal that was identified via each of the classification methods: manual search and keyword search. The results of each search were then combined, and all duplicates were removed. Finally, all articles were manually reviewed to ensure they were within the scope of this study. Articles that met keyword search but were removed include those that mentioned security in passing, where security concerns were a secondary factor, and editorials that mentioned security as part of a greater discussion.

Extracting Data

Each unique article that was selected as part of the initial search was then inspected in detail to determine information related to the research questions. Specifically, each article was first searched for "subjects", "participants" and other similar terms. If these terms did not readily uncover relevant information about the participants in the study, then a manual review of the abstract, introduction, methodology and discussion sections were performed until information on the subjects were identified. In situations where there were subjects from multiple sampling frames, such as students and professionals, even if they were for different parts of the study, they

https://aisel.aisnet.org/jsais/vol8/iss1/4
DOI: 10.17705/3JSIS.00018

were included in the findings. In situations where the study had no participants that could be identified, they were categorized into unknown. This category included a variety of article types such as editorials (Siponen & Baskerville, 2018), research agendas (Lowry, Dinev, & Willison, 2017), panel reports (Crossler, Di Gangi, Johnston, Bélanger, & Warkentin, 2018; French, Guo, & Shim, 2014) and literature reviews (Zafar & Clark, 2009) to name a few. Finally, the articles were assessed to identify the view of technology. Specific technical artifacts within the realm of information systems security (ISS) were noted, and gathered together to provide broad themes in the types of artifact that were under investigation in articles assessed.

RESULTS

The results of the initial literature review are listed below in Table 4, with information on the manual search, keyword search and final articles that were selected.

Journal	Manual Search	Abstract Keyword "Security" - All	Abstract Keyword "Security" - Selected	Final Selection, duplicates removed
CAIS	23	53	35	35
EJIS	22	20	18	18
I&M	15	52	38	38
ISJ	9	18	10	9
ISR	17	27	19	19
JAIS	16	23	18	21
JMIS	20	32	23	23
MISQ	25	40	33	35
Total	147	265	194	198

Table 4: Number of Articles Discovered During the Literature Review

This resulted in a total of 198 articles that were categorized as relating to information security. An additional, 96 articles were located in the JISSEC, which was included in the work of Zafar and Clark (2009), but were not summarized in this work, bringing the total count of articles in the realm of information security to 294 over the prior decade.

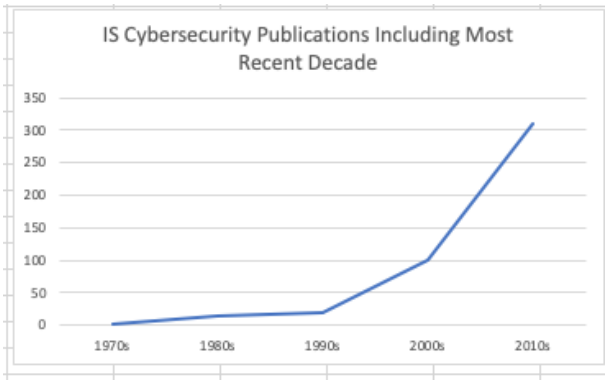

Figure 2: ISS Publications in Specified IS Journals From 2009-2019

Among the 198 articles identified, the level-of-analysis was identified through manual review of each articles abstract, introduction, methodology and conclusion/discussion sections. The level of analysis categories that emerged included from the articles reviewed included country, firm, individual, artifact, and Unknown/Miscellaneous. The number of articles identified that performed a study at each of these level of analysis are listed below in Table 5.

Country	1
Firm	41
Individual	99
Artifact	16
Unknown	39
Group	2
Total	198

Table 5: Summarized By Level of Analysis

While the levels of analysis were commonly the same as the primary subjects in each of the studies reviewed, there were a number of situations when either the subjects were aggregated to draw inferences about a higher level of analysis, such as primarily interviewing employees to make cross firm comparisons. Another situation that occurred somewhat frequently was a publication that utilized multiple types of subjects at different points in a study, for example, using students to validate a survey that was then sent to a group of professionals. The categories that emerged for the units included countries, firms, projects, employees, professionals, students, users, artifacts and uncategorized/miscellaneous. The number of articles identified that utilized subjects at these varying levels are reported below in Table 6.

Country	2
Firm	30
Projects	1
Employees	49
Professionals	20
Students	30
Users	22
Artifacts	18
Misc	40

Table 6: Summarized by Subjects

Finally, the last pieces of data that was collected from the studies reviewed, was information on studies that primarily focused on an artifact, as opposed to user behaviors or firm decisions. An overview of these studies, and the artifact explored are listed in Table 7 below.

Artifact	**Studies**
Software, Applications, Vulnerabilities, Malware	(Galbreth & Shor, 2010; Mitra & Ransbotham, 2015; Ransbotham, Mitra, & Ramsey, 2012; Seung Hyun & Byung Cho, 2014; Temizkan, Park, & Saydam, 2018; Wang, Gupta, & Rao, 2015)

https://aisel.aisnet.org/jsais/vol8/iss1/4
DOI: 10.17705/3JSIS.00018

Websites, Software as a Service, Web Content, Dark Web, Phishing Sites	(Abbasi, Zhang, Zimbra, Chen, & Nunamaker, 2010; August, Florin Niculescu, & Hyoduk, 2014; Benjamin, Valacich, & Hsinchun, 2019; Glisson & Welland, 2014; Jae Kyu, Daegon, & Gyoo Gun, 2018)
Prevention Technology (IDS, IPS, Firewall)	(Cavusoglu, Raghunathan, & Cavusoglu, 2009; Ransbotham & Mitra, 2009)
Cyberphysical components (Sensor Data, Digital Signage)	(Chanson, Bogner, Bilgeri, Fleisch, & Wortmann, 2019; Yadav & Dong, 2014)

Table 7: Overview of Articles and Associated Artifacts

DISCUSSION

The trend in information system security (ISS) research in the between 2009 and 2019 shows a clear and marked increase from the prior decade, with 294 articles being identified in the same journal basket as the work of Zafar and Clark (2009). This nearly 200% increase in published articles over the prior decade provides evidence for the continuing and significant importance of ISS research in IS publication outlets. Far from a fashion wave (Baskerville & Myers, 2009), this multi decade marked increase in scholarly output indicates that ISS is likely to be a topic of continuing importance. This continuing trend of research in this area may also provide evidence of how IS researchers as a whole are successfully boundary spanning across the market of ideas that is relevant to human endeavor (Lyytinen & King, 2004).

Across the studies identified, the level of analysis showed that nearly 50% of all identified studies focused on individuals as the focus of the study. Approximately 20% focused on firms or organizations. Another approximately 20% did not clearly utilize subjects in a research capacity, either providing editorials, reporting on conference panel sessions, or providing literature reviews. The remaining approximate 20% focused on either team/group or the artifact explicitly. This distribution of level of analysis provides the ability to draw interesting inferences, specifically, the recognition that individuals or users are the primary decision makers and action performs in security, but that they also represent a potential weak link in the chain of security (Whitten & Tygar, 1999).

For the subjects of the identified studies, students tied for 3rd place with 30 articles identified as using student subjects capacity, tied with those that sampled at the firm/organization level. The most frequent subject was organizational employees, used in 49 of the publications. The more specific class of professional was used less frequently in 20 instances, with the more generic "users" used more frequently. Overall, reliance on students as the primary sampling frame in studies was not occurring frequently, with many situations where students were used as part of a larger sampling strategy, or research methodology.

Finally, within the studies focusing exclusively on the artifact, 16 of the 198, there were several articles with a clear focus on the technology behind security, for example Intrusion Detection Systems and Firewalls (Cavusoglu et al., 2009), Phishing Websites (Abbasi et al., 2010), the dark web (Benjamin et al., 2019) and vulnerabilities (Mitra & Ransbotham, 2015). Of the artifacts discussed, the most frequent was software/application based.

CONCLUSION

We find that with respect to RQ1, that information system security (ISS) research is a continuing and important part of IS research, with significant increases in publications in this topic area within the past decade. We find that with respect to RQ2, that there is significant variation in the level of analysis and the subjects sampled. The patterns do represent a connection to the core of IS, with a focus on individuals and organizations, and their intersection. Students do not represent the most frequent sampling frame, but do play a non-trivial role in the published research explored. Specifically, students were frequently used in instrument validation, and in some cases were the primary

subjects in a study. Finally, with respect to RQ3, we find that when the primary focus is on the artifact, it focuses around security related technology, or general applications. This focus on the artifact, however, was a relatively small portion of the overall research explored.

This paper has several limitations. The first major limitation is that a very limited number of IS journals were explored. While the practice of selecting only top journals is discouraged (Webster & Watson, 2002). This study chose to focus on the selected journals to build on prior work, and draw inferences about the core of the IS research output. Future studies could expand the range explored to better draw inferences about quality across the spectrum of IS publication outlets. The second major limitation is that all categorization was done by a single reviewer. As a result, it is possible that classification could be influenced by bias or lack of knowledge. Future work could utilize multiple experts within the field to perform classification to provide better evidence of reliability via inter-rater reliability.

REFERENCES

1. Abbasi, A., Zhang, Z., Zimbra, D., Chen, H., & Nunamaker, J. J. F. (2010). Detecting Fake Websites: The Contribution Of Statistical Learning Theory. *MIS Quarterly, 34*(3), 435-461. doi:10.2307/25750686
2. August, T., Florin Niculescu, M., & Hyoduk, S. (2014). Cloud Implications on Software Network Structure and Security Risks. *Information Systems Research, 25*(3), 489-510. doi:10.1287/isre.2014.0527
3. Baskerville, R. L., & Myers, M. D. (2009). Fashion Waves in Information Systems Research and Practice. *MIS Quarterly, 33*(4), 647-662.
4. Benjamin, V., Valacich, J. S., & Hsinchun, C. (2019). DICE-E: A Framework For Conducting Darknet Identification, Collection, Evaluation With Ethics. *MIS Quarterly, 43*(1), 1-22. doi:10.25300/MISQ/2019/13808
5. Cavusoglu, H., Raghunathan, S., & Cavusoglu, H. (2009). Configuration of and Interaction Between Information Security Technologies: The Case of Firewalls and Intrusion Detection Systems. *Information Systems Research, 20*(2), 198-217. doi:10.1287/isre.1080.0180
6. Chanson, M., Bogner, A., Bilgeri, D., Fleisch, E., & Wortmann, F. (2019). Blockchain for the IoT: Privacy-Preserving Protection of Sensor Data. *Journal of the Association for Information Systems, 20*(9), 1271-1307. doi:10.17705/1jais.00567
7. Chatterjee, S., Sarker, S., & Valacich, J. S. (2015). The Behavioral Roots of Information Systems Security: Exploring Key Factors Related to Unethical IT Use. *Journal of Management Information Systems, 31*(4), 49-87. doi:10.1080/07421222.2014.1001257
8. Cram, W. A., D'Arcy, J., & Proudfoot, J. G. (2019). Seeing The Forest And The Trees: A Meta-Analysis Of The Antecedents To Information Security Policy Compliance. *MIS Quarterly, 43*(2), 525-554. doi:10.25300/MISQ/2019/15117
9. Crossler, R. E., Di Gangi, P. M., Johnston, A. C., Bélanger, F., & Warkentin, M. (2018). *Providing Theoretical Foundations: Developing an Integrated Set of Guidelines for Theory Adaptation* (Vol. 43).
10. French, A. M., Guo, C., & Shim, J. P. (2014). *Current Status, Issues, and Future of Bring Your Own Device (BYOD)* (Vol. 35).
11. Galbreth, M. R., & Shor, M. (2010). The Impact Of Malicious Agents On The Enterprise Software Industry. *MIS Quarterly, 34*(3), 595-A510. doi:10.2307/25750693
12. Glisson, W. B., & Welland, R. (2014). Web Engineering Security (WES) Methodology. *Communications of the Association for Information Systems, 34*(1).
13. Huigang, L., Yajiong, X., Pinsonneault, A., & Yu, W. (2019). What Users Do Besides Problem-Focused Coping When Facing IT Securty Threats: An Emotion-Focused Coping Perspective. *MIS Quarterly, 43*(2), 373-394.
14. Jae Kyu, L., Daegon, C., & Gyoo Gun, L. (2018). Design and Validation of the Bright Internet. *Journal of the Association for Information Systems, 19*(2), 63-85. doi:10.17705/1jais.00484

15. Lebek, B., Uffen, J., Neumann, M., Hohler, B., & Breitner, M. H. (2014). Information security awareness and behavior: a theory-based literature review. *Management Research Review*.
16. Lee, A. S., & Hubona, G. S. (2009). A Scientific Basis For Rigor In Information Systems Research. In (Vol. 33, pp. 237-262): MIS Quarterly.
17. Lowry, P. B., Dinev, T., & Willison, R. (2017). Why security and privacy research lies at the centre of the information systems (IS) artefact: proposing a bold research agenda. *European Journal of Information Systems, 26*(6), 546-563.
18. Lyytinen, K., & King, J. L. (2004). Nothing At The Center?: Academic Legitimacy in the Information Systems Field 12. *Journal of the Association for Information Systems, 5*(6), 220-246.
19. Mitra, S., & Ransbotham, S. (2015). Information Disclosure and the Diffusion of Information Security Attacks. *Information Systems Research, 26*(3), 565-584. doi:10.1287/isre.2015.0587
20. Orlikowski, W. J., & Lacono, C. S. (2001). Research Commentary: Desperately Seeking the 'IT' in IT Research--A Call to Theorizing the IT Artifact. *Information Systems Research, 12*(2), 121.
21. Ransbotham, S., & Mitra, S. (2009). Choice and Chance: A Conceptual Model of Paths to Information Security Compromise. *Information Systems Research, 20*(1), 121-139. doi:10.1287/isre.1080.0174
22. Ransbotham, S., Mitra, S., & Ramsey, J. (2012). Are Markets For Vulnerabilities Effective? *MIS Quarterly, 36*(1), 43-64. doi:10.2307/41410405
23. Seung Hyun, K., & Byung Cho, K. (2014). Differential Effects Of Prior Experience On The Malware Resolution Process. *MIS Quarterly, 38*(3), 655-678. Retrieved from
24. Siponen, M., & Baskerville, R. (2018). Intervention Effect Rates as a Path to Research Relevance: Information Systems Security Example. *Journal of the Association for Information Systems, 19*(4), 247-265. doi:10.17705/1jais.00491
25. Steinbart, P. J., Keith, M. J., & Babb, J. (2016). Examining the Continuance of Secure Behavior: A Longitudinal Field Study of Mobile Device Authentication. *Information Systems Research, 27*(2), 219-239. doi:10.1287/isre.2016.0634
26. Straub, D., & Ang, S. (2011). Rigor and Relevance in IS Research:Redefining the Debate and a Call for Future Research. *MIS Quarterly, 35*(1), iii-xi. Retrieved from
27. Temizkan, O., Park, S., & Saydam, C. (2018). Software Diversity for Improved Network Security: Optimal Distribution of Software-Based Shared Vulnerabilities. *Information Systems Research, 29*(4), 828-849. doi:10.1287/isre.2017.0722
28. Templier, M., & Paré, G. (2015). A framework for guiding and evaluating literature reviews. *Communications of the Association for Information Systems, 37*(1), 6.
29. Wang, J., Gupta, M., & Rao, H. R. (2015). Insider Threats In A Financial Institution: Analysis Of Attack-Proneness Of Information Systems Applications. *MIS Quarterly, 39*(1), 91-A97.
30. Webster, J., & Watson, R. T. (2002). Analyzing the Past to Prepare for the Future: Writing a Literature Review. *MIS Quarterly, 26*(2), xiii-xxiii. Retrieved from
31. Whitten, A., & Tygar, J. D. (1999). *Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0.* Paper presented at the USENIX Security Symposium.
32. Yadav, S. B. P. D., & Dong, T. (2014). A Comprehensive Method to Assess Work System Security Risk. *Communications of the Association for Information Systems, 34*(1).
33. Zafar, H., & Clark, J. G. (2009). Current State of Information Security Research In IS. *Communications of the Association for Information Systems, 24*(34), 557-596.

ABOUT THE AUTHOR

Christopher Kreider: Chris is faculty at Christopher Newport University, and coordinator for their IS and cybersecurity majors. Chris' research is primarily interested in the human elements of cybersecurity, and how cybersecurity research fits into the greater IS research agenda.

https://aisel.aisnet.org/jsais/vol8/iss1/4
DOI: 10.17705/3JSIS.00018