Association for Information Systems

AIS Electronic Library (AISeL)

AMCIS 2020 Proceedings

Information Security and Privacy (SIGSEC)

Aug 10th, 12:00 AM

Information Security Research within the Information Systems Discipline: Analyzing, Categorizing, and Classifying the Historical Underpinnings and Theoretical Assumptions

Alan Rea
Western Michigan University, alan.rea@wmich.edu

Kaitlin Marshall
Western Michigan University, kaitlin.m.marshall@wmich.edu

Information Security Research within the Information Systems Discipline: Analyzing, Categorizing, and Classifying the Historical Underpinnings and Theoretical Assumptions

Completed Research

Alan Rea
Western Michigan University
alan.rea@wmich.edu

Kate Marshall
Western Michigan University
kaitlin.m.marshall@wmich.edu

Abstract

Academics examine and improve organizational systems, but oftentimes lag in techniques and theories because time is necessary to thoroughly study solutions. This research explores Information Security (InfoSec) concepts and theories within the Information Systems (IS) discipline to determine historical approaches, theoretical assumptions, and suggest where to strengthen InfoSec research areas.

In our paper, we present our basic methodology; illustrate our approach by applying it to one of the "Basket of Eight" Association for Information Systems journals, the *European Journal of Information Systems;* and report our initial results. In subsequent research we will then use our proposed methodology for the remaining seven journals and beyond. By analyzing how researchers have historically examined information security, we can focus future InfoSec studies in necessary critical directions and maintain a closer pace with new techniques and theories to secure organizational information systems.

Keywords

Information Security, Cybersecurity, Historical Research, Scholarly Trends

Introduction

Computing systems have become the de facto tools for collecting and processing data, as well as providing massive amounts of information. In the organizational sector this has been the case for many years and security professionals have developed tools and approaches to ensure the confidentiality, integrity, and availability of these systems and the data they contain.

However, the security professional's toolkit has changed dramatically over time and has failed to meet contemporary challenges. This too can be seen in Information Security research and we will explore in this paper—via a topical literature methodology—why this might be the case. This quandary is best illustrated by the evolution of how we have academically and pragmatically approached secure systems via system and security policies.

First-generation system policies primarily focused on checklists for specific solutions that focus on what can be done rather than what needs to be done (Baskerville 1993). Although we might be quick to argue these are no longer used, one only needs to go as far as help desk checklists designed to address general computing problems, or user manuals for a variety of peripheral devices. First-generation policies are easy for users to follow as long as there are no outliers that would cause the steps or checklist to fail. In the security realm we still see attempts to implement these policies in areas such as wireless home router setups.

As we add more systems to our cars, homes, and organizations, they quickly become more complex. It is this complexity that brings us to second-generation system policies. Here, we move from checklists and steps at the physical level to more conceptual security concepts. Many highly technical system procedures in use today are based on second-generation security policies. It is here we also see the emergence of system requirement specifications such as entity relationship diagrams to determine system and security needs.

This interconnectedness does not automatically imply social connectivity (e.g., shared network printers). To underscore this Baskerville notes that second-generation approaches focus on the mechanistic aspects of systems rather than business process needs that can result in functionality versus security conflicts (Baskerville 1993). We are all well aware that when users are not part of the system design process that implements a secure mechanism, there is a tendency for users to find a "work-around" in order to efficiently complete their tasks. Many times, these lead to lapses in security procedures (e.g., computer passwords taped to monitors).

Of course, we know now that systems designed for security without considering human interaction will be compromised. It is this shift into taking the social into account that moves us into third-generation model to include both behavior and organizational needs (Baskerville, 1993). In the early nineties there were not many third-generational systems to analyze, but Baskerville's work has been built upon and expanded with the influx of organizational system integrations.

One such expansion discusses how Baskerville's third-generational model does not quite take into the account what we now consider social although it does address organizational (Siponen 2001). Instead, Siponen creates a fourth-generational socio-technical approach where the communication between responsible system parties is understandable for both normal users and system designers – therefore breaking the possible communication gap (Siponen 2001). In this approach we can see the true complexity and interconnected system matrices inherent in organizational systems.

Generational policy research illustrates the challenges we face in Information Security research within the Information Systems discipline. Unlike the more mature Computer Science discipline, Information Systems is a relative newcomer in the last 50 years working through organizational and managerial issues within the realm of computers and larger information systems. Even more challenging is the IS foray into information security in the last 20 years.

This research, then will explore the concepts, approaches, and theories of Information Security (InfoSec) within the realm of Information Systems (IS) to determine what historical boundaries we operate within as well as point toward where we might look to strengthen our InfoSec research approaches. To accomplish this, we must look at the most representative element of IS research: our top academic journals. Analyzing how researchers and scholars have examined information security can help us focus our studies in critical directions.

For this paper, we set the historical and organizational context for InfoSec within the IS discipline. We will then focus on one of the top Association for Information Systems' academic journals—the *European Journal of Information Systems*—that contained some of the first extended Information Security discussions within Information Systems to set forth our methodology that will be used in further research as we chart the path and influence of InfoSec within the IS discipline.

Literature Review

Considering the time required to adequately research and study information security within the IS discipline and rapidity of change within InfoSec itself, disparities in terminology are not entirely unexpected. These variations include considering cybersecurity and information security as the same; framing information security as a subset of cybersecurity; and believing cybersecurity has replaced information security as an all-inclusive term (von Solms and von Solms 2018). Within the more mature Computer Science discipline, multiple studies have been published exploring differences in these definitions (Maurer and Morgus 2014; von Solms and von Solms 2018; von Solms and van Niekerk 2013). In contrast, within our search results of articles in the *EJIS*, it isn't until 2017 that we see a comparison of information security and computer security; the authors argue that computer security, contrary to information security, is associated with technical security policies (Cram et al. 2017). Furthermore, we note that "InfoSec" as a synonym for Information Security is not utilized until 2019 (Niemimaa and Niemimaa 2019). It is, however, mentioned in two other documents: once as a departmental abbreviation and once as a direct quote from an article in *Computers & Security* (Brinton Anderson et al. 2016; Crossler et al. 2013; Herath and Rao 2009). In fact, *Computers & Security* is cited 66 times in our search of the *EJIS*, with the oldest reference dating back to 1994 (Ølnes 1994). Recognizing the depth of InfoSec research within the Computer Science discipline underscores the importance of exploring the evolution of information security research within the IS discipline, which requires one to understand the distinct appearance of the IS discipline itself.

Information Systems as a Discipline

The discipline of Information Systems plays a major role in how we can best design and develop organizational system. It was with this focus that Gordan Davis started the first program in Management Information Systems at the University of Minnesota in 1967 (Association for Information Systems (AIS) n.d.-a). Unlike other disciplines, IS is still fairly new with the first major professional organization, the Association of Information Systems (AIS), not coming into its own until 25 years ago. Before this time, IS professionals were most likely found in Computer Science departments (and some still are) as CS is a discipline with a longer history dating back to Ada Lovelace and her support for Charles Babbage's Analytical Engine with major advancements coming during World War II and then moving quickly into the forefront in the 1960s with ARPANET before hurtling into common usage in the late 90s as the World Wide Web became available to many (Lukasik 2011).

As the connectivity of the Internet become more integrated into business, so too did Information Systems become more focused. AIS became a professional organization and quickly grew to international stature. It is considered by many to be our discipline's major organization with annual regional, national, and international conferences that showcase research, serve as recruiting venues, and offer professional growth and training opportunities.

Top Information Systems Journals

A major part of the AIS effort to establish research and scholarship venues was its establishment of what is deemed the "Basket of Eight" journals (Association for Information Systems (AIS) n.d.-b). The AIS Senior Scholars' "Basket of Journals" is comprised of the eight (8) "A" category journals in the Information Systems discipline:

- European Journal of Information Systems (EJIS)
- Information Systems Journal (ISJ)
- Information Systems Research (ISR)
- Journal of AIS (JAIS)
- Journal of Information Technology
- Journal of MIS (JMIS)
- Journal of Strategic Information Systems (JSIS)
- MIS Quarterly (MISQ)

Publishing in these journals is expected at almost all PhD-granting, research-oriented universities (Association for Information Systems (AIS) n.d.-b).The senior scholars who made the case for these journals all have served, at one time or another, as the editor-in-chief of one of the journals. This list was created in April of 2007 and revised in December of 2011 (Association for Information Systems (AIS) n.d.-c). It is reviewed annually to determine if the list remains valid.

Because the AIS organization and scholars realize the "Basket of Eight" are limited to just the Information Systems field and not inclusive of other technical, multi-disciplinary, or specialty areas within the discipline, each of the AIS Special Interest groups has put forth a list of five (5) journals.

Information Security Research within Information Systems

Still, the "Basket of Eight" embody the most important research in our field and both reflect, and establish, scholarship trends. This research then will use these eight journals as the source material to track how our discipline is addressing the multitude of computer and information security issues so that we may look at the discipline-specific history as it works through challenges, as well as suggestions, shortcomings, and potential areas for future research endeavors. By doing so, we can help chart how the IS discipline can specifically help organizations secure not only applications but also practices as they relate to the overall security and privacy of information systems.

The Special Interest Group in Security (SIGSEC) journal list will be consulted as part of this research for terms and particular Information Security approaches within the discipline ("SIGSEC" n.d.). However, the journals will not be used in the overall study as this would skew the results.

- Computers & Security
- International Journal of Information Security
- Journal of Information System Security
- Journal of Information Security
- Digital Investigation

Of special note is that except for the highly technical Computer Science journal, *Computers & Security*, all relevant information security publications do not start until the 21st century. This underscores the importance of tracking the evolution of computer and information security as it has formed within the top Information Systems' journals.

Methodology

For this current paper, we will discuss our methodology and initial findings for one of the "Basket of Eight" journals: the *European Journal of Information Systems (EJIS)*. We use the EJIS because it has some of the first preliminary clusters of Information Security research in a non-Information Security focused journal. We focus on the methodology in this paper to put forth our entire approach that will be utilized as we move forward with the remaining seven top AIS journals. In future research we will present a more encompassing study that will better illustrate complete InfoSec research trends within the larger IS discipline.

Data Collection

In an effort to be inclusive of all types of security (information, cyber, data, computer, physical, etc.) within the information systems discipline, we used the broad term "security" to search for mentions throughout *EJIS*. More specifically, we looked for mentions of security in *EJIS* article titles, abstracts, and/or keywords. The following databases were used for the initial collection of data: *Taylor & Francis Online* (*T&F*), *Springer*, *ProQuest*, and *Google Scholar*. Table1 provides a breakdown of search specifics and results for each database. It is important to note that *Springer* is not included in the table because the database did not allow for a specific term to be searched in the title, abstract, or keywords; instead, *Springer* only allowed for a blanket search in all elements, including full text, which resulted in 349 hits.

Source	Search term(s)	# results
ProQuest	pubid(30520) AND (ab(security) OR ti(security))	36
T&F	[Publication Title: security] AND [in Journal: European Journal of Information Systems]	32
	[Keywords: security] AND [in Journal: European Journal of Information Systems]	23
Google Scholar	allintitle: security source:"European Journal of Information Systems"	26

Table1: Search Criteria and Results

For each search, results were aggregated into a spreadsheet via the following methods: *ProQuest* search results were exported to .csv, which could be directly copied to the spreadsheet; *T&F* searches were input manually as there was no option to export; *Google Scholar* results were collected via the program *Publish or Perish* (Harzing 2007). Once all results were contained in a single spreadsheet, they were cross-referenced for duplicates based on title. Results that were contained in only one database (i.e. had no duplicate value) were manually checked for mentions of security in title, abstract, and/or keywords. Most non-duplicate values were found to be a valid result based on our criteria, but a total of five were still eliminated from the *T&F* title search results. These inaccuracies resulted from the journal issue title containing the word "security" rather than the article itself containing "security" in its title. Once these were removed, 41 articles remained in total containing “security” in the title, abstract, and/or keywords. The results were then collated into a single list and PDFs were gathered for 40 out of 41 of the documents. One result did not have a PDF version available. Of these 41 remaining, three were book reviews and one was an article focused on job security within the Information Systems field, not information security. These four results were omitted from our data collection on the grounds of irrelevance for a total of 37 articles.

When selecting criterium for our search, we anticipated a much greater volume of hits when searching all titles, abstracts, and keywords. However, the final number of 37 articles represents only one journal out of eight we will ultimately examine. Additionally, each database contained limitations of its own. While Springer allows for “title only” searches across its entire database of journals, when searching within a specific journal publication, we could only search all mentions of security throughout the entirety of an article. It is important to note that when searching the exact phrase “European Journal of Information Systems” alongside “security” in the title via *Springer’s* advanced search, 70 results were returned. These results, however, were deemed inaccurate because returned results contained “European Journal of Information Systems” within full text and article citations. Furthermore, *ProQuest* allowed “security” to be searched exclusively within the title and abstract, but did not have the ability to search for “security” as an article keyword; *T&F* did not have functionality to search via abstract; and Google Scholar could only perform a search within the title or throughout the full text. These limitations inhibited our ability to cross-reference sources with identical criteria applied for the search. More work will need to be done in this area to create a more robust data set.

Throughout our search and subsequent collection, we noticed numerous articles whose title, abstract, and/or keywords did not contain the term security, but were still focused heavily on security throughout, which could explain our lack of findings in any article for the year 2018. For example, when performing a search for security in all text via *T&F*, 441 results were returned compared to the 32 results obtained when searching specifically in the title. Results were also hindered by use of closely-related terms, such as privacy, which is not a synonym of security per se, but is oftentimes closely related. We will consider this as we move forward with our research to account for such term association.

As we moved into greater analysis of the data, basic statistics were gathered based on mentions for certain terms or phrases within the 40 documents. First, to identity potential patterns and trends, each article returned from our initial search was manually searched for each mention of “security” throughout the entirety of each document’s text. For each instance of the word security within both the full text and abstract, relevant surrounding keywords were documented. As patterns emerged, we underwent deeper analysis of keywords related to identified trends. Data collection of more precise keywords was performed via a search of all PDFs. Each mention returned was then inspected manually for validity and context. A count was kept of the number of unique documents the terms appeared in, not all individual mentions. It is important to note that when searching in text, only the body of the text was used for data collection, statistics, and pattern/trend recognition. Mentions were excluded if they appeared in the following sections: “about the authors,” “acknowledgements,” and/or “references.”

Moving forward, it may be best to broaden our search criteria to include all mentions held within full text rather than attempt to pinpoint results based on title, abstract, and/or keywords to circumvent the aforementioned limitations. Approaches to remedy these search limitations via custom natural language processing (NLP) scripts are in development to more thoroughly track and discover research stream trends. See Table 1 below. Generally, text in each field of a table will look better if it has equal amounts of spacing above and below it, as in Table 1.)

Data Analysis

Of approximately 1200 potential documents published in *EJIS* between 1991 and 2019 (including articles, discussions, editorials, brief reports, review articles, corrections, and book reviews), we estimate that nearly 400 mention the word “security” at least once within their full text. This estimate is based on the 349 results returned from *Springer,* 441 from *T&F*, and 396 from *Google Scholar* when performing full text searches. However, only 41 documents out of these 400 potential results contain “security” at least once in the title, abstract, and/or keywords. Statistics were gathered from the 40 available PDFs out of 41 total documents for each mention and broken down into the following categories: General Terminology;

Trends/Innovations; Common Attack Types; Managerial Terminology; and Miscellaneous. Table2 details terms searched, number of document hits, and other statistically relevant information, including whether results were omitted when contained within a book review.

Category	Term	Number of Documents	Notes
General Terminology	Authentication	13	Over the course of 1991-2017
	Access Control	13	Over the course of 1991-2017
	Password	20	Mentions cover policy, complexity, guidelines, habits, protection, user use and abuse
	Privacy	22	Over the course of 1991-2019
	Encryption	11	Over the course of 1991-2017
	Cryptography/ cryptographic systems	9	Appeared in 1991 book review, but was omitted for relevance
	CIA triad	3	Individual mentions of confidentiality, integrity, and availability are present, but only 3 occurrences where they are referenced together (in 2009, 2012, and 2014)
	Black hat research	1	No mentions of either white hat or red hat
	Attack vector	1	Only mentioned in 2016
	Hacker/hacking	12	Over the course of 1992-2019
	NIST	5	First mention in 2008; mentioned again in 2009, 2012, 2014, and 2017
	Best practices	9	First mentioned in 2005; not again until 2009. Then 2012, 2017, 2019.
Trends/ Innovations	Cryptocurrency/ blockchain	1	Only mentioned in 2017
	Artificial Intelligence (AI)	1	Only mentioned in 2009
	IoT	2	Only mentions were in 2017 and 2019
	Big Data	1	Only mentioned in 2017
	Open Source Development	2	Only mentioned in 2011 and 2012
	Automation	2	5 total documents, but only 2 discuss automation directly related to security
	Cloud Computing	1	Only mentioned in 2017
	2FA (search: secondary authentication)	1	Only mentioned in 2009
	Biometric(s)	5	2006, 2007, 2009, 2014

Common Attack Types	Malware/anti-malware	10	10 combined
	Virus/anti-virus	11	9 documents with virus; 3 with anti-virus; 11 combined
	Worm	3	Mentioned in 2009, 2012, 2016
	Trojan	1	Mentioned in 2009, 2015
	DDoS/DoS	3	Mentioned in 2009, 2016, 2016
	Flood(ing)	0	Only mentioned as an "act of God"
	Injection	1	Specifically, SQL injection
	Spyware/anti-spyware	8	6 documents with spyware; 4 anti-spyware; 8 combined
	Rootkit	2	Mentioned in 2009 and 2017
	Man-in-the-middle	2	Only mentions were in 2016 and 2017
	Sniffing	0	
	Spoofing	2	Mentioned in 2016 and 2017; one mentioned was specified as "IP spoofing"
	Ransomware	1	Only mention was in 2017
	Phishing/anti-phishing	7	6 documents with phishing; 1 anti-phishing; 7 combined
	Spear Phishing	2	Only mentions were in 2016 and 2017
Managerial Terminology	Policy/Policies	33	Over the course of 1992-2019
	Procedures	25	Over the course of 1992-2019
	Practices	30	Over the course of 1992-2019
	Standards	24	Over the course of 1991-2019
	Security awareness	18	Mentions are general and related to programs and/or training. First mentioned in 2003, then in 2005, 2006, 2008-2011, 2014-2017, and 2019
	SETA	3	Mentioned for the first time in 2016; then twice more in 2017.
	Employees	25	Discuss human error, employee as the weakest link, employee training, employee adherence, and compliance to policy
	Spending	3	Specifically, spending on IT
	Budget	8	11 total hits, but only 8 discussed budget directly in connection to security initiatives (awareness, training, infrastructure, etc.)
	Investment	12	14 total documents, but only 12 reference investment related to security
	(Information) Security Officer	3	IT security manager was mentioned as far back as 1992; security officer mentioned first in 2012, then again in 2014 and 2015

	CSO	2	First mentioned in 2014, then again in 2017
	CISO	2	First mentioned in 2017 and then again in 2019
Miscellaneous	European Union Data Protection Directive/ GDPR	3	A fourth document alluded to exploration of regulatory options in the EU, but did not specifically mention the directive or GDPR. The first mention was in 2014, then not again until 2017 and 2019.
	Supply Chain	3	Mentions occurred in 2009, 2010, 2017
	Customer Relationship Management	1	Only mentioned in 2007
	Enterprise Resource Planning	4	Mentions occurred in 2007, 2009, 2010, and 2011

Table2: Search Results per Document

The data contained in Table2 reveals a great deal about industry dialogue concerning information security both past and present. It is clear that many general concepts and terms such as "policy" and "procedure" are used consistently and regularly throughout the 28 years *EJIS* has been in publication. However, the number of results returned on more security-specific searches such as "attack vector," "CIA" or "CIA triad" were minimal. There is also a surprisingly small number of results returned for searches of NIST, which occurred in only five documents. This in itself did not meet our expectations because of the NIST's significant contributions and relevance to the security field. We will need to account for this and consider more searches for accepted frameworks such as ISO 27000 to account for a more international focus. In the same vein, there is a distinct lack of consistent research on types of attacks. Table2 shows that exceptionally common types of attack vectors, such as malware or viruses, are still only mentioned ten and 11 times respectively out of the available documents. Less common attack means such as rootkits, man-in-the-middle, and DDoS/DoS attacks returned results in the low single digits. Such a great discrepancy could of course result simply from sheer volume of malware and virus types, but it is still important for research to be equitable for both organizations and managers; to have a full understanding of what to be prepared for, all avenues need to be explored.

Initial Results and Discussion

Upon inspecting the data, other, less clear patterns emerge. One such pattern is a lacking standardization of terminology in an industry that many consider to be still maturing. For example, information security is used consistently, but it isn't until 2019 that "InfoSec" is used as its own term (Niemimaa and Niemimaa 2019). In addition to information security, a plethora of different types of security are mentioned, including cybersecurity, physical security, computer security, network security, data security, web security, IT security, IS security, email security, end-user security, and password security. Not until 2017 was there a document exploring the fundamental differences between information and computer security policies (Cram et al. 2017). Cybersecurity, which only showed up twice in our data collection, and was hyphenated in its first use but not in the second. Likewise, the use of "cyber" as a prefix is used sparingly; its first mention refers to cyber-merchant in 2007 and it isn't until two years later, in 2009, that we begin seeing "cyber" as it is oftentimes recognized presently (e.g. cyberspace, cybercrime, cybersecurity) (Boss et al. 2009; Herath and Rao 2009; Khalifa and Liu 2007; Warkentin and Willison 2009).

Increased usage of "cyber" as a prefix could represent a maturing industry, which is also displayed by the transition from general mentions of "security awareness" in the early 2000s to the more established SETA (security education, training, and awareness) mentioned for the first time in 2016 (Brinton Anderson et al. 2016). Increased maturity is further reflected through the establishment of a chief information security officer (CISO); while the first mention of an IT security manager dates back to 1992, we can trace its history from information security officer in 2012 to chief security officer (CSO) in 2014 to the first mention of a CISO in 2017 (Niemimaa and Niemimaa 2017; Njenga and Brown 2012; Siponen and Vance 2014; Warman 1992). An increased number of mentions of "best practices" is another primary example of the field's ongoing establishment of maturity. After its first mention in 2005, four years pass (Siponen 2005). Best practices are then mentioned with increasing frequency beginning in 2009; furthermore, best practices are also referenced alongside frameworks for best practice guidelines such as ISO, IEC, CobiT, and NIST. Presence and reference to established frameworks underscores a maturing security industry.

Despite the aforementioned signs of maturity and increased standardization of terminology, there is a definite deficiency in discussion regarding present trends. Biometrics, which has the most appearances, still only showed up in five documents throughout the 28 year tenure of *EJIS*. Of the other current trends searched, IoT, open source development, and automation occur only twice; cryptocurrency/blockchain, artificial intelligence, big data, cloud computing, and two factor authentication (2FA) appear only once. Machine learning is not mentioned at all. The minimal number of times these trends arise in analyzed documents is inherently concerning because it exhibits the lack of research and information available regarding current trends and technologies in security. Preparing and defending properly against dynamic security threats becomes increasingly difficult when resources and subsequent potential preparation is hindered by a sheer lack in research. Ideally, preparation and overall defense will naturally strengthen alongside an upsurge in adoption of security climate and culture. Combined, the two appear in six documents since 2009, including a mention as recently as 2017 (Boss et al. 2009; Cram et al. 2017; Foth 2016; Herath and Rao 2009; Hsu 2009; Siponen and Vance 2014). Adoption of and organizational change toward a stronger security climate and culture could also help reinforce the necessity of greater emphasis placed on researching areas of security that are lacking, such as types of attacks or security trends mentioned previously.

Conclusion and Future Research

By undertaking this research using our methodology, we will plot the evolution of information security research within the IS discipline. Although other disciplines, such as Computer Science, have contributed a great deal to computer and information security, IS must also carve out a distinct path within the information security and cybersecurity realm so that we may map our contribution to the multi-faceted challenges that come with securing computer, data, operations, and network systems within diverse organizational contexts, as well as chart new areas for security research. Plotting these historical trends within top academic research journals will allow us to identify and analyze trends and pattern within information security scholarship. Then, taking these trends into consideration, our research proves that we must put forth effort toward adequately exploring and researching information security topics that are thus far lacking, such as common attack types and security innovations/trends. Without adequate exploration into these topics and others that will be discovered through our findings, carving out an appropriate path will prove difficult.

Ultimately, these findings will inform future scholarship paths and perhaps offer new techniques and approaches that have been relegated to footnotes in our brief discipline's scholarship history.

REFERENCES

Association for Information Systems (AIS). (n.d.). "Gordon Davis." (https://aisnet.org/page/GordonDavis, accessed February 2, 2020 a).

Association for Information Systems (AIS). (n.d.). "Senior Scholars' Basket of Journals." (https://aisnet.org/general/custom.asp?page=SeniorScholarBasket, accessed February 22, 2020 b).

Association for Information Systems (AIS). (n.d.). "Senior Scholars Journal Review Quality Survey." (https://aisnet.org/page/SeniorScholarSurvey/Senior-Scholars-Journal-Review-Quality-Survey.htm, accessed January 20, 2020 c).

Baskerville, R. 1993. "Information Systems Security Design Methods: Implications for Information Systems Development," *ACM Comput. Surv.* (25:4), New York, NY, USA: Association for Computing Machinery, pp. 375–414. (https://doi.org/10.1145/162124.162127).

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., and Boss, R. W. 2009. "If Someone Is Watching, I'll Do What I'm Asked: Mandatoriness, Control, and Information Security," *European Journal of Information Systems* (18:2), pp. 151–164. (https://doi.org/10.1057/ejis.2009.8).

Brinton Anderson, B., Vance, A., Kirwan, C. B., Eargle, D., and Jenkins, J. L. 2016. "How Users Perceive and Respond to Security Messages: A NeuroIS Research Agenda and Empirical Study," *European Journal of Information Systems* (25:4), pp. 364–390. (https://doi.org/10.1057/ejis.2015.21).

Cram, W. A., Proudfoot, J. G., and D'Arcy, J. 2017. "Organizational Information Security Policies: A Review and Research Framework," *European Journal of Information Systems* (26:6), pp. 605–641. (https://doi.org/10.1057/s41303-017-0059-9).

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., and Baskerville, R. 2013. "Future Directions for Behavioral Information Security Research," *Computers & Security* (32), pp. 90–101. (https://doi.org/https://doi.org/10.1016/j.cose.2012.09.010).

Foth, M. 2016. "Factors Influencing the Intention to Comply with Data Protection Regulations in Hospitals: Based on Gender Differences in Behaviour and Deterrence," *European Journal of Information Systems* (25:2), pp. 91–109. (https://doi.org/10.1057/ejis.2015.9).

Herath, T., and Rao, H. R. 2009. "Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations," *European Journal of Information Systems* (18:2), pp. 106–125. (https://doi.org/10.1057/ejis.2009.6).

Hsu, C. W. 2009. "Frame Misalignment: Interpreting the Implementation of Information Systems Security Certification in an Organization," *European Journal of Information Systems* (18:2), pp. 140–150. (https://doi.org/10.1057/ejis.2009.7).

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), pp. 780–792. (https://doi.org/10.1057/palgrave.ejis.3000711).

Lukasik, S. 2011. "Why the Arpanet Was Built," *IEEE Annals of the History of Computing* (33:3), pp. 4–21. (https://doi.org/10.1109/MAHC.2010.11).

Maurer, T., and Morgus, R. 2014. "Compilation of Existing Cybersecurity and Information Security Related Definitions," *New America*.

Niemimaa, E., and Niemimaa, M. 2017. "Information Systems Security Policy Implementation in Practice: From Best Practices to Situated Practices," *European Journal of Information Systems* (26:1), pp. 1–20. (https://doi.org/10.1057/s41303-016-0025-y).

Niemimaa, M., and Niemimaa, E. 2019. "Abductive Innovations in Information Security Policy Development: An Ethnographic Study," *European Journal of Information Systems* (28:5), Taylor & Francis, pp. 566–589. (https://doi.org/10.1080/0960085X.2019.1624141).

Njenga, K., and Brown, I. 2012. "Conceptualising Improvisation in Information Systems Security," *European Journal of Information Systems* (21:6), pp. 592–607. (https://doi.org/10.1057/ejis.2012.3).

Ølnes, J. 1994. "Development of Security Policies," *Computers & Security* (13:8), Elsevier, pp. 628–636.

"SIGSEC." (n.d.). (https://communities.aisnet.org/sigsec/home, accessed January 21, 2020).

Siponen, M. T. 2001. "An Analysis of the Recent IS Security Development Approaches," in *Information Security Management: Global Challenges in the New Millenium*, IGI Global, pp. 101–124. (https://doi.org/10.4018/978-1-878289-78-0.ch008).

Siponen, M. T. 2005. "An Analysis of the Traditional IS Security Approaches: Implications for Research and Practice," *European Journal of Information Systems* (14:3), pp. 303–315. (https://doi.org/10.1057/palgrave.ejis.3000537).

Siponen, M., and Vance, A. 2014. "Guidelines for Improving the Contextual Relevance of Field Surveys: The Case of Information Security Policy Violations," *European Journal of Information Systems* (23:3), pp. 289–305. (https://doi.org/10.1057/ejis.2012.59).

von Solms, B., and von Solms, R. 2018. "Cybersecurity and Information Security – What Goes Where?," *Information &amp; Computer Security* (26:1), Emerald Publishing Limited, pp. 2–9. (https://doi.org/10.1108/ICS-04-2017-0025).

von Solms, R., and van Niekerk, J. 2013. "From Information Security to Cyber Security," *Computers & Security* (38), pp. 97–102. (https://doi.org/https://doi.org/10.1016/j.cose.2013.04.004).

Warkentin, M., and Willison, R. 2009. "Behavioral and Policy Issues in Information Systems Security: The Insider Threat," *European Journal of Information Systems* (18:2), Taylor & Francis, pp. 101–105. (https://doi.org/10.1057/ejis.2009.12).

Warman, A. R. 1992. "Organizational Computer Security Policy: The Reality," *European Journal of Information Systems* (1:5), pp. 305–310. (https://doi.org/10.1057/ejis.1992.2).