2022

A Decade in Review: Aligning Information Systems Security (ISS) with the NICE framework

Christopher Kreider

Omar El-Gayar

Aug 10th, 12:00 AM

A Decade in Review: Aligning Information Systems Security (ISS) with the NICE framework

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

Omar El-Gayar
Dakota State University, omar.el-gayar@dsu.edu

A Decade in Review: Aligning Information Systems Security (ISS) with the NICE framework

Completed Research

Christopher Kreider
Dakota State University
chris.kreider@trojans.dsu.edu

Omar El-Gayar
Dakota State University
omar.el-gayar@dsu.edu

Abstract

Information systems security (ISS) research has emerged increasing consistently since the 1970s through the 2000's with significant connections to the organizations, the users, and the technology. Work has been done to better understand what knowledge is necessary with developments such as the National Initiative for Cybersecurity Education (NICE) framework. As ISS research exists at the intersection of technology, people, and organizations, IS researchers are uniquely qualified to contribute to this burgeoning area. As we continue to contribute, we should do so mindfully of how it draws on our strengths, and contributes to the identity of the discipline, as well as the evolving nature subject matter. Utilizing the NICE framework, we perform a decade long assessment of ISS research within top IS journals. We identify major themes in ISS research, and identify gaps where future IS researchers may be able to contribute.

Keywords

Cybersecurity, Information Systems Security, NICE Framework

Introduction

One challenge to effective use of information systems are security related incidents, with current global cybersecurity costs estimated at $575 billion (Huigang et al. 2019). Additionally, cybersecurity implications can be broad, applying to individual users, organizations, and governments. Information security has also emerged in the past decade as a priority for organizations and governments, with jobs gap being identified whereby there are insufficient qualified individuals to fill the necessary positions (Kreider and Almalag 2019). Given the importance of information security to successful information systems, Zafar and Clark (2009) performed a review of security related literature across 9 top journals in the IS field starting in the 1970's. They found that the incidence of security related research increased through the decades, with 3 studies in the 1970s, 14 studies in the 1980s, 20 studies in 1990s, and 100 in the 2000s. This increase in research within this domain supports their contention "…that the information systems discipline can, and should contribute to information security research" (Zafar and Clark 2009,p. 572). Over a decade has passed since their detailed review was published, with significant advances in both the academic and practitioner worlds of cybersecurity occurring. Additionally, significant advances in terms of widely adopted frameworks for categorizing cybersecurity related topics have emerged, such as the National Initiative for Cybersecurity Education (NICE) framework. Extending the work of Zafar and Clark (2009), to include an additional 10 years of analysis categorized over a more recent and comprehensive framework can provide scholars unique insight into current trends in cybersecurity research within IS. The National Initiative for Cybersecurity Education (NICE) framework identifies seven key areas of cybersecurity, which are highlighted in table 1 below (Newhouse et al. 2017). Within each category in this framework, there are sub-categories, identifying specific activities and knowledge areas of which each of these categories are comprised. By using this framework, we will be able to organize the work of authors in the field along a framework that has emerged based on the market of knowledge and ideas necessary to be covered within the field. Finally, an additional category, the "meta" category has been identified, which coincides with the disciplines effort to self-regulate this area within the discipline and guide its further direction.

Category	Description
Securely Provision (SP)	Related to the conceptualization, design, procurement and/or building of secure information technology systems focusing on the system and/or network development
Operate & Maintain (OM)	Based on providing support, administration and maintenance that is required to ensure IT systems provide effective and efficient performance and security
Oversee & Govern (OV)	Relates to leadership, management, direction, development or advocacy that enables organizations to effectively conduct cybersecurity work
Protect & Defend (PR)	Performs identification, analysis and mitigation to threats to IT systems and/or networks that are within scope
Analyze (AN)	Enables evaluation and review of cybersecurity information as it arrives to determine its usefulness in the generation of intelligence.
Collect & Operate (CO)	Involved the collection of relevant cybersecurity information for the development of intelligence, as well as specialized operations involving denial and deception.
Investigate (IN)	Provides investigations into crimes and other cybersecurity events that are related to IT systems, their networks, and associated digital evidence

Table 1: NICE framework categories

This paper will provide several benefits, for scholars and practitioners. Scholars will be able to use the findings in this paper to identify emergent trends in ISS research over the prior decade, while also identifying new areas to contribute based on a more recent framework. Practitioners may use this to identify areas of research within the IS discipline that are directly related to current cybersecurity topics, skills, and knowledge, and the academic venues that cover these topics. The rest of this paper will be structured as follows. We will first provide an overview of the National Initiative for Cybersecurity Education (NICE) Cybersecurity framework. We will then provide a description of our methodology for this literature review, and categorization with the NICE framework. We will then summarize the literature found in the last decade, structuring it along the categories from this framework. Finally, we will discuss the implications for IS researchers, and the identity of the IS discipline, and draw conclusions from our work.

Methodology

The objective of this paper is twofold, to assess progress in IS security research compared to the prior decade, as reported by Zafar and Clark (2009), and assess the progress of the ISS research within the IS discipline with respect to an identity that boundary spans across a market of scholar and practitioner ideas at the intersection of human and technological endeavors (Lyytinen and King 2004). We have decided to replicate the journals reviewed by Zafar and Clark (2009), extending the review to the 10 years since their work. Additionally, limiting our review to these journals enables our review to be completed successfully given the wide scope of the topic of ISS as a whole, while building on the prior work. While existing reviews have been completed within this area, most reviews focus on small areas such as threat modeling (Xiong and Lagerström 2019), risk analysis in the cloud, block chain (Taylor et al. 2020), and usability of firewalls (Voronkov et al. 2017) to name a few. Additionally, To understand how the work identified relates to a current market of ideas in this area, we have chosen to use the more recent NICE framework, as the field has evolved since the prior work, and the NICE framework has emerged as a tool used by educators, professionals, and academics (Kim et al. 2018; Quiroz et al. 2021) for categorizing important knowledge areas within the field of security.

Specifically, we focus on the journals within this IS discipline as identified in the prior review. By focusing on these journals, we gain the ability 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 Communications of the Association for Information Systems (CAIS), European Journal of Information Systems (EJIS), Information & Management (I&M), Information Systems Journal (ISJ), Information Systems Research (ISR), Journal of the Association for Information Systems (JAIS), Journal of Information System Security (JISSEC), Journal of Management Information Systems (JMIS) and Management Information Systems Quarterly (MISQ) as shown in Table 2 below. For each of the journals selected, all articles in the selected time frame were collected. Each of the articles then had the title, keywords and abstract manually reviewed to identify any articles related to ISS. Once manual review of all articles was completed, a broad keyword search for the term "security" was performed across the same set of articles. This keyword search was not completed for the Journal of Information System Security (JISSEC), as all of the articles were related ISS. After completing our review, we first identified the

total number of articles in each journal that was identified via each of the classification methods: comprehensive manual search and keyword search.

Journal	CAIS	EJIS	I&M	ISJ	ISR	JAIS	JMIS	MISQ	JISSEC
Date Range Examined	Jan 2009 - Dec 2019								
Date Range Zafar and Clark (2009)	1999-2007	1993-2007	1977-2007	1991-2007	1990-2007	2000-2007	1984-2007	1977-2007	2005-2007

Table 2: Journals selected

The results of each search were then combined, with duplicates removed. Finally, all articles were manually reviewed again to ensure they were within the scope of this study, if necessary, reviewing the full text of the article. We used an inclusion criterion that the contribution of the article must be primarily related to security. This could either have been self-reported in the keywords, or assessed by reviewing the article to determine whether the subject matter fell under the "holistic view" of security including the people, the processes and the technology (Zafar and Clark 2009). Articles that were excluded include those that mentioned security in passing, where security concerns were a secondary factor, book reviews, tutorials, and editorials that mentioned security as part of a greater discussion. It is possible that an article was placed into two or more categories when the subject matter was clear such as with, "Top Management Support, External and Internal Organizational Collaboration and organizational flexibility in preparation for extreme events" (Skipper et al. 2009) was classified into the Cybersecurity Management and incident response.

Results

Overall, the search resulted in 311 articles that were categorized as relating ISS as shown in table 3.

Journal	Manual Search	Keyword Search (All)	Keyword Search (Kept)	Final Count
CAIS	23	53	35	37
EJIS	22	20	18	23
I&M	15	52	38	38
ISJ	9	18	10	9
ISR	17	27	19	21
JAIS	16	23	18	21
JMIS	20	32	23	29
MISQ	25	40	33	35
JISSEC	n/a	n/a	n/a	98
			Total	311

Table 3: Number of articles discovered during the literature review

The distribution of articles by journal in each of the 7 categories of the NICE framework is shown in table 4 while the following sub-sections summarizes the findings for each of these categories. Within each subsection, we provide an overview of the research trends. A selection of the articles is briefly categorized using the NICE framework.

Category	CAIS	EJIS	I&M	ISJ	ISR	JAIS	JMIS	MISQ	JISSEC	TOTALS
Securely Provision	10	4	2	1	2	3	2	4	35	63
Operate & Maintain	0	1	1	0	0	1	1	0	5	9
Oversee & Govern	14	9	35	8	18	10	15	22	19	150
Protect & Defend	2	0	5	1	3	2	2	4	18	37
Analyze	4	3	4	0	5	4	5	3	15	43
Collect & Operate	0	1	0	0	0	0	1	1	1	5
Investigate	0	0	0	0	0	0	2	1	3	6
Meta	5	4	0	0	0	1	0	0	6	16

Table 4: Total count of articles per journal in each category of the NICE framework

Securely Provision

The first category of the NICE framework specialty areas is Securely Provision (SP). The categories in this area align with many analysis and design related decisions necessary to securely prepare an information

system to fulfill its desired purpose. The sub-categories in the SP area include Risk Management (RSK), Software Development (DEV), System Architecture (ARC), Technology R&D (TRD), Systems Requirement Planning (SRP), Test and Evaluation (TST) and Systems Development (SYS). As shown in table 5, two categories emerge in the SP category: Risk Management and Tech R&D. Examples of research in the Risk category included exploring the risk of insider threats in applications (Wang et al. 2015) and an exploration of user participation in risk management (Spears and Barki 2010).

Risk Mgmt. (RSK)	Software Dev. (DEV)	Systems Arch. (ARC)	Tech R&D (TRD)	Systems Reqs. Planning (SRP)	Test& Eval (TST)	Systems Dev. (SYS)	Total
19	1	6	22	8	3	4	63

Table 5: Article counts in each subcategory of the securely provision (SP) category

The R&D category included research that sought to develop new security artifacts, or develop new enhancements such as an exploration of typing patterns as a biometric (Ngugi et al. 2012) or development and assessment of a new stream encryption algorithm (Barnawi et al. 2018). The remaining research identified was primarily associated with the role security played in the development, analysis and design of an information system, usually in a specific context such as healthcare.

Operate and Maintain

The *operate and maintain*_category of the NICE framework includes sub-categories pertaining to data administration (DTA), knowledge management (KMG), Customer Support and Technical Service (STS), Network Services (NET), Systems Administration (ADM) and Systems Analysis. As shown in table 6, within the operate and maintain category, the most frequently occurring research was related to Network services such as roaming user-based distributed firewalls explored by Luse et al. (2009) and firewalls for suspicious traffic (Week et al. 2011). Other research in this category focused on data administration such as data administration in the cloud (Tjoa et al.) and understanding the role of data in a breach (Sen and Borle 2015).

Data Admin. (DTA)	Knowledge Mgmt. (KMG)	Customer/ Tech. Support (STS)	Network Services (NET)	Systems Admin. (ADM)	Systems Analysis (ANA)	Total
3	0	0	5	0	1	9

Table 6: Article counts in each subcategory of the operate and maintain (OM) category

Oversee & Govern

Within the Oversee and Govern (OV) category of the NICE framework, subcategories included Legal Advice and Advocacy (LGA); Training, Education and Awareness (TEA); Cybersecurity Management (MGT); Strategic Planning and Policy (SPP); Executive Cyber Leadership (EXL); and Program/Program Management and Acquisition (PMA). As shown in table 7, research articles included in the OV fell into multiple broad categories: User's secure behaviors and compliance with policy, which was based off of the SPP and TEA categories and the security decisions within an organization and the relationship between market value and security decisions, which was grouped under MGT and EX. Examples in the MGT and EX categories include research exploring how to best frame security budget requests to get the best outcome (Beebe et al. 2014b) and understanding how security breaches impact firm value (Goel and Shawky 2009). Within the SPP and TEA categories, significant research explored information security policy adherence and education such as why users may choose to adhere to policy (Myyry et al. 2009), and understanding how the severity of sanctions relates to policy adherence (Chen et al. 2018), and better understanding security awareness training (Tsohou et al. 2015).

Legal Advice & Advocacy (LGA)	Training, Education and Awareness (TEA)	Cyber. Sec. Mgmt. (MGT)	Executive Cyber. Sec. Leadership (EXL)	Strategic Policy & Planning (SPP)	Prog./ Proj Mgmt and Acquisition (PMA)	Total
5	57	89	11	64	5	231

Table 7: Article counts in each subcategory of the oversee and govern (OG) category

Protect & Defend

The protect and defend category included the sub-categories cyber defense analysis (CDA), cyber defense infrastructure support (INF), incident response (CIR) and vulnerability and assessment management (VAM). Within the Protect and Defend category shown in table 8. The most common topic pertained to protection infrastructure such as intrusion detection/prevention (Goodall et al. 2009) and tools for detection and removal of undesirable software (Martins and Furnell 2011). The second most frequently appearing category relates to vulnerability and assessment management, such as patching (Temizkan et al. 2012) and mitigation techniques such as software diversity (Temizkan et al. 2018).

Cyber Def. Analysis (CDA)	Cyber Def. Infrastructure Support (INF)	Incident Response (CIR)	Vuln. Assessment & Mgmt. (VAM)	Total
3	17	5	11	36

Table 8: Article counts in each subcategory of the protect and defend (PR) category

Analyze

The analyze (AN) area of the NICE framework focused on a variety of analysis related activities including threat analysis (TWA) and target analysis (TGT). Additional categories identify other relevant areas of information security analysis including Exploitation Analysis (EXP) and Language Analysis (LA). Finally, All-source analysis (ASA) focuses on analyzing threat information from various locations including multiple sources, disciplines and agencies (Newhouse et al. 2017). Within the analyze section (table 9), the most frequent category represented pertained to threat analysis, followed by exploitation analysis. Topics in threat analysis included understanding deviant behavior (Chu et al. 2015), insider threats (Nicho and Kamoun 2014), and understanding hackers (Mookerjee et al. 2011). Exploitation analysis covered topics related to understanding malware propagation (Guo et al. 2016), social engineering (Nohlberg et al. 2011), and technically specific exploitation mechanisms, such as DNS tunneling (Born and Gustafson 2011).

Threat Analysis (TWA)	Exploitation Analysis (EXP)	All-Source Analysis (ASA)	Targets (TGT)	Language Analysis (LNG)	Total
22	14	6	3	0	45

Table 9: Article counts in each subcategory of the analyze (AN) category

Collect and Operate

The collect and operate categories included the sub-categories of collection operations (CO), cyber operations planning (OPL) and cyber operations (OPS).Within this category (table 10), research primarily studied complex cybersecurity planning operations such as how digital security service firms meet the contradictory goals of speed and accuracy (Salovaara et al. 2019).

Collection Operations (CLO)	Cyber Operations Planning (OPL)	Cyber Operations (OPS)	Total
0	3	1	4

Table 10: Article counts in each subcategory of the collect and operate (CO) category

Investigate

The investigate category contains two sub-categories which included cyber investigations (INV) and digital forensics (FOR). As shown in table 11, research in this category explored investigative and forensic related processes and tools, such as the DICE-E framework for researching the darknet (Benjamin et al. 2019), and forensic techniques related to deleted files (Schmidt and Condon 2011), and forensics on traditional hard drives (HDD) versus solid state drives (SSD) (Benusa et al. 2016).

Cyber Investigation (INV)	Digital Forensics (FOR)	Total
4	2	6

Table 11: Article counts in each subcategory of the Investigate (IN) category

Meta Research in ISS

The last category of research is concerned with research that does not necessarily align with the technical nature of the NICE framework. Most of this work was related to the internal processes that the IS community uses through the community of discourse to identify and discuss its boundaries. One such paper is the work of Siponen and Baskerville (2018) who discuss research relevance within information systems security (ISS) research, noting that the lack of intervention effectiveness that has been demonstrated may inhibit this research from achieving relevance in practice. Additionally, internal discussions within the field, such what is the definition of security (Chowdhuri and Dhillon 2012), assessment of academic outlets in the context of security (Beebe et al. 2014a), and systematic literature reviews (Nunes 2019) were included in this category.

Discussion

The results provide evidence of the emergent themes as this area of IS research continues to mature. Specifically, as seen in table 7, the Oversee and Govern (OG) category represents the persistent theme in the scholarly output, with much of the work relating to users' security behaviors and information security policy, with the ability to guide management and executive decision making. Additionally, there are several categories where research is beginning to emerge, specifically software related categories aligning along the analysis and design activities and analysis activities. In terms of the identity of the IS discipline, these areas align with what are generally thought to be core components of information systems, their development, functionality and operation.

Alternatively, there are several areas where research is limited. We believe this is not because information systems researchers cannot, or should not contribute to them, however, that they have not yet considered these as relevant areas. Specifically, the categories of Operate and Maintain (OM), Collect and Operate (CO), and Investigate (IN) show limited research in the IS area. It is likely that these areas are already covered by other disciplines, including computer science and law. However, each of these areas should have unique interplay where IS scholars can provide unique insight and contribution. Based on the total number of each category, we find that, 1 of the 7 categories in the NICE frameworks is strongly represented, 3 of the categories are lacking and 3 are severely limited in their representation ISS research, briefly discussed below.

One category, Oversee & Govern (OV) was well represented, accounting for over 45% of identified research. This research represents subcategories pertaining to management, policy, and user awareness/education to name a few. These areas of research align well with the interdisciplinary nature of IS research, with a strong focus on organizations, organizational decision making, and users. Of the remaining categories, which will be focused on in the research agenda below, some have been covered more than others.

We identify three categories of the NICE framework that IS information security research has addressed, moderately, but significantly less the Oversee and Govern category. Specifically, the categories of Securely Provision (SP), Protect & Defend (PR) and Analyze (AN). Each of these categories is discussed below with suggestions for future research.

The Securely Provision category covers activities related to the initiation of an information system, including risk management (RSK) software development (DEV), system architecture (ARC), Technology Research and Development (TRD), Systems Requirements Planning (SRP), Test and Evaluation (TST) and Systems Development (SYS). In the prior decade, key gaps were identified in the areas of Test and Development, with less contributions in this area. Activities, such as software development, system architecture, and testing represented 5 of the total articles categorized. Finally, activities such as risk management and systems requirements planning had the highest representation within this category with a total of 24 categorized articles. While overall, the entire category of Securely Provision represents a small portion of overall research, there are categories that emerge as dominant, including risk management and

systems requirements planning. These tasks, generally higher-level planning activities leading to lower-level activities such as systems development and system architecture, the next lower categorization. Finally. Low level activities such as test development and testing seemed to be unrepresented in the literature explored. As IS scholars seek to develop research that is both rigorous and relevant, attempts to apply existing research method specializations in this area is seen as potentially fruitful, with the potential to extend existing theories and methodologies pertaining to software development, to security specific contexts.

The protect and Defend category identifies subcategories that pertain to the cyber-defensive and protective related tasks including the following: Cybersecurity Defense Analysis (CDA), Cybersecurity Defense Infrastructure Support (INF), Incident Response (CIR) and Vulnerability Assessment and Management (VAM). In our literature review, 36 of the articles reviewed contained content that covered by this category, approximately 11%. Researchers in IS could look to apply theories applied to other areas of software development, and even protection related theories, usually applied at the organizational level, to security related research. We see significant potential to extend IS research into this category without a loss of rigor, identity, and potential to increase relevance of IS research.

The Analyze category has several sub-categories, including Threat Analysis (TWA). Exploitation Analysis (EXP), All-Source Analysis (ASA), Targets (TGT) and Language Analysis (LNG). The 45 articles identified in our review represent approximately 13% of all articles explored. This is significantly more than the several of the categories which accounted for 5% or less of the reviewed research, but significantly less than the dominant theme of Oversee & Govern which accounted for > 45%. As this category is emerging in IS research, we believe researchers can further extend existing methodologies and theories to cover subsets of this category, specifically all-source-analysis, which is the interdisciplinary example of security analysis crossing sources, disciplines and agencies with the goal of placing information in context and drawing insight and implications. Additionally, exploitation analysis (EXP), specifically social engineering as an exploitation vector is identified as an area lacking in IS research, that IS researchers should be qualified and capable of contributing to.

The following categories of Research, Operate & Maintain (OM), Collect and Operate (CO) and Investigate (IN) respectively represented approximately 5% or less of the research summarized above. We find this surprising as two of these categories, OM and CO appear on the surface to align with IS priorities in IS research. We briefly summarize each of these categories below, and provide insight into potential research that could be explored in each of these areas.

The Operate and Maintain Category, accounting for ~ 2% of research explored, contains subcategories pertaining to the following: Data Administration (DTA), Knowledge Management (KMG), Customer Support and Technical Service (STS), Network Services (NET), Systems Administration (ADM) and Systems Analysis (ANA). We recognize that several of these categories address more technical issues, likely more relevant as topics in computer science or software engineering. There are, however, several categories that seem ripe for IS researchers to explore further, applying existing methodologies and theories to security specific applications, specifically Analysis, Customer Support and Knowledge Management.

Collect and Operate, in the NICE framework, includes categories such as collection operations (CLO), Cyber Operations Planning (OPL) and Cyber Operations (OPS). We see this area being highly specialized to cybersecurity, with many technical components. Within this category, we identify Cyber Operations Planning as an area that IS researchers could extend existing methodologies and theories to while preserving the identity characteristics of the IS Discipline (Lyytinen and King 2004).

The final category in the NICE framework, investigate, has two sub-categories Investigation and Digital Forensics. Of the 7 categories in this framework, this is the smallest, however, we still believe that IS researchers have potential to contribute to this area. Specifically, as researchers we are all investigators. As investigators specifically trained in investigating IS related phenomena, and as information security has been identified as a prevalent theme in IS researcher, researchers should explore opportunities to apply the tools and theories used in other IS areas of research, to the investigation phased of information security.

Conclusions

The discipline of IS has made marked increases in information security output over the prior decade, marked by an ~200% increase in the decade since the review of Zafar and Clark (2009), with an increase from 100 to ~300. Compared to the prior decade which saw a 400% increase from 20 to 100, this represents a stabilization of the information security research within IS research. While this progress is promising, there are still several areas for improvement that IS researchers in the information security realm can explore entering the next decade. Specifically, by using a framework, structured around organizational goals and objectives, such as the NICE framework, ISS researchers may identify relevant areas to apply existing IS theories and methodologies to better explore, specifically, with categories such as Collect & Operate and Investigate, which accounted for approximately 3% of all work reported on.

Another potential direction for future work could be the extension of more general research into security specific contexts. For example, sub-categories such as Knowledge Management and Data Administration showed low number of related studies, topics commonly researched in IS scholarly work. This may be primarily due to the search terms and focus of this paper, which focused on information system security (ISS) research, and as such, may have omitted papers on knowledge management and data administration in the general term.

Finally, ISS researchers going forward could use a framework, such as the NICE framework, to better categorize and assess the quality of the work within this subspecialty of IS research. Specifically, researchers may be able to explore issues with theoretical convergence (Cram et al. 2019), or lack of quality with respect to current best practices and professional insight (Siponen and Baskerville 2018).

This paper has a number of limitations. First, this review relied on a relatively simple search, “security” in the abstract, coupled with a manual review of every article title/abstract for the selected articles. It is possible that some articles were missed. The number of articles missed would have been small given the manual review of every article title and abstract within the time frame, and given the clear emergence of the themes of research in the area, would be unlikely to compromise the validity of the findings. Secondly, there were several times when a study would seem to fit in multiple categories. For simplicity, we would try to categorize with the best fit, especially when it fit within an emerging themes. Work that espoused multiple categories would need to provide significant contribution above and beyond the emergent theme if present to be categorized in the alternative categories. There were a number of studies that were categorized into multiple categories, specifically with topics related to user awareness training, management and security policy as these three topics are frequently covered in ISS research, and are closely related. Finally, in this version of the paper, only some of the articles within each category are summarized.

References

Barnawi, M., Alajmi, S., and Mai, B. 2018. "A Hive Stream Encryption (Hse): A New Stream Encryption Algorithm," *Journal of Information System Security* (14:2).

Beebe, N., Clark, J., Chang, F., and Padmanabhan, P. 2014a. "Ranking Publication Outlets for Information Security Research," *Journal of Information System Security* (10:2).

Beebe, N. L., Young, D. K., and Chang, F. R. 2014b. "Framing Information Security Budget Requests to Influence Investment Decisions," *Communications of the Association for Information Systems* (35:1).

Benjamin, V., Valacich, J. S., and Hsinchun, C. 2019. "Dice-E: A Framework for Conducting Darknet Identification, Collection, Evaluation with Ethics," *MIS Quarterly* (43:1), pp. 1-22.

Benusa, A., Jeganathan, S., and Schmidt, M. 2016. "Forensic Analysis Challenges: Shifting from Hdd to Ssd Storage," *Journal of Information System Security* (12:3).

Born, K., and Gustafson, D. A. 2011. "Detecting and Visualizing Domain-Based Dns Tunnels through N-Gram Frequency Analysis," *Journal of Information System Security* (7:2).

Chen, X., Wu, D., Chen, L., and Teng, J. K. L. 2018. "Sanction Severity and Employees' Information Security Policy Compliance: Investigating Mediating, Moderating, and Control Variables," *Information & Management* (55:8), pp. 1049-1060.

Chowdhuri, R., and Dhillon, G. 2012. "Understanding Information Security," *Journal of Information System Security* (8:2).

Chu, A. M. Y., Chau, P. Y. K., and So, M. K. P. 2015. "Developing a Typological Theory Using a Quantitative Approach: A Case of Information Security Deviant Behavior," *Communications of the Association for Information Systems* (37:1).

Cram, W. A., D'Arcy, J., and 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), pp. 525-554.

Goel, S., and Shawky, H. A. 2009. "Estimating the Market Impact of Security Breach Announcements on Firm Values," *Information & Management* (46:7), pp. 404-410.

Goodall, J. R., Lutters, W. G., and Komlodi, A. 2009. "Supporting Intrusion Detection Work Practice," *Journal of Information System Security* (5:2), pp. 42-73.

Guo, H., Cheng, H. K., and Kelley, K. 2016. "Impact of Network Structure on Malware Propagation: A Growth Curve Perspective," *Journal of Management Information Systems* (33:1), pp. 296-325.

Huigang, L., Yajiong, X., Pinsonneault, A., and Yu, W. 2019. "What Users Do Besides Problem-Focused Coping When Facing It Securty Threats: An Emotion-Focused Coping Perspective," *MIS Quarterly* (43:2), pp. 373-394.

Kim, K., Smith, J., Yang, T. A., and Kim, D. J. 2018. "An Exploratory Analysis on Cybersecurity Ecosystem Utilizing the Nice Framework," *2018 National Cyber Summit (NCS)*: IEEE, pp. 1-7.

Kreider, C., and Almalag, M. 2019. "A Framework for Cybersecurity Gap Analysis in Higher Education," in: *Southern Association for Information Systems*. St. Simons Island, GA.

Luse, A., Scheibe, K. P., and Townsend, A. M. 2009. "Addressing Internal Security Threats with Roaming User-Based Distributed Firewalls," *Journal of Information System Security* (5:2).

Lyytinen, K., and 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), pp. 220-246.

Martins, W., and Furnell, S. 2011. "Comparing the Effectiveness of Antispyware Removal Tools," *Journal of Information System Security* (7:2).

Mookerjee, V., Mookerjee, R., and Bensoussan, A. 2011. "When Hackers Talk: Managing Information Security under Variable Attack Rates and Knowledge Dissemination," *Information Systems Research* (22:3), pp. 606-623.

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., and Vance, A. 2009. "What Levels of Moral Reasoning and Values Explain Adherence to Information Security Rules? An Empirical Study," *European Journal of Information Systems* (18:2), pp. 126-139.

Newhouse, W., Keith, S., Scribner, B., and Witte, G. 2017. "National Initiative for Cybersecurity Education (Nice) Cybersecurity Workforce Framework," *NIST Special Publication* (800), p. 181.

Ngugi, B., Wu, D., and Frank, J. 2012. "Biometric Keypad Reliability: Stability of Typing Patterns and Authentication Accuracy," *Journal of Information System Security* (8:3).

Nicho, M., and Kamoun, F. 2014. "Multiple Case Study Approach to Identify Aggravating Variables of Insider Threats in Information Systems," *Communications of the Association for Information Systems* (35:1).

Nohlberg, M., Wangler, B., and Kowalski, S. 2011. "A Conceptual Model of Social Engineering," *Journal of Information System Security* (7:2).

Nunes, S. 2019. "Information Security Risk Management: A Systematic Literature Review," *Journal of Information System Security* (15:3).

Quiroz, J. T., Oscategui, M. A. A., and Armas-Aguirre, J. 2021. "Cybersecurity Taxonomy: Research and Knowledge Areas," *2021 IEEE 1st International Conference on Advanced Learning Technologies on Education & Research (ICALTER)*: IEEE, pp. 1-4.

Salovaara, A., Lyytinen, K., and Penttinen, E. 2019. "High Reliability in Digital Organizing: Mindlessness, the Frame Problem, and Digital Operations," *MIS Quarterly* (43:2), pp. 555-578.

Schmidt, M. B., and Condon, M. J. 2011. "Computer Forensics: Examining the Effectiveness of File Deletion," *Journal of Information System Security* (7:3).

Sen, R., and Borle, S. 2015. "Estimating the Contextual Risk of Data Breach: An Empirical Approach," *Journal of Management Information Systems* (32:2), pp. 314-341.

Siponen, M., and 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), pp. 247-265.

Skipper, J. B., Hall, D. J., and Hanna, J. B. 2009. "Top Management Support, External and Internal Organizational Collaboration, and Organizational Flexibility in Preparation for Extreme Events," *Journal of Information System Security* (5:1).

Spears, J. L., and Barki, H. 2010. "User Participation in Information Systems Security Risk Management," *MIS Quarterly* (34:3), pp. 503-A505.

Taylor, P. J., Dargahi, T., Dehghantanha, A., Parizi, R. M., and Choo, K.-K. R. 2020. "A Systematic Literature Review of Blockchain Cyber Security," *Digital Communications and Networks* (6:2), pp. 147-156.

Temizkan, O., Kumar, R. L., Park, S., and Subramaniam, C. 2012. "Patch Release Behaviors of Software Vendors in Response to Vulnerabilities: An Empirical Analysis," *Journal of Management Information Systems* (28:4), pp. 305-338.

Temizkan, O., Park, S., and Saydam, C. 2018. "Software Diversity for Improved Network Security: Optimal Distribution of Software-Based Shared Vulnerabilities," *Information Systems Research* (29:4), pp. 828-849.

Tjoa, A., Huemer, D., Descher, M., Masser, P., and Feilhauer, T. "" On Retaining Data Control to the Client in Infrastructure Clouds"; Journal of Information System Security, 5 (2009), 4; S. 27-46,").

Tsohou, A., Karyda, M., Kokolakis, S., and Kiountouzis, E. 2015. "Managing the Introduction of Information Security Awareness Programmes in Organisations," *European Journal of Information Systems* (24:1), pp. 38-58.

Voronkov, A., Iwaya, L. H., Martucci, L. A., and Lindskog, S. 2017. "Systematic Literature Review on Usability of Firewall Configuration," *ACM Computing Surveys (CSUR)* (50:6), pp. 1-35.

Wang, J., Gupta, M., and Rao, H. R. 2015. "Insider Threats in a Financial Institution: Analysis of Attack-Proneness of Information Systems Applications," *MIS Quarterly* (39:1), pp. 91-A97.

Week, J., Ivanova, P., Week, S., and McLeod, A. 2011. "A Firewall Data Log Analysis of Unauthorized and Suspicious Traffic," *Journal of Information System Security* (7:3).

Xiong, W., and Lagerström, R. 2019. "Threat Modeling–a Systematic Literature Review," *Computers & security* (84), pp. 53-69.

Zafar, H., and Clark, J. G. 2009. "Current State of Information Security Research in Is," *Communications of the Association for Information Systems* (24:34), pp. 557-596.