Journal of Strategic Information Systems 30 (2021) 101693

Contents lists available at ScienceDirect

Journal of Strategic Information Systems

journal homepage: www.elsevier.com/locate/jsis

Information systems security research agenda: Exploring the gap between research and practice

Gurpreet Dhillon [a,*], Kane Smith [b], Indika Dissanayaka [b]

[a] *Information Technology and Decision Sciences Department, G. Brint Ryan College of Business, University of North Texas, Denton, TX 26203, United States*

[b] *Information Systems and Supply Chain Management Department, Bryan School of Business & Economics, UNC Greensboro, Greensboro, NC 27402, United States*

ARTICLE INFO

Keywords:
Information Systems Security Research
Delphi Study
Topic Modeling
Literature Review

ABSTRACT

This paper undertakes a systematic review of the Information Systems Security literature. The literature review consists of three parts: First, we perform topic modeling of major Information Systems journals to understand the field's debates. Second, we conduct a Delphi Study composed of the Chief Information Security Officers of major corporations in the US to identify security issues that they view as important. Third, we compare Topic Modeling and the Delphi Study results and discuss key debates, gaps, and contradictions within the academic literature. Further, extant Information Systems Security literature is reviewed to discuss where the academic community has placed the research emphasis and what is now required in the discipline. Based on our analysis, we propose a future agenda for Information Systems security research.

Introduction

Information Systems (IS) Security has long been a concern for both academics and practitioners. As a Forbes[1] article notes, "if recent global security breaches impacting over 200,000 computers in 150 countries and costing millions are anything to go by, it could not be clearer that cybersecurity impacts businesses as a whole, not just IT departments." Businesses have therefore recognized IS security to be a strategic issue. Practitioners[2] have argued that there is a "disconnect between an organization's risk-management efforts and the development of necessary cybersecurity capabilities." It is therefore essential to review state of the art in terms of academic efforts and practitioner perspectives. Over the years an extensive body of academic research has been built around the need for protecting vital technical systems and the information contained within them. However, over the last several decades, this body of IS security research has evolved with technology in numerous ways. For instance, see Ande et al (2020), who sketch the evolution of technologies and related IS security challenges. This evolution creates a great deal of difficulty for researchers seeking to identify under-represented aspects of IS security research to ensure all relevant areas of concern are addressed. For instance, research into studying just malware has evolved into the study of self-propagating malware; today ransomware isn't only for ransom, but adversaries are trying to destroy systems and data, while also stepping up their evasion capabilities; and phishing attacks are becoming a

* Corresponding author.
E-mail addresses: gurpreet.dhillon@unt.edu (G. Dhillon), Kjsmith9@uncg.edu (K. Smith), i_dissan@uncg.edu (I. Dissanayaka).

[1] https://www.forbes.com/sites/edelmantechnology/2017/10/11/cyber-security-is-a-business-risk-not-just-an-it-problem/#7445cb9f7832. Accessed 9 May 2020.

[2] https://www.bain.com/insights/why-cybersecurity-is-a-strategic-issue/ Accessed 7 July 2021.

https://doi.org/10.1016/j.jsis.2021.101693

Available online 8 October 2021

significant threat vector. In an interesting study, Eder-Neuhauser et al (2018) simulate the propagation of an endemic malware. The authors also present a comparison of the three types of malwares – endemic, pandemic, and contagion, to develop a threat matrix for a smart grid. The study has important lessons for a balance between establishing adequate controls and the ever-changing nature of infections. The 2021 Colonial Pipeline[3] ransomware attack is illustrative of the case where consideration of evolving threats was not suitably addressed. The 2017 Equifax breach is also an interesting case in point. While originally construed as a data breach resulting in identity theft, it soon became clear that it was indeed a case of cyberterrorism and possibly espionage[4]. For reasons such as these, the research presented in this paper seeks to discern where our field has previously been, where it is currently at, and prognosticate where we believe it should be heading to maximize its valuable contributions to IS security.

For the purpose of our study, we restrict our review to the field of Information Systems. The topic of security has also been well researched in Computer Science, where the emphasis has been more on the algorithmic aspects. In the literature, different terms have occasionally been used to refer to IS security. These include cybersecurity, information security, and computer security. While sometimes the authors use them interchangeably, our review is limited to only IS security (as originally proposed by Baskerville, 1993; Dhillon and Backhouse, 2001; Siponen, 2005; among others). To establish conceptual clarity, we adopt the classic definition of IS security from Dhillon (1997), who notes that IS security is related to maintaining the integrity of the technical, formal, and informal aspects of an information system. Dhillon (2007) also notes, “it goes without saying that the wealth of our society is a product of our ability to organize, and this ability is realized through information handling …which occurs at the technical, formal and informal level” (p. 3). Consequently, IS security is the protection of information handling at the technical, formal, and informal levels. Similar conceptualizations of information systems and security have been presented in the extant literature (e.g., see Bostrom and Heinen 1977, Luse et al. 2013, Samonas and Coss 2014, among others).

An overview of prior IS security literature reviews

The body of knowledge regarding IS security research has continued to evolve since the work of Baskerville (1993), Dhillon and Backhouse (2001), and Siponen (2005). These three works were comprehensive assessments of the literature, and each prognosticates future directions of research for the field. In our review, we also uncovered two additional holistic reviews of IS security research, McFadzean et al. (2006) and Siponen and Oinas-Kukkonen (2007), which are extensions of Dhillon and Backhouse (2001) and Siponen (2005), respectively. Since Siponen and Oinas-Kukkonen (2007), all additional literature reviews in IS security research have only been focused on specific streams of research (e.g., compliance) within the field instead of all-encompassing assessments of the direction of IS security research.

Duality in security design

The first IS security literature review, presented by Baskerville (1993), conceptualizes IS security as a model composed of three generations that are linear with respect to time and progress. Each of these generations is composed of both methods as well as different objectives, means, challenges, and intellectual assumptions that are used to distinguish them from one another. Baskerville terms the first generation as Checklist methods that first appeared in the early 1970s with the purpose of mapping limited solutions onto an information problem. The security aspect of this generation was accomplished through the use of checklists and risk analysis and was usually based on a product vendor’s literature. The second generation is termed as mechanistic engineering methods, appearing first in the early 1980s, which evolved from the first generation to create a partitioned complex solution that matched functional requirements. System development methods for this generation include top-down engineering and rapid prototyping. Security tools for this generation often consisted of control points and exposure matrices. The last generation conceptualized by Baskerville is the third generation of logical transformational methods, which consists of highly abstracted design that expresses problem and solution space. Some typical development methods and tools for this generation are structured analysis data modeling and entity-relationship diagrams, while typical security tools are logical controls design and data flow diagrams.

Based on his review, Baskerville (1993) presents three different concerns about security. First, Baskerville argues that management of IS security adopts a mechanistic partitioning of complexity approach. Second, there is an emphasis on a minimum set of controls to satisfy protection requirements. Third, there is a prevalence of development duality. Baskerville claims that information systems design simply deals with security as an add-on to the overall design. He suggests instead that information systems design should comprehensively include all aspects of security from the onset.

Paradigmatic view of IS security research

In the literature review by Dhillon and Backhouse (2001) and McFadzean et al. (2006), a paradigmatic view of IS security research is adopted. The literature review is based on a basic premise, drawn from Burrell and Morgan (1979) that “all theories of organization rely upon a philosophy of science and a theory of society” (p. 1). Therefore, Dhillon and Backhouse (2001) classify the IS security literature within the four paradigms - functionalist, interpretive, radical humanist, and radical structuralist.

The main contribution of the Dhillon and Backhouse (2001) security literature review is the identification of three problematic

[3] https://www.nytimes.com/2021/05/13/us/politics/biden-colonial-pipeline-ransomware.html. Accessed July 1, 2021.

[4] https://www.fbi.gov/news/stories/chinese-hackers-charged-in-equifax-breach-021020. Accessed 9 May 2020.

issues regarding the nature of the research they reviewed. The first concern suggests that security approaches grounded in functionalism provide a very narrow view of security for organizations (p. 138). Dhillon and Backhouse observed that strict boundaries can preclude examination of security controls outside of the boundaries that should be considered equally relevant to those controls within the boundaries. They also posit that IS security management is conceptualized as processes and thus security evaluation primarily focuses on input, throughput, output, and feedback, which completely ignores the human and asocial element of IS security. In short, the scope of IS security analysis is very specific and very granular, which leads to another problem identified by Dhillon and Backhouse – lack of customizability.

A one-size-fits-all approach to security management is patently ineffective; this is the second shortcoming of IS security literature identified by Dhillon and Backhouse. As previously discussed, the heavy focus on functionalism has sufficiently predicated the academic nature of IS security on checklists, risk analysis, and evaluation. The third concern expressed by Dhillon and Backhouse (2001) is that highly structured methodologies are insufficient because they are impractical and offer little value to practitioners outside of the organizations and hierarchies they were originally designed for (e.g., the military). They suggest, "…risk analysis, rooted in the functionalist paradigm, is extremely useful for evaluating security, but it cannot form the basis of an entire security strategy," and "traditional evaluation methods can be useful in assessing the extent of security, but a corporate strategy to prevent the occurrence of negative events cannot be based on the highly structured security evaluation criteria" (p. 147). Given these three primary concerns, Dhillon and Backhouse suggest that the way forward with respect to the field of IS security is toward an interpretive, socio-organizational perspective. As is evident in their literature review, socio-organizational perspectives were not prevalent prior to and up through 2001.

Re-evaluating the generational view

In a review by Siponen (2005), he posits that while scholars have developed several modern methods, yet the traditional approaches such as checklists, standards, maturity criteria, risk management, and formal methods, still dominate research. The review attempts to make sense of these traditional security methods by comparing their key underlying assumptions. One of the key findings presented in the literature review was that there is relatively little evidence on the use of the later-generation methods in practice (as originally proposed by Baskerville, 1993). Thus, suggesting that despite the development duality problems identified in 1993 by Baskerville, little progress had been made over the following decade. To understand the underlying root cause of the aforementioned phenomenon, Siponen (2005) shows that the flood of available methods forms a pressure on practitioners to understand their variances. This perception lacks the needed understanding of the underlying assumptions behind the methods leading to the continuous development of methods that are based on "repeating certain undesirable assumptions" (p. 304). The solution proposed by Siponen (2005) is similar to what was suggested by Dhillon and Backhouse (2001). Siponen (2005) makes a call to not rely exclusively on technical methods and highlights the "importance of the socio-organizational nature of IS [information systems] … [and] consequently, the need for social ISS [information systems security] methods" (p. 314).

Duality in secure systems development is succinctly defined by White and Dhillon (2005) as resulting when an "information system and its security are designed, built and implemented into an organizational environment separately, allowing for the possibility of conflict between a system's functionality and its security." System developers continue to consider security as an afterthought in terms of having different priorities between security goals and information use (Karlsson et al. 2017), or even when the proposed system sees resistance to security implementation (Albrechtsen 2007). Spagnoletti and Resca (2008) characterize such duality in terms of a "drift" - when the technological system does not match the original design. As originally conceptualized by Baskerville, evidence of development duality prevails, and several studies point to this fact (e.g., see Paananen et al. 2020).

In subsequent years other IS security scholars while acknowledging the problem of duality, have made calls for an understanding of human factors in the analysis, design, and management of IS security. Notable among these are Hitchings (1995) as well as Furnell and Clarke (2012). Scholars have also explored or made calls to study aspects around behavioral IS security (e.g., Crossler et al. 2013). However, in a 2001 literature review paper, Dhillon and Backhouse (2001), very succinctly ask for future studies to incorporate social and organizational factors in IS security research. The social and organizational factors subsume the human and behavioral aspects. In subsequent years the need for considering such factors was reiterated by McFadzean et al. (2006), Siponen (2005), and Siponen and Oinas-Kukkonen (2007). Many other researchers have recognized the inherent organizational challenges, particularly as these relate to compliance with policies (e.g., see Karjalainen et al. 2019).

In another later review, Siponen and Oinas-Kukkonen (2007) identify four security issues – access to information systems, secure communication, security management, and development of secure information systems, with their work examining the extent to which these security issues have been addressed by existing academic efforts. Research contributions concerning these four security issues were analyzed from three viewpoints: a meta-model for information systems, the research approaches used, and the reference disciplines used. The security conceptualizations put forward by Siponen and Oinas-Kukkonen (2007) are placed in terms of levels and then classified in terms of security requirements. All four security concerns are dealt with on three levels: technical, conceptual, and organizational. The survey of IS security research by Siponen and Oinas-Kukkonen (2007) reveals that most research has focused on the technical context and issues of access to information systems and secure communication. Based on this analysis, they suggest new directions for studying IS security from an information systems viewpoint, with respect to research methodology as well as research questions. Further, they claim empirical studies about the issues of security management and the development of secure systems based on suitable reference theories are particularly necessary.

Table 1 summarizes the main findings of the IS security literature until 2007. The literature reviews surveyed prominent IS security research in the field – each providing a different characterization of the research. Baskerville (1993), for example, looked at the

Table 1
Summary of historical overview of IS security research (until 2007).

Literature review	Approach Used	Main Contribution
Baskerville (1993): Information systems security design methods: implications for information systems development	Uses a temporal perspective. Established generation of systems development and security design.	Makes a call to move away from mechanistic approaches to designing security. Defined the problem of duality in secure system design.
Dhillon and Backhouse (2001): Current directions in IS security research: towards socio-organizational perspectives	Classified literature using sociological paradigms focusing on ontological and epistemological origin of approaches.	Makes a call to move away from purely functionalist approaches. Urges to adopt a socio-organizational and a socio-technical orientation.
Siponen (2005): An analysis of the traditional IS security approaches: implications for research and practice	Uses a temporal perspective. Extends Baskerville's (1993) generations of secure development.	Makes a call for considering social aspects in IS security approaches.
Siponen and Oinas-Kukkonen, (2007): A review of IS security issues and respective research contributions	Identifies security issues (access, secure communication, management, and development) and then analyzes the literature.	Identifies most research to be in the area of access and secure communication. Makes a call for using reference theories to study security management and development.

literature from a temporal perspective and prescribed an evolutionary taxonomy to accommodate the changes in the research field as information system utilization, purpose, and application evolved. Dhillon and Backhouse (2001) took a different approach, where they classified various information systems security research into four paradigmatic categorizations and made a call for a socio-organizational understanding of IS security problems. Siponen and Oinas-Kukkonen (2007) extended Baskerville's conceptualization, adding new evolutions (generations) of security research while maintaining a temporal view on the body of research. Each conceptualization of security provided a different lens by which the field, on the whole, may be viewed and understood.

Content analysis of IS security research

In this section, we discuss the methodology used and evaluate the content of IS security research. First, we present the methodology. Second, the content of IS security research and the emergent themes is discussed.

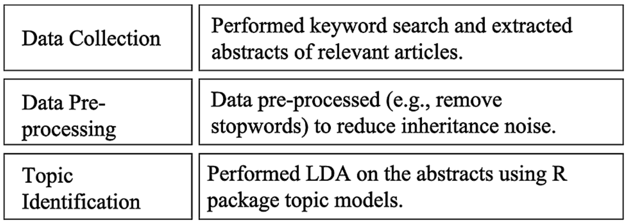
Methodology used to identify researched IS security topics

The objective of topic modelling is to discover hidden thematic structures in a collection of documents. The Latent Dirichlet Allocation (LDA) algorithm (Blei et al. 2003) has become a popular means to conduct topic modeling studies. LDA uses a statistical generative model that assumes each word in a document is generated in a two-step process. First, a topic is randomly drawn based on the topic distribution in the document. Second, a word is randomly drawn based on the word distribution of the topic in the document. The process is iteratively applied till the time the observed words in the document find the best set of variables describing the topic and word distributions. A detailed description of the technique can be found in Blei et al and the application appears in several IS research studies, including (Huang et al. 2018).

In undertaking a literature review, we used the topic modeling approach to unravel key latent themes in the burgeoning academic IS security literature. A three-step approach to operationalize topic modeling was utilized (see Fig. 1). First, we performed a keyword search using relevant search terms[5] to extract abstracts from the Scopus database. Our search was limited to abstracts, titles, and author keywords of articles published between January 1990 to January 2020 in information management journals with ratings 3 or higher in the academic journal guide 2018 published by the Chartered Association of Business Schools (CABS). In addition, we also included *Information and Computer Security* journal, which is a CABS 2, but one of the few information systems security-specific journals. Our initial search yielded 2283 articles. We manually evaluated and removed abstracts of unrelated articles (e.g., financial securities, national security, homeland security, etc.). Our final sample consisted of 2129 abstracts. Based on our sample, we noticed that the number of security-related articles in academia grew at a very slow rate until 2006 and increased dramatically thereafter.

The collected data (abstracts) were pre-processed to remove irrelevant and noisy data. Pre-processing steps include converting text to lower case, removing punctuation and numbers, removing frequently occurring stop words (e.g., "the", "a", "are", "of"), and lemmatization to reduce the inflectional form of a word to a base/dictionary form (lemma). Finally, we conducted topic modeling with the LDA algorithm to identify latent themes in those articles' abstracts (Blei et al. 2003). The LDA algorithm requires the number of topics to be prespecified as an input parameter. This is not easy to determine as a high value could lead to more meaningless topics, while a low value could eliminate more important topics. We calculated the optimum number of topics using four algorithms: two minimization algorithms proposed by Cao et al. (2009) and Arun et al. (2010); as well as two maximization algorithms proposed by Griffiths and Steyvers (2004) and Deveaud et al. (2014). Based on these algorithms, the suggested optimum number is noted as 23 (see Fig. 2). Therefore, we extracted 23 topics using LDA implemented in the R topicmodels package.

[5] *security* OR *privacy* OR cyberaggression OR cybercrime OR cyberdeviance OR cyberinsurance OR cyberloafing OR cyberslacking OR cyberrisk OR confidentiality OR integrity OR authentication OR non-repudiation OR encryption OR cryptography OR "denial of service" OR hacking OR firewall OR "access control" OR phishing



Data Collection	Performed keyword search and extracted abstracts of relevant articles.
Data Pre-processing	Data pre-processed (e.g., remove stopwords) to reduce inheritance noise.
Topic Identification	Performed LDA on the abstracts using R package topic models.

Fig. 1. Sequence of topic modeling methodological steps.

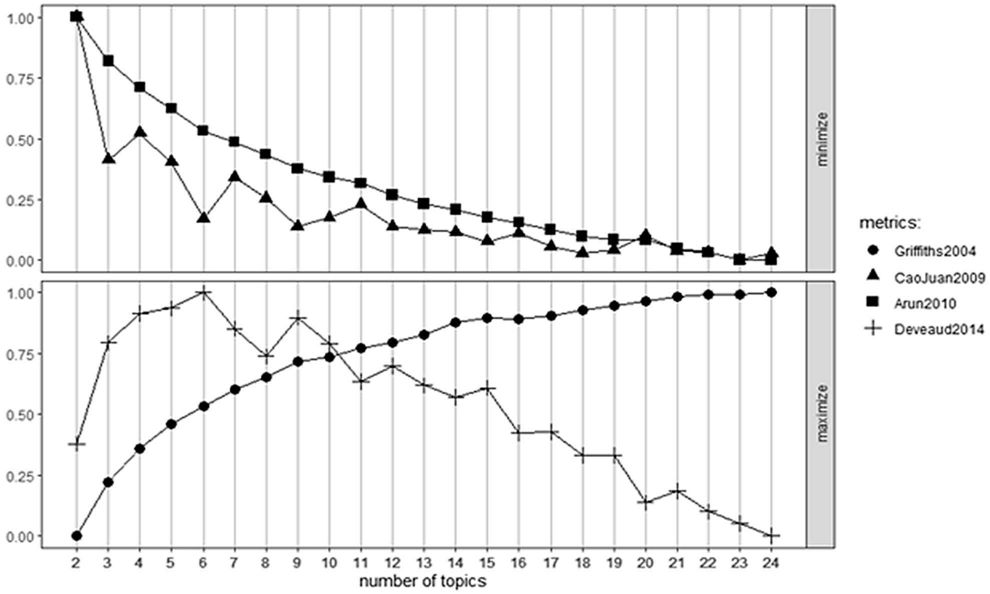


Fig. 2. Optimal Number of Topics.

We then manually evaluated these 23 topics and categorized them into 14 key topic themes for IS security as presented in Table 2. The table also presents the 20 most frequent words for each topic.

Discussion of content analysis findings

As discussed in the previous section, our data analysis revealed 14 topic areas researched in mainstream IS security research (see Table 3). The topic areas fall into four categories, namely: *Security Policy Compliance and Management, IS Security Behavior and Privacy, System Design and Vulnerability Management,* and *Information Security Attack and Threat Detection Technologies* (see table 2). The heat maps presented in the appendix (Figs. A1 and A2) show dominant thematic areas across the years. Based on the analysis, it's evident that the topic areas of *Information Security Behaviors and Privacy Concerns*, and *Security Policy Compliance and Management* dominate the field. In many research studies, behavioral aspects have been closely aligned with compliance-oriented research. It is but natural for such a connection, particularly within the IS discipline since most studies seek to bring some kind of a behavioral change to encourage security policy compliance or reduce violations. A recent study by Karjalainen et al. (2019) is a case in point where the authors make a call for studying intrinsic behaviors of individuals leading to non-compliance. In the context of IS security behavior, the authors note, "non-compliance is driven not necessarily by malicious intentions but by benevolent ones; ISSBs [Information Systems Security Behaviors] are not strongly constrained by extrinsic pressures; individuals perceive rules (here, ISSPs) to be equivocal" (p. 699). Interestingly, in research conducted by Dhillon et al. (2020), the importance of intrinsic motivation is highlighted, besides exploring the role of structural and psychological empowerment in compliant behavior.

As shown in Table 3, each main area has several topic themes. *Privacy and Security in Online Social Networks* is another important theme within *Information Security Behaviors and Privacy Concerns* that has received much attention in recent IS literature (see topic V5 in Fig. A2). Several studies have used the privacy calculus perspective to investigate how individuals' beliefs about the costs and benefits of sharing sensitive information influence their online behaviors (e.g., Jian et al., 2013; Kordzadeh and Warren, 2017; Dhillon and Coss, 2019). Choi et al. (2015) showed that information dissemination and network commonality influence individuals' perceptions of privacy invasions and network bonding. That, in turn, impacts their behaviors in online social networks.

The third most researched topic area in IS security academic research is the *Systems Design and Vulnerability Management*. In the IS research community, there is a rich tradition of research that explores system design issues and vulnerabilities. This is evidenced from

Table 2
Topic analysis.

Topic ID	20 most frequent words	Key Topic Theme
V3	security risk management cyber manager assessment manage incident resource analysis base asset critical apply determine assess measure key culture include	Security Risk Management
V10	public government health article state policy national country citizen healthcare agency law protection issue egovernment year society unite include electronic	E-government, Security Policy & Standards
V2	process knowledge share business case organization challenge company development develop requirement standard analyze management fraud internal collaboration project integrate success	
V15	Security policy; Employee/organization compliance; Organizational work practice behavior violation; Cyberloafing; Examine Information Security Policy; Professional job conflict norm; Understand workplace deterrence effort	Security Policy Compliance
V21	firm market cost software breach increase investment loss optimal level vulnerability impact high vendor numb financial estimate price lead trade	Firm Security Decisions (Security Investments and Vulnerability Management)
V5	social network medium facebook online student site sns relationship self-disclosure behavior gender age discuss examine high activity participant personality communication	Privacy and Security in Online Social Networks
V11	internet group communication issue community identity people member virtual property current reveal discuss form tool nature potential activity discussion contribution	
V6	trust online consumer web website customer transaction purchase ecommerce internet personalization shop assurance integrity site commerce examine provide product type	Trust
V8	privacy concern personal individual disclosure online disclose private protection increase benefit control provide understand context survey general explore perspective calculus	Information Privacy Concerns
V13	perceive influence intention factor perception risk survey attitude relationship difference positive theoretical variable affect impact investigate moderate belief outcome strong	Information Security Behaviors
V19	framework behaviour address aim awareness focus analysis identify exist cybersecurity organisation issue principle future researcher aspect practical understand practice conduct	
V22	behavior threat computer individual role response context motivation play examine behavioral potential theoretical action cope protection self-efficacy impact consequence understand	
V1	method feature image base algorithm recognition performance face rate accuracy watermark biometric experimental error technique compare classification neural embed scheme	Privacy Enhancing Technologies
V4	user mobile device application provide app interaction content interface usability experience location conduct preference focus developer recommendation utilize expect smartphone	Mobile Security
V7	task event numb perform time expert term monitor provide identify include human activity type search domain evaluate tool condition RFID	Data and Application Security (Cloud, IoT, Technology adoption)
V14	service technology adoption quality adopt customer factor offer benefit impact acceptance provider bank support develop development advance innovation opportunity product	
V17	decision strategy support compute cloud objective concept dynamic game environment base goal order power selection case enterprise analysis capability phase	
V23	datum set rule algorithm database collect protect sensitive technique base pattern hide method association form attribute preserve cluster prediction protection	
V16	password authentication key scheme secure agent protocol problem digital improve electronic time protect create server addition signature access generate payment	Access Management (Access control, Authentication)
V20	control access application problem mechanism structure solution define architecture complex resource order issue constraint environment represent implementation document object distribute	
V12	attack network detection learn detect technique method malicious intrusion machine performance dataset accuracy false rate algorithm time evaluate malware vulnerability	Security Threat Detection Technologies
V18	level phishing high participant email target type message stage train low increase effective link question people individual report evidence current	Phishing

Table 3
Analysis of IS Security Research in academic journals.

	Topic Theme	Classification
1	Security Policy Compliance Security Risk Management Firm Security Decisions (Security Investments/ Vulnerability Management) E-government, Security Policy & Standards	Security Policy Compliance and Management
2	Privacy and Security in Online Social Networks Information Privacy Concerns Trust in security systems Information Security Behaviors	IS Security Behaviors and Privacy Concerns
3	Privacy Enhancing Technologies Data and Application Security (Cloud, IoT, RFID) Mobile Security Access Management (Authentication, Access Control)	System Design and Vulnerability Management
4	Phishing Security Threat Detection Technologies	IS Security Attacks and Threat Detection Technologies

the earlier work of Baskerville (1987; 1988), which highlighted the prevalence of security threats because of duality in system design to the more recent research on critical infrastructure protection (Paté-Cornell et al. 2018) and cybersafety of industrial systems (Khan and Madnick 2019).

While the topic areas of *Information Security Behaviors and Privacy Concerns*, and *Security Policy Compliance and Management* are dominated by IS research, some sub-themes in the *Systems Design and Vulnerability Management* area such as *Privacy Enhancing Technologies* and *Access Management* research lean towards Computer Science (CS). Specifically, we identified several publications related to biometric identification and authentication systems that were published in the *Expert Systems with Applications* journal.

Access Management related topics (see topic V20 in Fig. A2) such as access control mechanisms (e.g., role-based Cheng, 2000, purpose-based Kabir et al., 2012), and authentication methods are a few dominant topics in this area. Modern technology applications such as mobile interfaces encourage shifting from text-based authentication mechanisms to more advanced multifactor approaches including biometric authentication systems (Steinbart et al., 2016). While CS scholars have focused on developing these advanced authentication technologies, IS research has mainly been conducted on the interface of technology and users. For example, IS scholars have explored topics such as the effect of the user interface and login success rate on authentication behaviors (Steinbart et al., 2016), secure password practices (Zviran et al., 1999), and passphrase design and effectiveness (Keith et al., 2009).

The fourth most researched area of study amongst IS security academic researchers is around aspects related to *IS Security Attacks and Threat Detection*. Mainstream IS research has not significantly researched this topic and the area is mainly limited to *Phishing* related studies (see topic V18 in Fig. A2) (e.g., anti-phishing techniques, Ramesh et al. 2014), anti-phishing training (Jensen et al. 2017) while research on the sub-theme *Security Threat detection Technologies* leans towards CS. There are occasional IS research papers that relate to detecting and thwarting attacks (e.g., Nazareth and Choi 2015), detecting fake websites (e.g., Abbasi et al., 2010), and preemptively detecting intrusions (Patterson et al. 2017).

Perceived importance of IS security concerns

In the previous section, we presented an analysis of published research in academic journals over the past 30 years and identified the thematics that had received the most attention. To be comprehensive, we sought additional input from sitting Chief Information Security Officers (CISOs) to understand what they thought was important from the practitioners' perspective. The motivation to seek an opinion of what practitioners consider to be important has long been discussed in the literature. We believe that it is important for research to be grounded in what is relevant in practice. Mainstream IS researchers hold a similar opinion. An editorial in *MIS Quarterly* (Straub and Ang 2011) identified two alleged gaps with respect to relevance and rigor - *topic usefulness*, and *knowledge transference*. Topic usefulness is defined as "themes that researchers tackle and their alignment with what practitioners deem to be central to their needs." Knowledge transference is defined as "whether research conducted by academics is made accessible to and is actually used by practitioners." In an earlier *MIS Quarterly* article, Rosemann and Vessey (2008) had argued that relevance is necessary to satisfy the practitioner constituents that academia educates. While it is not our intent to engage in a debate of relevance versus rigor in this paper, in understanding the progress made in the IS security research literature, we take a cue from Straub and Ang (2011) as they allege a gap of *topic usefulness*. The concept of topic usefulness has multiple perspectives. Straub and Ang (2011), as well as Rosemann and Vessey (2008), discuss some of these in their work. In the context of this paper, we take particular credence to what Rosemann and Vessey note:

> "We view research that is important as that which meets the needs of practice by addressing a real-world problem in a timely manner, and in such a way that it can act as the starting point for providing an eventual solution. (p. 3)."

In this spirit, we seek the practitioner's opinions as to what they consider important IS security issues. To systematically understand and rank order these issues, we utilized the Delphi methodology.

Methodology used to identify and rank order practitioner IS security concerns

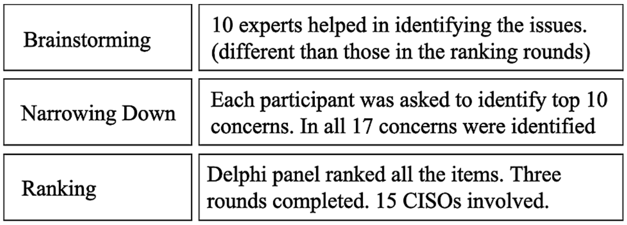
The objective of the Delphi study is to develop a comprehensive list of key IS security concerns as perceived by the CISOs. The Delphi method provides a suitable means to elicit opinions from a panel of experts as well as to develop a consensus as to what the top issues are. As the purpose of this paper is to undertake a literature review and assess the gaps between what practitioners think to be important IS security issues and the current research emphasis, we rank-ordered all the issues and consider them holistically. In conducting the Delphi study for this research, we follow Okoli and Pawlowski (2004) as well as the ranking approach suggested by Schmidt (1997). The Delphi approach is particularly useful for our purposes because of the following reasons:

1) The approach allowed us to seek divergent opinions and experiences of CISOs and translate them to a reliable list of security issues.

2) Since we used the Schmidt (1997) ranking style method, using controlled inquiry and feedback, it allowed us to converge upon the issues that are important for the CISOs.

3) It is challenging to get fifteen CISOs from Fortune 500 companies together in one place to seek their opinion. The Delphi method allowed us to conduct the study while the participants were not co-located.

The steps followed in undertaking the Delphi study appear in Fig. 3. We began the process with a blank sheet approach, starting with the identification of ten IS security experts. These included: one IS security professor, three information security officers working in a US state agency, three consultants (one of the three consultants worked for a boutique firm that had contracts with the State IT Agency, while the other two worked for big four consulting firms), two CISOs from major corporations, and one IS security investigator



Brainstorming

10 experts helped in identifying the issues. (different than those in the ranking rounds)

Narrowing Down

Each participant was asked to identify top 10 concerns. In all 17 concerns were identified

Ranking

Delphi panel ranked all the items. Three rounds completed. 15 CISOs involved.

Fig. 3. Sequence of methodological steps.

Table 4
Key issues identified by information security practitioners.

	Round 1 k = 15		Round 2 k = 15		Round 3 k = 15	
Issue	Mean Rank	D2	Mean Rank	D2	Mean Rank	D2
Preponderance of Data Breaches	3.47	16.27	2.20	76.19	2.13	77.36
Cloud Abuse by individuals	7.8	0.09	9.33	2.54	8.33	6.74
Hacking	6.2	1.69	4.53	40.90	4.67	39.21
Internet of Things Security	10.67	10.03	13.60	7.14	14.13	10.27
Phishing Attacks	5.87	2.67	3.47	55.68	3.53	54.69
Malware based attacks	3.73	14.19	2.93	63.92	3.40	56.68
Reliance on Single Factor Passwords	7.93	0.19	10.20	0.53	10.47	0.21
Insecure User Application Interface	8	0.25	10.80	0.02	10.60	0.11
Loss of Data Availability	6.2	1.69	6.53	19.32	6.33	21.12
Shadow IT Systems	9.87	5.60	12.27	1.79	11.80	0.76
Insider Threat	6.93	0.32	6.33	21.12	5.07	34.36
Critical Infrastructure Protection	7.27	0.05	6.67	18.16	7.13	14.40
Security Policy Compliance	9.87	5.60	12.67	3.02	12.73	3.26
Cybersecurity Skill Shortage	11.2	13.69	13.67	7.50	15.13	17.68
SQL Injection Attacks			12.33	1.97	11.87	0.88
Security Policy Misalignment			14.93	16.04	16.00	25.72
Access Control Management			10.53	0.16	9.67	1.59
Totals	105.00	72.33	153.00	335.99	153.00	365.03
Grand Means	7.5		10.9		10.9	
	W	X^2	W	X^2	W	X^2
*p < .001	0.318	61.99*	0.669	160.45*	0.74	177.53*
Rho	0.511		0.602		0.578	

Table 5
Final ranking after three rounds.

Rank	Information Security Issue	Classification / Clusters
1	Preponderance of Data Breaches	IS Security Attacks
2	Malware	
3	Phishing Attacks	
4	Hacking	
5	Insider Threats	
13	SQL Injection Attacks	
6	Loss of Data Availability	System Design and Infrastructure Vulnerabilities
7	Critical Infrastructure Protection	
8	Cloud Abuse by individuals	
9	Access Control Management	
10	Reliance on Single Factor Passwords	
11	Insecure User Application Interface	
12	Shadow IT Systems	
14	Security Policy Compliance	IS Security Management and Regulatory Issues
15	Internet of Things Security	
16	Cybersecurity Skill Shortage	
17	Security Policy Misalignment	

from a federal agency. The experts were asked to think freely and list up to 10 IS security concerns they felt were critically important. The diversity of the individuals allowed us to get a cross-section of concerns. The ten individuals providing 10 concerns each resulted in a list of over 100 issues. There were many overlaps and repetitions. We manually tallied the issues to generate the list of 17 concerns, which we used for the first round. The sheer volume of the data and the saturation point that we achieved helped us have significant data confidence. Practitioners were used at two stages in this research - first, in the Delphi study to rank order the security topic areas; second, to provide insight into the relevance of our proposed research questions and propositions. For us, seeking comments from the practitioners enriches our interpretations.

Three rounds of the Delphi study were conducted using a separate panel (different from those who participated in the brainstorming session) of fifteen CISOs. All participants worked for Fortune 500 companies. The ranking of IS security concerns occurred over several rounds until consensus among the experts was achieved. Kendall's Coefficient of Concordance (*W*) was used to measure the level of consensus. Schmidt (1997) suggests that the usual range is between 0.1 where there is a very weak agreement, and 0.9, where the agreement is usually strong. We also used Spearman's Rank Correlation Coefficient (*Rho*) to measure the stability between successive ranking rounds. *Rho* can range from −1, a perfect negative correlation, to + 1, a perfect positive correlation. Ranking of rounds is stopped if Kendall's Coefficient indicates a strong consensus (>0.7). The ranking is also stopped if the level of consensus tapers off. In round 3 of our study, Kendall's *W* was 0.740, indicating a strong consensus. *Rho* for the three rounds was 0.511, 0.602, 0.578, also indicating a strong consensus. Detailed statistics related to each round, sorted by rank order, appear in Table 4.

The final rank order of all 17 issues appears in Table 5. We categorize them into three main clusters of information systems security issues, namely, *IS Security Attacks; System Design and Infrastructure Vulnerabilities;* and *IS Security Management and Regulatory Issues.* The results of the Delphi study indicate that practitioners are mainly concerned and interested in various types of *IS Security Attacks*. The second most concerning area is the *System Design and Infrastructure Vulnerabilities*. Unlike academic literature, *IS Security Management and Regulatory Issues* were relegated to the bottom of the rank order. In the next section, we propose a future research agenda to reduce the gap between academic literature and practitioner interests.

Analysis and defining a future research agenda

In this section, we analyze the research findings and provide a future research agenda. We do so in two steps: First, we provide specific research questions, which arose from the review of the literature. Second, while considering the research questions, we develop propositions. The propositions are informed based on the perceptions of the CISOs as well as supported by the literature review.

Emergent research questions

Our review of the literature and the Delphi study provide a basis for specific research questions and propositions. Following the Delphi study, we formed a panel of 6 CISOs to discuss our findings. These included: two CISOs from a state agency in the US, one CISO from a utility company, two CISOs from the retail industry, and one CISO from a large public university. We observed three emergent themes around which we develop the research questions: *IS Security Attacks*; *System Design and Vulnerabilities*; *IS Security Compliance and Behavior*. Based on the extant literature and our discussions with the CISOs, we developed the research propositions. The CISOs commented on the relevance of research questions and the propositions. Table 6 presents a comparative overview of IS security issues and concerns identified by the CISOs and through Topic Modeling. The comments and observations emerged from our open discussions. Below, we discuss each of the themes, the emergent research questions, and the related propositions.

IS Security Attacks

IS security attacks, including relevant threat detection technologies, emerged as one of the thematics. While the Delphi study ranked issues such as the preponderance of data breaches, malware, phishing attacks, hacking, insider threats, and SQL injection attacks as reasonably high, our IS literature survey found limited research in the area. Much of the existing IS security literature, at best, has been restricted to phishing and that too using traditional methods such as surveys and experiments with a few notable exceptions (e.g., Silic and Lowry 2020; Dincelli and Chengalur-Smith 2020). Further, while the IS security literature has investigated various aspects of data breaches over the years, the focus has been on a range of psychological characteristics. For instance, Chatterjee

Table 6
Comparative overview of IS security issues and concerns.

Themes identified by CISOs – rank-ordered (rank-ordered	Topic Modeling themes (in order of importance)	Comments and Observations
IS Security Attacks	Security Policy Compliance and Management	CISOs consider management of security attacks to be the most important issue as opposed to the dominant academic research
System Design and Infrastructure Vulnerabilities	IS Security Behaviors and Privacy Concerns	For CISOs, security design and development issues remain central.
IS Security Management and Regulatory Issues	System Design and Vulnerability Management	Academic research is close behind practitioners' concerns about system design, vulnerability management has a higher concern for practitioners.
	IS Security Attacks and Threat Detection Technologies	Academic research and practitioner concerns seem to have different focuses. There is a need for recalibration.

et al. (2019) investigate the role of fear and anger in dealing with a data breach. Syed (2019) studies the impact of security breaches on a firm's reputation. Goode et al. (2017) evaluate the role of user compensation following a data breach.

While the importance of psychological aspects related to phishing attacks and data breaches is equally paramount, it is of further importance to investigate other kinds of IS security attacks and threat detection techniques. For instance, the increased availability of big data related to breaches allows us to model and investigate the root causes of breaches and propose appropriate mitigation strategies. To this point, researchers have only begun to explore how network flow traffic can be analyzed and categorized as malicious (Sun et al. 2019), as big data analytics now allows for such analysis to be conducted. Therefore, we propose the following research questions to guide future research:

> RQ1: How can IS researchers apply data science methods and techniques such as machine learning to a) investigate the root causes of IS security attacks while considering the organizational and behavioral aspects, b) identify IS security incident patterns, both technical and organizational, and predict threats, c) identify IS vulnerabilities, and d) propose more effective risk mitigation strategies that consider technical and organizational aspects?
>
> RQ2: How can IS researchers use data science-based techniques to analyze identity, access, sentiment, and behavioral data drawn from various sources to provide a holistic view of access-related risks and vulnerabilities in different contexts (e.g., Cloud, IoT, and mobile) and provide actionable insights.

Our CISO panelists strongly indicated that over the next 5–7 years, *data breaches*, *malware*, *phishing attacks*, *hacking*, and *insider threats*, will continue to be important concerns and pose a management challenge. One CISO from a large public university narrated a story of a hack that brought havoc to the university systems and then said the following:

> "Perpetrators are now becoming exceptionally sophisticated. They use a combination of tools. A phishing attack may result in a DMZ server getting compromised, resulting in a data breach, which in turn may result in malware being installed."

In a case study of a computer hack, Perez (2005) documents a similar situation. Perez (2005) notes, "lack of manpower, new priorities, resistance to change and reluctance to modify what currently functioned caused a delay of several months" (p. 58), which perpetuated the hack. There is limited academic IS research exploring aspects of data breaches. In a study by Hammouchia et al. (2019), however, 9000 data breaches made public since 2005 are analyzed. The authors found an apparent increase in hacking breaches. Interestingly they also found the healthcare sector to have an increased number of attacks, particularly since 2013. Therefore, we propose the following:

> P1: Malware is a consequence of a combination of phishing attacks and other types of security incidents. When researching IS security attacks the focus should be on interdependencies of various attack modes that span technical and organizational boundaries.
>
> P2: Emerging big data and data science techniques help in identifying IS security vulnerabilities. When researching IS security vulnerabilities, the interconnections between seemingly unrelated attack vectors should inform theory building, particularly in light of big data and advanced data science techniques.
>
> P3. Identity, behavior, and sentiment analytics enhance the prediction accuracy of insider threats and other types of security threats. When researching IS security threats, the focus should go beyond intrinsic and extrinsic factors. Techniques such as text mining, sentiment analysis, and machine learning algorithms to identify deviations from normal behavior patterns (behavior anomalies) will significantly improve the predictive power.

System Design and Vulnerability Management

System design and vulnerability management emerged as another key theme in IS security literature. While the importance of secure systems design was first introduced by Richard Baskerville (1993), the topic has received limited interest. Over the years, occasionally researchers have proposed methodologies for secure systems design (e.g., Fernandez and Larrondo-Petrie 2008; White and Dhillon 2005). Researchers have also made calls for managing vulnerabilities and problems in inadequate system designs by proposing modeling of responsibilities (e.g., Backhouse and Dhillon 1996; Dobson 1991) accountability (e.g., Nissenbaum 1994), and understanding *deep structures* of organizations and information systems (e.g. Thomas and Dhillon 2012; Leifer et al. 1994; Wing 1998). More recently, scholars have begun discussions on the role of accountability in an artificial intelligence-enabled world, particularly how transparency takes center stage in ensuring security and privacy (e.g., Vedder and Naudts 2017).

A recurring theme in the security research related to system design issues is the concept of the *correctness of specification* (for an original conceptualization, see the seminal work by Wing 1990). Ensuring access to the right assets is integral to the correct specifications. Hence, much of the earlier work is related to providing proper access to systems. One of the prominent models to emerge from this research relates to defining roles to ensure access control (Sandhu and Munawer 1998). The role-based access control models simplified how a set of users were given a set of permissions to access computing resources. While the access control models were originally proposed by computer scientists, there are several implications for IS security, particularly when designing systems. Today, advances in the Internet of Things and big data have identified the limitations of role-based access control. Newer concepts, such as *attribute-based access control* (see Gupta et al. 2021), have now been introduced. Therefore, we see several research questions related to system design and vulnerability management that require addressing. These include:

> RQ3: What are the fundamental and measurable elements to assure the security of software systems, including a) verification and validation of system security and b) development of context and threat-specific vulnerability models to be investigated using design science approaches.

RQ4: Investigate complex security access control strategies by analyzing a) identity, b) attributes related to access, and c) provide holistic access control scenarios in new and varied contexts (e.g., Cloud, IoT, Mobile).

Our CISO panelists felt strongly regarding vulnerabilities resulting from either system design flaws or some critical infrastructure failure. One of the CISOs from a large consumer bank in the US said:

> “When there is a system design issue, it can cause a significant headache to the security team. While these errors still occur, the advances in development techniques have more or less minimized them.”

There is some merit to what the CISO had to say. Early work in system specification (e.g., see Wing 1990) has helped define conceptual models and protocols for reducing errors in systems analysis and design. Nevertheless, scholars continue to study various aspects of system design and security, ranging from user interface design (Mohamed et al. 2017) to critical infrastructure protection (Hurst et al. 2014). We, therefore, propose the following:

P4: IS Security incident patterns are a predictor of possible new threats. Research should correlate one set of security incident patterns with another to identify possible new threat vectors (e.g., a series of denial of service attacks may be linked to possible identity thefts).

P5: Correctness in system specification determines the nature and scope of vulnerabilities. A lot of IS security threats persist because there were errors in the specification of systems, i.e., linking requirements to design, and implementation.

Security compliance and behavior

Research in security compliance is very closely related to behavioral security work. Hence, regarding the famous phenomenon that employees are the weakest link in the security chain, we can consider them as potential threats to IS security. However, different insiders have different motivations (see Homoliak et al. 2019, for a detailed review). Having well-established policies and standards does not guarantee the success of IS security management practices. Yet, employee compliance plays an integral role in securing company data and assets, and thus with this notion, attracting many security researchers to this topic. There are myriad studies (e.g., Siponen and Vance 2010; Johnston and Warkentin 2010; Bulgurcu et al., 2010; Xue et al. 2011; Ifinedo 2012; Vance et al. 2012; Moody et al. 2018; Dhillon et al. 2020) published in academic IS literature that investigates varied aspects of compliance with different conceptual models. These studies utilize numerous constructs to evaluate different behavioral perspectives in security policy compliance. They all argue that managers and executives should consider both technical and human perspectives in IS security management.

In recent years, mainstream IS literature has considered context to be an essential aspect in developing theories (e.g., see Hong et al. 2014). As Johns (2006) notes, “context can have both subtle and powerful effects on research results” (p. 386). Johns also defines context as “situational opportunities and constraints that affect the occurrence and of organizational behavior as well as functional relationships between variables” (p. 386). Research in IS security also alludes to the relevance of context on various variables, including compliance. Aurigemma and Mattson (2019), for instance, undertook two studies comparing compliance intentions and threat-specific compliance intentions. In both studies, the authors found that compliance intentions varied significantly. Therefore, it is prudent that proper consideration is given to context to study and theorize about a range of IS security variables. Hence, we propose the following research questions:

RQ5: Explore the importance of moving from general IS security behavioral contexts to a) single context theorization of IS security contexts b) cross-context theory replication (see Hong et al. (2014) for context-specific theorizing guidelines).

RQ6: How to integrate traditional theory-based research frameworks with User and Entity Behavior Analytics based approaches to resolve context-specific issues related to security compliance?

Associated with the behavioral and management aspects of IS security research are the human and social aspects. Human aspects of IS security were first introduced by Hitchings (1995). She argued that implementing security followed an outdated approach and a new methodology should be developed, which “ideally [should] follow the soft systems approach, in keeping with current trends in systems analysis” (p. 382). Around the same time, Helen Armstrong evaluated the usefulness of the Soft Systems Methodology and proposed an IS security model (James 1996; Armstrong 1999). Over the years other scholars have used and acknowledged the importance of the soft systems approach and in appreciating the socio-technical aspects (e.g., Damenu and Beaumont 2017; Craig et al. 2014). Spagnoletti and Resca (2008), in particular, introduce the notion of duality in IS security and rely on systems’ socio-technicality to address predictable and unpredictable threats.

Subsequently, Williams et al. (2013) studied fourteen Australian Critical Infrastructure Organizations. They found that security governance is a “socio-technical, emergent and situated practice and revealed institutional sources of variations in practice” (p. 352). Along a similar line, Charitoudi and Blyth (2014) undertook a socio-technical simulation of a critical infrastructure to model consequences across different levels of organizations’ networks. While earlier research (e.g., Dhillon and Backhouse 2001; Baskerville 1993) made calls for IS security research to explore the socio-technical aspects, progress has been limited. There have only been a few limited efforts, particularly in the mainstream IS journals. The inherent complexity of security and system dynamics cannot be underestimated. Further work in this area is critical. We, therefore, propose the following research question:

RQ7: Explore IS security threats and vulnerabilities with a socio-technical perspective to identify advanced risk and vulnerability management strategies.

Our CISO panelists were more or less in agreement with the inherent complexity in IS security management. Yet, they introduced another kind of compliance that should be considered, i.e., regulatory. While agreeing that policy alignment and regulatory

Table 7
Summary of future research questions and propositions.

IS Security Attacks
RQ1: How can IS researchers apply data science methods and techniques such as machine learning to a) investigate the root causes of IS security attacks while considering the organizational and behavioral aspects, b) identify IS security incident patterns, both technical and organizational, and predict threats, c) identify IS vulnerabilities, and d) propose more effective risk mitigation strategies that consider technical and organizational aspects?RQ2: How to use data science-based techniques to analyze identity, access, and behavior data drawn from various sources to provide a holistic view of access-related risks and vulnerabilities in different contexts (e.g., Cloud, IoT, and mobile) and provide actionable insights.
P1: Malware is a consequence of a combination of phishing attacks and other types of security incidents. When researching IS security attacks the focus should be on interdependencies of various attack modes that span technical and organizational boundaries.
P2: Emerging big data and data science techniques help in identifying IS security vulnerabilities. When researching IS security vulnerabilities, the interconnections between seemingly unrelated attack vectors should inform theory building, particularly in light of big data and advanced data science techniques.
P3. Identity, behavior, and sentiment analytics enhance the prediction accuracy of insider threats and other types of security threats. When researching IS security threats, the focus should go beyond intrinsic and extrinsic factors. Techniques such as text mining, sentiment analysis, and machine learning algorithms to identify deviations from normal behavior patterns (behavior anomalies) will significantly improve the predictive power.
Systems Design and Vulnerability Management
RQ3: What are the fundamental and measurable elements to assure the security of software systems, including a) verification and validation of system security b) development of context and threat-specific vulnerability models to be investigated using design science approaches.RQ4: Investigate complex security access control strategies by analyzing a) identity b) attributes related to access and c) provide holistic access control scenarios in varied contexts (e.g., Cloud, IoT, mobile).
P4: IS Security incident patterns are a predictor of possible new threats. Research should correlate one set of security incident patterns with another to identify possible new threat vectors (e.g., a series of denial of service attacks may be linked to possible identity thefts).
P5: Correctness in system specification determines the nature and scope of vulnerabilities. A lot of IS security threats persist because there were errors in the specification of systems, i.e., linking requirements to design, and implementation.
Security Compliance and Behavior
RQ5: Explore the importance of moving from general IS security behavioral contexts to a) single context theorization of IS security contexts b) cross-context theory replication. See (Hong et al. 2014) for context-specific theorizing guidelines.RQ6: How to integrate traditional theory-based research frameworks with User and Entity Behavior Analytics based approaches to resolve context-specific issues related to security compliance?RQ7: Explore IS security threats and vulnerabilities with a socio-technical perspective to identify advanced risk and vulnerability management strategies.
P6. Context-specific (e.g., threat-specific) guidelines enhance IS security compliance
P7. Well-integrated technical and social countermeasures provide effective risk mitigation and vulnerability management strategies

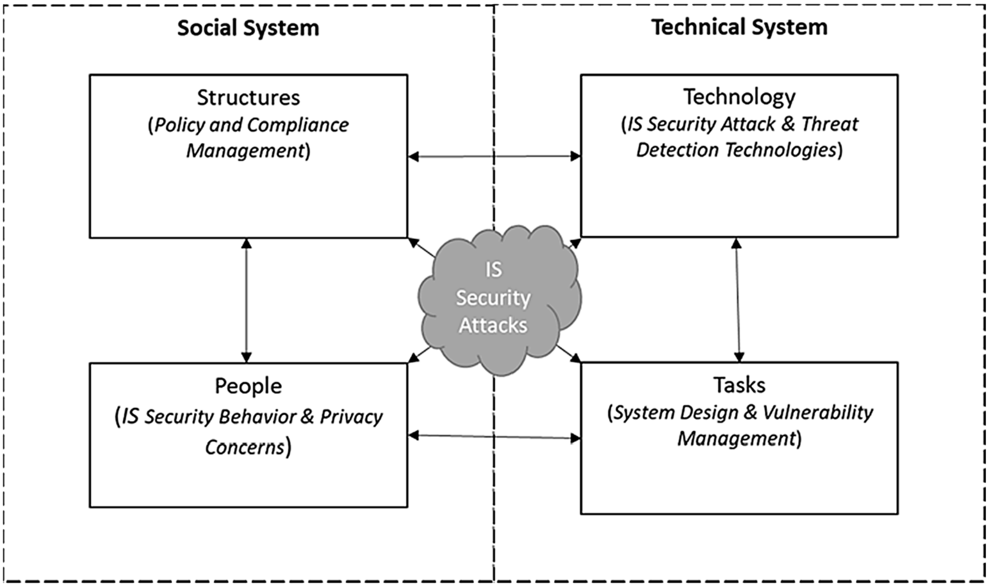

Social System
Technical System
Structures
(Policy and Compliance Management)
Technology
(IS Security Attack & Threat Detection Technologies)
IS Security Attacks
People
(IS Security Behavior & Privacy Concerns)
Tasks
(System Design & Vulnerability Management)

Fig. 4. Conceptualizing IS Security Research Agenda.

compliance issues more or less have been incorporated and institutionalized in the organizations, they acknowledged that ongoing attention is still necessary. A CISO, who had previously served as Senior Compliance Analyst in a public utility company noted:

> "Ever since the Sarbanes-Oxley Act of 2002 came into effect, the importance of compliance and regulation has become a norm. There was indeed a lot of resistance and discord, mainly when it came to section 404. However, there is very little evidence to

> suggest that there is resistance or there are any problems, at least in our company. As a compliance officer, I have to stay on top of all the rules and regulations. Whenever there is a radical change, we need to ensure that we remain in compliance."

The compliance officer's observation is relevant, mainly when the majority of the academic research has focused on sanctions and rewards in ensuring security policy compliance. There are isolated attempts in the literature that break away from the rewards and punishment aspect of compliance. For instance, Bauer and Bernroider (2017) argue, "ISA [information security awareness] programs should emphasize positive frames and the value for the organization gained by compliant IS [information systems] behavior instead of overly stressing sanctions" (p. 59). In the literature, there are even fewer attempts to study the regulatory compliance aspects. Kwon and Johnson (2011), for instance, found prevalent security practices to impact regulatory compliance. We, therefore, propose the following:

> P6. Context-specific (e.g., threat-specific) guidelines enhance IS security compliance.
>
> P7. Well-integrated technical and social countermeasures provide effective risk mitigation and vulnerability management strategies.

Implications

Earlier on we first presented questions that future research should address. These were largely based on what we found in our literature review using content analysis. We then evaluated the research questions in light of our panel discussion with the CISOs. The introspection allowed us to develop specific propositions. A summary of the research questions and the propositions are presented in Table 7. As is evident, we compressed the two categories of *Security Policy Compliance and Management* and *IS Security Behaviors and Privacy Concerns* into one - *Security Compliance and Behavior*, because of significant overlaps.

In the literature, as noted previously, socio-technical concepts have been used to understand and conceptualize how technical and social systems interact. By socio-technical, we mean how structures (laws and regulations), people (individuals, groups, roles, and organizations), technology (physical technology), and tasks (what data is kept, in what format, who has access) interact (see Fig. 4). Our literature review suggests that most of the current emphasis has focused on individual elements of the socio-technical system. Our discussions with the CISOs, however, suggested, while focusing on *structures*, *people, technology, and tasks* was important, IS security attacks typically occur when the subsystems interact. One CISO from a Fortune 500 company succinctly noted:

> The attack landscape is such where a perpetrator may use the weakest link in the chain, which is usually the people, to subvert the existing rules and bypass all available threat detection technologies. Remember the Home Depot attack!

The CISO had a point to make. The Home Depot case[6], besides many others, was a reminder that attacks on systems are usually successful because the integrity of the socio-technical system is compromised. When probed as to where he saw the contribution of the research community in understanding IS security issues, he said:

> Gone are the days when technology remained static. When I started my career, we could pretty much lock up the data center and have a good night's sleep assuming that things would be relatively secure. Today things are different. Not only is the technology changing so quickly, but the tasks individuals complete are evolving, as are the regulations and competence of individuals.

The CISO makes an interesting point, suggesting that IS security attack scenarios exist at the subsystems' intersections. Based on the in-depth analysis of both the academic literature and the practitioner-based Delphi study, we can arrive at two distinct conclusions; First, current academic research and practitioner concerns are out of sync. Holistically, research occurs in overlapping areas of concern, yet a disproportionate amount of academic interest lies in topics that practitioners seemingly considered resolved. Second, the cybersecurity concerns of practitioners and research investment of academics point to serious gaps in the literature that lies at the intersection of the socio-technical system. This is to say, while not all research is so strictly bounded, much of the current academic literature is heavily grounded in singular aspects of the socio-technical system. Therefore, to such an end, the research questions and propositions developed based on our analysis of the literature offer an opportunity to the academic community. By driving new research to the intersections of the socio-technical system, we identify unique opportunities that provide both academic and practitioner contributions and highlight areas where the value of continued exploration offers a suboptimal opportunity for theoretical advancement.

Conclusion

In this study, we conducted a rigorous and comprehensive review of the academic information systems security literature and a Delphi study of CISOs, thus identifying key academic and practitioner trends in research. This is an essential contribution as it represents the first comprehensive literature review of both the academic and practitioner information systems security trends.

Our findings show that *IS Security Behaviors and Privacy Concerns*, and *Security Policy Complianc*e literature dominates IS literature, yet the practitioner concerns focus on *IS Security Attack* issues. To address the lack of synergy between academic research and practitioner concerns this paper presents a comprehensive analysis of existing literature to propose a future research agenda under three broad thematics, namely: *IS Security Attacks*; *System Design and Vulnerabilities*; and *IS Security Compliance and Behavior*. This holistic IS security review helps us identify critical gaps within these trends and provide a clear roadmap for future IS Security research. The

[6] https://www.infosecurity-magazine.com/news/home-depot-to-pay-2725m/ Accessed 15 Oct 2020.

proposed research agenda makes important contributions to IS security research and practice.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Appendix

Figs. A1 and A2 show a clustered heat map and a heat map of topics across years respectively. The heat maps use cool-to-warm color spectrum to represent how research focus varies across time. Less dominant topics tend towards cool blue tones and while dominant topics tend towards hotter orange tones on the color scale. We used the seaborn[7] python package to generate heatmaps. Fig. A3

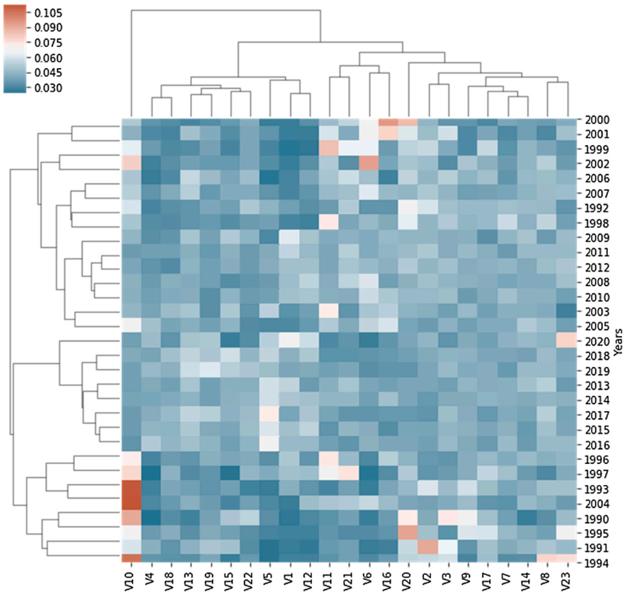


Fig. A1. Dominant topics across years (Clustered heat map).

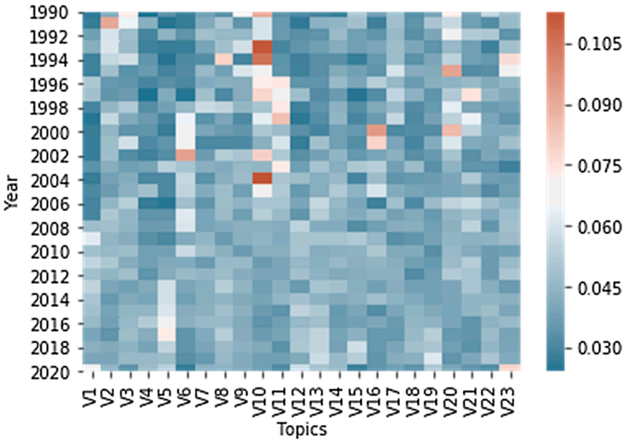


Fig. A2. Dominant topics across years (Heat map).

[7] https://seaborn.pydata.org/

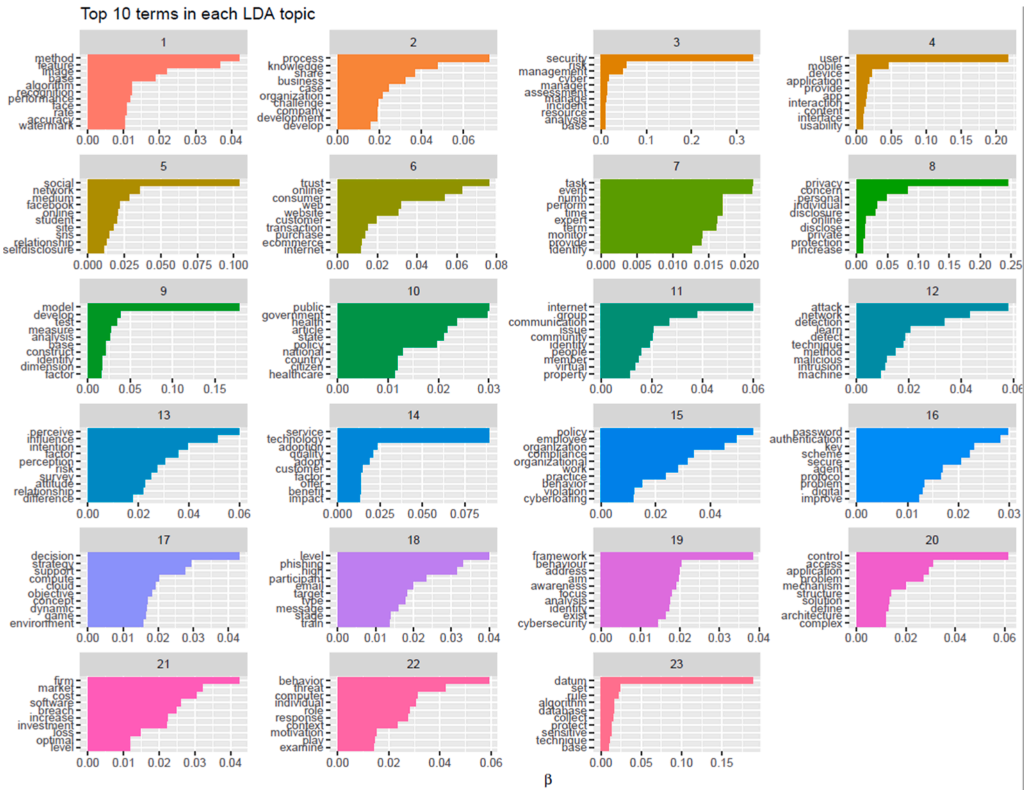


Fig. A3. Top 10 terms in each LDA topic.

References

Abbasi, A., Zhang, Z., Zimbra, D., Chen, H., Nunamaker Jr, J.F., 2010. Detecting fake websites: The contribution of statistical learning theory. MIS Quarterly 34 (3), 435–461.

Albrechtsen, E., 2007. A Qualitative Study of Users' View on Information Security. Computers & Security 26 (4), 276–289.

Ande, R., Adebisi, B., Hammoudeh, M., Saleem, J., 2020. Internet of Things: Evolution and technologies from a security perspective. Sustainable Cities and Society 54, 101728. https://doi.org/10.1016/j.scs.2019.101728.

Armstrong, H. 1999. "A Soft Approach to Management of Information Security," PhD thesis in: School of Public Health. Perth, Australia: Curtin University, p. 343.

Arun, R., Suresh, V., Madhavan, C. V., and Murthy, M. N. 2010. "On Finding the Natural Number of Topics with Latent Dirichlet Allocation: Some Observations," Pacific-Asia Conference on Knowledge Discovery and Data Mining: Springer, p. 391-402.

Aurigemma, S., Mattson, T., 2019. Generally Speaking, Context Matters: Making the Case for a Change from Universal to Particular ISP Research. Journal of the Association for Information Systems 20:12, 7.

Backhouse, J., Dhillon, G., 1996. Structures of Responsibility and Security of Information Systems. European Journal of Information Systems 5 (1), 2–9.

Baskerville, R., 1987. "Logical Controls Specification," *Information systems development for human progress in organizations. IFIP TC WG 8.2*. North-Holland, Atlanta, Georgia.

Baskerville, R., 1988. Designing Information Systems Security. John Wiley & Sons, New York.

Baskerville, R., 1993. Information Systems Security Design Methods: Implications for Information Systems Development. ACM Computing Surveys 25 (4), 375–414.

Bauer, S., Bernroider, E.W., 2017. From Information Security Awareness to Reasoned Compliant Action: Analyzing Information Security Policy Compliance in a Large Banking Organization. Database for Advances in Information Systems 48 (3), 44–68.

Blei, D.M., Ng, A.Y., Jordan, M.I., 2003. Latent Dirichlet Allocation. Journal of Machine Learning Research 3:Jan, 993–1022.

Bostrom, R.P., Heinen, J.S., 1977. MIS Problems and Failures: A Socio-Technical Perspective. Part I: The Causes. MIS Quarterly 1 (1), 17–32.

Burrell, G., Morgan, G., 1979. Sociological Paradigms and Organisational Analysis. Heinemann, London.

Cao, J., Xia, T., Li, J., Zhang, Y., Tang, S., 2009. A Density-Based Method for Adaptive LDA Model Selection. Neurocomputing 72 (7–9), 1775–1781.

Charitoudi, K., Blyth, A.J., 2014. An Agent-Based Socio-Technical Approach to Impact Assessment for Cyber Defense. Information Security Journal: A Global Perspective 23 (4–6), 125–136.

Chatterjee, S., Gao, X., Sarkar, S., Uzmanoglu, C., 2019. Reacting to the Scope of a Data Breach: The Differential Role of Fear and Anger. Journal of Business Research 101, 183–193.

Cheng, E.C., 2000. An object-oriented organizational model to support dynamic role-based access control in electronic commerce. Decision Support Systems 29 (4), 357–369.

Choi, B.C.F., Jiang, Z.(., Xiao, B.o., Kim, S.S., 2015. Embarrassing exposures in online social networks: An integrated perspective of privacy invasion and relationship bonding. Information Systems Research 26 (4), 675–694.

Craig, R., Spyridopoulos, T., Tryfonas, T., May, J., 2014. In: Soft Systems Methodology in Net-Centric Cyber Defence System Development. IEEE, Man, and Cybernetics (SMC), pp. 672–677.

Crossler, R.E., Johnston, A.C., Lowry, P.B., Hu, Q., Warkentin, M., Baskerville, R., 2013. Future Directions for Behavioral Information Security Research. Computers & Security 32, 90–101.

Damenu, T.K., Beaumont, C., 2017. Analysing Information Security in a Bank Using Soft Systems Methodology. Information & Computer Security 25 (3), 240–258.

Deveaud, R., SanJuan, E., Bellot, P., 2014. Accurate and Effective Latent Concept Modeling for Ad Hoc Information Retrieval. Document numérique 17 (1), 61–84.

Dhillon, G. (Ed.), 1997. Managing Information System Security. Macmillan Education UK, London.

Dhillon, G., 2007. Principles of Information Systems Security: Text and Cases. John Wiley & Sons, Hoboken, NJ.

Dhillon, G., Abdul Talib, Y.Y., Picoto, W.N., 2020. The Mediating Role of Psychological Empowerment in Information Security Compliance Intentions. Journal of the Association for Information Systems 21 (1), 152–174.

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

Dhillon, S., and Coss, D. "Information Privacy Literature: issues and challenges," Journal of Information System Security (15:3), p. 185-198.

Dincelli, E., Chengalur-Smith, I., 2020. Choose Your Own Training Adventure: Designing a Gamified Seta Artefact for Improving Information Security and Privacy through Interactive Storytelling. European Journal of Information Systems 1–19.

Dobson, J., 1991. A Methodology for Analyzing Human and Computer-Related Issues in Secure Systems. In: Dittrich, K., Rautakivi, S., Saari, J. (Eds.), Computer Security and Information Integrity. Elsevier Science Publishers, Amsterdam, pp. 151–170.

Eder-Neuhauser, P., Zseby, T., Fabini, J., 2018. Malware propagation in smart grid monoculturesMalware-Ausbreitung in Smart Grid-Monokulturen. Elektrotechnik and Informationstechnik 135 (3), 264–269.

Fernandez, E.B., Larrondo-Petrie, M.M., 2008. "A Methodology to Develop Secure Systems Using Patterns," in *Information Security and Ethics: Concepts, Methodologies, Tools, and Applications*. IGI Global 654–670.

Furnell, S., Clarke, N., 2012. Power to the People? The Evolving Recognition of Human Aspects of Security. Computers & Security 31 (8), 983–988.

Goode, S., Hoehle, H., Venkatesh, V., Brown, S.A., 2017. User Compensation as a Data Breach Recovery Action: An Investigation of the Sony Playstation Network Breach. MIS Quarterly 41 (3), 703–727.

Griffiths, T.L., Steyvers, M., 2004. Finding Scientific Topics. Proceedings of the National Academy of Sciences 101 (suppl 1), 5228–5235.

Gupta, M., Awaysheh, F.M., Benson, J., Al Azab, M., Patwa, F., Sandhu, R., 2021. An Attribute-Based Access Control for Cloud-Enabled Industrial Smart Vehicles. IEEE Transactions on Industrial Informatics 17 (6), 4288–7297.

Hammouchia, H., Cherqia, O., Mezzoura, G., Ghoghoa, M., El Koutbib, M., 2019. Digging Deeper into Data Breaches: An Exploratory Data Analysis of Hacking Breaches over Time. Procedia Computer Science 151, 1004–1009.

Hitchings, J., 1995. Deficiencies of the Traditional Approach to Information Security and the Requirements for a New Methodology. Computers & Security 14 (5), 377–383.

Homoliak, I., Toffalini, F., Guarnizo, J., Elovici, Y., Ochoa, M., 2019. Insight into Insiders and It: A Survey of Insider Threat Taxonomies, Analysis, Modeling, and Countermeasures. ACM Computing Surveys (CSUR) 52 (2), 1–40.

Hong, W., Chan, F.K.Y., Thong, J.Y.L., Chasalow, L.C., Dhillon, G., 2014. A Framework and Guidelines for Context-Specific Theorizing in Information Systems Research. Information Systems Research 25 (1), 111–136.

Huang, A.H., Lehavy, R., Zang, A.Y., Zheng, R., 2018. Analyst Information Discovery and Interpretation Roles: A Topic Modeling Approach. Management Science 64 (6), 2833–2855.

Hurst, W., Merabti, M., and Fergus, P. 2014. "A Survey of Critical Infrastructure Security," International Conference on Critical Infrastructure Protection, J. Butts and S. Shenoi (eds.), Arlington, VA: Springer, p. 127-138.

Ifinedo, P., 2012. Understanding Information Systems Security Policy Compliance: An Integration of the Theory of Planned Behavior and the Protection Motivation Theory. Computers & Security 31 (1), 83–95.

James, H. 1996. "Managing Information Systems Security: A Soft Approach," Information Systems Conference of New Zealand: IEEE Society Press.

Jensen, M.L., Dinger, M., Wright, R.T., Thatcher, J.B., 2017. Training to mitigate phishing attacks using mindfulness techniques. Journal of Management Information Systems 34 (2), 597–626.

Jiang, Z., Heng, C.S., Choi, B.C., 2013. Research note—privacy concerns and privacy-protective behavior in synchronous online social interactions. Information Systems Research 24 (3), 579–595.

Johns, G., 2006. The Essential Impact of Context on Organizational Behavior. Academy of Management Review 31 (2), 386–408.

Johnston, A.C., Warkentin, M., 2010. Fear Appeals and Information Security Behaviors: An Empirical Study. MIS Quarterly 34 (3), 549–566.

Karjalainen, M., Sarker, S., Siponen, M., 2019. Toward a Theory of Information Systems Security Behaviors of Organizational Employees: A Dialectical Process Perspective. Information Systems Research 30 (2), 687–704.

Kabir, M.E., Wang, H., Bertino, E., 2012. A role-involved purpose-based access control model. Information Systems Frontiers 14 (3), 809–822.

Karlsson, F., Hedström, K., Goldkuhl, G., 2017. Practice-Based Discourse Analysis of Information Security Policies. Computers & Security 67, 267–279.

Keith, M., Shao, B., Steinbart, P., 2009. A behavioral analysis of passphrase design and effectiveness. Journal of the Association for Information Systems 10 (2), 63–89.

Khan, S., and Madnick, S. 2019. "Cybersafety: A System-Theoretic Approach to Identify Cyber-Vulnerabilities & Mitigations in Industrial Control Systems," Available at SSRN 3542551).

Kordzadeh, N., Warren, J., 2017. Communicating personal health information in virtual health communities: An integration of privacy calculus model and affective commitment. Journal of the Association for Information Systems 18 (1), 45–81.

Kwon, J., and Johnson, M. E. 2011. "The Impact of Security Practices on Regulatory Compliance and Security Performance," 32nd International Conference on Information Systems (ICIS). December 4-7, Shanghai, China.

Leifer, R., Lee, S., and Durgee, J. 1994. "Deep Structures: Real Information Requirements Determination," Information & Management 27(5), p. 275-285.

Luse, A., Mennecke, B., Townsend, A., and Demarie, S. 2013. "Strategic Information Systems Security: Definition and Theoretical Model," AMCIS 2013, August 15-17. Chicago, USA.

McFadzean, E., Ezingeard, J.-N., and Birchall, D. 2006. "Anchoring Information Security Governance Research: Sociological Groundings and Future Directions," Journal of Information System Security 2(3), p. 3-48.

Mohamed, M.A., Chakraborty, J., Dehlinger, J., 2017. Trading Off Usability and Security in User Interface Design through Mental Models. Behaviour & Information Technology 36 (5), 493–516.

Moody, G.D., Siponen, M., Pahnila, S., 2018. Toward a Unified Model of Information Security Policy Compliance. MIS Quarterly 42 (1), 285–311.

Nazareth, D.L., Choi, J., 2015. A System Dynamics Model for Information Security Management. Information & Management 52 (1), 123–134.

Nissenbaum, H., 1994. Computing and Accountability. Communications of the ACM 37 (1), 73–80.

Okoli, C., Pawlowski, S.D., 2004. The Delphi Method as a Research Tool: An Example, Design Considerations and Applications. Information & Management 42 (1), 15–29.

Paananen, H., Lapke, M., Siponen, M., 2020. State of the Art in Information Security Policy Development. Computers & Security 88, 1–14.

Paté-Cornell, M.E., Kuypers, M., Smith, M., Keller, P., 2018. Cyber Risk Management for Critical Infrastructure: A Risk Analysis Model and Three Case Studies. Risk Analysis 38 (2), 226–241.

Patterson, N., Hobbs, M., Zhu, T., 2017. A Cyber-Threat Analytic Model for Autonomous Detection of Virtual Property Theft. Information & Computer Security 25 (4), 358–381.

Perez, S., 2005. The Case of a Computer Hack. Journal of Information System Security 1 (2), 53–63.

Ramesh, G., Krishnamurthi, I., Kumar, K.S.S., 2014. An efficacious method for detecting phishing webpages through target domain identification. Decision Support Systems 61, 12–22.

Rosemann, M., Vessey, I., 2008. Toward Improving the Relevance of Information Systems Research to Practice: The Role of Applicability Checks. MIS Quarterly 32 (1), 1–22.

Samonas, S., Coss, D., 2014. The CIA Strikes Back: Redefining Confidentiality, Integrity and Availability in Security. Journal of Information System Security 10 (3), 21–45.

Sandhu, R., and Munawer, Q. 1998. "How to Do Discretionary Access Control Using Roles," Proceedings of the third ACM workshop on Role-based access control, p. 47-54.

Schmidt, R.C., 1997. Managing Delphi Surveys Using Nonparametric Statistical Techniques. Decision Sciences 28 (3), 763–774.

Silic, M., Lowry, P.B., 2020. Using Design-Science Based Gamification to Improve Organizational Security Training and Compliance. Journal of Management Information Systems 37 (1), 129–161.

Siponen, M., Vance, A., 2010. Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations. MIS Quarterly 34 (3), 487–502.

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

Siponen, M.T., Oinas-Kukkonen, H., 2007. A Review of Information Security Issues and Respective Research Contributions. The Data Base for Advances in Information Systems 38 (1), 60–80.

Spagnoletti, P., Resca, A., 2008. The Duality of Information Security Management: Fighting against Predictable and Unpredictable Threats. Journal of Information System Security 4 (3), 46–62.

Steinbart, P.J., Keith, M.J., Babb, J., 2016. Examining the continuance of secure behavior: A longitudinal field study of mobile device authentication. I*nformation Systems Research* 27 (2), 219–239.

Straub, D., Ang, S., 2011. Editor's Comments: Rigor and Relevance in IS Research: Redefining the Debate and a Call for Future Research. MIS Quarterly 35 (1), iii–xi.

Sun, P., Li, J., Bhuiyan, M.Z.A., Wang, L., Li, B., 2019. Modeling and Clustering Attacker Activities in Iot through Machine Learning Techniques. Information Sciences 479, 456–471.

Syed, R., 2019. Enterprise Reputation Threats on Social Media: A Case of Data Breach Framing. Journal of Strategic Information Systems 28 (3), 257–274.

Thomas, M., Dhillon, G., 2012. Interpreting Deep Structures of Information Systems Security. The Computer Journal 55 (10), 1148–1156.

Vance, A., Siponen, M., Pahnila, S., 2012. Motivating Is Security Compliance: Insights from Habit and Protection Motivation Theory. Information & Management 49 (3), 190–198.

Vedder, A., Naudts, L., 2017. Accountability for the Use of Algorithms in a Big Data Environment. International Review of Law, Computers & Technology 31 (2), 206–224.

White, E. F., and Dhillon, G. 2005. "Synthesizing Information System Design Ideals to Overcome Developmental Duality in Securing Information Systems," Proceedings of the 38th Annual Hawaii International Conference on System Sciences: IEEE, p. 186a-186a.

Williams, S.P., Hardy, C.A., Holgate, J.A., 2013. Information Security Governance Practices in Critical Infrastructure Organizations: A Socio-Technical and Institutional Logic Perspective. Electronic Markets 23 (4), 341–354.

Wing, J.M., 1990. A Specifier's Introduction to Formal Methods. Computer 23 (9), 8–24.

Wing, J. M. 1998. "A Symbiotic Relationship between Formal Methods and Security," Proceedings from Workshops on Computer Security, Fault Tolerance, and Software Assurance: From Needs to Solution, CMU-CS-98-188, December.

Xue, Y., Liang, H., Wu, L., 2011. Punishment, Justice, and Compliance in Mandatory It Settings. Information Systems Research 22 (2), 400–414.

Zviran, M., Haga, W.J., 1999. Password security: an empirical study. Journal of Management Information Systems 15 (4), 161–185.