A closer look at organizational cybersecurity research trending topics and limitations

Allen C. Johnston
*Department of Information Systems, Statistics, and Management Science,
The University of Alabama, Tuscaloosa, Alabama, USA*

Received 12 July 2022
Revised 17 October 2022
Accepted 17 October 2022

Abstract

Purpose – In identifying both the topics of interest and key limitations of the extant organizational security research, both opportunities for future research as well as some underlying challenges for conducting this research may be revealed.

Design/methodology/approach – To identify the leading organizational cybersecurity research topics of interest and their key limitations, the author conducted a topic modeling analysis of the organizational level studies published in the Association for Information Systems (AIS) senior scholars' "basket of eight journals" (Association for Information Systems, 2022) over the past five years.

Findings – Leading topics include (1) organizational security research concerns governance and strategic level decision-making and their role in shaping organizational security successes and failures, (2) cybercriminals and organizations' ability to monitor and detect them from both within and outside the firm; (3) cost, liability and security negligence, (4) organizations' innovation dispositions for security products and services and (5) organizational breach response efficacy; while key limitations of this study include the following: (1) scholars' ability to propose and assess strategic and operational level threat response recommendations, (2) their understanding how influence is formed and maintained among employees and groups and (3) their measurement instruments and models.

Originality/value – Organizations remained plagued by an ever-emerging set of threats to the security of their digital and informational assets. New threats are regularly discovered and remedies to existing threats are continually proven ineffective against these new threats. Providing an orientation to the current research on organizational security can help advance their security efforts.

Keywords Security, Limitations, Organization, Topic modeling

Paper type Conceptual paper

Over the past few years, cybersecurity research in the field of information systems (IS) has been incredibly diverse, with topics ranging from the design of systems and system interfaces to aid in employee security compliance behaviors (Vance *et al.*, 2015) to the study of uncertainty mitigation in information technology (IT) investments (Benaroch, 2018). Among these topics, scholars have flocked to some, while others are no less important but have not had the same level of continued inspection. For those of us that focus the majority of our research on security concerns, we are already aware that within the broad scope of cybersecurity research, individual level studies have dominated. From insider abuse perspectives to security technology adoption to behavioral response modeling, scholars have invested far more energy and effort inspecting individual level phenomena than those of the organization.

We are also aware that organizational cybersecurity is an important area of study. Organizations remained plagued by an ever-emerging set of threats to the security of their

Organizational Cybersecurity Journal: Practice, Process and People
Vol. 2 No. 2, 2022
pp. 124-133
Emerald Publishing Limited
e-ISSN: 2635-0289
p-ISSN: 2635-0270
DOI 10.1108/OCJ-07-2022-0013

digital and informational assets. New threats are regularly discovered and remedies to existing threats are continually proven ineffective against these new threats. It is a dynamic battleground, replete with shifting priorities and societal expectations, obstacles, both internal and external, resources and resource constraints and regulatory pressures. Just when we think we have a firm grasp of one particular aspect of organizational security, events occur, circumstances change and what we thought we knew quickly becomes obsolete. For example, the Securities and Exchange Commission (SEC) recently proposed rules governing the manner in which publicly listed companies must make cybersecurity incident disclosures and the management and governance of cyber risks (Tremaine, 2022). Given this rapidly changing landscape, what we are talking about is the study of something that is incredibly complex, varied and evolving. Adding to this the general hypercautious nature by which most firms approach the sharing of their security-related successes and failures, and you have yourself a real challenge indeed.

But, among the studies that have taken on this challenge, perhaps what we do not have is a great sense of what have been the dominant areas of interest and the key limitations that scholars have informally coalesced around; thus, the driving motivations for this conceptual article to shed some light and offer a helpful perspective. In identifying both the topics of interest and key limitations of the extant organizational security research, we may be able to reveal both opportunities for future research as well as some underlying challenges for conducting this research.

Published topics of interest

To identify the leading organizational cybersecurity research topics of interest, I conducted a topic modeling analysis of the organizational level studies published in the Association for Information Systems (AIS) senior scholars' "basket of eight journals" (Association for Information Systems, 2022). This includes articles published in *MIS Quarterly (MISQ), Information Systems Research (ISR), Journal of Management Information Systems (JMIS), Journal of the Association for Information Systems (JAIS), European Journal of Information Systems (EJIS), Information Systems Journal (ISJ), Journal of Information Technology (JIT)* and *Journal of Strategic Information Systems (JSIS)*. These journals are generally regarded by the community of management information system (MIS) scholars as our leading academic outlets and, as such, the work published in them as some of our most interesting and important research.

From 2016 to 2021, a total of 40 organizational-level security articles were published in these eight journals. To be as inclusive as possible, articles were considered to be organizational level security articles if they had a unit of analysis at the organizational level and/or had a focus on organizational phenomena or interventions. I did not include literature reviews or meta-analysis papers in this exercise. Using the structural topic modeling (stm) package (v1.3.6) in R (v4.1.2 (2021-11-01)), I generated a model based on keywords of the 40 organizational security articles published in the journals from 2016–2021, the results of which suggest five leading topics that have dominated our recent attention. Table 1 presents the count of these articles across journals from 2016–2021.

First, the model shows that one leading topic of organizational cybersecurity research concerns *governance and strategic level decision-making and their role in shaping organizational security successes and failures*. The extant research in this broad area includes studies that examine the importance of corporate social performance, such as philanthropy and green IT investments, to a firm's likelihood of being targeted by malicious actors (D'Arcy *et al.*, 2020), the impact of centralized decision making on the likelihood of cybersecurity breaches (Liu *et al.*, 2020) and the correlation of IT security investments and network embeddedness on a firm's likelihood of experiencing a data breach. Also included in this focal area are studies that touch on executive leadership (Guhr *et al.*, 2019) and other institutional factors (Angst *et al.*, 2017) as determinants of a firm's security outcomes. Given the historical tendencies of security to be pigeonholed as primarily a tactical or operational concern, it is good to see that research that focused at the strategic level become more prevalent in the literature.

Second, the model shows that scholars have been interested in *cybercriminals and our ability to monitor and detect them from both within and outside the firm* (Ji *et al.*, 2016; Siering *et al.*, 2021). Included in this research are studies that provide guidance for darknet research (Benjamin *et al.*, 2019; Ebrahimi *et al.*, 2020) and for the analysis of cybercriminal Internet Relay Chat (IRC) communities (Benjamin *et al.*, 2016), as well as studies focused on the influence of peer monitoring on employee information security policy (ISP) violations (Yazdanmehr and Wang, 2021).

The third topic of interest revolves around *cost, liability and security negligence*. This includes research on the influence of customer restitution on customer outcomes post data breach (Goode *et al.*, 2017), the efficiency of bilateral liability-based contracts in managed security services (MSSs) (Hui *et al.*, 2019) and the importance of cloud service certifications as indicators of a cloud provider's future service quality (Lansing *et al.*, 2019). Post-breach reputation management (Gwebu *et al.*, 2018; Syed, 2019) also falls into the topic of interest, as reputation loss is an important cost to a company when recovering from a data breach. So do MSSs, as the contractual outsourcing of security operations involves considerations of cost and liability (Wu *et al.*, 2021).

The model shows another topic of interest among organizational cybersecurity scholars is the *risk to digital infrastructure and data*. Within this topic space, research has included studies that examined the impact of electronic health record's meaningful-use attestation on the occurrence of data breaches (Kwon and Johnson, 2018), developed design principles for an automated fraud detection system (Siering *et al.*, 2021), developed a taxonomy of various organizational personally identifiable information breaches (Posey *et al.*, 2017) and examined the role of algorithms as key elements underlying threats to digital high-reliability (Salovaara *et al.*, 2019). Also included in this research is a study that examined how information systems security (ISS) best practices are translated into situated practices (Niemimaa and Niemimaa, 2017).

Finally, the model shows *organizational breach response efficacy* to be another focus of the research. The extant research in this topic area included studies that examined the security efficacy of collectives (Johnston *et al.*, 2019; Yoo *et al.*, 2020), as well as the consequences of privacy safeguard enactments in medical practices (Parks *et al.*, 2017).

By no means is this topic a modeling exercise or the mapping of research to the prevailing topics comprehensive. Some of the studies I mention could map to more than one topic, and there may be accidental omissions on my part of studies that could firmly fit in at least one topic area. Even with these limitations, I believe the exercise does provide us with a sense of the prevailing topics of interest among organizational research scholars.

Table 1.
Number of organizational cybersecurity articles in AIS "basket of eight journals" by year

	2016	2017	2018	2019	2020	2021	Total per journal
MISQ	0	2	1	3	1	0	7
ISR	1	1	1	1	1	0	5
JMIS	1	2	1	0	3	1	8
JAIS	1	1	0	1	0	2	5
EJIS	0	3	0	1	0	1	5
ISJ	0	0	1	3	1	0	5
JIT	0	0	0	0	1	1	2
JSIS	0	0	0	3	0	0	3
Total per year	3	9	4	12	7	5	40

Conspicuously underrepresented from the literature are organizational-level studies focused on security climate, security culture and the social structures, either as determinants of organizational security outcomes or as outcomes themselves. There are a few studies in this area (Johnston *et al.*, 2019; Yazdanmehr *et al.*, 2020; Yoo *et al.*, 2020), but for the most part, scholars have not given these topics nearly the same level of attention as their nonsecurity specific organizational counterparts of organizational culture and climate. Effective organizational security requires a collective effort and the ability of employees to remind, encourage or assist each other with appropriate protective security behaviors is essential to a positive security posture. For instance, while most information security policies will prohibit the use of account and password sharing, or the use of sticky notes to aid in the recollection of particularly complex and difficult to remember passwords, enforcement of those behavioral controls by security personnel is difficult and is reliant, to some degree, upon the involvement of conscientious employees in providing encouragement and/or guidance to their colleagues. For this reason and others, security climates and the cultures and social structures that help establish and support them represent critical topics that have yet to gain a sufficient level of attention.

Another potential area of organizational security research concerns an organization's innovation disposition for security products and services. With more and more firms adopting open business models with an eye toward open innovation, how does that model impact their strategic approach to security? What may be interesting here is the notion of co-created policy; looking at policy as a product of an open governance model (i.e. co-created governance). The general premise is that the more externally-oriented the policy creators are, the more open their approach to governance, and particularly policy development, will be. Does this sort of security governance model work, and, if so, how and what are its advantages and consequences?

Finally, in terms of underserved topics, what also seems relatively absent from the leading articles on organizational security are multilevel studies that examine the interaction of organizational and individual level factors. As an example, an organization's information security policies reflect its desired security posture, but they are idyllically relative to the actual level at which they are implemented. While the policies may establish expectations of secure behavior among insiders, how these expectations are ultimately fulfilled is determined at both the individual and organizational levels. It is this combination of individual and organizational-level influences that define an organization's security posture. Insiders will engage in policy-prescribed secure behaviors due to the individual-level influence of a number of factors, including policy awareness, deterrence factors, threat and efficacy perceptions and normative beliefs, among others. However, the information security posture of an organization is also dependent upon the interactive, coordinative and synergistic capabilities of its insiders in the form of insider communities. How these communities are formed, are responsive to organizational cultures and climates, and ultimately influence individual behaviors need further exploration.

Summary of research limitations

In the important research on the organizational cybersecurity topics that has occurred, scholars have been relatively consistent in their views of the limitations of their work. Using a similar approach to structural topic modeling as performed on the keywords of the published work in the AIS senior scholars' basket of eight, I generated a model based on the author-described limitations of these studies. The results of this model point to three key limitations.

First, scholars point to limitations concerning their ability to propose and assess strategic and operational level threat response recommendations, such as those that encourage increased security-related investments or revised approaches to SETA engagements.

This concern is rooted in scholars' limited access to threat response recommendations and their ability to propose and assess the impact of the recommendations as they are implemented in corporate settings. Either way, threat response recommendations are highly contextual and difficult to capture and implement at the organizational level due to the varied and highly dynamic nature of an organization's security environments and workforces. Consider, for example, the study of organizations' risk management investments and decision-making. Access to the inner workings of an organization's risk management processes and decision-making is not easily obtained, but because of the highly contextualized and specialized nature of risk management, access is a critical requirement for scholars' ability to conceptualize and execute impactful research. This may explain why we see so many single case studies is this space; where typically, one of the co-authors of a study will have relationships with a company that allows for some level of access. Replicating this level of access across multiple firms is a difficult proposition.

Second, scholars appear to struggle to understand how influence is formed and maintained among employees and groups. It is likely that the primary reasons for this commonly cited limitation stem also from issues of accessibility; access to organizations at a level that provides an in-depth exposure of the cultures, styles and norms that define their less structured, informal workings. For example, in their study of the correlation of a firm's social performance and data breach experiences, D'Arcy *et al.* (2020) state a limitation that they were reliant upon public announcements of data breaches and did not have access to internal reports that may have provided a more robust accounting of their breach activity. This limitation is an important one and really captures the essence of what organizational research scholars face when contemplating the operationalization of their studies.

It strikes me that in my own research, it is generally not too difficult to capture a firm's formal, public-facing artifacts (e.g., vision and mission statements, financial reports, enterprise security policies, etc.). Where difficulty arises is when we take the next steps into the firm and start asking for face time with employees or reports of known maleficence or data breach activity. Where the security policies, processes and data are fairly formalized and regularly distributed, access is rather straightforward and not too often denied; however, where the policies, processes and data are not well-structured, and there is a prevailing sense of uncertainty about what might be discovered if rocks are overturned, access is more often denied or severely constrained, at best.

Finally, the topic model suggests scholars point to concerns for their measurement instruments and models. This is honestly not too surprising as this concern is something that is also rather prevalent among the individual-level security research and one of the reasons we, as an academic community, place such an emphasis on our theory contextualization and instrument validation efforts. Reflecting on this more closely as a primary stated limitation of organizational security scholarship, however, I cannot help but wonder how much constraints of access that contribute to the first two limitations derived from the topic analysis also play a role in concerns for measurement instruments and models.

Given the dynamic and highly complex nature of organizational settings, it strikes me that mixed-method research designs should play a big role in how we approach our studies. Particularly important are the designs that incorporate both qualitative and quantitative approaches in the same study. For example, in attempting to gain a level of familiarity with an organization's informal elements, such as its security culture or social reporting hierarchies, qualitative approaches such as interviews or active research engagements can go a long way toward providing a level of immersion necessary for the development of new theories or middle-range theories and models. Such an approach could help not only in theory contextualization efforts but could also aid scholars by improving the ecological validity of their research designs, providing a level of assurance that the operationalization of constructs in their instruments are consistent with what employees face in their typical workplace setting. If measurement instruments are truly a concern of organizational security researchers, then having this assurance could go a long way in mitigating this concern.

Moving forward

Based on a structural topic model of the limitations provided by articles published between 2016 and 2021 in the AIS senior scholars' "basket of eight journals," I believe there are some clear lines of inquiry through which we can work to progress the research on organizational security. Underlying these limitations is a clear need for a more immersive phenomenological experience by scholars in the organizational security phenomena they seek to study. My point here is not to rehash prior calls for research relevance (i.e. Grover and Lyytinen, 2015; Nunamaker *et al.*, 2017; Te'eni *et al.*, 2017). Those remain the cornerstone of important conversations we must have as academics for how to advance our research among practitioners, including how to identify important research questions, how to approach the study of them and how to articulate their findings in a way that has meaning and value to practice. Rather, my point is more in line with the suggestions of Lang (2003) that organizational security scholars need to reconnect with practice and its varied and complex contextual environments. We can learn from the principles of organizational anthropology, which concerns the application of immersive diagnostic techniques to the study of organizational problems and situations.

As an example, consider the limitations expressed in the topic modeling results. For each of these, the common underlying element is the *obstacle of abstraction*. By this, I mean the limitations we introduce into our study by approaching narrowly scoped phenomena without sufficient access to the settings in which they exist. With a limited phenomenological experience, scholars are left with only abstract conceptualizations of the more difficult to reach organizational elements, such as security cultures and intra-group dynamics. This limitation, in turn, affects not only the theorizing and contextualization efforts of the scholars but also their research design choices and the subsequent conclusions drawn from their work.

I also believe scholars would benefit from first taking a holistic view of an organization's security profile before narrowing down to the more nuanced phenomenon of interest. By doing so, researchers would more fully understand the context of their phenomenon, including an understanding of how firms derive value from their external resources and leverage both their formal and informal processes and structures to develop their security outcomes. As an aid in forming this more holistic view, there are a few frameworks that could be applied, including Nadler and Tushman's (1980) congruence model for assessing organizational behavior, neo-institutional theory (Hu *et al.*, 2007) and organizational mindfulness (Levinthal and Rerup, 2006), among others.

The congruence model for assessing organizational behavior (henceforth referred to simply as the congruence model) has been used in the literature to explain processes related to organizational transformation such as the transformation of performance management processes (Garavan *et al.*, 2020; Schleicher *et al.*, 2018), resource allocation strategies (Dellestrand *et al.*, 2020) and organizational structural changes (Král and Králová, 2016). The model suggests that a critical success factor in the formation of effective organizational outcomes is the process through which the organization is able to leverage its advantages and mitigate its disadvantages. This process is described as an organizational transformation process.

Applied to the context of organizational security, the external inputs to an organization present varying degrees of advantage or disadvantage as they devise their strategic approach to the development and management of their information security programs. These external factors may include their regulatory environment, their access to and ability to acquire and retain quality human and technological resources and their history of InfoSec successes and failures. Further, the process by which organizations are able to transform these external inputs into security outcomes is crucial to the effectiveness of the outcomes and is dependent upon a number of interrelated factors, including the individuals involved in the transformation process, the tasks performed as part of the process and instantiations of the formal and informal organizational environments. Ultimately, the congruence among these interrelated organizational factors dictates the effectiveness of the security solutions.

Another lens, through which scholars could first gain a holistic view of organizational security before narrowing their focus, could be through the application of the neo-institutional theory. The neo-institutional theory helps explain how rationalized institutional elements and networks of social organizations influence formal organizational structures (Meyer and Rowan, 1977). This holistic lens has been applied in prior security studies with great success (Hu *et al.*, 2007), including studies focused on understanding organizational security implementations in higher education (Kam and Katerattanakul, 2014; Kam *et al.*, 2013) and in small- and medium-sized enterprises (SMEs) (Barton *et al.*, 2016).

As a final example of a framework or theory that could be applied by scholars to gain an initial perspective of an organization's security posture, we can look to organizational mindfulness. Over the past few decades, researchers have ported the concept of mindfulness into the organizational setting and have been able to characterize mindfulness as an organizational phenomenon (Levinthal and Rerup, 2006). Collective mindfulness, also known as mindful organizing, is defined as a team's combined ability to come up with a rich awareness of both internal and external processes and to regulate team behaviors based on that awareness (Dierynck *et al.*, 2017). The concept of mindfulness has strong roots in the psychology literature and tells us that mindful organizations will engage in nonroutine thought processes if they are receptive to intricate logic, sensitive to their environment and committed to the resolution of failures within that environment (Langer, 1989; Sternberg, 2000; Weick and Roberts, 1993). For circumstances in which an organization is exposed to InfoSec threats and their formal policies and procedures are restrictive, limited or non-existent in guiding a response, a collective, mindful approach by the organization may result in the formation of innovative solutions to the threats that provide security benefits otherwise unattainable to the firm.

Mindful organizations are those that are preoccupied with failure, are reluctant to simplify, are attentive to operations, are focused on resilience and are able to deviate from hierarchical decision structures in order to migrate problems to the experts to which the problems are best suited (Levinthal and Rerup, 2006). In the context of cybersecurity, a preoccupation with failure manifests in an organization's determination to turn security incidents into teachable moments in which they are able to learn from their mistakes. A reluctance to simplify refers to an organization's insistence on viewing failures from multiple perspectives, while attentiveness to operations refers to an organization's focus on the operations of the firm and their role in InfoSec failures. An organization's focus on resilience refers to its propensity to addressing attacks as they occur, while their migrating of decisions to expertise refers to their ability to deviate from hierarchical decision structures and migrate problems to the appropriate experts.

Conclusion

With the relatively limited amount of extant cybersecurity research focused at the organizational level, my goals with this thought piece were twofold. First, I wanted to establish an awareness of the current topics of interest and those topics that are perhaps deserving of increased attention. Based on a topic modeling exercise of the keywords provided by organizational-level cybersecurity articles published in the AIS basket of eight journals between 2016 and 2021, these topics include (1) organizational security research concerns governance and strategic level decision making and their role in shaping organizational security successes and failures, (2) cybercriminals and our ability to monitor and detect them from both within and outside the firm, (3) cost, liability and security negligence, (4) organizations' innovation dispositions for security products and services and (5) organizational breach response efficacy. Underserved topics in this space may include (1) studies focused on security climate, security culture, and the social structures, (2) organizations' innovation dispositions for security products and services and (3) multilevel studies that examine the interaction of organizational and individual level factors.

Second, I wanted to present the current set of limitations that are common to the extant organizational cybersecurity research. Based on a similar topic modeling exercise as that conducted on the keywords, I conducted one using the same set of articles' limitations and found that scholars point to limitations concerning (1) their ability to propose and assess strategic and operational level threat response recommendations, (2) their understanding of how influence is formed and maintained among employees and groups and (3) their measurement instruments and models. Based on these limitations, I provided a set of suggestions for how scholars could mitigate these limitations in their own research. My hope is that these findings and suggestions will inspire, expand and enhance future organizational cybersecurity research activity.

References

Angst, C.M., Block, E.S., D'arcy, J. and Kelley, K. (2017), "When do IT security investments matter? Accounting for the influence of institutional factors in the context of healthcare data breaches", *MIS Quarterly*, Vol. 41 No. 3, pp. 893-916.

Association for Information Systems (2022), "Senior scholars' basket of journals", available at: https://aisnet.org/page/SeniorScholarBasket.

Barton, K.A., Tejay, G., Lane, M. and Terrell, S. (2016), "Information system security commitment: a study of external influences on senior management", *Computers and Security*, Vol. 59, pp. 9-25.

Benaroch, M. (2018), "Real options models for proactive uncertainty-reducing mitigations and applications in cybersecurity investment decision making", *Information Systems Research*, Vol. 29 No. 2, pp. 315-340.

Benjamin, V., Valacich, J.S. and Chen, H. (2019), "DICE-E: a framework for conducting Darknet identification, collection, evaluation with ethics", *MIS Quarterly*, Vol. 43 No. 1.

Benjamin, V., Zhang, B., Nunamaker, J.F. Jr and Chen, H. (2016), "Examining hacker participation length in cybercriminal internet-relay-chat communities", *Journal of Management Information Systems*, Vol. 33 No. 2, pp. 482-510.

Dellestrand, H., Kappen, P. and Lindahl, O. (2020), "Headquarter resource allocation strategies and subsidiary competitive or cooperative behavior: achieving a fit for value creation", *Journal of Organization Design*, Vol. 9, pp. 1-16.

D'Arcy, J., Adjerid, I., Angst, C.M. and Glavas, A. (2020), "Too good to be true: firm social performance and the risk of data breach", *Information Systems Research*, Vol. 31 No. 4, pp. 1200-1223.

Dierynck, B., Leroy, H. and Savage, G. (2017), "The role of individual and collective mindfulness in promoting occupational safety in health care", *Medical Care Research and Review*, Vol. 74 No. 1, pp. 79-96.

Ebrahimi, M., Nunamaker, J.F. Jr and Chen, H. (2020), "Semi-supervised cyber threat identification in dark net markets: a transductive and deep learning approach", *Journal of Management Information Systems*, Vol. 37 No. 3, pp. 694-722.

Garavan, T., McCarthy, A., Lai, Y., Murphy, K., Sheehan, M. and Carbery, R. (2020), "Training and organisational performance: a meta-analysis of temporal, institutional, and organisational context moderators", *Human Resource Management Journal*, Advance online publication, Vol. 31 No. 1, pp. 1-26.

Goode, S., Hoehle, H., Venkatesh, V. and Brown, S.A. (2017), “User compensation as a data breach recovery action: an investigation of the Sony PlayStation network breach”, *MIS Quarterly*, Vol. 41 No. 3, pp. 703-727.

Grover, V. and Lyytinen, K. (2015), “New state of play in information systems research”, *MIS Quarterly*, Vol. 39 No. 2, pp. 271-296.

Guhr, N., Lebek, B. and Breitner, M.H. (2019), “The impact of leadership on employees’ intended information security behaviour: an examination of the full-range leadership theory”, *Information Systems Journal*, Vol. 29 No. 2, pp. 340-362.

Gwebu, K.L., Wang, J. and Wang, L. (2018), “The role of corporate reputation and crisis response strategies in data breach management”, *Journal of Management Information Systems*, Vol. 35 No. 2, pp. 683-714.

Hu, Q., Hart, P. and Cooke, D. (2007), “The role of external and internal influences on information systems security–a neo-institutional perspective”, *The Journal of Strategic Information Systems*, Vol. 16 No. 2, pp. 153-172.

Hui, K.-L., Ke, P.F., Yao, Y. and Yue, W.T. (2019), “Bilateral liability-based contracts in information security outsourcing”, *Information Systems Research*, Vol. 30 No. 2, pp. 411-429.

Ji, Y., Kumar, S. and Mookerjee, V. (2016), “When being hot is not cool: monitoring hot lists for information security”, *Information Systems Research*, Vol. 27 No. 4, pp. 897-918.

Johnston, A.C., Di Gangi, P.M., Howard, J. and Worrell, J. (2019), “It takes a village: understanding the collective security efficacy of employee groups”, *Journal of the Association for Information Systems*, Vol. 20 No. 3, pp. 186-212.

Kam, H. and Katerattanakul, P. (2014), “Information security in higher education: a neo-institutional perspective”, *Journal of Information Privacy and Security*, Vol. 10 No. 1, pp. 28-43.

Kam, H., Katerattanakul, P., Gogolin, G. and Hong, S. (2013), “Information security policy compliance in higher education: a neo-institutional perspective”, *PACIS*.

Král, P. and Králová, V. (2016), “Approaches to changing organizational structure: the effect of drivers and communication”, *Journal of Business Research*, Vol. 69 No. 11, pp. 5169-5174.

Kwon, J. and Johnson, M.E. (2018), “Meaningful healthcare security: does meaningful-use attestation improve information security performance?”, *MIS Quarterly*, Vol. 42 No. 4, pp. 1043-1068.

Lang, M. (2003), “Communicating academic research findings to IS professionals: an analysis of problems”, *Informing Science*, Vol. 6, pp. 21-29.

Langer, E.J. (1989), *Mindfulness*, Addison-Wesley/Addison Wesley Longman, Reading, MA.

Lansing, J., Siegfried, N., Sunyaev, A. and Benlian, A. (2019), “Strategic signaling through cloud service certifications: comparing the relative importance of certifications’ assurances to companies and consumers”, *The Journal of Strategic Information Systems*, Vol. 28 No. 4, 101579.

Levinthal, D. and Rerup, C. (2006), “Crossing an apparent chasm: bridging mindful and less-mindful perspectives on organizational learning”, *Organization Science*, Vol. 17 No. 4, pp. 502-513.

Liu, C.-W., Huang, P. and Lucas, H.C., Jr (2020), “Centralized IT decision making and cybersecurity breaches: evidence from US higher education institutions”, *Journal of Management Information Systems*, Vol. 37 No. 3, pp. 758-787.

Meyer, J.W. and Rowan, B. (1977), “Institutionalized organizations: formal structure as myth and ceremony”, *American Journal of Sociology*, Vol. 83 No. 2, pp. 340-363.

Nadler, D. and Tushman, M.L. (1980), “A congruence model for diagnosing organizational behavior”, *Resource Book in Macro Organizational Behavior*, pp. 30-49.

Niemimaa, E. and Niemimaa, M. (2017), “Information systems security policy implementation in practice: from best practices to situated practices”, *European Journal of Information Systems*, Vol. 26 No. 1, pp. 1-20.

Nunamaker, J.F., Twyman, N.W., Giboney, J.S. and Briggs, R.O. (2017), "Creating high-value real-world impact through systematic programs of research", *MIS Quarterly*, Vol. 41 No. 2, pp. 335-351.

Parks, R., Xu, H., Chu, C.-H. and Lowry, P.B. (2017), "Examining the intended and unintended consequences of organisational privacy safeguards", *European Journal of Information Systems*, Vol. 26 No. 1, pp. 37-65.

Posey, C., Raja, U., Crossler, R.E. and Burns, A. (2017), "Taking stock of organisations' protection of privacy: categorising and assessing threats to personally identifiable information in the USA", *European Journal of Information Systems*, Vol. 26 No. 6, pp. 585-604.

Salovaara, A., Lyytinen, K. and Penttinen, E. (2019), "High reliability in digital organizing: mindlessness, the frame problem, and digital operations", *MIS Quarterly*, Vol. 43 No. 2, pp. 555-578.

Schleicher, D.J., Baumann, H.M., Sullivan, D.W., Levy, P.E., Hargrove, D.C. and Barros-Rivera, B.A. (2018), "Putting the system into performance management systems: a review and agenda for performance management research", *Journal of Management*, Vol. 44 No. 6, pp. 2209-2245.

Siering, M., Muntermann, J. and Grčar, M. (2021), "Design principles for robust fraud detection: the case of stock market manipulations", *Journal of the Association for Information Systems*, Vol. 22 No. 1, p. 4.

Sternberg, R.J. (2000), "Images of mindfulness", *Journal of Social Issues*, Vol. 56 No. 1, pp. 11-26.

Syed, R. (2019), "Enterprise reputation threats on social media: a case of data breach framing", *The Journal of Strategic Information Systems*, Vol. 28 No. 3, pp. 257-274.

Te'eni, D., Seidel, S. and Brocke, J. (2017), "Stimulating dialog between information systems research and practice", *European Journal of Information Systems*, Vol. 26 No. 6, pp. 541-545.

Tremaine, D.W. (2022), "SEC proposes new cyber disclosure rules for public companies", Privacy & Security Law Blog, available at: https://www.lexology.com/library/detail.aspx?g=0ae50342-3c49-4464-a7a5-060d7794f5df.

Vance, A., Lowry, P.B. and Eggett, D. (2015), "Increasing accountability through user-interface design artifacts", *MIS Quarterly*, Vol. 39 No. 2, pp. 345-366.

Weick, K.E. and Roberts, K.H. (1993), "Collective mind in organizations: heedful interrelating on flight decks", *Administrative Science Quarterly*, Vol. 38 No. 3, pp. 357-381.

Wu, Y., Tayi, G.K., Feng, G. and Fung, R.Y. (2021), "Managing information security outsourcing in a dynamic cooperation environment", *Journal of the Association for Information Systems*, Vol. 22 No. 3, p. 2.

Yazdanmehr, A. and Wang, J. (2021), "Can peers help reduce violations of information security policies? The role of peer monitoring", *European Journal of Information Systems*, pp. 1-21.

Yazdanmehr, A., Wang, J. and Yang, Z. (2020), "Peers matter: the moderating role of social influence on information security policy compliance", *Information Systems Journal*, Vol. 30 No. 5, pp. 791-844.

Yoo, C.W., Goo, J. and Rao, H.R. (2020), "Is cybersecurity a team sport? A multilevel examination of workgroup information security effectiveness", *MIS Quarterly*, Vol. 44 No. 2, pp. 907-931.

Corresponding author
Allen C. Johnston can be contacted at: ajohnston@cba.ua.edu