Information Security Awareness: Literature Review and Integrative Framework

Lennart Jaeger
German Graduate School of Management and Law
lennart.jaeger@ggs.de

Abstract

Individuals' information security awareness (ISA) plays a critical role in determining their security-related behavior in both organizational and private contexts. Understanding this relationship has important implications for individuals and organizations alike who continuously struggle to protect their information security. Despite much research on ISA, there is a lack of an overarching picture of the concept of ISA and its relationship with other constructs. By reviewing 40 studies, this study synthesizes the relationship between ISA and its antecedents and consequences. In particular, we (1) examine definitions of ISA; (2) categorize antecedents of ISA according to their level of origin; and (3) identify consequences of ISA in terms of changes in beliefs, attitudes, intentions, and actual security-related behaviors. A framework illustrating the relationships between the constructs is provided and areas for future research are identified.

1. Introduction

In today's digital world, which is characterized by a strong reliance on information systems (IS), organizations continuously aim to uphold their information security. To protect IS and organizational information assets at the individual level, information security awareness (ISA) is considered a crucial factor in influencing secure behavior [7, 13]. In general, ISA considers an individual's knowledge and understanding of topics related to information security (e.g., security risks and threats, organizational security objectives, procedures, and policies) [37, 39, 42].

To attain deeper knowledge of individuals' ISA, IS scholars have carried out research to conceptualize the construct (e.g., [37]) and to analyze the associated antecedent and outcome factors through the lens of their respective discipline (e.g., [7, 13, 14]).

Despite the considerable advancements in this research area, several important issues remain to be addressed. First, some studies refer to the term ISA as a cognitive state of mind in the form of knowledge and understanding [7], a continuous intra-organizational process to achieve this state of mind [43], and/or some kind of security-related behavior [14], calling for clarification of the concept of ISA.

Second, since multiple factors related to ISA were examined, a framework for consolidating them and building a holistic view of ISA is needed. Related to this issue, very different types of antecedents were identified, which range from individual characteristics through organizational and regulatory awareness-raising activities to software applications with awareness-features (e.g. [21, 26, 38, 43]). Yet, the different levels from where they influence ISA are not well established, which raises the issue of how to utilize these factors to increase an individual's ISA in an effective manner.

In a similar way, several consequences and outcomes of ISA were studied, including belief factors, attitudes, behavioral intentions and actual behaviors, but how they are organized and interrelated is not clear, either (for instance, prior literature reviews allegedly deal with ISA but rather consider security behavior; cf. [30]). Without an organization of factors, it is difficult to use them to develop and implement adequate action plans to manage information security.

To address these issues, this study provides a review on ISA, including its definition, its antecedents, and its outcomes. Building on the review, the relationships between the factors are illustrated in a framework and further research opportunities are identified. Thus, the research objectives include (1) the integration of research in the behavioral information security field and the development of a comprehensive view on ISA, (2) the organization of the antecedents and outcomes of ISA to better understand their impact, and (3) the provision of prescriptions for future research.

URI: http://hdl.handle.net/10125/50482
ISBN: 978-0-9981331-1-9

The remainder of the paper is structured as follows. Next, the methodology for identifying, selecting and classifying articles is described. The third section reports the findings of the review followed by the provision of an integrative framework and identification of eight prescriptions for future research. Finally, implications and limitations are discussed.

2. Research methodology

This study follows the common approaches of a literature review (e.g., [45]). In the first step, the search criteria are specified, the journal pool, search string and time range are selected, and articles are extracted. Next, the unit of analysis and coding scheme are determined, i.e. constructs are coded and categorized. Finally, the data is analyzed. A detailed description of these steps follows.

With regard to the specification of search criteria, the following inclusion and exclusion criteria were applied. First, only studies in the information security domain are considered, whereas other topics such as physical security are not discussed. The second criterion relates to the individual-level, as we consider only employees' and IS users' ISA. Other levels of research such as from a social perspective are excluded. Third, this study analyzes empirically tested or proposed behavioral studies only, which excludes other types of research such as design studies and descriptive studies. Fourth, to be included, studies needed to have a construct related to ISA, which means that studies considering awareness without a construct or merely mentioning its importance are not considered. Finally, to improve rigor, the focus of this review is on peer-reviewed academic research, which excludes practitioner articles, dissertations, and books.

To ensure a rigorous and systematic search [45], a meta-search engine that integrates search results from several academic literature databases (see www.litsonar.com) was used. Here, all 109 publication outlets of the "Association for Information Systems (AIS) Toplist" were selected and then searched whether a publication contained the term 'awareness' in the title, abstract or keywords by directly accessing the outlet or generating search queries for the following databases: ACM Digital Library, AISeL, EBSCO Business Source Complete, ScienceDirect, and IEEEXplore. Further search options included that no restrictions for a time period were set and that only peer-reviewed articles should be considered. By using 'awareness' as a broad search term, a search result as comprehensive as possible was generated, i.e. 1832 potentially relevant publications were identified in total. These articles were manually examined to filter out those publications that did not meet our previously described inclusion and exclusion criteria. This filtering process resulted in 26 conceptual and empirical articles. Next, these articles were used to conduct backward and forward searches resulting in additional 32 articles, of which 14 were selected following the previously described filtering criteria.

The unit of analysis considers constructs and their causal relationships including the following items: (1) explicit definitions of awareness constructs, (2) antecedents, and (3) outcomes. The coding results of the final set of 40 selected publications on ISA including authors, publication outlet, and their allocation to the three criteria are presented in Table 1 in the appendix.

3. Research findings

In this section, findings from the content analysis are reported, including a categorization of definitions, antecedents, and outcomes of ISA.

3.1 Definitions of ISA

By analyzing the concept of awareness as it is perceived in the IS security literature, several more or less distinctive definitions are identified. Awareness does not only cover aspects of an individual's *cognitive state of mind*, such as being conscious or having knowledge of something (e.g., [7, 13, 35]), some definitions also include *procedural aspects*, i.e. the processes used to achieve this state of mind (e.g., [43]). Few definitions do not distinguish awareness from a certain kind of *behavior* (e.g., [18, 38]).

By understanding information security awareness (ISA) as cognitive state of mind, Bulgurcu et al. [7] distinguish the concept into the overall knowledge and understanding about security issues and their potential consequences on the one hand, and about requirements prescribed in the organization's information security policies on the other hand. A further example is provided by Rhee et al. [35], who define ISA as "the vigilance in understanding various information security threats and in perceiving one's vulnerability related to these threats" (p. 2). In contrast, Tsohou et al. [43] regard ISA as "a process that aims at changing individuals' perceptions, values, attitudes, behavior, norms, work habits, and organizational culture and structures with regard to secure information practices" (p. 1). Behavioral aspects are considered by Spears and Barki [38] who regard ISA as a state reflected in the behavior of target groups (e.g., employees) and by Galvez and Guzman [18] who consider ISA as one of the information security behaviors.

In the remainder of the review, we consider ISA from the cognitive state of mind perspective to clearly differentiate it from the awareness-raising processes and subsequent outcome factors, such as behavioral reactions. This perspective implies that awareness-raising processes (i.e., antecedents of ISA) represent input variables of ISA, whereas the subsequent belief, attitudinal and behavioral reactions represent output variables.

3.2 Antecedents of ISA

This section reviews publications proposing or empirically investigating antecedents of ISA. The antecedents are organized based on their levels of origin: individual factors, organizational factors, social-environmental factors, and technological factors. In the following, a summary of these factors is provided.

3.2.1. Individual antecedents. The individual level includes factors originating from the employee or IS user. An individual's general *IS knowledge* has been empirically found as a determinant of ISA, since the higher their knowledge of basic IS applications the more likely individuals are aware of security-related issues [21, 36]. Previous *negative experience* with information security incidents has been found to lead to higher levels of an individual's ISA [21]. On the other hand, *computer anxiety* (i.e., the fears users feel in working with computers) has been found to negatively impact users' awareness of security measures [29].

3.2.2. Organizational antecedents. The organizational level covers factors under the influence of an organization. It is suggested that the *formalization of work procedures*, which make it more likely that awareness-increasing security controls exist, organizational *IS security communication*, and the individual's *perception of value of information* increases an individual's ISA through a heightened perception of the importance of information protection [20]. In addition, *management's support of IS security initiatives* by championing them is considered to be a main driver for making each individual aware of the importance of information security and evoking a company-wide ISA [25]. Furthermore, information security policies (ISPs) are considered to be an important information security management practice and the *provision and promotion of IPSs* has been empirically found to be an effective organizational practice to increase individuals' awareness of information security issues [21]. Another important information security management practice to increase ISA of various stakeholders are *security education, training, and awareness raising (SETA) programs*. SETA programs aim to increase employees' security expertise, to develop security-relevant skills and competencies, and to make them aware of the importance of security and potential security issues (e.g. risks, threats) as well as procedures, rules, and procedures stated in the ISPs [13, 39, 47]. Empirical support for SETA programs increasing individuals' ISA has been provided by several studies [9, 13, 21, 39]. Another valuable method for raising ISA is the involvement of IS end-users in the development process of organizational information security controls. Spears and Barki [38], for instance, applied user participation theories and empirically demonstrated that *users' participation* in security risk management processes contributed to an increased awareness of organizational policies, procedures and security risks along different target groups.

3.2.3. Social-environmental antecedents. The social-environmental level incorporates factors not under the direct influence of the organization's management and originates from individuals' interaction with their social environment. Hadasch et al. [20] proposed that *public expectations of information protection* as well as *security requirements from regulatory bodies and business partners* heighten an individual's ISA through the individual's perception of information leakage incidents as being a threat. *Secondary sources* (e.g. media information about security issues) have a positive impact on ISA by awakening interest and knowledge about information security [21, 33]. Social learning cues that positively impact employees' awareness of organizational ISPs include *security-related peer behavior* (also termed vicarious experience) [21, 27], *situational support* (i.e., the degree to which employees perceive their task environment favors ISP compliance) and *verbal persuasion* (i.e., feedback or instructions received by others to support ISP compliance) [27]. Albeit not empirically tested, it is suggested that *public awareness campaigns* or awareness programs are possible measures to raise users' awareness and sensitize them towards protecting their data [28].

3.2.4. Technological antecedents. Influencing factors at the technological level originate from technical tools with integrated awareness features that were designed and developed with the objective to increase users' ISA in specific software applications by alerting the users to possible security threats that may arise. *Just-in-time reminders* in the form of pop-ups as SETA program components intended to raise employees' ISA attract employees' attention and reminds them of what has been learned in previous security training about, for instance, disclosing customer information [26]. Similarly, the frequency of received information *security warning messages* was proposed but not yet empirically tested to increase individuals' levels of ISA [49].

3.3 Outcomes of ISA

The outcomes of ISA also received considerable attention in research. Most of these factors were analyzed using the perspective of the theory of reasoned action (TRA; [17]) and the theory of planned behavior (TPB; [1]). This includes belief factors, attitudes, behavioral intentions, and actual behaviors, which are summarized in the following.

3.3.1. Beliefs. We identified 17 variables through which ISA indirectly affects attitudes, behavioral intentions, and actual behaviors (owing to the limitations of space, definitions are not provided but are available from the authors upon request). These variables relate to behavioral beliefs, instrumental beliefs, and normative beliefs.

With regard to behavioral beliefs, an individual's increased ISA leads to the formation of outcome beliefs of a certain kind of behavior. For instance, ISA is positively associated with beliefs about the benefit of ISP compliant behavior, which include *intrinsic benefit*, *safety*, *rewards* [7], *perceived response efficacy* [34], and *ISP-related personal norms* [48]. Further, ISA is associated with beliefs about the costs of ISP compliant behavior, which includes a negative relationship with *work impediment* [7] and a positive relationship with *perceived response cost* [34]. With regard to beliefs about the cost of noncompliant behavior, ISA is positively associated with *intrinsic cost*, *vulnerability*, and *sanctions* [7]. Sanctions have also been considered as a dyadic construct including *perceived certainty of sanctions* and *perceived severity of sanctions,* which are positively influenced by user awareness of security countermeasures (security policies, SETA programs, and computer monitoring) [10, 12, 13, 24]. With regard to instrumental beliefs about adopting technologies, ISA positively influences both *perceived usefulness* (e.g., of firewalls to protect home computers [29] and of ISPs [2]) and *perceived ease of use* (e.g., of ISPs [2]). With regard to normative beliefs, ISA positively influences *subjective norm* about using protective technologies, such as antispyware software [14], and *social norms* about acceptable ISP compliant behavior [4].

3.3.2. Attitudes. Following TRA and TPB, attitude is the direct outcome of beliefs, which was examined in many studies. Several studies found empirical evidence that ISA positively impacts attitudes toward ISPs compliance directly [4–7] and indirectly via several belief factors [6, 7]. Similarly, Dinev and Hu [14] showed that technology awareness positively influenced attitude toward using security technologies (e.g., anti-spyware software) and Kumar et al. [29] showed a direct positive effect of awareness of security measures on attitude towards using a firewall and an indirect positive impact via perceived usefulness.

3.3.3. Behavioral intentions. *Behavioral intention* has an essential role in human behavior [1, 17]. Empirical studies in this area have been categorized into two fields with regard to whether they refer to behavior that is supportive vs. disruptive of security. Examples of behavioral intentions that are supportive of security include intentions to comply with ISPs [3, 7, 21, 34, 37] and to adopt security technologies [14, 22, 29, 31]. Examples of behavioral intentions that are disruptive of security include intention to commit IS access policy violation [44] and to misuse IS [13, 24]. Here, the general conclusion is that ISA has a positive impact on behavioral intentions that are supportive of security and a negative impact on intentions that are disruptive of security.

3.3.4. Actual behaviors. Several studies also analyzed the impact of ISA on *actual behavior*. Following the same two-field classification as described in the previous subsection, examples of actual behaviors that are supportive of security include controlling insider threats to information security [47], information security practices at work [18], coping with system risk [39], managerial actions toward information security [8], ISP compliant behavior [48], and desktop security behaviors [23, 46]. The first two studies are of conceptual nature and propose that ISA may be a major factor in reducing insider threats and increasing security practices at work. The last five studies find empirical evidence that ISA positively impacts managers' coping behavior with system risk and their actions towards information security, increases employees' ISP compliance, and improves home users' desktop security behaviors.

In contrast, actual security disruptive behaviors include problematic IS security behavior [40] and unauthorized information disclosure [26]. Takemura [40], for instance, found that problematic IS security behavior with regard to organizational information security measures is reduced significantly when individuals have higher levels of ISA.

3.4 Moderating effects involving ISA

Some studies examined factors that moderate the relationship between ISA and outcome variables. *Computer self-efficacy* and *perceived virtual status* were found to negatively moderate the effects of ISA on unauthorized access intentions [11]. Further, the relationship between social learning cues and ISA has been weaker for remote employees in comparison to in-house employees, suggesting a moderating role of *"remote" status* [27]. Further studies have proposed that personality attributes and traits (e.g., *conscientiousness*; [32]) might have an important role in the relationship between ISA and security behavior.

4. Discussion

The review identified multiple antecedents and outcomes related to information security awareness (ISA) and building a holistic view of these factors is important for additional research and practice.

Based on our review, an integrative framework for the study on ISA as an individual's cognitive state of mind is provided in Figure 1. The central construct in this figure is ISA, with its antecedents originating from the individual, organizational, social-environmental, and technological level (on the left) as well as its outcomes and their relationships (on the right). The literature review described in detail the, so that the emphasis in the following is to work out prescriptions for future research using the insights of the literature review and the framework. Dotted circles in Figure 1 indicate where the prescriptions fit into the framework.

4.1. Prescriptions from the definition of awareness analysis

The first objective was to analyze how ISA is perceived and conceptualized in the information security community by looking at the various definitions. Although a considerable amount of research has been done, a coherent conceptualization of awareness is lacking. While a concerning amount of studies do not provide an explicit definition, the analysis showed that ISA is perceived as a multidimensional issue covering cognitive, process, and behavioral aspects.

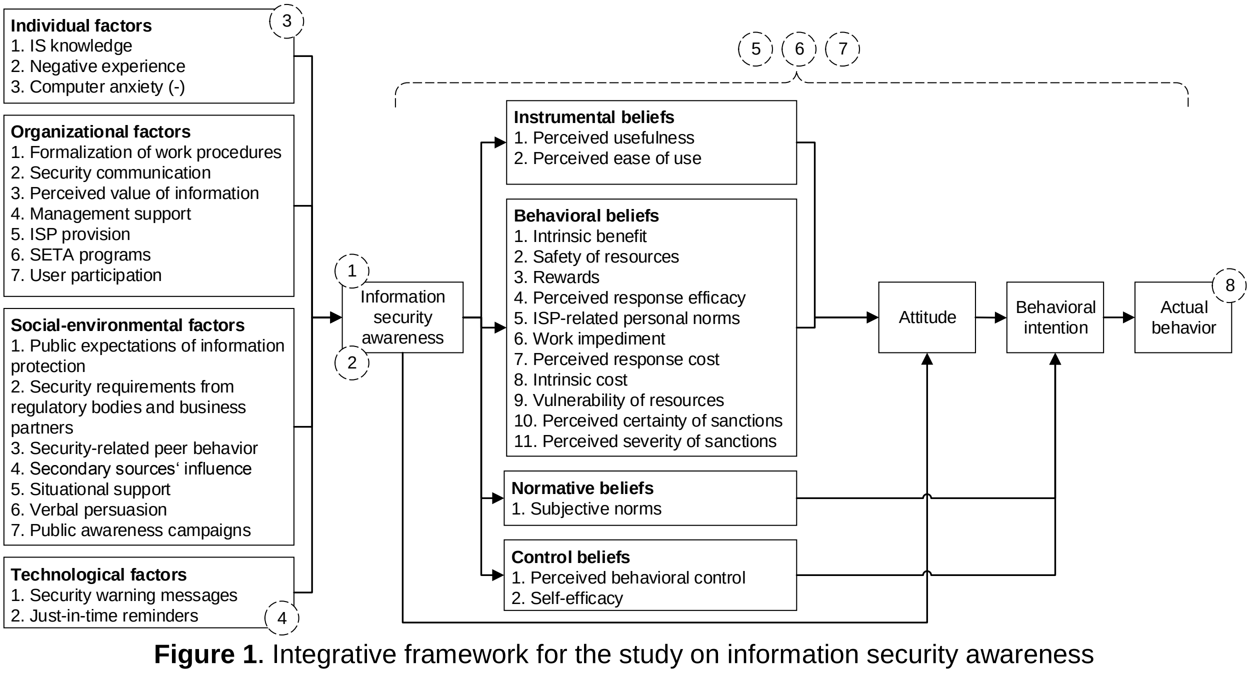
Individual factors
1. IS knowledge
2. Negative experience
3. Computer anxiety (-)
Organizational factors
1. Formalization of work procedures
2. Security communication
3. Perceived value of information
4. Management support
5. ISP provision
6. SETA programs
7. User participation
Social-environmental factors
1. Public expectations of information protection
2. Security requirements from regulatory bodies and business partners
3. Security-related peer behavior
4. Secondary sources' influence
5. Situational support
6. Verbal persuasion
7. Public awareness campaigns
Technological factors
1. Security warning messages
2. Just-in-time reminders
Information security awareness
Instrumental beliefs
1. Perceived usefulness
2. Perceived ease of use
Behavioral beliefs
1. Intrinsic benefit
2. Safety of resources
3. Rewards
4. Perceived response efficacy
5. ISP-related personal norms
6. Work impediment
7. Perceived response cost
8. Intrinsic cost
9. Vulnerability of resources
10. Perceived certainty of sanctions
11. Perceived severity of sanctions
Normative beliefs
1. Subjective norms
Control beliefs
1. Perceived behavioral control
2. Self-efficacy
Attitude
Behavioral intention
Actual behavior
1
2
3
4
5
6
7
8

Figure 1. Integrative framework for the study on information security awareness

Accordingly, different understandings of the concept of awareness exist, and consequently different angles from which it can be approached and examined. However, by not clearly separating those three aspects but merging them, a diffuse and partially inconsistent understanding of the term prevails.

The revelation of terminology ambiguity implies a need for future research to create a well-defined set of terms for awareness, since a consistent understanding of the subject matter is crucial for value-adding studies. The study findings and insights could be considered as a starting point to further examine the conceptualization and nature of awareness. We suggest that research should explicitly indicate which aspect of awareness (either cognitive, process, or behavior) is examined. This helps to clearly specify the impact of the antecedent factors and the effect on the outcome factors. In particular, our integrative framework (Figure 1) implies that awareness raising processes represent an input variable of ISA (as a cognitive state of mind), whereas behavior represents an output variable. The first prescription includes:

1. *Overcome terminology ambiguity by establishing a basic consensus of the nature of awareness and by differentiating ISA as a cognitive state of mind from awareness-raising activities and subsequent behaviors.*

Current research predominantly relies on static aspects of ISA, such as the general knowledge and understanding of security threats and information security policies (e.g., [7]). However, static awareness concepts are often formed before individuals perform a security-relevant behavior and thus do not reflect situation-specific aspects of the process individuals follow while performing secure behavior. Individuals may be considered security aware in general, but in a certain usage situation they might be unaware that they are confronted with a security-related issue. Little attention has been paid to the role that a specific situation plays in regulating awareness and its behavioral outcomes. We propose to consider situational aspects in explaining individuals' security-related behavior by conceptualizing and examining individuals' level of situation awareness of security threats. The three-level model of situation awareness [16] could be used as a theoretical foundation and an individual's perception, comprehension, and projection of information security threats could be measured by applying experimental study designs. Hence:

2. *Reflect individuals' level of situation awareness in information security to further investigate the concept of ISA.*

4.1. Prescriptions from the antecedents of awareness analysis

Within the in-depth analysis, a broad set of determinants are discovered and classified into individual, organizational, social-environmental, and technological influencing factors of awareness according to their levels of origin.

On the individual level, general IS knowledge, negative experience with incidents and computer anxiety were found to determine ISA. As research on individual-level antecedents is limited, more attention towards them is still required. Further individual-level antecedents, such as personality traits, demographics (age, gender, education, income) or characteristics (workload, overall job attitude, organizational commitment) should be examined with empirical research. One particular direction for future research could be to investigate the individuals' hierarchy level in a company, i.e. whether factors influencing employees' ISA (as it has been mainly examined in the reviewed studies) also influence managers' ISA (which has been largely left unregarded). This line of research is particularly important in light of a study done by Taylor [41] who identified an optimistic bias among managers, in particular managers were unaware of the security risk arising from employees' unintentional actions. Hence:

3. *Study different types of stakeholders while further investigating influencing factors of ISA.*

On the organizational level, SETA programs and the provision of ISPs have been identified as important security management practices to increase an individual's ISA. Whereas these security management practices focus on non-technical means to increase an individual's ISA, future research should aim to explore further potential antecedents, which are of technical nature. For this purpose, the effectiveness of tools providing information about security issues or referring to the organization's ISPs immediately before a foreseeable security breach (e.g., an ISP violation) in raising an individual's ISA could be examined. This line of thought has been investigated in information privacy research (e.g., warning mechanisms provided by tools before disclosing personal information), but with few exceptions neglected to a large extent in information security research. Thus:

4. *Further investigate the effectiveness of technical means to increase ISA.*

4.2. Prescriptions from the outcomes of awareness analysis

The last focus of this review was to provide insights into outcomes of awareness and associated relationships with other constructs. The in-depth analysis has shown that an individual's ISA is regarded as one of the central antecedents of behavior that is supportive or disruptive of security. However, there are several limitations to the empirical studies investigating the effect of ISA on security-related behavior.

Many studies are conducted in western cultures (e.g., USA), thereby neglecting possible cultural differences. However, findings of Hovav and D'Arcy [24] indicate that cultural differences associated with ISA's impact on IS misuse might exist between South Korean and US users. Further insights into the relationship between ISA and security-related behavior with samples from different countries needs to be gained. In addition to cross-cultural differences with regard to cultural values (e.g., power distance, individualism, uncertainty avoidance), regulatory structures (omnibus, sectoral, or non-regulation/self-help) might differ across countries and should be examined in greater detail. Thus:

5. *Further investigate cross-cultural differences involving ISA and security-related behavior.*

With the increasing use of private devices (e.g., private smartphones, home computers) to access organizational IS and the blurring boundaries between work and personal business, security-related behavior is also relevant in contexts outside of the organization. However, many studies focus on behaviors of individuals within organizational settings. Remote employees, for instance, are an understudied class of employees who tend to exhibit lower levels of ISA in comparison with their in-house colleagues [27]. As organizational security practices may be less prevalent in remote workplaces and own practices of security protection may be more dominant, potential distinctions in ISA and its relationship with behavior regarding different work settings should be analyzed. Hence:

6. *Consider the influence of ISA on behavior in contexts outside of the organization.*

Some studies indicate that individual characteristics (personality attributes and traits) may moderate the relationship between ISA and behavior. However, few studies address the effects of individual characteristics on this relationship empirically. Understanding the differences between individuals is essential to understanding underlying psychological mechanisms impacting the relationship between ISA and behavior. Thus, the effects of demographic factors (e.g., age, gender, education, income), personality traits (e.g., Big Five personality traits), and psychological states (e.g., a psychological need for safety, risk-taking propensity) should be further investigated with cumulative research. Thus:

7. *Conduct additional research for a better understanding of moderating effects involving ISA and behavior.*

Finally, several studies used very static and generic measures for behavioral intention, like ISP compliance [7, 34] or IS misuse intentions [13, 24]. Further studies could enquire situation-specific behaviors, i.e. behavioral reactions at the moment that a security-related event occurs. For instance, upon receiving a phishing mail, security aware employees may try to verify the sender address, delete it and/or inform colleagues or the IT department in the organization. On the other hand, unaware employees may download a malicious attachment followed by executing it. By capturing the nuances of the process individuals follow while performing secure or unsecure behavior, new insights into the complex interaction of information processing (how employees become aware of a threat) and decision making can be gained. Thus:

8. *Apply more situation-specific measures of ISA and behavior.*

4.3. Theoretical and practical implications

This study contributes to the literature in several ways by providing a comprehensive review of studies on individual's ISA and creating a holistic picture of the construct and its relationship with several antecedent and outcome factors.

First, researchers are advised to explicitly indicate which type and aspect of awareness, either cognitive, process, or behavior, is examined in their study on ISA. This contributes to unambiguously determining the impact of the antecedent factors and the effect on the outcome factors. Further, the categorization of antecedent factors into four levels of origin may help empirical studies to structure their factors and by considering all four levels in their research help to provide a more comprehensive picture. Last but not least, the categorization of behaviors according to their supportive vs. disruptive nature helps to identify which kind of behaviors have been neglected by prior studies and should be further examined. Naturally, it is desirable that the framework for ISA research based on the in-depth analysis is empirically tested in whole or in blocks using surveys or experiments, or by conducting meta-analyses on prior research.

For practitioners, identifying and understanding the different types of antecedents of ISA at four different levels yields crucial insights to ensure the success of information security objectives and encourage the desired security-related behavior. A combination of antecedents at different levels seems promising. For instance, managers could increase their employees' ISA not only through SETA programs and ISPs but also by identifying and supporting security-aware employees, who champion information security awareness among other employees (since observing peers' compliant behavior has been found to increase ISA).

For individuals, several factors influencing their security-related behaviors were highlighted. A selected combination of the identified antecedents of awareness may help individuals to become equipped with the necessary knowledge and skills to make informed decisions on how to deal with security issues.

4.4. Limitations of the literature review

Although this literature review provides valuable insights into the concept of awareness within IS security research and points to several research gaps, some limitations need to be considered. First, the findings of this review are limited by the selection of the literature. The review is based on a comprehensive evaluation of peer-reviewed journals and conference proceedings. Although the inclusion of publications of controlled quality ensures a high quality of the literature base, some relevant contributions may be missing in the review due to the exclusion of non-peer-reviewed publications. Second, the search and selection process further restricts the results. In particular, the search term applied is limited to the English language by which publications in other languages are neglected. Third, this research considers only awareness-related constructs in the information security realm. A comparison with similar constructs such as security knowledge or mindfulness could help to enhance knowledge of the employees' cognitive states of mind related to security.

In conclusion, research on information security awareness is still an evolving field with many uncharted areas to be explored. Further empirical studies that build upon the research opportunities recognized in this study are needed.

5. References

[1] Ajzen, I., "The theory of planned behavior", Organizational Behavior and Human Decision Processes, 50(2), 1991, pp. 179–211.

[2] Al-Omari, A., O. El-Gayar, and A. Deokar, "Information security policy compliance: A user acceptance perspective", in MWAIS 2011 Proceedings, Omaha, NE, 2011.

[3] Al-Omari, A., Omar El-Gayar, and Amit Deokar, "Security policy compliance: User acceptance perspective.", in HICSSS 2012 Proceedings, Hawaii, Honolulu, 2012.

[4] Bauer, S. and E.W. Bernroider, "From Information Security Awareness to Reasoned Compliant Action", ACM SIGMIS Database: the DATABASE for Advances in Information Systems, 48(3), 2017, pp. 44–68.

[5] Bélanger, F., S. Collignon, K. Enget, and E. Negangard, "Determinants of early conformance with information security policies", Information & Management(In Press), 2017.

[6] Bulgurcu, B., H. Cavusoglu, and I. Benbasat, "Roles of information security awareness and perceived fairness in information security policy compliance", in AMCIS 2009 Proceedings, San Francisco, California, USA, 2009.

[7] Bulgurcu, B., H. Cavusoglu, and I. Benbasat, "Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness", MIS Quarterly, 34(3), 2010, pp. 523–548.

[8] Choi, N., D. Kim, J. Goo, and A. Whitmore, "Knowing is doing: An empirical validation of the relationship between managerial information security awareness and action", Information Management & Computer Security, 16(5), 2008, pp. 484–501.

[9] Culnan, M.J., E.R. Foxman, and A.W. Ray, "Why IT Executives Should Help Employees Secure Their Home Computers", MIS Quarterly Executive, 7(1), 2008, pp. 49–56.

[10] D'Arcy, J. and A. Hovav, "Towards a best fit between organizational security countermeasures and information systems misuse behaviors", Journal of Information System Security, 3(2), 2007, pp. 3–30.

[11] D'Arcy, J. and A. Hovav, "Does one size fit all? Examining the differential effects of IS security countermeasures", Journal of Business Ethics, 89, 2009, pp. 59–71.

[12] D'Arcy, J. and A. Hovav, "Deterring internal information systems misuse", Communications of the ACM, 50(10), 2007, pp. 113–117.

[13] D'Arcy, J., A. Hovav, and D. Galletta, "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach", Information Systems Research, 20(1), 2009, pp. 79–98.

[14] Dinev, T. and Q. Hu, "The Centrality of Awareness in the Formation of User Behavioral Intention toward Protective Information Technologies", Journal of the Association for Information Systems, 8(7), 2007, pp. 386–408.

[15] El-Haddadeh, R., A. Tsohou, and M. Karyda, "Implementation Challenges for Information Security Awareness Initiatives in E-Government", in ECIS 2012 Proceedings, Barcelona, Spain, 2012.

[16] Endsley, M.R., "Toward a Theory of Situation Awareness in Dynamic Systems", Human Factors: The Journal of the Human Factors and Ergonomics Society, 37(1), 1995, pp. 32–64.

[17] Fishbein, M. and I. Ajzen, Belief, attitude, intention and behavior: An introduction to theory and research, Reading, MA: Addison-Wesley, 1975.

[18] Galvez, S.M. and I.R. Guzman, "Identifying factors that influence corporate information security behavior", in AMCIS 2009 Proceedings, San Francisco, California, USA, 2009.

[19] Goodhue, D.L. and D.W. Straub, "Security concerns of system users", Information & Management, 20(1), 1991, pp. 13–27.

[20] Hadasch, F., B. Mueller, and A. Maedche, "Exploring Antecedent Environmental and Organizational Factors to User-Caused Information Leaks: a Qualitative Study", in ECIS 2012 Proceedings, Barcelona, Spain, 2012.

[21] Haeussinger, F. and J. Kranz, "Information Security Awareness: Its Antecedents and Mediating Effects on Security Compliant Behavior", in ICIS 2013 Proceedings, Milan, Italy, 2013.

[22] Han, B., Y. Wu, and J. Windsor, "User's adoption of free third-party security apps", Journal of Computer Information Systems, 54(3), 2014, pp. 77–86.

[23] Hanus, B. and Y. Wu, "Impact of Users' Security Awareness on Desktop Security Behavior: A Protection Motivation Theory Perspective", Information Systems Management, 33(1), 2016, pp. 2–16.

[24] Hovav, A. and J. D'Arcy, "Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the U.S. and South Korea", Information & Management, 49(2), 2012, pp. 99–110.

[25] Hu, Q., P. Hart, and D. Cooke, "The role of external and internal influences on information systems security – a neo-institutional perspective", The Journal of Strategic Information Systems, 16(2), 2007, pp. 153–172.

[26] Jenkins, J.L. and A. Durcikova, "What, I Shouldn't Have Done That?: The Influence of Training and Just-in-Time Reminders on Secure Behavior", in ICIS 2013 Proceedings, Milan, Italy, 2013.

[27] Johnston, A.C., B. Wech, and E. Jack, "Engaging Remote Employees: The Moderating Role of "Remote" Status in Determining Employee Information Security Policy Awareness", Journal of Organizational and End User Computing, 25(1), 2013, pp. 1–23.

[28] Ku, Y.-C., R. Chen, and H. Zhang, "Why do users continue using social networking sites? An exploratory study of members in the United States and Taiwan", Information & Management, 50(7), 2013, pp. 571–581.

[29] Kumar, N., K. Mohan, and R. Holowczak, "Locking the door but leaving the computer vulnerable: Factors inhibiting home users' adoption of software firewalls", Decision Support Systems, 46(1), 2008, pp. 254–264.

[30] Lebek, B., J. Uffen, M. Neumann, B. Hohler, and M. H. Breitner, "Information security awareness and behavior: A theory-based literature review", Management Research Review, 37(12), 2014, pp. 1049–1092.

[31] Maitland, C.F., H.F. Thomas, and L.-M.N. Tchouakeu, "Internet censorship circumvention technology use in human rights organizations: An exploratory analysis", Journal of Information Technology, 27(4), 2012, pp. 285–300.

[32] Mancha, R. and G. Dietrich, "Development of a Framework for Analyzing Individual and Environmental Factors Preceding Attitude toward Information Security", in AMCIS 2007 Proceedings, Keystone, Colorado, USA, 2007.

[33] Mani, D., S. Mubarak, and K.-K.R. Choo, "Understanding the Information Security Awareness Process in Real Estate Organizations Using the Seci Model", in AMCIS 2014 Proceedings, Savanna, Georgia, USA, 2014.

[34] Putri, F.F. and A. Hovav, "Employees' Compliance with BYOD Security Policy: Insights from Reactance, Organizational Justice, and Protection Motivation Theory", in ECIS 2014 Proceedings, Tel Aviv, Israel, 2014.

[35] Rhee, H.-S., Y.U. Ryu, and C.-T. Kim, "I Am Fine but You Are Not: Optimistic Bias and Illusion of Control on Information Security", in Proceedings of the 26th International Conference, Las Vegas, NV, 2005.

[36] Ryan, J., "Information security awareness: an evaluation among business students with regard to computer self-efficacy and personal innovation", in AMCIS 2007 Proceedings, Keystone, Colorado, USA, 2007.

[37] Siponen, M.T., "A conceptual foundation for organizational information security awareness", Information Management & Computer Security, 8(1), 2000, pp. 31–41.

[38] Spears, J.L. and H. Barki, "User participation in information systems security risk management", MIS Quarterly, 34(3), 2010, pp. 503–522.

[39] Straub, D.W. and R.J. Welke, "Coping with Systems Risk: Security Planning Models for Management Decision Making", MIS Quarterly, 22(4), 1998, pp. 441–469.

[40] Takemura, T., "Statistical Analysis on Relation between Workers' Information Security Awareness and the Behaviors in Japan", Journal of Management Policy and Practice, 12(3), 2011, p. 27.

[41] Taylor, R., "Management Perception of Unintentional Information Security Risks", in ICIS 2006 Proceedings, Milwaukee, Wisconsin, USA, 2006.

[42] Thomson, M.E. and R. von Solms, "Information security awareness: educating your users effectively",

Information Management & Computer Security, 6(4), 1998, pp. 167–173.

[43] Tsohou, A., M. Karyda, S. Kokolakis, and E. Kiountouzis, "Managing the introduction of information security awareness programmes in organisations", European Journal of Information Systems, 24(1), 2015, pp. 38–58.

[44] Vance, A., P.B. Lowry, and D. Eggett, "Using Accountability to Reduce Access Policy Violations in Information Systems", Journal of Management Information Systems, 29(4), 2013, pp. 263–290.

[45] Webster, J. and R.T. Watson, "Analyzing the past to prepare for the future: Writing a literature review", MIS Quarterly, 26(2), 2002, p. 3.

[46] White, G., T. Ekin, and L. Visinescu, "Analysis of Protective Behavior and Security Incidents for Home Computers", Journal of Computer Information Systems, 57(4), 2017, pp. 353–363.

[47] Yayla, A.A., "Controlling insider threats with information security policies", in ECIS 2011 Proceedings, Helsinki, Finland, 2011.

[48] Yazdanmehr, A. and J. Wang, "Employees' information security policy compliance: A norm activation perspective", Decision Support Systems, 92, 2016, pp. 36–46.

[49] Zhang, P. and X. Li, "Determinants of Information Security Awareness: An Empirical Investigation in Higher Education", in ICIS 2015 Proceedings, Fort Worth, USA, 2015.

Appendix

Table 1. Literature reviewed in the study and unit of analysis (1-3)

Author	Outlet	Definition (1)	Antecedents (2)	Outcomes (3)	Author	Outlet	Definition (1)	Antecedents (2)	Outcomes (3)
[2]	MWAIS	A		*	[24]	IM	A		*
[3]	HICSS	A		*	[25]	JSIS		*	
[4]	SIGMIS	A	*	*	[26]	ICIS			*
[5]	IM	A	*	*	[27]	JOEUC	A	*	
[6]	AMCIS	A		*	[28]	IM		*	
[7]	MISQ	A	*	*	[29]	DSS			*
[8]	IMCS	A		*	[33]	AMCIS	A	*	
[9]	MISQE			*	[34]	ECIS			*
[10]	JISSEC	A		*	[35]	ICIS	A		
[11]	JBE	A		*	[36]	AMCIS		*	
[12]	CACM	A		*	[37]	IMCS	A,C	*	*
[13]	ISR	A		*	[38]	MISQ	A,C	*	
[14]	JAIS	A,C		*	[39]	MISQ		*	*
[15]	ECIS	B	*		[40]	JMPP	A	*	
[18]	AMCIS	A,C		*	[43]	EJIS	B	*	
[19]	IM			*	[44]	JMIS			*
[20]	ECIS		*		[46]	JCIS			*
[21]	ICIS	A	*	*	[47]	ECIS		*	*
[22]	JCIS	A		*	[48]	DSS	A		*
[23]	ISM	A		*	[49]	ICIS	A	*	*

Note: A = cognitive aspects; B = process aspects; C = behavioural aspects. CACM = Communications of the ACM; DSS = Decision Support Systems; ECIS = Proceedings of the European Conference on Information Systems; EJIS = European Journal of Information Systems; IM = Information & Management; IMCS = Information Management & Computer Security; HICSS = Proceedings of the Hawaii International Conference on System Sciences; ICIS = Proceedings of the International Conference on Information Systems; IJEC = International Journal of Electronic Commerce; ISM = Information Systems Management; ISR = Information Systems Research; JAIS = Journal of the Association for Information Systems; JBE = Journal of Business Ethics; JCIS = Journal of Computer Information Systems; JISSEC = Journal of Information System Security; JMIS = Journal of Management Information Systems; JMPP = Journal of Management Policy and Practice; JOEUC = Journal of Organizational and End User Computing; JSIS = The Journal of Strategic Information Systems; MISQ = Management Information Systems Quarterly; MISQE = MIS Quarterly Executive; MWAIS = Proceedings of the Midwest United States Association for Information Systems; SIGMIS = ACM SIGMIS Database: the DATABASE for Advances in Information Systems