A descriptive review and classification of organizational information security awareness research

Gershon Hutchinson
Jacques Ophoff

This is the Author Accepted Manuscript of a conference paper published in Information and cyber security: 18th International conference, ISSA 2019, Johannesburg, South Africa, August 15, 2019, proceedings

The final authenticated version is available online at: https://doi.org/10.1007/978-3-030-43276-8_9

A Descriptive Review and Classification of Organizational Information Security Awareness Research

Gershon Hutchinson and Jacques Ophoff[0000-0003-0634-5248]

University of Cape Town, Cape Town, South Africa
HTCGER001@myuct.ac.za, jacques.ophoff@uct.ac.za

Abstract. Information security awareness (ISA) is a vital component of information security in organizations. The purpose of this research is to descriptively review and classify the current body of knowledge on ISA. A sample of 59 peer-reviewed academic journal articles, which were published over the last decade from 2008 to 2018, were analyzed. Articles were classified using coding techniques from the grounded theory literature-review method. The results show that ISA research is evolving with behavioral research studies still being explored. Quantitative empirical research is the dominant methodology and the top three theories used are general deterrence theory, theory of planned behavior, and protection motivation theory. Future research could focus on qualitative approaches to provide greater depth of ISA understanding.

Keywords: Organizational Information Security Awareness, Literature Review.

1 Introduction

Information security is still a cause of significant concern for modern organizations despite the variety of technological solutions developed to combat this problem [1] as the literature repeatedly stresses that humans are the weakest link in the information security chain [2, 3]. Information systems (IS) and organizations require the interactions of humans to exist. Humans build systems; humans use networks and services; humans manage organizations; organizations render services to humans; humans attack IS and organizations and not computing devices. With the impact that humans have on organizations and IT, it should be of no surprise the effect humans can have on information security [4].

Information security ensures business continuity and limits the impact of security incidents which can harm the organization [5]. The importance of human behavior in the context of information security has been recognized [e.g. 6, 7], particularly regarding user compliance to organizational information security policies (ISPs) [8, 9]. ISA is a vital component of information security [10, 11] and consists of general knowledge of information security and cognizance of organizational ISP awareness [9]. Information security challenges can be managed more successfully when the human factor is considered in combination with technological solutions [12].

This research aims to descriptively review and classify the current body of knowledge on organizational ISA research to answer the question: *What is the current state of organizational information security awareness research?* Okoli and Schabram [13] argue that literature reviews, per se, can constitute valuable and original work and it can be a starting point for individuals interested in a specific topic. An interpretive research stance was taken, with an inductive approach used to analyze secondary data and identified themes and patterns from the data.

The remainder of this paper is organized as follows: Section 2 reviews ISA key concepts and the extant literature in general. In Section 3, the research methodology is presented where the approach, philosophy, and methodologies used to carry out the research is explained. The classification and descriptive review provide a detailed analysis of the data in Section 4, and in Section 5, a discussion on the findings is presented. Finally, the conclusion summarizes the key findings, describes the practical implications, and provides recommendations for future research.

2 Background

ISA is a vital component of an effective information security management program [14]. Kruger and Kearney [15] state that the primary objective of ISA is to ensure that individuals are conscious of threats related to the use of IT and comply with the organization's policies and procedures. This definition recognizes a cognitive state of mind whereby the user's perception concerning secure information practices within the organization is pertinent and framed by ISPs [6]. Bulgurcu et al. [9] note that to have ISA, you should not only be information security conscious (understand that passwords are a necessary precaution) but also ISP conscious (understand the organizational requirements for passwords).

Due to its social nature, there is no general approach, definition, or method to ISA [16, 17]. Many studies consider ISA to be a cognitive state of mind which knows and understands information security risks, threats, organizational processes, policies, security objectives [9, 10, 18]. Bulgurcu et al. [9] and Parsons et al. [3] define ISA as the staff's cognizance of information security and ISPs of their organization. Rhee et al. [19] define ISA as alertness in understanding the different security threats and one's exposure to these threats, which contrasts with Tsohou et al. [20] who consider the procedural aspect to ISA, i.e. the process required to achieve secure information practices. One can define ISA as a process which changes user perceptions, behavior, norms, habits, attitudes and organizational culture and structure towards information security practices [21].

Defining a measurable criterion for a security conscious person is an important and challenging component for assessing ISA [11]. Based on the above definitions of ISA, we define ISA as an individual's general knowledge of information security and cognizance of their organization's ISPs. This definition is suitable as it contains both a cognitive state of mind where users know and understand the security mission of their organization [9] and the importance and significance of information security [3].

2.1 Measuring Information Security Awareness

IT has evolved to a point where actual behavioral monitoring of individuals is possible. However, researchers still find it difficult to conduct such studies due to factors such as company buy-in, legal ramifications, and community relations [7]. Most studies on ISA therefore use self-reporting measures, such as surveys, to measure perceptions of risk. The advantages of self-reporting measures are that they are easy to develop, distribute, and analyze. The disadvantages are that they are prone to demand effects and well-known biases such as demand bias, common methods bias, subjectivity bias, and social desirability bias [22].

2.2 Information Security Awareness Antecedents

Organizations recognize that staff can either be a risk or an asset in the fight against information security threats [9]. Awareness remains a vital issue of information security. Increasing individuals ISA through training and awareness programs could lead to safer technology use. However, such solutions are often overlooked by organizations [23]. Tsohou et al. [24] conclude that training and awareness programs are not efficient due to inadequate investments by organizations. Khan et al. [25] mention several recommended solutions which can be used to improve ISA such as computer-based training, video games, newsletters, information sessions, posters, and messages. They consider group discussion as the most effective method for measuring ISA as it enables two-way communication whereby each user can share experiences and knowledge.

Individual Antecedents. This level focuses on factors originating from the individual. Individuals with higher levels of ISA usually had prior security training or has a higher level of education [9]. Haeussinger and Kranz [16] noted that previous negative experiences with information security, such as malware or phishing attacks, are also likely to increase individuals' levels of ISA.

Organizational Antecedents. This level focuses on factors originating from the organization. This includes formalization of work procedures which identifies that security awareness controls exist and heightens individuals ISA [21]. Top management support is a crucial factor in ensuring staff compliance with ISPs [26] and organizational culture change [27]. Merete Hagen et al. [28] exclusively looked at non-technological solutions for information security and found ISPs to be a vital and critical component for the success of these solutions. The importance of ISPs has been established by several sources [9, 29, 30]. Another crucial antecedent is awareness campaigns such as security education, training and awareness (SETA) programs which strengthen individuals ISA [31]. SETA programs ensure the sustainability of ISPs by educating individuals of their importance and necessary precautions [29]. Other solutions include procedures [32], guidelines [29], campaigns, incentive programs [33], and fear appeals [34].

2.3 Theoretical Perspectives

Studies on behavior have stemmed from the disciplines of psychology and sociology which have been used and adapted by criminology. Information security researchers have often adapted criminology theories [35, 36] for investigating information security [e.g. 6, 25]. Reasons to use behavioral theories include a more profound consideration and understanding of the behavior problem and solutions to address the problem [6]. However, the main aim of behavioral research in information security is to understand why only specific individuals adhere to organizational ISPs [36]. Lebek et al. [36] conducted a theory-based review of security awareness in behavioral research and identified 54 theories. Below, the three most used theories in ISA research are summarized.

General Deterrence Theory. General Deterrence Theory (GDT) in relation to information security comes from the discipline of criminology, which is used as a deterrent mechanism by heightening the perceived threat of penalties or punishments for IS misuse [29]. Classic deterrence theory posits that individuals will be deterred from illicit acts with greater certainty, severity, and celerity of sanctions [37].

Theory of Planned Behavior. A literature review conducted by Sommestad et al. [38] and Lebek et al. [36] on contributing factors of security compliance and information security behavior, found the Theory of Planned Behavior (TPB) to be the most used theory by researchers. TPB is an extension of the Theory of Reasoned Action (TRA), and posits that human behavior is moved by three forms of beliefs: behavioral, normative, and control. Humans are prepared to behave a certain way if it is favorable unto them or if they perceive social pressure from important others. The necessary extension of TPB would be the perception of control over the behavior [39, 40]. In addition, if humans assess behavior as positive (attitude), or they believe that influential others would like them to perform the behavior (subjective norms) this should lead to higher intentions and they would be inclined to perform a behavior [41].

Protection Motivation Theory. Protection Motivation Theory (PMT) originated in health psychology and explains the coping procedure towards possible threats by considering various protective behaviors [36]. There are two main parts to the theory: threat appraisal and coping appraisal. Threat appraisal relates to the individual's assessment of risk for misuse of IS. Perceived vulnerability and perceived severity are the two main components of threat appraisal. The coping appraisal is the individual's ability to deal with the potential threat or risk [42].

3 Methodology

An interpretive approach was used for this study as the purpose of this research was to review and classify the literature. Interpretive research starts with the assumption that access to reality is shaped by social construction such as shared meanings, language

and consciousness [43]. The research attempted to make sense of the publications being reviewed by analyzing secondary data and identified themes and patterns from the data.

King and He [44] state that there are four main approaches to reviewing literature namely, narrative review, descriptive review, vote-counting, and meta-analysis. The purpose of a descriptive review is to explore the literature to find propositions and interpretable patterns in data. The descriptive review is positioned on the qualitative-quantitative continuum and an appropriate method for achieving the research objective. The descriptive review's main component is qualitative. However, quantitative elements are present in specific processes, e.g. statistical analysis [44].

3.1 Grounded Theory Literature-Review Method

The research strategy followed a five-stage approach, referred to as the Grounded Theory Literature-Review Method (GTLRM), developed by Wolfswinkel et al. [45]. While this is not a grounded theory study, aspects of the grounded theory method were used in the coding and classification process.

The first (Define) stage of the GTLRM consists of the inclusion and exclusion criteria, as well as the scope of the review for articles in the data set. In step one, the criteria for inclusion or exclusion of articles is defined, such as determining a time frame for the publication, as an example, the last five years. In step two appropriate research fields are stipulated, step three involves the selection of appropriate database sources, and in step four the possible search terms, methods, and criteria are identified.

The second (Search) stage consists of the search process using the criteria defined in the first stage. The search process can be long and tedious, with possible outcomes ranging from many to few. It may transpire that specific synonyms required to complete the search are missing and that the first stage needs to be revisited. New search terms may possibly be found during this process. Documentation of searches, sources used, and results is important for the transparency and replicability of the study.

In the third (Select) stage, qualifying sample articles get selected. This process involves the removal of duplicates and confirming that the selected articles meet the requirements. This can be accomplished by reviewing the title, abstract, introduction, full text and by executing a forward and backward citation for additional articles. If new articles are found the process is repeated.

The fourth (Analyze) stage is where the fundamental principles of grounded theory are implemented. The researcher starts reading articles individually and performs three steps of coding in a systematic process. The three stages of coding which is used are open, axial and selective coding. Open coding utilizes a bird's eye view of the data collected to abstract high-level classes from sets of variables or concepts. This can be in the form of a word, statement or paragraph. Next, axial coding identifies the interrelationships between categories and their subcategories. Finally, the categories identified will be integrated and refined in the selective coding process; categories and subcategories can evolve during the reading and analyses of excerpts.

Finally, the fifth (Present) stage, presents the research findings and the documented steps taken to acquire these findings. This empirical data can be exhibited using various methods such as diagrams, tables, graphical representations.

3.2 Sampling and Data collection

This study utilized theoretical sampling, which is a form of purposive sampling. Theoretical sampling pursues theoretical lines of enquiry for the identification of core themes, relationships or processes on which to focus the research. Theoretical saturation occurs when the collected and analyzed data stops producing new properties which are relevant to a category and where the relationships among classes have been verified [46].

For practical purposes the sample range was over a period of ten years, ranging from 2008 to 2018. Initially, this research study was restricted to the basket of 8 IS journal databases which are listed by the Association for Information Systems. However, due to an insufficient number of articles which were found in the journal databases, the search source criteria had to be amended. The inclusion of two specialized information security journals namely, 'Computers & Security' and 'Information & Computer Security' were added to the list of AIS basket of eight journals as this was not only an IS study but also an information security study and these journals contained relevant articles on the topic. 'Information Management & Computer Security' or 'Information & Computer Security' was selected as it is listed in the Google Scholar Top 20 publications for information security, and it was from an IS field. 'Computers & Security' is a highly ranked information security journal in Google Scholar and SCImago Journal & Country Rank.

Only peer-reviewed academic journals were considered for this research. Non-peer-reviewed articles, publications not written in English, books, working papers or conference proceedings were excluded. Articles which were not in an organizational setting (such as home users) or only marginally included ISA (such as studies focused on specific systems such as email, BYOD, or malware) were excluded. The pre-defined search terms that were used to conduct the literature search for relevant articles were: Information Security Awareness, awareness program, security education, information security cognizance, information security behavior, information security knowledge, security awareness. The search terms were split, combined and the use of Boolean operators was used under the search options of the journal databases. Table 1 lists the journal databases used, and total articles found in the initial search.

Table 1. Journal database and initial search count

Journal Database	Initial Search Count
Journal of Information Technology	341
Journal of Association for Information Systems	107
European Journal of Information Systems	684
Journal of Strategic Information Systems	70
Journal of Management Information Systems	530
Information Systems Research	799
Information Systems Journal	333
MIS Quarterly	469
Computers & Security	688
Information & Computer Security	532

A total of 4553 articles were found. Using the select stage of the GTLRM and the exclusion criteria above, the final sample was brought down to 59 articles which were used for the data analysis.

3.3 Analysis

The coding methods from stage four of the GTLRM was used to analyze the sample collected. The first step was open coding, which utilizes a bird's eye view of the data collected to abstract high-level classes from sets of variables or concepts. In the next step, axial coding was used to identify the interrelationship between categories and their subcategories. The categories identified was integrated and refined in the selective coding process [45]. NVivo 12 Pro was the Computer-Aided Qualitative Data Analysis Software (CAQDAS) used to assist with the analysis process. The collected sample was added to the NVivo project, and the data was analyzed, classified and developed into themes.

4 Classification and Descriptive Review

The classification and descriptive review consists of two sections. First, a detailed breakdown of the classification framework which was developed through the analysis process is provided. Second, a further breakdown of the articles and categories are explored in the descriptive review.

4.1 Classification

A classification framework was developed through the analysis process of open, axial and selective coding as recommended by Wolfswinkel et al. [45]. The rereading of articles ensured the effectiveness and relevancy of the framework. Themes and categories were highlighted and extracted from the articles which have also led to the formation of subthemes and subcategories.

The results of the analyses' resulted in four top-level categories and eight subcategories. The top-level categories which were developed from the full-text review of the 59 articles are 'Behavior', 'Antecedents', 'ISP' and 'Theory Development'. The 'Behavior' category focuses on the behavior of insiders within the organization, while the 'Antecedents' category looks at how individuals and organizations can increase or improve their levels of ISA. The 'ISP' category focuses on the compliance and violations of ISPs within the organization. 'Theory Development' use existing theories, extends theories or proposes new theories, frameworks or technologies to improve or understand behavior.

The subcategories were derived by assigning individual articles according to their specific research interest. Many of the themes and views expressed in the articles were similar, and it is more than likely that articles could contribute to more than one subcategory. However, by utilizing only one subcategory for each article, the classification

of the main categories and subcategories of ISA Research is simplified, structured and the relationships between the two are conceptualized.

Behavior. This category focuses on the human attributes of the individual/s towards secure information security practices within the organization. These attributes can consist of perceptions, attitudes, behavior, knowledge, work habits and values [47]. The success or failure of the organization's approach to information security ultimately lies in the way employees conduct themselves [48, 49].

Analysis. This subcategory covers articles focusing on research studies attempting to understand the behavior of individuals. The motivation behind the behavior of Individuals towards secure information security practices can vary from individual to individual, and there seems to be no one-size-fits-all approach to address the problem currently. Öİütçü et al. [50] used data collected from surveys to rate behavior on a four-scale system, which are: Risk Perception Scale (RPS), Exposure to Offence Scale (EOS), Conservative Behavior Scale (CBS) and Risky Behavior Scale (RBS). Snyman and Kruger [51] exploratory investigation found behavioral threshold analysis to be feasible for constructing ISA programs.

Culture. The articles listed in this subcategory focuses on the habitual practice of doing things by the organizations and its individuals. The way things are done around here is the common theme found in the articles about organizational culture [48, 52]. The way things are done around here to protect organizational information assets is the common theme to describe information security culture [48, 53, 54]. Da Veiga and Martins [55] state that organizations with a strong security culture have higher compliance with ISPs and regulatory requirements by employees.

Future Research Areas. This subcategory consists of two articles which discuss future directions for information security behavioral research. Crossler et al. [7] found that future research should focus on: separating insider deviant behavior from insider misbehavior; behavioral research; approaches to understand cyberattacks and to improve ISP compliance.

Antecedents. This category contains articles which focus on ways in which organizations can increase or improve their levels and the levels of their employees ISA. The effectiveness of information security requires the participation and commitment of all parties [28].

Non-technological. This subcategory has the highest article count and provides non-technological solutions to prevent Information Security threats or improve ISA. The human element within the organization is the central theme. Adequate SETA programs are the most effective non-technological solution for both staff and the organization [31, 55, 56].

Information Security Policies. Articles in this category focus on the compliance and non-compliance of ISPs and covers how ISP effectiveness can be achieved or increased. Theories used in criminology, social psychology and other related disciplines are referenced extensively for testing user ISP compliance/non-compliance [9, 34, 57, 58]. Many techniques used by security managers are listed such as SETA programs [29], guidelines and policies [9]. Other techniques such as positive reinforcement strategy (reward), negative enforcement strategy (punishment) [57] and campaigns [33] were also used.

Compliance. This subcategory examines approaches for ensuring ISP compliance. It looks at various strategies for management to consider such as stick vs carrot approach [57]. Sommestad et al. [38] conducted a review of 29 quantitative studies dealing with individual ISP compliance/non-compliance and found that factors such as self-efficacy, subjective norms, response cost, perceived severity and certainty of sanctions can be used to identify compliant behavior. Perceived severity of security breaches, perceived probability [30] and habits are also antecedents of ISP compliance [58].

Violation. This subcategory contains articles discussing the non-compliance of ISPs by staff. Like the compliance subcategory above, researchers try to understand the rationale behind information security policy violations. Findings reveal that employees are not the same and that individuals have different reactions to information security interventions [34].

Theory Development. This category consists of articles which use existing, extends, or proposes new theories, frameworks or technologies to improve our understand employee behavior.

Application of Existing Theory. The articles listed in this in this subcategory use existing theories or technologies to understand, explain or deter behavioral traits. Thomson and van Niekerk [59] use goal-setting theory from social sciences to encourage employees to contribute to good information security practices.

Advancement in Research. This subcategory contains the second largest article count dealing with new or extended theories, frameworks or technologies. Johnston et al. [33] created an Enhanced Fear Appeal Rhetorical Framework as they felt that the current fear appeal rhetorical framework was inadequate. Liang and Xue [49] developed the Technology Threat Avoidance Theory (TTAT) to understand users' IT threat avoidance behavior using elements from cybernetic theory and coping theory.

4.2 Descriptive Review

The map in Fig. 1 displays the article count by the first author's country. The USA had the highest article count with 20 articles (34 percent). South Africa had nine articles (15 percent). Norway and Finland had four articles (7 percent) while Greece, Australia,

England and Sweden had three articles (5 percent). Canada and Germany had two articles (3 percent) with Malaysia. Austria, Qatar, Ireland, Turkey and China only having one article (2 percent).

Fig. 1. Distribution of articles by the first author's country

Distribution of Articles by Year. Fig. 2 displays the distribution of articles published from the year 2008 to 2018. From 2011 to 2013 there was a decline in the number of articles published. From 2014 to 2018 the number of published articles increased with the highest published article count being for the year 2017, which had 12 articles. The sudden increase in published articles for 2017 could possibly be related to stricter privacy/regulatory laws such as the General Data Protection Regulation (GDPR) which was adopted in April 2016. Due to data collection occurring in the second quarter of 2018, only five articles were recorded for the year. Therefore, this is not a complete list of articles for the year 2018.

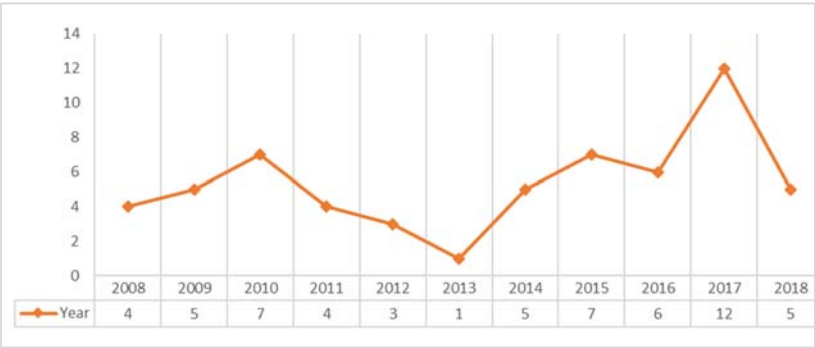

Fig. 2. Distribution of articles per year

Distribution of Articles by Category. 'Theory Development' is the most published research category with 18 articles (30 percent). The remainder of the categories, namely, 'Behavior' and 'Antecedents' have 14 articles (24 percent) while, the 'ISP' category has the lowest article count with 13 articles (22 percent). In Fig. 3 the articles distributed by category per year are displayed.

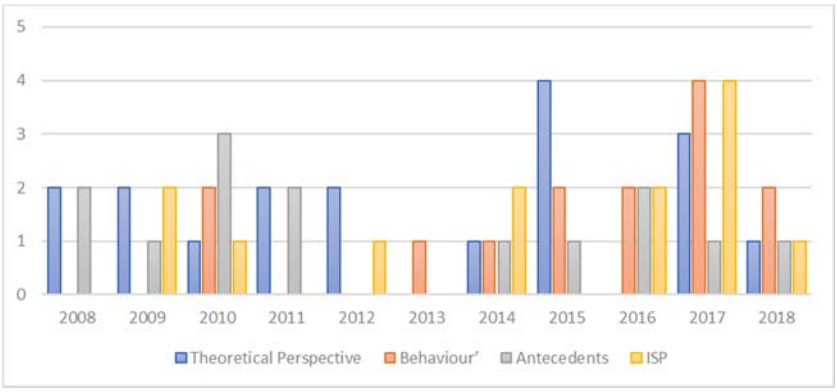

Fig. 3. Distribution of articles by category per year

The category 'Antecedent' research articles appear throughout the review period, except for 2012 and 2013 which had no articles. The 'Theory Development' category was prevalent throughout the review period except for 2012, 2013 and 2016 where no articles were recorded. From the year 2013 to 2018, the research articles for the 'Behavior' category appeared each year, and before this, except for two articles in the year 2010, no other articles were listed. The years' 2010, 2014, 2017 and 2018 features all the main categories appearing together with 'Antecedents' being the dominant category for the year 2010, 'ISP' for 2014, 'Behavior' and 'ISP' for 2017 and 'Behavior' the dominant category for 2018.

Distribution of Articles by Applied Research Methodologies. The chart in Fig. 4 displays the research methodologies used throughout the publications. Four different research methodologies were identified, namely, literature review, empirical research, proposed model/method and action research. 'Empirical Research' clearly stands out as the dominant applied research methodology with 42 articles (71 percent) of which 30 articles (72 percent) were 'Quantitative', nine articles (21 percent) were 'Qualitative', and three articles (7 percent) used a 'Mixed Methods' approach. This was followed by 'Literature Review' eight articles (13 percent) and 'Proposed Model/Method' eight articles (14 percent). 'Action Research' was only used in one article.

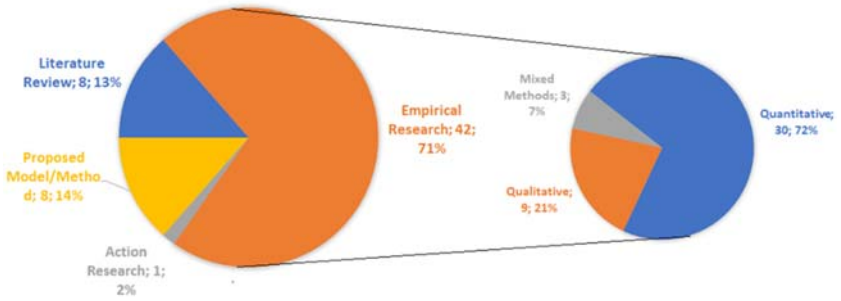

Fig. 4. Applied research methodologies

Theories used in articles. Twenty-six different theories were used in the research articles. Some theories were combined to form a new one, while other theories were extended. The most commonly used theories in the reviewed articles were: General Deterrence Theory in eight articles (14 percent); Theory of Reasoned Action or Theory Planned Behavior in seven articles (12 percent); and Protection Motivation Theory in six articles (10 percent). Other theories, appearing once each, were: Actor-Network Theory; Theory of Cognitive Moral Development; Theory of Contextualism; Control Balance Theory; Elaboration Likelihood Model; Fairness Theory; Health Belief Model; Information Foraging Theory; Theory of Interpersonal Behavior; Theory of Motivational Types of Values; Neutralization Theory; Organizational Justice Theory; Rational Choice Theory; Reactance Theory; Regret Theory; Self-Determination Theory; Theory of Self-Regulation; Social Bond Theory; Structuration Theory; Technology Threat Avoidance Theory; Unified Model of Information Security Policy Compliance; Universal Constructive Instructional Theory; and Value-Based Compliance Theory.

5 Discussion

Although 26 theories were identified during the data analysis most of these theories were only used once except for GDT, TRA/TPB and PMT which were the dominant three applied theories. GDT is the most applied theory in the articles for this research study as with the case of D'Arcy and Herath [37] who found GDT to be the most widely applied theory in IS security research. While GDT, TRA/TPB and PMT provides essential insights for behavioral IS security studies, some researchers have doubts regarding their effectiveness. D'Arcy and Herath [37] argue that deterrence theory in the context of IS security provides inconsistent and sometimes contradictory findings while, Johnston et al. [33] found the conventional PMT to be inadequate due to its focus being on individual's things (e.g. data) instead of physical self, as is the case in the healthcare context. Bulgurcu et al. [9] note that a problem with TPB is that nearly an infinite number of variables can affect the performance or non-performance of any behavior. This would explain why 'Theory Development' is the number one category in this research study as researchers are still using theories from other fields to try and understand this phenomenon.

Behavioral research studies seem to be on the rise over the last few years. Behavioral research has mainly used self-reporting measures to understand the factors leading to ISA [22]. These factors such as individuals' attitudes, satisfaction, motivations or intentions are only verifiable through self-reporting [36] which makes it unsurprising that most empirical studies in the reviewed publications used quantitative methods. Johnston et al. [33] and Menard et al. [60] state that the use of intentions rather than actual behavior is the biggest challenge for behavioral information security research. Crossler et al. [7] emphasize that this is a challenge that researchers need to overcome as it is a limitation to theory development or theory validation.

This research study looked at antecedents from an organizational perspective to include everything operating within the organization setting such as technology, staff and managers. At the organizational level, management's understanding and identification of the factors influencing ISA is required for effective ISA training and ISA programs. Management ISA support and commitment to information security are positive attributes to increased staff ISA. The most crucial non-technological security management practices, protecting the organization and increasing staff ISA, are the provisioning of ISPs and SETA programs. At the individual level, higher education or security training, prior negative experiences with information security or previously reprimanded for security violations have found to increase individual's ISA.

6 Conclusion

This research presented a review of organizational ISA research. A total of 59 articles which met the search criteria were used for the data analysis, which resulted in four high-level categories and eight subcategories. The review revealed that ISA research is evolving with theory development having the highest research focus. The top three theories used for ISA research are GDT, TPB, and PMT. Various approaches are used to ensure ISP compliance ranging from sanctions to campaigns, of which SETA programs are the most common.

Like most academic studies, this descriptive review and classification has limitations. First, only articles that were published in English were considered for this review. Furthermore, this study used a predefined list of search terms which was not refined as new search terms arose during the search or analysis process. Second, non-peer-reviewed journals and other potential sources of information such as whitepapers, conference proceedings and books were excluded. These limitations may put this study at a disadvantage of presenting a complete picture of the ISA research landscape. Future studies could include all relevant IS journal databases, specialized information security journals, and other relevant potential sources of ISA research such as books, whitepapers or conference proceedings. Also, search terms should be refined as new terms arise and the use of backward and forward citations should also be considered to increase the sample size.

Acknowledgements. This work is based on the research supported wholly / in part by the National Research Foundation of South Africa (Grant Numbers 114838).

References

1. Grant, K., Edgar, D., Sukumar, A., & Meyer, M. (2014). Risky business: Perceptions of e-business risk by UK small and medium sized enterprises (SMEs). International Journal of Information Management, 34(2), 99–122. https://doi.org/10.1016/j.ijinfomgt.2013.11.001
2. Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. Computers in Human Behavior, 38, 304–312. https://doi.org/10.1016/j.chb.2014.05.046
3. Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. Computers and Security, 66, 40–51. https://doi.org/10.1016/j.cose.2017.01.004
4. Metalidou, E., Marinagi, C., Trivellas, P., Eberhagen, N., Giannakopoulos, G., & Skourlas, C. (2014). Human factor and information security in higher education. Journal of Systems and Information Technology, 16(3), 210–221. https://doi.org/10.1108/JSIT-01-2014-0007
5. Kruger, H. A., Drevin, L., & Steyn, T. (2010). A vocabulary test to assess information security awareness. Information Management & Computer Security, 18(5), 316–327. https://doi.org/10.1108/09685221011095236
6. Bauer, S., & Bernroider, E. W. N. (2017). From Information Security Awareness to Reasoned Compliant Action. ACM SIGMIS Database: The DATABASE for Advances in Information Systems, 48(3), 44–68. https://doi.org/10.1145/3130515.3130519
7. Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. Computers and Security, 32, 90–101. https://doi.org/10.1016/j.cose.2012.09.010
8. Bauer, S., Bernroider, E. W. N., & Chudzikowski, K. (2017). Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks. Computers and Security, 68, 145–159. https://doi.org/10.1016/j.cose.2017.04.009
9. Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-based Beliefs and Information Security Awareness. MIS Q., 34(3), 523–548.
10. Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. Information Management & Computer Security, 8(1), 31–41. https://doi.org/10.1108/09685220010371394
11. Bitton, R., Finkelshtein, A., Sidi, L., Puzis, R., Rokach, L., & Shabtai, A. (2018). Taxonomy of mobile users' security awareness. Computers and Security, 73, 266–293. https://doi.org/10.1016/j.cose.2017.10.015
12. Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). Computers and Security, 42, 165–176. https://doi.org/10.1016/j.cose.2013.12.003
13. Okoli, C., & Schabram, K. (2010). A Guide to Conducting a Systematic Literature Review of Information Systems Research. Working Papers on Information Systems, 10(26), 1–51. https://doi.org/10.2139/ssrn.1954824
14. Prasetio, A., Sari, P. K., & Ramadhani, D. P. (2016). Electronic Word-of-Mouth (EWOM) Adoption Model for Information Security Awareness: A Case Study in University Students, (2015), 154–159.
15. Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. Computers and Security, 25(4), 289–296. https://doi.org/10.1016/j.cose.2006.02.008

16. Haeussinger, F., & Kranz, J. (2013). Understanding the Antecedents of Information Security Awareness - An Empirical Study. Proceedings of the Nineteenth Americas Conference on Information Systems, (section 6), 1–9.
17. Tsohou, A., Kokolakis, S., Karyda, M., & Kiountouzis, E. (2008). Investigating information security awareness: Research and practice gaps. Information Security Journal, 17(5–6), 207–227. https://doi.org/10.1080/19393550802492487
18. Straub, D. W., & Welke, R. J. (1998). Coping with Systems Risk: Security Planning Models for Management Decision Making. MIS Quarterly, 22(4), 441–469. https://doi.org/10.2307/249551
19. Rhee, H., Ryu, Y., & Kim, C.-T. (2005). I Am Fine but You Are Not: Optimistic Bias and Illusion of Control on Information Security. ICIS, (April), 381–394.
20. Tsohou, A., Karyda, M., Kokolakis, S., & Kiountouzis, E. (2013). Managing the introduction of information security awareness programmes in organisations. European Journal of Information Systems, 24, 38–58.
21. Jaeger, L. (2018). Information Security Awareness: Literature Review and Integrative Framework. 51st Hawaii International Conference on System Sciences., 9(3), 4703–4712.
22. Anderson, B. B., Kirwan, C. B., & Eargle, D. (2014). Using Measures of Risk Perception to Predict Information Security Behavior: Insights from Using Measures of Risk Perception to Predict Information Security Behavior: Insights from Electroencephalography (EEG). J Assoc Inf Syst, 15(April 2013), 679–722.
23. Scholl, M. C., Wildau, T., Fuhrmann, F., & Scholl, L. R. (2018). Scientific Knowledge of the Human Side of Information Security as a Basis for Sustainable Trainings in Organizational Practices. Hawaii International Conference on System Sciences, 9, 10.
24. Tsohou, A., Karyda, M., Kokolakis, S., & Kiountouzis, E. (2012). Analyzing trajectories of information security awareness. Information Technology & People, 25(3), 327–352. https://doi.org/10.1108/09593841211254358
25. Khan, B., Alghathbar, K., Nabi, S., & Khan, K. (2011). Effectiveness of information security awareness methods based on psychological theories. African Journal of Business Management, 5.
26. Puhakainen, P., & Siponen, M. (2010). Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study. MIS Quarterly (Vol. 34). https://doi.org/10.2307/25750704
27. Posey, C., Roberts, T. L., & Lowry, P. B. (2015). The impact of organizational commitment on insiders motivation to protect organizational information assets. Journal of Management Information Systems, 32(4), 179–214. https://doi.org/10.1080/07421222.2015.1138374
28. Merete Hagen, J., Albrechtsen, E., & Hovden, J. (2008). Implementation and effectiveness of organizational information security measures. Information Management and Computer Security, 16(4), 377–397. https://doi.org/10.1108/09685220810908796
29. D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. Information Systems Research, 20(1), 79–98. https://doi.org/10.1287/isre.1070.0160
30. Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. European Journal of Information Systems, 18(2), 106–125. https://doi.org/10.1057/ejis.2009.6
31. Chen, C. C., Medlin, B. D., & Shaw, R. S. (2008). A cross-cultural investigation of situational information security awareness programs. Information Management and Computer Security, 16(4), 360–376. https://doi.org/10.1108/09685220810908787

32. Karjalainen, M., & Siponen, M. (2011). Toward a New Meta-Theory for Designing Information Systems (IS) Security Training Approaches. Journal of the Association of Information Systems, 12(8), 518–555.
33. Johnston, A. C., Warkentin, M., & Siponen, M. (2015). An Enhanced Fear Appeal Rhetorical Framework: Leveraging Threats to the Human Asset Through Sanctioning Rhetoric. MIS Quarterly, 39(1), 113–134. https://doi.org/10.25300/MISQ/2015/39.1.06
34. Johnston, A. C., Warkentin, M., McBride, M., & Carter, L. (2016). Dispositional and situational factors: Influences on information security policy violations. European Journal of Information Systems, 25(3), 231–251. https://doi.org/10.1057/ejis.2015.15
35. Lebek, B., Uffen, J., Breitner, M. H., Neumann, M., & Hohler, B. (2013). Employees' information security awareness and behavior: A literature review. Proceedings of the Annual Hawaii International Conference on System Sciences, 2978–2987. https://doi.org/10.1109/HICSS.2013.192
36. Lebek, B., Uffen, J., Neumann, M., Hohler, B., & Breitner, M. (2014). Information security awareness and behavior: a theory-based literature review. Management Research Review, 37(12), 1049–1092. https://doi.org/10.1108/MRR-04-2013-0085
37. D'Arcy, J., & Herath, T. (2011). A review and analysis of deterrence theory in the IS security literature: Making sense of the disparate findings. European Journal of Information Systems, 20(6), 643–658. https://doi.org/10.1057/ejis.2011.23
38. Sommestad, T., Hallberg, J., Lundholm, K., & Bengtsson, J. (2014). Variables influencing information security policy compliance: A systematic review of quantitative studies. Information Management and Computer Security, 22(1), 42–75. https://doi.org/10.1108/IMCS-08-2012-0045
39. Dang-Pham, D., Pittayachawan, S., & Bruno, V. (2017). Why employees share information security advice? Exploring the contributing factors and structural patterns of security advice sharing in the workplace. Computers in Human Behavior, 67, 196–206. https://doi.org/10.1016/j.chb.2016.10.025
40. Sparks, P., Ajzen, I., & Hall-box, T. (2002). Perceived Behavioral Control, Self-Efficacy, Locus of Control, and the Theory of Planned Behavior, 665–683.
41. Safa, N., & von Solms, R. (2016). An information security knowledge sharing model in organizations. Computers in Human Behavior, 57, 442–451. https://doi.org/10.1016/j.chb.2015.12.037
42. Safa, N., Sookhak, M., von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. Computers and Security, 53, 65–78. https://doi.org/10.1016/j.cose.2015.05.012
43. Myers, M.D.: Qualitative Research in Business and Management. SAGE Publications Ltd, London (2013).
44. King, W. R., & He, J. (2005). Understanding the Role and Methods of Meta- Analysis in IS Research. Communications of the Association of Information Systems, 16(October), 654.
45. Wolfswinkel, J. F., Furtmueller, E., & Wilderom, C. P. M. (2011). Using grounded theory as a method for rigorously reviewing literature. European Journal of Information Systems, 22(1), 45–55. https://doi.org/10.1057/ejis.2011.51
46. Saunders, M. N. K., Lewis, P., & Thornhill, A. (2015). Research Methods for Business Students. Pearson Education Limited.
47. Tsohou, A., Karyda, M., & Kokolakis, S. (2015). Analyzing the role of cognitive and cultural biases in the internalization of information security policies: Recommendations for information security awareness programs. Computers and Security, 52, 128–141. https://doi.org/10.1016/j.cose.2015.04.006

48. Da Veiga, A., & Eloff, J. H. P. (2010). A framework and assessment instrument for information security culture. Computers and Security, 29(2), 196–207. https://doi.org/10.1016/j.cose.2009.09.002
49. Liang, H., & Xue, Y. (2009). Avoidance of Information Technology Threats: A Theoretical Perspective. MIS Quarterly, 33(1), 71–90. https://doi.org/10.2307/20650279
50. Öİütçü, G., Testik, Ö. M., & Chouseinoglou, O. (2016). Analysis of personal information security behavior and awareness. Computers and Security, 56, 83–93. https://doi.org/10.1016/j.cose.2015.10.002
51. Snyman, D., & Kruger, H. A. (2017). The application of behavioural thresholds to analyse collective behaviour in information security. Information and Computer Security, 25(2), 152–164. https://doi.org/10.1108/ICS-03-2017-0015
52. Connolly, L., Lang, M., Gathegi, J., & Tygar, D. J. (2017). Organisational culture, procedural countermeasures, and employee security behaviour: A qualitative study. Information and Computer Security, 25(2), 118–136. https://doi.org/10.1108/ICS-03-2017-0013
53. D'Arcy, J., & Greene, G. (2014). Security culture and the employment relationship as drivers of employees' security compliance. Information Management and Computer Security, 22(5), 474–489. https://doi.org/10.1108/IMCS-08-2013-0057
54. Da Veiga, A., & Martins, N. (2017). Defining and identifying dominant information security cultures and subcultures. Computers and Security, 70, 72–94. https://doi.org/10.1016/j.cose.2017.05.002
55. Da Veiga, A., & Martins, N. (2015). Improving the information security culture through monitoring and implementation actions illustrated through a case study. Computers and Security, 49, 162–176. https://doi.org/10.1016/j.cose.2014.12.006
56. Merete Hagen, J., & Albrechtsen, E. (2009). Effects on employees' information security abilities by e-learning. Information Management and Computer Security, 17(5), 388–407. https://doi.org/10.1108/09685220911006687
57. Chen, C. C., Ramamurthy, K., & Wen, K.-W. (2012). Organizations' Information Security Policy Compliance: Stick or Carrot Approach? Journal of Management Information Systems, 29(3), 157–188. https://doi.org/10.2753/MIS0742-1222290305
58. Tsohou, A., Karyda, M., Kokolakis, S., & Kiountouzis, E. (2015). Managing the introduction of information security awareness programmes in organisations. European Journal of Information Systems, 24(1), 38–58. https://doi.org/10.1057/ejis.2013.27
59. Thomson, K., & van Niekerk, J. (2012). Combating information security apathy by encouraging prosocial organisational behaviour. Information Management and Computer Security, 20(1), 39–46. https://doi.org/10.1108/09685221211219191
60. Menard, P., Bott, G. J., & Crossler, R. E. (2017). User Motivations in Protecting Information Security: Protection Motivation Theory Versus Self-Determination Theory. Journal of Management Information Systems, 34(4), 1203–1230. https://doi.org/10.1080/07421222.2017.1394083