Available online at www.sciencedirect.com

ScienceDirect

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

Computers & Security

Enhancing employees information security awareness in private and public organisations: A systematic literature review

Khando Khando[a], Shang Gao[a,*], Sirajul M. Islam[a], Ali Salman[a]

[a] Department of Informatics, Örebro University, Örebro, Sweden

ARTICLE INFO

Article history:
Received 15 September 2020
Revised 24 March 2021
Accepted 25 March 2021
Available online 16 April 2021

Keywords:
Information security awareness
Literature review
Private organisations
Public organisations
Information Security Management
Awareness methods
Awareness factors

ABSTRACT

Preserving the confidentiality, integrity and availability (CIA) of an organisation's sensitive information systems assets against attacks and threats is a challenge in this digital age. Organisations worldwide make huge investments in information security technological countermeasures. Nonetheless, organisations in many cases fail to protect their information assets as they rely mainly on technical solutions which are not contextually compatible and sufficient. As a matter of fact, a significant number of organisational information security incidents are due to the exploitation of human elements that directly and/or indirectly cause the majority of security incidents. Therefore, employees' information security awareness (ISA) becomes one of the critical aspects of protection against undesirable information security behaviours. However, to date, there is limited synthesised knowledge about methods for enhancing ISA and integrated insights on factors affecting employees' ISA levels. This study, therefore, provides a systematic review of the literature on ISA and puts forward a state-of-the-art collection of ISA methods and factors for enhancing employees' ISA within both private and public sector organisations. The results indicate that various methods and factors are used to enhance employees' ISA in organisations. Theoretical models and gamification are the methods widely used in both private and public organisations, whereas the constructivist approach and violation detections are some of the methods used only in private organisations. Furthermore, this study offers some insights into the latest trends in ISA content development methods and factors, and fosters good ISA practice by disseminating information and knowledge amongst Information Security professionals to help them build an overarching ISA development programme in their organisations.

1. Introduction

In today's digital world, securing information systems assets has become a top priority for organisations in order to protect them from malicious attacks. Both the cybercriminals and data breaches have increased dramatically in recent years. According to the Cybersecurity Business Report, cyber-crime is expected to cost "more than $6 trillion by 2021, up from $3 trillion in 2015" (Morgan, 2016). Therefore, organisations continuously struggle to maintain the security of their information

* Corresponding author.
E-mail addresses: kkhandu@gmail.com (K. Khando), shang.gao@oru.se (S. Gao), Sirajul.Islam@oru.se (S.M. Islam), ali@digilano.se (A. Salman).

https://doi.org/10.1016/j.cose.2021.102267

assets which in turn force them to make huge investments into technological countermeasures (Spears and Barki, 2010). However, merely focusing on the technical aspects of information security is not enough as information security is a multidisciplinary in nature and the human aspect plays a major part in it. A significant number of organisational information security incidents are due to exploitation of human elements (e.g., (Stahl, Doherty, & Shaw, 2012)). In other words, human errors are the direct and/or indirect cause of the majority of security incidents including both intentional and unintentional misbehaviours (Siponen and Vance, 2010). ENISA (2019) indicated that about 77% of the companies' data breaches are due to exploitation of human weaknesses. It was also found previously that over half of all information security breaches involved employees' poor information security compliances (Humaidi and Balakrishnan, 2015; Waly et al., 2012).

In view of this context, employees' Information Security Awareness (ISA) exerts a significant impact on information security behaviours and employees' security policy compliance (Bulgurcu et al., 2010; DeGroot et al., 2012). Previous studies have argued that a lack of employees' ISA through Information Security Policies (ISP) and procedures was the major cause of mishandling of sensitive information (e.g., (Siponen, 2000 & Abraham, 2011)). Further, ISA has become a top priority both in research and practice (Haeussinger and Kranz, 2017) mainly because humans are found to be one of the weakest links in attempts to secure systems and networks (Imgraben et al., 2014; Spears and Barki, 2010). It has been reported that 88% of UK data breaches were caused by human errors, not by cyber-attacks (Ingham, 2018). According to Ingham (2018), the most common error was sending sensitive data to the wrong recipient which mostly happened through email or via post or fax and other issues included the loss or theft of paperwork, forgetting to redact data or storing data in an insecure location, such as a public cloud server. According to Ernst and Young's 2018-2019 Global Information Security Survey, 34% of organisations find unaware employees to be the biggest vulnerability. These vulnerabilities can be the cause of huge financial losses and reputational damages to the businesses, more so with the advent of stringent data protection laws such as the EU's General Data Protection Regulation (GDPR). This is also one of the main reasons why the latest Cyber Security Breaches Survey 2019 shows that cybersecurity is a high priority for the senior management of organisations (Vaidya, 2019).

Despite due importance being given to employees' ISA by research and practice, most employees lack awareness of information security threats and issues (Lim et al., 2010). For example, "about 90% of the cybersecurity professionals reported that the company they work for felt vulnerable to insider threats" (ENISA, 2019). Jaeger (2018) indicated that "research on information security awareness is still an evolving field with many uncharted areas to be explored". Additionally, there was a lack of an overarching picture of the concept of ISA and its relationship with other constructs, despite numerous studies on ISA (Jaeger, 2018). This is supported by other literature stating that ISA campaigns and training are failing to change employees' behaviour for various reasons (Abawajy, 2014; Annetta, 2010; Cone et al., 2007).

It is further discovered that organisations are failing with their ISA campaigns as they do not reflect adequately on the factors affecting the employees' ISA levels while developing the content for the ISA campaigns (Bada et al., 2019). Most importantly it was found that there was a lack of methods to create "engaging and appropriate materials" for enhancing ISA, and on top of that, several behavioural factors were not considered in developing ISA campaigns or programmes in the past to improve ISA levels (Bada et al., 2019).

This study, therefore, seeks to understand the organisational context in terms of using ISA methods and factors that influence employees' ISA. Hence, the study aims to provide a comparative analysis of various methods and factors between private and public sector organisations through a systematic literature review. During the last few years, there is a significant body of research focusing on methods and factors for enhancing employees' ISA in private and public organisations. However, there is a lack of systematic work that summarises and conceptualises the existing findings on the methods and factors. Thus, this study addresses the following research question: *What are the methods and factors used in IS literature to enhance employees' ISA in organisations within both the private and public sector?*

A systematic analysis of the widely dispersed knowledge on ISA methods and factors would be useful for the information security practitioners such as Information Security Officers and Information Security Managers alike as it would be of help for them to know about the overall picture of the concept of the existing ISA methods and factors. This, in turn, will help them to build effective ISA programmes and ultimately achieve employees' information security compliant behaviours amongst employees. The findings are also intended to serve as a benchmark for further research in the field.

The rest of the paper is structured as follows: Section 2 defines the major concepts used in the context of this study and draws on the related works within the scope of this study. Section 3 describes the underlying research methodology. The literature search process, as well as the literature analysis process, is demonstrated in detail in the methodology section. The findings from the literature review are presented in Section 4. The findings are compared and discussed in Section 5. Section 6 discusses the limitations of the study. Finally, in Section 7, we conclude this study and point out some future research directions .

2. Research background

2.1. *The scope of ISA*

Information security management system includes ISA processes and activities International Organization for Standardization (ISO 2013). The role of ISA is to ensure that all employees within an organisation are aware of the policies, rules and regulations regarding securing the information (Khan et al., 2011). It also involves a state of consciousness and knowledge about security issues and can be a strong predictor of security compliant behaviour (Haeussinger and Kranz, 2017; Bulgurcu et al., 2010). Employees must have the ability to make decisive information security decisions when the need arises. ISA has become an essential part of information security in mitigating the security risks and beyond this, it makes employees understand the organisational and personal consequences of mishandling sensitive information (PCI Security Standards Council, 2014). We adapted the ISA definition offered by Tsohou et al., p.1) which defines ISA as “a process that aims at changing individuals’ perceptions, values, attitudes, behaviour, norms, work habits, and organizational culture and structures with regard to secure information practices” (p.1). This is in-line with definitions of ISA (e.g., ENISA (2010); Maeyer (2007)) that refers to an organised and ongoing effort to guide the behaviour and culture of an organisation with regard to information security issues. This definition covers procedural aspects and suits our review since we consider ISA from the perspective of awareness-raising. Therefore, physical security (Alshboul, 2010) and intensive technical focused security such as IT security issues were not covered. The review is within the scope of methods used in raising ISA and factors affecting it with the aim to provide up-to-date trends in ISA content development.

Out of the three key aspects of information security – technical, formal and social, our focus is more on the social aspect which essentially deals with culture, values and the belief system of the individual concerned (Dhillon, 2001). According to Dhillon (2001), mere technical or formal control measures are inadequate to prevent computer security breaches. Thus, earlier definitions in the area of insecure behaviours are covered inclusively in our paper, such as Parker’s (1976) definition of the term computer abuse which states “Computer abuse is defined as any intentional act in which one or more victims suffered or could have suffered a loss, and one or more perpetrators made or could have made a gain” and as well as a later definition introduced by Straub (1990) which refers to “an unauthorized and deliberate misuse of assets of the local organisational institution system by individuals, including violations against: hardware, programs, data and computer service”.

2.2. Methods for enhancing ISA

Methods in the context of this research mean the techniques or ‘means and ways’ to create or develop ‘engaging and appropriate materials’ to enhance employees’ ISA level. The various methods used in the existing literature which were empirically investigated and found to be effective in achieving subsequent positive belief, attitude and behavioural changes (e.g. Valentine, 2006; Shaw et al., 2009) were extracted through the systematic literature review (SLR) process and reported in the results section.

Well-developed ISA content is an essential element to enhance employees’ ISA. There are various methods and factors for ISA content development. Having a good understanding of these methods and factors would contribute to the enhancement of employees’ ISA. For example, Amankwa et al. (2015) found that prevalent methods were used in developing ISA content for enhancing employees’ information security education and awareness. Methods provide step-by-step problem-solving opportunities which are critical in developing ISA content. Similarly, Haeussinger and Kranz (2017) emphasized the importance of identifying and understanding the useful factors to improve the effectiveness of ISA content development methods, in increasing employees’ ISA.

2.3. Factors for enhancing ISA

Whereas factors, on the other hand, are the several behavioural aspects to be considered in developing content for the ISA campaigns or programs (Bada et al., 2019). These considerations should be incorporated as ‘part of’ the methods mentioned above to influence the methods used for enhancing employees’ the ISA levels of employees (Bada et al., 2019; Siponen, 2001).

The methods and factors are closely associated and considered as the building blocks of ISA content development - both must be included in the ISA content development approaches to enhance employees’ ISA levels as factors influencing employees’ ISA should be identified and understood for an ISA content to be developed.

2.4. ISA in the private and public sectors

ISA within the private and public sectors are segregated. This is mainly because these two sectors have a distinct feature in terms of functions and motives. Unlike in public, the private sector is guided by the motive of profit maximisation, so, not all but a remarkable number of private sector organisations are run with the intention of making a profit . In addition, Solic et al. (2015) found that employees within the private sector tended to have higher risky information system behaviour and lower ISA than their colleagues in the public sector. This is mainly because private sector enterprises today are highly dependant on IS to carry out their missions and business functions; thus, the systems must be appropriately protected to achieve IS dependability (Abrams and Weiss, 2008). Moreover, (Gundu and Flowerday, 2013) found that a significant number of companies were more concerned with vulnerabilities from external threats. The commercial organisations around the globe deploy security measures and policies that specify the ‘correct’ behaviour of employees (Bada et al., 2019). Therefore, management of information security within private organizations requires effective actions in order to have positive organisational impacts (Tsohou et al., 2012), which calls for an ISA process that seeks to cultivate positive security behaviours. On the other hand, a significant number of public organizations around the world rely on digitally-enabled government services. The use of technology to provide online services to the stakeholders increases the risks for data breaches and cybercrimes (Tassabehji et al., 2007). Hence, ISA is essential to ensure the CIA of the critical information in the e-government systems.

2.5. Related work

In order to achieve the best possible understanding of ISA content development methods and factors in the current research and to find out the possible gaps in the existing literature, the relevant or related literature review studies were analysed. ISA is relatively new in the field of research and there are only a few systematic literature reviews as is evident from our investigation for the period 2009 to March 2020 (Table 1). To this end,

Table 1 – Our review vs earlier literature reviews (2009- March 2020).

Reviews	No. of papers	Focus of the study
Our review (2020)	64	Focus on providing a systematic summary of the widely dispersed ISA content development methods and factors for enhancing employees' ISA level
Haeussinger and Kranz (2017)	44	On factors affecting ISA in the context of institutional, individual, and socio-environmental- reviewed ISA antecedents
Lindberg (2016)	32	Using gamification as ISA methods and compared their results to study the relation between game elements, user and riskful behaviour to motivate users to change to a more secure behaviour
Lebek et al. (2013)	113	Use of behavioural theories as ISA method to change employees' information security behaviours
Amankwa et al. (2015)	15	Use of models for enhancing ISA and categorized the models into three stakeholder domains: End-User, Institutions and Industry domains and conducted a comparative analysis of models identified in these three domains
Bawazir et al. (2016)	17	Use of Persuasive Technology as methods for enhancing employees' ISA
Jaeger (2018)	40	Investigated the factors affecting ISA at different levels - individual, organisational, socio-environmental and technological level

Haeussinger and Kranz (2017) did an extensive systematic literature review on the antecedents of ISA, analysing 44 publications to discern various institutional, individual, and socio-environmental ISA antecedents. But they did not focus solely on putting forward a state-of-the-art collection of ISA content development methods and factors impacting ISA from an organisational perspective.

Amankwa et al. (2014) conducted a conceptual analysis of Information Security Education, Information Security Training and Information Security Awareness definitions to ascertain if any differences existed between them. Their study helped institutions to determine when they needed training or education for their employees and when to introduce security awareness programmes. They proposed a working definition based on the conceptual analysis of the existing literature, which can be used as a reference point for further research in the field. On the other hand, Lindberg (2016) analysed literature studies conducted with gamified systems and compared their results to study the relationship between game elements, users and riskful behaviour to motivate users to change to a more secure behaviour. However, he didn't draw a conclusion from the literature analysis as to which game elements had a positive or negative effect on the users, citing that there were not enough gamified systems within a security context.

Lebek et al. (2013) conducted a literature review on employees' ISA and behaviours and found that there an agreement in the literature that employees are the one of the weakest links in IS security. They presented a theory-based literature review of 113 publications related to the existing methods used within employees' ISA and behaviour, focusing mainly on the behavioural theories and covering 54 different theories. Nonetheless, their study is exclusively on reviewing the use of behavioural theories to change employees' information security behaviours, which is only one of the methods used to enhance employees' ISA and they did not cover all the publications related to ISA methods and factors. Moreover, the theories studied in the review were not contextualised from a private or public organisational perspective. In a similar way, Amankwa et al. (2015) reviewed the literature to study the use of models as methods to enhance information security education and awareness. They categorised models for enhancing ISA based on their three stakeholder domains: End-User, Institutions and Industry domains and conducted a comparative analysis of models identified in these three domains. They were able to describe a gap identified in the existing ISA models and presented the relevant characteristics for developing ISA models to bridge the gap in the institutional domain, however, they did not explore the other ISA methods apart from the models used as one of the ISA content development methods.

Bawazir et al. (2016) reviewed the literature focusing on a perspective on how to create awareness amongst users for good information security practices by applying Persuasive Technology techniques and methods. They found that there is a tremendous potential for Persuasive Technology to be applied to persuade users to change their behaviour and perception toward Information Security practices. However, their study was limited to testing very few security measures and they felt there was a need to include other security topics in future research. Moreover, it was reported that their field of research does not have any clear model or framework that helps designers to create more efficient systems. Similarly, Scholl (2019) reviewed the scientific literature of leading academic journals in the area of IS to study increasing Information Security Awareness in the Field of Urban and Regional Planning through serious games. He presented Serious Games as a way to achieve a deeper understanding of how to promote sustainable ISA using creative methods. Furthermore, ideas about how to apply the Fun Theory and its practice to integrate awareness into modern urban and regional planning was also discussed, however, his work was also not comprehensive as it is concentrated solely on the use of serious games which is merely one of the methods employed in the process of ISA programme development. A literature review by Jaeger (2018) provided valuable insights into the concept of awareness with Information System research and identified several research gaps. He discovered that ISA research is an evolving domain with many uncharted areas which need to be explored further. However, his study concentrated only on employees' cognitive states of mind related to security and his review investigated the factors affecting ISA at different levels – the individual, organisational, socio-environmental and technological levels.

In contrast, this paper provides a systematic review of all the widely dispersed knowledge on ISA methods and factors. It puts forward a state-of-the-art review of various methods for enhancing ISA and in a similar way; identifies the factors affecting the ISA content development within both private and public sector organisations. A clear and concise comparative analysis of various themes in terms of methods and factors in the context of private and public sector organisations will be demonstrated through the SLR process which serves as a benchmark for the IS practitioners and academicians while developing ISA strategies and recommending further research in the domain respectively. Thus, this paper puts forward a state-of-the-art overview of various methods for enhancing ISA and in a similar way, and identifies the factors affecting the ISA content development in the organisational context, both within the private and public sector.

3. Methodology

This study is based on a systematic review of the literature relevant to the development of ISA content within both private and public sector organisations. The findings from the reviewed studies are analysed using a systematic, rigorous process (Okoli and Schabram, 2010). In order to confirm that the review process is rigorous and valid, the guidelines suggested by Okoli and Schabram (2010) and Webster and Watson (2002) have been followed. A systematic literature review is most appropriate to answer the stated research question as a structured and rigorous approach ensure comprehensive coverage of the research topic and identify the current body of knowledge in the field of ISA content development.

The Eight-Step Systematic Guide provided by Okoli and Schabram (2010) to carry out the rigorous, scientific literature review has been particularly used in this paper (see Fig. 1), as it focuses specifically on the information systems field and incorporates SLR guides from related fields as well as covering a synthesis of both quantitative and qualitative primary studies.

Step 1: Purpose - Defining the purpose of the review is the first step of conducting a literature review (Okoli and Schabram, 2010). The purpose of this research is to analyse the progress of ISA content development and provide the current state-of-the-art in the content development of ISA within both the private and public sector through identifying and understanding various ISA content development methods and factors that influence employee's ISA. The research aims to fill the gap identified in the related research section by answering our research question: *What are the methods and factors used in IS literature to enhance employees' ISA in organisations within both the private and public sectors?*

Step 2: Protocol - Inclusion and exclusion criteria were used as per the publications' relevance to the research question. The studies related to employees' ISA and behaviours which provide methods and factors for ISA content development in both private and public sector organisations were included. However, publications on ISA evaluations were excluded since it is beyond the scope of this review. Only English publications that were published between the years 2009 and 2020 were included and articles in other languages and articles published prior to the year 2009 were excluded. Peer-reviewed conference papers and journal articles were included and non-academic publications such as white papers, books and company reports were excluded. Another criterion was to check if the publications' journals were listed in Beall's list of predatory journals to ensure the authenticity and quality of the publications, therefore those papers listed there were excluded. All the excluded publications were cross-checked by each author to ensure that all authors agreed about the exclusion.

Step 3: Searching for the Literature - With the use of the protocols stated above, the third step of 'searching for the literature' began with the selection stage. To maintain reliability and consistency throughout the process, it is critical that the actual search procedure is carefully documented so that the reviewer can report in explicit detail on how the search was conducted (Okoli and Schabram, 2010). Table 1 shows the list of databases searched, keywords, criteria and delimitation used, along with the number of papers found and selected through the search process.

These major keywords (see Table 1) were used alternatively or sequentially based on the situation to narrow down the number of papers and find and select the most relevant papers.

Relevant keywords for the research questions were selected as mentioned in Table 1. The keyword "*information security awareness*" was used with the Boolean operator 'AND' to get more related results. We also did a general search where we used only the "*information security awareness*" keyword, this covers all publications within the information security awareness domain, including ISA methods and ISA factors. This general search was important to make sure that we did not miss any relevant publications for the review.

The search was limited to studies in the English language. The focus of the study was on gathering scientific knowledge on the current state-of-the-art in ISA content development. Only peer-reviewed scholarly articles from journals and conferences published during the last ten years were taken into account.

To search for the literature, we used the following three databases: Elsevier's database (i.e., Scopus), Clarivate Analytics' database (i.e., Web of Science), and Google Scholar. Firstly, we searched for the literature through the Web of Science (WoS) since it provides comprehensive in-depth coverage of peer-reviewed articles with high-quality content (Falagas et al., 2008). Next, we expanded our search through the Scopus database as it offers a wider range of peer-reviewed journals compared to Web of Science (Falagas et al., 2008). Both Scopus and WoS complement each other as neither resource is all-inclusive. Additionally, in order to widen our scope for the search and to avoid the limitation of only searching in top journals as well as providing a more in-depth SLR, we used Google Scholar as to cover most if not all of the available journals and conference proceedings. We exhausted our search through google-scholar, however, while saturating our search, we have also cross-checked the relevant papers found

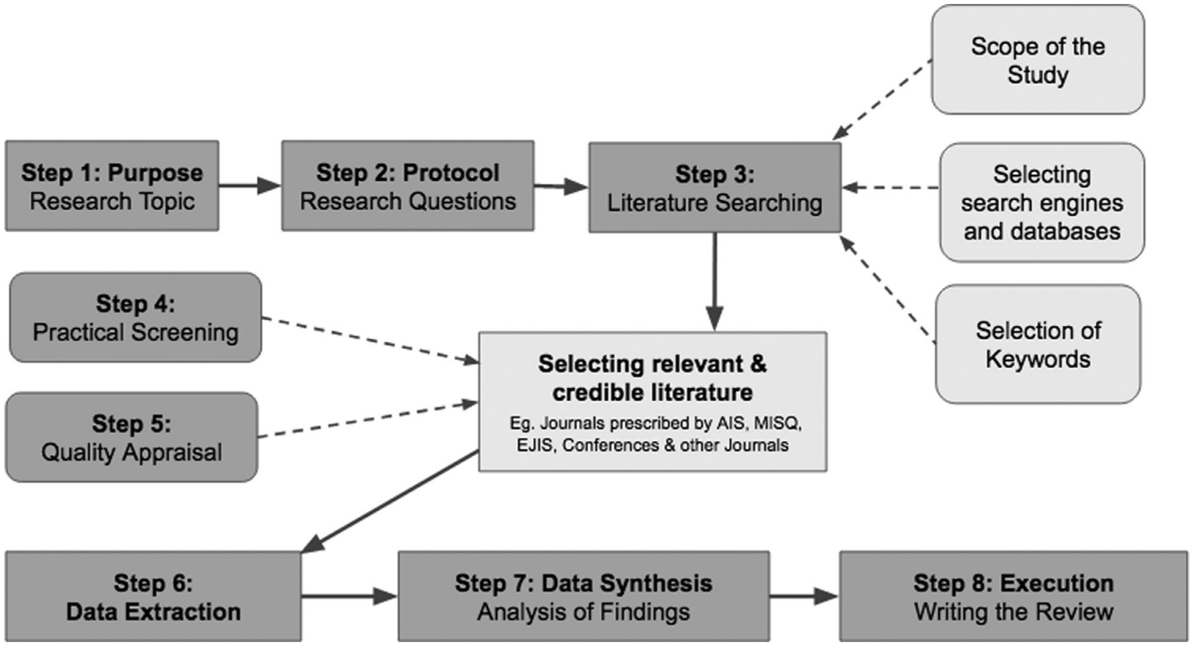
Scope of the Study
Step 1: Purpose Research Topic
Step 2: Protocol Research Questions
Step 3: Literature Searching
Selecting search engines and databases
Step 4: Practical Screening
Selecting relevant & credible literature
Eg. Journals prescribed by AIS, MISQ, EJIS, Conferences & other Journals
Selection of Keywords
Step 5: Quality Appraisal
Step 6: Data Extraction
Step 7: Data Synthesis Analysis of Findings
Step 8: Execution Writing the Review

Fig. 1 – Illustrating Systematic Review Process (Okoli and Schabram, 2010).

Table 2 – List of databases searched, criteria and delimitation used and hits obtained.

Keywords	Database/ Journals/ Conferences	Delimitation Criteria	Hits	Selection after reading the title
“information security awareness” OR “Information security awareness AND development” OR “Information security awareness AND method*” OR “Information security awareness AND factor*” OR	Web of Science	Language: English Document Type: Conference and Journal Articles Publication stage: Limit to Final Publication Year: from “2009” to “2020”	184	98
“Information security awareness AND program*” OR	Scopus		220	115
“Information security awareness AND campaign”	Google Scholar		640	102
Total	1044	315		
Subtracted the Duplications (131 Duplicate Articles)	−131			
Total Articles selected through the search process	184			

through google-scholar against Beall’s list of predatory journals to ensure authenticity and quality of the publications obtained through this search engine. A total of 184 relevant publications were identified for the review, after reading the titles, applying the delimitation criteria and sorting out the duplications on ‘March 3, 2020’ (Table 2).

Step 4: Practical Screen – A list of potential articles (i.e., 184) obtained through the ‘searching’ step were screened for inclusion by carefully reading the abstract, to decide if they were worthwhile for the purposes of the review. The articles were weeded out here based on two criteria - content applicability and being explicitly focussed on the research question to restrict the number of articles so that the study was practically manageable (Okoli and Schabram, 2010). Keeping this in mind, after reading the abstract, the studies not related to our research questions were excluded. For instance, studies related to ISA programme evaluation or articles on the assessment of ISA were excluded since this area is outside of the scope of this review. In total, 105 articles were screened out in this step and only 79 publications were considered for the quality screening in the next step. In addition, the journals were segregated based on the studies conducted in private and public settings in order to draw a comparison later in the discussion section (studies conducted in universities and healthcare institutions were included as public). This screening was performed mainly focusing on the state-of-the-art approaches in ISA content development in terms of methods and factors affecting employees' ISA in private and public sector organisations.

Step 5: Quality Screen - The 79 articles which were potentially eligible and collected through the practical screen were examined more closely to assess their quality. Firstly, the articles that did not meet the standard or scoring of the methodological quality were screened out. Methodological quality refers to "the extent to which the design and conduct of a study are likely to have prevented systematic errors (bias) and, as a result, identified the truth in its results and inferences" (Samuel et al., 2016 p.4). As recommended by Fink (2005), we developed a standard form and distributed it amongst us to carry out a quality appraisal, and assessed each article separately.

We screened out the articles based on the in-depth judgement of an article's data collection methodology (Fink, 2005). We assessed whether the study holds up to test-retest reliability in terms of methods used, inter or intra-rater reliability, homogeneity of data and if the study applied acceptable statistical methods, more specifically whether the study has used reliable and valid independent and dependant variables to validate it for quality (Fink, 2005). We assessed the external validity - the extent to which a study provides a correct basis for generalising to other circumstances (Henderson et al., 2013) and also checked the internal validity - the extent to which the design and conduct of study minimised bias and errors (Henderson et al., 2013).

With regard to knowledge type, only empirical findings were included in the study to ensure the quality of the review. The theoretical articles that exclusively relied on theory or model-building without an empirical component and literature review articles that relied on secondary sources for data were excluded, although their findings were taken into account, e.g., in the related work (Section 2.3). The quality screening was done by reading through each article, its title and abstract as well as skimming through the full text. A total of 27 articles were screened out through this quality screen and only 52 articles were selected for the final review. Citations of these 52 selected articles were reviewed if found relevant to the research question, for example; going backwards by reviewing the citations for the selected articles and going forward to relevant sources such as in the Web of Science database (Webster and Watson, 2002). As a result, 12 additional relevant articles were identified. In total, 64 articles were finally selected and confirmed for the review as shown in Table 3.

Step 6: Data Extraction - The practical screening and quality appraisal have left us with a complete list of articles (i.e., 64) that comprise the materials for the final systematic review. As recommended by Okoli and Schabram (2010), a clean extraction form was developed to store information about each study with provision for the required details and authors' comments.

Step 7: Data Synthesis - Our literature review is concept centric (Webster and Watson, 2002). We synthesised the extracted data into several themes and categorised them into ISA content development methods and factors, as concepts to determine the organising framework of a review. The concept-centric method of Webster and Watson (2002) was used in synthesising the data by following the systematic process (refer to Fig. 2 under Section 4).

The articles were divided amongst the authors and were analysed individually. The uncovered ISA content development methods and factors were grouped and presented in a logical approach. Further as stated by Webster and Watson (2002), we organised and presented the methods and factors into a tabular format under each category in the results section (Tables 3-6). The categories were contextualised and considered them from the organisational perspective both within private and public organsations. We intentionally avoided repeating the similar work from previous literature reviews into our analysis. However, the findings of the previous literature studies are considered in the review.

Step 8: Writing the Review - After following all 7 of the steps above, we have arrived at the final step of reporting the findings and writing the review paper. We have not only reported the procedures but also highlighted the themes and have drawn a comparative analysis between the themes including setting the contexts, which will contribute to existing knowledge on ISA content development.

4. Results

In this section, findings from our literature analysis are presented. Fig. 2 illustrates the main findings from the SLR. Out of 64 articles reviewed for the study, 42 articles revealed methods and factors in the private sectors and 22 articles focus on public sector organisations.

4.1. *ISA content development methods in the private sector*

An overview of the identified ISA content development methods from the selected literature which shows that empirical evidence exist for these methods for enhancing employees' ISA levels is presented in Table 4.

4.1.1. *Theory/Framework/Models*

For ISA content development methods to be successful, the content of the ISA programmes cannot be developed based only on what the technical experts want to teach or based just on technical requirements or best practices, rather it is critical to understanding the relevant beliefs of the employees (Stewart and Lacey, 2012). In the light of these perspectives, psychological concepts are used for ISA content development. The frameworks such as bounded rationality, mental models and the Extended Parallel Processing Model are useful in promoting awareness education in organisations. Bounded rationality helps explain why logical people do apparently illogical things. Mental models show the importance of existing beliefs and how they can be used to identify requirements for specific items of awareness content. The Extended Parallel Processing Model shows how risk outcomes can be traced back to specific problems with one of four message components. These three conceptual frameworks offer an opportunity for a more formal and consistent approach to planning and developing ISA content (Stewart and Lacey,2012).

Table 3 – Selection of papers through practical and quality screening (Step 4 & 5).

Total No. of paper from search	Criteria used for Practical Screening	No. of papers screened out	No. of papers selected after practical screen		Criteria used for Quality Screening	No. of papers screened out	No. of papers selected after Quality Screen	
			Pvt 47	Pub 32			Pvt 35	Pub 17
184 (Papers found through the Searching process)	Inclusion criteria: - Content applicable to the research question - Studies related to employees' ISA & behaviours - Articles on ISA Methods/Factors in public/private sector Exclusion criteria: - Articles out of the scope of this review e.g., excluded studies related to ISA program evaluation - Non-academic publications such as white papers, book chapters & company reports - Access to full text not possible for some relevant articles beyond the abstract, therefore excluded	105	79		Inclusion criteria: - Appropriate use of methodology and data collection strategies with clarity and valid arguments - Studies providing clear and valid practical and theoretical contributions - Studies providing quality arguments in favour of central statements with validity and reliability Exclusion criteria: - Low scoring rate on "hierarchy of evidence", articles intrinsically providing less validity and reliability results - the in-depth judgement of an article's data collection methodology. E.g. studies that do not hold up to test-retest reliability in terms of methods used, inter or intra-rater reliability, homogeneity of data and studies that did not apply acceptable statistical methods - Studies with low sample size to generalize findings - Theoretical studies and literature review articles were excluded - Central statements lack sufficient quality of argumentations that contains fallacies	27	52	
Additional articles (12 papers) selected through backward citation searching							7	5
							+12	
Total number of papers used for the review							42	22
							64	

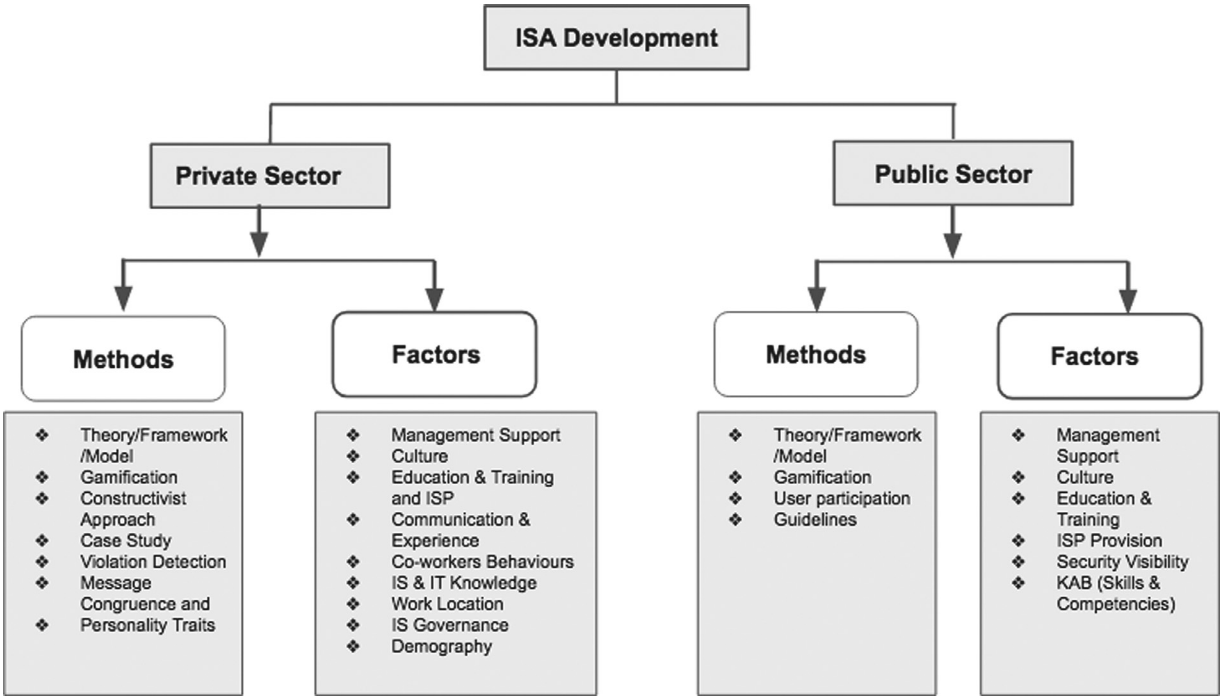

Fig. 2 – Methods and factors in the process of ISA development in private and public organisations.

Table 4 – ISA Content development methods in the private sector.

Methods	Author (Empirical Evidence)
Theory/Framework/Model (influencing behaviour)	Stewart and Lacey (2012); Gundu and Flowerday (2013); Poepjes and Lane (2012); Allam et al. (2014); Bauer et al. (2017); Singh et al. (2013)
Gamification (Play, Engagement)	Gjertsen et al. (2017)
Constructivist approach (Self-building)	Boujettif and Wang (2010)
Violation Detection (information security policy violation)	Choi and Lee (2015)
Case study (Contextualisation)	Parsons et al. (2014)
Message Congruence and personality traits (Information richness)	Kajzer et al. (2014); Myyry et al. (2009); D'Arcy et al., (2009); Anderson and Agarwal (2010); Puhakainen and Siponen (2010); Shaw et al. (2009); Ki-Aries and Faily (2017); Abawajy (2014); Al Sabbagh et al. (2012)

A substantial portion of information security incidents in the small-and-medium-sized enterprises (SMEs) originates from employees within the firm (Gundu and Flowerday, 2013). This is mainly due to employees increasingly having access to their own personal workstations. The technical security measures can solve only some of the issues since uninformed naive employees pose great risks to the firms due to lack of security knowledge. The use of theories in developing the content for ISA programmes has proved effective in such cases. The Theory of Reasoned Action (TRA), the Protection Motivation Theory (PMT) and the Behaviourism Theory (BT) have been used in developing ISA content to achieve a positive influence on the employees' behavioural intention. TRA suggests that a person's Behavioural Intention depends on the person's Attitude about the behaviour and Subjective Norms. So, using TRA in developing content for ISA programmes, helps to change employee attitudes towards information security and will help in communicating the firm's expectations to its employees (Gundu and Flowerday, 2013).

On the other hand, PMT aims to assist and clarify fear appeals. It is known to predict an individual's intention to engage in protective actions. Information security awareness instils knowledge in the employees and assists in motivating protection. ISA programmes are designed to communicate the company's subjective norms on information security, threat appraisal, coping appraisal and an effort to change the employees' attitudes towards greater IS compliance (Gundu and Flowerday, 2013). The BT explains the learning process built on four basic assumptions, Firstly, learning is manifested by a change in behaviour and the environment shapes behaviour. Thirdly, the principles of contiguity (how close in time two events must be for a bond to be formed) and reinforcement (any means of increasing the likelihood that an event will be repeated) are relevant. These ideas explain that learning is obtained through new behavioural changes. For example, BT is used in creating the content for the ISA campaign, so that an employee who perceives the high risk to their firm's information system resource will be more likely to adopt new protective behaviours. Thus, it was observed that the TRA, PMT or the BT can affect desirable behavioural intention and these persuasive theories can be used effectively as methods for enhancing employees' ISA (Gundu and Flowerday, 2013).

Models are also used as methods for improving the employee's ISA level. Poepjes and Lane (2012) developed an Information Security Awareness Capability Model (ISACM) in accordance with ISO/IEC 27,002. The model maintains an appropriate level of awareness for Information Security Controls as it highlights critical aspects of ISA - Awareness Importance, which refers to how important awareness is, Awareness Capability, which refers to how capable a person is when faced with a decision, and Awareness Risk, which is the gap that results from the required amount of awareness (Poepjes and Lane, 2012).

An iterative management cycle process, such as the Plan-Do-Check-Act (PDCA), is recommended to be incorporated in the ISA programmes development and adaptations to ensure continuous improvement (Bauer et al., 2017; Singh et al., 2013). Development of ISA programmes content should be planned, executed, and evaluated. Based on the outcome of the first three steps, further action for the next iteration should be taken (Bauer et al., 2017; Singh et al., 2013). This iterative method improves ISA levels and achieves ISP compliance.

4.1.2. *Gamification*

Gamification is relatively new in the area of ISA. It means that employees can play and engage with a specially developed game to become more aware of the information security threats and vulnerabilities. Gamification is found to be a suitable solution for enhancing employees' ISA level since it personalises the ISA training content to suit the needs (Flores and Ekstedt, 2016). Similarly, Gjertsen et al. (2017) conducted an empirical study to investigate the efficacy of the gamification in Scandinavian companies. The authors presented an interactive prototype game to employees in workshops and the results showed that the employees were more motivated and willing to adhere to the ISA methods being used. Gamification provides mastery and progression which engages people at the personal level which in turn improves the ISA levels of employees (Gjertsen et al., 2017).

4.1.3. *Constructivist approach*

A constructivist approach means that the employees are the ones who build and develop the ISA campaign and ISA training. This approach is used as a method for enhancing employees' ISA (Boujettif and Wang, 2010). This particular approach makes employees more concerned and aware of information security. This approach was carried out in more than 30 private companies in Saudi Arabia. Through enjoyable and interactive collaboration activities, the employees in that study were asked to develop content for an ISA campaign. This method was based on practices amongst companies in the Middle East and was found to have enhanced employees' level of ISA in industrial settings (Boujettif and Wang, 2010).

4.1.4. *Violation detection*

The Violation Detection method is used to develop content for the ISA campaigns (Choi and Lee, 2015). This method basically means developing content for ISA campaigns based on employees' ISP violation. It is used through a physical access control method by Radio-Frequency Identification (RFID) that protects data from being accessed by unauthorised persons. The RFID technology will detect and register any unauthorised access to the information by an employee. Hence, an ISA message about this specific violation will be sent to that particular employee. The number of instances of unauthorised access has been dramatically decreased in the organisation when this method was adapted. And at the same time, the ISA level amongst the employees has improved by using this approach.

4.1.5. *Case study*

Generic ISA campaigns are limited to increasing employees' knowledge about ISP and security procedures, while contextualisation of the ISA campaigns will lead to increased knowledge and an improved attitude towards ISP and security procedures (Parsons et al. 2014). The case study can be utilized as a tool to raise ISA about the ISP which also helps to set out the importance of ISP compliance. Hence, case studies proved to be an effective tool to increase employees' knowledge and behaviour with regard to ISP (Parsons et al. 2014).

4.1.6. *Message congruence and personality traits*

Several techniques are employed to deliver the contents of the ISA campaigns including emails, workshops, e-learning, hyper multimedia, multimedia hypertext (Shaw et al., 2009; Wilson and Hash, 2003). Hypermedia has a positive influence on ISA (Shaw et al., 2009; Abawajy, 2014; Al Sabbagh et al., 2012). In hypermedia, the information is presented visually with video, audio, graphics and text. This indicates that information richness is important in developing materials for ISA programmes. The 'messages' conveyed through these delivery methods are normally focused on a particular theme or set of themes such as deference, morality, regret, feedback and incentive (Kajzer et al., 2014; Johnston et al., 2016). Applying these message themes in the ISA development training and communications has proved effective in enhancing employees' ISA knowledge, preventing undesirable security behaviours and encouraging security-conscious decision-making behaviours (Anderson and Agarwal, 2010; Puhakainen and Siponen, 2010). For instance, it was found that a security awareness message which contains 'morality' helped to increase compliant behaviour and deterrence-focused messages detailing punishment for employees can prevent IS misuse (Myyry et al., 2009; D'Arcy et al., 2009).

On the other hand, personality also plays a vital role in ISA message effectiveness (Kajzer et al., 2014). Even though not all users respond to ISA messages in the same manner, it is possible that more effective ISA and change in awareness behaviour can be achieved through personality traits identified in the most widely accepted model, the Big Five - openness, conscientiousness, extraversion, agreeableness and neuroticism. It is evident that top management staff who understand the personality of an at-risk employee can strategically prevent him/her from insider incidents. By concentrat-

Table 5 – ISA content development factors in private sector.

Factors	Author (Empirical Evidence)
Management Support (Management Security participation)	Hwang et al. (2019); Hadasch et al. (2012); Bulgurcu et al. (2010); Hwang and Kim (2016); Tsohou et al. (2010)
Culture (Cultural background influence security perception)	Al Sabbagh et al. (2012); Talib et al. (2010); Da Veiga, 2015; Wiley et al. (2020); Mani et al. (2014); Hovav and D'Arcy (2012)
Education & Training and ISP (Information Security Policies)	Haeussinger and Kranz (2013); Hwang et al. (2019); Eminağaoğlu et al. (2009); D'Arcy et al. (2009)
Communication and Experience	Hadasch et al. (2012); Haeussinger and Kranz (2013); Hwang et al. (2019)
Co-worker behaviours (autonomy, shareability and openness)	Choi and Kim (2015); Dinev et al. (2009); Mani et al. (2014); Haeussinger and Kranz (2013); Siponen and Vance (2010); Herath and Rao (2009)
IS & IT-knowledge (General knowledge about basic IT applications)	Mejias (2012); Haeussinger (2013)
Work Location (working remotely vs organisational environment)	Hadlington et al. (2019)
Information Security Governance (Separate department/unit for Information security)	Flores and Ekstedt (2015);
Demographic Characteristics (age, sex, working industry and education levels)	Chua et al. (2018)

ing on personality traits, organisations can strategically create and customise content for their ISA campaigns down to an individual level as the employees' receptive nature towards awareness messages can be easily known (Kajzer et al., 2014; Johnston et al., 2016). Hence, personal traits are used as methods to enhance employees' ISA level.

4.2. *Factors for ISA content development in the private sector*

In addition to the identified ISA methods in private organisations, an overview of ISA factors identified from the literature that empirically investigates ISA content developments in private organisations is presented in Table 5. The identified factors affecting employees' ISA should be considered in order to achieve positive information security behaviour in the organisation. The ISA factors go hand in hand with ISA methods since both complement each other in building relevant contents for effective ISA campaigns.

4.2.1. *Management support*

The management's support for information security yields better ISA practices and results in increased ISA in companies (Tu and Yuan, 2014). Management support is also crucial in facilitating the resources needed for ISA development. This is further emphasised by Tsohou et al. (2010) who state that reasonable resources for security management are essential for establishing sufficient levels of security awareness amongst employees. Tu and Yuan (2014) analysed the factors leading to effective information security management and found that top management support leads to enhanced ISA in an organisation. Hadasch et al. (2012) also found in their empirical study that the shared understanding amongst employees is influenced by the way they perceive the role of management and the persuasiveness of communication by the managers. Hwang at al. (2019) states "Interestingly, managerial security participation has the strongest relationship to employees' awareness". In their empirical study respondents identified several factors positively contributing to their information security awareness and found that top management participation strengthens the links between organisational security efforts and security awareness.

It was claimed that the voluntary participation of managers serves as a catalyst for enhancing ISA amongst employees. However, the challenge is that at the time of ISA program implementation the employees' security consciousness may be limited to the information provided (e.g., Bulgurcu et al., 2010; Hwang and Kim, 2016). Nonetheless, there is a positive effect of managerial participation on the learning process which acts as a catalyst for ISA of the employees.

4.2.2. *Culture*

Jaeger (2018) states that many studies tend to neglect possible cultural differences because they are conducted in Western cultures. Nevertheless, Hovav and D'Arcy (2012) investigated information systems misuse in the US and South Korea and found that cultural differences associated with ISA's impact on IS misuse existed between these two countries. This is further supported by Al Sabbagh et al. (2012) stating that individual cultural aspects influence security awareness and learning. They also developed a tool as a platform that can help in enabling a global security culture by creating a common understanding of security best practices, improve individual security awareness and learn more about how their cultural background influences their perception of security. Talib et al. (2010) emphasised the development of an information security culture within the organisation and embedding long-term security practice within employees. They argue that through establishing an information security culture in the organisation, employees can become self-fulfilling with regard to ISA issues and be proactive about their security practices. Da Veiga, 2015 proposed an Information Security Training and Awareness Approach (ISTAAP) to foster an Information Security- Positive Culture. The model serves as an effective approach to implement information security training and awareness initiatives whereby success can be measured in the context of an information security culture. Through this model, it was found that the group of employees that had been exposed to prior information security awareness had a more positive information security culture compared with those that had not (Veiga, 2015).

On the other hand, Wiley et al. (2020) empirically examined the relationship between culture and Information Security Awareness. The study shows that there is a strong relationship between the security culture and ISA - improving the security culture influences and improves employees' ISA. Another important finding from their study is that the security culture mediates the relationship between organisational culture and ISA. Mani et al. (2014) surveyed real estate organisations in Australia to examine employees' ISA creation process by applying Nonaka's SECI model. It was found that Socialisation, Internalisation and Combination appeared to wield a positive influence on developing a culture of information security that, in turn, positively impacted the ISA level in real estate organisations.

4.2.3. *Education & training and ISP*

Employee's information security knowledge is one of the key determinants of ISA as the increased knowledge of basic security applications lead to higher ISA level (Haeussinger and Kranz, 2013). Further, Hwang et al. (2019) indicated that knowledge of a physical system had a very negligible effect on ISA but security education and policy influenced ISA.

Information Security Policies (ISP) is a crucial factor when it comes to information security management practices (Haeussinger and Kranz, 2013). It was discovered that provision and promotion of ISP was an effective way to increase employees' ISA. Other factors that have a positive effect on the ISA of employees in the private sector includes security education, and training and awareness (SETA) raising programmes. The employees' ISA is improved through the SETA programme which aims to develop their competencies and the skills required to be aware of the potential security risks and threats and also to make them understand the rules and regulations laid down in the ISP (D'Arcy et al., 2009; Eminağaoğlu et al., 2009). Studies have shown that the level of an individual's ISA is increased by SETA programmes in private sector organisations (Haeussinger and Kranz, 2013; Eminağaoğlu et al., 2009).

4.2.4. *Communication and experience*

Identifying and communicating the topics that have the greatest value to the organisation represent the first step in planning a security awareness programme as these actions have the greatest positive impact (SANS 2020 Security Awareness. n.d). An employee's perception of the value of information and an organisation's information security communication enhances ISA through a higher perception of the importance of information protection (Hadasch et al., 2012). Similarly, previous negative experience with information security incidents lead to higher levels of an employee's ISA (Haeussinger & Kranz (2013). Hwang et al. (2019) recently linked workplace security-related experiences and observations to employees' security awareness and found that security awareness arose from both explicit and subjective security experiences in the workplace. They argued that awareness was not only the conscious awareness of stimuli in a present experience but also occurrences of the past, present or future, therefore, the past and current security programmes experiences would contribute to employees' ISA.

4.2.5. *Co-worker behaviours*

The ISP compliant behaviour of co-workers has a positive impact on the information security behaviours of other employees in organisations (Siponen and Vance, 2010; Herath and Rao, 2009). Choi and Kim (2015) investigated the co-working environment's influence on ISA and identified three characteristics of the co-working environment autonomy, shareability and openness. The findings indicated that autonomy and shareability had a positive influence on ISA and information security behaviour. This was also supported by Haeussinger and Kranz (2013) who found a significant effect of peer behaviour on the ISA of employees. Further, it was empirically shown that business employees gained ISA through conversations with their counterparts and through learning from other peoples' IS incident events (Mani et al., 2014). In addition, the values of the social group that the employees are associated with have a positive impact on how the employees deal with ISA (Dinev et al., 2009).

4.2.6. *IS & IT-Knowledge*

Improving employees' IT knowledge is one of the most influential antecedents of ISA (Haeussinger, 2013). Employees' IT knowledge refers to general knowledge of the basic IT applications used in daily business, such as computers, email systems, and the internet. The level of general IT knowledge positively influences employees' level of ISA (Haeussinger, 2013). The more knowledgeable the employees are about information security and IT, the more they are aware of information security issues. Thus, organisations are advised to enhance the IT knowledge of employees to prevent them from unintentional misbehaviours (Haeussinger, 2013). This was further supported by Mejias (2012) who empirically concluded that technical knowledge of employees about malicious IT is positively associated with ISA.

4.2.7. *Work location*

Employees' work locus of control is a factor that influences ISA, as employees who are used to working remotely or externally have a low level of ISA compared to those who are working in the organisational environment (Hadlington et al., 2019).

4.2.8. *Information security governance*

The information security governance structure in an organisation can influence employees' ISA level. For example, having an information security department or an information security officer role within the organisation enhances employees' ISA level (Power and Forte, 2006; ENISA, 2008). It was found that having a unit or department explicitly promoting and working with information security had a huge impact on employees ISA (Flores and Ekstedt, 2015). This is because organisations with an information security unit prioritise information security awareness activities and can establish an information security culture within the organisation. (Flores and Ekstedt, 2015).

Table 6 – ISA content development methods in the public sector.

Methods	Author (Empirical Evidence)
Theory/Framework/Model	Tsohou et al. (2015); Serfontein et al. (2018); Saraçlı and Erdoğmuş (2019); Tsohou et al. (2012)
Gamification (Paly, Engagement)	Ghazvini and Shukur (2018)
User participation / group dialogue (workshops, discussion)	Albrechtsen and Hovden (2010); Khan et al. (2011)
Guidelines (instructions)	Ghazvini and Shukur (2017b); Ghazvini and Shukur (2016)

4.2.9. *Demographic characteristics*

Demographic characteristics such as age, working industry and education levels have significant effects on ISA (Chua et al., 2018). Their study states that many employees are unaware of the Personal Data Protection laws enforced by the government such as GDPR, Fair Information Practices (FIPs), Personal Data Protection Act (PDPA), which raises the concern of consumer data privacy, particularly in terms of how consumer data is handled by the organisations (Callanan et al., 2016). Profiles of employees' policy awareness level and their intention to comply were created through demographic factors to assist companies to reduce the risk of non-compliance (Chua et al., 2018). It was observed that there was no statistically significant difference in policy awareness and compliance between males and females, and different ethnic groups. However, significant differences were observed between age, work experiences distributions and education level. For example, the older or more experienced the employees were, the more they were aware of the data protection laws (Chua et al., 2018).

4.3. *ISA content development methods in the public sector*

ISA should be an integrated part of digital changes taking place in the society including the digital transformation in the private as well as in the public sector (Scholl et al., 2018). Scholl et al. (2018) argued that humans should not be called the weakest link in the security chain because the institutions still lacked some of the fundamental strategic functions such as sustainable awareness-raising and training which can be achieved through using various ISA content development methods. Table 6 presents the content development methods used for enhancing employees' ISA in public organisations.

4.3.1. *Theory/Framework/Model*

The main purpose of ISA is to change behaviour and ISA changes are attached to interrelated changes that occur at the organisational, individual, and technological level (Tsohou et al., 2015, 2012). Organisational behaviour presents an integrated analytical framework comprising actor-network theory (ANT), structuration theory and contextualism theory to consider the multi-level changes at an organisation. It was found that synergies of the three theories were needed to study and manage awareness-related changes at all three levels - the individual, organisational and technological level. On the other hand, there were limitations discovered when they are individually applied to study information security awareness (Tsohou et al., 2015).

Security awareness is socially constructed rather than an objective tool or technique. ANT is applied to analyse organisational problems with regard to ISA (Tsohou et al., 2012). According to Tsohou et al. (2012), psychological and behavioural theories cannot adequately address social and organisational aspects of security awareness. They applied ANT through the due process model extension which considers that ISA initiatives involve different stakeholders, with often differing interest (Tsohou et al., 2012). ISA involves diverse stakeholders from different sections of the organisation and ANT forms the actor-network which includes not only human actors but also non-human actors such as ISP and standards, and other awareness related materials. The interests of each actor group differ from those of another and these need to be aligned in order to gain commitment for security. The study recommends security practitioners to develop negotiation and management skills to address these organisational issues (Tsohou et al., 2012).

Serfontein et al. (2018) suggest using the Social Network Analysis (SNA) in the academic environment to develop and improve ISA. Since universities as an organisation differ from other traditional organisations due to their structure and users, formal ISA programmes can't target both personnel and students as they may not be feasible for the students. The SNA approach can help to design targeted informal ISA programmes for the students to be more effective and feasible (Serfontein et al., 2018).

Saraçlı and Erdoğmuş (2019) empirically investigated the ISA of university students through statistical techniques. They used Structural Equation modeling (SEM) in their study which revealed the awareness status quo and gave some suggestions to improve the awareness. Their results have shown that to improve ISA, users at a university should have adequate knowledge about spyware, generate a strong password, be careful about sharing location information and personal pictures (Saraçlı and Erdoğmuş, 2019).

4.3.2. *Gamification*

Ghazvini and Shukur (2018) designed a serious game (i.e., InfoSecure) to improve ISA in the healthcare sector. The game consists of a few topics, like phishing, web use, malicious codes and password protection. Employees found it interactive and enjoyed playing the game. The evaluation shows that employees' ISA level has relatively increased after playing the game. Moreover, employees showed a willingness to participate in ISA training as they had a pleasant time playing the game (Ghazvini and Shukur, 2018).

4.3.3. *User participation and group dialogue*

User participation and employee engagement are fundamental for a successful ISA (Power and Forte, 2006). Albrechtsen and Hovden (2010) undertook research on improving information security awareness through workshops, dialogue and user participation. The results indicated that workshops, dialogue and user participation had a huge impact on the user's awareness and behaviour with regard to information security. With user participation, users are involved and engaged with the ISA content development activities. This would make them share the sense of ownership which can increase compliance. The public organisations use group dialogue/discussion for employees to participate and share knowledge and experiences amongst themselves where everyone is given an equal chance to share their viewpoint on security issues and other policies and procedures regarding ISA (Albrechsten and Hovden, 2010). Through this platform; participants are given the opportunity to explain their personal security incidents and experiences with other group members thereby motivating the participants to adopt positive information security behaviour. This approach employs TRA to alter intention by changing attitudes and norms. Group discussion is more interactive and thus, draws more attention and promotes improved behavioural intentions amongst participant with regard to ISA (Albrechsten and Hovden, 2010). Group discussion uses knowledge, attention, attitude, social norms, motivation and behavioural strategies to influence an employee's understanding of information security and enhance the level of ISA (Khan et al., 2011).

4.3.4. *Use of guidelines*

One of the methods for enhancing employees' ISA is through the use of guidelines. Ghazvini and Shukur (2017b) presented guidelines on how to develop ISA content in the context of healthcare. The ISA campaigns and training must be developed based on: "i) the healthcare organization's internal ISP; ii) information security international standards; iii) common information security mistakes made by employees; iv) selected training delivery method; and iv) targeted audience profile" (Ghazvini and Shukur, 2017a, p. 194). The same authors previously provided guidelines on how to decide on awareness delivery methods for health organisations (Ghazvini and Shukur, 2016). They have stressed focusing on training delivery methods and training success factors to develop effective awareness training.

4.4. *Factors affecting ISA content development in the public sector*

Studies on ISA in public administration discovered that more than 50% of the institutions did not train or educate their employees in information security (Scholl et al., 2018). Scholl's study concentrated on the practice of public administration in Germany and found that only 63% of respondents in Germany take measures to raise awareness of information security, and the Ponemon Institute Report 2017 reported that 74% of security incidents remain undetected for more than six months. The finding of all the investigated reports showed that cyberattacks shifted their target to the people - naive employees because they have found it is harder to break into the organisational IT systems (Scholl et al., 2018). In addition, it was found that there was a strong ISA correlation with the measure relating to the behaviours (Pattinson et al., 2016) and that the human element played a significant role in the successful delivery of information security in the public organisations (Scholl et al., 2018). The following factors presented in Table 7 are as result found to be impacting the ISA content development in the public institutions.

4.4.1. *Management support*

Top management support plays an important role in the management of ISA as the top management is mandated with the correct functioning of the institution as well as information security. If managers are not engaged with the ISA then employees are not likely to change their ISA behaviours (Maeyer, 2007). Another important factor that influences the ISA efforts is the role of an information security officer. The management has responsibility for integrating information security into the institutional systems and actively initiates and manages the security process. Management has the authority to mobilise or allocate funds for the IS (Ponemon Institute Report, 2017; Scholl et al., 2018; El-Haddadeh et al., 2012). Moreover, they have the opportunity to display leadership and be a role models for other employees. The management's participation in the development and implementation of ISA programmes can motivate the employees and improve their level of ISA (Hu et al., 2012, Hwang et al., 2019; El-Haddadeh et al., 2012). Verizon's data breach investigations Report 2017 reveals that the most difficult tasks for top management are to justify the cost of information security initiatives against the benefits and risks. Top management support is also crucial for security cultural changes to take place in the organisation which in turn has a positive impact on ISA development (Marks and Rezgui, 2009; El-Haddadeh et al., 2012).

4.4.2. *Culture*

A comparative study between universities shows sociocultural factors including conscientiousness, cultural assumptions and beliefs, and social conditions affect university end-users' behaviour and attitudes with regard to ISA (Marks and Rezgui, 2009). The ways in which the causes and sources of IS threats are perceived by end-users are rooted deep within cultural and religious beliefs based on the location of the institute. Research suggests concentrating more on security culture proves to be more practical because organisations effectively manage their time and resources by focusing on what is needed to enhance employee ISA (Wiley et al., 2020). The cultural factors such as mother tongue, the area where one grew up, etc., greatly impact employees' ISA level and should be considered in the ISA content development plans and programmes (Kruger et al., 2011).

4.4.3. *Education and training*

Security education and training have a positive impact on the ISA of the employees (Hwang et al., 2019; Haeussinger and Kranz, 2013). Information Security Education is positively related to Information Security Awareness as security education leads to security awareness and organisational education and training improves the level of ISA (D'Arcy & Hovav, 2009;

Table 7 – Factors affecting ISA content development in public sector.

Factors	Author (Empirical Evidence)
Management Support (motivation, allocate resources and fund)	Hwang et al., (2019); Marks and Rezgui (2009); Hu et al. (2012); El-Haddadeh et al. (2012);
Culture (conscientiousness, cultural assumptions and beliefs, and social conditions)	Marks and Rezgui (2009); Wiley et al. (2020); Kruger et al. (2011)
Education and Training	Hwang et al. (2019); Haeussinger and Kranz (2013); D'Arcy and Hovav (2009); Ahlan et al. (2015)
ISP provision (Understandable and easily accessible policies)	Haeussinger and Kranz, 2013; Hwang et al., (2019); D'Arcy and Hovav (2009); Herath and Rao (2009); Puhakainen and Siponen (2010); Hwang and Kim (2016)
Security visibility (Exposure)	Hwang et al. (2019); Steinbart et al. (2013);
KAB - Knowledge Attitude Behaviours (Skills & Competencies)	Parsons et al. (2014)b; Budiningsih et al. (2019); Tarmizi et al. (2018); Kusumawati (2018)

Hwang et al., 2019; Ahlan et al., 2015). Institutional education such as Security Education Training Awareness (SETA) Programmes plays a pivotal role in improving employees' ISA (Haeussinger and Kranz, 2013; Ahlan et al., 2015).

4.4.4. *ISP provision (understandable and accessible policy)*

An ISP is an organisational tool that defines rules and guidelines for the appropriate use of information security resources in an organisation (D'Arcy & Hovav, 2009). Herath and Rao (2009) emphasise that ISP should be made easily accessible to the employees and should be written in clear understandable language as it affects employees' intention to comply. This element of effectively promoting ISPs reports a positive impact on employees' ISA since it raises their contextual awareness and knowledge and also their situational intention to comply with. Therefore, it was found that ISP provision positively influenced employees' level of ISA (Haeussinger and Kranz, 2013). An ISP can influence employees' behaviours by reminding them of sanctions and consequences for noncompliance which attracts their attention and stimulates ISA (Hwang and Kim, 2016). It is also confirmed that employees' ISA levels would be elevated through clear and concrete promotion of the ISPs (Puhakainen and Siponen, 2010). Therefore, there is a positive relationship between ISPs and ISA (Hwang et al., 2019).

4.4.5. *Security visibility (Exposure)*

Security visibility is conceptualised as the extent to which employees observe IS processes, activities and security incidents (Hwang et al., 2019). Thus, it also plays a vital role in maintaining ISP compliance (Siponen et al., 2009). The security compliance researchers find security visibility positively affects ISA. It was found that employees' non-compliance behaviours declined due to increased security visibility (Steinbart et al., 2013). Visibility activities such as displaying organisational security goals and objectives, promoting security activities and incidents stimulate awareness thereby improving employees' ISA (Hwang et al., 2019).

4.4.6. *KAB – Knowledge, attitude and behaviour*

Employees' knowledge of IS affects employee attitude to information security which in turn affects employee behaviour in reducing security risks and adapting to ISA (Tarmizi et al., 2018; Parsons et al., 2014a). Strong relationships are found between knowledge and attitude. However, it was found that employees did not necessarily change their behaviours towards ISA by having adequate knowledge as there are other factors which are likely to influence employees' behaviours such as personality and culture (Tarmizi et al., 2018). A recent ISA measurement in the government organisations found that even though the employees knew about ISA, they did't act in line with what they knew. Knowledge that is not optimal is also a result of the attitude and behaviour of low ISA (Kusumawati, 2018).

ISA is also influenced positively and significantly by the organisational support perception, competence and motivation. Amongst these three factors, the aspect of competence is the dominant factor that contributes to the ISA and the organisational support perception and motivation are found to be less significant in raising ISA. Therefore, the focus of the policy is to secure information to increase the competencies. The empirical investigation shows that ISA can be improved by competencies, knowledge, and skills (Budiningsih et al., 2019).

5. Discussion

Information security awareness (ISA) is one of the major elements to ensure information security and protect an organisation's assets from cyberattacks. The goal of this study is to investigate what are the ISA content development methods and factors used in the IS literature to enhance employees' ISA in both the public and private sectors. Hence, a comparative analysis of ISA methods and factors used in these two sectors is crucial in order to gain clear and concise knowledge in the field.

5.1. *Differences and similarities for ISA methods in the private and public sector*

An overview of the differences and similarities for ISA methods in the private and public sector is presented in Fig. 3. Theories, frameworks and models are widely and frequently used methods in the public and private sectors to develop

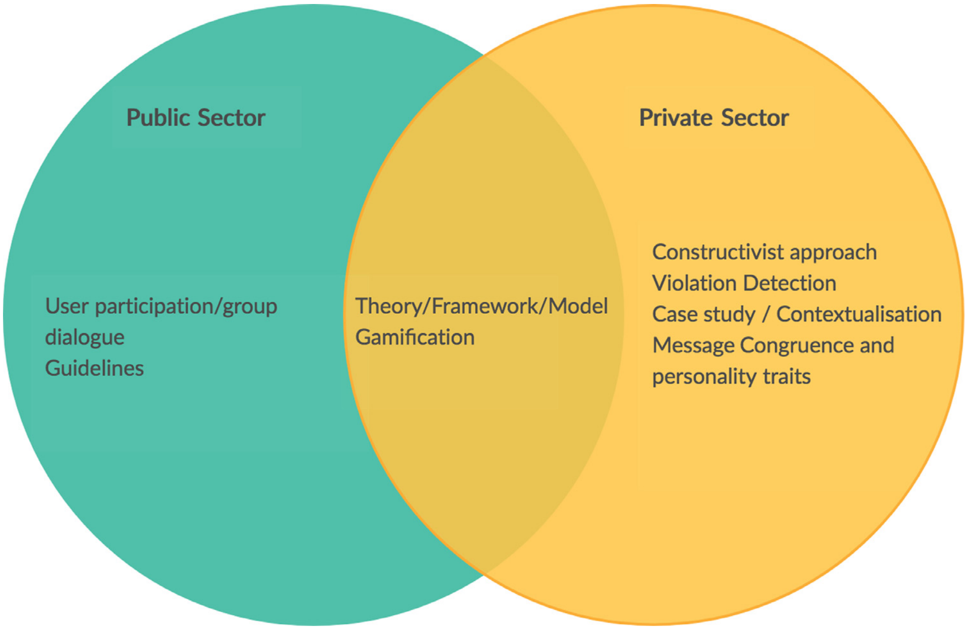

Fig. 3 – ISA methods in the private and public sector - differences & similarities.

ISA content. Theories are used often to analyse employees' security behaviour but we found that they are also used to enhance employee's ISA. In the public sector, Actor-Network Theory (ANT), structuration theory, contextualism theory and SNA theory were used as methods to develop ISA content and improve employees' level of ISA (Tsohou et al.,2015; Serfontein et al.,2018). These theories are known to be very well suited to large organisations with thousands of employees. The focus seems to be on the larger groups of employees and on the organisational level. Meanwhile in the private sector the focus is more on the individual employees' level. The goal is to understand the individual's belief by utilising mental models and behavioural theories. This indicates that the ISA content is developed based on the individual employee's belief and knowledge in order to change the behavioural intention in line with greater information security compliance (Stewart and Lacey, 2012; Gundu and Flowerday, 2013). Similarly, gamification has been proven to be one of the most effective and appropriate methods to develop ISA content. Therefore, our findings show that it has been used both in the public and private sectors (Gjertsen et al., 2017; Ghazvini and Shukur, 2018). The major difference spotted is that in the private sector a prototype game was used while a real game was developed in the public sector. However, the gamification method shares a lot of similarities when it is used in both sectors. The constructive approach is a new method to develop ISA content. Companies in the private sector ask their employees to propose and build their own ISA content (Boujettif and Wang, 2010). This method is not used in the public sector, the hierarchical structure and the limited work freedom in the public sector might be the reason.

The violation detection method is a new method to strengthen and develop ISA content based on ISP violation (Choi and Lee, 2015). This method has been empirically tested in the private sector and shown to have effective results (Choi and Lee, 2015). However, the method may require a larger budget since it includes implementing physical access controls. In general, we found that the literature has no clear, unified and sufficient number of guidelines on ISA programme or content development. However, there are guidelines that help practitioners to develop ISA programmes and content in the healthcare sector (Ghazvini and Shukur, 2017b). Guidelines can facilitate the process of ISA content development. However, the literature lacks the presence of comprehensive guidelines which can act as a reference for organisations. Thus, this area needs to be explored more by researchers. Management models such as PDCA are used in the private sector only (Bauer et al., 2017; Singh et al., 2013). The PDCA cycle model is known to be used to implement information security management systems and has proved its efficiency. The empirical studies also show its efficiency in creating content for the ISA programmes.

Overall, the ISA content development methods used for increasing employees' ISA in the private sector focus more on the individual level. Analysing and understanding the personality traits to build a user-adapted ISA programme is common in private sector organisations (Ki-Aries and Faily 2017; Kajzer et al., 2014). On the other hand, user participation is used in the public sector (Albrechtsen and Hovden, 2010), which also takes into account that individuals share feedback on ISA activities. However, it is also important to mention that user participation is different from adapting personality traits. By using an approach to adapt personality traits approach, content for an ISA programme is developed based on the knowledge, attitude and motivation of the users, which can lead to effective results. We also found that in the private sector they did consider the message congruence, information richness and how the information was formulated, designed and delivered (Shaw et al., 2009; Abawajy, 2014; Johnston et al., 2016). Further, an interesting method found in the private

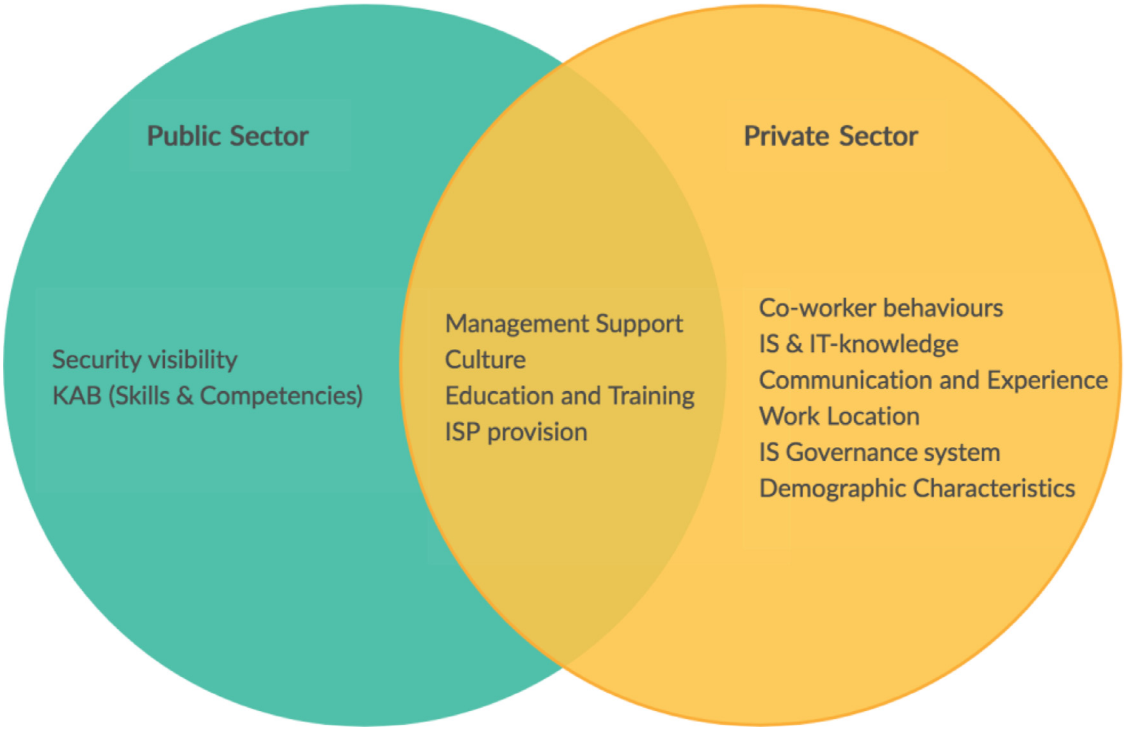

Fig. 4 – ISA content development factors in the private and public sectors.

sector is using the case studies of real information security incidents to contextualise the ISA efforts (Parsons et al. 2014a). Since this is a novel approach, more research is desired to determine its efficiency and effectiveness in developing ISA.

5.2. *Differences and similarities for ISA content development factors in the private and public sector*

An overview of the differences and similarities of ISA content development factors in the private and public sector is presented in Fig. 4. Top management support is a crucial factor in the success of ISA (Maeyer, 2007). Our research findings confirm this since this particular factor has been strongly considered in both the public and private sectors (Hwang et al., 2019; Marks and Rezgui ,2009; Scholl et al., 2018). Management support has been emphasised in most literature which reflects its importance; for instance, management support is necessary to gain a sufficient budget for the ISA activities. Establishing a security culture has become a key factor in the success of information security management (Van Niekerk and Von Solms, 2010). The security culture positively influences the ISA levels of the employees which can lead to behavioural change. We found that security culture as a factor has been mentioned both in the public and private sectors and it mediates the relationship between organisational culture and ISA (Wiley et al., 2020). At the individual level, cultural aspects like socio-cultural factors, cultural assumptions and beliefs, mother tongue, and religion impact ISA (Kruger et al., 2011; Marks and Rezgui, 2009). Thus, understanding and identifying the individual employee's cultural traits can impact employees' ISA positively.

Security education, training and awareness (SETA) programmes are one of the most effective factors that influence employees' ISA levels. Our findings reveal that SETA programs as a factor are appropriately considered in the public and private sectors (D'Arcy et al., 2009; Haeussinger and Kranz, 2013; Ahlan et al., 2015). They contribute substantially to developing employees' competence and ISA knowledge. One of the main goals of ISA is to increase ISP compliance. Therefore, ISP should be comprehensible, understandable and easily accessible, or else ISA efforts can be useless. This draws attention to accessible ISP as a factor that influences ISA (Haeussinger and Kranz 2013; Hwang et al., 2019).

There are ISA content development factors that influence ISA levels of employees only in the private sector. As more open offices have become common recently in the private sector, autonomy and shareability positively influence employees' ISA and behaviour in the co-working environment (Choi and Kim, 2015). Additionally, general IT-knowledge about the systems and applications that are used in daily business is a factor that influences ISA as more IT-knowledge means more awareness about IT security issues (Haeussinger, 2013). Work location is the only factor identified in the private sector. Companies in the private sector tend to allow employees to work remotely. This has an effect on ISA (Hadlington et al., 2019). This is not the case in the public sector as most of the job within this sector require employees to work within the organisations' offices. The visibility of the information security work and process in the organisation can impact the employees' willingness to comply with ISP. Thus, having a unit or information security department in the organisation positively influences employees' ISA. This factor has been identified in the private sector

(Flores and Ekstedt, 2015). Similarly, increasing the visibility of information security activities and processes impacts the employees' ISA in the public sector as well (Hwang et al., 2019; Steinbart et al., 2013).

There are some ISA content development methods that are common between the public and private sector organisations while others are different. The same case applies to the factors that influence employees' ISA. Even though ISA is relatively new in the field of IS research, there are a reasonable number of empirical studies done to date which specifically investigate ISA content development methods for enhancing employees' ISA level. However, in order to choose the right method, considering relevant factors that influence employees' ISA is critical. This is mainly because based on carefully identified factors, an appropriate method or a combination of methods can be chosen to build an effective ISA programme. An ISA programme that not only raises and increases knowledge and awareness but also changes behaviour and employees' attitude to ensure ISP compliance. Thus, preventing and minimising the risks of information security incidents.

6. Limitations of this study

In order to ensure that the review process is rigorous and valid, a systematic review process has been used to search the relevant literature. However, to assure the quality of the review, only the peer-reviewed empirical studies from reputed journals and conference proceedings have been used and other publications such as books, white papers and organisational reports, were excluded which otherwise would have provided more insights for this review. In addition, the list of search keywords was predefined and not formed inductively which may have limited the review to a certain extent. Some additional terms could have been used to conduct another literature search. For example, terms arose during the data analysis phase that could have been used as search-keywords again to find additional relevant literature for the review. We could have used different terms (e.g., computer abuse, information systems misuse) rather than "awareness" proposed by other scholars to conduct another literature search. In terms of content, physical security and intensively technically focused research, for example, the ISA program method developed through the use of honeypots (Christopher et al., 2017) was excluded. The review is within the scope of methods used in raising ISA and factors affecting it and does not cover the implementation and the evaluation element of ISA. The focus has been on providing up-to-date trends in ISA content development. Thus, studies conducted prior to 2009 were excluded from this study.

Although only empirical studies were used in the review, the sample sizes in some studies was relatively too small to generalise the results. For example, a few quantitative experiments have been conducted with a smaller sample size (of less than 20); therefore, we could not consider their findings to be valid unless further research is carried out and the result is just an indicative figure in the review. Moreover, a couple of studies were found to have based their results on single group studies which basically relied on online surveys and questionnaires, and not on control group studies. Thus, the results of such studies may be questionable as they did not compare between control groups and experimental groups but were rather based on surveys and interviews.

As reported in the method section, we have comprehensively covered our search process through Web of Science and Scopus, and saturated our search through Google Scholar. However, in the interest of time, we did not search through other databases which may contain relevant publications for our study that would have enhanced the validity and reliability of our findings. As it is an entirely qualitative study, the findings of this study are based on our own interpretation of the data collected from the selected publications.

7. Conclusion and further work

It is crucial for every organisation to understand how ISA content is developed and sustained in today's ever-increasingly connected world. Although ISA is relatively a new domain in the field of research, it can be concluded that there have been a good number of empirical studies investigating ISA content development over the past decade. This paper examines the ISA content development trends during the period between 2009 and March 2020. It provides a synthesised review of the ISA literature and thereby identifies and classifies ISA methods and factors in the organisational context of both the private and public sectors. Overall, the review findings have shown that the number of ISA content development publications in the private sector outnumbers the number of publications focusing on ISA content development in the public sector. In particular, our review finds that 1). The theory/framework/model and gamification have been proven to be common ISA methods in both the private sector and the public sector; 2). the applied ISA methods in the private sector tends to focus more on the individual level; 3). the PDCA cycle model has proved its efficiency in creating content for the ISA programmes in previous empirical studies; 4). management support, education training, culture, and ISP provision are the common factors for enhancing ISA in both the private sector and the public sector; 5) SETA programmes are identified as one of the most effective factors for enhancing individual employee's ISA in both the private sector and the public sector; 6). work location has been identified as one factor influencing employees' ISA only in the private sector.

The study is intended to help future researchers to gain insight into the latest trends in ISA content development methods and factors, and foster good ISA practice by disseminating information and knowledge amongst Information Security professionals to help them build an overarching ISA development programme in their respective organisations. The conducted review provides an overall picture and state-of-the-art overview of the widely dispersed knowledge of ISA methods and factors.

There are some opportunities for future research. Firstly, we could further explore the uncovered part of ISA which is to provide a systematic summary of the widely dispersed knowledge on the ISA evaluation methods to further strengthen the insights in this domain. Our study focuses on ISA content development both within the private as well as public organisational context and future research can cover context outside of the organisation, for example, there is an opportunity to explore an understudied group of 'remote employees' whose ISA level is found to be lower than their counterparts in organisations (Johnston et al., 2000). This context is deemed relevant with the ever-increasing use of the Internet-Of-Things by remote employees to access organisational networks and the BSI survey on information and cyber challenges in the public sector reveals that 40% of the respondents have not considered the security around the IoT, while another 40% said 'it is not required' (BSI - British Standards Institution 2018). Secondly, some additional terms (e.g., computer abuse, information systems misuse) could be used for another round of literature review to complement the findings in this study. Thirdly, empirical studies could be carried out to further verify the findings in this study.

Declaration of Competing Interest

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

CRediT authorship contribution statement

Khando Khando: Conceptualization, Methodology, Data curation, Formal analysis, Writing - original draft. **Shang Gao:** Supervision, Data curation, Formal analysis, Writing - original draft. **Sirajul M. Islam:** Supervision, Data curation, Formal analysis, Writing - original draft. **Ali Salman:** Conceptualization, Methodology, Data curation, Formal analysis, Writing - original draft.

REFERENCES

Abawajy J. User preference of cyber security awareness delivery methods. Behav. Inf. Technol. 2014;33(3):237–48.

Abraham S. Information Security Behavior: factors and Research Directions. Proceedings of the 17th Americas Conference on Information Systems (AMCIS), 2011.

Abrams, M., Weiss, J. (2008). Malicious control system cyber security attack case study–Maroochy Water Services, Australia. McLean, VA: The MITRE Corporation.

Ahlan AR, Lubis M, Lubis AR. Information security awareness at the knowledge-based institution: its antecedents and measures. Procedia Comput. Sci. 2015;72:361–73.

Albrechtsen E, Hovden J. Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. Comput. Secur. 2010;29(4):432–45.

Allam S, Flowerday SV, Flowerday E. Smartphone information security awareness: a victim of operational pressures. Comput. Secur. 2014;42:56–65.

Ameen M, Wätterstam T, Kowalski S. A prototype For HI 2 Ping information security culture and awareness training. In: 2012 International Conference on E-Learning and E-Technologies in Education (ICEEE). IEEE; 2012. p. 32–6.

Alshboul A. Information systems security measures and countermeasures: protecting organizational assets from malicious attacks. Commun. IBIMA 2010.

Amankwa E, Loock M, Kritzinger E. A conceptual analysis of information security education, information security training and information security awareness definitions. In: The 9th International Conference for Internet Technology and Secured Transactions. IEEE; 2014. p. 248–52 *(ICITST-2014)*.

Amankwa E, Marianne L, Elmarie K. In: 2015 S International Conference on Information Security and Cyber *Forensics (InfoSec)*. Enhancing information security education and awareness: proposed characteristics for a model. IEEE; 2015. 2015.

Anderson CL, Agarwal R. Practicing safe computing: a multimedia empirical examination of home computer user security behavioral intentions. MIS Q. 2010;34(3):613–43.

Annetta LA. The "I's" have it: a framework for serious educational game design. Rev. Gen. Psychol. 2010;14(2):105–13.

Bada, M., Sasse, A.M., Nurse, J.R. (2019). Cyber security awareness campaigns: why do they fail to change behaviour?. *arXiv preprint* arXiv:1901.02672.

Bauer S, Bernroider EW, Chudzikowski K. Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks. Comput. Secur. 2017;68:145–59.

Bawazir MA, Mahmud M, Molok NNA, Ibrahim J. Persuasive Technology for Improving Information Security Awareness and Behavior: literature Review. In: 2016 6th International Conference on Information and Communication Technology for The Muslim World (ICT4M). IEEE; 2016. p. 228–33.

Boujettif M, Wang Y. Constructivist approach to information security awareness in the Middle East. In: 2010 International Conference on Broadband, Wireless Computing, Communication and Applications. IEEE; 2010. p. 192–9.

BSI - British Standards Institution. (2018). Information and Cyber Challenges in the Public Sector Survey 2018. Retrieved 2020-05-04 from https://www.bsigroup.com/globalassets/localfiles/en-ie/csir/resources/whitepaper/uk-engb-survey-wp-challenges-public-sector-cloud.pdf

Budiningsih I, Soehari TD, Irwansyah I. The Dominant Factor For Improving Information Security Awareness. Jurnal Cakrawala Pendidikan 2019;38(3):490–8.

Bulgurcu B, Cavusoglu H, Benbasat I. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS Q. 2010;34(3):523–48.

Callanan C, Jerman-Blažič B, Blažič AJ. User awareness and tolerance of privacy abuse on mobile Internet: an exploratory study. Telematics Inform. 2016;33(1):109–28.

Choi KH, Lee D. A study on strengthening security awareness programs based on an RFID access control system for inside information leakage prevention. Multimed. Tools Appl. 2015;74(20):8927–37.

Choi M, Kim D. The Influence of the Co-Working Office Environment Characteristics on Information Security Awareness and Behavior. Acad. Entrepreneurship J. 2015;21(3):97.

Christopher L, Choo KK, Dehghantanha A. Honeypots for employee information security awareness and education training: a conceptual EASY training model. In: Contemporary Digital Forensic Investigations of Cloud and Mobile Applications. Syngress; 2017. p. 111–29.

Chua HN, Wong SF, Low YC, Chang Y. Impact of employees' demographic characteristics on the awareness and compliance of information security policy in organizations. Telematics Inform. 2018;35(6):1770–80.

Cone BD, Irvine CE, Thompson MF, Nguyen TD. A video game for cyber security training and awareness. Comput. Secur. 2007;26(1):63–72.

Dhillon, G. (2001). Violation of safeguards by trusted personnel and understanding related information security concerns. Comput. Secur. 20(2), 165-172.

D'Arcy J, Hovav A. Does one size fit all? Examining the differential effects of IS security countermeasures. J. Bus. Ethc. 2009;89(1):59–71.

D'Arcy J, Hovav A, Galletta D. User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. Inf. Syst. Res. 2009;20(1):79–98.

Da Veiga, A. (2015). An Information Security Training and Awareness Approach (ISTAAP) to Instil an Information Security-Positive Culture. In *HAISA* (pp. 95–107).

DeGroot III H, Weir R, Al-omari A, Gomes B. Intra-articular injection of hyaluronic acid is not superior to saline solution injection for ankle arthritis: a randomized, double-blind, placebo-controlled study. JBJS 2012;94(1):2–8.

Maeyer, D.D. (2007). Setting up an effective information security awareness programme. In *ISSE/SECURE 2007 Securing Electronic Business Processes* (pp. 49-58).

Dinev T, Goo J, Hu Q, Nam K. User behaviour towards protective information technologies: the role of national cultural differences. Inf. Syst. J. 2009;19(4):391–412.

El-Haddadeh, R., Tsohou, A., Karyda, M. (2012). Implementation challenges for information security awareness initiatives in e-government.

Eminağaoğlu, M., Uçar, E., Eren, Ş. (2009) The positive outcomes of information security awareness training in companies–A case study. *information security technical report* 14, no. 4 (2009): 223–229.

Ernst, Y., 2018, 2019. Global Information Security Survey, New York. Retrieved 2020-04-25 from https://assets.ey.com/content/dam/ey-sites/ey-com/en_ca/topics/advisory/ey-global-information-security-survey-2018-19.pdf

ENISA, (2008). A new Users' Guide: how to Raise Information Security Awareness. European Network and Information Security Agency.

ENISA, (2010). A new users' guide: how to raise information security awareness. European Network and Information Security Agency (ENISA). Retrieved 2020-05-11 from https://www.enisa.europa.eu/publications/archive/copy_of_new-users-guide.

ENISA. (2019). ENISA threat landscape report 2018: 15 Top Cyber-Threats and Trends. Heraklion: european Network and Information Security Agency (ENISA). doi:10.2824/622757.

Falagas ME, Pitsouni EI, Malietzis GA, Pappas G. Comparison of PubMed, Scopus, web of science, and Google scholar: strengths and weaknesses. FASEB J. 2008;22(2):338–42.

Fink A. Conducting Research Literature reviews: From the Internet to Paper. Thousand Oaks, Calif: Sage Publications; 2005.

Flores, W.R., Ekstedt, M. (2015). Exploring the Link Between Behavioural Information Security Governance and Employee Information Security Awareness. In *HAISA* (pp. 82–94).

Flores, W. R., & Ekstedt, M. (2016). Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. Comput. Secur. 59, 26-44.

Ghazvini A, Shukur Z. Awareness training transfer and information security content development for healthcare industry. Int. J. Adv. Comput. Sci. Appl. 2016;7(5):361–70.

Ghazvini A, Shukur Z. A Framework for an Effective Information Security Awareness Program in Healthcare. Int. J. Adv. Comput. Sci. Appl. (IJACSA) 2017a;8(2):193–205.

Ghazvini A, Shukur Z. Information security content development for awareness training programs in healthcare. Int. J. Secur. Appl. 2017b;11(7):87–96.

Ghazvini A, Shukur Z. A Serious Game for Healthcare Industry: information Security Awareness Training Program for Hospital Universiti Kebangsaan Malaysia. Int. J. Adv. Comput. Sci. Appl. 2018;9(9):236–45.

Gjertsen, E.G.B., Gjære, E.A., Bartnes, M., Flores, W.R. (2017). Gamification of Information Security Awareness and Training. In *ICISSP* (pp. 59–70).

Gundu T, Flowerday SV. Ignorance to awareness: towards an information security awareness process. SAIEE Africa Res. J. 2013;104(2):69–79.

Hadasch, F., Mueller, B., Maedche, A. (2012). Exploring Antecedent Environmental and Organizational Factors to User-Caused Information Leaks: a Qualitative Study.

Hadlington L, Popovac M, Janicke H, Yevseyeva I, Jones K. Exploring the role of work identity and work locus of control in information security awareness. Comput. Secur. 2019;81:41–8.

Haeussinger, F., Kranz, J. (2013). Information security awareness: its antecedents and mediating effects on security compliant behavior.

Haeussinger, F., Kranz, J. (2017). Antecedents of employees information security awareness-review, synthesis, and directions for future research.

Haeussinger, F. (2013). Understanding the Antecedents of Information Security Awareness-An Empirical Study.

Henderson VC, Kimmelman J, Fergusson D, Grimshaw JM, Hackam DG. Threats to validity in the design and conduct of preclinical efficacy studies: a systematic review of guidelines for in vivo animal experiments. PLoS Med. 2013;10(7).

Herath T, Rao HR. Encouraging information security behaviors in organizations: role of penalties, pressures and perceived effectiveness. Decis. Support Syst. 2009;47(2):154–65.

Hovav A, D'Arcy J. Applying an extended model of deterrence across cultures: an investigation of information systems misuse in the US and South Korea. Inf. Manage. 2012;49(2):99–110.

Hu Q, Dinev T, Hart P, Cooke D. Managing employee compliance with information security policies: the critical role of top management and organizational culture. Decis. Sci. 2012;43(4):615–60.

Humaidi, N., Balakrishnan, V. (2015). Leadership styles and information security compliance behavior: the mediator effect of information security awareness. *International Journal of Information and Education Technology*

Hwang I, Kim D. The effect of organizational information security environment on the compliance intention of employee. J. Inf. Syst. 2016;25(2):51–77.

Hwang I, Wakefield R, Kim S, Kim T. Security Awareness: the First Step in Information Security Compliance Behavior. J. Comput. Inf. Syst. 2019:1–12.

Imgraben J, Engelbrecht A, Choo KKR. Always connected, but are smart mobile users getting more security savvy? A survey of smart mobile device users. Behav. Inf. Technol. 2014;33(12):1347–60.

Industry, P.C. Security Standards Council (2014). Best Practices for implementing a Security Awareness Program. PCI DSS. Retrieved 2020-04-04 from https://www.pcisecuritystandards.org/documents/PCI_DSS_V1.0_Best_Practices_for_Implementing_Security_Awareness_Program.pdf.

Ingham, L. (2018). 88% of UK data breaches caused by human error, not cyberattacks. The Verdict Magazine. https://www.verdict.co.uk/uk-data-breaches-human-error/.

International Organization for Standardization (ISO). (2013). ISO/IEC 27001: 2013: Information Technology–Security Techniques–Information Security Management Systems–Requirements. International Organization for Standardization.

Jaeger L. Information security awareness: literature review and integrative framework. Proceedings of the 51st Hawaii International Conference on System Sciences, 2018.

Johnston AC, Warkentin M, McBride M, Carter L. Dispositional and situational factors: influences on information security policy violations. Eur. J. Inf. Syst. 2016;25(3):231–51.

Johnston AC, Wech B, Jack E. Engaging remote employees: the moderating role of “remote” status in determining employee information security policy awareness. J. Org. End User Comput. (JOEUC) 2000;25(1):1–23.

Kajzer M, D’Arcy J, Crowell CR, Striegel A, Van Bruggen D. An exploratory investigation of message-person congruence in information security awareness campaigns. Comput. Secur. 2014;43:64–76.

Khan B, Alghathbar KS, Nabi SI, Khan MK. Effectiveness of information security awareness methods based on psychological theories. African J. Bus. Manage. 2011;5(26):10862.

Ki-Aries D, Faily S. Persona-centred information security awareness. Comput. Secur. 2017;70:663–74.

Kruger HA, Drevin L, Flowerday S, Steyn T. An assessment of the role of cultural factors in information security awareness. 2011 Information Security for South Africa 2011:1–7 IEEE.

Kusumawati A. Information Security Awareness: study on a Government Agency. In: 2018 International Conference on Sustainable Information Engineering and Technology (SIET). IEEE; 2018. p. 224–9.

Lebek B, Uffen J, Breitner MH, Neumann M, Hohler B. Employees’ information security awareness and behavior: a literature review. In: 2013 46th Hawaii International Conference on System Sciences. IEEE; 2013. p. 2978–87.

Lim, J.S., Ahmad, A., Chang, S., Maynard, S.B. (2010). Embedding Information Security Culture Emerging Concerns and Challenges. In *PACIS 2010* (p. 43).

Lindberg, D. (2016). Gamified systems for security awareness: a literature analysis.

Mani D, Mubarak S, Choo KKR. Understanding the information security awareness process in real estate organizations using the SECI model. In: 20th Americas Conference on Information Systems; 2014. p. 7–10 *(AMCIS 2014)*.

Marks A, Rezgui Y. A comparative study of information security awareness in higher education based on the concept of design theorizing. In: 2009 International Conference on Management and Service Science. IEEE; 2009. p. 1–7.

Morgan, S. (2016). Cybersecurity business report. Retrieved 2020-05-04 from https://www.csoonline.com/article/3110467/cybercrime-damages-expected-to-cost-the-world-6-trillion-by-2021.html.

Myyry L, Siponen M, Pahnila S, Vartiainen T, Vance A. What levels of moral reasoning and values explain adherence to information security rules? An empirical study. Eur. J. Inf. Syst. 2009;18(2):126–39.

Okoli, C., Schabram, K. (2010). A guide to conducting a systematic literature review of information systems research. Retrieved 2020-02-26 from https://www.researchgate.net/publication/228276975_A_Guide_to_Conducting_a_Systematic_Literature_Review_of_Information_Systems_Research.

Ponemon Institute Report (2017). 2017 Cost of Data Breach Study Global Overview. Retrieved 2020-05-04 from https://www.ibm.com/downloads/cas/ZYKLN2E3.

Parker, D.B. (1976, June). Computer abuse perpetrators and vulnerabilities of computer systems. In *Proceedings of the June 7-10, 1976, national computer conference and exposition*.

Parsons K, McCormac A, Butavicius M, Pattinson M, Jerram C. Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). Comput. Secur. 2014a;42:165–76.

Parsons K, McCormac A, Butavicius M, Pattinson M, Butavicius M, Jerram C. A study of information security awareness in Australian government organisations.. Inf. Manage. Comput. Secur. 2014b;22(4):334–45. doi:10.1108/IMCS-10-2013-0078.

Pattinson, M., Parsons, K., Butavicius, M., McCormac, A., Calic, D. (2016). Assessing information security attitudes: a comparison of two studies. *Information & Computer Security*.

Poepjes, R., Lane, M. (2012). An information security awareness capability model (ISACM). Retrieved 2020-04-09 from https://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1136&context=ism.

Power R, Forte D. Case Study: a bold new approach to awareness and education, and how it met an ignoble fate. Comput. Fraud Secur. 2006(5):7–10 2006.

Puhakainen P, Siponen M. Improving employees’ compliance through information systems security training: an action research study. MIS quarterly 2010:757–78.

Mejias RJ. An Integrative Model of Information Security Awareness for Assessing Information Systems Security Risk. In: 45th Hawaii International Conference on System Sciences. Maui; 2012. p. 3258–67 2012 pp.

Samuel GO, Hoffmann S, Wright RA, Lalu MM, Patlewicz G, Becker RA, DeGeorge GL, Fergusson D, Hartung T, Lewis RJ, Martin Stephens ML. Guidance on assessing the methodological and reporting quality of toxicologically relevant studies: a scoping review. Environ. Int. 2016;92:630–46.

SANS, 2020, Security Awareness. (n.d). Security awareness – How to communicate. Retrieved 2020-05-25 from https://www.sans.org/security-awareness-training/blog/security-awareness-how-communicate.

Saraçlı S, Erdoğmuş A. Determining the effects of information security knowledge on information security awareness via structural equation modelings. Hacettepe J. Math. Stat. 2019;48(4):1201–12.

Scholl, M.C., Fuhrmann, F., Scholl, L.R. (2018). Scientific Knowledge of the Human Side of Information Security as a Basis for Sustainable Trainings in Organizational Practices.

Scholl MC. Raising Information Security Awareness in the Field of Urban and Regional Planning. Int. J. E-Planning Res. (IJEPR) 2019;8(3):62–86.

Serfontein R, Drevin L, Kruger H. The feasibility of raising information security awareness in an academic environment using SNA. In: IFIP World Conference on Information Security Education. Springer; 2018. p. 69–80.

Shaw RS, Chen CC, Harris AL, Huang HJ. The impact of information richness on information security awareness training effectiveness. Comput. Educ. 2009;52(1):92–100.

Singh AN, Picot A, Kranz J, Gupta MP, Ojha A. Information security management (ism) practices: lessons from select cases from India and Germany. Global J. Flexible Syst. Manage. 2013;14(4):225–39.

Stahl BC, Doherty NF, Shaw M. Information security policies in the UK healthcare sector: a critical evaluation. Infor. Syst. Jour. 2012;22(1):77–94.

Siponen, M., Mahmood, M. A., & Pahnila, S. (2009). Technical opinion Are employees putting your company at risk by not following information security policies? Communications of the ACM, 52(12), 145-147.

Siponen M, Vance A. Neutralization: new insights into the problem of employee information systems security policy violations. MIS Quarterly 2010:487–502.

Siponen, M.T. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*.

Siponen MT. Five dimensions of information security awareness. SIGCAS Comput. Soc. 2001;31(2):24–9.

Solic K, Velki T, Galba T. Empirical study on ICT system’s users’ risky behavior and security awareness. In: 2015 38th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO). IEEE; 2015. p. 1356–9.

Spears JL, Barki H. User participation in information systems security risk management. MIS Q. 2010;34(3):503–22.

Steinbart PJ, Raschke RL, Gal G, Dilla WN. Information security professionals' perceptions about the relationship between the information security and internal audit functions. J. Inf. Syst. 2013;27(2):65–86.

Stewart G, Lacey D. Death by a thousand facts: criticising the technocratic approach to information security awareness. Inf. Manage. Comput. Secur. 2012;20(1):29–38.

Straub Jr DW. Effective IS security: an empirical study. Inf. Syst. Res. 1990.

Talib S, Clarke NL, Furnell SM. An analysis of information security awareness within home and work environments. In: 2010 International Conference on Availability, Reliability and Security. IEEE; 2010. p. 196–203.

Tarmizi A, Hapsari IC, Hidayanto AN, LY AY. Information Security Awareness National Nuclear Energy Agency of Indonesia (BATAN). In: 2018 International Conference on Computing, Engineering, and Design (ICCED). IEEE; 2018. p. 35–9.

Tassabehji, R., Elliman, T., Mellor, J. (2007). Generating citizen trust in e-government security: challenging perceptions. *International Journal of Cases on Electronic Commerce (IJCEC)*, *3*(3).

Tsohou A, Karyda M, Kokolakis S, Kiountouzis E. Analyzing information security awareness through networks of association. In: International Conference on Trust, Privacy and Security in Digital Business. Springer; 2010. p. 227–37.

Tsohou A, Karyda M, Kokolakis S, Kiountouzis E. Analyzing trajectories of information security awareness. Inf. Technol. People 2012.

Tsohou A, Karyda M, Kokolakis S, Kiountouzis E. Managing the introduction of information security awareness programmes in organisations. Eur. J. Inf. Syst. 2015;24(1):38–58.

Tu, Z., Yuan, Y. (2014). Critical success factors analysis on effective information security management: a literature review.

Vaidya, R. (2019). Cyber Security Breaches Survey, 2019. Retrieved 2020-05-04 from https://drj.com/wp-content/uploads/2019/04/Cyber_Security_Breaches_Survey_2019_-_Main_Report.PDF.

Valentine JA. Enhancing the employee security awareness model. Comput. Fraud Secur. 2006(6):17–19 2006.

Van Niekerk JF, Von Solms R. Information security culture: a management perspective. Comput. Secur. 2010;29(4):476–86.

Waly N, Tassabehji R, Kamala M. In: 2012 IEEE 14th International Conference on High Performance Computing and Communication & 2012 IEEE 9th International Conference on Embedded Software and Systems. Improving organisational information security management: the impact of training and awareness; 2012.

Webster J, Watson R. Analyzing the Past to Prepare for the Future: writing a Literature Review. MIS Q. 2002;26(2) Xiii-Xxiii. Retrieved 2020-04-04 from www.jstor.org/stable/4132319.

Wiley A, McCormac A, Calic D. More than the individual: examining the relationship between culture and Information Security Awareness. Comput. Secur. 2020;88.

Wilson M, Hash J. Building an information technology security awareness and training program. NIST Spec. Publ. 2003;800(50):1–39.

Khando Khando obtained his M.Sc. in Information Security Management in 2020 from Örebro University, Sweden. His-research interest includes information security awareness.

Shang Gao is an Associate Professor of Informatics at Örebro University, Sweden. He obtained his Ph.D. in Information Systems in 2011 from Norwegian University of Science and Technology, Norway. His-research interests include mobile information systems, technology diffusion, information security management, information systems modelling, and requirement engineering. He has published more than 70 refereed papers in journals, books and archival proceedings since 2006.

M. Sirajul Islam is an Associate Professor in information systems at the Informatics unit of Örebro University School of Business, Sweden. Siraj is specialized in teaching and research in the areas of e-government, information and communications technology for development (ICT4D), and education with a special interest in marginalized communities in developing regions. He is teaching both at the bachelor and master levels. He has also been involved with some journal editorial/review committees and international conferences relevant to ICT4D and e-government.

Ali Salman obtained his M.Sc. in Information Security Management in 2020 from Örebro University, Sweden. His-research interest includes information security awareness.