Computer Science Review 50 (2023) 100592

Contents lists available at ScienceDirect

Computer Science Review

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

Review article

A quest for research and knowledge gaps in cybersecurity awareness for small and medium-sized enterprises[☆]

Sunil Chaudhary [a,*], Vasileios Gkioulos [b], Sokratis Katsikas [b]

[a] European Centre on Privacy and Cybersecurity (ECPC), Faculty of Law, Maastricht University, Bouillonstraat 3, 6211 LH Maastricht, The Netherlands
[b] Department of Information Security and Communication Technology, Norwegian University of Science and Technology, Teknologivegen 22, 2815, Gjøvik, Norway

ARTICLE INFO

Article history:
Received 25 December 2020
Received in revised form 8 April 2023
Accepted 22 August 2023
Available online xxxx

Keywords:
Cybersecurity awareness
Small and medium-sized enterprises
Systematic literature review
Research and knowledge gaps

ABSTRACT

The proliferation of information and communication technologies in enterprises enables them to develop new business models and enhance their operational and commercial activities. Nevertheless, this practice also introduces new cybersecurity risks and vulnerabilities. This may not be an issue for large organizations with the resources and mature cybersecurity programs in place; the situation with small and medium-sized enterprises (SMEs) is different since they often lack the resources, expertise, and incentives to prioritize cybersecurity. In such cases, cybersecurity awareness can be a critical component of cyberdefense. However, research studies dealing with cybersecurity awareness or related domains exclusively for SMEs are rare, indicating a pressing need for research addressing the cybersecurity awareness requirements of SMEs.

Prior to that, though, it is crucial to identify which aspects of cybersecurity awareness require further research in order to adapt or conform to the needs of SMEs. In this study, we conducted a systematic literature review that focused on cybersecurity awareness, prioritizing those performed with a particular focus on SMEs. The study seeks to analyze and evaluate such studies primarily to determine knowledge and research gaps in the cybersecurity awareness field for SMEs, thus providing a direction for future research.

Contents

[☆] This work was financially supported by the CyberSec4Europe, Belgium project (Proposal No. 830929). This paper is an extended and revised version of the deliverable report D9.6 SME cybersecurity awareness program 1 [1] from CyberSec4Europe's WP9: Dissemination, Outreach, Spreading of Competence, Raising Awareness.

[*] Corresponding author.
E-mail address: sunil.chaudhary@maastrichtuniversity.nl (S. Chaudhary).

https://doi.org/10.1016/j.cosrev.2023.100592

1. Introduction

The European Commission [2] has categorized enterprises into medium-, small-, and micro-sized according to the following two main criteria: (i) the staff headcount, and (ii) the annual turnover or balance sheet total. A medium-sized enterprise has less than 250 employees and an annual turnover of no more than €50 million, or a balance sheet total of no more than €43 million. Similarly, a small enterprise has less than 50 employees and at most €10 million in turnover or balance sheet total, and finally, a micro-enterprise has less than 10 employees and at most €2 million in turnover or balance sheet total. Based on these definitions, around 99% of the enterprises in the European Union (EU) represent small and medium-sized enterprises (SMEs), i.e., approximately 25.1 million SMEs in 2018 [3]. SMEs are an essential component of Europe's economic growth, innovation, job creation, and social integration [4]. This could be a reason why the EU promotes SME development by simplifying the regulatory and policy environment and facilitating various critical business development activities, such as access to new markets and internationalization, finance, key support networks, and others.

In general, SMEs are characterized by their limited resources, informal management style with multitasking employees, dependence on an individual decision-maker (i.e., usually the business owner), and low adherence to the established procedures and standards [5]. Despite these challenges, SMEs are evolving steadily, with some at the productivity frontier and among the most innovative enterprises, such as start-ups, which have emerged as key sources of radical and disruptive innovations [6]. They are more adaptable to new technologies or commercial opportunities compared to their large counterparts. Many of these SMEs make extensive use of information and communication technology (ICT) systems and online services, such as staff email addresses, company websites, online banking, and others. They use, produce, and store large amounts of sensitive data and heavily rely on cloud-based platforms and services [7] for their everyday operations. Indeed, the adoption of ICT systems and online services has offered significant opportunities to these enterprises; more importantly, it has improved their operational efficiency and broadened their business horizons. This, however, also introduces many cybersecurity challenges and exposes them to continuously evolving cybersecurity threats. It has been found that enterprises that hold personal data, use cloud-based platforms and services, and whose staff use personal devices for work (i.e., bring your own device) encounter security breaches more frequently [8].

While advanced cyberattacks typically target large enterprises with strategic resources, cybercrimes also pose threats to SMEs [9]. Nevertheless, this pattern is rapidly changing, and SMEs are now subject to the same cybersecurity threats as their large counterparts [7]. Studies have shown that SMEs are hardest hit by cyber breaches, although they may not make the headlines [10]. Over the years, cybercrimes and attacks targeting SMEs have steadily increased, and to make matters worse, many SMEs do not see them as a problem [11]. Even among them, SMEs that have direct or indirect relationships with large organizations become more vulnerable to security breaches, mainly because attackers ultimately plan to reach large organizations by using the smaller organization as a gateway [11,12]. More importantly, due to their budgetary constraints, a cyberattack is a more serious concern for small and micro enterprises, which are less likely to recover from it [12].

SMEs often plan their cybersecurity defenses inappropriately, either by underestimating the risks and consequences of cyberattacks or by not being able to keep pace with ever-evolving cybersecurity challenges. Several studies have revealed that the majority of SMEs do not apply adequate security defenses [11,13,14] for continuous monitoring and analytics (i.e., prevention, detection, and response) of cyber vulnerabilities and threats. Furthermore, they generally lack the ability to comply with regulatory standards, for example, the General Data Protection Regulation [15] and others, which have been designed to improve organizational cybersecurity practices and culture. Compounding the problem, there is a mindset among SME executives and senior managers that cyberattacks prefer high-profile organizations and not SMEs, so cybersecurity is less critical to them [7,10,16]. Even when dealing with cybersecurity issues, SMEs only consider the immediate future scope and focus on provable threats, focusing on costless mitigations [17]. These all make them an ideal and common target for cyberattacks, requiring minimal effort to launch but with a substantial cumulative payoff.

Most businesses today, including SMEs, agree that cyberattacks and cybercrimes are imminent threats that need to be addressed immediately. Their actions and behavior, however, do not reflect that; many of them neglect cybersecurity until they are directly impacted by an incident. Yet, they start to take an interest in the matter when a cyber-breach occurs and the consequences become evident. The problem with this reactive approach is that, if recovery is even conceivable, it necessitates a significant investment of effort and resources [18]. Hence, it is the responsibility of every enterprise to comprehend the effects of cyberattacks, maintain the online safety of its employees, clients, and stakeholders, and act proactively or on time to do that. While doing that, it is important to keep in mind that even a single vulnerability could leave the entire enterprise open to attacks.

Countering a cyberattack demands multiple layers of security measures that comprise both technological measures and consideration of human factors of security. Unquestionably, technological measures are crucial for every enterprise, but it has also been widely acknowledged that cybersecurity is not solely a technological problem but also a socio-technical one. This has been evident in several security breaches brought on by human error and negligence. For instance, a recent study found that human error alone was to blame for 60% of personal data breaches [19]. This is further corroborated by the results of a 2017 Ponemon Institute study of SMEs, in which 54% of the participants claimed that negligent employees were to blame for data breaches in their organizations [20]. Employees make security errors maybe because they are not naturally equipped with the skills, instincts, and behavior required to assure proper protection, necessitating more cybersecurity awareness (CSA) programs to comprehend what they should do and learn how to do it [21]. Similarly, negligence may result from employees' ignorance of the risks and their failure to know and understand the 'correct' security behavior [22]. On top of that, social engineering has been a factor in virtually all cyberattacks [23], which, unfortunately, cannot be remedied exclusively by technology. The technological measures will have limited effect if the people using them do not understand their security responsibilities or are susceptible to psychological manipulation by social engineering techniques. After all, it makes no difference how many layers of sophisticated security measures an enterprise has implemented if its employees misuse them, deliberately bypass them due to negligence and recklessness, or continue to be cognitively biased.

In this circumstance, CSA can become a reasonable and critical countermeasure in the fight against cyberattacks. Enterprises can organize CSA programs regularly to keep their employees up to date on the latest cybersecurity threats and technologies, as well as organizational policies and procedures that are pertinent to their job function. Raising the CSA level of employees will encourage them to adopt secure attitudes and behavior, as well as promote a sense of responsibility for cybersecurity among employees. Employees aware of cybersecurity in their area of work, which includes but is not limited to understanding the potential risks they may encounter, their cybersecurity responsibilities, and the organizational security policies and procedures, have a high chance of making informed security decisions and acting accordingly. Moreover, these informed and aware employees will presumably lessen human errors, negligence, and vulnerabilities due to human factors, enhancing the organization's overall cybersecurity posture. As a result, the primary goal of this study is to examine CSA explicitly while concentrating on the needs and constraints of SMEs. We utilized a systematic literature review to accomplish that.

Initially, we provide a brief overview of CSA, focusing on its definition and basic taxonomy. This is followed by a detailed description of the research methodology and objectives of this research work. Next, a discussion of selected related works was presented. After that, articles on the CSA and its related aspects, as well as the problems they address, are scrutinized. Consequently, we present a similar analysis for articles that focused on SMEs within and outside the EU to complement the presented findings and support their comparative analysis. Finally, we present a synthesis of results and discussion across the major findings, while also outlining future research directions.

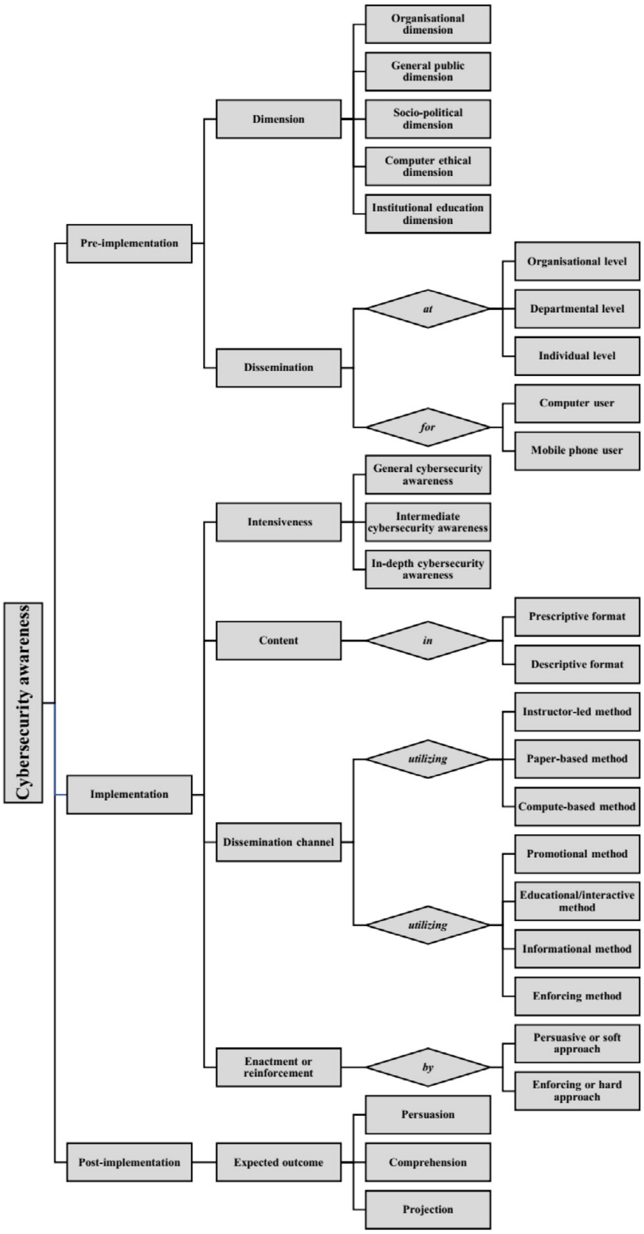

Fig. 1. Taxonomy of cybersecurity awareness.

2. Overview of cybersecurity awareness

We believe that a consistent definition and coherent understanding of the CSA are essential for its investigation. Similar to the Hanus et al. [24] study, we observed a level of inconsistency in the definition of CSA. Several past studies have shaped the meaning and definition of CSA in accordance with their understanding, knowledge, and needs by emphasizing one or multiple determinants of security-related behaviors [24]. Even worse, there exists a common misunderstanding among some past studies that have interchangeably used CSA for security education and training. Indeed, security education and training contribute to raising the CSA level [25], but they differ significantly from one another (see [26–29]). Such inconsistency in the definition and understanding of CSA may be due to its non-technical nature and a dependency on unspecified boundaries to distinguish it from cybersecurity education and training.

In general, CSA is used to communicate or disseminate security requirements and appropriate behavior to people [22] so that they have a level of skepticism when encountering situations that are unorthodox or out of the ordinary [21]. It does not equal in-depth knowledge but is aimed at directing the attention of individuals to a security issue or set of issues, realizing their potential implications, and acting accordingly [26]. It is delivered through a variety of channels, generally using a less formal, less intensive, and shorter session compared to security training and education [30]. Its activities are usually directed at broad audiences, who are mostly passive recipients of the information. The learning achieved from CSA is short-term, immediate, and specific unless the activities are repeatedly exercised [31]. A basic taxonomy of CSA is given in Fig. 1.

Nonetheless, even within the CSA for enterprises, its intensity and depth vary depending on the complexity of the security risk the audience is expected to encounter. An organization could need CSA for its diversified user groups, for example, top management, information technology (IT) and information systems (IS) management, information security staff, computing and IS professionals, end-users of various kinds (e.g., casual end-users, parametric end-users, sophisticated end-users, and stand-alone users), and third parties [18]. Accordingly, there can be a general or introductory awareness of the general security practices, for example, password policies, malware protection, data backup and recovery, email and Internet use, etc., that apply to all users within the organization. On the contrary, management and personnel with specialized roles may require more comprehensive awareness of contents specific to their roles and responsibilities; for example, the Human Resources (HR) department must notify the IT department when an employee has left their employment to revoke all his or her rights [32]. A more formal categorization of security awareness depending on its intensity can be general CSA (i.e., suitable for all personnel), intermediate CSA (i.e., suitable for management, decision-makers, and some specialized roles), and in-depth CSA (i.e., suitable for specialized roles and some management) [28].

As IT has been embedded in every aspect of modern life, so has the need for and concern for CSA among everyone using IT services. Based on this assertion, CSA can be categorized into the following five dimensions: organizational dimension, general public dimension, socio-political dimension, computer ethical dimension, and institutional education dimension (refer to [18]). Because of the informal nature of the CSA, however, there may not be a clear or distinct border between these dimensions in every case. This also implies that CSA for SMEs could involve other dimensions in addition to the organizational dimension.

In an organization, the audience can be addressed or targeted at various levels. For example, general CSA can be targeted at the organizational level; awareness needs specific to a particular department can be conducted at the departmental level; and finally, high-level executives and managers responsible for managing other users may need awareness at the individual level [28]. However, if the audience group is homogeneous, for example, in the case of small and micro enterprises where there may not exist a clear demarcation of an employee's role and responsibility, then conducting CSA at the organizational level will help to minimize its complexity [30] and presumably cost. Another classification could be CSA for computer users (i.e., target desktop and laptop users) and CSA for mobile phone users (i.e., target smartphone users). Both computers and mobile phones are widely used to access the Internet and perform organizational activities; however, they differ in their usability, situation awareness, mobility [33], layers of protection [34], and users' security-related perceptions and behavior [35].

The reinforcement or enactment of CSA learning is performed generally through these two approaches: the persuasive or soft approach (i.e., persuade the users to comply through motivations or rewards) or the enforcing or hard approach (i.e., compel the users to comply through threats of sanctions) [36]. In general, it is often recommended to apply a soft approach for long-term behavioral change in the CSA [36–38]. However, there exists a contrary belief that advocates for the hard approach in the CSA [39]. It is based on the rationale that, although the soft approach improves persuasion, introducing a level of fear into CSA will make people care about compliance.

On the Internet, a broad range of CSA resources are available for purchase or free download [40]. Their content can be in the prescriptive format (i.e., action-guiding commitment) or the descriptive format (i.e., providing some level of knowledge of security) [18]. In the organizational dimension, prescriptiveness is preferred, maybe because there is a degree of homogeneity in its users and activity types. In contrast, other dimensions deal with heterogeneous users and activity types. Thus, it is relatively difficult to achieve prescriptiveness in them. Moreover, having prescriptiveness in other dimensions may raise an ethical concern about indoctrination.

Next, the channel used for the dissemination of CSA contents could be instructor-led (i.e., people listen to the instructor talk in real-time, and this is generally suitable for a small and limited group of audience, e.g., workshops and training), paper-based (i.e., a traditional method used to reach a large mass of audience at the organizational level, e.g., leaflets, newsletters, posters, and pamphlets), or computer-based (i.e., a convenient way to deliver to a large or widely distributed group of people, e.g., website posting, video, games, and quizzes) [41,42]. They can also be classified as promotional (e.g., events, posters, games), educational/interactive (e.g., presentations, brief sessions, workshops), informational (e.g., leaflets, newsletters, website postings, e-mails), or enforcing (e.g., confidentiality agreements, required awareness exams or tests) [43]. Each channel has its benefits, and different users can have different preferences for CSA delivery channels [30,44], so it is recommended to use multiple channels [45] to make the CSA suitable for diversified users and expose them to the same information multiple times in different ways.

Finally, the choice of CSA materials varies depending on the needs of the organization, its target group, and most importantly, the expected outcomes, which are perception (i.e., the ability to sense and detect potential security risks), comprehension (i.e., the ability to comprehend, understand, and assess the dangers posed by different threats, integrate information from multiple sources, and interpret them in the right direction), and projection (i.e., the ability to project or predict the future course of security attacks to prevent potential risks from occurring) [46]. The information richness [47] of the medium selected for CSA dissemination determines the expected outcome and is thus critical for the CSA's overall success [46].

3. Research methodology: Systematic literature review

A systematic literature review is particularly suitable in two situations: (i) to deal with a mature topic where an accumulated body of research exists that needs analysis and synthesis, and (ii) to tackle an emerging issue that would benefit from exposure to potential theoretical foundations [48]. In the case of this study, even though CSA has been a mature topic, at least from the perspective of accumulated literature, only a few of the studies exclusively deal with CSA for SMEs. We utilized mainly the method described by Okoli & Schabram [49] for conducting a systematic literature review of information systems research for this research purpose. The method consists of multiple steps, as shown in Fig. 2 (refer to [49]).

SMEs depend primarily on CSA designs that are produced for contexts other than their own. However, relevant studies and tools are available in an extensive range and volume, and selecting the most suitable one from them is a difficult and resource-taxing process [22,50]. Moreover, for a researcher, it is unclear which aspects of the CSA fit SMEs' needs and which require further investigation to make them appropriate for SMEs. Therefore, this study analyzes the past studies concerning the current state of the CSA and mechanisms employed for its enhancement, with a focus on SMEs, in order to determine knowledge and research gaps in the CSA. Complementary to this, we seek to investigate trends, research tracks, and methodologies used in CSA research, and finally to make recommendations for future research.

Accordingly, the executed tasks seek to satisfy the following explicit goals:

i. To analyze and evaluate the research papers published on CSA and related topics and those directed towards SMEs, and to synthesize the detailed research results in terms of:

   a. Which technologies, areas of focus, aspects, and concerns have been specifically addressed by CSA studies focusing on SMEs in the past?
   b. Which research methodologies have they found to be most effective for their studies?

ii. To make recommendations on CSA that required further research to make it appropriate for SME purposes.

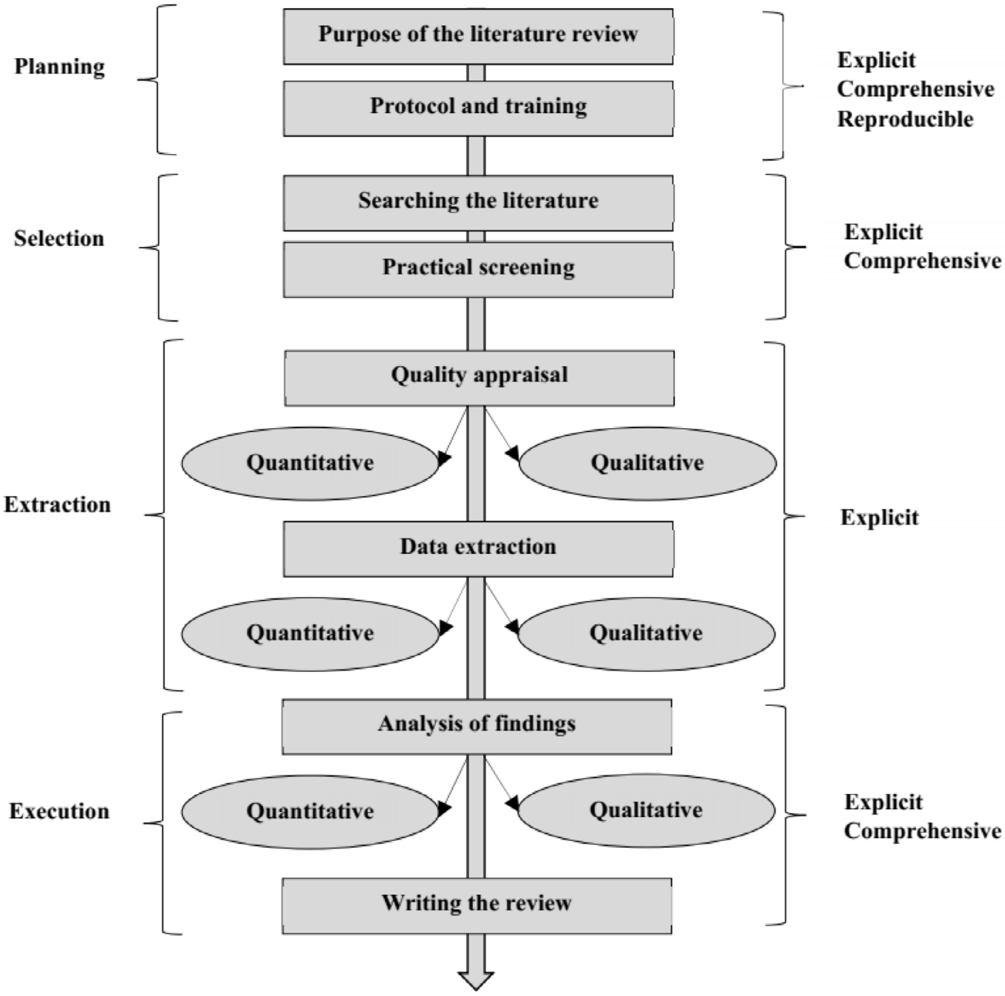

Fig. 2. A systematic guide to literature review development [49].

Collecting relevant literature that captures the essence of these research objectives is of paramount importance in a systematic literature review. It plays a significant role in augmenting the researchers' knowledge and advancing the ultimate outcomes of the study [48]. In order to determine such published works of literature, the reviewers have to be clear on the following fundamental aspects: where and how to locate the relevant literature and their selection criteria [48,51]. The sources of selected literature should be those with a reputation for quality. Since justifying the quality of any individual work may be difficult and controversial, for this study, we have selected the following academic research databases: IEEE Xplore, ACM Digital Library, ScienceDirect, and Scopus.

The identification and extraction of related literature were finalized on January 15, 2020. This process was executed by the explicit combination of three keyword groups, namely:

- security + awareness + SME,
- security + awareness + "small and medium-sized enterprises" and
- security + awareness

Where '+' represents a logical 'AND'.

We established a number of inclusion and exclusion criteria for the main review's paper selection, as follows:

- Articles published in languages other than English were excluded.
- Except for the first copy found, duplicate articles that appeared across the examined scientific databases were excluded.
- Reports, presentations, editorials, and posters were excluded.
- Articles that studied topics related to CSA with various types of users, including SMEs, were excluded since their results do not solely represent SMEs but are influenced by other users as well.
- Even those articles that did not mention the type of organization where the study was conducted were excluded from the main review; however, the suggestions made by them that we believed could be equally useful and relevant for SMEs have been used to enhance our analysis and scrutiny.
- Articles included are directly related to CSA studies, results, or tools directed toward SMEs.

However, no exclusion criteria were defined following the year of publication, publisher, or author affiliation. We believe that these three keyword groups are adequate to retrieve the relevant literature. The earlier two keyword groups were used for collecting CSA papers that particularly focus on SMEs, while the last keyword group was used as a precaution to collect all the papers that deal with CSA so that we can cross-check and verify that any relevant literature is not missed. After making queries to the databases, we were able to download 248 papers. This is when we conducted the first level of screening and downloaded only those papers that had the query keyword groups in their title, keywords, or abstract.

Among the screened papers, 13 from European SMEs and 7 from non-European SMEs met the inclusion criteria. These 20 papers have been mainly examined and reviewed in our study. Additionally, we also reviewed 88 papers that deal with CSA and its related domains in general to acquire a broader perspective on CSA. It is important to highlight that the other papers being considered do not cover CSA for SMEs in particular; instead, they concentrate on topics related to it, such as cybersecurity culture or management in SMEs. These are pertinent to include, mainly because CSA is closely related to an organization's cybersecurity culture and management processes [52].

4. Related works

There are not many research studies that exclusively focus on CSA or related topics for SMEs, and among them, those that deal with SMEs based within the EU are extremely rare. Nonetheless, there are several studies focusing on CSA and its related topics in general that use a systematic literature review as their primary or secondary research method.

Lebek et al. [53] conducted a systematic literature review to identify the behavioral theories that have widely been implemented to study human behavior for CSA purposes, and their study resulted in the following four theories: theory of reasoned action (TRA) or theory of planned behavior (TPB), general deterrence theory (GDT), protection motivation theory (PMT), and technology acceptance model (TAM). Utilizing the earlier study as the foundation, Mayer et al. [54] performed a systematic literature review to determine the behavioral factors that exhibit reliable effects in the context of information security. They collected behavioral factors used by the behavioral theories that are most frequently studied in the context of information security and then used effect size to measure the effect of those behavioral factors on information security. They identified only two factors, "attitude" and "perceived usefulness", that exhibit a reliable association with secure IS-related behavior.

Another similar study is by Aldawood & Skinner [55], which used a literature review to identify various social engineering threats. Their findings revealed a security budget deficit to be the major challenge in providing CSA to counteract social engineering. They recommended that an organization should not be limited to traditional types and techniques for CSA, for example, posters and screensavers, for all employees. Instead, they should choose CSA programs based on the target audiences' roles, responsibilities, and preferences. They also noted the possibility of using a novel technology like simulation to investigate any flaws or vulnerabilities in the organization's security system. Finally, they recommended that organizations adopt techniques like real-world situations and case studies to increase employees' awareness of sophisticated social engineering strategies. Although this paper's results and recommendations are valuable, they conflict with one another. The results showed that budget was a significant constraint, but recommendations call for the adoption of methods like simulation, personalized content types and dissemination techniques, and case scenarios and studies. We believe that these recommendations are time- and budget-intensive, demand a certain level of technical expertise, and could be less appealing to a small audience.

Other related studies are by Mayer et al. [56] and Mayer & Volkamer [57]. They conducted a systematic literature review in order to design password awareness-raising materials and elicit misconceptions about password security so that they could suggest appropriate interventions to address them. Similar to them, Sherif et al. [52] carried out a systematic literature review to investigate how security awareness and behavior contribute to the development of a security culture inside an organization. Based on their results, they proposed a framework that shows how awareness, behavior, and organizational culture are interconnected. Such a framework could be useful in cultivating the information security culture of an organization.

A study that dealt with CSA for SMEs is from Lejaka et al. [58]. They used a systematic literature review to investigate cybersecurity frameworks and components that could be suitable for South African SMEs. The study indicated that not a single CSA framework designed for South Africa fulfilled the needs of South African SMEs; thus, they concluded with a need for security frameworks that suit the specific needs and circumstances of SMEs.

Finally, two ongoing research works by the same author group, Ponsard et al. [5] and Ponsard et al. [59], delivered some insight into CSA for European SMEs. In their earlier work, the authors proposed an approach that used the five functions of the National Institute of Standards and Technology (NIST) cybersecurity framework, with each function using a tiered approach. Their proposition is flexible and adaptable, even for companies with tight resources and budgets. An accredited monitoring or governance body can use its approach to get a clear overview of SMEs' cybersecurity situations and their context and accordingly label them with a tier level. Their main idea is that such labeling will raise the awareness of SMEs concerning cybersecurity and help them achieve their cybersecurity defense. The latter work presents learning derived from various CSA workshop sessions organized for diverse SMEs. Their main findings were that (i) CSA campaigns must be able to rely on bigger initiatives with a good dynamic, and (ii) CSA campaigns should combine both passive channels (to reach a wide audience) and active events (where SMEs can actively participate).

All of the studies, except for those focusing on SMEs, conducted a systematic literature review using similar steps to those used in our study. Despite mentioning the use of a literature review, the study by Lejaka et al. [58] does not fully and clearly explain, for example, the criteria, keywords, and screening processes for the relevant literature selection. Similar to this, Ponsard et al.'s study [5] focused primarily on national and international labels and frameworks that address cybersecurity for SMEs. Finally, Ponsard et al. [59] used a survey for their study. The latter two studies were still in progress when this study was conducted.

5. Review of overall past research studies on CSA

In addition to the chosen papers that address CSA for SMEs, we looked at 88 papers related to CSA in order to determine the types of research they have covered in the domain of CSA. Among them, only a few addressed smartphone users, while the majority of studies focused on computer users or other unspecified IS users. The topics covered by the reviewed past studies can be broadly categorized into six types, as shown in Fig. 3.

5.1. Cybersecurity for smartphone users

Almost half of the world's population uses mobile phones, and this number is steadily increasing. Above all, smartphones are now widely used to access the Internet and perform sensitive operations that involve storing, accessing, and sharing information. This could be a reason why cyber threats targeting mobile phone users are surging rapidly every day [60]. Yet, only a few of the papers considered focused on addressing the cybersecurity issues of smartphone users. These studies attempt to assess the CSA level of smartphone users [61–64], investigate the role of various influencing factors on CSA [62,65], make recommendations for raising CSA [66–69], and assess the effectiveness of the applied CSA measures [70].

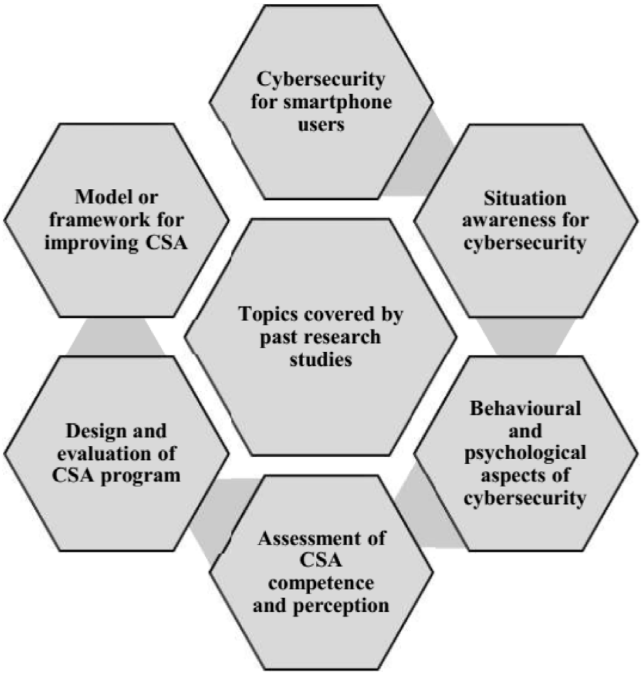
Cybersecurity for smartphone users
Model or framework for improving CSA
Situation awareness for cybersecurity
Topics covered by past research studies
Design and evaluation of CSA program
Behavioural and psychological aspects of cybersecurity
Assessment of CSA competence and perception

Fig. 3. Topics covered by past research studies in overall.

Among the chosen papers, several of them [61,62,64] pointed out a severe lack of CSA among smartphone users. In fact, smartphone users are relatively less aware than computer users [64, 71]. They further divulged that people's security backgrounds or levels of expertise do not significantly influence their CSA in the smartphone ecosystem [62,64]. For example, although smartphone users are aware of authentication techniques and mobile screen locks, they disregard several other security practices, such as turning off Wi-Fi and Bluetooth when not in use [64]. Furthermore, most users trust the app repository and disregard even basic security during application selection and installation [61]. Such risky behaviors become worth mentioning in the current situation when cybercriminals have adapted to and are exploiting the mobile threat landscape. Cyber attackers and criminals are circumventing the security measures adopted by app repositories despite their efforts to detect and avoid untrusted and malicious software from being published on repositories [60,72].

A few studies presumed factors like language, ethnicity, culture, age, and gender could influence CSA and thus suggested further investigation to determine their impacts [61,70]. Interestingly, their suggestions were partially pursued by a recent study by Ameen et al. [65], which implemented PMT, GDT, and Hofstede's cultural dimensions to investigate the influence of gender and national culture on smartphone users' cybersecurity behavior. The study revealed a significant impact of gender and national culture on the security behavior of smartphone users, regardless of how technologically advanced a country is or the type of society it has (i.e., a masculine or a feminine society). In the same way, Parker et al. [70] explored the security awareness (perception) and behavior of smartphone users. They observed a rise in CSA among younger smartphone users.

Some studies explored ways in which CSA can be raised in smartphone users, and they resulted in a comprehensive list of recommendations for mobile phone user safety [66] and a hierarchical taxonomy for mobile phone users' security awareness [68]. Then, some studies assessed the effectiveness of games in raising the CSA of smartphone users and found it to be effective [67,69].

Although the aforementioned studies have made efforts to cover and address a wide range of mobile phone security and awareness, they are not as diversified as studies focusing on computer users' security. Secondly, no study has adequately explained why and how CSA for mobile phone users differs from that for computer users. For example, the mobile phone possesses a higher risk for theft or loss (thus putting the data stored on it at risk), is accessed frequently (therefore users tend to choose weak passwords) [73], and is charged via a USB cable (since power supply and data stream pass through the same cable, this exposes the device to juice jacking). No study has succinctly described what must be done to successfully manage and address the risk posed by these differences. Finally, there is a need for more studies that investigate and discuss how enterprises should use mobile phones for organizational activities, the vulnerabilities they will introduce to the organization, and how those vulnerabilities could be mitigated through CSA.

5.2. Situational Awareness (SA) for cybersecurity

In a complex and dynamic system where the situation is rapidly changing, decision-makers need constant access to timely, accurate, and comprehensible information about the system and its environment that can facilitate critical decision-making. This is where situational awareness (SA) becomes essential. SA is defined as "the perception of elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future" [74]. In addition to perception, comprehension, and projection, the fourth layer of SA could be the resolution of the perceived situation [75]. SA has been recognized as a critical foundation for successful decision-making across a broad range of situations, including cybersecurity.

One fundamental aspect of SA is its ability to respond to new and evolving situations. This dynamic nature of SA makes it suitable for the cybersecurity domain, where the traditional (or static) cybersecurity paradigm cannot capture and respond to continuously and rapidly evolving cyber threats. The new cybersecurity paradigm using SA introduces the ability to respond to cyber incidents when they occur. This paradigm can apply several monitoring and analysis techniques and can be useful for both short-term operational as well as long-term strategic decision-making [76]. In terms of cybersecurity, perception involves the evidence gathering of the situations in the cyberinfrastructure; comprehension involves the analysis of the gathered evidence to deduce the threat level, type of attack, and associated or independent risks; projection involves predictive valuation to address future incidents; and resolution involves the countermeasure controls required to treat the risks inherent or interdependent in the cyberinfrastructure [77].

Most reviewed studies on SA focused on the visualization or graphical representation of security-relevant events and phenomena to enhance the capability of cybersecurity personnel to perceive and manage security-related events [78–81]. They came up with several proposals and recommendations, including

- to visualize the set of security metrics used to evaluate network security levels and the impact of attacks, as well as countermeasures implemented by security officers [79];
- to use multiple views, multiple angles, and multiple levels for the visualization of security situation data for network security [78];
- to represent the network security metrics in three-dimensional (3D) visualization [81]; and
- to visualize the attacks on the cloud computing network environment [80].

In addition to visualization, other aspects of SA focused on in past studies include:

- to build a taxonomy of SA in relation to its goals, information gathering, and analysis aspects, which can be valuable in understanding the concept and contents of SA and helping select effective SA techniques to be used in a specific situation awareness implementation [76];
- to propose a theoretical model to enhance SA and make it suitable for cross-domain working environments in organizations [82], which is relevant to modern-day organizations that work in various sectors and across many domains; and
- to design and propose approaches that can help identify malicious traffic efficiently, for example,
  - to use a Hidden Markov Model (HMM) for the intent recognition of network traffic in order to predict concrete network attacks [83];
  - to use a near real-time analysis of ongoing events on controlled networks that can provide situational awareness in the case of network incidents [84];
  - to use an intention-based analysis approach for network security data collection, which includes compiling connection-level data (frequency, length, bandwidth, data transferred, etc.) and 'offline data' with implications for behavior (i.e., the system's level of security, as perceived by a potential attacker) for the SA [84]; and
  - to assess mission-related assets' criticality to improve the SA [85].

To sum up, these studies mainly utilized techniques like visualization, anomaly detection, and intention recognition in network traffic for situation assessment, projection, and visualization. Their main objective is to keep users informed about their environment so that they can identify potential cyber threats on time and take precautionary measures.

However, most of the studies focused on the visualization of security events, primarily focusing on network security management when, in reality, SA can be much broader than this. Many other cybersecurity domains that need continuous monitoring need exploration to investigate the prospects of SA in them. In reality, the potential of SA has not been realized as much in cybersecurity as it has in other areas, such as aviation, nuclear plants, automated driving, and interaction with different autonomous systems [86]. Similarly, their visualizations seem to be primarily intended for operational-level staff, leaving out other groups like managers, high-level decision-makers, and non-expert users [87] who could also greatly benefit from appropriate SA visualizations in their cybersecurity decision-making. Additionally, the majority of these studies have used toy examples and demonstrations to support their proposed visualizations, with only a few visualizations being used in actual industrial practice [87].

Most importantly, the reviewed studies do not appear to address all four SA levels; most visualizations appear to facilitate perception and, to some extent, comprehension while disregarding projection and response levels. Next, they have considered one cyberinfrastructure component at a time and not the whole cyber system; thus, there is a need for research on an integrated SA framework [77]. Finally, yet importantly, they have focused exclusively on the design of visualizations, paying little consideration to the assessment and evaluation of the visualizations to determine, for example, how the visualizations affect the behavior or actions of human users and how much cybersecurity activity performance is improved by the visualizations [86].

5.3. Behavioral and psychological aspects of cybersecurity

In cybersecurity, certain types of behavior are encouraged while others are warned against. There is an increasing body of research that examines the relationship between human behavior and susceptibility to cyberattacks. They implement theories from different fields of study, such as social science, economics, psychology, and behavioral science. The main goal of these studies is to get cybersecurity behavioral insights that may be applied to the creation of successful CSA programs, or, in other words, to encourage security behavior or motivate people to adhere to security guidelines and procedures. In general, these studies can be divided into two categories: the first category applies psychological, social, economic, and behavioral modeling theories to investigate the effects of their recommended factors on cybersecurity behavior, while the second category directly examines behavioral determinants.

In order to understand how people behave when it comes to cybersecurity, the first category has utilized modeling theories like TRA, TPB, GDT, PMT, TAM, the health belief model (HBM), actor-network theory (ANT), the due process model, psychological ownership theory, flow theory, cybernetic theory, and the technological threat avoidance theory (TTAT) [54,88–91]. The most popular theories for cybersecurity applications among them are TRA/TBP, TAM, GDT, and PMT [53]. These studies have used a combination of two or more theories to conduct their investigation. In some studies, they have adopted and suggested utilizing the theory as it is [90] or with some modification [88] for understanding security behavior and ways to promote it among individuals and employees. While the remaining studies have attempted to investigate the role of behavioral factors from these theories in persuading people to embrace or comply with security policies and guidelines. As a result, the latter studies identified components like attitude, perceived usefulness [54], and psychological ownership [91] as exhibiting a reliable association with security behavior.

The second category then investigated the impact of various behavioral determinants on cybersecurity and its awareness. They discovered the following factors have varying degrees of effect on cybersecurity behavior:

- organizational, social, and personal factors [92],
- socio-demographic factors (e.g., age, gender, persona, education level, academic field, national culture, work experience, security-related training, job hierarchy) [93–98],
- reason and frequency of ICT usage [99],
- previous cyberattack experience [100],
- technical expertise, understanding of the business impact of a cyberattack [89],
- cognitive factors [101],
- attitude, self-efficacy, normative beliefs, and perceived expectations [102,103],
- conceptual and procedural knowledge [104], and
- perceived usefulness, user satisfaction, as well as information and system quality [105].

Although these studies provide many valuable findings on the factors that affect the user's psychology and behavior in cybersecurity, there is a need for more coherent and consistent findings with practical relevance. For example, these studies primarily relied on quantitative studies (or quantifying the behaviors that are likely to attract cyberattacks) that specifically could answer the question of whether there exists a relationship between two variables. However, this statistical validity cannot provide insight into the problem and ways to mitigate it. Therefore, there is a need for studies that can provide internal, external, and construct validity. In other words, there is a need for more qualitative studies that can evaluate the problem in detail and shed light on aspects that were not initially realized or considered. In addition, these studies are typically conducted in artificial lab settings with a small number of mainly homogeneous participants. This is problematic mainly because people become conscious when participating in a lab setting and start to behave analytically and logically. Their response and feedback are unlikely to match that when interacting with or reacting to a real cyberattack. Thus, there is a need to conduct experiments on real-world conditions or organization-specific scenarios (with actual users or heterogeneous users) as much as possible to achieve a more realistic and pragmatic result.

Furthermore, behavioral and psychological aspects of cybersecurity are still in their infancy, and many behavioral or persuasion theories, principles, and processes are yet to be explored from a cybersecurity perspective. For example, social-psychological techniques like instrumental learning, social learning, conformity, obedience, reciprocity, and commitment that are used to persuade people to behave in a certain way need exploration in order to determine the possibilities they can offer for CSA and cybersecurity purposes [106]. Then, almost all the existing studies investigate the behavioral and psychological aspects of the end-users but fail to explore the perspectives of offenders engaged in various forms of cyberattacks and cybercrimes, an important stakeholder in cybersecurity. It is still not known if and how offender characteristics interact with the motives for the execution of certain cybercrimes [107]. Research to understand the social and psychological characteristics of offenders that play a role in the development of offenses can presumably help in producing better CSA content and cybersecurity mitigation techniques. Finally, a majority of these studies are carried out in engineering disciplines, where they have attempted to specify and control human behavior through a small set of drivers, which social scientists may consider a misdirection [108]. This brings forth a need for multidisciplinary collaboration, for example, considering psychological, economic, social, and other drivers in order to understand cybersecurity behavior.

5.4. Assessment of CSA competence and perception

Several studies have assessed the cybersecurity competence and perception of people or employees. These studies measured the awareness levels on subjects like social engineering, organizational regulations and policies, password etiquette and management, phishing attacks, sensitive data protection and privacy, malware, software updates, and Internet and online service usage (such as social media, cloud services, email, and e-banking), among others [96,103,104,109–114]. They performed their research in a variety of organizations, including those involved in banking, insurance, healthcare, IT, and telecommunications. They pointed out an exhibit of misconceptions and stereotypical understandings of cyberattacks among people and employees. To make matters worse, these people lack proper awareness of even the most basic security issues. As a result, people and employees act irresponsibly and readily reveal private and sensitive information. Additionally, some technical teams in organizations believe that employees should be compensated with technological security solutions since they lack CSA, are incapable of handling security-related activities, and cannot make acceptable security-related decisions [110]. Although this proposition from technical teams may seem promising, in cybersecurity it may not be infeasible to replace all users' activities and decisions with automation, at least with the available technology [115,116]. However, the situations do strongly indicate a severe need for relevant CSA programs and training for people and all levels of staff. Furthermore, these CSA programs should be organized regularly, their impact measured, and their quality accordingly improved in the future [110].

Next, some studies classified the users based on their CSA. For example, Ahmad et al. [97] classified employees' behavior based on the knowledge-behavior spectrum into four groups: the rebel, the discerning, the oblivious, and the obedient. They also concluded that the rebels are more challenging to change using CSA. Similarly, Ög˘ütçü et al. [117] investigated the IS users' risky behaviors that might threaten information security. Their investigation resulted in the following four metrics: the risky behavior scale (RBS), the conservative behavior scale (CBS), the exposure to offense scale (EOS), and the risk perception scale (RPS). Finally, Kirlappos et al. [36] examined employee behavior and identified a third category of employees apart from those who do and do not comply with prescribed security policies. This third type of employee believes that they cannot comply with the prescribed security policies, so they create a more suitable alternative to the policies and mechanisms in order to get the job done and manage the risks. Further, they concluded that the organization should learn from these employees, who devise 'workable' security solutions that offer effective security and fit with the organization's business. In addition to these studies, Solic et al. [118] provided an approach to gauge users' security awareness. Their suggested approach uses a cluster analysis method to classify email users according to their level of security awareness.

The first step in any CSA program is to define its goal (i.e., security issues) and target (i.e., audiences). Such assessments of organizations and their employees can be valuable in identifying the goal and target audience. Moreover, they evaluate the maturity level of security capabilities, identify vulnerable areas, and provide recommendations on prioritizing areas for remediation. However, an inherent limitation of such assessments is that their results can quickly go out of date with the ever-changing cyber threat landscape and other factors like changing technologies, business requirements, or compliance standards. Additionally, there is always a risk that the outcome may not reflect the actual situation since even highly educated and aware people may not behave as expected [64]. Hence, such assessments should be conducted periodically and employ techniques that assess the participants in as many real-life situations as possible so that their results remain up-to-date and valid.

Furthermore, such assessments of CSA competence and perception largely depend on self-reported measures, for example, surveys and interviews. This preference for the self-reported measures could be due to the low costs and resources required to implement them and the flexibility they provide to easily integrate different aspects of cybersecurity into the measurement. However, a major problem in many studies is that they use self-designed questionnaires, which are often non-standardized (i.e., do not adhere to standard procedures to design the questionnaire) and only focus on one or a small number of specifically chosen components of cybersecurity. Because of this, the results of studies using poorly designed questionnaires may not accurately reflect actual cybersecurity situations. In order to create standardized questionnaires and use them to evaluate CSA perception and competence, more study is required.

5.5. Design and evaluation of a CSA program

The quality of awareness materials and the effectiveness of the dissemination methods used are two critical components that contribute to the success of CSA programs or campaigns. These components play a significant role in determining how well the key message will be received, comprehended, and ultimately applied by the target audiences. If the awareness materials used have an unclear and confusing message or piece of information, the chance of people misinterpreting or ignoring it will increase. Therefore, CSA information should be relevant, timely, and consistent [96]. Similarly, selecting a dissemination method that the target audiences do not like or prefer would make them less interested in CSA programs.

Several studies have proposed, designed, and evaluated different awareness materials and delivery methods for CSA purposes. For example, games [55,119–132], web browser add-ons or plugin tools [133–136], online portals [137], social media [138], online quizzes [139], hacking contests [140], phishing emails [141], simulations [55], etc., have been suggested as dissemination methods for effective CSA programs. It is interesting to note that among the papers analyzed, the use of games was the most popular, followed by browser add-ons or plugin tools. Serious games that provide a more natural environment for learning and require users to think about security concepts [126], role-playing quizzes and games [129,130], humorous decision-making games [132], ethical hacking simulation games [121,140], and games hosted on social networking sites [119] were a few types of games used for CSA purposes. At the same time, their work on web browser add-ons or plugin tools was associated with security-oriented design or usable security. Moreover, these studies have targeted security issues like social engineering, phishing, data security, misconfiguration and associated risks, password security, social networking, cloud security, and mobile security for awareness.

In addition to these, some other propositions made by the considered studies were:

- To use anomalous data for perspective and conceptual change in employees [142]. This was based on the assumption that users will learn or invent new conceptions when they experience cognitive disequilibrium after failing to explain the anomaly.
- To apply persuasive technology in the field of CSA to persuade users to change their behavior and perception toward information security practices [38].
- To provide exposure to news stories about corporate security breaches to employees [143]. This was based on the assumption that knowing about cyber breaches would affect employees' behavior and make them more cautious in cyberspace.

Almost all the studies have focused primarily on computer- and online-based learning techniques that are interactive and demand the active participation of the audience during CSA events. They recommended computer- and online-based techniques for promoting both introductory CSA for general users as well as more specific CSA for staff with greater security responsibilities [55,123]. Such methods can be suitable to instill awareness mainly because they can be accessed on-demand and learning can be performed in a self-paced manner. Another reason could be that learners using paper-based CSA materials can perform better at only the perception level, whereas learners using multimedia-based CSA materials can perform better at both the comprehension and projection levels [46]. However, in the end, it has been recommended to rely on mixed delivery methods, and the selection of methods should be based on the audience's preference [55,144]. Eventually, this is also supported by [45], who evaluated the appropriateness of delivery methods and found combined methods (e.g., text-based, game-based, and video-based) to be better than individual ones for CSA.

Regarding materials used for CSA, organizations often rely on security reports from security organizations, such as the Verizon Data Breach Report or the Symantec Internet Security Threat Report [145]. Such reports contain valuable information for the enterprise and are useful overall; however, the organization using them should be able to filter out the information applicable to it and its employees. A good CSA resource should be relevant to the organization and, more specifically, to the audiences. Moreover, the organization should not limit itself to larger and more common threats but also cover threats specific to it in CSA programs. After all, a variety of CSA tools and other resources are accessible online, and many of them are free, though they might require some level of customization to suit an organization's needs [40].

One of the main limitations of the considered studies is their evaluation process. Firstly, most studies have not evaluated the effectiveness of their propositions. Even those that have been evaluated take into account aspects like usability and user satisfaction. These elements are crucial, but they do not account for all the elements that should be measured. Secondly, their sample selection method was not bias-free, consequently affecting the results' significance. For example, the evaluation process relied heavily on college or university students as participants, among whom, for example, games may be more popular. Generalizing the results of a study conducted on students for other types of users may not provide the actual scenario and preferences of those users. Thirdly, the evaluation process does not capture the main essence of evaluation, which is the effectiveness of the method in communicating the message and information and the user's preference for that method. Fourthly, no research has examined the applicability and effectiveness of CSA materials and dissemination strategies based on factors such as:

- Awareness topics; for example, types of material and dissemination methods suitable for social engineering awareness may not fit for cloud security awareness;
- Audiences' job designations and responsibilities; for example, types of material and dissemination methods suitable for the awareness of staff in the accounting department may not be the same as those in the IT department; and
- Audiences' age (generation), gender, academic education, work experience, and cultural aspects; for example, younger generations may prefer other awareness materials and dissemination methods than those preferred by older generations.

Finally, most past studies depended on evaluating one or a set of factors like gains in knowledge and competencies; positive changes in attitude, behavior, belief, and intentions; increases in interest (of users, organizers, and management/sponsors) towards CSA; and improvements in the usability of CSA materials. Further, they implement diversified methods to measure those factors, for example, surveys, interviews, simulated attacks, observation, etc. However, the problem is that there is no consensus on what factors to measure and, above all, how to measure them to evaluate the effectiveness of a CSA program. Equally important is how a weight can be assigned to each factor measured when they rely on multiple factors to determine the effectiveness and what is an acceptable level of CSA (or how to know if it is an acceptable level of CSA). Interestingly, three recent studies have attempted to address the problems encountered in these studies and facilitate the evaluation of CSA programs. First, Chaudhary et al. [146] have listed a set of properties that could contribute to improving the effectiveness of awareness materials. Second, Chaudhary and Gkioulos [116] have proposed a framework for designing an effective CSA program. Third, Chaudhary et al. [147] have suggested metrics for the comprehensive evaluation of a CSA program.

5.6. Model or framework for improving CSA

A model or framework within cybersecurity is essential because it helps to gain a better understanding of the problem and thus streamline the implementation of effective cybersecurity measures. It enables an organization to quantify its current state, which subsequently enables understandable and repeatable results to be communicated [148]. Moreover, it helps to prioritize requirements, based on which an organization can optimally align its capabilities in order to achieve them. The reviewed studies have proposed conceptual models or frameworks for various purposes, for example, to assess a user's CSA [112,149], understand the issues or influencing factors of CSA [88,90,150], design an effective CSA program [32,151], and assess a CSA program [152].

First, Hassanzadeh et al.'s conceptual model [112] employed seven independent variables to evaluate the user's CSA, among which gender, IT awareness, occupation area, and job category had substantial correlations to CSA. Similar to this, Andrews [149] proposed a model to analyze data privacy awareness based on how data is stored and shared on the Internet, which can assist people in making informed decisions before disclosing their personal information.

Second, some studies have put forth frameworks or models to comprehend the factors that may have an impact on CSA. For example, Tsohou et al. [88] realized that the majority of existing CSA frameworks lack theoretical justification or explanation of why a particular choice, such as a security message and dissemination method, has been made. Furthermore, these frameworks examined CSA problems and challenges solely based on psychological or behavioral theories. Therefore, in order to facilitate analysis and understanding of the issues that are intertwined with awareness activities and the due process model, Tsohou et al. proposed a theoretical and methodological framework. Similarly, Li et al. [90] believed that influence from peer behavior and an employee's action experience with cybersecurity are essential factors in improving cybersecurity behavior in organizations. Thus, they proposed a model that extends the PMT and HBM to validate the relationships among peer behavior, the cue to action, and the employee's action experience of cybersecurity, threat perception, response perception, and the employee's cybersecurity behavior.

Third, Vroom & von Solms [32] posited the view that CSA should be specified in the security policies of organizations and encompass every aspect of security that is worthy as well as feasible to implement. They further recommended that the fundamentals, such as who will develop the program, how the program will be structured, and what dissemination strategy will be adopted, should be established prior to the execution of a CSA program. On the basis of these recommendations, Vroom & von Solms proposed an information security awareness model. In this model, the high management is first made aware of cybersecurity; the management later designs the organizational security policies using international security standards as guidelines; and finally, the practice of the International Standard Organization (ISO) for the review and maintenance of organizational cybersecurity, including CSA programs for general and role-specific users, is implemented. Similarly, Kritzinger & Smith [153] proposed an Information Security Retrieval and Awareness (ISRA) model that can be used by the industry to enhance information security awareness among employees. Their model comprises three parts, namely, the ISRA dimensions (non-technical information security issues, IT authority levels, and information security documents), information security retrieval and awareness, and measuring and monitoring. Then, Jixing et al. [151] proposed a CSA model based on connectionism.

Finally, Al-Hamdani [152] proposed an assessment model for quantifying CSA programs needed for a larger population. This model is based on two assessments: the first focuses on security in general, and the second assesses comprehensive awareness of specialized domains. Moreover, they found out that CSA for a larger population needs to allocate an instructor per 1,000 people and should focus on 'out of class awareness' programs.

Despite all these propositions, there are still not adequate frameworks or models, which brings a need for more assessment frameworks or models that can overcome all the challenges and limitations mentioned so far and be more specific to organizational domains and needs, for example, SMEs, by considering their institutional constraints during the planning, execution, and evaluation of CSA. Interestingly, a conceptual framework for CSA has been proposed by Chaudhary et al. [154], which consolidates the key stages, factors, and recommendations from various existing frameworks and other important studies. This framework has included many best practices as recommendations, from which organizations can choose those applicable to their business domains and situations.

6. Review of past research studies on CSA that focused on SME

Among the 20 selected papers focusing on SMEs, only nine of them directly relate to CSA [16,54,57,155–160], whereas the remaining papers discuss the overall security aspects (i.e., both technical and human aspects of cybersecurity) of SMEs, while CSA is only a part of their discussion. Similar to this, five papers proposed a model, framework, or process [157,159,161–163] and tested their proposition in SMEs, while other papers assessed either the effect of specific parameters on SMEs' cybersecurity or the overall security, status, or culture of SMEs.

It is interesting to note that, except for SA, the CSA challenges encountered by SMEs and raised by the reviewed papers were comparable to those discussed in Section 5 (of Fig. 3). SMEs can be broadly categorized into four categories based on CSA at the organizational level, as shown in Fig. 4. This classification takes into account SMEs' willingness to acknowledge cybersecurity problems and invest money in effective defenses.

- **Type I:** The owners and executive management of these SMEs possess the misconception that cyberattacks target only large organizations, so SMEs should not worry about cybersecurity. On the contrary, such a tendency towards cybersecurity was only noticed in some old studies. The situation seems to have largely improved now.
- **Type II:** These SMEs accept cybersecurity as an imminent threat but, due to their limited budgets, must prioritize investment in areas that can contribute to their business growth. Most of the studies found this type to be prominent in SMEs. Such SMEs mostly rely on security measures that come inbuilt with other necessary technologies or are available for free or at a lower price, such as operating system security and workshops and materials provided for free by some governmental and non-governmental agencies.
- **Type III:** These SMEs accept cybersecurity as essential and allocate some budget to it, but lack the awareness or qualified human resources to implement the budget. They try to manage their IT security by themselves, and as a result, not all aspects of IT security are sufficiently covered. They mostly focus on technical measures. Their policies and regulations are designed based on their limited understanding of cybersecurity, and they often do not comply with the established regulations and standards for cybersecurity.
- **Type IV:** These SMEs depend on third parties for their cybersecurity. Studies showed that this group was more confident about their cybersecurity.

Similarly, the main challenges of CSA that the reviewed papers have raised are presented in Fig. 5. These are also the research directions that future research should focus on. They ought to concentrate on addressing these challenges so that a better CSA for SMEs can be produced.

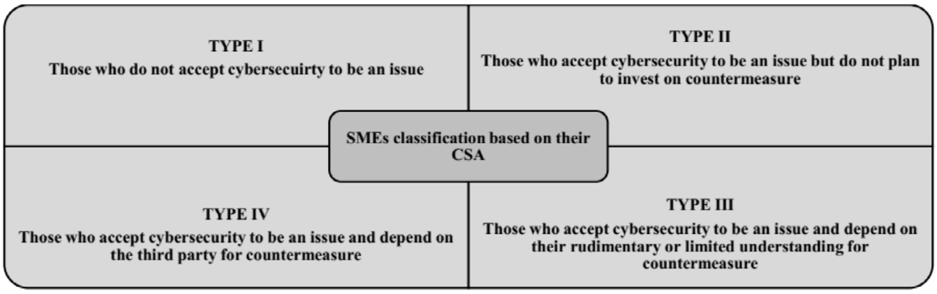
TYPE I
Those who do not accept cybersecuirty to be an issue
TYPE II
Those who accept cybersecurity to be an issue but do not plan to invest on countermeasure
SMEs classification based on their CSA
TYPE IV
Those who accept cybersecurity to be an issue and depend on the third party for countermeasure
TYPE III
Those who accept cybersecurity to be an issue and depend on their rudimentary or limited understanding for countermeasure

Fig. 4. Classification of SMEs based on their CSA.

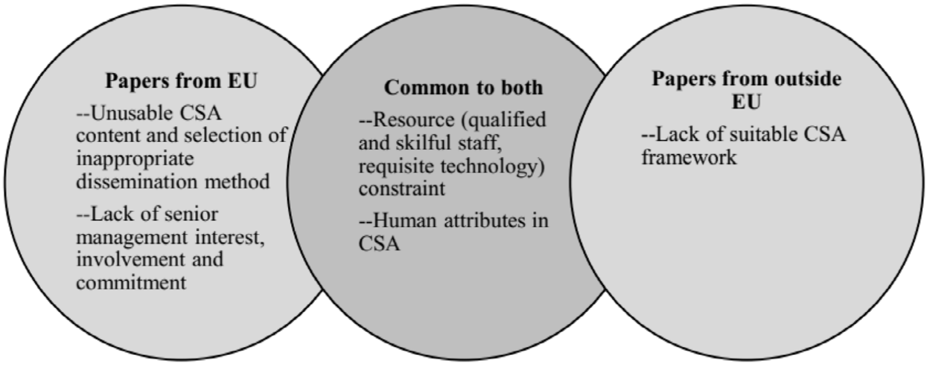
Papers from EU
--Unusable CSA content and selection of inappropriate dissemination method
--Lack of senior management interest, involvement and commitment
Common to both
--Resource (qualified and skilful staff, requisite technology) constraint
--Human attributes in CSA
Papers from outside EU
--Lack of suitable CSA framework

Fig. 5. Challenges of CSA for SMEs.

6.1. Resource constraints

Many studies, both from within and outside the EU [16,114,158,161,162], have identified resource constraints as one of the major contributing factors behind the poor CSA of SMEs and their overall cybersecurity posture. The budget constraint adversely affects their ability to hire qualified and skilled cybersecurity professionals, particularly for CSA, to coordinate pertinent CSA programs, equip themselves with the requisite cybersecurity technologies, and comply with the established regulations and standards. Even SMEs that acknowledge security comprehend the value of cybersecurity policies and regulations, but they still design and implement those policies and regulations based on their rudimentary and limited knowledge of cybersecurity and end up including implausible defense presumptions [164]. Additionally, there is no individual tasked with increasing the employee's awareness of security policies and regulations and enforcing their compliance. There are a number of causes for CSA's financial limitations, but primarily three:

- SMEs are growing companies with modest financial resources. As a result, they do not place a high emphasis on cybersecurity [7,156]. They prefer to invest in projects and activities that will bring the company tangible growth or gains, such as a higher return on investment (ROI) or lower operating costs [165].
- Some owners, executives, or senior management disregard the risk of cyberattacks because they believe it only applies to large corporations [16].
- Even those organizations whose leadership acknowledges it as a problem, prioritizes it in their budget, and invests money in technical measures [162,166]. When they invest in technologies without understanding how effective they will be in overall security control, this issue gets worse. The management feels that they are wasting money on security because, while spending a lot of money on technology, the organization is also experiencing cyberattacks and data leaks.

Ironically, the issue of resource constraints is common even among other types of organizations [165]. Large organizations may not have monetary issues, but many still lack dedicated security professionals assigned to CSA. This is supported by a 2019 SANS Institute survey [167], which found that over 75% of security awareness professionals work part-time and devote less than half of their time to security awareness [167]. The same survey also showed that CSA is an added responsibility to cybersecurity professionals' other employment responsibilities. Additionally, it discovered a significant correlation between full-time employees dedicated to CSA and the organization's CSA maturity level.

There are mainly two ways to handle the issue due to resource constraints for cybersecurity and the CSA program, which are: (i) lowering or minimizing the cost of cybersecurity; and (ii) allocating enough budget for cybersecurity. Since the second option directly affects finances and the executive management of the organization only holds the authority to make it different, this issue can be handled only with the involvement and commitment of senior management, as discussed later in Section 6.3. Determining how much is enough is difficult, though, because cybersecurity is dynamic in nature [165].

Regarding the first option, there are several strategies that can help lower cybersecurity costs and advance CSA programs.

- It is unfortunate that technical staff frequently try to make up for the absence of CSA by using technical IT security solutions [110]. These individuals in charge of an organization's cybersecurity must be aware that the tendency toward relying heavily on technological solutions is not only unsuitable but also costly for the business. It may also hurt the employee's productivity and lower morale if the employees are not trusted and treated as culprits or enemies [110]. So, tightening security by deploying sophisticated technology and imposing stringent rules and policies that are difficult to adhere to may not improve cybersecurity to the level expected. It is, therefore, suggested to use CSA where necessary, which can be less expensive while still being an effective security countermeasure.

- It is becoming more common to advocate for and make use of expensive, cutting-edge security technology. Obviously, if the organization can afford the technology, it might not be an issue, but for SMEs, this might not be a viable option. Even if the business must use technological solutions, it is advised against jumping headfirst into everything novel. Not every cutting-edge technology will be ideal for the organization. The kinds of businesses an organization has will significantly affect the types of technology it should acquire. Therefore, it is suggested to learn from experience and research more to identify what best fits the organization's needs. This is possible by understanding the organization's current business circumstances, risk profiles, and weaknesses. If the organization is traditional or unchanging, it is suggested to delay the implementation of enhanced capabilities and focus on minimal requirements, whereas for one that is expanding, choices should be based on the business value of implementing robust capabilities [164].
- In SMEs, if the employee size is small, considering them as a homogeneous target group can help to decrease the complexity and cost of CSA [30].
- It may not always be necessary for an organization to design its own resources for cybersecurity and CSA programs. Many freely available resources can be of great value and are less expensive to use. Such freely available materials can be of great use for small businesses, but only if they struggle with the selection of suitable materials [50]. It is advised to select materials that align with industry standards and guidelines [168] and may need little or no tailoring [40].
- Many times, face-to-face instructor-led CSA (that needs more logistics and is expensive to conduct [43]) can be replaced with online learning materials, which can be cheaper when the target audiences are in mass [46]. Even in face-to-face instructor-led CSA, a need-to-know basis can be followed, i.e., staff should know and stay aware of only those things that are related to them. All staff attending all CSA events could make the endeavor expensive for the organization.

6.2. Unusable CSA content and the selection of an inappropriate dissemination method

Some studies [13,131,155,157] made suggestions to improve the usability of CSA programs. This is mainly because the existing CSA programs do not seem to address the needs of SMEs. As a matter of fact, this issue has been equally encountered by other types of organizations. Even among the enterprises that flag cybersecurity as a high priority and have been allocating resources for CSA, they do not see any tangible effect on their unaware employees [21], and organizations still have to deal with the risks resulting from people who do not follow security policies and procedures or fail to understand the awareness materials [169]. This may be attributed to poorly tailored awareness-raising materials and techniques that are implicitly based upon the assumption that "one size fits all" [21]. Due to the ineffectiveness of CSA, some people are frustrated and even believe that such awareness activities are a waste of money and should be abandoned [169,170]. This belief in abandoning CSA may be too harsh, but it is also eye-opening and specifies that things need to be done differently or need improvement.

There is a need for CSA content and dissemination methods that support the organization's business requirements, are pertinent to its culture, and take into account its IT infrastructure. If employees believe the message is explicitly and appropriately aimed at them rather than generically at everyone, cybersecurity is more likely to be accepted and acted upon. Currently, any tailoring of CSA materials is most frequently done, at best, from the standpoint of framing the messages to match the type of organization or sector concerned. Rarely do things reach the degree that each user might require based on their preferred learning styles or prior predisposition towards security. The most effective awareness campaigns are the ones that participants believe are pertinent to the problems and issues raised. The goal should not be what the staff needs to know but how we can get them to know it.

Furthermore, it should preferably be tailored and personalized to the needs of the recipients. These flaws in the design of CSA contents and the selection of dissemination methods exist maybe because the majority of awareness professionals have technical backgrounds; over 80% of them do [167]. A technical background is unquestionably advantageous, but such professionals often lack the soft skills, such as communication skills, personal attributes, career and collaborative attributes, and people skills [171], needed to effectively communicate cyber-risks to audiences in a way that changes behavior. Besides, they suffer from a cognitive bias called the "curse of knowledge", i.e., the more expertise a person has on a subject, the more difficult it can be for them to teach or communicate [167].

The CSA contents should be clear, consistent, and relevant to the target audiences, and more importantly, they should be actionable [57,155] and meet the mission of the organization [166]. Further consideration should also be given to the localization of security awareness material. That does not mean that terms such as phishing should be translated, but rather that the concept and associated risks be presented and explained in the appropriate languages. In addition, they should meet the mission of the organization [166]. Chaudhary et al. [146] have presented a more comprehensive list of properties that should be considered for CSA content design.

When selecting a dissemination or delivery method, it has been suggested to consider multiple (i.e., alternative) techniques that are suitable for diversified users [131,155]. Further, the CSA contents and dissemination methods need continuous improvement based on their effectiveness with the audiences [13,155, 157]. Finally, learners with text materials perform better at the perception level, whereas those with multimedia materials perform better at the comprehension level and projection level [46], so these materials should be selected accordingly.

The types of audiences (i.e., learners) also help in deciding the types of CSA material and dissemination methods that will be usable or relevant. For example, audiences with experience in security may become bored and distracted if they are forced to repeat simple activities meant to improve the knowledge level of beginners; vice versa, they may find these activities irrelevant and burdensome. Similarly, if the security processes and procedures are difficult to comply with or their compliance cost (i.e., interfere with primary tasks or are resource-taxing) exceeds that of disobeying them, then no matter how aware an individual is, s/he will find CSA unusable [64]. Therefore, CSA materials must satisfy end-user needs, be cost- and effort-effective, not necessitate effort-taxing activities that can slow down users' tasks, be accessible and appropriate for users' circumstances, situations, or conditions, and employ communication strategies and techniques that align with users' preferences.

6.3. Lack of senior management interest, involvement, and commitment

CSA is most effective when it is fully supported by the leadership within the organization. If users perceive that leadership is fully committed, they are more likely to take it seriously. Therefore, CSA should be a part of any security plan and be seen as an integral part of the security program. In fact, the organization should include it as part of its organizational policies. One of the primary causes behind the low priority of cybersecurity in organizations is a lack of senior management support and commitment [50]. This has a negative effect on an organization's overall cybersecurity, including its CSA. This is especially true for SMEs, whose management has to prioritize other activities over cybersecurity due to resource limitations. Additionally, SMEs lack qualified and experienced personnel who can effectively communicate with top management to convey the relevance and significance of cybersecurity.

There are no definite strategies to ensure senior management's involvement in and dedication to cybersecurity and CSA. However, the following are some potential strategies:

- To show and explain the cost-benefit of CSA to senior management [162] and the need to raise the awareness of senior management. It is suggested to provide them with evidence on what value CSA would add or explain to them beyond what they already feel they know. A study like, for example, Park et al. [25], which measured the impact of cybersecurity training and education and utilized the following parameters for assessment: educational satisfaction, academic achievements, job application, and economic ROI, can be useful. Further, explain to them the cyber risks by using clear narratives and connecting with areas that the decision-makers understand and deeply care about [165].
- To design and organize CSA programs that require procurement of the least level of resources, preferably CSA activities that can be conducted for minimal cost [131] and can utilize cost-effective ways like e-learning and collaborative platforms [16,159].
- To leverage peer comparisons via benchmarking, i.e., to show leadership how competitors are spending significantly on CSA [165,167].
- To demonstrate to them that CSA is effective in reality. For example, demonstrate that CSA plays a positive role in effective compliance with security policies and proper integration of 'people,' 'process,' and 'technology' [172].

6.4. Human attributes in the CSA

The majority of research studies focused on determining human characteristics or factors that may motivate security behavior [16,114,155–158,173]. They have suggested factors like avoiding fear as a way to raise awareness, considering cultural aspects in CSA, using a promotion or award approach to encourage aware people to comply with security policies, a preventive approach for both aware and unaware people, better usability design to encourage people to adhere to security procedures, etc. Similar to this, it has been suggested that many other factors be taken into account during CSA programs, including self-efficacy, prior IT skills and knowledge, job category, gender, language, etc.

In fact, the human factor is also the most challenging and intricate issue in the design and implementation of CSA, since it involves domains like behavioral psychology, cognitive psychology, and neuropsychology [174]. According to a report by the Information Security Forum [174], CSA initiatives are failing for the following six reasons:

i. solutions are not aligned to the business risks,
ii. neither progress nor values are measured,
iii. incorrect assumptions are made about people and their motivations,
iv. unrealistic expectations are set,
v. the correct skills are not deployed, and
vi. awareness is just background noise.

Further, the same study suggested utilizing behavioral psychology (to understand the history and context that drives behaviors and change the consequences in this context to eliminate unwanted behaviors and promote target behaviors), cognitive psychology (to deliver solutions in small chunks using a "simple to complex" principle; to include opportunities to sufficient practice the target behaviors, and to have an effective evaluation process that the individual can use to monitor their progress) and neuropsychology (to challenge the individual sufficiently so a new mental map can be formed; where possible, help the individual come to his/her own conclusions and generate insight-facilitate "key moments" rather than teach; and where possible, keep the individual focused on their new insights) to mitigate the six problems mentioned above.

Other reasons behind the failure of CSA initiatives could be

- a lack of time,
- a lack of communication,
- a lack of incentives to study the documentation, and
- a lack of understanding of the instructions [175].

The NIST [27] then advised

- correctly planning and structuring CSA initiatives;
- defining the CSA initiatives' coverage priorities;
- setting the bar for the complexity of the subject matter that CSA initiatives should cover; and
- conducting an assessment to measure the effectiveness of CSA initiatives.

Similarly, Furnell & Vasileiou [21] recommended taking into account audiences' prior knowledge, barriers, learning styles, and security perceptions when designing and conducting CSA programs. Last but not least, Bada et al. [22] suggested that awareness content should be engaging, appropriate, and ongoing, with a range of relevant topics that are targeted, actionable, and doable, and provide feedback to help sustain people's willingness to change. However, the art of persuasion rests in simplifying something down to its essence and making it clear to others what they truly care about, and while fulfilling this, one must be aware that every individual has a unique reality.

6.5. Lack of suitable CSA frameworks

Most of the existing CSA frameworks are not designed with SMEs in mind [58]. The needs and circumstances of SMEs are different from their larger counterparts; thus, the existing frameworks do not exactly meet SMEs' requirements. There are two potential solutions to this problem: (i) creating a new framework and (ii) modifying the existing frameworks to serve the needs of SMEs. Some studies [54,56,57,131] have attempted to develop frameworks and models that could accommodate the requirements and circumstances of SMEs. The issue with these frameworks and models is that they primarily try to address the financial limitations faced by SMEs. Undoubtedly, a major obstacle for SMEs is a lack of resources, but they also have to deal with other obstacles, including multi-tasking employees, centralized decision-making, and so on (see [176]), which may have an impact on their CSA effectiveness.

7. Preferred research methodology for the CSA study

Among the 108 reviewed papers (i.e., papers considered for Sections 5 and 6), most studies implemented a survey to investigate the user's response. This is followed by a literature review, primarily using a systematic literature review. Other popular research methods used were prototype design, interviews, and case studies organized in descending order, as shown in

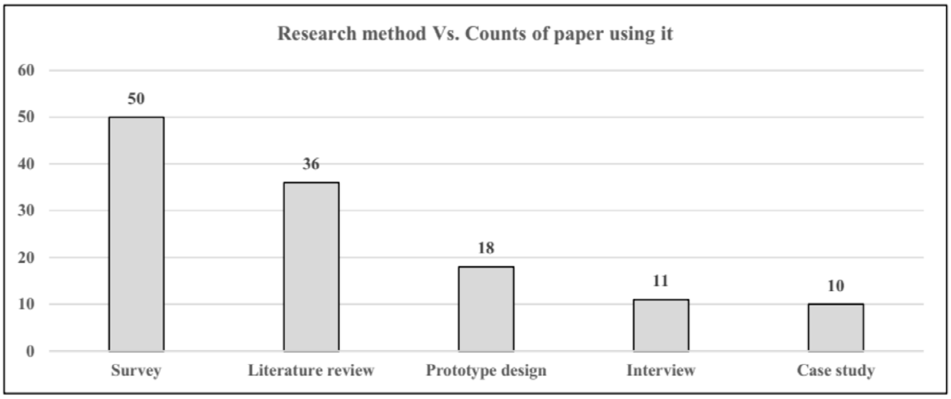

Fig. 6. Counts of papers using a research method.

Fig. 6. In addition to these popular research methods, some studies have also used autoethnography, laboratory experimentation, user study, observation, simulation, manual analysis and assessment, focus groups, expert views, metamodels, method engineering, and mathematical proof.

A survey has widely been utilized either as the sole research method or as a follow-up method to test a proposition, design, model, or prototype. It is generally conducted using an online questionnaire and, in rare cases, an offline questionnaire. Most of them used a five-point Likert scale approach to specify the level of response. More importantly, these studies have largely relied on quantitative data analysis, except for a few that used interviews to perform qualitative data analysis. Similarly, a literature review has also been used either as the sole method or in combination with other methods. When used along with other methods, a literature review is primarily used to develop research hypotheses or constructs. The prototype design has been used in studies that investigated suitable CSA dissemination strategies and situational awareness systems. It is generally a semi-structured interview that has been used mostly to investigate human behavior or its influencing factors. Some studies have used interviews to measure the perceptual differences among the participants or to collect participant feedback after laboratory experiments. It is a case study that has been used in a variety of domains, but with a focus on investigating the needs of specific cases, such as financial institutions, telecom industries, and so on.

Most studies relied on quantitative data analysis, which may be because they were more interested in quantifying the results in numerical terms. Only a few studies used qualitative data analysis, with some relying on the sequential mixed method, which entails collecting one type of data (in this case, always quantitative using a survey), which serves as a foundation for collecting another type of data (in this case, always qualitative using an interview), and the final inference is based on both data. Since CSA involves convincing people who understand in terms of numerical figures to realize the magnitude and seriousness of the problem and its human aspects that demand an in-depth understanding of human attitude and behavior, a mixed method can be a better fit for its study. Quantitative research can help in understanding the gravity of the problem and identifying the areas that need attention or investigation, whereas qualitative research can help in exploring and broadening the underlying knowledge contributing to the phenomenon in the study. An exploratory method of research also allows flexibility in research and seeks to establish the boundaries of problems.

In self-reported measurements like surveys and interviews, the use of high-quality questions and questionnaires is crucial. Broadly divided, the questionnaires in practice for CSA purposes fall into three categories:

i. Questionnaires are prepared based on some standards, such as ISO, NIST, and others, and cover the subjects or topics recommended by them.
ii. Questionnaires are designed and validated by adhering to certain standardized and established processes used for questionnaire development.
iii. Questionnaires are designed by organizations and researchers to serve their needs.

The first two categories of questionnaires should not have any significant issues with the subject matter covered. We do, however, believe that studies using the third category of questionnaires, in essence, when many studies do not validate their questionnaires through, for instance, a pilot survey or expert comments before employing them for the main study, can have issues. The ultimate objective while using questionnaires should be to collect as much unbiased, relevant, and complete data as possible, but not data that supports the proposed or developed tools, models, or frameworks. This means the questionnaires should include all pertinent security topics and be tested before being used.

Furthermore, organizations can only genuinely benefit from CSA initiatives if staff put the knowledge they have acquired into practice. This implies that CSA initiatives ought to be studied and investigated in terms of the actual positive changes they brought about in staff security behavior and action after participation. However, contrary to this view, the majority of CSA studies still employ self-reported methodologies, which cannot adequately capture the real purpose and essence of CSA. Many times people state or intend to do one thing, but their behavior or action conveys something entirely different, also known as the “intention-behavior gap”. Consequently, there is a need for more CSA studies that adopt and employ research methods such as simulated attacks, log data analysis, games, non-intrusive observation in actual scenarios, and possibly a cyber range environment. These methods not only assist in producing realistic scenarios and gathering accurate data, but they also aid in learning about cybersecurity’s “unknown-unknown”. The term “unknown-unknown” refers to those sensitive elements that even security specialists are unsure of, such as what they are and how human behavior could endanger them.

Finally, when employing any method for CSA research, it is important to understand that doing so has a cost. As a result, it is required to determine whether using the method would be worthwhile from a financial, practical, and realistic standpoint. For example, it can be expensive to adopt methods like games, simulations, and cyber range, which many SMEs might not be able to afford.

8. Discussion and conclusions

Cybersecurity is a shared responsibility, and every employee of an enterprise is critical to its cyber defense and countermeasure efficiency. As a result, all employees must be aware of potential threats in their area of work and keep up-to-date on organizational policies and procedures relevant to their job function. Additionally, they should be able to recognize, report, and, if possible, mitigate suspicious cyber activities. By raising the CSA of employees, an organization will be able to reduce its exposure to cyberattacks caused by human error and prevent accidental data breaches. However, while designing CSA for organizations, it is important to realize that the needs and circumstances of different-sized enterprises can vary; that is, we cannot put resourceful enterprises in the same basket as resource-constrained SMEs. Further, a variety of organizational, societal, environmental, and individual factors can influence employees' security behavior, and thus, CSA.

Many past studies have investigated the issues and concerns of CSA, but those performed exclusively for SMEs are not adequate. This means there is a significant need for such studies that focus on the CSA needs and requirements of SMEs. Prior to that, it is vital to identify which CSA components will require additional research for SME needs. Therefore, in this study, we have identified several research and knowledge gaps in CSA for SMEs. In order to accomplish this, we have conducted a systematic literature review. We have largely focused on the CSA problems that need more research to meet the requirements and circumstances of SMEs. Further, we have also suggested research methods that could be applied to future CSA studies.

We found out that one of the main challenges in the case of SMEs is their resource constraints for cybersecurity and CSA. Moreover, this mainly occurs due to a lack of support and commitment from the executive management, i.e., the difference between what they say about the importance of CSA and what they actually do in terms of policies and spending. To some extent, the technical staff in charge of cybersecurity is to blame for the management's attitude toward CSA. They try to compensate CSA with technological solutions and convey the same message to them, thus reducing the priority of CSA. Therefore, there is a need for strong advocacy for the importance of CSA and, more importantly, for affordable and effective CSA that fulfills the needs of SMEs. The CSA content should always consider its compliance costs and benefits (financial or economic costs and benefits, and intangible costs and benefits), and the CSA delivery technique should take into consideration the nature of the organization and its affordability.

The next challenge is the usability of CSA materials and delivery methods (the general extent of acceptance), which needs further investigation. However, regardless of the formats and types of CSA contents, their message should be simple and easy to understand (i.e., cognitively friendly), complete, correct, actionable (or compliant), and, more importantly, relevant and meaningful to the target audience in SMEs. Similarly, their delivery methods should be interactive and innovative in order to engage audiences, as well as inclusive in order to ensure that no segment of the audience feels excluded. To sum up, both CSA materials and delivery methods should be appropriate to the needs and constraints of SMEs.

The human attributes of SME employees that can encourage safe and secure behavior in SME employees equally need further investigation. For this, it is necessary to identify the crucial moments and reasons when people are most likely to fail to meet these goals in cybersecurity. Furthermore, it is necessary to investigate various social, psychological, and behavioral theories that can stimulate, motivate, remind the audience of what is expected of them, and teach them the consequences of their actions in a more effective manner.

Then, there is a severe need for suitable CSA frameworks or models for SMEs. SMEs should no longer depend on the frameworks or models that have been designed considering different needs, contexts, and target groups. These CSA frameworks and models should be exclusively for SMEs and take into account the organizational, economic, and other factors of an SME.

Last but not least, the CSA's coverage of security issues is quite limited, both in general and for SMEs. The majority of studies have concentrated on common security issues, which are certainly crucial. However, many security-related challenges, particularly those pertaining to emerging technologies and threat landscapes, have gone largely unnoticed. There is an urgent need for research on cutting-edge and novel topics, such as security issues raised by the use of artificial intelligence technology, the Internet of Things, and related topics.

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.

Data availability

No data was used for the research described in the article.

References

[1] S. Chaudhary, V. Gkioulos, D9.6 SME cybersecurity awareness program 1, 2020, https://cybersec4europe.eu/wp-content/uploads/2020/04/D9.6-SME-cybersecurity-awareness-program-1-V-1.0-Submitted-1.pdf.(Accessed on 25 March 2023).

[2] European Commission, Internal market, industry, entrepreneurship and SMEs: Entrepreneurship and small and mediumsized enterprises (SMEs), 2020, https://ec.europa.eu/growth/smes_en. (Accessed on 20 September 2020).

[3] D. Clark, Number of small and medium-sized enterprises (SMEs) the European union in 2018, 2020, https://www.statista.com/statistics/878412/number-of-smes-ineurope-by-size/. (Accessed on 20 September 2020).

[4] G. Papadopoulos, S. Rikama, P. Alaj¨a¨ask¨oa, Z. SalahEddine, A. Airaksinen, H. Luomaranta, Statistics on small and medium-sized enterprises, 2020, https://ec.europa.eu/eurostat/web/structural-business-statistics/information-on-data/small-and-medium-sized-enterprises. (Accessed on 20 September 2020).

[5] C. Ponsard, J. Grandclaudon, G. Dallons, Towards a cyber security label for SMEs: A European perspective, in: Proceedings of the 4th International Conference on Information Systems Security and Privacy, Funchal, Madeira, Portugal, January 22-24, 2018, pp. 426–431.

[6] OECD, Strengthening SMEs and entrepreneurship for productivity and inclusive growth, 2018, https://www.oecd.org/cfe/smes/ministerial/documents/2018-SMEMinisterial-Conference-Key-Issues.pdf. (Accessed on 20 September 2020).

[7] T. Kurpjuhn, The SME security challenge, Comput. Fradu Secur. 2015 (3) (2015) 5–7.

[8] R. Vaidya, Cyber security breaches survey 2018: Statistical release, 2018, https://assets.publishing.service.gov.uk/government/uploadssystem/uploads/attachmeatdata/file/702074/Cyber_Breaches_2018_-_Main_Report.pdf. (Accessed on 20 September 2020).

[9] P. Chen, J. Visschers, C. Verstraete, L. Paoli, C. Huygens, L. Desmet, W. Joosen, The relationship between the cost of cybercrime and web security posture: A case study on belgian companies, in: Proceedings of the 11th European Conference on Software Architecture. Canterbury, UK, September 11-15, 2017, pp. 115–120.

[10] P. Millaire, A. Sathe, P. Thielen, What all cyber criminals know: Small & midsize businesses with little or no cybersecurity are idea targets, 2017, https://www.chubb.com/usen/assets/doc/17010201-cyber-for-small_midsize-businesses-10.17.pdf. (Accessed on 20 September 2020).

[11] FireEye, Small and midsize enterprises: Stopping cyber crime against small and midsize enterprises, 2020, https://www.fireeye.com/offers/stop-cyber-crime-against-smallmedium-enterprises.html. (Accessed on 20 September 2020).

[12] L.A. Aguilar, The need for greater focus on the cybersecurity challenges facing small and midsize businesses, 2015, https://www.sec.gov/news/statement/cybersecurity-challengesfor-small-midsize-businesses.html. (Accessed on 20 September 2020).

[13] M. Heidenreich, Conceptualization of a measurement method proposal for the assessment of IT security in the status quo of microenterprises, in: Proceedings of the International Conference on Computing, Electronics & Communication Engineering. London, UK, August, 2 2-23, 2019.

[14] G. Erdogan, R. Halvorsrud, C. Boletsis, S. Tverdal, J.B. Pickering, Cybersecurity awareness and capacities of SMEs, in: Proceedings of the 9th International Conference on Information Systems Security and Privacy, ICISSP 2023, Lisbon, Portugal, Feburary, 2023, pp. 22–24.

[15] M. Brodin, A framework for GDPR compliance for small and medium sized enterprises, Eur. J. Secur. Res. 2019 (4) (2019) 243–264.

[16] S. Dojkovski, S. Lichtenstein, W. Matthew, Challenges in fostering an information security culture in Australian small and medium sized enterprises, in: Proceedings of the European Conference on Information Warfare and Security. Helsinki, Finland, June 1-2, 2006.

[17] D.C. Marinos, Accessing a simplified information security approach: Feedback from RA/RM pilot, 2009, https://www.enisa.europa.eu/publications/archive/assessing-asimplified-information-security-approach. (Accessed on 20 September 2020).

[18] M.T. Siponen, Five dimensions of information security awareness, ACM SIGCAS Comput. Soc. 31 (2) (2001) 24–29.

[19] S. Williams, More than half of personal data breaches caused by human error, 2019, https://itbrief.com.au/story/more-than-half-of-personal-data-breachescaused-by-human-error. (Accessed on 20 September 2020).

[20] Ponemon Institute, 2017 State of cybersecurity in Small & Medium-sized Businesses (SMB), 2017, https://www.keepersecurity.com/assets/pdf/Keeper-2017-Ponemon-Report.pdf. (Accessed on 20 September 2020).

[21] S. Furnell, I. Vasileiou, Security education and awareness: Just let them burn? Netw. Secur. 2017 (12) (2017) 5–9.

[22] M. Bada, A.M. Sasse, Cyber security awareness campaigns: Why do they fail to change behaviour? in: Proceedings of the International Conference on Cyber Security for Sustainable Society. Coventry, UK, February, 26, 2015.

[23] A. Scroxton, Social Engineering a Factor in Virtually All Cyber Attacks, Report Claims, 2019, https://www.computerweekly.com/news/252470384/Social-engineering-afactor-in-virtually-all-cyber-attacks-report-claims. (Accessed on 20 September 2020).

[24] B. Hanus, J.C. Windson, Y. Wu, Definition and multidimensionality of security, DATA BASE Adv. Inf. Syst. 49 (SI)) (2018) 103–132.

[25] S. Park, S. Lee, T. Kim, H. Jun, T. Kim, A performance evaluation of information security training in public sector, J. Comput. Virol. Hack. Tech. 13 (2017) 289–296.

[26] S. CKatsikas, Health care management and information security: Awareness, training or education? Int. J. Med. Inf. 60 (1) (2000) 129–135.

[27] M. Wilson, J. Hash, Building an information technology security awareness and training program, 2003, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-50.pdf. (Accessed on 20 September 2020).

[28] A Caballero, Security education, training, and awareness, in: J.R. Vacca (Ed.), Computer and Information Security Handbook, third ed., Morgan Kaufmann, Burlington, MA, USA, 2017, pp. 497–505.

[29] E. Amankwa, M. Loock, E. Kritzinger, A conceptual analysis of information security education, information security training and information security awareness definitions, in: Proceedings of the 9th International Conference for Internet Technology and Secured Transactions. London, UK, December 8-10, 2014.

[30] ENISA, The new UsersGuide: How to raise information security awareness, 2010, https://www.enisa.europa.eu/publications/archive/copy_of_new-usersguide. (Accessed on 20 September 2020).

[31] M. Wilson, D.E. de Zafra, S.I. Pitcher, J.D. Tressler, J.B. Ippolito, Information technology security training requirements: A role- and performance-based model, 1998, https://www.nist.gov/publications/information-technology-securitytraining-requirements-role-and-performance-based-model. (Accessed on 20 September 2020).

[32] C. Vroom, R. von Solms, A practical approach to information security awareness in the organization, in: Ghonaimy M.A., El-Hadidi M.T., Aslan H.K. (Eds.), Security in the Information Society, Vol. 86, Springer, Boston, MA, USA, 2002.

[33] F. Wolf, R. Kuber, A.J. Aviv, An empirical study examining the perceptions and behaviours of security conscious users of mobile authentication, Behav. Inf. Technol. 37 (4) (2018) 320–334.

[34] Kaspersky, Mobile security threats stay on the move, 2020, https://www.kaspersky.com/resourcecenter/preemptive-safety/mobile-security-threats-on-the-move. (Accessed on 20 September 2020).

[35] T. McGill, N. Thompson, Old risks, new challenges: exploring differences in security between home computer and mobile device use, Behav. Inf. Technol. 36 (11) (2016) 1111–1124.

[36] I. Kirlappos, S. Parkin, Shadow security as a tool for learning organization, ACM SIGCAS Comput. Soc. 45 (1) (2015) 29–37.

[37] A. Adams, M.A. Sasse, Users are not the enemy, Commun. ACM 44 (12) (1999) 41–46.

[38] M. Bawazir, M. Mahmud, N.N.A. Molok, J. Ibrahim, Persuasive technology for improving information security awareness and behaviour: A literature review, in: Proceedings of the 6th International Conference on Information and Communication Technology for the Muslim World. Jakarta, Indonesia, November 22-24, 2016.

[39] K. Renaud, M. Dupuis, Cyber security fear appeals: Unexpectedly complicated, in: Proceedings of the New Security Paradigm Workshop, San Carlos, Costa Rica. September 23-26, 2019.

[40] S.G. Chaudhary, V. kioulos, D. Goodman, Cybersecurity awareness for small and medium-sized enterprises (SMEs): Availability and scope of free and inexpensive awareness resources, in: Proceedings of the ESORICS 2022 International Workshops: CyberICPS 20222. Copenhagen, Denmark, September 29, 2022.

[41] S. Stockhardt, B.M. Berens, M. Volkamer, P. Mayer, A. Kunz, P. Rack, D. D. Lehmann, Teaching phishing security: Which way is best? in: Proceedings of the 31st International Conference on ICT System Security and Privacy Protection. Ghent, Belgium, May 30 -June 1.

[42] J. Andress, M. Leary, Conducting security awareness and training, in: Building a Practical Information Security Program. 1st Edition; Syngress: Burlington, MA, USA, October 14, 2016, pp. 135–155.

[43] E.C. Johnson, Security awareness: Switch to a better program, Netw. Secur. 2006 (2) (2006) 15–18.

[44] J. Abawajy, User preference of cyber security awareness delivery methods, Behav. Inf. Technol. 33 (3) (2012) 237–248.

[45] J. Abawajy, T. Kim, Performance analysis of cyber security awareness delivery methods, in: T. Kim, et al. (Eds.), Security Technology, Disaster Recovery and Business Continuity: Communications in Computer and Information Science, Vol. 122, Springer-Verlag, Berlin, Germany, 2010, pp. 142–148.

[46] R.S. Shaw, C.C. Chen, A.L. Harris, H. Huang, The impact of information richness on information security awareness, Comput. Educ. 52 (1) (2009) 92–100.

[47] R. Daft, R. Griffin, Information richness: A new approach to managerial behaviour and organization design, 1983, https://apps.dtic.mil/dtic/tr/fulltext/u2/a128980.pdf. (Accessed on 20 September 2020).

[48] J. Webster, R.T. Watson, Analyzing the past to prepare for the future: Writing a literature review, MIS Q. 26 (2) (2002) xiii–xxiii.

[49] C. Okoli, K. Schabram, A guide to conducting a systematic literature review of information systems research, SSRN Electron. J. 37 (43) (2010) 879–910.

[50] K. Renaud, How smaller businesses struggle with security advice, Comput. Fraud Secur. 2016 (8) (2016) 10–18.

[51] Y. Levy, T. Ellis, A systems approach to conduct an effective literature, Int. J. Emerg. Transdiscipline 9 (2006) 181–212.

[52] E. Sherif, S. Furnell, Awareness, behaviour and culture: The ABC in cultivating security compliance, in: Proceedings of the 10th International Conference for Internet Technology and Secured Transactions. London, UK, December 14-16, 2015.

[53] B. Lebek, J. Uffen, M.H. Breitner, M. Neumann, B. Hohler, Employees' information security awareness and behavior: A literature review, in: Proceedings of the 46th Hawaii International Conference on System Sciences. Wailea, Hawaii, USA, January 7-10, 2013.

[54] P. Mayer, A. Kunz, M. Volkamer, Reliable behavioural factor in the information security context, in: Proceedings of the 12th International Conference on Availability, Reliability and Security. Reggio, Calabria, Italy, August 29 September 1, 2017.

[55] H. Aldawood, G. Skinner, Educating and raising awareness on cyber security social engineering: A literature review, in: Proceedings of the IEEE International Conference on Teaching, Assessment, and Learning for Engineering. Wollongong, NSW, Australia, December 4-7, 2018.

[56] P. Mayer, M. Volkamer, Addressing misconceptions about password security effectively, in: Proceedings of the 7th Workshop on SocioTechnical Aspects in Security and Trust. Orlando, Florida, USA, December 5, 2017, pp. 16–27.

[57] P. Mayer, C. Schwartz, M. Volkamer, On the systematic development and evaluation of password security awareness-raising materials, in: Proceedings of the 34th Annual Computer Security Applications Conference. San Juan, PR, USA, December 3-7, 2018.

[58] T.K. Lejaka, A. Da Veiga, M. Loock, Cyber security awareness for small, medium and micro enterprises (SMMEs) in South Africa, in: Proceedings of the Conference on Information Communications Technology and Society. Durban, South Africa, March 6-8, 2019.

[59] C. Ponsard, J. Grandclaudon, S. Bal, Survey lessons learned on raising SMEs awareness about cybersecurity, in: Proceedings of the 5th International Conference on Information Systems Security and Privacy. Prague, Czech Republic, February 23-25, 2019.

[60] R. Samani, G. Davis, Mcfee mobile threat report Q1, 2020, https://www.mcafee.com/content/dam/consumer/en-us/docs/2020-Mobile-Threat-Report.pdf. (Accessed on 20 September 2020).

[61] A. Mylonas, A. Kastania, Delegate the smartphone user? Security awareness in smartphone platforms, Comput. Secur. 34 (2013) 47–66.

[62] A. Mylonas, D. Gritzalis, B. Tsoumas, T. Apostolopoulos, A qualitative metrics vector for the awareness of smartphone security users, in: Proceedings of the 10th International Conference on Trust, Privacy and Security in Digital Business. Prague, Czech Republic, August 28-29, 2013, pp. 173–184.

[63] M. Al-Hadadi, A. Al Shidhani, Smartphone security awareness: Time to act, in: Proceedings of the International Conference on Current Trends in Information Technology. Dubai, UAE, December 11-12, 2013.

[64] F. Breitinger, R. Tully-Doyle, C.C. Hassenfeldt, A srvey on smartphone user's security choices, awareness and education, Comput. Secur. 88 (2020).

[65] N. Ameen, A. Tarhini, M.H. Shah, N.O. Madichie, Employees' behavioural intention to smartphone security: A gender-based, crossnational study, Comput. Hum. Behav. 104 (2020).

[66] B. Watson, J. Zheng, On the user awareness of mobile security recommendations, in: Proceedings of the ACM Southeast Regional Conference. Kennesaw, GA, USA, April 13-15, 2017, pp. 120–127.

[67] T. Shabe, E. Kritzinger, M. Loock, Scorecard approach for cybersecurity awareness, in: Proceedings of the International Symposium on Emerging Technologies for Education. Cape Town, South Africa, September 20-22, 2017, pp. 144–153.

[68] R. Bitton, A. Finkelshtein, L. Sidi, R. Puzis, L. Rokach, A. Shabtai, Taxonomy of mobile users' security awareness, Comput. Secur. 73 (2018) 266–293.

[69] M. Bahrini, G. Volkmar, J. Schmutte, N. Wenig, K. Sohr, R.R. Malaka, Make my phone secure! using gamification for mobile security settings, in: Proceedings of Mensch und Computer. Hamburg, Germany, September 8-, 11 (2019) 299–308.

[70] F. Parker, J. Ophoff, J. Van Belle, R.R. Karia, Security awareness and adoption of security controls by smartphone users, in: Proceedings of the 2nd International Conference on Information Security and Cyber Forensics. Cape Town, South Africa, November 15-17, 2015.

[71] J. Imgraben, A. Engelbrecht, K.R. Choo, Always connected, but are smart mobile users getting more security savvy? A survey of smart mobile device users, Behav. Inf. Technol. 33 (12) (2014) 1347–1360.

[72] BlackBerry, Mobile malware and APT espionage: Prolific, pervasive, and cross-platform, 2019, https://blogs.blackberry.com/en/2019/10/mobile-malware-and-aptespionage-prolific-pervasive-and-cross-platform. (Accessed on 20 September 2020).

[73] W. Melicher, D. Kurilova, S.M. Segreti, P. Kalvani, U.B. Shay, L. Bauer, N. Christin, L.F. Cranor, M.L. Mazurek, Usability and security of text passwords on mobile devices, in: Proceedings of the 34th Annual CHI Conference on Human Factors in Computing Systems. San Jose, CA, USA, May 7-12, 2016, pp. 527–539.

[74] M. Endsley, Towards a theory of situation awareness in dynamic systems, Human Factors 37 (1) (1995) 32–64.

[75] B. McGuinness, L. Foy, A subjective measure of SA: The crew awareness rating scale (CARS), in: Proceedings of the 1st Human performance, situation awareness and automation conference; user-centered design for the new millennium. Savannah, GA, USA: 286-291, 2000.

[76] A. Evesti, T. Kanstren, T. Frantti, Cybersecurity situational awareness taxonomy, in: Proceedings of the International Conference on Cyber Situational Awareness, Data Analytics and Assessment. London, UK, June 19-20, 2017.

[77] H. Tianfield, Cyber security situational awareness, in: Proceedings of the IEEE International Conference on iThings) and GreenCom and CPSCom and SmartData. Chengdu, China, December 15-18, 2016.

[78] X. Li, Q. Wang, L. Yang, X. Luo, Network security situation awareness method based on visualization, in: Proceedings of the Third International Conference on Multimedia Information Networking and Security. Shanghai, China, November 4-6, 2011.

[79] I. Kotenko, E. Novikova, Visualization of security metrics for cyber situation awareness, in: Proceedings of the 9th International Conference on Availability, Reliability and Security. Fribourg, Switzerland, September 8-12, 2014.

[80] M. Evangelopoulou, C.W. Johnson, Attack visualization for cyber security situation awareness, in: Proceedings of the 9th IET International Conference on System Safety and Cyber Security. Manchester, UK, October 15-16, 2014.

[81] A. Evesti, C. Wieser, T. Zhao, Improved information security situational awareness by manifold visualization, in: Proceedings of the 10th European Conference on Software Architecture, Copenhagen. Denmark, November 28- December 2, 2016.

[82] M.J. Hall, D.D. Hansen, K. Jones, Cross-domain situational awareness and collaborative working for cyber security, in: Proceedings of the International Conference on Cyber Situational Awareness, Data Analytics and Assessment. London, UK, June 8-9, 2015.

[83] Q. Zhang, D. Man, W. Yang, Using HMM for intent recognition in cyber security situation awareness, in: Proceedings of the Second International Symposium on Knowledge Acquisition and Modeling. Wuhan, China, November 30- December 1, 2009.

[84] A.C. Squicciarini, G. Petracca, W.G. Horne, A. Nath, Situational awareness through reasoning on network incidents, in: Proceedings of the 4th ACM conference on Data and Application Security and Privacy. San Antonio, TX, USA, March 3-5, 2014, pp. 111–122.

[85] F.R.L. Silva, P. Jacob, Mission-centric risk assessment to improve cyber situational awareness, in: Proceedings of the 13th International Conference on Availability, Reliability and Security. Hamburg, Germany, August 27-28, 2018, pp. 1–8.

[86] R. Rutzwiller, J. Dykstra, B. Payne, Gaps and opportunities in situational awareness for cybersecurity, Digital Threats: Res. Pract. 1 (3) (2020) 18:1–18:6.

[87] L. Jiang, A. Jayatilaka, M. Nasim, M. Grobler, M. Zahedi, A.L. Babar, Systematic literature review on cyber situational awareness visualization, IEEE Access 10 (2022) 57525–57554.

[88] Tsohou A., M. Karyda, S. Kokolakis, E. Kiountouzis, Analyzing information security awareness through network association, in: Proceedings of the 7th International Conference on Trust, Privacy and Security in Digital Business. Bilbao, Spain, August 30-31, 2010, pp. 227–237.

[89] R.J. Mejias, An integrative model of information security awareness for assessing information system security risk, in: Proceedings of the 45th Hawaii International Conference on System Sciences. Maui, HI, USA, January 4-7, 2012.

[90] L. Li, L. Xu, W. He, Y. Chen, H. Chen, Cyber security awareness and its impact on employee's behaviour, in: Proceedings of the International Conference on Research and Practical Issues of Enterprise Information Systems. Vienna, Austria, December 13–14, 2016, pp. 103–111.

[91] C.W. Yoo, G.L. Sanders, Exploring the influence of flow of psychological ownership on security education, training and awareness effectiveness and security compliance, 108, 2018, pp. 107–118,

[92] J. Simonet, S. Teufel, The influence of organizational, social and personal factors on cybersecurity awareness and behaviour of home computer users, in: Proceedings of the 34th International Conference on ICT Systems Security and Privacy Protection. Lisbon, Portugal, June 25-27, 2019, pp. 194–208.

[93] H.A. Kruger, S. Flowerday, L. Drevin, T.T. Steyn, An assessment of the role of cultural factors in information security awareness, in: Proceedings of the Information Security South Africa Conference. Johannesburg, South Africa, August 15-17, 2011.

[94] P. Tarwireyi, S. Flowerday, A. Bayaga, Information security competence test with regards to password management, in: Proceedings of the Information Security for South Africa. Johannesburg, South Africa, August 15-17, 2011.

[95] A. Farooq, J. Isoaho, S. Virtanen, J. Isoaho, Information security awareness in educational institution: An analysis of students'individual factors, in: Proceedings of the IEEE Trustcom/BigDataSE/ISPA. Helsinki, Finland, August 20-22, 2015.

[96] W.D. Kearney, H.A. Kruger, Can perceptual differences account for enigmatic information security behaviour in an organisation?, Comput. Secur. 61 (2016) 46–58.

[97] Z. Ahmad, M. Norhashim, O.T. Song, L.T. Hui, A typology of employees'information security behaviour, in: Proceedings of the 4th International Conference on Information and Communication Technology. Bandung, Indonesia, May 25-27, 2016.

[98] D. Ki-Aries, S. Faily, Persona centered information security awareness, Comput. Secur. 70 (2017) 663–674.

[99] A. Bostan, I. Akman, ICT user and usage characteristics and email security awareness, in: Proceedings of the International Conference on Electronics, Computer and Computation. Ankara, Turkey, November 7-9, 2013.

[100] H. Lee, O. Na, S. Sung, H. Chang, An analysis study on security activity changes by security accident, in: Proceedings of the 17th International Conference on Electronic Commerce. Seoul, South Korea, August 3-5, 2015, pp. 1–7.

[101] W. Sung, S. Kang, An empirical study on the effect of information security activities: Focusing on the technology, institution and awareness, 2017, pp. 84–93,

[102] R.R.J. Trim, Y. Lee, The role of B2B marketers in increasing cyber security awareness and influencing behavioural change, Ind. Mark. Manag. 83 (2019) 224–238.

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

[104] N.A.G. Arachchilage, S. Love, Security awareness of computer users: A phishing threat avoidance perspective, Comput. Hum. Behav. 38 (2014) 304–312.

[105] R. Kuo, EMRS adoption: Exploring the effects of information security management awareness and perceived service quality, Health Policy Technol. 7 (4) (2018) 365–373.

[106] M.E. Thomson, R. von Solms, Information security awareness: Educating your users effectively, Inf. Manag. Comput. Secur. 6 (4) (1998) 167–173.

[107] M.W. Kranenbarg, A. van der Laan, C. de Poot, M. Verhoeven, W. van der Wagen, G. Weijters, in: R. Leukfeldt (Ed.), Individual Cyber Crime Offenders, the Human Factor in Cybercrime and Cybersecurity, Eleven International Publishing, Hague, Netherlands, 2017, pp. 23–31.

[108] ENISA, Cybersecurity culture guidelines: Behavioural aspects of cybersecurity, 2018, https://www.thehaguesecuritydelta.com/media/comhsd/report/228/document/WP2012-O-3-3-2-Review-of-Behavioural-Sciences-Researchin-the-Field-of-Cybersecurity.pdf.

[109] H. Kruger, L. Drevin, T. Steyn, Email security awareness- a practical assessment of employee behaviour, in: Proceedings of the 5th World Conference on Information Security Education. West Point, NY, USA, June 19-21:33-40, 2007.

[110] M.A. Tariq, J. Brynielsson, H. Artman, The security awareness paradox: A case study, in: Proceedings of the International Conference on Advances in Social Networks Analysis and Mining. Beijing, China, August 17-20, 2014.

[111] M. Harbach, S. Fahl, M. Smith, Who's afraid of which bad wolf? A survey of IT security risk and awareness, in: Proceedings of the IEEE 27th Computer Security Foundations Symposium. Vienna, Austria, July 19-22, 2014.

[112] M. Hassanzadeh, N. Jahangiri, B. Brewster, A conceptual framework for information security awareness, assessment, and training, in: B. Akhgar, H.R. Arabnia (Eds.), Emerging Trends in ICT Security, Morgan Kaufmann, Burlington, MA, USA, 2014, pp. 99–110.

[113] X. Bellekens, A. Hamilton, P. Seeam, K. Nieradzinska, Q. Franssen, A. Seeam, Pervasive e-health services: A security and privacy risk awareness survey, in: Proceedings of the International Conference on Cyber Situational Awareness, Data Analytics and Assessment. London, UK, June 13-14, 2016.

[114] J.M. Torres, J.M. Sarriegi, J. Hernantes, A. Lauge, Steering security through management, in: Proceedings of the 6th International Conference on Trust, Privacy and Security in Digital Business. Linz, Austria, September 3-4, 2009, pp. 95–104.

[115] Algosec, The state of automation in security, 2016, https://www.algosec.com/wp-content/uploads/2016/03/The-State-of-Automation-in-Security-Survey-Final.pdf.(Accessed on 25 March 2023).

[116] O.A. Osoba, W. Welser, The risk of artificial intelligence to security and the future of work, 2017, https://cybersec4europe.eu/wp-content/uploads/2020/04/D9.6-SME-cybersecurity-awareness-program-1-V-1.0-Submitted-1.pdf.(Accessed on 25 March 2023).

[117] G. O˘g¨uţç¨u, ¨O.M. Testik, O. Oumout Chouseinoglou, Analysis of personal information security behaviour and awareness, Comput. Secur. 56 (C) (2016) 83–93.

[118] K. Solic, B. Tovjanin, V. Ilakovac, Assessment methodology for the categorization of ICT system users security awareness, in: Proceedings of the 35th International Convention MIPRO. Opatija, Croatia, May 21-25, 2012.

[119] B.D. Cone, C.E. Irvine, M.F. Thompson, T.D. Nguyen, A video game for cybersecurity training and awareness, Comput. Secur. 26 (1) (2007) 63–72.

[120] W.A. Labuschagne, I. Burke, N. Veerasamy, M.M. Eloff, Design of cyber security awareness game utilizing a social media framework, in: Proceedings of the Information Security for South Africa. Johannesburg, South Africa, August 15-17, 2011.

[121] T. Denning, A. Lerner, A. Shostack, T. Kohno, Control-AltHack: The design and evaluation of a card game for computer security awareness and education, in: Proceedings of the ACM SIGSAC Conference on Computer & Communications Security. Berlin, Germany, November 48, 2013, pp. 915–928.

[122] E.S. Ruboczki, How to develop cloud security awareness, in: Proceedings of the 10th Jubilee International Symposium on Applied Computational Intelligence and Informatics. Timisoara, Romania, May 21-23, 2015.

[123] V.N. Mathoosoothenen, J.S. Sundaram, R.A. Palanichamy, S.N. Brohi, An integrated real-time simulated ethical hacking toolkit with interactive gamification capabilities and cyber security educational platform, in: Proceedings of the International Conference on Computer Science and Artificial Intelligence. Jakarta, Indonesia, December 5-7, 2017, pp. 199–202.

[124] F. Alotaibi, S. Furnell, I. Stengel, M. Papadaki, Enhancing cyber security awareness with mobile games, in: Proceedings of the 12th International Conference for Internet Technology and Secured Transactions. Cambridge, UK, December 11-14, 2017.

[125] D. Huynh, P. Luong, H. Iida, R. Beuran, Design and evaluation of a cybersecurity awareness training game, in: Proceedings of the 16th IFIP TC 14 International Conference. Tsukuba City, Japan, September 18-21, 2017, pp. 183–188.

[126] E.G.B. Gjertsen, E.A. Gjære, M. Bartnes, W.R. Flores, Gamification of information security awareness training, in: Proceedings of the 3rd International Conference on Information Systems Security and Privacy. Porto, Portugal, February 19-21, 2017.

[127] V. Visoottiviseth, R. Sainont, T. Boonnak, V. Thammakulkrajang, POMEGA: Security game for building security awareness, in: Proceedings of the 7th ICT International Student Project Conference. Nakhon Pathom, Thailand, July 11-13, 2018.

[128] D. Filipczuk, C. Mason, S. Snow, Using a game to explore notions of responsibility for cyber security in organizations, in: Proceedings of the CHI Conference on Human Factors in Computing Systems. Glasgow, Scotland, UK, May 4-9, 2019, pp. 1–6.

[129] J.R. Cole, T. Pence, J. Cummings, E. Baker, Gamifying security awareness: A new prototype, in: Proceedings of the International Conference on Human-Computer Interaction. Orlando, Florida, USA, July 26-31, 2019.

[130] S. Scholefield, L. Shepherd, Gamification techniques for raising cyber security awareness, in: Proceedings of the 21st International Conference on Human-Computer Interaction. Orlando, Florida, USA, July 26-31, 2019, pp. 191–201.

[131] M. Bada, J.R.C. Nurse, Developing cybersecurity education and awareness programmers for small and medium-sized enterprises (SMEs), Inf. Comput. Secur. 27 (3) (2019) 393–410.

[132] N. Zargham, M. Bahrini, G. Volkmar, D. Wenig, K. Sohr, R. Malaka, What could go wrong? Raising mobile privacy and security awareness through a decision-making game, in: Proceedings of the CHI PLAY. Barcelona, Spain, October 22-25, 2019, pp. 805–812.

[133] M. Maurer, A. De Luca, S. Kempe, Using data type based security alert dialogs to raise online security awareness, in: Proceedings of the Seventh Symposium on Usable Privacy and Security, Pittsburgh, PA USA, July 20-22, 2011, pp. 1–13.

[134] M. Serrhini, A. Dargham, A.A. Ait-Moussa, Improve security of browser with stand-alone e-learning awareness application, in: Proceedings of the International Conference on Multimedia Computing and Systems. Tangier, Morocco, May 10-12, 2012.

[135] M. Potgieter, C. Marais, M. Gerber, Fostering content relevant information security awareness through browser extensions, in: Proceedings of the 8th IFIP World Conference on Information Security Education. Auckland, New Zealand, July 8-10, 2013, pp. 58–67.

[136] D. Malandrino, A. Petta, V. Scarano, L. Serra, R. Spinelli, B. Krishnamurthy, Privacy awareness about information leakage: Who knows what about me?, in: Proceedings of the 12th ACM Workshop on Privacy in the Electronic Society, Berlin, Germany, November 4, 2013, pp. 279–284.

[137] A. Tolnai, S. von Solms, Solving security issues using information security awareness portal, in: Proceedings of the International Conference for Internet Technology and Secured Transactions. London, UK, November 9-12, 2009.

[138] P.K.A. Sari, A. Prasetio, Knowledge sharing and electronic word of mouth to promote information security awareness in social network site, in: Proceedings of the International Workshop on Big Data and Information Security. Jakarta, Indonesia, September 23-24, 2017.

[139] A. Smith, M. Papadaki, S.M. Furnell, Improving awareness of social engineering attacks, in: Proceedings of the 8th World Conference on Information Security Education. Bento Gonçalves, Brazil, July 27-31, 2009, pp. 249–256.

[140] B. Endicott-Popovsky, I. Orton, K. Bailey, D. Frincke, Community security awareness training, in: Proceedings of the Sixth Annual IEEE SMC Information Assurance Workshop. West Point, NY, USA, June 15-17, 2005.

[141] A.J. DodgeCarver Jr., R.C.C. Ferguson, Phishing for user security awareness, Comput. Secur. 26 (1) (2007) 73–80.

[142] Y. Chen, Using anomalous data to foster conceptual change in security awareness, in: Proceedings of the International Symposium on Intelligent Signal Processing and Communication Systems. Kanazawa, Japan, January 7-9, 2009.

[143] S. Mamonova, R. Benbunan-Fich, The impact of information security threat awareness on privacy protective behaviour, Comput. Hum. Behav. 83 (C) (2018) 32–44.

[144] D.D. Maeyer, Setting up an effective information security awareness programme, in: Proceedings of the SECURE Conference. Warsaw, Poland, September 25-27, 2007, pp. 49–58.

[145] A. Liska, Fusing internal and external intelligence, in: Building an Intelligence- Led Security Program, Syngress:123-137, 2014.

[146] S. Chaudhary, S. Kompara, V. Pape, M. Gkioulos, Properties for cybersecurity awareness posters' design and quality assessment, in: Proceedings of the 17th International Conference on Availability, Reliability and Security, ARES 2022, Vienna, Austrai, August, 2022, pp. 23–26.

[147] S.G. Chaudhary, V. Gkioulos, S. Katsikar, Developing metrics to assess the effectiveness of cybersecurity awareness program, J. Cybersecur. 8 (1) (2022) tyac006.

[148] M. Evans, L.A. Maglara, Y. He, H. Janicke, Human behaviour as an aspect of cyber security assurance, Secur. Commun. Netw. 9 (17) (2016) 4667–4679.

[149] V. Andrews, Analyzing awareness on data privacy, in: Proceedings of the ACM Southeast Conference. Kennesaw, Georgia, USA, April 18-20:, 2019, pp. 198–201.

[150] S.M. Furnell, A.G. Warren, P.S. Dowland, Improving security awareness through computer-based training, in: C. Irvine, H. Armstrong (Eds.), Security Education and Critical Infrastructures, Springer, New York, US, 2003, pp. 287–301.

[151] L. Jixing, W. Yu, Q. Bin, Discussion on cyber security awareness and awareness model building based on connectionism, in: Proceedings of the IEEE 4th Information Technology and Mechatronics Engineering Conference. Chongqing, China, December 14-16, 2018.

[152] W.A. Al-Hamdani, Assessment of need and method of delivery for information security awareness program, in: Proceedings of the 3rd Annual Conference on Information Security Curriculum Development. Kennesaw, GA, USA, September 22-23, 2006, pp. 102–108.

[153] E. Kritzinger, E. Smith, Information security management: An information security retrieval and awareness model for industry, Comput. Secur. 27 (5–6) (2008) 224–231.

[154] S. Chaudhary, P. Sebastian, M. Kompara, G. Kavallieratos, V. Gkioulos, D3.19 guidelines for enhancement of societal security awareness, 2022, https://cybersec4europe.eu/wp-content/uploads/2022/04/D3.19-Guidelines-for-Enhancement-of-Societal-Security-Awareness_v1.0_submitted.pdf. (Accessed on 25 March 2023).

[155] U. Gattiker, Can an early warning system for home users and SMEs make a difference? A field study, in: Proceedings of the International Workshop on Critical Information Infrastructures Security. Samos Island, Greece, August 31 - September 1, 2006.

[156] L. Ngo, W. Zhou, A. Chonka, J. Singh, Assessing the level of I.T, security culture improvement: results from three Australian SMEs, in: Proceedings of the 35th Annual Conference of the IEEE Industrial Electronic Society. Porto, Portugal, November 3-5, 2009.

[157] L.E. S´anchez, A. Santos-Olmo, E. Fern´andez-Medina, M. Piattini, Security culture in small and medium-size enterprise, in: Proceedings of the CENTERIS. Viana do Castelo, Portugal, October 20-22, 2010, pp. 315–324.

[158] L. Freeman, The utilization of information systems security in SMEs in the south east of Ireland, in: A. DAtri, M. de Marco, A. Braccini, F. Cabiddu (Eds.), Management of the Interconnected World, Physica-Verlag HD, 2010, pp. 121–128.

[159] T. Gundu, S.V. Flowerday, Ignorance to awareness: Towards an information security awareness process, South African Inst. Electr. Eng. 104 (2) (2013) 69–79.

[160] H. Shih, X. Guo, K. Lai, T.C.E. Cheng, Taking promotion and prevention mechanisms matter for information systems security policy in Chinese SMEs, in: Proceedings of the 2nd International Conference on Information Management. London, UK, May 7-8, 2016.

[161] A. Tawileh, J. Hilton, S. McIntosh, Managing information security in small and medium sized enterprises: A holistic approach, in: N. Pohlmann, H. Reimer, W. Schneider (Eds.), Securing Electronic Business Processes, Springer Vieweg Verlag, 2010, pp. 331–339.

[162] R. Groner, P. Brune, Towards an empirical examination of IT security infrastructures in SME, in: Proceedings of the 17th Nordic Conference on Secure IT Systems. Karlskrona, Sweden, October 31- November 2, 2012.

[163] S. Parkin, A. Fielder, A.P. Ashby, Pragmatic security: Modelling IT security management responsibilities for SME archetypes, in: Proceedings of the 8th ACM CCS International Workshop on Managing Insider Security Threats. Vienna, Austria, October, 24-28.

[164] E.Y. Yeldirim, G. Akalp, S. Aytac, N. Bayram, Factors influencing information security management in small- and medium-sized enterprises: A case study from Turkey, Int. J. Inf. Manage. 31 (4) (2011) 360–365.

[165] A. Blau, The behavioral economics of why executives underinvest in cybersecurity, 2017, https://hbr.org/2017/06/the-behavioral-economics-of-why-executivesunderinvest-in-cybersecurity. (Accessed on 20 September 2020).

[166] I. Lopes, P. Oliveira, Understanding information security culture: A survey in small and medium sized enterprises, in: A. Rocha, A. Correia, ´F. Tan, K. Stroetmann (Eds.), New Perspectives in Information Systems and Technologies, Springer International Publishing, Switzerland, 2014, pp. 277–286.

[167] L. Spitzner, D. deBeaubien, A. Ideboen, The rising era of awareness training, 2019, https://adcg.org/wp-content/uploads/2020/02/SANS-SecurityAwareness-Report-2019.pdf. (Accessed on 20 September 2020).

[168] J.P. Pironti, Developing an information security and risk management strategy, 2010, https://www.isaca.org/resources/isaca-journal/pastissues/2010/developing-an-information-security-and-risk-managementstrategy. (Accessed on 20 September 2020).

[169] J. Schroeder, Challenges faced by organizations, in: Advanced Persistent Training: Take Your Security Awareness Program to the Next Level, A Press, Edinburgh, UK, 2017, p. 1, 1-6.

[170] D. Aitel, Why you shouldn't train employees for security awareness, 2012, https://www.csoonline.com/article/2131941/why-you-shouldn-t-trainemployees-for-security-awareness.html. (Accessed on 20 September 2020).

[171] J.M. Haney, W.G. Lutters, Skills and characteristics of successful cybersecurity advocates, in: Proceedings of the Workshop on Security Information Workers, Symposium on Usable Privacy and Security (SOUPS), Santa Clara, CA, USA, July 12-14, 2017, pp. 1663–1670.

[172] M. Eminağgaoğlu, E. Uçar, S. Eren, The positive outcomes of information security awareness training in companies-a case study, Inf. Secur. Tech. Rep. 14 (4) (2009) 223–229.

[173] J. Kaur, N. Mustafa, Examining the effects of knowledge, attitude and behavior on information security awareness: A case on SME, in: Proceedings of the 3rd International Conference on Research and Innovation in Information System. Kuala Lumpur, Malaysia, November 27-28, 2013.

[174] ISF 30, From promoting awareness to embedding behaviours: Secure by choice, not by chance, 2020, ISF 30. https://www.securityforum.org/research/from-promotingawareness-to-embedding-behaviours/. (Accessed on 20 September 2020).

[175] E. Albrechtsen, A quality study of users'view on information security, Comput. Secur. 26 (4) (2007) 276–289.

[176] N. Farvaque, E. Voss, M. Lefebvre, K. Schutze, Guide for training in SMEs. DG employment, social affairs and equal opportunities, Brussels, Belgium, 2009, 2009, https://ec.europa.eu/social/BlobServlet?docId=3074. (Accessed on 20 September 2020) & langId=en.