Proposal No. 830929 Project start: February 1, 2019

Call H2020-SU-ICT-03-2018 Project duration: 42 months

Cyber Security for Europe

D9.6

SME cybersecurity awareness program 1

Document Identification	
Due date	31 March 2020
Submission date	31 March 2020
Revision	1.0

Related WP	WP9	Dissemination Level	PU
Lead Participant	NTNU	Lead Author	Sunil Chaudhary
Contributing Beneficiaries	NTNU	Related Deliverables	-

Abstract: This document provides a systematic literature review of previously executed studies that focused on cybersecurity awareness across small and medium-sized enterprises within the European Union. The study seeks to: (i) identify and classify the research papers published on the topic of cybersecurity awareness, (ii) analyse and evaluate the identified studies, (iii) summarise the detailed research results, and (iv) to make recommendations for future research.

This document is issued within the CyberSec4Europe project. This project has received funding from the European Union's Horizon 2020 Programme under grant agreement no. 830929. This document and its content are the property of the CyberSec4Europe Consortium. All rights relevant to this document are determined by the applicable laws. Access to this document does not grant any right or license on the document or its contents. This document or its contents are not to be used or treated in any manner inconsistent with the rights or interests of the CyberSec4Europe Consortium and are not to be disclosed externally without prior written consent from the CyberSec4Europe Partners. Each CyberSec4Europe Partner may use this document in conformity with the CyberSec4Europe Consortium Grant Agreement provisions and the Consortium Agreement.

The information in this document is provided as is, and no warranty is given or implied that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

Executive Summary

The use of information and communication technologies across enterprises proliferates continuously, as it enables the development of new business models and the enhancement of operational and commercial activities. Nevertheless, this practice induces new vulnerabilities, which require the deployment of suitable countermeasures, in order to be treated and prevent their exploitation by various threat agents. Larger organisations possess both the resources and often the maturity, to establish the required mechanisms for continuous monitoring and enhancement of holistic cybersecurity programs. However, small and medium-sized enterprises, more often than not, lack both the resources and the incentives to prioritise this practice, while they constitute a significant portion of the European economy, both numerically and in terms of revenue.

As the European digital value and digital supply chains increase in complexity and cross border/ market dependencies, the impact and spillovers of each cybersecurity incident become more severe. Furthermore, prior studies have shown that numerous security breaches occur due to negligence or nescience of the personnel within an organisation and that many times attackers structure malicious actions by exploiting one or more human factor weaknesses. To this end, this report focuses on the systematic collection and analysis of prior studies on cybersecurity awareness for small and medium-sized enterprises across the European Union.

Initially, we provide a brief introduction to the core concepts of cybersecurity awareness, focusing on its various dimensions and levels, also discussing a corresponding maturity model. Accordingly, we present the selected methodology and the articles that have been collected and analysed, providing for each of them the objectives of the authors, the selected methodology and their core findings. Consequently, we present a similar analysis for articles that focused on small and medium-sized enterprises but have been targeted outside the European Union in order to interlard the presented findings and support their comparative analysis. Finally, the report presents a summary of results and discussion across the major findings, also providing recommendations for future work.

Document information

Contributors

Name	Partner
Vasileios Gkioulos	NTNU
Sunil Chaudhary	NTNU

Reviewers

Name	Partner
David Goodman	TDL
Stephan Krenn	AIT
Jozef Vyskoc	VAF
Ahad Niknia (High-level review)	GUF

History

0.01	2019-06-28	Vasileios Gkioulos	1st Draft
0.02	2020-02-14	Sunil Chaudhary	2nd Draft
0.03	2020-02-15	Vasileios Gkioulos	1st Version
0.04	2020-03-15	Vasileios Gkioulos	1st After Review
0.05	2020-03-23	Vasileios Gkioulos	Integration of review comments
0.06	2020-03-26	Vasileios Gkioulos	Final version
1.0	2020-03-30	Ahad Niknia	High-level review, final check and preparation for submission

Table of Contents

List of Figures

List of Tables

List of Acronyms

B	**BYOD**	Bringing Your Own Device
C	**CES**	Cyber Essentials Scheme
	CSA	Cyber Security Awareness
	CSF	Critical Security Factor
E	**EC**	European Commission
	EU	European Union
G	**GDPR**	General Data Protection Regulation
	GDT	General Deterrence Theory
I	**ICT**	Information and Communication Technology

	IEC	International Electrotechnical Commission
	IS	Information System
	iSC	Implanted Security Culture
	ISMS	Information Security Management System
	ISO	International Organization for Standardization
	IT	Information Technology
	ICT	Information and Communication Technology
N	**NIST**	National Institute of Standards and Technology
P	**PMT**	Protection Motivation Theory
S	**SA**	Situation Awareness
	SMEs	Small and Medium-Sized Enterprises
	SMMEs	Small, Medium and Micro Enterprises
T	**TAM**	Technology Acceptance Model
	TPB	Theory of Planned Behavior
	TRA	Theory of Reasoned Action

1 Introduction

Nowadays, nearly all enterprises make extensive use of ICT systems and the internet, such as for staff email addresses, company websites, online banking and other online services, to perform daily operations. Indeed, the adoption of ICT systems and the internet have offered significant opportunities to enterprises, more importantly, to broaden their business horizons; however, they also expose 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 (known as bring your own device, or BYOD), encounter security breaches more frequently [1].

While advanced cyberattacks usually target large enterprises that possess strategic resources, cybercrimes also pose threats to small and medium-sized enterprises (SMEs) [2] as SMEs have started to face the same cybersecurity threats as their larger counterparts [3]. As a matter of fact, SMEs are hardest hit by cyber breaches, although they may not make it to headline news. Although metrics regarding the impact of the attacks are not readily available, by the current number of estimated and reported incidents, over 77% of cyberattacks and cybercrimes target SMEs and to make the problem worse, around 44% of SMEs do not see them as a risk [4]. Those SMEs that have direct or indirect relationships with large organisations become more vulnerable to security breaches mainly because attackers ultimately plan to reach large organisations by using smaller enterprises as a gateway [4] [5].

Present-day SMEs use, produce, and store large amounts of sensitive data, and highly rely on cloud-based platforms and services [3] for their everyday operations. However, at the same time, they face resource constraints due to which they cannot afford adequate security levels [4] [6] and face difficulties with complying with regulatory standards like the General Data Protection Regulation (GDPR) [7]. Further, to compound the problem, there is a mindset among SMEs' executives and managers that cyber attackers prefer high profile organisations and not SMEs, so cybersecurity is less critical and may not be applicable to them [3]. Even while addressing security issues, SMEs only take into account the near future scope and focus for the provable threats focusing on costless or very cheap cybersecurity solutions [8]. These make them an attractive and lucrative target for cyber attacks.

Most enterprises agree that cyber attacks and cyber crimes are imminent threats, and should be of utmost importance. Nevertheless, in reality, their actions do not reflect that, and many of them fail to prioritise cybersecurity until they are directly affected by an incident. However, when a cyber breach happens, and the consequences become evident, they do become interested in the issue [9]. The problem with this *reactive approach* is that it requires considerable effort and resources to recover from the situation if recovery is possible at all. Therefore, it is the responsibility of every enterprise, including SMEs, to understand the impact of cyberattacks in order to keep its employees, clients, and stakeholders safe online and act *proactively* or *on time* to do that. One must keep in mind that even a single vulnerability may expose the entire enterprise to attackers. This becomes more serious in the case of SMEs, specifically, to small and micro enterprises that are less likely to recover from advanced cyber attacks [5]. To counteract a cyber attack demands multiple layers of security measures that include both technical measures and consideration of human aspects (i.e., to deal with the weakest link in the security chain) of security through, for example, security procedures and policies. It does not matter how many layers of sophisticated security measures an enterprise have been implemented, if employees misuse them, or bypass them deliberately due to negligence or recklessness. One of the most significant non-technical security measures is '*Cybersecurity awareness*' (CSA) that is used as a means for fostering good security behaviour and attitudes of employees and is the focus of this study. This research, however, will only focus on CSA for SMEs in Europe.

Technical security measures are essential for every enterprise, but it has also been readily recognised that cybersecurity is not just a technical problem, also evident from several security breaches caused by human errors. A majority of security problems occur due to *poor awareness, attitudes* or *behaviour* of employees, for instance, a study found out that 60% of personal data breaches occurred simply due to human errors [10].

In another similar study conducted in 2017 by Ponemon Institute with SMEs, around 54% of the participants said that the root cause of data breach in their company is negligent employees [11]. People making errors may be because they are not naturally equipped with skills, instincts and behaviours required to ensure appropriate protection and so need help to understand what they should be doing and learn how to do it [12]. Apart from that, two of the most compelling reasons for this are: people are either not aware of (or do not perceive) the risks, or, they do not know (or fully do not understand) the 'correct' behaviour [13].

Furthermore, *social engineering* has been a factor virtually in all cyber attacks [14], which, unfortunately, cannot be solved solely by technology. The technical measures will have limited use if the people involved in their lifecycle do not understand their security responsibilities and remain vulnerable to cyber threats. In a situation like this, CSA can play a crucial role in influencing the adoption of secure behaviour and attitudes, and a sense of responsibility towards cybersecurity. When people are made aware of cybersecurity in their area of work, this helps them to understand risks, and thus their ability to make decisive security decisions, respond, and accordingly improve. These informed and aware or qualified people will reduce human errors and security vulnerabilities, leading to proper security hygiene within an organisation. A key question, however, is "*what is the current status of* CSA*, preferably CSA for SMEs in Europe?*". Moreover, to answer this, we have used a systematic literature review, and have attempted to incorporate various dimensions of CSA in our answer.

A systematic literature review is suitable for study particularly 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 [15].

In our case, even though CSA has been a mature topic, at least from the accumulated literature perspective, not many research studies have been performed explicitly targeting CSA in SMEs. Therefore, through this study, we have tried to explore and recognise the areas, aspects and concerns of CSA in the context of SMEs that need further research attention, as well as pathways to achieve them based on the past research works on CSA, including those conducted for other contexts.

2 Small and medium-sized enterprises (SMEs)

According to the current definition provided by the European Commission (EC) [16], two main factors determine the categorisation of enterprises into medium-sized, small, and micro. These are:

i. The staff headcount
ii. The annual turnover or balance sheet total, following the latest approved accounting period and calculated on an annual basis

Accordingly, the limits for classification are defined as presented in Table 1.

Table 1: Margins for company classification [16].

Company category	Staff headcount	Turnover		Balance sheet total
Medium-sized	< 250	≤ 50m €	**OR**	≤ 43m €
Small	< 50	≤ 10m €		≤ 10m €
Micro	<10	≤ 2m €		≤ 2m €

Moreover, SMEs represent around 99% of the enterprises in the European Union (EU) and are considered as a key to economic growth, innovation, and job creation in Europe [17]. The Statista's report [18] estimated that there were approximately 25.1 million SMEs in the EU in 2018. It must be noted that the definitions of SMEs used outside the EU are different from the one presented above.

3 Cybersecurity awareness (CSA)

Before we delve into the systematic literature review, it is essential to clarify the concept of CSA mainly because of the inconsistencies found in many past studies. Similar to the B. Hanus, J.C. Windsor, and Y. Wu [19] study, we observed that most of the past research studies tried to shape the definition of CSA according to their need by emphasising one or multiple of the following determinants of security-related behaviours, that include:

- knowledge of threats and vulnerabilities
- overall knowledge of information security
- knowledge of countermeasures and safeguards
- understanding one's responsibilities
- understanding information security procedures and policies
- ability to comply with security measures
- understanding the importance of information security

Furthermore, there are research studies, for example, Vroom and von Solms [20] and Yildirim [21], that have interchangeably used security awareness for security education and training. No doubt, security education and training can influence raising awareness about cybersecurity issues, but they are not the same and have distinct differences (see [22] and [23] [24]). Such inconsistencies may have occurred primarily because different researchers considered different dimensions of CSA [19]. For instance, M.T. Siponen [9] has categorised the dimensions of CSA into the following five types:

1. *Organisational*
2. *General public*
3. *Socio-political*
4. *Computer ethical*
5. *Institutional education* (for details refer to [9]).

His classification is asserted on the belief that CSA should be of concern for everyone using IT services in the internet environment. He has further notified that there may not exist a clear or distinct border between these dimensions in every case - not to mention the non-technical nature of CSA and related areas so that many researchers do not cover CSA comprehensively or may not feel the need to cover it outside their scope of interest [9].

In general, CSA activities are used to communicate or disseminate security requirements and appropriate behaviour to people [13] so that they develop a certain level of scepticism when encountering a situation that is unorthodox or out of the ordinary [25]. CSA activities do not equal in-depth knowledge but are aimed at only directing the attention of individuals to security issues, realising their potential implications, and responding accordingly [22]. Such activities are usually directed towards broad audiences, who are mostly passive recipients of the information, while their motivation for participating and their understanding of the significance is also questionable. The learning achieved from CSA is short-term, immediate and specific unless the activities are repeatedly exercised [26]. CSA activities may not be as intensive as security training and education; nonetheless, even within CSA, the intensiveness and depth may vary depending on the security risks the audience is expected to encounter, as depicted in Figure 1.

Furthermore, the levels of CSA can be categorised as:

1. *perception* (i.e., the ability to sense and detect potential security risks)

2. *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 way); and
3. *projection* (i.e., the ability to project or predict the future course of security attacks to prevent potential risks from occurring) [27].

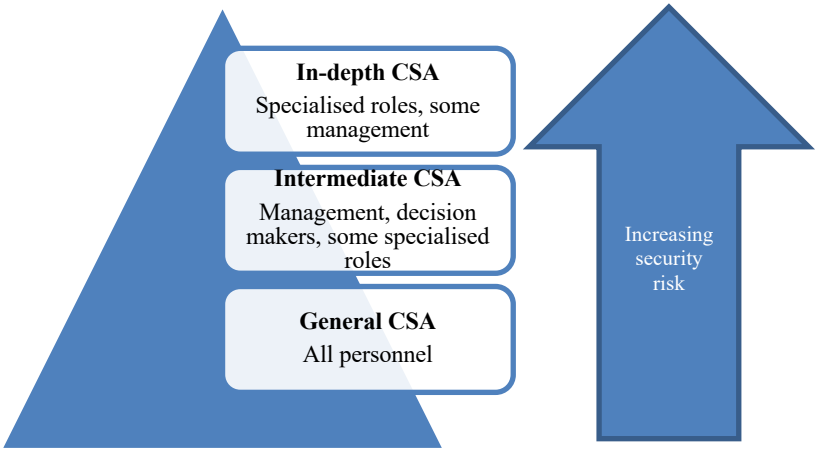

Figure 1: Depth of cybersecurity awareness [24]

The CSA content types and formats and their delivery/dissemination techniques may vary depending on the needs of the organisation and the target audiences.

Regarding the content types of CSA, *general* or *introductory* awareness may be suitable for all personnel and clients/customers; whereas decision-makers, management and personnel with specialised roles may require more *comprehensive* awareness content specific to their roles and responsibilities. Similarly, their formats can be in the forms of *promotional* (e.g., events, posters, games), *educational/interactive* (e.g., presentations, brief sessions, workshops), *informational* (e.g., leaflets, newsletters, website postings, emails), and *enforcing* (e.g., confidentiality agreements, required awareness exam or test) [28]. They can also be classified as *prescriptive* (i.e., in the form of checklists and is preferred for the organisational dimension), and *descriptive* (i.e., in the form of explanation and is preferred for other dimensions) [9].

Then, the delivery or dissemination techniques, in general, can be *instructor-led* (in which people listen to the instructor talk in real-time and is generally suitable for a limited group of audience, e.g., workshop and training), *paper-based* (it is a traditional method used to reach a large mass of audience at the organisational level, e.g., leaflets, newsletters, posters and pamphlets), and *computer-based* (it is a convenient way to deliver to a large or widely distributed group of people, e.g., website posting, video, games, and quizzes) [29] [30].

Further, the enactment of CSA can be through a *persuasive or soft approach* (i.e., persuade users to comply through motivations or rewards) or an *enforcing or hard approach* (i.e., compel users to comply through threats of sanctions) [31]. CSA audiences can be treated at different levels, based on multiple parameters which can include their background knowledge, operational needs, cognitive, mental and psychological qualities. For example, in an enterprise, general CSA can be targeted at the *organisational level*, then awareness needs specific to a particular department can be conducted at the *departmental level*; and finally, top executives and managers responsible for managing other users may need awareness at the *individual level* [24]. They can also be classified as *CSA for computer users* (i.e., target to desktop and laptop users) and *CSA for mobile phone users* (i.e., focus on smartphone users), since both computers and mobile phones are widely used to access the internet and perform organisational activities. However, they differ in, for example, their usability, situational awareness, and mobility. Regardless of the formats and types of CSA content, their message should be *simple* and *easy to understand*, *complete*, *correct*, *actionable (or compliable)*, and more importantly *relevant* and *meaningful* to the target audience. Similarly, their delivery

techniques should be *interactive* and *innovative* to engage audiences and be *inclusive* so that no subset of the audience feels left out.

Based on the SANS Security Awareness Maturity Model, an enterprise can lie in one of these five distinct stages, shown in Figure 2 (for details refer [32]).

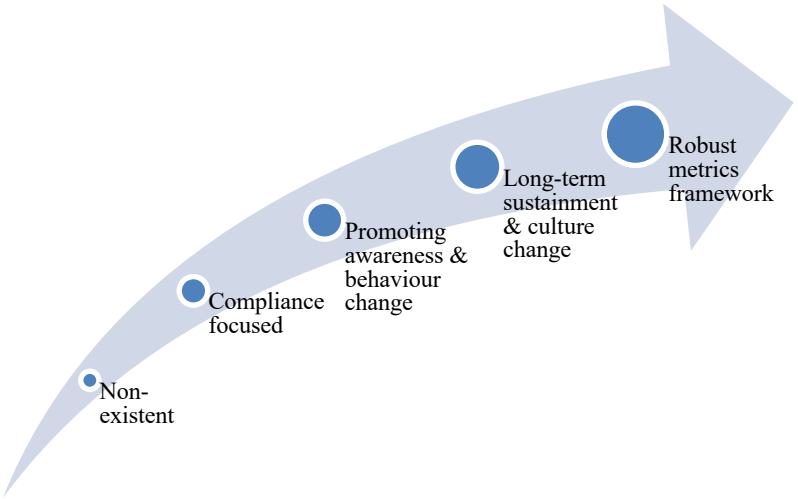

Figure 2: SANS security awareness maturity model [32]

4 Methodology

Undertaking this study, we utilised the method described by Okoli and Schabram [33] for conducting a systematic literature review of information systems research, also adopting procedural components from the studies presented in section "Background and related work". This method consists of the following steps (shown in Figure 3):

i. **Purpose of the literature review:** The first step in any review requires the reviewer to identify the purpose and intended goals of the review. This step is necessary for the review to be explicit to its readers.
ii. **Protocol and training:** For any review that employs more than one reviewer, the reviewers must be in agreement about the detailed procedure to be followed. This process requires both a written, detailed protocol document and training for all reviewers to ensure consistency in the execution of the review.
iii. **Searching for the literature:** The reviewer needs to be explicit in describing the details of the literature search and needs to explain and justify how the comprehensiveness of the search was assured.
iv. **Practical screen:** Also known as screening for inclusion, this step requires that the reviewer be explicit about what studies were considered for review, and which ones were eliminated without further examination (an essential part of any literature review). For excluded studies, the reviewer must state what the practical reasons were for their non-consideration and justify how the resulting review can still be comprehensive, given the exclusion criteria.
v. **Quality appraisal:** Also known as screening for exclusion, the reviewer needs to explicitly spell out the criteria for judging which articles are of insufficient quality to be included in the review synthesis. All included articles need to be scored for their quality, depending on the research methodologies employed by them.
vi. **Data extraction:** After all the studies that should be included in the review have been identified, the reviewers need to extract the applicable information from each study systematically.
vii. **Synthesis of studies:** Also known as analysis, this step involves combining the facts derived from the studies using appropriate techniques, whether quantitative, qualitative or both.

viii. **Writing the review:** In addition to the standard principles to be followed in writing research articles, the process of a systematic literature review needs to be reported in sufficient detail that the results of the review can be independently reproduced.

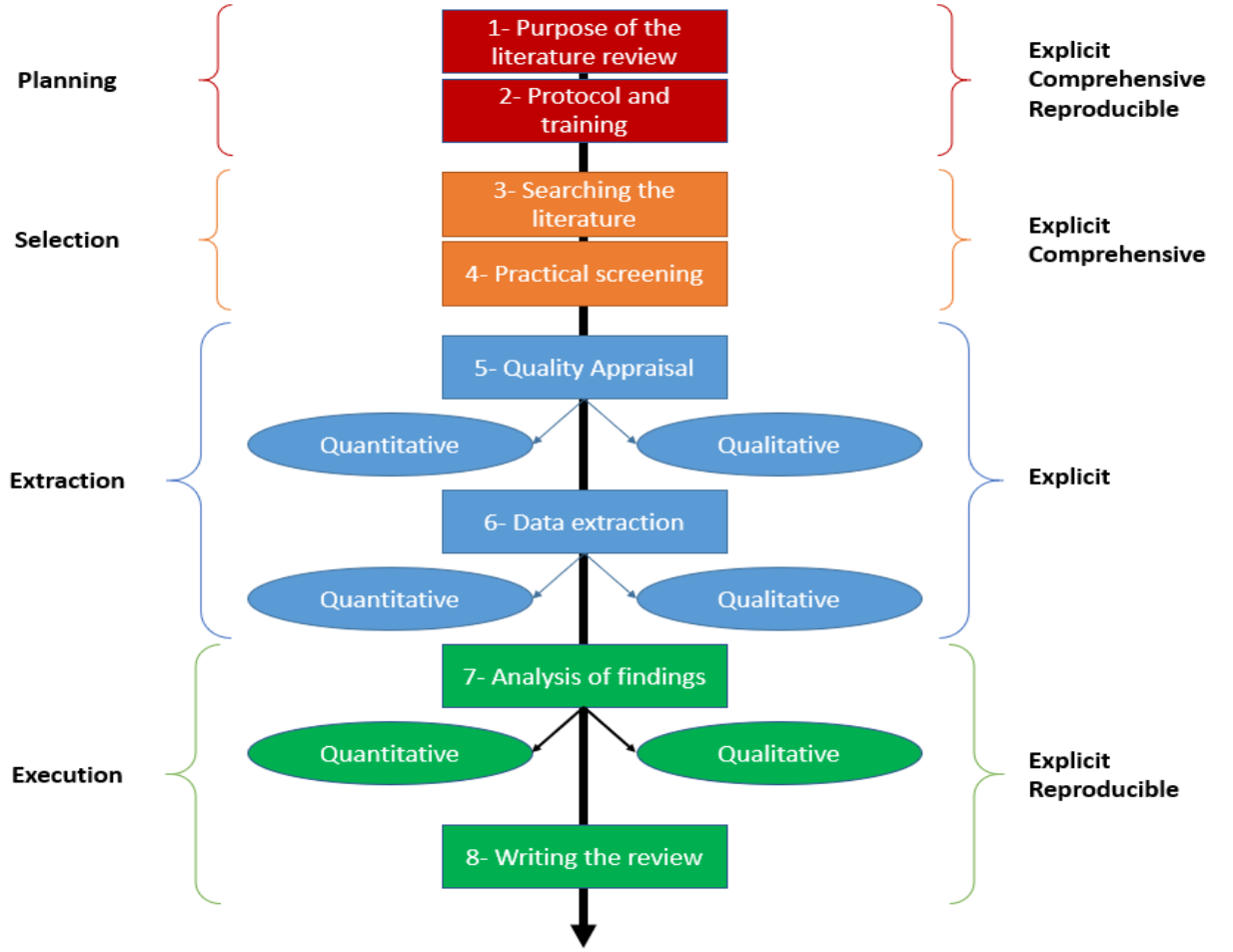

Figure 3: A systematic guide to literature review development [33]

5 Purpose of this literature review

The purpose of this study has been defined as: to analyse the existing studies concerning the current state of CSA, and the mechanisms employed for its enhancement, primarily across but also outside Europe, with particular focus on SMEs and their position within digital value/supply chains. Complementary to this, we seek to investigate research tracks, publications, methods, trends, and to make recommendations for future research. Accordingly, the executed tasks seek to satisfy the following explicit goals:

i. To identify and classify the research papers published on the topic of CSA.
ii. To analyse and evaluate the identified studies, and to summarise the detailed research results in terms of:
    a. Which technologies and focus areas have been targeted by prior security awareness studies?
    b. Which research methodologies have been preferred for their studies?
iii. To make recommendations for future research.

6 Searching for the literature, practical screening, and quality appraisal

Collecting relevant literature that captures the essence of 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 [15]. In order to determine such published works of literature, the reviewers have to be clear with the following fundamental aspects: *where* and *how* to locate the relevant literature, and their *selection criteria* [15] [34].

The sources of selected literature should be those with a reputation for quality [15]. Since justifying the quality of any individual piece of literature may be difficult and controversial, therefore, for this study, we have selected the following academic research databases, which are generally reputed for publishing quality works: IEEE Xplore, ACM Digital Library, ScienceDirect, and Scopus.

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

i. Security + awareness + SME
ii. Security + awareness + "Small and medium-sized enterprises"
iii. Security + awareness

We believe that these three keyword groups are sufficient to retrieve the necessary literature. The earlier two keyword groups were used for collecting CSA papers that particularly focused 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 does not remain left out. 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 the title or keywords or abstract of the papers.

For the selection of papers, we defined several exclusion criteria, as follows:

i. Articles published in languages other than English.
ii. Duplicate articles that appear across the examined scientific databases.
iii. Reports
iv. Presentations
v. Editorials
vi. Posters
vii. The article must be directly related to CSA studies/results/tools directed towards SMEs.
viii. Articles that have studied topics related to CSA in various types of user, including SMEs, are excluded since their results do not solely represent SMEs but are influenced by other users as well.
ix. Even those articles that do not mention the type of organisation where the study was conducted, were excluded from our review; however, the suggestions made by them that we believe can be equally useful and relevant for SMEs have been used to enhance our analysis and scrutiny.

However, no exclusion criteria were defined following the year of publication, publisher, and author affiliation. Among the studies reviewed, 13 for European SMEs and 7 for non-European SMEs papers, met the inclusion criteria.

7 Background and related work

Only a small number of research studies exists that have dealt with CSA for SMEs, and those that dealt with SMEs based within Europe are even less in number. Research studies that dealt with SMEs within and outside Europe and some related studies have been selected for further analysis in the upcoming sections.

There are only a few studies that have used systematic literature review for studying CSA and its related domains. For example, B. Lebek et al. [35] conducted a systematic literature review to identify the behavioral theories that have widely been implemented to study human behaviour for CSA purposes, and their study resulted in the following four theories:

- Theory of Reasoned Action (TRA) / Theory of Planned Behaviour (TPB)
- General Deterrence Theory (GDT)
- Protection Motivation Theory (PMT), and
- Technology Acceptance Model (TAM).

Then, P. Mayer, A. Kunz, and M. Volkamer [36] utilised the study by B. Lebek et al. [35] as a base and performed a systematic literature review to determine the behavioural factors which exhibit a reliable effect in the information security context. They collected behavioural factors used by the behavioural theories that are most frequently studied in the information security context and then used *effect-size* to measure the effect of those behavioural factors in the information security context. They identified 11 out of 14 behavioural factors that they used for their investigation to be reliably associated with secure information system (IS) related behaviour. However, they further ascertained that most of those factors, nine out of eleven, (i.e., "self-efficacy", "response cost", "response efficacy", "perceived severity of threats", "subjective norms", "perceived behavioural control", "perceived certainty of sanctions", "perceived severity of sanctions", and "perceived ease of use") exhibit mostly weak effects. Only two factors "*attitude*" and "*perceived usefulness*" were reliably associated with secure IS-related behaviour.

Another similar study is by H. Aldawood and G. Skinner [37], who used a literature review to identify various social engineering threats. Their findings revealed the lack of a budget for security to be a significant challenge in providing CSA to counteract social engineering. They recommended that organisations should not be limited to traditional types and techniques for CSA, for example, posters and screensavers, for all employees. Instead, they should select or design CSA programs depending on the role, responsibility and preference of the target audiences. Further, they mentioned that a new method like simulation could be utilised to explore the loopholes or gaps in a security chain of an organisation. Finally, they suggested that organisations can make use of methods like real case scenarios and case studies to raise their employees' awareness against innovative social engineering techniques. Although the findings and recommendations of this paper are valuable and relevant, they contradict each other. On the one hand, its findings reveal the budget to be a significant constraint to providing CSA, whereas it recommends adopting, for instance, simulation, personalised content types and dissemination techniques, as well as case scenarios/studies, all of which are both budget and time taxing methods.

Finally, a study that particularly dealt with SMEs was by T.K. Lejaka, A.D. Veiga, and M. Loock [38], who used a systematic literature review to investigate frameworks and their components that can be suitable for South African SMEs. Based on their study, they found that not a single CSA framework designed for South Africa fulfils the needs of SMEs in South Africa.

Apart from the last paper, all the studies followed similar steps as our study for their systematic literature review. Also, it is noticeable that the availability of relevant literature depends on how broad and mature the selected topic is. This can further be affected depending on the numbers and types of databases used for the relevant literature search.

8 Summary of overall research studies on CSA

Apart from the selected papers that discuss CSA in SMEs, we also briefly reviewed more than 100 papers related to CSA to determine the types of research that have been conducted on CSA and the utilised research methodologies. Most of the papers targeted computer users or undefined IS users, and only a few of them specifically targeted smartphone users.

8.1 Topics covered by past research studies on CSA

The topics covered by the reviewed past research works can be broadly classified into the five types, shown in Figure 4:

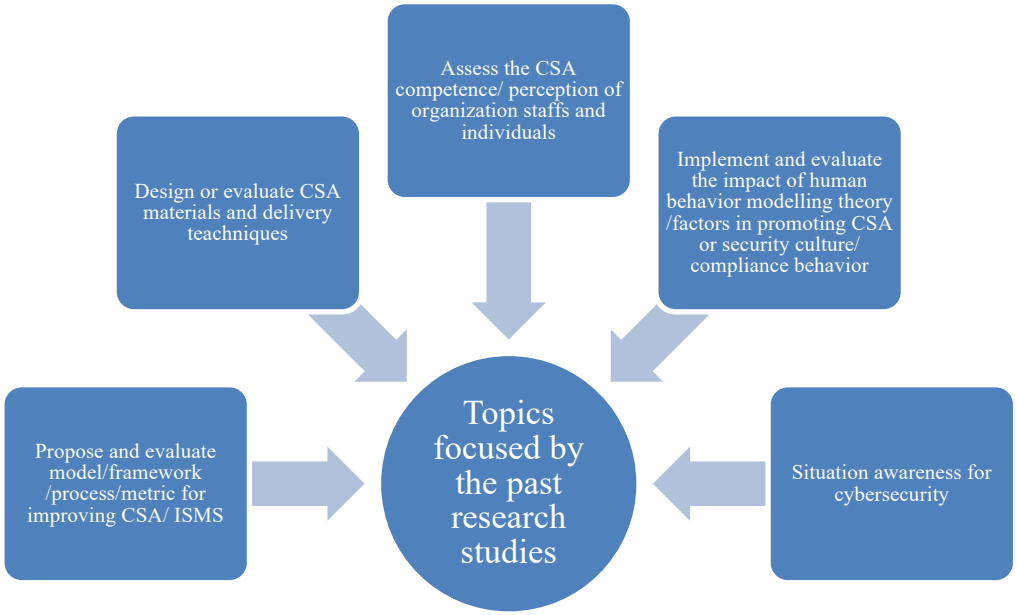

Figure 4: Topics covered by the past research works

8.1.1 Situational Awareness for cybersecurity

Some of the research works recognise and suggest situational awareness (SA) as being essential for successful decision-making in the cybersecurity domain. They cover topics like SA for network and cloud security, taxonomies of SA and elements for SA. They utilise mainly the visualisation of security-relevant events and phenomena, for example, anomaly detection, network traffic and intention recognition. 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.

8.1.2 Implement and evaluate the impact of human behaviour modelling theory/ factors in promoting CSA or security culture/ compliance behaviour

These research works utilise various behaviour modelling theories, for example, TRA / TPB, GDT, PMT, and TAM, and factors or determinants that promote CSA or security culture or compliance behaviour. They determine various factors like personal initiative, persuasion and social influence, encouragement, organisational support, cognitive aspects, age, work experience, culture, etc. as having an impact on CSA.

8.1.3 Assess the CSA competence/ perception of organisation staff and individuals

Many research works assess the CSA competence or perception of individuals and organisation staff. They cover topics like awareness about social engineering, organisation regulations and policies, password management, phishing, data privacy, social media security, email and cloud security, etc. All such studies find a lack of privacy and security awareness both in individuals and organisation staff. They conduct their studies in diverse types of organisations, such as insurance, healthcare, IT, banking, telecommunication, etc. They point out that there were misconceptions and stereotypical misunderstandings of cyberattacks among individuals and organisation staff. They suggest a severe need for relevant CSA programs/training for them.

Moreover, such programs or training should be arranged regularly, and their impact should be measured, and accordingly improved in the future.

8.1.4 Design or evaluate CSA delivery techniques

These studies propose, design and evaluate various materials and delivery techniques, for example, games, online portals, social media, web browser add-ons or plugin tools, online quizzes, etc., for an effective CSA. They mainly focus on computer and online-based learning techniques, that are interactive and demand the active participation of the audience during CSA training. The majority of studies recommend games to be effective for CSA. However, it is suggested that relying on mixed delivery methods, and a selection of methods based on an audience's preference can make CSA more effective.

8.1.5 Propose and evaluate model/framework / process/metric for improving CSA/ information security management system (ISMS)

These studies propose and evaluate models/frameworks/processes/metrics for the security understanding of organisations, assessment of IT security in an organisation, awareness programs, ICT system user security awareness, etc. Most of these studies use a literature review as the foundation for their conceptual or theoretical frameworks, which are later tested.

8.2 Preferred research methodology for the CSA research studies

Maybe due to human involvement, most studies implement user-study methodologies like a survey (mostly through a questionnaire) or an interview. They use user-study either in isolation or as a follow-up method to test their proposition/design. The second most popular research methodology is a literature review, mainly used for framework or model design. Other research methods used were: argumentative method, observation, case study, and method engineering.

9 Summary of the selected papers

After multiple rounds of screening, we selected 20 papers comprising 13 papers that deal with cybersecurity issues of SMEs within Europe and seven with a focus outside Europe. The research objectives, a summary of methodologies and findings of the selected papers are available in chronological order in Tables 2 & 3.

Among all the selected papers, only nine of them directly relate to CSA (references [39] [40] [41] [36] [42] [43] [44] [45] [46]). In contrast, the remaining 11 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. Similarly, five papers propose a model/framework/process (references [47] [40] [48] [49] [45]) and verify their proposition in SMEs; whereas other papers assess either the impact of specific parameters on the cybersecurity of SMEs or an overall security strategy/status/culture of SMEs.

9.1 Papers that deal with CSA for SMEs within Europe

Table 2: Summary of papers that deal with CSA for SMEs within Europe

Author	Objective	Methodology	Finding
U.E. Gattiker (2006) [39]	To study the impact of early alert systems in the security hygiene of SMEs.	Designed and hosted CASEScontact.org, to realise security awareness of SMEs and general people mostly from European countries. They targeted younger adults and teenagers. The website contained advisories and	Every user group is different, so must be served with different types of awareness content that are clear, consistent and relevant to them. More importantly, there should be alternatives to choose with content types and delivery methods. However, to gain the user's trust so that they comply with the awareness, the content types and delivery method should be of quality and

		security guides for home-users and SMEs.	innovative and need continuous adjustments and improvements.
A. Tawileh, J. Hilton, S. McIntosh (2007) [47]	To identify the challenges faced by SMEs that are impeding their implementation of information security management.	Proposed a holistic approach for the ISMS in SMEs and used a case study to support their proposition.	Due to resource (skilful human, financial or needed technology) constraints of SMEs, merely raising their awareness and understanding of security issues may not produce positive results. Proposed a holistic approach based on Soft Systems Methodology for ISMS in SMEs. Their proposition is dependent on the following factors: Customer of the system, Actors in the system, the transformation process that the system should undertake, World view upon which the system is based, Owner of the system, and Environmental constraints (i.e., CATWOE).
J.M. Torres, J.M. Sarriegi, and J. Hernantes (2009) [50]	To classify, by importance, 11 Critical Security Factors (CSFs) and 62 indicators that are important for the success of security management in SMEs. The outcomes can be used by IT administrators to build a personal security scorecard choosing the CSFs and indicators that fit best to improve the information security SMEs from technical, managerial and human aspects.	Surveyed 170 IT administrators from SMEs located in Spain using an online exploratory questionnaire. The questionnaire was answered anonymously.	Identified the following CSFs and their 62 indicators arranged in descending priority order: Security policies enforcement and compliance, Dynamic evaluation of implemented controls, Security integration, Security budget, Security implementation efficacy, Administrator competence, IS infrastructure security, Dynamic risk analysis, Security strategy, and Top management commitment. However, one must consider the resource constraints of SMEs, and recommend less complicated, scaled-down security management practices that can be implemented in a reasonable time frame and with available resources in SMEs.
L.E. Sánchez, A. Santos-Olmo, E. Fernández-Medin, M. Piattini (2010) [40]	To design and propose a model for installing security culture in SMEs, which they called "Implanted Security Culture (iSC)."	Reviewed and evaluated past models designed to establish a security culture in SMEs.	Designed a cost-effective model for installing security culture in SMEs. The model, along with technical and management aspects, also considered institutional aspect into account. The principal idea of this model is to examine the employees' knowledge through a series of security-related tests associated with ISMS regulation. Only those employees who passed the test (i.e., obtain 50% or above) and obtain a certificate to get access to the information system. More importantly, the employees must renew their certificate periodically, i.e., must attempt such tests periodically, to guarantee that the necessary level of security culture continues to be maintained.
A. Freeman and L. Doyle (2010) [41]	To investigate the perception of information security in SMEs and how they are handling IS security issues.	Used a quantitative approach and a postal questionnaire (using a Likert scale) for the data collection. The questionnaire was prepared based on the literature review and was organised into six sections examining:	Awareness of security is on the rise within SMEs (71.9%); however, senior management still does not have much involvement in the security process (only 57.1% of senior management receives proper reports on security issues). 10% of the companies outsourced their security and were most confident with their level of security protection. External attacks were more prevalent, and only 9.1% reported about internal

		organisational environment, Computer security environment, Computer security threats and technologies, Staff and training, Policies and procedures, and Further information. 100 SMEs within Ireland were selected randomly for the study and received responses from 57 of them.	attacks. More important, over 70% of the companies had people without a formal IT qualification responsible for security, and only 61.4% of the companies reported that security training was important or very important. Budget constraints, technical challenges/ complexity of products and lack of end-user awareness were identified as the three main obstacles that the SMEs felt they faced in terms of securing their organisation. Other obstacles mentioned were lack of internal security policies, lack of managerial support and unclear responsibilities.
R. Groner and P. Brune (2012) [48]	To develop and propose an IT security infrastructure framework especially suited for SME and to determine the requirements and boundary conditions that are relevant for its development.	Literature review of the past studies accompanied with interviews and discussions with experts in the IT security fields to develop the framework. Furthermore, to evaluate the practical value of the proposed model conducted an empirical study using a survey performed among SMEs (some large companies that are still considered to be medium-sized were also included) within Germany. A survey questionnaire was sent to 20 random companies and received anonymous responses from 15 of them.	Since SMEs have financial constraints, therefore, when developing any information security model or framework for SME, one should consider its cost-effectiveness, ease of use, technical complexity and benefit/cost ratio. Their proposed model consists of four layers: Information security threats perceived by IT stakeholders, Perceived importance of requirements, Adoption of IT security components, and Perceived quality of IT security components. Based on the empirical study, the importance of various IT security requirements was as follows (in descending order): authentication, authorisation, intrusion detection, immunity, security auditing, privacy, identification, integrity and non-repudiation. Similarly, the components were (in descending order): Network firewall, Directory services, Web proxy server, Demilitarized zone, Monitoring system, Transport layer encryption, Application firewall, Intrusion Prevention System, Network Access Control, Digital Signatures. Further, they found out that Application firewall has the highest benefit/cost ratio, is easy to use and technically less complex. Similarly, multi-factor authentication has the least benefit/cost ratio and is technically very sophisticated.
I. Lopes and P. Oliveira (2014) [51]	To study the security culture in SMEs. The study relied on the International Organization for Standardization (ISO) International Electrotechnical Commission (IEC) 270002:2005 to measure security culture. Enterprises that satisfy at least five parameters of the	Conducted a survey using a questionnaire distributed through email to 350 SMEs in Portugal and received valid answers from 307 of them. The SMEs selection was random. The Questionnaire was designed through a literature review.	52% of the surveyed companies had an internal department to handle IT issues, whereas 48% of the companies had outsourced to external parties to do the task. Only 9% of the companies had adopted security culture, whereas the remaining 91% did not. 54% of the companies without security culture had no plans to adopt security culture despite their belief that it is necessary. Even in those companies that have adopted security culture had their security measures implemented for the followings: electric failure protection, firewall, access passwords to the

	ISO standards are considered to have adopted information security culture.		network, cryptography, software update, information security policies, and disaster recovery plan.
S. Parkin, A. Fielder, and A. Shby (2016) [49]	To model the indirect costs of deploying security controls in SMEs to manage security threats. Used Cyber Essentials Scheme (CES) (it recommends addressing the following basic online cyber threats, Boundary Firewalls and Internet Gateways, Secure Configuration, Access Control, Malware Protection, and Patch Management) as a framework for basic cyber-security protections.	Used CES to model the framework, in which • Modelling security investment (includes Targets and attacks, and Controls) • Modelling indirect end-user costs (includes Morale, System performance, and Retraining), • Modelling SME diversity (includes Size of companies, Network design, and Daily interaction) They verified their model through an experiment conducted in SMEs.	Found that 2-factor authentication (2FA) can be the most effective and usable controls for small organisations, as it directly addresses theft of financial credentials. However, companies with less available capacity for security is suggested to adopt a less effortful protection measure. Of all the basic controls suggested by the CES, Anti-malware and Application Firewall is most effective. When combined with 2FA, they manage the majority of malware and vulnerabilities. Other controls suggested by the CES are interchangeable depending on their needs. Access control privileges are unavoidable controls initially; however, once a security responsibility is delegated, usable security solutions become essential.
P.Mayer and M. Volkamer (2017) [52]	To address the misconceptions about password security that exist even among the security researchers.	Used a systematic literature review to elicit the misconceptions about password security. They identified 23 misconceptions classified into four categories: composition, handling, attacks, and miscellaneous, then used text-based interventions to address those misconceptions that are refined based on feedback by 13 experts—at last, conducted user study with 90 participants from 3 SMEs to refine and validate them.	Password security has many misconceptions, and based on systematic literature review; the authors identified 23 misconceptions that can broadly be classified into a composition of password, handling of password, attacks to password and miscellaneous misconceptions.
P. Mayer, C. Shwartz, and M. Volkamer (2018) [42]	To develop and evaluate password security awareness raising materials suitable for SMEs.	Used literature review to design the initial iteration of the password security awareness raising materials. Next, it is refined by incorporating feedback from independent	Password policies should provide more detailed rules on how to choose passwords. Moreover, awareness information should be relevant, helpful and actionable. Last but not least, positive phrasing instead of risk and fear in

		information security experts from academia and industry (materials completeness and correctness). Lastly, it is evaluated in the real work environment (mainly visual appeal and the understandability) by using the employees of three German SMEs (30 participants from each SME) and further refined based on their feedback.	awareness materials and use of image are more effective.
M. Bada and J.R.C Nurse (2019) [53]	To study an organization's cybersecurity strategy and propose a high-level program for cybersecurity education and awareness specifically targeted to SMEs.	Used literature review of cybersecurity awareness, education and training initiatives to design the questionnaire. Then a survey was conducted to collect the necessary quantitative and qualitative. The questionnaire was sent to 626 SMEs in the UK and received responses from 27 of them, but only 20 responses were complete.	Depending on diversified methods for security awareness can result in better outcomes in SMEs than relying on only a few. Additionally, Participating in workshops and interaction with different security experts are good for security hygiene of SMEs. The authors also suggest that building a relationship of trust can be a good way to engage with SMEs to promote a cybersecurity culture, while ersonalised assessment of the organisation's security posture can be helpful for SMEs to understand their cyber risk and develop an action plan to deal with it. Finally, freely available services, awareness materials and support are useful for SMEs, while SMEs need information and advice on available services in the market based on the requirements of SMEs. However, they must be appropriately communicated. A cybersecurity awareness program for SMEs (generally initiative from the Government) need consideration of the following five areas: Initial engagement with SMEs, Improving security policies and culture, Program resources, Trusted third-party resources/ services, and Communication strategy.
M. Heidenreish (2019) [6]	To study the security status of the German micro-enterprises and mitigate their security issue with an appropriate solution.	Used a literature review to identify the current security status of micro-enterprises in Germany. Next, the author applied method engineering concept and proposed a generic self-measurement method (that uses questionnaire for subjective awareness measurement and a checklist for objective	Micro-enterprises have limited IT security and resources. Further, they lack awareness and knowledge to solve their security issues. Thus, there is a need for a method/technique that should be cost-efficient, understandable and fast to measure their security vulnerabilities and raise their awareness.

		awareness measurement) for the assessment of IT security in the status quo of micro-enterprises.	

9.2 Papers that deal with CSA for SMEs outside Europe

Table 3: Summary of papers that deal with CSA for SMEs outside Europe

Author	Objective	Methodology	Finding
S. Dojkovski, S. Lichtenstein, M.J. Warren (2007) [43]	To investigate the challenges faced by SMEs in fostering information security culture in the Australian context.	Used review and synthesis of relevant literature to build a framework for developing information security culture in SME and this is followed by a focus group conducted with four IT consultants that provide security services to SMEs in Australia.	The major challenges of SMEs are: • The misconception among SME owners who believe that cyber threats are only a concern for large business and not SMEs, and thus they are unwilling to allocate budget for it. • Lack of suitable human resources to report about and deals with cybersecurity issues. Moreover, the authors suggest the following: • Employees should be explained about security policies at the time of employment and ramification of security breaches. • SMEs can utilise e-learning at a collaborative and cooperative level where knowledge sharing at all levels takes place, including the sharing of values, experiences and emotions to raise security awareness. • Should consider the cultural aspects and include a variety of cases to grasp the interest of diversities.
L. Ngo, W. Zhou, A. Chonka, J. Singh (2009) [44]	To assess the level of IT security culture in Australian SMEs to determine the improvements needed to achieve the desired IT security culture.	The study was conducted in multiple phases with three SMEs: • Used informal interviews, document analysis, and IT security controls checklist for the preliminary assessment to determine the level of IT security establishment, and the desired IT security culture of each SME. • Used questionnaire (paper-based seven-point Likert scale questionnaire) and follow-up semi-structured interview for the primary assessment to	Based on a preliminary assessment, they found seven IT security establishment levels: • Level 1: Technical Controls 'Initiative' • Level 2: Technical Controls 'Developing' • Level 3: Technical Controls 'Established' and Management Controls 'Initiative' • Level 4: Management Controls 'Developing' • Level 5: Management Controls 'Established' and Organization Controls 'Initiative' • Level 6: Organization Controls 'Developing' • Level 7: Organization Controls 'Established' Based on primary assessment, they found that the desired IT security level should include the followings: • Staff shares the IT security responsibility • Staff needs basic IT security literacy

		determine the current IT security culture of each SME.	• Staff complies with the company policy • Staff should have a proactive IT security attitude • Staff should be constantly aware of IT security always. Again, based on primary assessment, they found that IT security was not a priority in all three SMEs, and two of the SMEs were at level 3 and one at level 5. Finally, the improvements needed for IT security in SMEs are: • A commitment and support of senior management • Properly structure and organise security policies, procedures, and guidelines • Organise IT security awareness, training and education program • Clearly define roles and responsibilities • Establish policy-compliant behaviour • Stay abreast of current and changing laws and regulations • Focus on product security and standards • Exploit technology effectively and • Periodically measure and review security efforts
E. Y. Yildirim, G. Akalp, S. Aytac, N. Bayram (2011) [54]	To examine enterprises information security in SMEs in Turkey and to compare the results with similar data gathered from different countries	Used descriptive, cross-sectional, self-reported questionnaire consisting of 49 questions grouped into nine sections titled Security Policy, Organizational Security, Asset Classification and Control, Personnel Security, Physical and Environmental Security, Communications and Operations Management, Access Control, System Development and Maintenance and Business Continuity Management. The questionnaire used a 5-point Likert scale. It was delivered to 97 SMEs in Turkey.	Although 77% of the companies had issued information security policies, and their 70% of employees were aware of those policies, those policies were designed and applied based on their limited understanding of "information security management". Thus, it has been suggested to follow internationally agreed and tested standards for information security policies. Furthermore, half (50%) of the respondents had encountered security vulnerabilities, and the most common cause for them was human carelessness. A majority (81%) of the respondents considered information security to be essential and should be considered for their organisation.
T. Gundu and S.V. Flowerday (2013) [45]	To propose an iterative information security awareness process suitable for SMEs.	Utilised the following behavioural theories: TRA, PMT and BT to design their process (presented in the form of a flowchart) and used action research method over 10 months period in an engineering firm from South Africa to refine and validate their proposition.	Merely having information security policy in an organisation cannot produce an expected outcome unless it is aligned with a suitable awareness campaign. Additionally, an increase in security knowledge marginally helps in improving employees' attitude and behavior towards security. Furtehrmore, information security awareness programs are expensive and resource-consuming endeavours. Thus, e-learning campaigns can be effective in reducing costs.

J. Kaur and N. Mustafa (2013) [55]	To investigate the relationship of knowledge, attitude, and behavior of Malaysian SMEs employees with confidentiality, integrity and availability (CIA) triad.	Used survey questionnaire to collect data about information security awareness. The partial square was used for the data analysis. There were 85 participants.	There exists no significant relationship between knowledge and CIA triad, while attitude and behavior are determinants of confidentiality and integrity. Finally, only behaviour influences integrity.
H. Shih et al. (2016) [46]	To study the impact of promotion and prevention approaches in motivating employees to comply with information systems security policy (ISSP).	Used scenario-based questionnaire (that used a five-point Likert scale) to survey employees of Chinese SMEs. The survey attempts to determine the employees' perceptions and intention to comply with ISSP in the workplace. The survey questionnaire was sent distributed to 267 SMEs via their top management and received responses from 216 of them.	Both promotion-approach and promotion-avoidance mechanisms are effective in motivating employees with awareness of ISSP; however, promotion-approach has a better performance than the latter. These mechanisms are ineffective in case of unaware employees may be due to such employees' low self-efficacy to comply with ISSP in the promotion-approach and promotion-avoidance mechanisms. Prevention-approach and prevention-avoidance mechanisms are suitable in case of employees with awareness or unawareness of ISSP; however, prevention approach has a better performance than the latter.
T.K. Lejaka, A.D. Veiga, and M. Loock (2019) [38]	To find out studies that deal with cybersecurity awareness for Small, Medium and Micro Enterprises (SMMEs) in South Africa and to investigate frameworks and their components that can be suitable for South African SMMEs.	Used a systematic literature review for their study.	Found 22 works of literature that dealt with cybersecurity awareness for SMMEs in South Africa but did not find any of the frameworks designed and proposed by those studies to be complete and effective for the South African SMMEs. They suggest frameworks that should include the following components: • Clearly articulated goals and objectives • Appoint a dedicated team • Identify current training needs • Obtain support in the form of partnerships • Identify target audiences • Define topics to cover and their delivery methods • Establish a security policy • Develop a strategy for implementation • Design awareness and training • Define evaluation methods

10 Summary of findings and discussion

The challenges of CSA faced by SMEs and raised by the reviewed papers are similar to those discussed in section 8.1 (or Figure 4, except situation awareness). Once again, the reviewed papers mostly use user-study (using survey), followed by a literature review.

Based on CSA at an organisational level, SMEs can broadly be categorised into four types, shown in Figure 5. This classification considers SME interest in accepting cybersecurity issues and investing in suitable countermeasures.

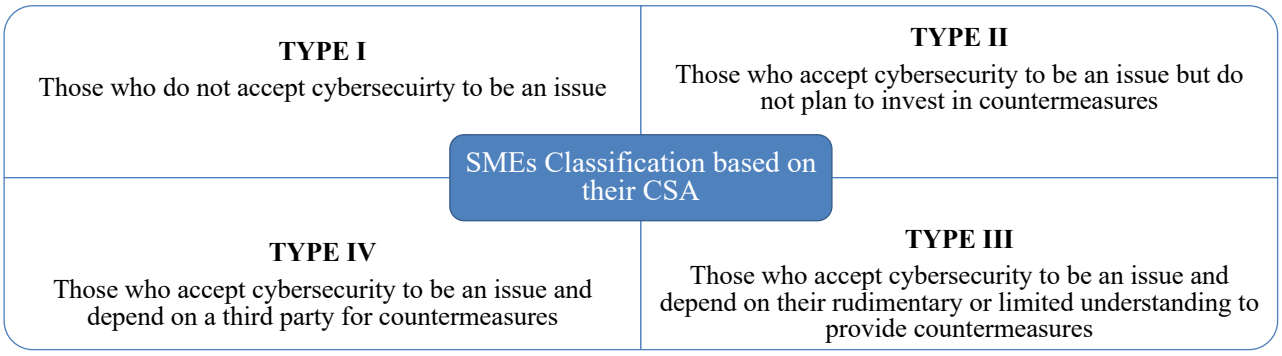

Figure 5: Classification of SMEs based on their CSA

- **Type I:** The owner and executive management of these SMEs have a misconception that cyberattacks target only large organisations so SMEs should not worry about cybersecurity. Such a tendency towards cybersecurity was noticed only by some old studies. The situation seems to have improved now.
- **Type II:** These are SMEs that accept cybersecurity to be an imminent threat, but due to their limited budget must prioritise investment in areas that can contribute to their business growth. Most of the studies found this type to be prominent. Such SMEs mostly rely on security measures that come in-built with other necessary technologies or are available for free or inexpensively, such as operating system security, in addition to workshops and materials provided for free by some governmental and non-governmental agencies.
- **Type III**: These SMEs accept cybersecurity to be essential and allocate some budget to it, but lack aware or qualified human resources to implement the budget. They try to manage their IT security 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 show this group to be more confident about their cybersecurity.

Similarly, the main challenges of CSA that the reviewed papers raise are presented in Figure 6. It must be noted though that the distinction between “within” and ”outside” Europe is explicitly based on the scope and the recommendations of the corresponding papers.

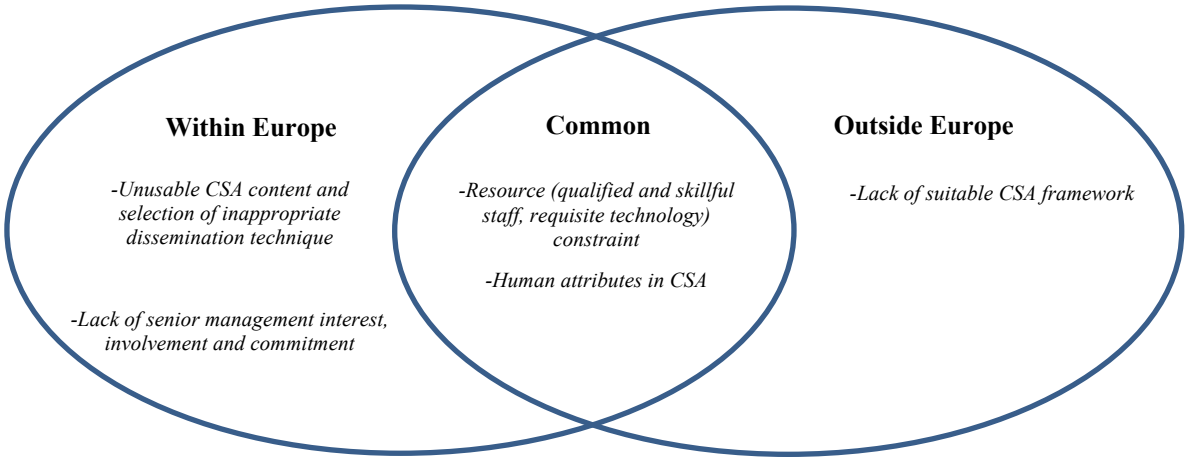

Figure 6: Challenges of CSA for SMEs

10.1 Resource constraints

Many studies both from within and outside Europe [47] [50] [41] [48] [43] point out resource constraints as being one of the major contributing factors behind the poor CSA of SMEs, and their overall cybersecurity. The budget constraint adversely impacts their ability to hire qualified and skilful cybersecurity staff particularly for CSA, to organise relevant CSA programs, to equip themselves with the requisite cybersecurity technologies, and to comply with established regulations and standards. Even those SMEs which accept security and realise the importance of cybersecurity policies and regulations design and implement them based on their limited or rudimentary understanding of cybersecurity, and include their own assumptions about cybersecurity [54]. Moreover, there exists no individual tasked with increasing employee awareness about security policies and regulations and to ensure their compliance. These resource constraints for CSA can be attributed to various reasons, but mainly three:

- SMEs are growing companies with a limited budget available. Due to this, cybersecurity is not prioritised [3] [44]. They prefer to invest in activities that can result in tangible growth or benefits for the organisation.
- Some owners or executive/senior management of SMEs believe that the risk of cyberattacks is only for large organisations and thus, they are dismissive of the risk [43].
- Even those organisations with a leadership accepting cybersecurity to be a real issue prioritise and invest in technical measures [51] [48]. This becomes a more severe problem when they invest in technologies without knowledge about their effectiveness in overall security control.

Ironically, the issue of resource constraints is not uncommon among other types of organisations as well. Large organisations may not have monetary issues, but many still lack dedicated security professionals assigned to CSA. This is evident from a recent survey conducted in 2019 by the SANS Institute [32] which revealed that over 75% of security awareness professionals are part-time and spend less than half their time on security awareness [32]. This survey also divulges that, for cybersecurity professionals, CSA is just a secondary task mounted on their other job requirements. Further, the same study finds a strong correlation between full-time employees dedicated to CSA and the organisational CSA maturity.

Since resources directly relate to finance, and only the executive management of an organisation have the authority to make significant financial decisions, this issue can only be handled by the involvement and commitment of senior management, which is discussed in section 10.3.

10.2 Unusable CSA content and selection of inappropriate dissemination technique

Some studies [6] [39] [40] [53] make suggestions to improve the usability of CSA programs. This is mainly because the existing CSA programs did not seem to address the needs of SMEs. As a matter of fact, this issue is equally encountered by other types of organisations. Even among enterprises that flag cybersecurity as a high priority and allocate resources for CSA do not see any tangible effect on their unaware employees [25] and organisations still have to deal with risks resulting from people who do not follow security policies and procedures or fail to understand the awareness materials [56]. This may be attributed to poorly tailored awareness-raising materials and techniques that are implicitly based upon an assumption "*one-size-fits-all*" [25]. Maybe due to this ineffectiveness of CSA, some people are frustrated and even believe that such awareness activities are a waste of money and should be abandoned [56] [57]. This belief to abandon CSA may be too harsh, but it is also an eye-opener that things have to be done differently or need improvement.

There is a need for CSA content and dissemination techniques designed with an organisational mission that supports its business needs and is relevant to its culture and IT infrastructure. Cybersecurity is more likely to be accepted and acted upon if employees feel the message is explicitly and appropriately directed at them rather than generically to everyone. At present, any tailoring of CSA materials is often, at best, done from the perspective of framing the messages to match the type of organisation or sector concerned. It is rare to

see anything getting down to the level of what each user might need based on their learning style or prior predisposition towards security. The most successful awareness programs are those that users feel are relevant to the subject matter and issues presented. Therefore the objective of security awareness programs must be formulated as "How we can convey, imprint and habituate tailored security principles to a target audience, which are necessary for them to securely and safely perform their tasks and how to enable them to map such principles into their work routines".

Accordingly, the CSA material and communication techniques should preferably be tailored to the needs of the recipients, i.e., personalised. Faults in the design of CSA content and selection of delivery techniques exist maybe because awareness professionals mostly come from some technical background; over 80% of them come from a technical background [32]. No doubt, a technical background can be an advantage, but such professionals often lack the soft skills needed to effectively communicate cyber risks to audiences in a way that changes behaviour. Besides, they suffer from a cognitive bias called "*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 [32].

The CSA content should be clear, consistent, and relevant to the target audiences, and more importantly, it should be actionable [39] [42]. When selecting dissemination or delivery techniques, it is suggested to consider multiple (i.e., alternative) techniques that are suitable for diverse groups of users [39] [53]. Further, the CSA content and dissemination techniques need continuous improvement based on their effectiveness on the audiences [6] [39] [40]. 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 [27] , so these materials should be selected accordingly.

10.3 Lack of senior management interest, involvement, and commitment

A lack of senior management involvement and commitment to cybersecurity [41] is one of the main reasons behind its low priority. This adversely impacts the overall cybersecurity, including its CSA, of an organisation. This becomes more prominent in the case of SMEs, which suffer from resource constraints, due to which management teams have to prioritise other activities over cybersecurity. Furthermore, there are no qualified and skilful personnel in SMEs who can communicate and make senior management understand the relevance or importance of cybersecurity.

There are no definite ways that can guarantee the involvement and commitment of senior management to cybersecurity and CSA. However, some possible ways could be:

- To show and explain the cost-benefit of CSA to senior management [48], and the need to raise the awareness of senior management.
- To design and organise CSA programs that require procurement of the least level of resources, preferably CSA activities that can be conducted for minimal cost [53], and can utilise cost-effective ways like e-learning and collaborative platforms [43] [45].
- To leverage peer comparisons via benchmarking, i.e., to show leadership how competitors are spending significantly on CSA [32].

10.4 Human attributes in CSA

Most research studies work on determining human attributes or determining factors that can motivate security behaviour [39] [40] [41] [43] [44] [50] [55]. They suggest factors like:

- avoiding fear as a means of awareness
- considering cultural aspects in CSA
- using a promotion or award approach to encourage aware people to comply with policies and a preventive approach for both aware and unaware people
- designing better usability to encourage people to follow security procedures, etc.

Similarly, many other factors like self-efficacy, into under consideration during CSA programs.

As a matter of fact, the human factor is also the most challenging and intricate issue in the design and implementation of CSA, since it involves domains like behavioural psychology, cognitive psychology, and neuropsychology [58]. A study conducted by the Information Security Forum [58] found the following six reasons why CSA activities fail:

- Solutions are not aligned to business risks
- Neither progress nor value is measured
- Incorrect assumptions are made about people and their motivations
- Unrealistic expectations are set
- The correct skills are not deployed
- Awareness is just background noise

Further, to mitigate the six problems mentioned above [58], the same study suggests utilising:

- behavioural psychology – to understand the history and context that drives behaviours and change the consequences in this context to eliminate unwanted behaviours and promote target behaviours
- cognitive psychology – to deliver solutions in small chunks using a 'simple to complex' principle; to include opportunities to sufficient practice the target behaviours, 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 focussed on their new insights.

Then, the National Institute of Standards and Technology (NIST) [23] recommends:

- plan and structure the CSA properly
- establish priorities that CSA should cover,
- set the bar of the complexity of the subject matter that CSA should cover, and
- conduct an assessment to measure the effectiveness of CSA

Similarly, S. Furnell and I. Vasileiou [12] suggest employing the roles of, prior knowledge, barriers, learning styles, and security perception of the audience in designing and conducting a CSA program. Finally, M. Bada, A.M. Sasse, and J.R.C. Nurse [13] suggest that awareness content should be engaging, appropriate and on-going, with a range of relevant topics that are targeted, actionable, do-able, and provide feedback to help sustain people's willingness to change.

10.5 Lack of suitable CSA framework

Most of the existing CSA frameworks are not designed with SMEs in mind [38]. The needs and circumstances of SMEs are different from their larger counterparts, thus the existing frameworks do not fit SME needs. There are two possible ways to deal with this issue:

i) to design a completely new framework, and
ii) to modify the existing framework to suit the purpose of SMEs. Some studies [47] [40] [48] [45] have worked on a framework or model that could fulfil the needs and circumstances of SMEs.

11 Conclusions

Cybersecurity is a shared responsibility, and every employee of an enterprise can be critical of its cyber defence and countermeasure efficiency. Therefore, awareness about the possible threats in their area of work and regular updates on organisational policies and procedures, as relevant for their job function, is essential for all employees of an organisation [22] [26] [23]. Increased employee awareness can reduce the likelihood of accidental breaches and increase the probability of suspicious activities being recognised, reported and taken care of at the right time. However, the cybersecurity needs and circumstances of different sized

enterprises can vary. For example, resourceful large enterprises cannot be put in the same basket as resource-constrained SMEs. Also, there are many factors like organisational, social, environmental, and personal considerations that can influence CSA and behaviour. Therefore, in this report, we have tried to investigate the current status of CSA for SMEs, conducting a systematic literature review to achieve our objectives.

In this research, we mainly aimed to elicit the challenges in CSA that demand further research in order to suit the needs and circumstances of SMEs, particularly focusing on SMEs within Europe. Furthermore, we attempted to identify the potential CSA content and delivery techniques, and the possible research methodologies that can be implemented for our future research work.

We found that one of the main challenges in the case of SMEs is their resource constraints. Therefore, there is a need for affordable and effective CSA that fulfils the needs of SMEs. Any CSA content should always consider its compliance cost, and the CSA delivery technique should take into account the nature of the organisation and its affordability. The human characteristics of SME employees who can promote safe and secure behaviour in SMEs equally need further investigation. Last but not least, there is a severe need for suitable CSA frameworks or models for SMEs. SMEs should no longer depend on frameworks or models that were designed with the sole objective of meeting the requirements of large organisations.

The results of this study provide useful insights and firm foundations for the continuation of CyberSec4Europe both across the T9.4 and T3.10 tasks. In accordance with the results presented in this deliverable, a data collection process will be established, utilising both quantitative and qualitative methods, to shed light on areas where gaps have been identified and provide input towards the second iteration of this deliverable. Specifically, currently utilised awareness methods will be investigated, firstly to explore the breadth of this domain and concurrently to analyse their efficiency. This process will constitute the core of our awareness effectiveness study and will provide the initial input towards formulating supply chain security recommendations.

References

[1] R. Vaidya, "Cyber security breaches survey 2018: Statistical release," *Department for Digital, Culture, Media & Sport, UK,* 2018.

[2] Chen et al, "The relationship between the cost of cybercrime and web security posture: A case study on Belgian companies," in *11th European Conference on Software Architecture*, Canterbury, UK, 2017.

[3] T. Kurpjuhn, "The SME security challenge," *Computer Fradu & Security,* vol. 2015, no. 3, pp. 5-7, 2015.

[4] Fireeye, "Small and midsize enterprises: Stopping cyber crime against small and midsize enterprises," *https://www.fireeye.com/offers/stop-cyber-crime-against-small-medium-enterprises.html,* 2020.

[5] L. A. Aguilar, "The need for greater focus on the cybersecurity challenges facing small and midsize businesses," U.S. Securities and Exchange Commission, 2015.

[6] M. Heidenreich, "Conceptualization of a measurement method proposal for the assessment of IT security in the status quo of micro-enterprises," in *International Conference on Computing , Electronics & Communication Engineering*, London, UK, 2019.

[7] M. Brodin, "A Framework for GDPR Compliance for Small-," *European Journal for Security Research,* vol. 4, p. 243–264, 2019.

[8] D. Catteddu and L. Marinos, "Accesing a simplified information security approach: Feedback from RA/RM pilot," ENISA, 2009.

[9] M. T. Siponen, "Five dimensions of information security awareness," *ACM SIGCAS Computers and Society,* vol. 31, no. 2, pp. 24-29, 2001.

[10] S. WIliams, "More than half of personal data breaches caused by human error," *SecurityBrief,* 21 August 2019.

[11] Ponemon Institute, "State of cybersecurity in small & medium-sized businesses (SMB)," Traverse City, MI, USA, 2017.

[12] S. Furnell and I. Vasileiou, "Security education and awareness: Just let them burn?," *Network Security,* vol. 2017, no. 12, pp. 5-9, 2017.

[13] M. Bada et al., "Cyber security awareness campaigns: Why do they fail to change behaviour?," in *International Conference on Cyber Security for Sustainable Society*, Coventry, UK, 2015.

[14] A. Scroxton, "Social engineering a factor in virtually all cyber attacks, report claims," ComputerWeekly.com, 2019.

[15] J. Webster and R.T. Watson, "Analyzing the past to prepare for the future: Writing a literature review," *MIS Quarterly,* vol. 26, no. 2, pp. xiii-xxiii, 2002.

[16] European Commission, "What is an SME?," European Commission, Brussel, Belgium, Commission staff working document on implementation of commission recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises.

[17] G. Papadopoulos et al., "Statistics on small and medium-sized enterprises," Eurostat, 2015.

[18] D. Clark, "Number of small and medium-sized enterprises (SMEs) the European Union in 2018," Statista (https://www.statista.com/statistics/878412/number-of-smes-in-europe-by-size/), 2019.

[19] B. Hanus et al., "Definition and multidimensionality of security," *The DATA BASE for Advances in Information Systems,* vol. 49, no. Special Issue, pp. 103-132, 2018.

[20] C. Vroom and R. vonSolms, "A practical approach to information security awareness in the organization," in *M. A. Ghonaimy et al. (eds.), Security in the Information Society*, Boston, MA, Springer, 2002, pp. 19-37.

[21] E. Yildirim, "Awareness for the success of business enterprises," in *D. Nicholson (ed.), Advances in Human Factors in Cybersecurity*, Cham, Springer, 2016, pp. 211-222.

[22] S.K. Katsikas, "Health care management and information security: Awareness,training or education?," *International Journal of Medical Informatics,* vol. 60, no. 2, pp. 129-135, 2000.

[23] M. Wilson and J. Hash, "Building an Information Technology Security Awareness and Training Program," NIST Special Publication 800-50, Gaithersburg, USA, 2003.

[24] A. Caballero, "Security education, training, and awareness," in *J.R. Vacca (ed.) Computer and Information Security Handbook*, Burlington, MA, USA, Morgan Kaufmann, 2017, pp. 497-505.

[25] S. Furnell and I. Vasileiou, "Security education and awareness: Just let them burn?," *Network Security,* pp. 5-9, 2017.

[26] D.E. de Zafra et al, "Information Technology Security Training Requirements: A Role- and Performance-Based Model," NIST Special Publication 800-16, 1998.

[27] R.S. Shaw et al., "The impact of information richness on information security awareness," *Computers & Education,* vol. 52, p. 92–100, 2009.

[28] E. C. Johnson, "Security Awareness: Switch to a better programme," *Network Security,* vol. 2006, no. 2, p. 15–18, 2006.

[29] S. Stockhardt et al, "Teaching phishing security: Which way is best?," in *31st International Conference on ICT System Security and Privacy Protection*, Ghent, Belgium, 2016.

[30] J. Andress and M. Leary, "Conducting security awareness and training," in *Building a Practical Information Security Program*, Syngress, 2017, pp. 135-155.

[31] I. Kirlppos et al., "'Shadow security' as a tool for learning organization," *ACM SIGCAS Computer and Society,* vol. 45, no. 1, 2015.

[32] L. Spitzner et al., "The rising era of awareness training," *SANS Security Awareness Report,* 2019.

[33] "Okoli et al. "A guide to conducting a systematic literature review of information systems research." (2010)".

[34] Y. Levy and T.J. Ellis, "A systems approach to conduct an effective literature," *The International Journal of an Emerging Transdiscipline,* vol. 9, pp. 181-212, 2006.

[35] B. Lebek et al, "Employees' information security awareness and behavior: A literature review," in *46th Hawaii International Conference on System Sciences*, Wailea, [Maui], Hawaii, USA, 2013.

[36] P. Mayer et al., "Reliable behavioural factor in the information security context," in *International Conference on Availability, Reliability and Security*, Reggio, Calabria, Italy, 2017.

[37] H. Aldawood and G. Skinner, "Educating and raising awareness on cyber security social engineering: A literature review," in *IEEE International Conference on Teaching, Assessment, and Learning for Engineering*, Wollongong, NSW, Australia, 2018.

[38] T.K. Lejaka , "Cyber security awareness for small, medium and micro enterprises (SMMEs) in South Africa," in *Conference on Information Communications Technology and Society*, Durban, South Africa, 2019.

[39] U.E. Gattiker, "Can an early warning system for home users and SMEs make a difference? A field study," in *International Workshop on Critical Information Infrastructures Security*, Samos Island, Greece, 2006.

[40] L.E. Sánchez et al., "Security culture in small and medium-size enterprise," in *J. .E. Quintela Varajão et al. (Eds.) Communications in Computer and Information Science*, Springer, Berlin, Heidelberg, 2010, p. 315–324.

[41] A. Freeman and L. Doyle, "The utilization of information systems security in SMEs in the South East of Ireland," in *A. D'Atri et al. (eds.), Management of the Interconnected World*, Physica-Verlag HD, 2010, pp. 121-128.

[42] P. Mayer et al., "On the systematic development and evaluation of password security awareness-raising materials," in *34th Annual Computer Security Applications Conference*, San Juan PR USA, 2018.

[43] S. Dojkovski et al., "Challenges in fostering an information security culture in Australian small and medium sized enterprises," in *15th European Conference on Information Systems*, St. Gallen, Switzerland, 2007.

[44] L. Ngo et al., "Assessing the Level of I.T. Security Culture Improvement: Results from Three Australian SMEs," in *The 35th Annual Conference of the IEEE Industrial Electronic Society*, Porto, Portugal, 2009.

[45] T. Gundu and S.V. Flowerday, "Ignorance to awareness: Towards an information security awareness process," *South African Institute of Electrical Engineers,* vol. 104, no. 2, 2013.

[46] H. Shih et al., "Taking promotion and prevention mechanisms matter for information systems security policy in Chinese SMEs," in *2nd International Conference on Information Management*, London, UK, 2016.

[47] A. Tawileh et al., "Managing information security in small and medium sized enterprises: A holistic approach," in *N. Pohlmann, H. Reimer, W. Schneider (Editors): Securing Electronic Business Processes*, Springer Vieweg Verlag, 2007, pp. 331-339.

[48] R. Groner and P. Brune, "Towards an empirical examination of IT security infrastructures in SME," in *17th Nordic Conference on Secure IT Systems*, Karlskrona, Sweden, 2012.

[49] S. Parkin et al., "Pragmatic Security: Modelling IT Security Management Responsibilities for SME Archetypes," in *MIST '16*, Vienna, Austria, 2016.

[50] J.M. Torress et al., "Steering security through management," in *6th International Conference on Trust, Privacy and Security in Digital Business*, Linz, Austria, 2009.

[51] I. Lopes and P. Oliveira, "Understanding information security culture: A survey in small and medium sized enterprises," in *Á. Rocha et al. (eds.) New Perspectives in Information Systems and Technologies*, Switzerland, Springer International Publishing, 2014, pp. 277-286.

[52] P. Mayer and M. Volkamer, "Addressing misconceptions about password security effectively," in *7th Workshop on SocioTechnical Aspects in Security and Trust*, Orlando, Florida, USA, 2017.

[53] M. Bada and J.R.C. Nurse, "Developing cybersecurity education and awareness programmers for small and medium-sized enterprises (SMEs)," *Information & Computer Security,* vol. 27, no. 3, pp. 393-410, 2019.

[54] E. Y. Yildirim et al., "Factors influencing information security management in small- and medium-sized enterprises: A case study from Turkey," *International Journal of Information Management,* vol. 31, p. 360–365, 2011.

[55] J. Kaur and N. Mustafa, "Examining the effects of knowledge, attitude and behavior on information security awareness: A case on SME," in *3rd International Conference on Research and Innovation in Information Systems*, Kuala Lumpur, Malaysia, 2013.

[56] J. Schroeder, "Challnges faced by organizations," in *Advanced persistent training: Take your security awarenes program to the next level*, Edinburgh, UK, Apress, 2017, p. 1.

[57] D. Aitel, "Why you shouldn't train employees for security awareness," *CSO,* 18 July 2012.

[58] Information Security Forum, "From promoting awareness to embedding behaviours: Secure by choice, not by chance," 2019.

[59] J. Saleem et al., "A state of the art survey - Impact of cyber a,acks on SME's," in *ICFNDS '17*, Cambridge, UK, 2017.