A taxonomy of factors that contribute to organizational Cybersecurity Awareness (CSA)

Joakim Kävrestad
School of Engineering, Jönköping University, Jönköping, Sweden, and
Felicia Burvall and Marcus Nohlberg
School of Informatics, University of Skövde, Skövde, Sweden

Received 9 November 2023
Revised 2 January 2024
23 February 2024
17 April 2024
Accepted 20 May 2024

Abstract

Purpose – Developing cybersecurity awareness (CSA) is becoming a more and more important goal for modern organizations. CSA is a complex sociotechnical system where social, technical and organizational aspects affect each other in an intertwined way. With the goal of providing a holistic representation of CSA, this paper aims to develop a taxonomy of factors that contribute to organizational CSA.

Design/methodology/approach – The research used a design science approach including a literature review and practitioner interviews. A taxonomy was drafted based on 71 previous research publications. It was then updated and refined in two iterations of interviews with domain experts.

Findings – The result of this research is a taxonomy which outline six domains for importance for organization CSA. Each domain includes several activities which can be undertaken to increase CSA within an organization. As such, it provides a holistic overview of the CSA field.

Practical implications – Organizations can adopt the taxonomy to create a roadmap for internal CSA practices. For example, an organization could assess how well it performs in the six main themes and use the subthemes as inspiration when deciding on CSA activities.

Originality/value – The output of this research provides an overview of CSA based on information extracted from existing literature and then reviewed by practitioners. It also outlines how different aspects of CSA are interdependent on each other.

Keywords Awareness, Cybersecurity, Information security, Culture

Paper type Research paper

1. Introduction

The world is now in a state where technology is tightly incorporated into almost everything we do. That is positive in numerous ways, but the downside is that people are now exposed to countless security threats they would not have encountered previously. However awareness of digital threats does not seem to increase at the same pace as adoption of new technology (Zwilling *et al.*, 2022). While users are often experts on how to use IT, they are unaware of many related security issues. Subsequently, the average user has little or no awareness of how to

Information & Computer Security
Emerald Publishing Limited
2056-4961
DOI 10.1108/ICS-11-2023-0209

protect their devices and data against unauthorized access or attack (Kovačević *et al.*, 2020). For instance, users may have some knowledge from stories of cyberattacks and comprehend that security issues threaten the confidentiality of their data. However, many of these users remain uncertain of how to keep their data secure and are unaware of how their behavior can contribute to a systems compromise (Korovessis *et al.*, 2017).

Cybersecurity awareness (CSA) is defined by Shaw *et al.* (2009) as:

> the degree of understanding of users about the importance of information security and their responsibilities and acts to exercise sufficient levels of information security control to protect the organization's data and networks(p1).

National Institute of Standards and Technology (NIST) further describes that awareness-raising activities intend to change individuals' and organizations' attitudes and empower individuals to identify security concerns and respond to them appropriately (NIST, 2023). As such, CSA is an all-encompassing term referring to the culture within an organization as well as to the skills, attitudes, and practices of individuals. CSA is often described as the first line of defense of information systems and networks (Tasevski, 2016). Lack of CSA exposes vulnerabilities that adversaries can exploit for whatever nefarious purposes they have and attackers often focus their attention on humans rather than on technology (Kovačević *et al.*, 2020). Attacks targeting people are constantly evolving and increasing in frequency (Abawajy, 2014). Because of this, organizations are beginning to increase their efforts into CSA (Abawajy, 2014).

CSA is a complex domain dependent on individuals, organizations, technology and the interplay between those. Nevertheless, understanding what contributes to CSA is vital for future CSA practices. Consequently, *this research aims to develop a taxonomy of factors that contribute to organizational CSA*.

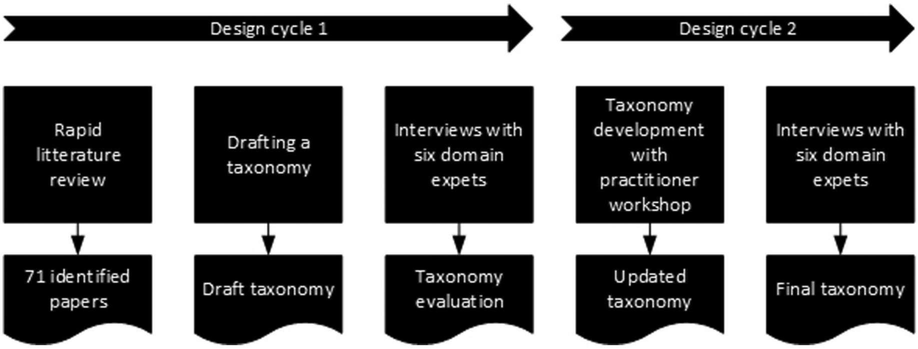
The result of this research is an overview of the CSA domain in the form of a taxonomy. The taxonomy outlines activities that can increase CSA organizations and is practically useful for those organizations. For example, the taxonomy can be used as a tool when developing internal CSA strategies.

2. Methodology

With the goal of creating a taxonomy that is useful for practitioners, this project adopted a Design Science Research (DSR) approach. DSR is characterized as a research approach where the current theory base is used to design artifacts of practical use in a certain domain (Gregor and Hevner, 2013; Hevner, 2007). The artifact design is central to the research and often iterative. Further, existing theory is used to inform the design process, while the design process, or output thereof, should contribute to the theory base (Hevner *et al.*, 2004). The DSR process in this research was influenced by the framework by Peffers *et al.* (2007) and included two design cycles. In short, the first design cycle began with a literature review, which was used to draft a taxonomy. The draft taxonomy was then evaluated in interviews with practitioners from large public sector organizations in Sweden and updated based on the data from the interviews. Finally, another round of interviews was conducted, and the final taxonomy was created. Figure 1 provides an overview of the research process. Detailed methodological considerations are discussed throughout the upcoming results chapter.

3. Results

This section will describe the activities and results of each design cycle before ending with a section describing the resulting taxonomy. A draft taxonomy was created at the start of the



Source: Created by the authors

Figure 1. Research process overview

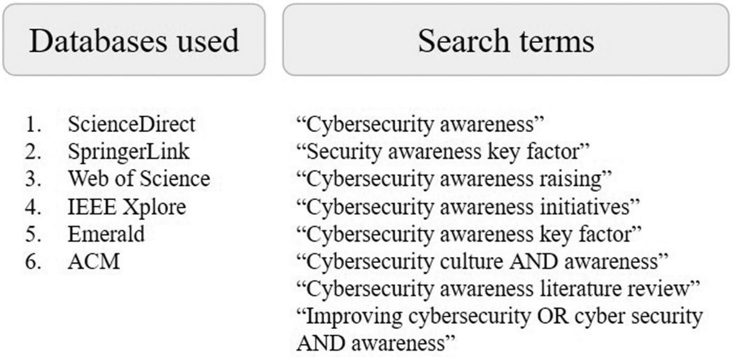
first design cycle and then continuously updated during the research process. For the sake of brevity, only the final taxonomy is presented in detail.

3.1 Design cycle 1

The first design cycle began with a rapid literature review with the purpose of identifying research on CSA. The data generated from the review was used to draft a taxonomy which was evaluated in interviews with six practitioners. The review is detailed next before the sections ends with a presentation of the expert interviews.

3.1.1 Drafting the taxonomy. A literature review was conducted using a rapid review methodology. A rapid review emphasizes quick collection of relevant literature on a subject while sacrificing completeness, compared to a structured literature review (Grant and Booth, 2009). In this case, it was used to efficiently gather existing knowledge about awareness raising and was considered sufficient to create a draft taxonomy. The databases and search terms listed in Figure 2 were used to identify potentially relevant publications. The selection process outlined in Figure 3 is used to identify 71 publications relevant to the study.

The included publications were analyzed using a thematic approach (Braun and Clarke, 2006). First, all included publications were reviewed and all mentions of CRA raising



Databases used

1. ScienceDirect
2. SpringerLink
3. Web of Science
4. IEEE Xplore
5. Emerald
6. ACM

Search terms

"Cybersecurity awareness"
"Security awareness key factor"
"Cybersecurity awareness raising"
"Cybersecurity awareness initiatives"
"Cybersecurity awareness key factor"
"Cybersecurity culture AND awareness"
"Cybersecurity awareness literature review"
"Improving cybersecurity OR cyber security AND awareness"

Source: Created by the authors

Figure 2. Databases and search terms used in the literature review

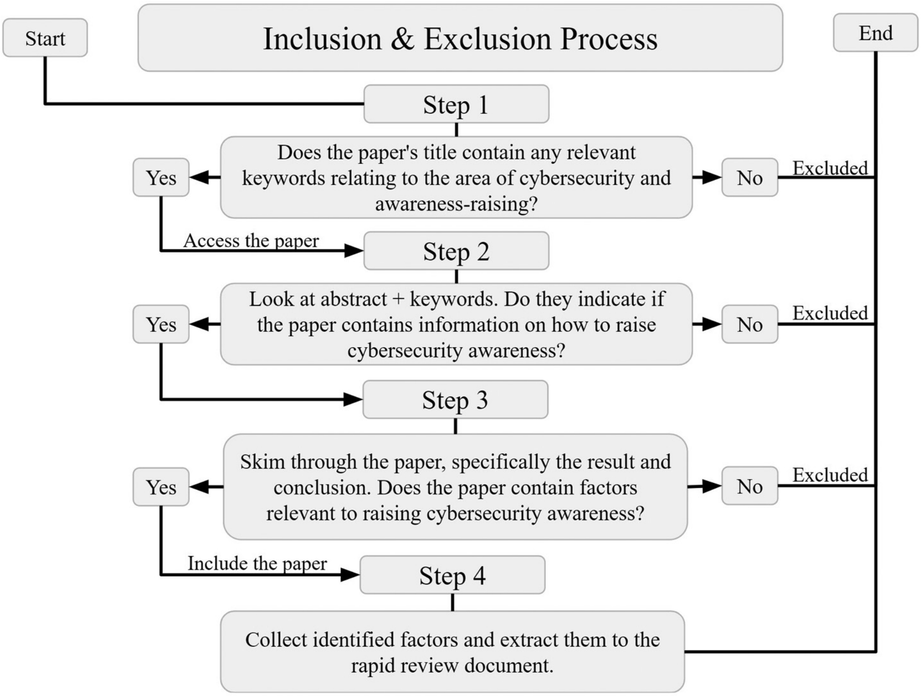

Start
Inclusion & Exclusion Process
End
Step 1
Does the paper's title contain any relevant keywords relating to the area of cybersecurity and awareness-raising?
Yes
No
Excluded
Access the paper
Step 2
Look at abstract + keywords. Do they indicate if the paper contains information on how to raise cybersecurity awareness?
Yes
No
Excluded
Step 3
Skim through the paper, specifically the result and conclusion. Does the paper contain factors relevant to raising cybersecurity awareness?
Yes
No
Excluded
Include the paper
Step 4
Collect identified factors and extract them to the rapid review document.

Figure 3.
Literature review selection process

Source: Created by the authors

activities were marked. The activities were then extracted and combined into themes. Eight themes were identified in this step, each reflecting a domain of importance for CSA. The themes, and publications relating to the respective themes are outlined below. Note than one publication may be relevant for several themes:

- *Top management support* (Aldawood and Skinner, 2019; Alshaikh *et al.*, 2021; Arbanas *et al.*, 2021; Bakari *et al.*, 2007; Caldwell, 2016; Dahabiyeh, 2021; Drevin *et al.*, 2007; Grassegger and Nedbal, 2021; Jouaibi *et al.*, 2022; Kemper, 2019; Khando *et al.*, 2021; Mansfield-Devine, 2017; Renaud, 2018; Tonkin *et al.*, 2022; Trim and Lee, 2019; Uchendu *et al.*, 2021).
- *User participation and engagement* (Abawajy and Kim, 2010; Alahmari and Duncan, 2020; Alahmari *et al.*, 2022; Albrechtsen and Hovden, 2010; Alshaikh *et al.*, 2021; Bada and Nurse, 2019; Caldwell, 2016; Cone *et al.*, 2006, 2007; Dahabiyeh, 2021; Drevin *et al.*, 2007; Haney and Lutters, 2018; Jouaibi *et al.*, 2022; Kalhoro *et al.*, 2021; Kemper, 2019; Khando *et al.*, 2021; Ki-Aries and Faily, 2017; Li *et al.*, 2016; Ruighaver *et al.*, 2007; Safa *et al.*, 2015; Safa and Maple, 2016; Sardar and Wahsheh, 2020; Stahl, 2006; Trim and Lee, 2019).
- *Interest and motivation* (Alanazi *et al.*, 2022; Albrechtsen and Hovden, 2010; Alshaikh *et al.*, 2021; Caldwell, 2016; De Bruijn and Janssen, 2017; Drevin *et al.*, 2007; Furnell and Rajendran, 2012; Haney and Lutters, 2018; Kemper, 2019; Ki-Aries and Faily, 2017; Parsons *et al.*, 2014; Rohan *et al.*, 2021; Ruighaver *et al.*, 2007; Tolah *et al.*, 2021; Trim and Lee, 2019; Uchendu *et al.*, 2021).

- *Cybersecurity policies* (Ahlan and Lubis, 2011; Alshaikh *et al.*, 2021; Alzubaidi, 2021; Bakari *et al.*, 2007; Cone *et al.*, 2006; De Bruijn and Janssen, 2017; Fielding, 2021; Georgiadou *et al.*, 2023; Parsons *et al.*, 2014; Rohan *et al.*, 2021, 2023; Tirumala *et al.*, 2019; Tolah *et al.*, 2021; Uchendu *et al.*, 2021; Whitman, 2004; Wong *et al.*, 2022).
- *Cybersecurity education, training and awareness* (Abawajy and Kim, 2010, 2010; Abu-Amara and Tamimi, 2021; Adelola *et al.*, 2015; A. Alahmari and Duncan, 2020; S. Alahmari *et al.*, 2022; Aldawood and Skinner, 2019, 2019; Alshaikh *et al.*, 2021; Alzubaidi, 2021; Amjad *et al.*, 2016; Arbanas *et al.*, 2021; Bada and Nurse, 2019; Caldwell, 2016; Chang and Coppel, 2020; Chaudhary *et al.*, 2022; Chung, 2020; Cone *et al.*, 2006, 2007; Fielding, 2020; Filipczuk *et al.*, 2019; Furnell and Vasileiou, 2017; Grassegger and Nedbal, 2021; Hart *et al.*, 2020; Jouaibi *et al.*, 2022; Kemper, 2019; Khando *et al.*, 2021; Ki-Aries and Faily, 2017; Mansfield-Devine, 2017; Parsons *et al.*, 2014; Quayyum *et al.*, 2021; Reeves *et al.*, 2021; Renaud, 2018; Rohan *et al.*, 2021, 2023; Safa *et al.*, 2015; Safa and Maple, 2016; Sardar and Wahsheh, 2020; Scholefield and Shepherd, 2019; Solomon *et al.*, 2022; Stahl, 2006; Tonkin *et al.*, 2022; Trim and Lee, 2019; Tschakert and Ngamsuriyaroj, 2019; Uchendu *et al.*, 2021; Wang *et al.*, 2018; Whitman, 2004; Wong *et al.*, 2022).
- *Attitudes and perceptions of cybersecurity* (Abawajy and Kim, 2010; Ahlan and Lubis, 2011; A. Alahmari and Duncan, 2020; Alanazi *et al.*, 2022; Albrechtsen and Hovden, 2010; Aldawood and Skinner, 2018, 2019; AL-Nuaimi, 2022; Alshaikh *et al.*, 2021; Bakari *et al.*, 2007; Caldwell, 2016; Chumaera and Ayu, 2022; Chung, 2020; Furnell and Rajendran, 2012; Furnell and Vasileiou, 2017; Georgiadou *et al.*, 2023; Grassegger and Nedbal, 2021; Hall, 2016; Hart *et al.*, 2020; Jouaibi *et al.*, 2022; Kalhoro *et al.*, 2021; Khando *et al.*, 2021; Ki-Aries and Faily, 2017; Kovačević *et al.*, 2020; Parsons *et al.*, 2014; Rohan *et al.*, 2021; Safa *et al.*, 2015; Safa and Maple, 2016; Tariq *et al.*, 2014; Tolah *et al.*, 2021; Wang *et al.*, 2018; Wong *et al.*, 2022).
- *Cybersecurity culture* (Abawajy and Kim, 2010; Aldawood and Skinner, 2019; AL-Nuaimi, 2022; Amjad *et al.*, 2016; Arbanas *et al.*, 2021; Bakari *et al.*, 2007; Caldwell, 2016; Chung, 2020; Fielding, 2020, 2021; Furnell and Rajendran, 2012; Furnell and Vasileiou, 2017; Georgiadou *et al.*, 2023; Hall, 2016; Kalhoro *et al.*, 2021; Kemper, 2019; Khando *et al.*, 2021; Kovačević *et al.*, 2020; Parsons *et al.*, 2014; Power and Forte, 2006; Rohan *et al.*, 2021, 2023; Ruighaver *et al.*, 2007; Safa *et al.*, 2015; Safa and Maple, 2016; Stahl, 2006; Tolah *et al.*, 2021; Trim and Lee, 2019; Uchendu *et al.*, 2021, 2021).
- *Cybersecurity advocates* (Arbanas *et al.*, 2021; Bada and Nurse, 2019; Caldwell, 2016; Chang and Coppel, 2020; Hall, 2016; Haney and Lutters, 2018; Kalhoro *et al.*, 2021; Power and Forte, 2006; Stahl, 2006; Trim and Lee, 2019; Uchendu *et al.*, 2021).

The included publications were analyzed in a second round, and subthemes were identified for all eight themes. The coding process is exemplified in Table 1 which illustrates how activities extracted from included sources formed themes, and how sub-themes were then formed.

The themes and subthemes were used to create the draft taxonomy used in the expert interviews. The taxonomy presented to interviewees was in the same format as the final taxonomy which is outlined in Appendix.

3.1.2 Interviews with practitioners. The taxonomy was evaluated using semi-structured interviews. The purpose of the interviews was to collect data from practitioners with experience of working with CSA in large public sector organizations. The rationale for focusing on participants in large public sector organization was that those organizations are expected to have more resources to put toward CSA and practitioners in those organizations will therefore provide

Source	Activity	Theme	Sub-theme	Comment
Khando *et al.*, 2021	Resources provided by management	Top management support	Allocate resources to governance	Presents a literature review on how organizations work with enhancing staff security awareness. Describes resources as crucial for development of CSA, and that managers are responsible for allowing the resources
Alshaikh *et al.*, 2021	Support and resources provided by management	Top management support	Allocate resources to governance	Develops a process for cybersecurity training of employees and reports that support and resources allocated by the management are crucial for a cybersecurity training strategy
Arbanas *et al.*, 2021	Include security management as a part of overall organizational management	Top management support	Establish clear visions and achievable goals	Presents a framework for evaluating information security culture based on a multi-stage methodology combining literature review and data collected from experts. Describes that support from the management is central and that security management should be included in the management of the organization so that security and business goals can be aligned
Kemper, 2019	The importance of cybersecurity should be emphasized by managers	Top management support	Establish clear visions and achievable goals	A feature article that argues that CSA starts from the top of an organization by the development of a policy where goals are outlined
Trim and Lee, 2019	Promote awareness increasing efforts	Top management support	Prepare a structured & organized CSA education plan	Employs group interviews to research the possible role of B2B marketers in cybersecurity awareness programs. They describe such programs as important for CSA and that awareness increasing activities should be promoted by senior management

Source: Created by the authors

Table 1.
Visualization of the coding process exemplifying how activities in included publications formed themes and sub-themes

more valuable responses. As such, a purposeful sampling strategy was used with the intention of recruiting participants who met those criteria (Marshall, 1996). The sampling criteria were:

- Should currently be working in a cybersecurity related position in a large public sector organization.
- Should have experience of working with CSA in large public sector organizations for several years.

Six participants, from different large public sector organizations in Sweden, were included in the research.

During the interviews, the participants were first asked about what they perceived to be good CSA practises. The taxonomy was then shown to the participants, and the participants were asked about their perception of it. The rationale for first asking questions about CSA was to allow participants to express their thoughts freely without being influenced by the taxonomy. The interviews were transcribed and analyzed using closed thematic coding (Braun and Clarke, 2006). The purpose of the analysis was to summarize the participants' perception of the taxonomy, identify if they described aspects that were missing and identify if they thought that some parts of the taxonomy could be removed. The analysis followed these steps and resulted in a table which is partially presented in Table 2:

(1) Transcription of the interview recordings

(2) Mark quotes which. . .
- . . .commented on the current taxonomy.
- . . .suggested modifications to the taxonomy.
- . . .suggested to remove something from the taxonomy.
- . . .suggested to add something to the taxonomy.

(3) Similar quotes from different participants were collected in themes.

(4) Quotes within the same theme was reviewed and the general opinion was identified.

(5) The interview results were summarized, and the summaries are presented in this article.

The general opinion was that the taxonomy was extensive, well-designed and summarized the main topics of the CSA in a way that would be practically useful. While they found that the taxonomy was accurate, several participants thought that it was too extensive and that some themes and subthemes could be combined to make it easier to get an overview of the taxonomy. All participants expressed that there was a significant overlap between "User Participation\& Engagement" and "Interest\& Motivation", one participant also expressed that "Cybersecurity Culture" was unnecessary, as cybersecurity culture is a goal of CSA rather than a part of it. Furthermore, it was expressed that "Cybersecurity Policies" was a too narrow topic for a main theme since laws and regulations are omitted by that term. Finally, one

Quote	Type	Theme	General opinion
It includes all the parts relevant for cybersecurity culture	Comment	Extensive taxonomy	The participants describe the taxonomy as extensive and includes what they perceived as the core topics for CSA. The taxonomy was described as containing too much information and reducing it would make it easier to comprehend
It could contain fewer factors to make it easier to absorb	Suggestion		
I recognize everything, but to see it so put together and compiled on a single page as this is fantastic	Comment		
There are a lot of things on one page that makes it very compact and a tad bit intimidating to grasp at first glance and some sub-factors are merely synonyms or examples of another so those could be combined with others, so focus on condensing and reducing the number of boxes without reducing the clarity and meaning of the guideline	Suggestion		

Source: Created by the authors

Table 2. Visualization of the coding of the first round of interviews (Quotes are translated from Swedish)

participant expressed a need to measure the effects of CSA activities as very important but lacking from the proposed taxonomy. Two participants also noted that that the taxonomy was not specific for public sector organizations and argued that it could be applied to any organization.

3.2 Design cycle 2

In the second design cycle, the taxonomy was revised and further evaluated. The modifications made are presented next.

3.2.1 Taxonomy development. Following the evaluation in design cycle 1, the following changes were made to the taxonomy:

- The number of themes was reduced from eight to six to make the taxonomy easier to overview, and to limit overlap between the themes. As a result, two changes were made. First, "User Participation and Engagement" and "Interest and Motivation" were combined into one theme named "User Participation, Engagement and Motivation". Second, "Cybersecurity Culture" was removed following the rationale that building a cybersecurity culture is the goal of everything in the taxonomy and therefore it does not require to be a theme.
- The second change was to rename the theme "Cybersecurity Policy" to "Governance of Information." The rationale was that the new name better includes laws and regulations. Three new subthemes were created to highlight the impact of laws on CSA.
- The last change was to add a subtheme called "measure effects of cybersecurity awareness work" to "Top Management Support" to ensure that measuring the effects of CSA activities is included in the taxonomy.

3.2.2 Practitioner interviews. The updated taxonomy was evaluated using the same process and participants as in design cycle 1. The interviews in this cycle focused on the changes made to the taxonomy and additional updates that were needed. The rationale for including the same participants again was that the time that passed since the first interviews could allow them to express ideas that they had thought about since then, in addition to any ideas that came up during the second interview. The interviews were again transcribed and analyzed using thematic coding (Braun and Clarke, 2006). The results of the interviews are summarized below.

The general perception was that the changes made the taxonomy more comprehensible without reducing its value. All participants expressed that it was now easier to get an overview of the taxonomy and that it could be a valuable tool for working with CSA within public sector organizations. Additionally, the addition of a subtheme to address measurability was considered positive by all participants. Several participants discussed the removal of "Cybersecurity Culture" as a theme. Although they agreed that it was not needed as a theme, since it is the implicit goal of everything in the taxonomy, they still argued that it needed to be highlighted in some way. Participants also suggested small changes that could be made to the taxonomy in two broad categories. First, it was suggested that some themes and subthemes could be renamed, and some subthemes combined to further limit the number of themes and subthemes. The second category contained suggestions on the addition of subthemes to show that it is important to provide users with time to participate in CSA activities.

3.2.3 Finalizing the taxonomy. The taxonomy was further revised following the input from the interviews. The changes were as follows:

- Emphasize the importance of cybersecurity culture by adding an overarching blue layer titled “Cybersecurity Culture” to the taxonomy.
- The names of all the subthemes were reviewed to ensure that they were accurately and precisely described. The language of several subthemes was updated in this process.
- The theme “Governance of Information” was renamed to “Governance”.
- The subthemes “Allocate time to cybersecurity awareness training” and “incentives” were added to the theme “User Participation, Engagement and Motivation” to highlight the importance of allowing time for CSA activities.

4. The taxonomy of factors that contribute to organizational CSA

It consists of six themes which reflect different areas of CSA practise. There are several sub-themes for each theme and those are suggestions for what could be included in the different areas of CSA practise. Cybersecurity culture is incorporated in the taxonomy as a blue box placed underneath to emphasize that cybersecurity culture is the goal of all CSA activities. The rest of this section will describe the six themes of the final taxonomy. The full taxonomy is visualized in Appendix.

4.1 Top management support

It well established that support from top management is essential to promote positive CSA behavior in organizations (Jouaibi *et al.*, 2022). Top management are able to allocate resources for CSA (Khando *et al.*, 2021). As leaders within the organization, managers can also act as role-models and thereby promote CSA activities. Khando *et al.* (2021) reinforces the importance of managers who show leadership because it is important to be a role model to motivate, engage and raise employees’ CSA. Khando *et al.* (2021) mentions that managerial security participation has one of the strongest effects on employees’ awareness. If managers are not engaged, nor will other members of the organization. Khando *et al.* (2021) continues by saying that top management support is critical for making cultural changes possible. Finally, this theme also highlights that the management has a large strategic responsibility to create strategies for CSA. The Top Management Support section of the taxonomy is displayed in Figure 4.

4.2 User attitudes and perceptions of cybersecurity

How humans interact with systems and processes needs to be acknowledged and understood if CSA in an organization is to be effectively addressed. Therefore, user-centred approaches must be integrated into organizations’ CSA programs to identify user needs, goals and capabilities as part of CSA efforts. The integration of strategies that aim to understand the human factor helps organizations reduce the risk of human errors and build a more positive cybersecurity culture (Ki-Aries and Faily, 2017). It is uncommon for organizations to have delved into what their users might need to raise their CSA based on their predisposition to cybersecurity. Consequently, these user-centred approaches must consider the user’s predisposition to cybersecurity when tailoring CSA for an individual’s needs and goals. These predispositions generally involve users’ individual attitudes and perceptions of cybersecurity, which are influenced by the organizations’ existing cybersecurity culture. For example, organizations need to reflect whether users want to comply with policies or not, if they are risk-tolerant or risk-averse and if they are accepting or resistant to cybersecurity. Understanding users feelings toward cybersecurity is essential to raise their CSA (Furnell and Vasileiou, 2017). Consequently, organizations should take user’s prior knowledge and experiences, user competencies, user

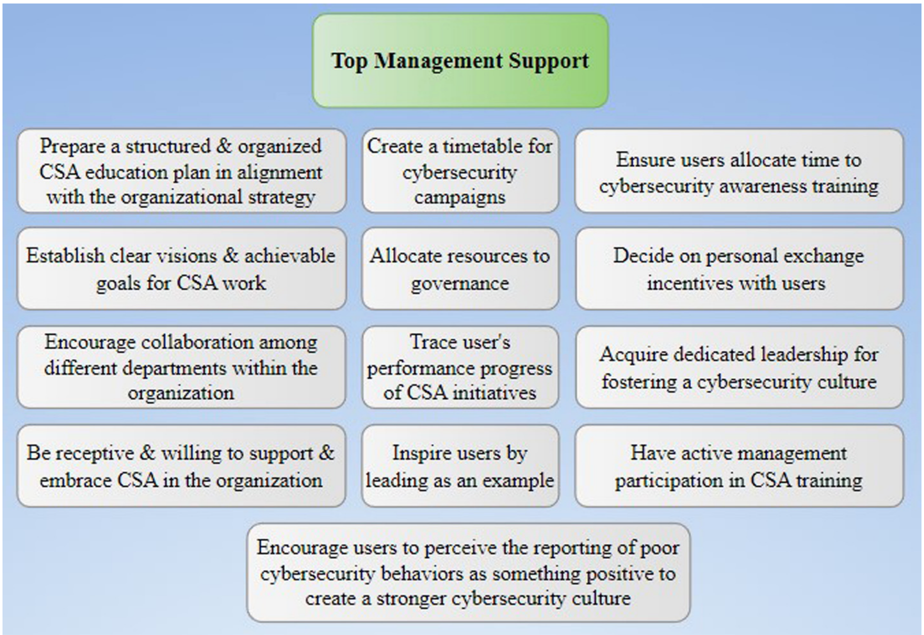

Top Management Support
Prepare a structured & organized CSA education plan in alignment with the organizational strategy
Create a timetable for cybersecurity campaigns
Ensure users allocate time to cybersecurity awareness training
Establish clear visions & achievable goals for CSA work
Allocate resources to governance
Decide on personal exchange incentives with users
Encourage collaboration among different departments within the organization
Trace user's performance progress of CSA initiatives
Acquire dedicated leadership for fostering a cybersecurity culture
Be receptive & willing to support & embrace CSA in the organization
Inspire users by leading as an example
Have active management participation in CSA training
Encourage users to perceive the reporting of poor cybersecurity behaviors as something positive to create a stronger cybersecurity culture

Figure 4. Top management support section of the taxonomy

Source: Created by the authors

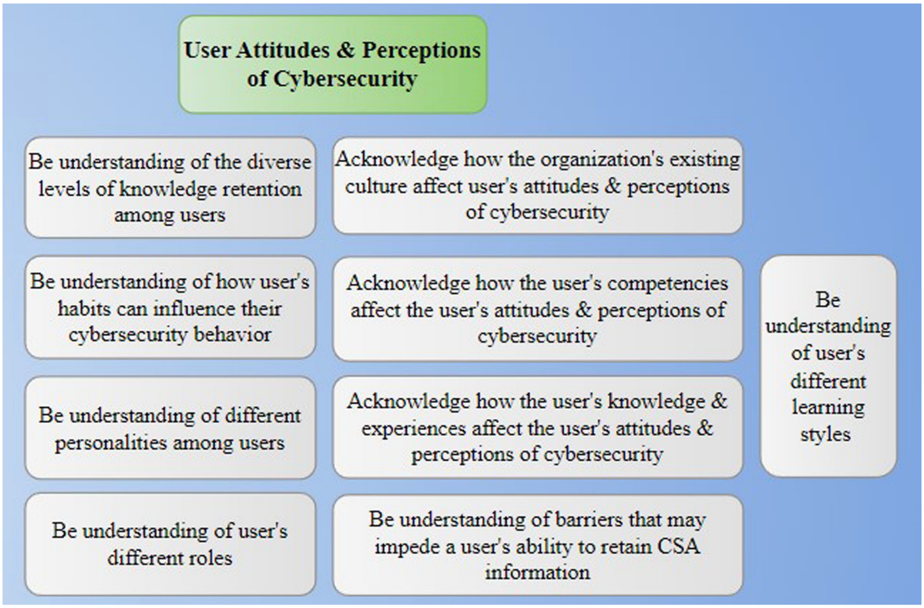
learning style, user barriers, user knowledge retention, user habit, user personality, etc., into account. Understanding personalities is also important (Tolah *et al.*, 2021). Organizations can, for instance, identify users that may be at risk of committing insider incidents through personality traits. The User Attitudes and Perceptions of Cybersecurity section of the taxonomy is displayed in Figure 5.

4.3 Cybersecurity advocates

Cybersecurity advocates encourage and facilitate the adoption of CSA best practices in organizations by advocating for beneficial security behaviors (Haney and Lutters, 2018). The taxonomy reflects traits that cybersecurity advocates often possess. Haney and Lutters (2018) highlights those traits by stating that it is essential for advocates to establish trust and be seen as reliable sources of information. Without having the ability to build trust and instill confidence in users, changing negative perceptions will not work. Additionally, advocates must have strong interpersonal skills to build relationships with managers and other users. Advocates can help to create a good understanding between departments. For example, the language used between technical and non-technical users can differ drastically and advocates can bridge the gap and translate concepts into words that various audiences can understand (Haney and Lutters, 2018). The Cybersecurity Advocates section of the taxonomy is displayed in Figure 6.

4.4 User participation, engagement and motivation

Reaching a state with an open and ongoing dialogue about cybersecurity is highly sought-after property for a security-aware organization. Such an environment requires the



User Attitudes & Perceptions of Cybersecurity

Be understanding of the diverse levels of knowledge retention among users

Acknowledge how the organization's existing culture affect user's attitudes & perceptions of cybersecurity

Be understanding of how user's habits can influence their cybersecurity behavior

Acknowledge how the user's competencies affect the user's attitudes & perceptions of cybersecurity

Be understanding of user's different learning styles

Be understanding of different personalities among users

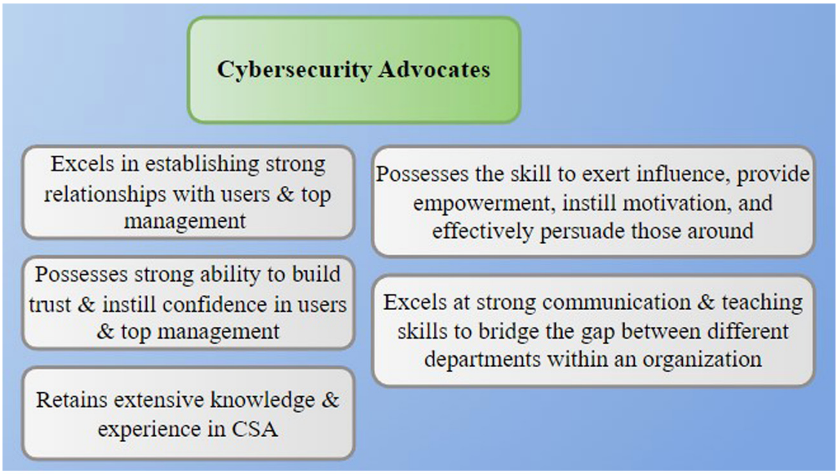
Acknowledge how the user's knowledge & experiences affect the user's attitudes & perceptions of cybersecurity

Be understanding of user's different roles

Be understanding of barriers that may impede a user's ability to retain CSA information

Source: Created by the authors

Figure 5. User attitudes and perceptions of cybersecurity section of the taxonomy



Cybersecurity Advocates

Excels in establishing strong relationships with users & top management

Possesses the skill to exert influence, provide empowerment, instill motivation, and effectively persuade those around

Possesses strong ability to build trust & instill confidence in users & top management

Excels at strong communication & teaching skills to bridge the gap between different departments within an organization

Retains extensive knowledge & experience in CSA

Source: Created by the authors

Figure 6. Cybersecurity advocates section of the taxonomy

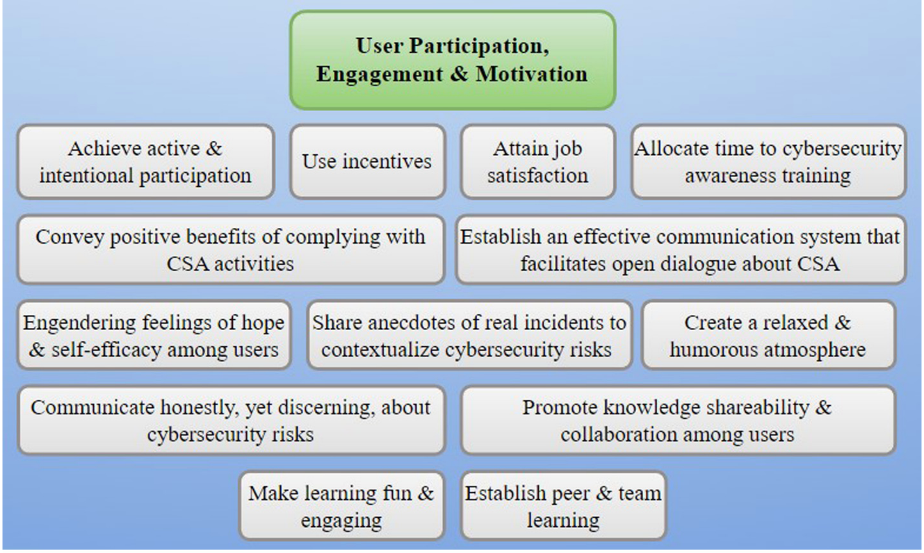
engagement and motivation of users. There are countless options for how to work toward that; for instance, organizations can provide users with the skills to increase self-efficacy with respect to CSA because users with higher self-efficacy are more motivated to participate in CSA initiatives and engage in positive security behaviors (Haney and Lutters, 2018). The sub-themes also demonstrate the importance of job satisfaction, a collaborative environment and peer learning are important factors for CSA. Furnell and Rajendran (2012) reinforces that job satisfaction is an important factor that influences cybersecurity behavior at work. For example, if users dislike their workplace, their interest in keeping it secure is reduced. The User Participation, Engagement and Motivation section of the taxonomy is displayed in Figure 7.

4.5 Governance

Governance is included in this taxonomy to highlight that regulatory requirements influence the CSA work of public sector organizations. Public organizations' governance differs from private organizations with public organizations' governance being more rigid. Governance in public organizations includes laws and regulations external to the organization that must be adhered to, and internal regulations such as policies, procedures, standards, best practices, programs and operating agreements related to the specific organization. The Governance section of the taxonomy is displayed in Figure 8.

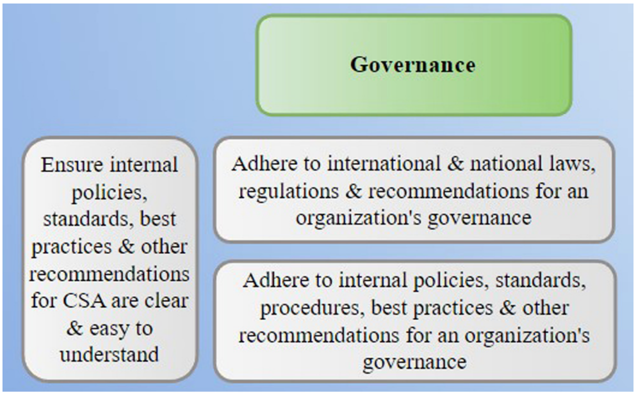
4.6 Cybersecurity education, training and awareness

Employing cybersecurity education, training and awareness programs in organizations is essential since they provide users with competencies and knowledge about cybersecurity (Khando *et al.*, 2021; Reeves *et al.*, 2021). CSA education, training and awareness programs aim to help users improve their ability to mitigate cybersecurity threats and become more aware of security (Abawajy, 2014). Without users who have this knowledge, fostering CSA is difficult. Education, training and awareness is frequently discussed in research and is a multifaceted topic. The many aspects of this theme are reflected in the various subthemes. Paterson (2021) reinforces the need to have tailored training and education within an organization and argues that choosing a one-size-fits-all approach is ineffective. This is because an organization needs to


User Participation, Engagement & Motivation
Achieve active & intentional participation
Use incentives
Attain job satisfaction
Allocate time to cybersecurity awareness training
Convey positive benefits of complying with CSA activities
Establish an effective communication system that facilitates open dialogue about CSA
Engendering feelings of hope & self-efficacy among users
Share anecdotes of real incidents to contextualize cybersecurity risks
Create a relaxed & humorous atmosphere
Communicate honestly, yet discerning, about cybersecurity risks
Promote knowledge shareability & collaboration among users
Make learning fun & engaging
Establish peer & team learning

Source: Created by the authors

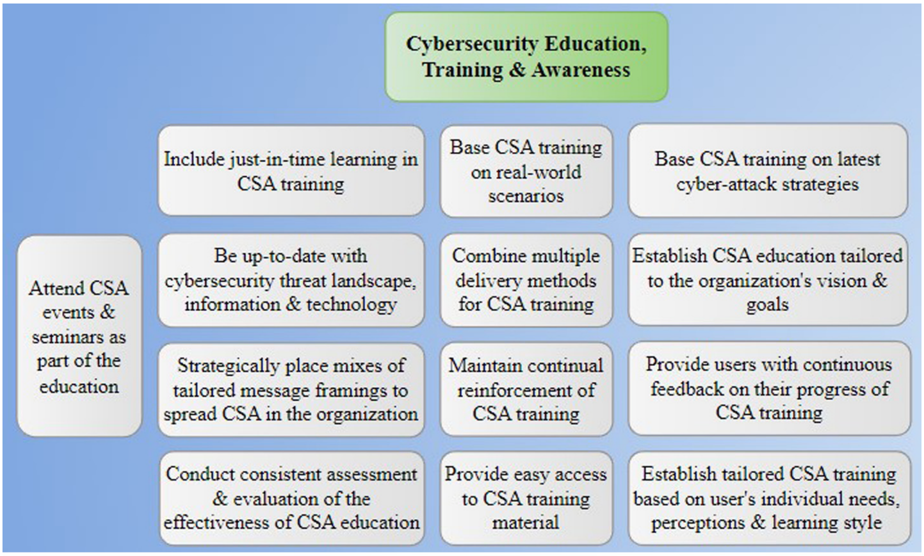
Figure 7. User participation, engagement and motivation section of the taxonomy


Governance
Ensure internal policies, standards, best practices & other recommendations for CSA are clear & easy to understand
Adhere to international & national laws, regulations & recommendations for an organization's governance
Adhere to internal policies, standards, procedures, best practices & other recommendations for an organization's governance

Source: Created by the authors

Figure 8. Governance section of the taxonomy

adjust its education and training to current threat conditions, the organizations current goals and the users' predispositions. Furthermore, training should be provided continuously and based on examples the users can relate to. To further respond to the heterogeneous nature of users, training should ideally be provided using different delivery methods such as game-based, simulation-based and online-based. For instance, game-based methods are typically highly interactive methods that challenge users and keep them interested and engaged, while simulation-based include simulations to assess users' susceptibility to different cyberattacks (Abawajy, 2014). The User Participation, Engagement and Motivation section of the taxonomy is displayed in Figure 9.


Cybersecurity Education, Training & Awareness
Include just-in-time learning in CSA training
Base CSA training on real-world scenarios
Base CSA training on latest cyber-attack strategies
Attend CSA events & seminars as part of the education
Be up-to-date with cybersecurity threat landscape, information & technology
Combine multiple delivery methods for CSA training
Establish CSA education tailored to the organization's vision & goals
Strategically place mixes of tailored message framings to spread CSA in the organization
Maintain continual reinforcement of CSA training
Provide users with continuous feedback on their progress of CSA training
Conduct consistent assessment & evaluation of the effectiveness of CSA education
Provide easy access to CSA training material
Establish tailored CSA training based on user's individual needs, perceptions & learning style

Source: Created by the authors

Figure 9. Cybersecurity education, training and awareness section of the taxonomy

5. Conclusions

The aim of this study was to develop a taxonomy of factors that contribute to organizational CSA. A design science approach was adopted with the goal of developing a taxonomy that could be used by practitioners. The taxonomy was first drafted using a literature review in which factors that contributed to CSA were identified from 71 existing research articles. The taxonomy was evaluated and refined in two rounds of semi-structured interviews with practitioners from large public organizations in Sweden. The final taxonomy is presented in Appendix and the section above. It presents six main themes representing different areas that impact organizational CSA. Furthermore, each main theme has several subthemes which represent possible processes and goals within the themes.

The primary outcome of this research is the developed taxonomy. Organizations can adopt it to create a roadmap for internal CSA practices. For example, an organization could assess how well it performs in the six main themes and use the subthemes as inspiration when deciding on CSA activities. The subthemes can be viewed as good practices where an organization may choose to adopt all or settle with adopting a subset. Similarly, different organizations may have different needs which may influence how they could use the taxonomy. The taxonomy developed in this research is based on a literature review and input from participants in large public organization. The taxonomy is, however, likely to be applicable for other types of organizations as well. That was also stated by several interview participants.

A second and more theoretical contribution of this research is that it highlights that CSA is a complex sociotechnical system where social, technical and organizational aspects affect each other in an intertwined way. For example, training is only effective when the material presented is easy to understand. To make the material easy to understand, technical prerequisites may have to be in place which require strategical decisions. On top of that, finding ways to measure CSA while maintaining the privacy of users, and avoiding sensitive usage information leaking to attackers, is sought after. In conclusion, this research demonstrates that CSA cannot be achieved with any silver bullet. Rather, it requires continuous and synchronized efforts in technology development, organizational culture, communication and promoting job satisfaction.

Regarding the limitations of this work, the first limitation is imposed by the selection of participants for this research, which included practitioners in large public organizations. First, large organizations are certainly more able to have large organizations around CSA (and cybersecurity in general) as opposed to smaller organizations. That was also the rationale for selection participants from those organizations. The developed taxonomy is extensive, and it is unseasonable to believe that it is a perfect fit for small and medium size organizations. All participants are also from Sweden which imposes another limitation. Regulations may differ between countries and the taxonomy may not be fully compatible with organizations in other countries. Owning to the fact that the purpose of the interviews was to refine a taxonomy based on the existing body of literature, the impact of the sampling frame limitations can be assumed to be small. Further, the themes and subthemes are generally framed to increase the applicability elsewhere. A further limitation is knowing to what extent the taxonomy is complete. While efforts have been made to ensure the completeness of this work, through the integration of previous research and practitioner interviews, it is possible that some aspects of CSA are missed. Furthermore, it is perhaps even possible that future research will uncover more aspects of CSA. This leaves a need for continuous revision of the taxonomy, but that will have to be left for future work.

The participants this research represent large public sector organizations in Sweden and the results should be interpreted with that in mind. As discussed during the interviews in this research it is, however, likely that other organizations can benefit from this research. To what extent the results applicable in other domains, and how the taxonomy needs to be modified to fit those domains are natural directions for future work. Further, this research presents a birds-eye view of CSA practise. Every subtheme can be implemented in different ways and there are different considerations that can be made. As such, future research focusing on detailing the optimal practises in the subthemes is reasonable.

References

Abawajy, J. (2014), "User preference of cyber security awareness delivery methods", *Behaviour and Information Technology*, Vol. 33 No. 3, pp. 237-248.

Abawajy, J. and Kim, T. (2010), "Performance analysis of cyber security awareness delivery methods", *Security Technology, Disaster Recovery and Business Continuity: International Conferences, SecTech and DRBC 2010, Held as Part of the Future Generation Information Technology Conference, FGIT 2010, Jeju Island, Korea,* December 13-15, 2010. Proceedings, pp.142-148.

Abu-Amara, F. and Tamimi, H. (2021), "Cyber shield security awareness program", *2021 8th International Conference on Computing for Sustainable Global Development (INDIACom)*, pp. 422-425.

Adelola, T., Dawson, R. and Batmaz, F. (2015), "The urgent need for an enforced awareness programme to create internet security awareness in Nigeria", *Proceedings of the 17th International Conference on Information Integration and Web-Based Applications and Services*, pp. 1-7.

Ahlan, A.R. and Lubis, M. (2011), "Information security awareness in university: maintaining learnability, performance and adaptability through roles of responsibility", *2011 7th International Conference on Information Assurance and Security (IAS)*, pp. 246-250.

Alahmari, A. and Duncan, B. (2020), "Cybersecurity risk management in small and medium-sized enterprises: a systematic review of recent evidence", *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, pp. 1-5.

Alahmari, S., Renaud, K. and Omoronyia, I. (2022), "Moving beyond cyber security awareness and training to engendering security knowledge sharing", *Information Systems and e-Business Management*, Vol. 21 No. 1, pp. 1-36.

Alanazi, M., Freeman, M. and Tootell, H. (2022), "Exploring the factors that influence the cybersecurity behaviors of young adults", *Computers in Human Behavior*, Vol. 136, p. 107376.

Albrechtsen, E. and Hovden, J. (2010), "Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study", *Computers and Security*, Vol. 29 No. 4, pp. 432-445.

Aldawood, H. and Skinner, G. (2018), "Educating and raising awareness on cyber security social engineering: a literature review", *In Proceedings of 2018 Ieee International Conference on Teaching, Assessment, and Learning for Engineering, IEEE (pp.62-68).* doi: 10.1109/TALE.2018.8615162.

Aldawood, H. and Skinner, G. (2019), "Reviewing cyber security social engineering training and awareness Programs-Pitfalls and ongoing issues", *Future Internet*, Vol. 11 No. 3, doi: 10.3390/fi11030073.

Al-Nuaimi, M.N. (2022), "Human and contextual factors influencing cyber-security in organizations, and implications for higher education institutions: a systematic review", *Global Knowledge, Memory and Communication*, Vol. 73 Nos 1/2.

Alshaikh, M., Maynard, S.B. and Ahmad, A. (2021), "Applying social marketing to evaluate current security education training and awareness programs in organisations", *Computers and Security*, Vol. 100, p. 102090.

Alzubaidi, A. (2021), "Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia", *Heliyon*, Vol. 7 No. 1, p. e06016.

Amjad, H.A.R., Zaffar, M.F., Naeem, U., Choo, K.K.R. and Zaffar, M.A. (2016), "Improving security awareness in the government sector", *ACM International Conference Proceeding Series*, 08-10-June-2016, 1-7. *Scopus*, doi: 10.1145/2912160.2912186.

Arbanas, K., Spremic, M. and Zajdela Hrustek, N. (2021), "Holistic framework for evaluating and improving information security culture", *Aslib Journal of Information Management*, Vol. 73 No. 5, pp. 699-719.

Bada, M. and Nurse, J.R. (2019), "Developing cybersecurity education and awareness programmes for small-and medium-sized enterprises (SMEs)", *Information and Computer Security*, Vol. 27 No. 3, pp. 393-410.

Bakari, J.K., Tarimo, C.N., Yngström, L., Magnusson, C. and Kowalski, S. (2007), "Bridging the gap between general management and technicians–a case study on ICT security in a developing country", *Computers and Security*, Vol. 26 No. 1, pp. 44-55.

Braun, V. and Clarke, V. (2006), "Using thematic analysis in psychology", *Qualitative Research in Psychology*, Vol. 3 No. 2, pp. 77-101, doi: 10.1191/1478088706qp063oa.

Caldwell, T. (2016), "Making security awareness training work", *Computer Fraud and Security*, Vol. 2016 No. 6, pp. 8-14, doi: 10.1016/S1361-3723(15)30046-4.

Chang, L.Y. and Coppel, N. (2020), "Building cyber security awareness in a developing country: lessons from Myanmar", *Computers and Security*, Vol. 97, p. 101959.

Chaudhary, S., Kompara, M., Pape, S. and Gkioulos, V. (2022), "Properties for cybersecurity awareness posters' design and quality assessment", *Proceedings of the 17th International Conference on Availability, Reliability and Security*, pp. 1-8.

Chumaera, M.M. and Ayu, M.A. (2022), "Assessing students' information security awareness through the knowledge, attitude, and behavior model", *2022 IEEE 8th International Conference on Computing, Engineering and Design (ICCED)*, pp. 1-6.

Chung, M. (2020), "Signs your cyber security is doomed to fail", *Computer Fraud and Security*, Vol. 2020 No. 3, pp. 10-13.

Cone, B.D., Irvine, C.E., Thompson, M.F. and Nguyen, T.D. (2007), "A video game for cyber security training and awareness", *Computers and Security*, Vol. 26 No. 1, pp. 63-72.

Cone, B.D., Thompson, M.F., Irvine, C.E. and Nguyen, T.D. (2006), "Cyber security training and awareness through game play", *Security and Privacy in Dynamic Environments: Proceedings of the IFIP TC-11 21st International Information Security Conference (SEC 2006)*, 22–24 May 2006, Karlstad, Sweden Vol. 21, pp. 431-436.

Dahabiyeh, L. (2021), "Factors affecting organizational adoption and acceptance of computer-based security awareness training tools", *Information and Computer Security*, Vol. 29 No. 5, doi: 10.1108/ICS-12-2020-0200.

De Bruijn, H. and Janssen, M. (2017), "Building cybersecurity awareness: the need for evidence-based framing strategies", *Government Information Quarterly*, Vol. 34 No. 1, pp. 1-7, doi: 10.1016/j.giq.2017.02.007.

Drevin, L., Kruger, H.A. and Steyn, T. (2007), "Value-focused assessment of ICT security awareness in an academic environment", *Computers and Security*, Vol. 26 No. 1, pp. 36-43.

Fielding, J. (2020), "The people problem: how cyber security's weakest link can become a formidable asset", *Computer Fraud and Security*, Vol. 2020 No. 1, pp. 6-9.

Fielding, J. (2021), "Building a culture of security", *Computer Fraud and Security*, Vol. 2021 No. 2, p. 20, doi: 10.1016/S1361-3723(21)00021-X.

Filipczuk, D., Mason, C. and Snow, S. (2019), "Using a game to explore notions of responsibility for cyber security in organisations", *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems*, pp. 1-6.

Furnell, S. and Rajendran, A. (2012), "Understanding the influences on information security behaviour", *Computer Fraud and Security*, Vol. 2012 No. 3, pp. 12-15, doi: 10.1016/S1361-3723(12)70053-2.

Furnell, S. and Vasileiou, I. (2017), "Security education and awareness: just let them burn?", *Network Security*, Vol. 2017 No. 12, pp. 5-9.

Georgiadou, A., Michalitsi-Psarrou, A. and Askounis, D. (2023), "A security awareness and competency evaluation in the energy sector", *Computers and Security*, Vol. 129, p. 103199.

Grant, M.J. and Booth, A. (2009), "A typology of reviews: an analysis of 14 review types and associated methodologies", *Health Information and Libraries Journal*, Vol. 26 No. 2, pp. 91-108.

Grassegger, T. and Nedbal, D. (2021), "The role of employees' information security awareness on the intention to resist social engineering", *Procedia Computer Science*, Vol. 181, pp. 59-66.

Gregor, S. and Hevner, A.R. (2013), "Positioning and presenting design science research for maximum impact", *MIS Quarterly*, Vol. 37 No. 2, pp. 337-355.

Hall, M. (2016), "Why people are key to cyber-security", *Network Security*, Vol. 2016 No. 6, pp. 9-10.

Haney, J.M. and Lutters, W.G. (2018), "It's scary ... it's confusing ... it's dull': how cybersecurity advocates overcome negative perceptions of security",pp. 411-425.

Hart, S., Margheri, A., Paci, F. and Sassone, V. (2020), "Riskio: a serious game for cyber security awareness and education", *Computers and Security*, Vol. 95, p. 101827.

Hevner, A.R. (2007), "A three cycle view of design science research", *Scandinavian Journal of Information Systems*, Vol. 19 No. 2, p. 4.

Hevner, A.R., March, S.T., Park, J. and Ram, S. (2004), "Design science in information systems research", *MIS Quarterly*, Vol. 28 No. 1, pp. 75-105, doi: 10.2307/25148625.

Jouaibi, R., Gaylard, A.K. and Lee, B. (2022), "Employee Cyber-Security awareness training (CSAT) programs in Ireland's financial institutions", *2022 Cyber Research Conference-Ireland (Cyber-RCI)*,pp. 1-4.

Kalhoro, S., Rehman, M., Ponnusamy, V. and Shaikh, F.B. (2021), "Extracting key factors of cyber hygiene behaviour among software engineers: a systematic literature review", *IEEE Access*, Vol. 9, pp. 99339-99363.

Kemper, G. (2019), "Improving employees' cyber security awareness", *Computer Fraud and Security*, Vol. 2019 No. 8, pp. 11-14.

Khando, K., Gao, S., Islam, S.M. and Salman, A. (2021), "Enhancing employees information security awareness in private and public organisations: a systematic literature review", *Computers and Security*, Vol. 106, p. 102267.

Ki-Aries, D. and Faily, S. (2017), "Persona-centred information security awareness", *Computers and Security*, Vol. 70, pp. 663-674.

Korovessis, P., Furnell, S., Papadaki, M. and Haskell-Dowland, P. (2017), "A toolkit approach to information security awareness and education", *Journal of Cybersecurity Education, Research and Practice*, Vol. 2017 No. 2, p. 5.

Kovačević, A., Putnik, N. and Tošković, O. (2020), "Factors related to cyber security behavior", *IEEE Access*, Vol. 8, pp. 125140-125148.

Li, L., Xu, L., He, W., Chen, Y. and Chen, H. (2016), "Cyber security awareness and its impact on employee's behavior", *Research and Practical Issues of Enterprise Information Systems: 10th IFIP WG 8.9 Working Conference, CONFENIS 2016, Vienna, Austria, December 13–14, 2016, Proceedings,* Vol. 10, pp. 103-111.

Mansfield-Devine, S. (2017), "Raising awareness: people are your last line of defence", *Computer Fraud and Security*, Vol. 2017 No. 11, pp. 10-14.

Marshall, M.N. (1996), "Sampling for qualitative research", *Family Practice*, Vol. 13 No. 6, pp. 522-526.

NIST (2023), "Awareness", available at: www.csrc.nist.gov/glossary/term/awareness

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M. and Jerram, C. (2014), "Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q)", *Computers and Security*, Vol. 42, pp. 165-176, doi: 10.1016/j.cose.2013.12.003.

Paterson, O. (2021), "Training is the foundation of security", *Computer Fraud and Security*, Vol. 2021 No. 8, pp. 10-13.

Peffers, K., Tuunanen, T., Rothenberger, M.A. and Chatterjee, S. (2007), "A design science research methodology for information systems research", *Journal of Management Information Systems*, Vol. 24 No. 3, pp. 45-77, doi: 10.2753/MIS0742-1222240302.

Power, R. and Forte, D. (2006), "Case study: a bold new approach to awareness and education, and how it met an ignoble fate", *Computer Fraud and Security*, Vol. 2006 No. 5, pp. 7-10.

Quayyum, F., Cruzes, D.S. and Jaccheri, L. (2021), "Cybersecurity awareness for children: a systematic literature review", *International Journal of Child-Computer Interaction*, Vol. 30, p. 100343.

Reeves, A., Calic, D. and Delfabbro, P. (2021), "Get a red-hot poker and open up my eyes, it's so boring" 1: Employee perceptions of cybersecurity training", *Computers and Security*, Vol. 106.

Renaud, K. (2018), "Cooking up security awareness and training", *Network Security*, Vol. 2018 No. 5, p. 20.

Rohan, R., Funilkul, S., Pal, D. and Chutimaskul, W. (2021), "Understanding of human factors in cybersecurity: a systematic literature review", *2021 International Conference on Computational Performance Evaluation (ComPE)*, pp. 133-140.

Rohan, R., Pal, D., Hautamäki, J., Funilkul, S., Chutimaskul, W. and Thapliyal, H. (2023), "A systematic literature review of cybersecurity scales assessing information security awareness", *Heliyon*, Vol. 9 No. 3.

Ruighaver, A.B., Maynard, S.B. and Chang, S. (2007), "Organisational security culture: extending the end-user perspective", *Computers and Security*, Vol. 26 No. 1, pp. 56-62.

Safa, N.S. and Maple, C. (2016), "Human errors in the information security realm–and how to fix them", *Computer Fraud and Security*, Vol. 2016 No. 9, pp. 17-20.

Safa, N.S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N.A. and Herawan, T. (2015), "Information security conscious care behaviour formation in organizations", *Computers and Security*, Vol. 53, pp. 65-78, doi: 10.1016/j.cose.2015.05.012.

Sardar, T. and Wahsheh, L.A. (2020), "Design of a cyber security awareness campaign to be implemented in a quarantine laboratory", *Journal of Computing Sciences in Colleges*, Vol. 35 No. 9, pp. 11-18.

Scholefield, S. and Shepherd, L.A. (2019), "Gamification techniques for raising cyber security awareness", *HCI for Cybersecurity, Privacy and Trust: First International Conference, HCI-CPT 2019, Held as Part of the 21st HCI International Conference, HCII 2019, Orlando, FL, USA, July 26–31, 2019, Proceedings*, 21, pp. 191-203.

Shaw, R.S., Chen, C.C., Harris, A.L. and Huang, H.-J. (2009), "The impact of information richness on information security awareness training effectiveness", *Computers and Education*, Vol. 52 No. 1, pp. 92-100.

Solomon, A., Michaelshvili, M., Bitton, R., Shapira, B., Rokach, L., Puzis, R. and Shabtai, A. (2022), "Contextual security awareness: a context-based approach for assessing the security awareness of users", *Knowledge-Based Systems*, Vol. 246, p. 108709.

Stahl, S. (2006), "Beyond information security awareness training: It's time to change the culture", *Inf. Secur. Manag. Handb*, Vol. 3 No. 3, p. 285.

Tariq, M.A., Brynielsson, J. and Artman, H. (2014), "The security awareness paradox: a case study", *2014 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM 2014)*, pp. 704-711.

Tasevski, P. (2016), "IT and cyber security awareness-raising campaigns", *Information and Security*, Vol. 34 No. 1, pp. 7-22.

Tirumala, S.S., Valluri, M.R. and Babu, G.A. (2019), "A survey on cybersecurity awareness concerns, practices and conceptual measures", *2019 International Conference on Computer Communication and Informatics, ICCCI 2019. Scopus*, doi: 10.1109/ICCCI.2019.8821951.

Tolah, A., Furnell, S.M. and Papadaki, M. (2021), "An empirical analysis of the information security culture key factors framework", *Computers and Security*, Vol. 108, p. 102354.

Tonkin, A., Kosasih, W., Grobler, M. and Nasim, M. (2022), "Simulating cyber security management: a gamified approach to executive decision making", *37th IEEE/ACM International Conference on Automated Software Engineering*, pp. 1-8.

Trim, P.R. and Lee, Y.-I. (2019), "The role of B2B marketers in increasing cyber security awareness and influencing behavioural change", *Industrial Marketing Management*, Vol. 83, pp. 224-238.

Tschakert, K.F. and Ngamsuriyaroj, S. (2019), "Effectiveness of and user preferences for security awareness training methodologies", *Heliyon*, Scopus, Vol. 5 No. 6, doi: 10.1016/j.heliyon.2019.e02010.

Uchendu, B., Nurse, J.R., Bada, M. and Furnell, S. (2021), "Developing a cyber security culture: current practices and future needs", *Computers and Security*, Vol. 109, p. 102387.

Wang, Y., Qi, B., Zou, H.-X. and Li, J.-X. (2018), "Framework of raising cyber security awareness", *2018 IEEE 18th International Conference on Communication Technology (ICCT)*, pp. 865-869, doi: 10.1109/ICCT.2018.8599967.

Whitman, M.E. (2004), "In defense of the realm: understanding the threats to information security", *International Journal of Information Management*, Vol. 24 No. 1, pp. 43-57.

Wong, L.-W., Lee, V.-H., Tan, G.W.-H., Ooi, K.-B. and Sohal, A. (2022), "The role of cybersecurity and policy awareness in shifting employee compliance attitudes: building supply chain capabilities", *International Journal of Information Management*, Vol. 66, p. 102520.

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F. and Basim, H.N. (2022), "Cyber security awareness, knowledge and behavior: a comparative study", *Journal of Computer Information Systems*, Vol. 62 No. 1, pp. 82-97.

Further reading

Aman, W. and Al Shukaili, J. (2021), "A classification of essential factors for the development and implementation of cyber security strategy in public sector organizations", *International Journal of Advanced Computer Science and Applications*, Vol. 12 No. 8.

Eurostat (2016), "Glossary: Enterprise size", available at: www.ec.europa.eu/eurostat/statistics-explained/index.php?title=Glossary:Enterprise_size

IPPF (2014), *Assessing Organizational Governance in the Public Sector*, *The Institute of Internal Auditors Global*.

Kovačević, A. and Radenković, S.D. (2020), "SAWIT-security awareness improvement tool in the workplace", *Applied Sciences*, Scopus,Vol. 10 No. 9, doi: 10.3390/app10093065.

Tu, C.Z., Yuan, Y., Archer, N. and Connelly, C.E. (2018), "Strategic value alignment for information security management: a critical success factor analysis", *Information and Computer Security*, Vol. 26 No. 2, pp. 150-170.

Appendix

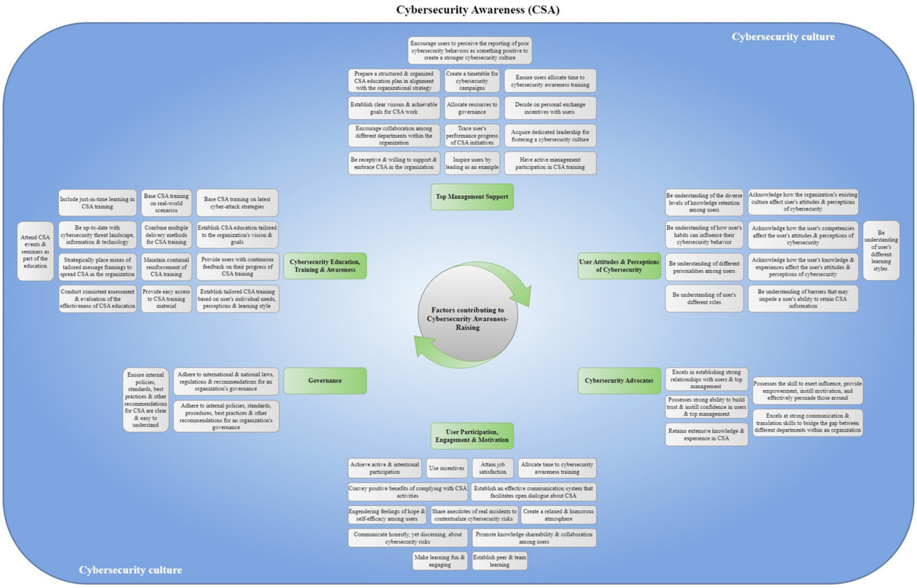

Cybersecurity Awareness (CSA)
Cybersecurity culture
Encourage users to perceive the reporting of poor cybersecurity behaviors as something positive to create a stronger cybersecurity culture
Prepare a structured & organized CSA education plan in alignment with the organizational strategy
Create a timetable for cybersecurity campaigns
Ensure users allocate time to cybersecurity awareness training
Establish clear visions & achievable goals for CSA work
Allocate resources to governance
Decide on personal exchange incentives with users
Encourage collaboration among different departments within the organization
Trace user's performance progress of CSA initiatives
Acquire dedicated leadership for fostering a cybersecurity culture
Be receptive & willing to support & embrace CSA in the organization
Inspire users by leading as an example
Have active management participation in CSA training
Top Management Support
Include just-in-time learning in CSA training
Base CSA training on real-world scenarios
Base CSA training on latest cyber-attack strategies
Attend CSA events & seminars as part of the education
Be up-to-date with cybersecurity threat landscape, information & technology
Combine multiple delivery methods for CSA training
Establish CSA education tailored to the organization's vision & goals
Strategically place mixes of tailored message framings to spread CSA in the organization
Maintain continual reinforcement of CSA training
Provide users with continuous feedback on their progress of CSA training
Conduct consistent assessment & evaluation of the effectiveness of CSA education
Provide easy access to CSA training material
Establish tailored CSA training based on user's individual needs, perceptions & learning style
Cybersecurity Education, Training & Awareness
Be understanding of the diverse levels of knowledge retention among users
Acknowledge how the organization's existing culture affect user's attitudes & perceptions of cybersecurity
Be understanding of how user's habits can influence their cybersecurity behavior
Acknowledge how the user's competencies affect the user's attitudes & perceptions of cybersecurity
Be understanding of user's different learning styles
User Attitudes & Perceptions of Cybersecurity
Be understanding of different personalities among users
Acknowledge how the user's knowledge & experiences affect the user's attitudes & perceptions of cybersecurity
Be understanding of user's different roles
Be understanding of barriers that may impede a user's ability to retain CSA information
Factors contributing to Cybersecurity Awareness-Raising
Ensure internal policies, standards, best practices & other recommendations for CSA are clear & easy to understand
Adhere to international & national laws, regulations & recommendations for an organization's governance
Adhere to internal policies, standards, procedures, best practices & other recommendations for an organization's governance
Governance
Cybersecurity Advocates
Excels in establishing strong relationships with users & top management
Possesses strong ability to build trust & instill confidence in users & top management
Retains extensive knowledge & experience in CSA
Possesses the skill to exert influence, provide empowerment, instill motivation, and effectively persuade those around
Excels at strong communication & translation skills to bridge the gap between different departments within an organization
User Participation, Engagement & Motivation
Achieve active & intentional participation
Use incentives
Attain job satisfaction
Allocate time to cybersecurity awareness training
Convey positive benefits of complying with CSA activities
Establish an effective communication system that facilitates open dialogue about CSA
Engendering feelings of hope & self-efficacy among users
Share anecdotes of real incidents to contextualize cybersecurity risks
Create a relaxed & humorous atmosphere
Communicate honestly, yet discerning, about cybersecurity risks
Promote knowledge shareability & collaboration among users
Make learning fun & engaging
Establish peer & team learning
Cybersecurity culture

Figure A1.
Final taxonomy

Source: Created by the authors

Corresponding author

Joakim Kävrestad can be contacted at: joakim.kavrestad@ju.se