Factors influencing the adoption of awareness-raising activities in SMEs

Erik Bergström[1,*], Joakim Kävrestad[1], Johannes Hou Gustafsson[1] and Hannes Jonsson[1]

[1]Department of Computer Science and Informatics, School of Engineering, Jönköping University, Jönköping, Sweden.

Abstract

Information security incidents are most commonly caused by user behaviour, placing the user in focus. In order to mitigate information security threats and thereby protect the organisation, more and more are adopting a socio-technical viewpoint, which implies adopting the belief that information security cannot be solved with technology alone. A common way to address the user is by adopting awareness-raising activities. All types of organisations struggle to raise awareness. Several studies have pointed out small and medium-sized enterprises (SMEs) as being extra vulnerable and, in addition, having more issues adopting awareness-raising activities. There are few studies investigating factors influencing the adoption of awareness-raising activities in general, and the body of literature is even more scarce when focusing on the factors from an SME perspective. This study targets the gap by investigating what factors influence the adoption of awareness-raising activities in SMEs. We did this by conducting a semi-structured interview study in 10 organisations. Five factors with a total of seven sub-factors were found: Resources (with the sub-factors time and cost), implementation, content (with the sub-factors quality, adaptability, and comprehensibility), compliance, management (with the sub-factors management support and motivation of the employees).

Keywords

Information security awareness, adoption factors, small and medium-sized enterprises

1. Introduction

It is estimated that a cyberattack occurs somewhere in the world every 39 seconds and costs businesses an average of $4.45 million in 2023 [1, 2]. Most of these attacks directly or indirectly target small and medium-sized enterprises (SMEs). SMEs are particularly vulnerable as they often do not have the capabilities or resources that larger companies have to secure their environment and train their employees to be more aware of information security [3]. Furthermore, ENISA (European Union Agency for Cybersecurity) describes that SMEs often work with critical information. Consequently, severe consequences could result if SMEs are compromised [4]. ENISA also shows that SMEs struggle to maintain sufficient information security awareness and establish a high level of protection for sensitive information [4].

The problem of low information security awareness was addressed in, for example, Erdogan et al.'s [5] paper on SME awareness and capabilities, where only 50% of the respondents rated

The 10th International Conference on Socio-Technical Perspectives in IS (STPIS'24) August 16-17 2024 Jönköping, Sweden.
*Corresponding author.
erik.bergstrom@ju.se (E. Bergström); joakim.kavrestad@ju.se (J. Kävrestad)
0000-0002-1436-2980 (E. Bergström); 0000-0003-2084-9119 (J. Kävrestad)

their awareness as moderate or higher. The human factor plays a major role in a company's information security, as it is becoming increasingly popular to carry out cyber attacks by exploiting employees. A report by Verizon Business [6] showed that 74% of data breaches were due to a lack of knowledge among employees. These breaches occur when employees lack the knowledge and security awareness to make the correct decisions when faced with a cyber threat [3]. To prevent social engineering, i.e. attacks that focus on tricking people into either giving out information or performing certain actions for malicious purposes, companies should adopt awareness-raising training and build a robust information security culture among employees [7].

The problems for SMEs lie in adopting awareness-raising activities and motivating employees to comply with company security policies. By creating a solid security culture among the company's employees and choosing the activities that best suit the company, companies can increase their information security and minimise the risk of data breaches [8]. Previous studies have focused on problems SMEs encounter when adopting awareness-raising activities to raise employee awareness, where employee motivation is often highlighted. SMEs need to choose the most suitable activity, where several options are available, such as text-based and instructor-based learning activities [9].

When adopting awareness-raising activities, SMEs face several factors influencing their choice and the extent to which they can adopt them. Heidt et al. [10] highlight that SMEs must consider financial, time and skill constraints when adopting activities. SMEs, compared to larger companies, do not have the same budget and, therefore, do not have the same opportunity to adopt awareness-raising activities to the extent that large companies can. This is worrying since studies show that the majority of SMEs close down after a major attack [1]. SME employees do not always have just one role. Someone who is a financial manager may also be in charge of IT, which means that the person in question does not have the time needed to investigate which solution is best for the company or to adopt activities correctly. This also affects competence, as SMEs do not always have dedicated IT staff; if they do, the IT staff often has sole responsibility for their environment. Therefore, managers must have the time and the skills to identify their business needs to adopt the most relevant activities [10].

We posit that information security is a socio-technical system (STS) where the interplay between technology, user and the organisation at large is paramount for the effectiveness of the system, in this case, the level of information security. Furthermore, the system entities are co-dependant and heavily influenced by each other [11]. Consider, for example, password-based authentication [12]. Technological rules will dictate what passwords users can create, policies establish rules for handling the passwords and users are ultimately responsible for creating the passwords and correctly handling them. Empowering the users will increase their ability to comply with technical and organisational rules. Likewise, adapting the technical implementation to the abilities of the users will make the users more able to comply [13].

This research explores SME adoption of awareness-raising activities through a socio-technical lens. How and why SMEs adopt different awareness-raising activities has not been extensively researched but is fundamental in understanding the motivations and obstacles SMEs face when adopting awareness-raising activities [14, 10]. This research takes its starting point in this problem and has focused on the following research question: *"What factors influence the adoption of awareness-raising activities in SMEs?"*

2. Background

2.1. Awareness-raising activities

Information security awareness can be defined as an employee's general awareness of information security and knowledge of the company's information security policies [15]. The role of information security awareness in an organisation, according to Khan et al. [16], is to ensure that employees are aware of applicable rules, regulations and policies. Through this awareness, employees can make informed decisions about information security.

Companies increasingly use different activities to raise employee awareness of security threats [3]. Employees in organisations need the right behaviours, knowledge, and attitudes to make the right decisions when technological protections cannot filter out the threats, which often occur via social engineering attacks. Organisations can minimise the risk of data breaches or other incidents by educating and preparing employees for the threats. Several methods exist to train employees, including instructor-based, text-based, and video-based training [9]. Instructor-based training is performed for a specific amount of time in a room with an instructor and is often perceived by employees as time-consuming [17]. Text-based interventions include information provided through emails or newsletters at regular intervals. Text-based training allows the user to read at their own pace and enables them to re-read if the information is difficult to understand. Still, it is difficult to force employees to consume the material. Video-based training uses videos, like text-based measures, allowing employees to revisit if something is unclear [9].

Organisations have many security awareness-raising activities to choose from, but a common problem is motivating employees to participate in and absorb information from the different activities. Previous publications show that employees feel bored with many types of activities, where, for example, instructor-led elements were highlighted as *"boring statement of policies and procedures"* [18, p. 250]. In addition, employees often lack motivation to participate in organisations' training programs as they feel they are not rewarded for the time spent on these activities. It is not enough for companies to only implement awareness-raising training; they must also adapt it to fit the employees. According to a study by Kävrestad et al. [19], the preferred delivery method for training is relevant and short sequences, such as password hints, when creating passwords. Their study also showed that the least preferred delivery method for training was through physical sessions attended at a specific time. Similarly, Johansson et al. [20] found that small, focused, and contained modules were preferred among SMEs in the manufacturing sector.

Chaudhary et al. [3] describes SMEs as companies with limited resources and with employees who fill more than one role in the organisation. Recommendations and frameworks exist to support SMEs in raising awareness of the company and employees by helping them prioritise what should be adopted based on their resources and making the whole adoption process more straightforward and easier to understand. However, studies show that the frameworks and models available to SMEs do not provide the support they need. For instance, there are no frameworks tailored to all the sectors in which SMEs are active [3]. Supporting SMEs in the domain of awareness-increasing activities is a goal of several authorities. ENISA, for instance, provide a tool called awareness-raising in a box (AR-in-a-box) to help SMEs work

with awareness-raising techniques [21]. Also, various national initiatives (such as The Swedish Civil Contingencies Agency [22]) offer information security training, guidance, templates, and advice for organisations regarding information security. In addition, there are directives aimed at creating a high level of readiness among companies and helping them prepare to defend against current and future threats. For example, the NIS2 directive will affect several sectors, including chemical manufacturing, food production and digital infrastructure in Europe [22].

SMEs need to choose the training that best suits the company and its employees and ensure the training is tailored to the needs of the company and its employees. Employees are more likely to absorb the presented information if they can relate it to their role within the organisation or the company's needs [18]. Furthermore, it is highlighted that if the information is related to employees' personal lives and how it can improve their safety at home and work, employees are more motivated to receive and apply the information [18].

2.2. Factors influencing the introduction of awareness-raising activities

While it is important to adopt awareness-raising activities, the organisation must strive for an activity that suits them, as one of the most critical factors in raising security awareness is the choice of activities. In a study by Dahabiyeh [9], the Technology-Organisation-Environment (TOE) (developed by Tornatzky et al. [23]) highlighted factors that influence organisations' adoption of new technologies. Dahabiyeh [9] used TOE to discuss the factors that influenced organisations' choice of information security awareness-raising measures, where the focus was computer-based tools. The technology aspect highlighted the factors of how easy the activity is to use and implement, the quality of the content, the integration and how easy it is for the organisation to adapt the content to their needs. From an organisational point of view, the support of the management team, the employees' commitment, and a dedicated IT security team were considered the most important factors. From the environmental point of view, two factors were considered to be most important, with the support of those delivering activities being considered important, including customer care and their technical competence. In addition, compliance was highlighted as an important factor [9].

SMEs often do not have the resources to adopt awareness-raising activities, as a study by Heidt et al. [10] showed. All those who participated in their study highlighted the lack of resources as an obstacle, where budget, time and workforce took up most of them. The budget was the main factor highlighted by management, and they did not have the finances to invest in activities but instead had to spend it on investments to increase the company's financial profit. Heidt et al. [10] found that the most commonly raised factor, regardless of the role in the company, was time constraints. Employees felt there was no time to adopt awareness-raising activities [10]. SMEs usually have employees with more than one role in the company and, therefore, do not have the time to read up and educate themselves on the best options for the company. Without dedicated information security staff, it is possible that SMEs do not have the skills and knowledge to understand why awareness-raising training is needed or how to implement it, and it is likely they end up choosing and prioritising the economic growth of the company [10].

3. Research approach

To be able to investigate what factors influence SMEs when adopting awareness-raising measures, we opted for a qualitative research approach. The study has been conducted by collecting data using semi-structured interviews and analysing that data thematically. Recent studies on awareness in SMEs have successfully used a similar approach with semi-structured interviews as a basis (e.g. [20, 24, 25]).

3.1. Data collection

Interviews are widely used for gathering data in qualitative research and can be performed in various ways [26]. As the aim of the study is exploratory, semi-structured interviews were selected as they allow the respondent to elaborate on their answers [27, 28], and because the interviewer can raise ideas and questions that emerge during the interview [29]. Thornhill et al. [30] highlight that semi-structured interviews allow, for example, the exploration of the ideas and word choices of the respondents, which in turn can lead to more in-depth answers and a deeper understanding. Qualitative interviews are designed to generate more detailed and in-depth data, which is useful when studying *"why"* factors [31].

Semi-structured interviews are characterized by open-ended questions and an interview guide where a broader theme is developed [28]. In this research, an interview guide was created and revised after the first interview. The guide consisted of three parts: an introductory part aimed at collecting background data on the respondent, a part that aimed at collecting more general data on how they work with awareness-raising activities, and the main part of the guide focusing on eliciting the adoption of awareness-raising activities. In the first part, a typical question was, *"How long have you been doing this?"* In the second part, *"How are you currently working on raising information security awareness?"* Finally, in the last part, we used questions like *"What factors limited the adoption of that specific activity?"*

Respondents were recruited through various channels, such as, emails available on company websites and via LinkedIn's message function. Around 60 company representatives were asked for an interview, but unfortunately, the majority of them did not respond to the request. Some respondents declined because they did not feel confident in their knowledge of the subject or because they did not have time, but we also know that security-related topics generally have issues finding participants [32, 33, 34]. In total, ten respondents who work at SMEs in different types of industries were interviewed. Table 1 shows an overview of the respondents and their experience of their current role.

The interviews were conducted using online conferencing software that allowed for the recording of the interviews. All interviews were recorded and transcribed.

3.2. Analysis

Thematic analysis was chosen to analyse the data from the semi-structured interviews. The thematic analysis focuses on identifying, analysing and interpreting themes from qualitative data [35]. When applying thematic analysis and identifying themes, looking for repetition, differences, and similarities is important [36]. The coding guidelines from Saldaña [36] were

Table 1
Overview of the respondents and their level of experience.

Respondent	Title	Experience
1	Operations engineer/IT architect	<5 years
2	Chief financial officer/Chief information officer	>5 years
3	IT manager	>5 years
4	System developer	>5 years
5	IT security engineer	<5 years
6	IT technician	>5 years
7	IT manager	<5 years
8	IT manager	<5 years
9	Chief information security officer	<5 years
10	IT operations manager	<5 years

followed. More specifically, a two-cycle coding procedure was adopted. The first cycle used structural coding, which is especially suitable when the data comes from semi-structured interviews [36]. In structural coding, large segments of text form the basis for in-depth analysis [37]. After this step, codes are developed that are categorised based on similarities, differences, and repetition [36]. Busetto et al. [28] highlight that it is important that at least two researchers are involved during the coding process, especially at the beginning, so it is possible to compare the coding to ensure that coding is applied consistently to the data [28]. Therefore, the data coding was first carried out individually by two authors, and then the categories identified were compared and consolidated jointly. The final process of deriving the themes was a joint effort. In this case, the themes were the factors found to influence the adoption of awareness-raising activities.

4. Results

The thematic analysis resulted in the identification of 5 factors with a total of 7 sub-factors. The following factors were found: *Resources* (with the sub-factors *time* and *cost*), *implementation*, *content* (with the sub-factors *quality*, *adaptability*, and *comprehensibility*), *compliance*, *management* (with the sub-factors *management support* and *motivation of the employees*).

4.1. Resources

Resources was found to contain two sub-factors: *time* and *cost*. Several respondents mentioned that *time* is a factor that affects them greatly, both when introducing and investigating new activities. Respondent 1 explains that the reason why they have not introduced even more awareness-raising activities is that *"we are a small company with few employees, and it's really only me who works with this ... and I have other things to do."* Several of the respondents raise similar arguments as to why they have not adopted more activities. Some respondents also expressed the time it takes to carry out the training, with staff feeling that they do not have time to, for example, do micro-training or attend lectures on information security because they

are already too busy. The *cost* was a well-discussed factor. The respondents were split into two groups: those who felt constrained by the costs and those who saw the costs as secondary to the potential benefit of raising awareness in the organisation. This can be exemplified by Respondent 1, who said: *"that it shouldn't cost too much is quite important because as we are a small company...* [where] *costs are a big issue,"* whereas Respondent 2 puts less emphasis on cost: *"money is secondary in the context of security."*

4.2. Implementation

Being able to *implement* an awareness-raising activity easily is considered an important factor by the respondents. Some respondents wanted measures that come pre-packaged by an external party so they don't have to spend too much time on them. Preferably, the activity should also be easy to manage after the implementation. This can be exemplified by Respondent 2: *"It is easier when you get it served by an external party so you do not have to sit and work on the issue yourself."*

4.3. Content

The *content* contained three sub-factors: *quality*, *adaptability* and *comprehensibility*. The respondents emphasise that the *quality* of the activity's content is important. What constitutes higher-quality material is, of course, something subjective. Here, it can be summarised from the respondents' descriptions as material that is not substandard and that the employees would not understand or consider when exposed to it. Interesting to note is that none of the respondents worked with the content quality actively to try to raise the level. Some respondents also address why they consider the information in awareness-raising activities should be *comprehensible*. For example, Respondent 5 explained that the quality of the content can be very high, but what is important is that employees can easily absorb the information: *"in the end, you can have the world's most high-quality material that does no good if no one reads it, so comprehensibility, there should be a very low threshold there, to absorb the information, so people actually do it."* Furthermore, it was explained that content needs to be *adapted* to the company's lowest level and that there are often very different digital maturity levels. That is to say, that content needs to be adapted in various ways, but most respondents did not adapt their awareness-raising activities. Especially the ones using micro-training did not adapt the content to fit the organisation. Respondents that used newsletters customised them for the threats they considered relevant at the moment, but other than that, they did not adapt them to fit the organisation either.

4.4. Compliance

Compliance is a factor that can potentially positively impact awareness-raising activities. As discussed previously, there is no guarantee that employees will remember the information in the awareness-raising activity. Depending on the type of awareness-raising activity, there are different possibilities from a compliance perspective. For example, newsletters and lectures were seen as difficult activities from a compliance perspective, i.e., the respondents had difficulties knowing if their employees actively read or absorbed the information. On the other hand,

activities like micro-training and simulated phishing attacks were seen as compliance enablers as they came with a built-in option to track statistics on completion rates and how many employees clicked on phishing emails. I.e., it allows the manager to measure the awareness temperature in the organisation or, as Respondent 9 phrased it: *"There* [in our micro-training system] *we have continuous monitoring and measurement."*

4.5. Management

Finally, *management* is a factor that contains two sub-factors: *management support* and how the management works with the *motivation of the employees*. Most respondents considered the support of management crucial. There was a belief in a need for management support for information security in general, but also that the management showed its commitment to the activities selected. By actively showing support, preferably repeatedly over time, the employees understand the importance of the activities. It was emphasised that management support should come not only from the highest level but also from other managers, such as IT managers. IT managers also explained that they needed support from upper management in terms of time, in this case, so that they could spend the necessary time to research possible future activities, properly implement activities, and to be able to follow up on the results. Motivating employees to take part in the awareness-raising activities was seen as a difficulty, or as it was described by Respondent 4: *"The first difficulty that I see is that people should understand that they should do it and then actually do it."* How the organisation worked to motivate employees differed. Several respondents talked directly to the employees since the investigated organisations were SMEs and hence had smaller organisations. The managers tried to explain why they had chosen their activities and why it was important that they take part in them. All respondents except one used a normative approach (i.e., moral reasoning and the values behind it). One respondent used a coercive approach (i.e., threats and punishments) by employing scare tactics. The normative group tried to highlight why taking part was good for the organisation and what could happen if there was an attack. The motivation of the employees to actively participate in an awareness-raising activity was seen as a very important factor, as without active participation, it doesn't matter what activities to adopt; the employee would not be actively involved anyway. I.e., employee motivation is crucial for the adoption of awareness-raising activities.

5. Discussion

This paper has investigated factors influencing the adoption of awareness-raising activities in SMEs. A number of factors were found, and a summary of these factors can be found in Table 2.

A recurring theme that emerged from the interviews was that *management* needs to be more engaged in awareness-raising activities. This is achieved by giving those responsible more time to work on these issues and by being involved in the adoption process to show employees that this is an important issue. These results are in line with, for example, Renaud [38] and Chaudhary et al. [3]. Management involvement in awareness-raising activities is crucial, and we know that awareness-raising activities are most effective when management fully *supports* them, as employees are more likely to participate more actively in these activities if they can see that management is dedicated to the issue. Much literature on the topic is getting

Table 2
Summary of the factors found that influence the adoption of awareness-raising activities, including a description of the factors.

Factor	Description
Resources	
Time	There is a lack of time for introducing and investigating new activities and carrying out the training.
Cost	Split into two groups: the ones feeling constrained by costs and the ones who perceive the cost to be secondary to the benefit.
Implementation	Implementation and maintenance should be easy. They should preferably come as pre-packaged solutions.
Content	
Quality	Content should be of a high standard, and users should understand and consider it when exposed.
Comprehensibility	Users should easily be able to absorb the content.
Adaptability	It should be possible to adapt the content to organisational needs and for users on different levels.
Compliance	Depending on the awareness-raising activity, there are different possibilities for tracking completion and absorption rates.
Management	
Management support	Show support by giving more time to work on awareness-raising activities and be active in the adoption process.
Motivation of the employees	Employee motivation for actively participating in awareness-raising activities.

somewhat old, and the advice for engaging management (e.g. by explaining the cost-benefit of awareness-raising activities [39], to design and utilise low-cost awareness-raising activities [40, 41], and to show that awareness-raising activities are effective [42]) does not seem to work, at least not for SMEs. Some newer suggestions could be interesting to pursue to see if they could affect SME management, for example, to utilise peer comparisons through benchmarking, illustrating to leadership the investments competitors are doing [3]. Our study also arrives at a slightly different conclusion than Dahabiyeh's [9] study that found management not as important a factor as we do in this study. Perhaps this can be explained by our respondents' perceptions of the limitations regarding available resources. There is also how management works to motivate the employees to partake in awareness-raising activities. Here, we found that all except one used a normative approach, which is an interesting find since previous literature has shown inconsistent findings [43], and there are many calls for more research on this aspect [43, 44].

Related to management is *resources*, as management can affect *time* constraints and *costs*. The respondents highlighted that IT managers need more time to implement and maintain awareness-raising activities. Also, the cost was found to be an obstacle, which has been observed as a general SME problem [18] as fewer financial resources imply having to choose between awareness-raising activities or economic growth. As this is such a big issue where the majority of companies are struggling, we recommend numerous national and international initiatives,

such as AR-in-a-box [21], to ramp up their marketing as the awareness of the initiatives is low. Another way to increase such initiatives' usage is to (further) adapt them to various sectors (e.g. manufacturing, healthcare, etc.) to make them more relevant for the target groups. It is also interesting to study in future research as little is known about the adaptation to different user groups or, for that matter, what types of user groups exist.

Several of the respondents thought that the *quality* of the *content* of the awareness-raising activity was the most important aspect. Previous research, such as He and Zhang [18], has discussed the importance of activities that should be adapted to the level of the employee so that the content is *comprehensible*. Here, we found that the respondents acknowledged this, but very few of them worked with this type of adaptation due to resource limitations. In general, *adaptability* was considered important, which is consistent with Dahabiyeh [9], but again, the respondents did not do it in practice. This further strengthens the argument above about the necessity to adapt awareness-raising activities sectorally and to different user groups so that the ones implementing them in the organisation can easily push out suitable content on the correct level to their colleagues. Especially since we know that the quality of the content is highlighted as a critical factor in successful awareness-raising activities [3].

Related to *implementation* is integration, which was raised in Dahabiyeh's [9] study as a factor, but this study showed that integration was not something respondents considered important. This may be due to the fact that SMEs rarely have systems that can be regarded as necessary for integrating awareness-raising activities. Regarding implementation, we found that pre-packaged content by an external provider was favoured among the respondents. Similarly, it should be easy to manage after the implementation. So, yet again, we find a gap between content providers and their users.

Finally, *compliance* was found to be a factor that ultimately can affect the type of activities to be adopted. Depending on the type of activity, there are different possibilities for tracking completion and absorption rates among employees. We found that activities that include such functionality (e.g. micro-training and simulated phishing emails) were seen positively. Being able to track performance, of course, also influences motivation as tracking enables finding those who do not participate in training or those who are performing poorly. With a normative approach, one can also possibly find the underlying reasons why someone is not participating. Is it too hard, or is there perhaps a problem with time?

6. Conclusion

The research question, *What factors influence the adoption of awareness-raising activities in SMEs?*, was addressed using semi-structured interviews with ten participants who are responsible for awareness-raising within their respective organisations. Adopting a socio-technical lens, this research confirms that awareness-raising is dependent on the interplay between management, technology and system users. The results show five main factors that are of importance for the organisational adoption of awareness-raising activities, which span the entire socio-technical spectrum. The perhaps most notable conclusion is that management is an enabler which can both provide resources and lead by example. Lack of resources is constantly mentioned as an obstacle by the participants who, for instance, describe a need for ready-to-use solutions to save

time or not being able to modify activities due to a lack of time. A second notable finding is that this research confirms the importance of activities that are adapted to the organisation where they are used. The respondents describe adaption as important to raise employee motivation and increase relevance. However, while the respondents emphasise the importance of adaptation, they do not work with it in practice. While this conclusion appears to be a conundrum, it is well aligned with the fact that SMEs are struggling to find resources for awareness-raising activities.

Acknowledgments

We gratefully acknowledge the grants from the Swedish Civil Contingencies Agency (MSB), projects VISKA (MSB 2021–14650) and ICANP (MSB 2023-10887).

References

[1] ThriveDX, 15 alarming cybersecurity facts and statistics, 2022. URL: https://thrivedx.com/resources/article/cyber-security-facts-statistics.

[2] I. Security, Cost of a data breach report 2023, 2023. URL: https://www.ibm.com/reports/data-breach.

[3] S. Chaudhary, V. Gkioulos, S. Katsikas, A quest for research and knowledge gaps in cybersecurity awareness for small and medium-sized enterprises, Computer Science Review 50 (2023) 100592. doi:https://doi.org/10.1016/j.cosrev.2023.100592.

[4] A. Sarri, V. Paggio, G. Bafoutsou, Cybersecurity for smes–challenges and recommendations, 2021. URL: https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes.

[5] G. Erdogan, R. Halvorsrud, C. Boletsis, S. Tverdal, J. Brian Pickering, Cybersecurity awareness and capacities of smes, in: 9th International Conference on Information Systems Security and Privacy - ICISSP, volume 1, SciTePress, 2023, pp. 296–304. doi:10.5220/0011609600003405.

[6] V. Business, 2024 data breach investigations report, 2024. URL: https://www.verizon.com/business/resources/reports/dbir/2023/summary-of-findings/.

[7] F. Salahdine, N. Kaabouch, Social engineering attacks: A survey, Future Internet 11 (2019) 89. URL: https://www.mdpi.com/1999-5903/11/4/89.

[8] M. Bada, J. R. C. Nurse, Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (smes), Information Computer Security 27 (2019) 393–410. doi:10.1108/ICS-07-2018-0080.

[9] L. Dahabiyeh, Factors affecting organizational adoption and acceptance of computer-based security awareness training tools, Information Computer Security 29 (2021) 836–849. doi:10.1108/ICS-12-2020-0200.

[10] M. Heidt, J. P. Gerlach, P. Buxmann, Investigating the security divide between sme and large companies: How sme characteristics influence organizational it security investments, Information Systems Frontiers 21 (2019) 1285–1305. doi:10.1007/s10796-019-09959-1.

[11] E. Mumford, The story of socio-technical design: Reflections on its successes, failures and potential, Information systems journal 16 (2006) 317–342.

[12] C. P. Pfleeger, S. L. Pfleeger, J. Margulies, Security in computing, fifth edition ed., Prentice Hall, Upper Saddle River, NJ, 2015.
[13] B. Ur, F. Noma, J. Bees, S. M. Segreti, R. Shay, L. Bauer, N. Christin, L. F. Cranor, " i added'!'at the end to make it secure": Observing password creation in the lab, in: Eleventh symposium on usable privacy and security (SOUPS 2015), 2015, pp. 123–140.
[14] A. Al-Salek, J. Kävrestad, M. Nohlberg, Exploring experiences of using seta in nordic municipalities, in: S. Furnell, N. Clarke (Eds.), Human Aspects of Information Security and Assurance, Springer International Publishing, 2021, pp. 22–31.
[15] B. Bulgurcu, H. Cavusoglu, I. Benbasat, Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness, MIS quarterly 34 (2010) 523–548.
[16] B. Khan, K. S. Alghathbar, S. I. Nabi, M. K. Khan, Effectiveness of information security awareness methods based on psychological theories, African journal of business management 5 (2011) 10862.
[17] K. F. Tschakert, S. Ngamsuriyaroj, Effectiveness of and user preferences for security awareness training methodologies, Heliyon 5 (2019). URL: https://doi.org/10.1016/j.heliyon.2019.e02010. doi:10.1016/j.heliyon.2019.e02010, doi: 10.1016/j.heliyon.2019.e02010.
[18] W. He, Z. Zhang, Enterprise cybersecurity training and awareness programs: Recommendations for success, Journal of Organizational Computing and Electronic Commerce 29 (2019) 249–257. URL: https://doi.org/10.1080/10919392.2019.1611528. doi:10.1080/10919392.2019.1611528.
[19] J. Kävrestad, M. Nohlberg, S. Furnell, A taxonomy of seta methods and linkage to delivery preferences, SIGMIS Database 54 (2023) 107–133. doi:10.1145/3631341.3631348.
[20] K. Johansson, T. Paulsson, E. Bergström, U. Seigerroth, Improving cybersecurity awareness among smes in the manufacturing industry, in: A. H. C. Ng, A. Syberfelt, D. Högberg, M. Holm (Eds.), SPS2022: Proceedings of the 10th Swedish production symposium, IOS Press, 2022, pp. 209–220.
[21] ENISA, Custom-made awareness raising to enhance cybersecurity culture, 2024. URL: https://www.enisa.europa.eu/news/custom-made-awareness-raising-to-enhance-cybersecurity-culture.
[22] The Swedish Civil Contingencies Agency, Informationssäkerhet för små och medelstora organisationer [information security for small and medium-sized organisations], 2024. URL: https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/arbeta-systematiskt-informationssakerhet-och-cybersakerhet/informationssakerhet-for-sma-och-medelstora-organisationer/.
[23] L. G. Tornatzky, M. Fleischer, A. K. Chakrabarti, The processes of technological innovation, Lexington Books, Lexington, MA, USA, 1990.
[24] M. Sadok, S. Alter, P. Bednar, It is not my job: exploring the disconnect between corporate security policies and actual security practices in smes, Information Computer Security 28 (2020) 467–483. doi:10.1108/ICS-01-2019-0010.
[25] N. Rawindaran, A. Jayal, E. Prakash, Exploration of the impact of cybersecurity awareness on small and medium enterprises (smes) in wales using intelligent software to combat cybercrime, Computers 11 (2022) 174. URL: https://www.mdpi.com/2073-431X/11/12/174.

[26] B. J. Oates, Researching Information Systems and Computing, Sage, London, 2006.
[27] W. C. Adams, Conducting Semi-Structured Interviews, 2015, pp. 492–505. doi:https://doi.org/10.1002/9781119171386.ch19.
[28] L. Busetto, W. Wick, C. Gumbinger, How to use and assess qualitative research methods, Neurological Research and Practice 2 (2020) 14. doi:10.1186/s42466-020-00059-z.
[29] O. A. Adeoye-Olatunde, N. L. Olenik, Research and scholarly methods: Semi-structured interviews, JACCP: JOURNAL OF THE AMERICAN COLLEGE OF CLINICAL PHARMACY 4 (2021) 1358–1367. doi:https://doi.org/10.1002/jac5.1441.
[30] A. Thornhill, M. Saunders, P. Lewis, Research methods for business students, seventh edition ed., Prentice Hall: London, 2016.
[31] A. Blackstone, Principles of sociological inquiry: Qualitative and quantitative methods, Saylor Academy Open Textbooks, 2018.
[32] R. Baskerville, F. Rowe, F.-C. Wolff, Integration of information systems and cybersecurity countermeasures: An exposure to risk perspective, SIGMIS Database 49 (2018) 33–52. doi:10.1145/3184444.3184448.
[33] K. Bernsmed, G. Bour, M. Lundgren, E. Bergström, An evaluation of practitioners' perceptions of a security risk assessment methodology in air traffic management projects, Journal of Air Transport Management 102 (2022) 102223. doi:10.1016/j.jairtraman.2022.102223.
[34] W. A. Cram, J. D'Arcy, J. G. Proudfoot, Seeing the forest and the trees: A meta-analysis of the antecedents to information security policy compliance, MIS Quarterly 43 (2019) 525–554. doi:10.25300/MISQ/2019/15117.
[35] V. Braun, V. Clarke, Using thematic analysis in psychology, Qualitative Research in Psychology 3 (2006) 77–101. doi:10.1191/1478088706qp063oa.
[36] J. Saldaña, The coding manual for qualitative researchers, 4th ed., SAGE Publications Inc., Thousand Oaks, CA, USA, 2021.
[37] K. M. MacQueen, E. McLellan-Lemal, K. Bartholow, B. Milstein, Team-based codebook development: Structure, process, and agreement, AltaMira Press, Lanham, MD, USA, 2008, pp. 119–135.
[38] K. Renaud, How smaller businesses struggle with security advice, Computer Fraud Security 2016 (2016) 10–18. doi:https://doi.org/10.1016/S1361-3723(16)30062-8.
[39] R. Groner, P. Brune, Towards an empirical examination of it security infrastructures in sme, in: Secure IT Systems: 17th Nordic Conference, NordSec 2012, Karlskrona, Sweden, October 31–November 2, 2012. Proceedings 17, Springer, 2012, pp. 73–88.
[40] T. Gundu, S. V. Flowerday, Ignorance to awareness: Towards an information security awareness process, SAIEE Africa Research Journal 104 (2013) 69–79. doi:10.23919/SAIEE.2013.8531867.
[41] S. Dojkovski, S. Lichtenstein, M. Warren, Challenges in fostering an information security culture in australian small and medium sized enterprises, in: 5th European conference on Information Warfare and Security, 2006, pp. 31–40.
[42] M. Eminağaoğlu, E. Uçar, S. Eren, The positive outcomes of information security awareness training in companies – a case study, Information Security Technical Report 14 (2009) 223–229. doi:https://doi.org/10.1016/j.istr.2010.05.002.
[43] C. Liu, H. Liang, N. Wang, Y. Xue, Ensuring employees' information security policy compli-

ance by carrot and stick: the moderating roles of organizational commitment and gender, Information Technology People 35 (2022) 802–834. doi:10.1108/ITP-09-2019-0452.
[44] M. I. Merhi, P. Ahluwalia, Examining the impact of deterrence factors and norms on resistance to information systems security, Computers in Human Behavior 92 (2019) 37–46. doi:https://doi.org/10.1016/j.chb.2018.10.031.