



Guidelines and Tool Support for Building a Cybersecurity Awareness Program for SMEs

Christophe Ponsard^(✉)  and Jeremy Grandclaudon

CETIC Research Center, Charleroi, Belgium
{Christophe.Ponsard, Jeremy.Grandclaudon}@cetic.be

Abstract. Nowadays companies have become highly dependent on digital technology for running their business, regardless their size or domain. Smaller organisations require a specific attention because of their lower level of protection, capability of reaction and recovery while they are increasingly being targeted by cyberattacks. In order to improve their level of cybersecurity and resilience, a first step is to raise awareness. It is however not an easy task because it is highly dependent on human factors, spread across the whole organisation, including managers, business users and IT staff. This paper aims at supporting the development of a cybersecurity awareness program for small and medium enterprises. In order to build the program on strong foundations, the current state of awareness of such companies is presented and a SWOT analysis carried out. Different instruments for efficiently supporting the deployment of the program are then presented. A practical experience carried out in Belgium to implement some of the proposed instruments is also presented and some lessons learned are discussed.

Keywords: Cybersecurity · Awareness · SME · Quiz · Assessment · Toolkit guidelines

1 Introduction

Small and Medium Enterprises (SMEs) are recognised worldwide as the drivers of socio-economic development. In Europe, it is estimated they produce between 50 and 60% of the total value added and they employ about two third of the workforce [46]. Their high level of adaptability and their need for innovation make them big adopters of digital technologies, which increases their exposure to cyberattacks. At the same time, it is well-known that SMEs have a low adherence to procedures and standards as they keep their focus on their business goals [29]. This can result of underestimating the risks related to their cyber security exposure or just think they are not worth being attacked given their size. Unfortunately, this belief is not any more valid nowadays, given a vast majority of attacks are now targeting SMEs. In the past years, the numbers of attacks increased dramatically with estimated around 60% and even 70% of attacked

SMEs [2, 41]. Unfortunately, more than half of the hacked SMEs are not able to recover and are going bankrupt within six months after the attack [47].

It is now well-known that technological tools cannot guarantee alone the security of a system involving IT components. It is also required to deal with the human beings within their organisation [34] and thus to consider actions for improving the awareness of all the people across the organisation. The concept of cybersecurity awareness can be defined as “the degree or extent to which every member of staff understands the importance of IT security, the levels of IT security appropriate to the organisation, and their individual security responsibilities” [36]. Awareness is also the first step in building a cybersecurity culture involving everyone within the organisation from the top-level management to low-level employees with each employee responsible for their cybersecurity practices [3].

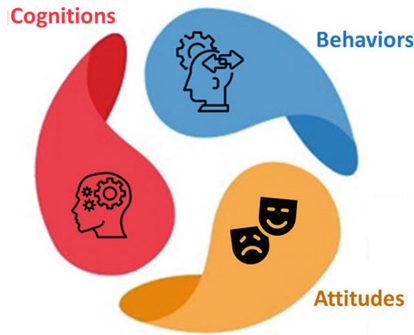


Fig. 1. Attitude, behaviour and cognition dimensions of cybersecurity awareness [61].

Human beings are complex, and their behaviour is quite influenced by organisational norms and habits through the pressure of their peers, even despite their knowledge. For example, even if people are told to use strong passwords and not reuse them, they may not behave like that. While the strength can be enforced at creation time, avoiding reuse generally relies on the people and potentially expose the company through personal social networks. To deal with this, awareness must not only rely on knowledge or cognitive aspects (i.e. teachable and verifiable aspects) but also attitudes (i.e. feelings and emotions in relation to security activities) and behaviours (i.e. actual/intended activities and risk-taking actions directly or indirectly impacting security), as depicted in Fig. 1.

The initial motivation of our work is the deployment of a programme aiming to help Belgian SMEs to better protect themselves against cybersecurity threats through audit and digital transformation actions supported by specific funding aids [19, 54]. In order to be successful, such a program must encourage SMEs to realise cybersecurity threats can endanger their business. At this point, they can engage in actions to assess how well they are protected against cyber attacks

and ready to react to them. As a consequence, our work also included actions to raise awareness.

This paper is an extended version of our initial report describing our learning path and our experience to setup a cybersecurity awareness programme and to deploy supporting tools matching our local context [53]. This previous work was significantly extended in the following ways across the structure of our paper which is also presented here. In Sect. 2, our study of the SME attitude towards cybersecurity is deeper: our survey on the current awareness was extended based on literature and interaction with specialised European organisation and network [24, 62]. It also contains an analysis of barriers and drivers for the adoption of cybersecurity by SMEs under the form of a SWOT analysis (i.e. strengths, weaknesses, opportunities and threats). In Sect. 3, our survey of existing cybersecurity awareness instruments is much more elaborated, especially to guide in the design of an awareness program and to deploy specific instruments like personae and gamification. Next, our own experience to raise awareness in Belgium is reported more extensively in Sect. 4. More lessons learned are also discussed in Sect. 5. Finally, our conclusions and perspectives are also refined based on the knowledge gained both from the literature, our interaction with key players and our practical experience.

2 Current SME Attitude w.r.t. CyberSecurity

This section first reports about the current level of cybersecurity awareness of SMEs in various domains and parts of the world. In a second part, a SWOT analysis is carried out in order to help in identifying drivers and barriers to the adoption of cybersecurity both within the companies (Strengths and Weaknesses) and in their environment (Opportunities and Threats).

2.1 Cybersecurity Awareness in SMEs

We review here different reports carried out over the past few years in various areas to show the global state and evolution of the awareness of SMEs are about cybersecurity threats.

A survey made in 2014 among UK SMEs revealed interesting facts about how SMEs deal with cybersecurity, especially about their perception and awareness [50]. Only 21% of SMEs have shown a low awareness about basic security guidelines, 39% have actually done a global risk analysis which included cybersecurity, and 48% keep the company's risk analysis, policies and backups up-to-date. The main reported barrier is the cost for implementing cybersecurity solutions and standards because they are designed for bigger companies.

In 2016, a survey was carried out by the Zurich Insurance Group across 2,600 SMEs across 13 countries in Europe, the Americas and Asia Pacific [69]. It reported an interesting evolution about the fact of how SMEs think they are protected by their size: they were 17% believing that in 2015 and only 10% in 2016. It also revealed that theft of customer data and reputation damage are

the most feared consequences of cyberattacks. Globally only 5% of SMEs have confidence in their cybersecurity measures. The less aware region of the globe seems to be South America, while it is improving quickly in some parts of Asia.

A recent survey carried out in North America by the Better Business Bureau also reported an increase in the awareness to cyberthreats, including the use of proactive security steps [6]. The awareness could be ranked between 76% (for fishing) to 93% (larger variety of threats). However, another survey carried out in Europe and related to the adoption of Big Data, Internet of Things and cybersecurity (BIC) revealed that the lack of understanding and awareness is cited in the top three barriers to the adoption of such technologies. While people in strategic position in SMEs are interested in investing in the right people and technologies, unfortunately, they often lack knowledge of what they need and how to obtain it [22].

Concerning developing countries, the adoption of information technology systems by SMEs has the potential to bring significant benefits and accelerate their growth. However, it will also expose them to online cybersecurity threats. Core cybersecurity characteristics identified in developing countries are poor practices, unique usage patterns (e.g. mobile payments in isolated areas), novice users, use of pirated software and limited understanding of the attacker's motivations. The challenges concern inadequate policies (e.g. limited allowance for encryption), technical specificities (shared computers, offline mode), business aspect (cheaper but less safe solutions and processes) and of course education and awareness [8]. In South Africa, a recent study showed that SMEs do not have to face complex business and legacy system which simplifies the enforcement of cybersecurity. However they are limited in their ability to improve their cybersecurity due to internal organisational factors of budget, management support, and attitudes [38]. A more specific study related to awareness showed that the current initiatives are effective and have been able to address cyber security issues although at a smaller scale [20]. The situation reported in Ghanah is far more worrying with a lack of adherence to standards and best practices, inadequate security solutions and systems protection. This result in about 35% SMEs perceiving the Internet service delivery in Ghana as risky, unsecured and vulnerable to cyber attacks [67].

The bottom line is that even when SMEs seem to have reached a good level of awareness, when looking at attack statistics, they still fail to make it effective. A first explanation is that security measures are perceived by SMEs as too complex, time consuming and requiring a high level of technical knowledge about IT systems. Another reason is the difficulty to transition from a step of initial awareness to the emergence of an internal cybersecurity culture, because of the lack of resources (money, time, expertise). They are also weak at deploying policies and defining responsibilities [57]. This last point is also crucial because security policies are not designed to put burden on the company but to help them protect their business and hence support their development in the long run.

2.2 SWOT Analysis

This section gives a summary of several strengths/weaknesses (internal at the organisation) and opportunities/threats (external to the organisation) that needs to be addressed (for negative factors) or used as drivers (for positive factors) when setting up an awareness program. It is based on a more detailed analysis of the awareness literature sketched in the previous section together with extra references, especially related to opportunities that can be mobilised to foster awareness. For weaknesses and threats, some actions to address them are also identified at this stage.

Strengths. The main strengths of SME were already identified and are further commented here:

- *Agility and Fast Reaction Time:* once SMEs realise securing their business is critical, they can take action quickly. However this should not happen due to an attack because in many cases it will be fatal to the company within a few months [47].
- *Business Alignment:* SMEs are focused on their business, hence all activities are directed towards supporting this objective, meaning that the implementation of cybersecurity will naturally be oriented on minimizing business risks.
- *Accessible Management and Willingness to Improve:* thanks to their flat structure, the management is close to the company operation and able to make the connection with important information being spread in his domain of operation, e.g. through a cybersecurity awareness program.

Weaknesses. A number of weaknesses are depicted in Fig. 2 under the form of a fishbone diagram which actually also includes some threats or opportunities, depending of the environment context. We comment here only SME weaknesses with some possible actions to cope with them.

- *Digital Immaturity:* many SMEs, especially growing startups are early technology adopters. While the technology can support their business growth, it might not be mastered from a security point of view. This could be related to the technology itself (see threats) but also to the lack of analysis of security impact of using a new technology (e.g. moving to smart manufacturing and getting attacked resulting in a costly production interruption).
- *Limited Availability of Resources* of different kinds. The competent people may also be too busy on short term tasks to implement a (see also strategic planning). The SME may lack technical expertise and may not be able to develop this skill internally (see last weakness). Often an external expertise is required, but the company may not have the budget for hiring a specialist or may have trouble in finding such an expert (see threats).
- *Overconfidence:* SMEs think they are protected by their small size and little relative value compared to big corporations. However, this is a wrong belief with estimates as high as 70% of attacks targeting SMEs [41]. The reason is

that attackers can count on a large pool of vulnerable SMEs. They can also be used as entry point to attack larger companies doing business with them, thus compromising relationship. SMEs are also too confident about their recovery capability which takes usually longer than expected, resulting in potentially large business loss.

- *Low Adherence to Standards.* SMEs generally reject standards and norms unless it is required by the market. In order to be successfully adopted, a cybersecurity standard should either be implied by some regulation (see GDPR in opportunities) or be lightweight and with a clear perception of its business benefit. Heavyweight standard like the ISO27K are not recommended.
- *Skill Management w.r.t. Cybersecurity* and more generally emerging technologies. While people in strategic position in SMEs are interested in investing in the right people and technologies, unfortunately, they often lack knowledge of what they need and how to obtain it [22].

Opportunities

- *General Data Protection Regulation (GDPR).* It has become enforceable on 25 May 2018 and has attracted the attention of many companies, including SMEs on the need to secure their IT infrastructure for the purpose of personal data protection. This regulation has a clear positive impact on cybersecurity awareness with many European organisations actually taking actions to improve their security performance over the past year [18]. In Belgium, a 50% increase in requests in some consulting companies in Belgium was reported [7]. For sure, GDPR will remain a strong driver in the next years as many companies are still on their way to achieve full compliance.

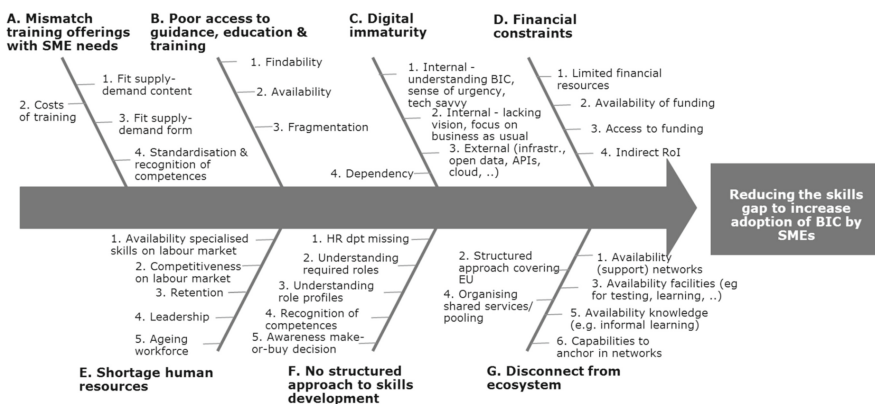


Fig. 2. Main barriers for skills development in SMEs [22].

- *Cyber Security Identified as High Priority in Europe:* improving cybersecurity is now recognised by Europe as a top priority in a world where battles are now carried out on the Internet. Strategic programs are being developed in order to structure the field with a European cybersecurity competence centre relying on networks of national coordination centres [21]. The importance to cope with SMEs and develop a common labelling scheme is also recognised and different organisations like ENISA and ECSO are working on this topic [25,26]. A wider survey of such initiative is presented in [54].
- *Local Initiatives:* in many countries, cybersecurity and GDPR are also being pushed by many SME association and sectorial federations which are organising specific workgroups and awareness events. Those are interesting instruments for SME managers to engage in an improvement process on those related topics. Specific projects like CYBER are also encouraging the direct sharing of good cybersecurity practices across regions in Europe [35].

Threats. Despite the actions taken to encourage SME to engage into cybersecurity improvement, a number of environmental limitations remain to be addressed:

- *Lack of Cybersecurity Experts:* unfortunately there are too few experts in cybersecurity. Consequently, they are highly demanded and hired by big companies. A solution is to increase the training program both at university level and through dedicated continuing education in cybersecurity. A number of such programs are now being proposed as specialised masters in university or by dedicated international institutes like the SANS Institute [58].
- *Fuzzy Recognition of Experts:* a direct consequence of the lack of cybersecurity experts is that people with insufficient skills can try to access the market to help SMEs looking for those skills. In order to guarantee SMEs can trust some expert, a form of expert certification can be organised, e.g. in the context of specific cybersecurity programs like the cyberessentials in UK [63]. Other similar schemes are reported in [54].
- *Emerging Technologies:* like Internet of Things or Big Data can have complex IT architectures with potential security issues. The general lack of standard in the proposed solution also increases cybersecurity risks. Although such technologies can contribute to the development of a company, the impact on risk should also be evaluated before deploying them.

3 Survey of Cybersecurity Awareness Instruments

This section reviews some interesting instruments for raising SME awareness about cybersecurity. They can be used alone or in combination in the scope of an awareness campaign. Before introducing specific instruments, the notion of campaign is elaborated and integrated in the wider context of a cybersecurity culture (CSC) program. Various awareness instruments are then presented from most introductory to more advanced ones.

3.1 Setting Up and Running an Awareness Program

Cybersecurity needs more than a “one time” effort to be and stay efficient. For this purpose, a specific program should actually be part of a global roadmap to setup a cybersecurity culture and result in the adoption of information security considerations in the day-to-day life of the employees of the targeted organisations. With the right approach, a natural CSC develop over time inside a company by evolving behaviours and attitudes of employees towards information assets, resulting in cybersecurity becoming part of a company’s wider organisational culture [26].

Any awareness campaign or more generally CSC program require a global strategy defined through the following key steps depicted in Fig. 3 [3,4,66]:

1. analyse the current situation in the target scope
2. clearly defining the awareness goal, target and means to be used
3. identifying and deploying the necessary instruments
4. communicating over the program
5. monitoring the effectiveness of the program and refine it as required

Those steps are further elaborated here but are also summarised in the compact of ten tactics on a poster by the SANS [59].

Current Situation. Security is not often seen a top priority by most organisations so building a good business case is an important step, even for a small organisation. An initial step is to gather evidence and statistics on cyber threats inside the organisation and in its sector. They can be evaluated in terms of attitude, behaviour and cognition aspects. Different instruments can be used here

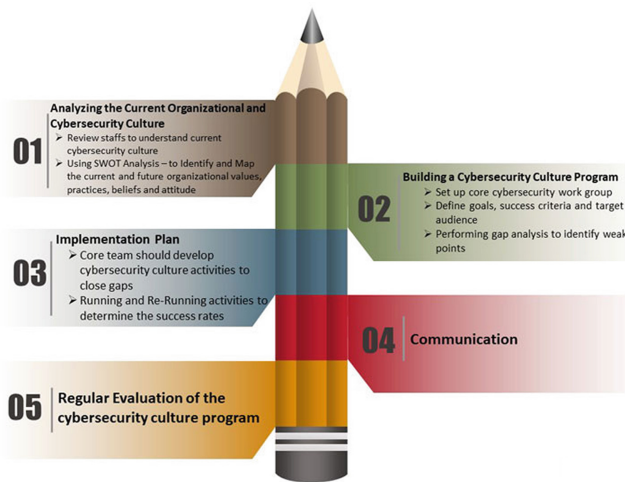


Fig. 3. Main steps for developing a cybersecurity culture program [3].

to gather such evidence, like assessment, surveys, quizzes, fishing tests (see relevant sections). A specific SWOT analysis is also useful at this step and can be elaborated based on the generic analysis presented in the previous section.

Defining Goals and Gap Analysis. The long term goal should be to establish a cybersecurity culture. However, progressing towards this goal is a long journey with different maturity milestones. A specific campaign should target the next milestone based on a gap analysis with the current situation. The focus of this paper is essentially the first milestone of reaching awareness.

A framework like Goal-Questions-Metrics can help in structuring a goals more systematically and also to define measurable success criteria [45].

The gap analysis between goals and the current situation can be combined with the SWOT analysis to identify the positive and negative factors that will help to define and conduct the implementation plan.

Implementation Plan. The implementation of specific actions to close the identified gaps can rely on a combination of different instruments proposed later in this section to support awareness raising actions. A balanced CSC program should of course focus on goals with the high priority considering the risks but can also include “quick wins” and actions that can have a good visible return and which can rewards the user for their engagement, keeping them motivated to also pursue their effort of less visible result.

In order to achieve the best results and implement a resilient CSC, a multi-pronged approach is required, involving senior management, key employees and ultimately all employees. A useful technique to build such a plan is the focus group [68]. Specific roadmaps for SMEs have also been defined, e.g. [28].

Communicating Over the Program. Well-defined communication channels should be set up and used to inform about the importance of cybersecurity, to attract attention about specific actions (e.g. passwords, backups, fishing, physical security, etc) and to give feedback about progress as measured. Those means can include: emails, social networks, websites and blogs. They can be company specific or wider but in all cases they need to use trustable channels, especially if external to the company. For wider campaigns, this can also include relays in traditional medias (newspaper, radio, television).

An important message is also to convince employees that improving the company’s resilience against most cyber threats does not impose a large burden on key business functions.

Program Evaluation. To be effective, the programme must reach its goals in a measurable way, based on the metrics defined earlier. Considering awareness, it is useful to be able to look for progress in the three key dimensions of attitude, behaviour and cognition. Means used for assessing the initial situation may be reused to measure the improvement on a similar scale of evaluation (e.g.

before/after surveys, observed behaviours) [66]. They can be complemented by data gathered from specific instruments, e.g. participation rate to some security event, number of reads of a security news, etc.

3.2 General Information, Posters and Guides

General information is provided by cybersecurity portals that are often proposed by an organisation supporting the improvement of cybersecurity at different levels: European, national or more local/dedicated security coalitions. At European level, October was selected as the month for cybersecurity, with a specific web site that is always available [23]. An example of national portal targeting the general public is the Belgian SafeOnWeb [56].

Posters are useful introductory material for raising awareness on specific topics, like phishing as shown in Fig. 4. They are easy to produce and can be displayed in a variety of places in workplaces, schools or public areas. Some nice posters are proposed by organisations like SANS and ENISA [27,60].

Guides aim at providing SMEs with an overview of basic and more advanced cybersecurity measures. Although the implementation depends on specific risks, quick checklists of generic security controls can be provided and are documented by several guides for SMEs, like in Belgium [10], in Germany [9] or in the US [47]. The Center for Internet Security (CIS) developed a set of 20 controls that are easy to implement by SMEs [12]. It also provides a specialised guide to help SMEs to implement the controls [11].

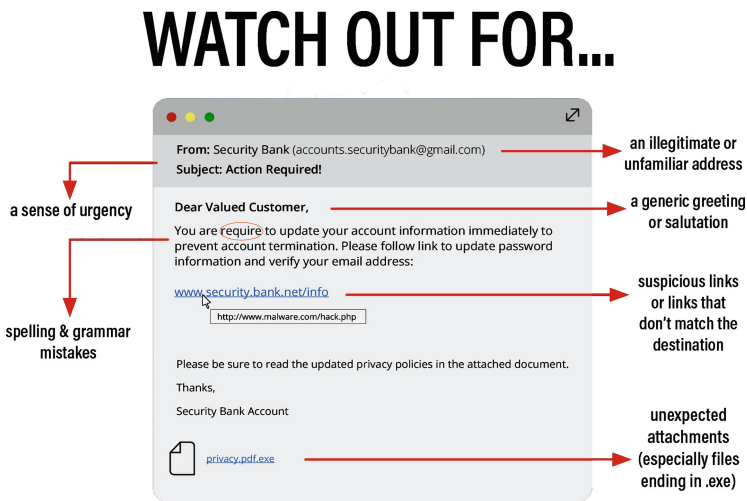


Fig. 4. Example of awareness poster about phishing.

3.3 Personae

Personae are archetypal descriptions of users that embody their goals [13]. Their focus on typical fictional business users helps in elaborating specific user aspects that may be missed by other approaches based on generic roles. Related to cybersecurity, personae can be useful for associating specific threats, vulnerabilities or risks in their environment [42]. Personae have proved very effective and there is psychological evidence about our natural and generative engagement with detailed representations of people [32].

This strong identification can be used both for designing training and communication material for raising cybersecurity awareness. At design time, it helps the trainer to build some concrete cases around the personae with specific characteristics, motivation, business needs, exposure to threads and business impacts. Based on this, the user can more easily imagine what should be done from an external point of view. But at the same time, she can realise (by herself or in a discussion session) that its own case is maybe quite similar to one or several personae and question its own attitude and behaviour. This process naturally leads to improvement decisions. As communication support, a persona can be given some graphical appearance which further allows the end-user identification. They can naturally be used in combination with other instruments, e.g. to illustrate a poster or a quiz.

A key issue is of course the selection process of the relevant personae. The selected archetypes must cover the broad spectrum of people with different backgrounds/experience/roles, more or less exposed and cybersecurity risks. The selected number should be kept minimal (no redundant personae) and low (because the more personae, the less effective the identification process). In practice, a handful of personae is usually used. However different dimensions can be covered independently using combination that makes sense, e.g. a startup company with a young computer literate at his head, a medium company with limited computer support but more aged and less computer literate manager.

Figure 5 shows some personae from an awareness raising web-site proposed in Michigan State, with the support of the U.S. Small Business Administration [61]. It relies on about 10 personae including end users (e.g. a coffee shop owner, a manufacturer and a plumber) with a good coverage of racial and gender diversity.



Fig. 5. Personae for various SME profiles [61].

Those have specific goals related to their business. In addition, some personae are also used to represent “villains”, i.e. some hacker possibly oriented to specific kinds of threats related to company data, financial transactions, physical security, etc. This is useful to associate some face and motivation behind threats and attackers that are most of the time invisible and faceless.

3.4 Gamification

A game can be defined as “a system in which players engage in an artificial conflict, defined by rules, that result in a quantifiable outcome” [37]. Gamification is “the use of game-based mechanics, aesthetics, and game-thinking to engage people, motivate action, promote learning, and solve problems” [39]. Gamification fits well the field of cybersecurity awareness because it must adhere to several of rules (i.e. security controls). Game situation can develop quite complex scenarios where the player must identify some threat and be able react in an adequate way. In addition to raising awareness, techniques derived from game-playing can also be used to upskill the staff in order to better cope with cyber threats [49]. Specific offers have developed in this area such as Game of Threats [55].

The rest of this section details a few interesting gamification techniques for awareness purposes: general quizzes and dealing with security threats scenarios. An important point is to encourage the candidate to try the quiz. Different incentives can be used: the fact it is anonymous (for a web-based quiz), playing in teams (group effect) or an attractive graphical design.

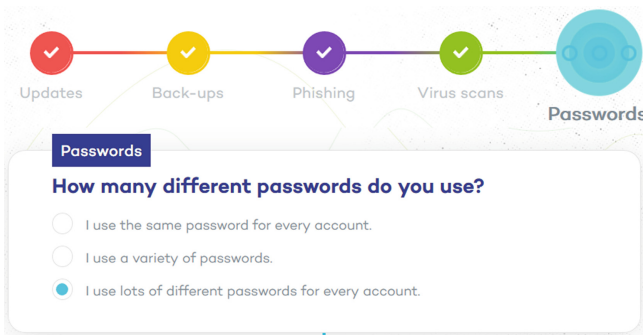


Fig. 6. SafeOnWeb digital health quiz [16].

Quizzes. A quiz is a game or light form of assessment used in education and awareness. Players must try to find the right answer to a series of question, either individually or in team. Quizzes often propose multiple-choice questions usually over a well-defined topic which enable automated correction and support. They are also easy to deploy on-line on a website or as mobile application. Those characteristics make the quiz an interesting tool to propose in a campaign after

some introductory material to engage the targeted audience in a first assessment in an entertaining way.

Quizzes generally also provide educational support to help correct wrong answer but also good ones by educating on the topic covered. They can also provide a summary and compare the score w.r.t. global statistics. After completing a quiz, a user might be more aware of the need to learn more and be helped. Pointers and contacts are typically proposed afterwards.

Many cybersecurity quizzes are elaborated in the above spirit. A representative illustration is the SafeOnWeb Belgian campaign which includes two quizzes [61]. One is specifically dedicated to phishing based on different scenarios (email, social networks), while the other, depicted on Fig. 6 is proposing to evaluate its Digital Health Index (DHI) based on questions covering updates, backups, fishing and anti-virus. The results are grouped by categories and globally under the form of a DIH between 0 and 10 which is positioned against the distribution of all collected DIH as shown in Fig. 7.

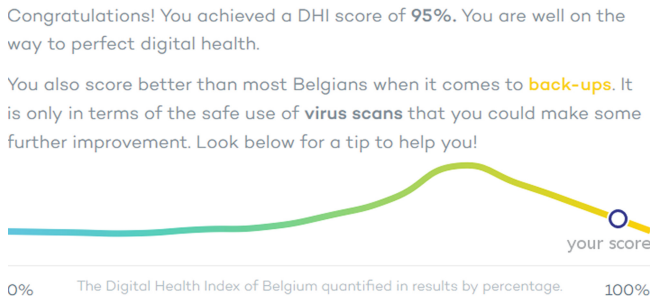


Fig. 7. SafeOnWeb quiz result analysis [16].

Other examples of interesting quizzes are the Network and Information Security Quiz [23] or the one developed by Lockheed [44], both proposed in the context of 2018 European Cyber Security Month.

Dealing with Security Threats Scenarios. Gamification can also explore common threat scenarios that an employee will have to face, for example dealing with passwords or recognising phishing attempts. Although those can be presented under the form of a quiz, more elaborated gaming supports can be proposed.

For helping the user to learn how easy a weak password can be broken and how to build a strong password, password checkers are available, e.g. the Kaspersky Lab's Secure Password Checker [40] and "How Secure Is My Password?" [17] from Dashlane. Both websites can be trusted and do not advise to use real password. Figure 8 shows the former with some weakness reported as well as the estimated time to crack the password compared to daily human activities.

To deal with phishing, different websites propose quiz-based test mixing legitimate requests and fishing requests through different media (SMS, social net-

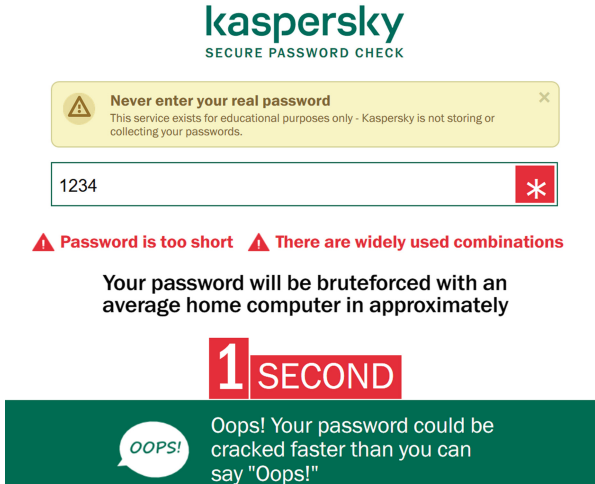


Fig. 8. Kaspersky password checker [40].

works, email) e.g. [51,61] A more elaborated gaming scenario is the setup of an internal phishing campaign which will send a fake yet realistic phishing email to employees and check how many employees are able to recognise the threat. Such a campaign must of course be endorsed by the management and different frameworks are available to conduct them, either commercial, e.g. PhishingBox [51] or Open Source, e.g. GoPhish [31] which is depicted in Fig. 9.

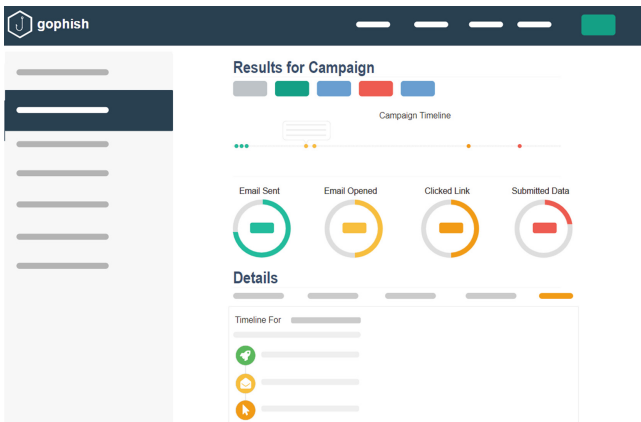


Fig. 9. Typical user interface of a phishing simulator [31].

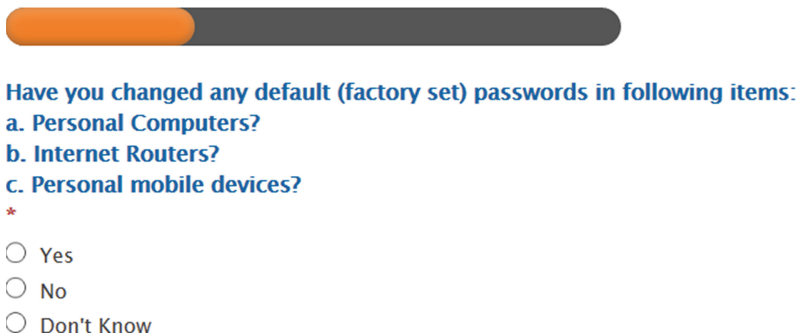
Of course, after the phishing campaign, awareness activities are organised to explain the risks and to help in better recognising the threat. Statistics typically

report 30% of click rate upon a first test campaign but also show it can quickly improve using such actions [33].

3.5 Self-assessments

Assessments are more advanced and structured form of evaluation. In opposition to quizzes which can be partial or even random, they cover a whole field at a certain level of details. They can take some form of audit when performed by a third-party expert in the field. However, like quizzes, it is also possible to propose a lighter and automated form of self-assessment generally based on a dedicated website. The later can be used as introduction for the former.

Cyber Essentials Self Assessment



Have you changed any default (factory set) passwords in following items:

a. Personal Computers?

b. Internet Routers?

c. Personal mobile devices?

*

Yes

No

Don't Know

Fig. 10. Cyber essentials self assessment [64].

In the area of SME cybersecurity, several initiatives across Europe propose methods including free self-assessment and/or more advanced assessments [54]. Some examples are the Cyber Essentials in the UK [63] or Vertrauen durch Sicherheit in Germany [65]. Self-assessments are often quite simple multiple choices quizzes [15, 64] as depicted in Fig. 10. They can also be more elaborated and involve personae such Small Business Big Threats [61]. Full assessments which cover classical security controls are paid-for, possibly with some funding aids by the local authorities.

3.6 Training, Courses and Tool Support

At this level, basic awareness is already reached but more specific actions can be taken using on-site training by experts but those can be costly. An alternative is to rely on MOOC (Massive Open Online Courses) which are free and with largely accessible in terms of prerequisites. An example of very successful MOOC is the French SecNumacadémie [1].

More advanced cybersecurity kits are also proposed by various organisations and groups a set of resources like slides, posters, guides, tools, etc. [14,30].

A few specific tools can be recommended to support raising awareness like password strength checkers, web-site vulnerability scanners, phishing simulators.

4 Setup of an Awareness Campaign in Wallonia

4.1 Context and Goals

The target of the cybersecurity campaign is SMEs. The goal is to raise awareness about the importance of deploying adequate cybersecurity measures both at technical and human levels w.r.t. the high impact an attack could have on their business. The awareness program is supported by the regional authorities with the goal to encourage many SMEs to engage in security audits and improvement through a validated network of security experts. In some countries, SMEs can benefit from specific funding for this, like the UK CyberEssentials vouchers.

4.2 Program Design

In order to have a good understanding of the current situation and make sure to have support of the existing actors in the cybersecurity area, specific actions were carried out over a period of roughly one year:

- with the end-users SMEs mainly through relay organisation like incubators for starters, usually relying a lot on IT and through sectoral organisation, dealing with a large variety of SMEs.
- with security experts through a local cybersecurity cluster, typically with quarterly meetings.

To support the launch of the program and encourage SMEs to keep joining it, a variety of instruments among those exposed in the previous sections were used like personae, Frequently Asked Questions (FAQ), a quiz and a self-assessment questionnaire. The rest of this section details them.

4.3 Frequently Asked Questions

In order to identify with each type of organisation, a first step was to try to figure out the reaction of both end-user SMEs and of the security experts that would have to interact with them. This was documented by building a list of questions either anticipated or collected during our interactions. Structuring those questions and building the answers contributed a large part of the program design itself and is still being used as a reference document for evolving it. At some point, a validated and cleaned form of the list resulted in a published Frequently Asked Questions (FAQ) used for communication purposes. This is quite convenient because it splits the description of an elaborated mechanism in progressive set of smaller and easier to explain questions.

Examples of questions from the end users are:

- Why should I ask to be checked for cybersecurity?
- What assurance do I have about being secure ?
- How much does it cost ?
- Can I put this forward to my client or prospects ?
- ...

Examples of questions from security experts are:

- What is the process/cost to join the initiative ?
- What check-list of controls should be enforced ?
- How much can I bill an SME ?
- ...

4.4 Personae

Personae were introduced in a second stage, mainly to segment the wide variety of SMEs. Only two personae were introduced:

- a persona familiar with IT technology from a startup but with little concern about cybersecurity when launching its Minimal Viable Product
- the other persona is the manager of a bigger SME active internationally with a low-tech manager that relies on different IT subcontractors with no idea of how well the business infrastructure is protected against cyber threats.

The personae are only slightly mentioned in the communication at this stage, but it is our plan to elaborate them. At this point, their main use is for assessing the security expert as it provides a nice way to propose a concrete situation in order to check the people expertise and methodology.

4.5 Quiz and Awareness Event

A quiz was developed initially as a support for a cybersecurity awareness event in the construction sector. The quiz is composed of a set of questions covering the three key dimensions presented previously:

- attitude and behaviour: in situations like managing password, performing backups, updates, etc.
- knowledge: more technical questions about key concepts either theoretical like electronic signature or practical like WIFI protection, what makes a good password, names of recent major attacks.

The quiz can be configured with a variable number of questions and was deployed both online using [43] and as a mobile application (see Fig. 11). To keep the rules simple, questions have multiple choices with only one correct answer. However, some questions are formulated negatively or can involve a final choice covering previous possibilities. Those were initially developed for supporting a cybersecurity awareness event. The mobile app is also available on the Play Store both in French and in English [52].



Fig. 11. Mobile application featuring a cybersecurity quiz [52].

4.6 Self-assessment Questionnaire

In order to encourage SMEs to engage into a cybersecurity improvement process, we developed a self-assessment questionnaire based on the 20 controls of Center for Internet Security [12] and using Lime Survey [43]. We revisited the grouping into categories based on priority criteria matching some typical SME profiles (through the associated persona). For very small companies relying on general purpose tools, web/email/WIFI aspects are considered first with lower priority on access control. Some organisational issues forming the last part of CIS20 are also considered much earlier to start growing a cybersecurity culture. The result is depicted in Fig. 12 and gives a good idea of what needs to be covered against what is already done.

A more elaborated version of the questionnaire was also used as a checklist to build the requirements and evaluation grid for authorising cybersecurity experts to help SMEs. In this more elaborated version, more structuring was introduced using the functions of the NIST cybersecurity framework (Identify, Protect, Detect, Respond, and Recover) [48].

5 Lessons Learned and Discussion

The feedback collected so far shows a good level of awareness in our SMEs during our interactions. For example, during workshop sessions mixing a dozen of SMEs

Questions	Answers
CIS Control 1: Inventory and Control of Hardware Assets	
Use an active discovery tool to identify devices connected to the company network and update the asset inventory.	Yes
User a passive discovery tool to identify devices connected to the company network and automatically update the device inventory.	Yes
Use Dynamic Host Configuration Protocol (DHCP) logging on all DHCP servers or IP address management tools to update the device inventory.	No
CIS Control 2: Inventory and Control of Software Assets	
Maintain an up-to-date list of all authorized software that is required in the enterprise for any business purpose.	Yes
Ensure that only software applications or OS currently supported are added to the authorized software inventory. Unsupported software should be tagged as so.	Yes
Use software inventory tools throughout the company to automate tracking of all software on business systems.	Yes
The software inventory system should track the name, version, publisher, and install date for all software, including OS authorized within the company.	Yes
The software inventory system should be tied into the hardware asset inventory so all devices and associated software are tracked from a single location.	No
Ensure that unauthorized software is either removed or the inventory is updated in a timely manner	No
CIS Control 3: Continuous Vulnerability Management	
Use an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.	Yes

Fig. 12. Self-assessment summary (updated version of [53]).

active in the construction domain, all the participants scored above the 80% in the quiz with a short cybersecurity reminder. Most SMEs were keen to share their experience, including negative ones (e.g. ransomware with no/corrupted backups). Participants also frequently mentioned having being told about GDPR and of its impact on cybersecurity, confirming the positive impact of GDPR [18].

Our experience is that awareness must be able to rely on bigger initiatives that have a good dynamics, for example the European Cyber Security Month was relayed a lot in national campaigns through emails and social networks [23]. Despite its regional scope, our initiative is not isolated and is actively exchanging with organisations at the Belgian federal level like our national authority (Center for Cybersecurity Belgium) and the federal cluster of companies (Cyber Security Coalition). At European level we have been sharing our practice at the European Cyber Security Organisation (ECSO) [24] and with the CYBER Interreg project [35]. Through those interactions, we can thus learn what is happening in other part of Europe and be part of the process to define a more global and unified way to deal with cybersecurity in Europe, while being able to select the means that best fits our context.

In order to maximise the success for reaching companies, the support of a wider organisation in which the SME is actively involved is really recommended. In our case the workshop co-organised with the construction federation was a success in terms of interactions and experience sharing. A lesson learned here is that campaigns must combine both passive channels to reach a wide audience but also active events where SMEs can meet experts, exchange together and actively

engage. As mentioned in the Attitude-Behaviour-Cognition reference framework, focusing on knowledge is far from enough, and more detailed evidence have been reported in the literature that if knowledge and awareness are necessary to initiate a change in behaviour, they are however not sufficient to realise it. Key success factors are a good preparation, not being driven by fear and being actionable in terms of follow-up (including training and feedback) [5].

About the use of personae: although we mainly use it for evaluating our experts, they helped a lot in defining typical usage scenarios and to provide an effective support for elaborating a case. More evolved personae are starting to emerge for people inside companies with specific threats, like having to deal with personal health information. Other usage of personae could also be investigated like complementary profiles inside a company w.r.t. position, level of experience with cybersecurity, using guidelines from [42].

Designing the quiz is an interesting and non-trivial exercise: questions must be clear, have a good technical coverage but also address attitude and behaviour. Our current version does not provide explanation nor introductory material because they were respectively provided through posters and a debriefing. Posters also revealed interesting to make available to SMEs for display in their premises.

6 Conclusion and Future Work

Raising cybersecurity awareness in an organisation is a prerequisite to initiate improvement actions and to start building a cybersecurity culture on top of a good knowledge but also with the right attitude and behaviour. If the staff is known to be a major weakness in cybersecurity, when engaged and correctly trained, it can become the first line of defence against attackers.

In this paper, we focused on the case of SMEs. After reporting about their current state of awareness and performing a general SWOT analysis w.r.t. cybersecurity, we surveyed available guidelines and tools to build a cybersecurity program and implement it through a variety of awareness raising tools. We also reported about our experience in conducting an awareness process in Belgium. This report substantially elaborates over our previous work [53] and although we do not claim to have performed a systematic literature survey, we believe we covered all important dimensions of this problem and that this work can be useful for others engaged in cybersecurity awareness with SMEs.

Our future work will refine the initial and final steps of the building an awareness program by defining more systematically the strategy based on the target audience and identifying more precise success factor that can be collected and monitored on the field over the long term. We also plan to elaborate the communication phase using more detailed personae. Finally, we keep our work evolving in parallel with the definition of European labelling scheme in which we are also actively involved.

Acknowledgements. This research was partly supported by Digital Wallonia and the DIGITRANS project (grant nr. 7618). We thank Infopole and the companies of the cybersecurity cluster for their support and feedback.

References

1. ANSSI: SecNumacadémie (2017). <https://secnumacademie.gouv.fr>
2. Ashford, W.: SMEs more vulnerable than ever to cyber attacks, survey shows, October 2017. <http://bit.do/computer-weekly-SME-cybersecurity>
3. Ashik, M.: Building an effective cybersecurity program (2018). <https://securereading.com/building-an-effective-cybersecurity-culture>
4. Bada, M., Nurse, J.R.C.: Developing cybersecurity education and awareness programmes for small and medium-sized enterprises (SMEs). CoRR abs/1906.09594 (2019)
5. Bada, M., Sasse, A.M., Nurse, J.R.C.: Cyber security awareness campaigns: why do they fail to change behaviour? (2019). <http://arxiv.org/abs/1901.02672>
6. BBB: State of cybersecurity among small businesses in North America. Better Business Bureau (2017). <http://bit.do/2017-state-of-cybersecurity>
7. BDO: Forte augmentation de la demande de services de cybersécurité suite au GDPR (2018). <http://bit.do/bdo18-cyber-gdpr>
8. Ben-David, Y., et al.: Computing security in the developing world: a case for multidisciplinary research. In: Proceedings of the 5th ACM Workshop on Networked Systems for Developing Regions, pp. 39–44. ACM (2011)
9. BSI: Cyber security for SMEs (2018). <https://www.bsigroup.com/en-GB/Cyber-Security/Cyber-security-for-SMEs>
10. CCB: Cyber security guide for SME (2016). <http://www.ccb.belgium.be/en/guide-sme>
11. CIS: CIS Controls - Implementation guide for Small and Medium-Sized Enterprises (SMEs) (2017). <https://www.cisecurity.org/wp-content/uploads/2017/09/CIS-Controls-Guide-for-SMEs.pdf>
12. CIS: CIS control - V7 (2018). <https://www.cisecurity.org/controls>
13. Cooper, A.: The Inmates are Running the Asylum. Macmillan Publishing Company Inc., New York City (1999)
14. Cyber Security Coalition: Cyber security KIT (2018). <https://www.cybersecuritycoalition.be/resource/cyber-security-kit>
15. Cyber Security Coalition: SME security scan (2018). <https://www.cybersecuritycoalition.be/sme-security-scan>
16. CybSafe: Enterprise IT leaders demanding more stringent cyber security from suppliers, July 2017. <http://bit.do/cybsafe>
17. Dahslane: How secure is my password (2019). <https://howsecureismypassword.net>
18. Davies, T.: Cybersecurity in Europe is improving: thank you GDPR? (2018). <https://gdpr.report/news/2018/12/27/cybersecurity-in-europe>
19. Digital Wallonia: Keep IT secure (2018). <https://www.digitalwallonia.be/keepitsecure>
20. Dlamini, Z., Modise, M.: Cyber security awareness initiatives in South Africa: a synergy approach. Case Stud. Inf. Warf. Secur. Res. Teach. Stud. 1 (2013)
21. EC: Proposal for a European cybersecurity competence network and centre (2017). <https://ec.europa.eu/digital-single-market/en/proposal-european-cybersecurity-competence-network-and-centre>

22. EC: Supporting specialised skills development: big data, Internet of Things and cybersecurity for SMEs. EASME/COSME/2017/007 Interim Report, March 2019
23. ECSM: European cyber security month quiz (2018). <https://cybersecuritymonth.eu/references/quiz-demonstration>
24. ECSO: European Cyber Security Organisation (2016). <https://ecs-org.eu>
25. ECSO: European Cyber Security Certification: a meta - scheme approach v1.0 (2017). <https://www.ecs-org.eu/documents/publications/5a3112ec2c891.pdf>
26. ENISA: Indispensable baseline security requirements for the procurement of secure ICT products and services (2016). <http://bit.do/ENISA-baseline-security>
27. ENISA: Posters for organisations (2019). <https://www.enisa.europa.eu/media/multimedia/material/awareness-raising-posters>
28. Fricker, S.: D2.3 security awareness plan report (2017). https://www.smesec.eu/doc/SMESEC_D2.3.Security_Awareness_Plan_Report_v1.0.pdf
29. Ghobadian, A., Gallea, D.: Total quality management and organization size. *Int. J. Oper. Prod. Manag.* **17**(2), 121–163 (1997)
30. Global Cyber Alliance: GCA cybersecurity toolkit for small businesses (2019)
31. GoPhish: Open-source phishing framework (2019). <https://getgophish.com>
32. Grudin, J.: Why personas work: the psychological evidence. In: *The Persona Lifecycle: Keeping People in Mind Throughout Product Design*, January 2006
33. Heat, E.: How to improve phishing awareness by 300% in 18 Months. In: *RSA Conference, San Francisco, 13–17 February 2017*
34. Herath, T., Rao, H.R.: Encouraging information security behaviors in organizations: role of penalties, pressures and perceived effectiveness. *Decis. Support Syst.* **47**(2), 154–165 (2009)
35. Interreg: Regional policies for competitive cybersecurity SMEs (2018). <https://www.interregeurope.eu/cyber>
36. ISF: Effective security awareness. *Information Security Forum*, April 2002
37. Juul, J.: The game, the player, the world: looking for a heart of gameness. In: *Digital Games Research Conference, 4–6 November 2003, University of Utrecht, The Netherlands* (2003)
38. Kabanda, S., Tanner, M., Kent, C.: Exploring SME cybersecurity practices in developing countries. *J. Organ. Comput. Electron. Comm.* **28**, 269–282 (2018). <https://doi.org/10.1080/10919392.2018.1484598>
39. Kapp, K.M.: *The Gamification of Learning and Instruction: Game-Based Methods and Strategies for Training and Education*, 1st edn. Pfeiffer & Company, Ablaer (2012)
40. Kasperski: Secure password check (2019). <https://password.kaspersky.com>
41. Keeper Security: 2018 state of cybersecurity in small and medium size businesses study (2018). <https://start.keeper.io/2018-ponemon-report>
42. Ki-Aries, D., Faily, S.: Persona-centred information security awareness. *Comput. Secur.* **70**, 663–674 (2017)
43. LimeSurvey: The online survey tool - open source surveys (2017). <https://www.limesurvey.org>
44. Lockheed Martin: Are you a cybersecurity ninja or n00b? (2018). <http://bit.do/lookheedmartin-quiz>
45. Mead, N., Woody, C.: *Cyber Security Engineering: A Practical Approach for Systems and Software Assurance*. Pearson Education, London (2016)
46. Muller, P., et al.: *Annual report on European SMEs 2014/2015*. European Commission (2015)
47. NCSA: stay safe online - cybersecurity awareness toolkit for SMB. *National Cyber Security Alliance* (2018)

48. NIST: Cybersecurity framework (2014). <https://www.nist.gov/cyberframework>
49. O’Flaherty, K.: How gamification can boost cyber security (2019). <https://www.information-age.com/gamification-can-boost-cyber-security-123479658/>
50. Osborn, E., et al.: Business versus tech: sources of the perceived lack of cyber security in SMEs. In: 1st International Conference on Cyber Security for Sustainable Society, February 2015
51. PhishingBox: Phishing simulator and test (2019). <https://www.phishingbox.com/phishing-test>
52. Ponsard, C.: Cybersecurity quizz (Google Play Store) (2018). <http://bit.do/QuizzCyberSecurity>
53. Ponsard, C., Grandclaudon, J., Bal, S.: Survey and lessons learned on raising SME awareness about cybersecurity. In: Proceedings of the 5th ICISSP, Prague, Czech Republic, 23–25 February, pp. 558–563 (2019)
54. Ponsard, C., Grandclaudon, J., Dallons, G.: Towards a cyber security label for SMEs: a European perspective. In: Proceedings of the 4th ICISSP, Funchal, Madeira, pp. 426–431 (2018)
55. PwC: Game of threats (2017)
56. SafeOnWeb: Test your digital health (2018). <https://campagne.safeonweb.be/en>
57. Sánchez, L.E., Santos-Olmo, A., Fernández-Medina, E., Piattini, M.: Security culture in small and medium-size enterprise. In: Quintela Varajão, J.E., Cruz-Cunha, M.M., Putnik, G.D., Trigo, A. (eds.) CENTERIS 2010. CCIS, vol. 110, pp. 315–324. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-16419-4_32
58. SANS: Computer security training and certification (1989). <https://www.sans.org>
59. SANS: 10 tactics for rolling out a successful awareness program (2018). https://www.sans.org/sites/default/files/2019-04/poster_10-tactics.pdf
60. SANS: Security awareness posters (2018). <https://www.sans.org/security-awareness-training/resources/posters>
61. SBDC, M.: Small business, big threat (2018). <https://smallbusinessbigthreat.com>
62. SPARTA: Strategic programs for advanced research and technology in Europe (2019). <https://www.sparta.eu>
63. UK Government: Cyber essentials (2016). <https://www.cyberaware.gov.uk/cyberessentials>
64. UK Government: Cyber essentials self assessment (2018). <https://www.cyberessentials.ie/self-assessment>
65. VDS: A brief assessment for SMEs - quick check for cyber security (2017). <http://vds-quick-check.de>
66. Veseli, I.: Measuring the effectiveness of information security awareness program. Msc., Department of Computer Science and Media Technology G’jovik University College, South Africa (2011)
67. Yeboah-Boateng, E.O.: Cyber-Security Challenges with SMEs in Developing Economies: Issues of Confidentiality, Integrity & Availability (CIA). Institut for Elektroniske Systemer, Aalborg Universitet, Aalborg (2013)
68. Yunos, Z., Hamid, R.S.A., Ahmad, M.: Development of a cyber security awareness strategy using focus group discussion. In: 2016 SAI Computing Conference (SAI), pp. 1063–1067, July 2016
69. Zurich Insurance Group: SMEs’ cyber risk awareness is on the rise (2016). <https://www.zurich.com/en/media/news-releases/2016/2016-1123-01>