Survey and Lessons Learned on Raising SME Awareness about Cybersecurity

Christophe Ponsard, Jeremy Grandclaudon and Sébastien Bal
CETIC Research Centre, Charleroi, Belgium

Keywords: Cybersecurity, Awareness, SME, Quiz, Assessment.

Abstract: Small and Medium Enterprises, like most companies, have become highly dependent on digital technology for running their business. Such companies are also increasingly targeted by cyberattacks while their level of protection, capability of reaction and recovery are low. The initial step to take them along the path of increasing their level of cybersecurity and resilience is to raise awareness. Achieving this step successfully is not an easy task and requires dealing mainly with human factors. This paper surveys a number of approaches and reports about our own experience with an cybersecurity awareness program targeting Belgian SMEs. Based on this, we propose some lessons learned and guidelines.

1 INTRODUCTION

Small and Medium Enterprises (SMEs) play a major role in the worldwide economy by generating between 50 and 60% of the total value added (Muller et al., 2015). SMEs are highly flexible and innovative but also show a low adherence to procedures and standards. In addition, their need for competitiveness makes them big adopters of digital technologies, which increases their exposure to cyberattacks. At the same time, their high focus on their business diverts their attention from those resulting threats or maybe they just think they are not worth being attacked. This statement is, however, not any more valid nowadays, when a vast majority of attacks are currently targeting SMEs. For example, in the UK, a survey reported than more than 60% of SMEs where attacked in 2017, especially from ransomware (Ashford, 2017). Unfortunately, more than half of the hacked SMEs are not able to recover and are going bankrupt within six month after the attack (NCSA, 2018).

It is now well-known that technological tools cannot guarantee alone the security of a IT system. This also requires to collaborate with the employees inside their organisation. Hence, cybersecurity awareness must be considered and tailored for both employees and their organisation. It 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 (ISF, 2002).

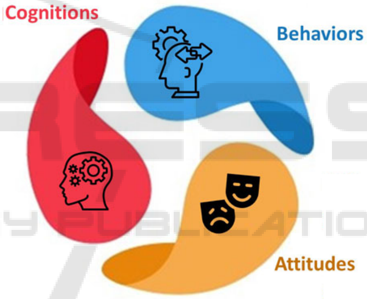


Figure 1: Attitude, Behaviour and Cognition dimensions of cybersecurity awareness (SBDC, 2018).

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 password and not reuse them, they may not behave like that. While the strength can be enforced at creation time, the reuse only 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 only (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 Figure 1.

The context of our work is the deployment of a programme aiming to help Belgian SMEs to better protect themselves against cybersecurity threats. In a previous paper, we have aligned our work with

Ponsard, C., Grandclaudon, J. and Bal, S.
Survey and Lessons Learned on Raising SME Awareness about Cybersecurity.
DOI: 10.5220/0007574305580563
In *Proceedings of the 5th International Conference on Information Systems Security and Privacy (ICISSP 2019)*, pages 558-563
ISBN: 978-989-758-359-9

other European initiative and sketched its global organisation (Ponsard et al., 2018). The programme itself will be carried out by authorised security experts. However, a prerequisite is precisely to raise the SME awareness in cybersecurity, so they will join the programme. This paper reports about our learning path to setup a cybersecurity awareness programme and our experience so far in deploying it in our area.

This paper is structured in the following way which is also representative of the logical steps we followed. Although our research centre knows quite well how SMEs behave, we studied more carefully what to expect from them w.r.t. cybersecurity. This is reported in Section 2. Section 3 gives our survey of different methods and supporting material that have been developed over time and on which we relied. Section 4 details how we designed and deployed our programme. Section 5 reports about our lessons learned so far. Finally, Section 6 concludes and discusses some next steps.

2 CURRENT CYBERSECURITY AWARENESS OF SMES

This section reviews some 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 (Osborn et al., 2015). 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 (Zurich IG, 2016). 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 revealed an increase in the awareness to cyberthreats, including the use of proactive security steps (BBB, 2017). The awareness could be ranked between 76% (for fishing) to 93% (larger variety of threats).

The bottom line is that most SMEs seem to have a good and even increasing level of awareness. However, when looking at attack statistics, they still fail to make it effective. A first explanation is that security measures are perceived as too complex, time consuming and requiring a high level of technical knowledge regarding 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 (Sánchez et al., 2010).

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 a campaign which is detailed in first place. Several tools are then listed from most introductory to more advanced ones.

3.1 Awareness Campaigns

Any awareness campaign or programme requires a global strategy that can be defined through the following steps:

- clearly defining the awareness goal, target and means to be used
- developing and deploying the necessary material
- implementing and monitoring the effectiveness of the programme

To be effective, the programme must reach its goals in a measurable way. This can be defined in terms of the three key dimensions exposed in the introduction: attitude, behaviour and cognition. Partial indicators can also be defined for the different instruments detailed hereafter. As each instrument is expected to be built on top of the result of the previous, one can expect some increased effect of their combination. This will be experimented in Section 4 and discussed in Section 5.

3.2 General Information 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 (ECSM, 2018). An example of national portal targeting the general public is the Belgian (SafeOnWeb, 2018).

Guides aims 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 (CCB, 2016), in Germany (BSI, 2018) or in the US (NCSA, 2018).

3.3 Personae

Personae are archetypal descriptions of users that embody their goals (Cooper, 1999). 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 (Ki-Aries and Faily, 2017). The strong identification can be used both for designing and in communication material. At design time, it helps the trainer to project into the end-user mind. As communication support, it allows the end-user to identify with a persona, especially in terms of attitudes and behaviours.

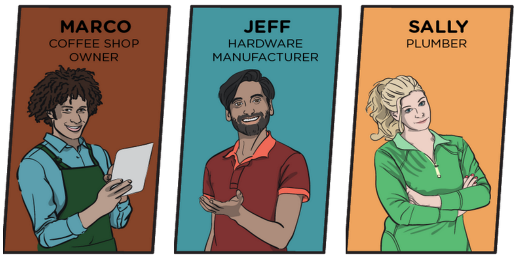
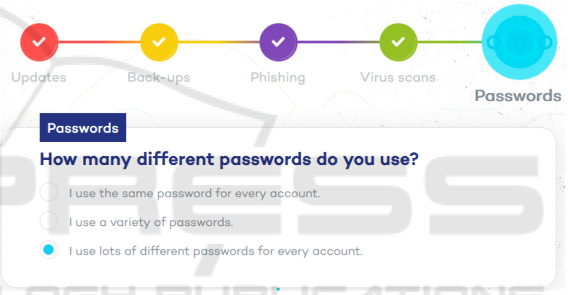


Figure 2: Personae for various SME profiles.

Figure 2 shows an example of awareness raising web-site proposed in Michigan State, with the support of the U.S. Small Business Administration (SBDC, 2018). 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. Those have specific goals related to their business. There are also some ”villains” that helps in putting some face and motivation behind threats that are most of the time invisible and faceless.

3.4 Quizzes

A quiz is a game or light form of assessment used in education and awareness. They are often organised as a series of 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 applications. Those characteristics make the quiz an interesting tool to propose in a campaign after some introductory material, so the targeted audience can engage in a first round of assessment usually anonymously and 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.



Passwords

How many different passwords do you use?

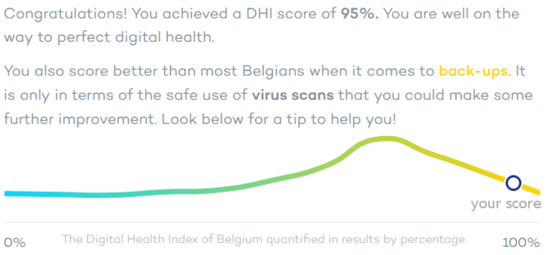
○ I use the same password for every account.

○ I use a variety of passwords.

● I use lots of different passwords for every account.

Figure 3: SafeOnWeb Digital Health Quiz.

Many cybersecurity quizzes are elaborated with the above spirit. A representative illustration is the SafeOnWeb Belgian campaign which includes two quizzes (SBDC, 2018). One is specifically dedicated to phishing based on different scenarios (email, social networks), while the other, depicted on Figure 3 is proposing to evaluate its Digital Health Index (DHI) based on questions covering updates, backups, fishing and anti-virus. The result is aggregated 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 Figure 4.



Congratulations! You achieved a DHI score of **95%**. You are well on the way to perfect digital health.

You also score better than most Belgians when it comes to back-ups. It is only in terms of the safe use of **virus scans** that you could make some further improvement. Look below for a tip to help you!

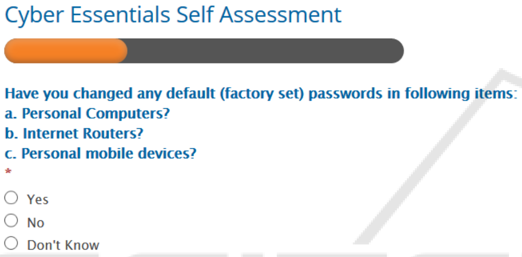
your score
0%
The Digital Health Index of Belgium quantified in results by percentage.
100%

Figure 4: SafeOnWeb Quiz result analysis.

Other examples of interesting quizzes are the Network and Information Security Quiz (ECSM, 2018) or another one developed by Lockheed (Lockheed Martin, 2018), both proposed in the context of 2018 European Cyber Security Month.

3.5 Assessments and Audits

Assessment 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 detail. They can take a more or less 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

Figure 5: Cyber Essentials self assessment (UK Gov., 2018).

In the area of SME cybersecurity, several initiatives across Europe propose methods including free self-assessment and/or more advanced assessments (Ponsard et al., 2018). Some examples are the Cyber Essentials in the UK (UK Gov., 2016) or Vertrauen durch Siecherhiet in Germany (VDS, 2017). Self-assessments can be quite simple multiple choices as depicted in Figure 5 or more elaborated and involve personae such Small Business Big Threats (SBDC, 2018). Full assessments which cover classical security controls are paid-for but with usually some support e.g. 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 (ANSSI, 2017).

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 programme 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. 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 ranging from single person to 100+ people with a dedicated IT department.
- with security experts through a local cybersecurity cluster, typically with quarterly meetings.

Although the programme is still in ramp-up phase, different instruments among those exposed in the previous sections were developed and are already used like personae, Frequently Asked Questions (FAQ), a quiz and a self-assessment questionnaire. The rest of this section details them.

4.3 FAQ and Personae

In order to identify with each type of organisation, a first step was to try to identify or anticipate a list of questions that would be asked given their concerns and try to provide a good answer from their perspective. The result is also naturally split in small topics that are easy to understand and can be later used for communication purposes.

Examples of questions from the end users are:

- why should I ask to be checked ?
- 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:

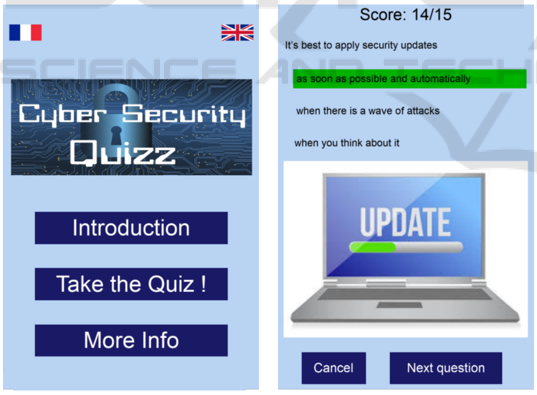
- what is the process/cost to join the programme ?
- what check-list of controls should be enforced ?
- how much can I bill an SME ?

Personae were introduced in a second stage, mainly to segment the wide variety of SMEs. So, we introduced a persona familiar with IT technology from a startup but with little concern about cybersecurity when launching its Minimal Viable Product. Another persona is 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.

4.4 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.



Score: 14/15

It's best to apply security updates

as soon as possible and automatically

when there is a wave of attacks

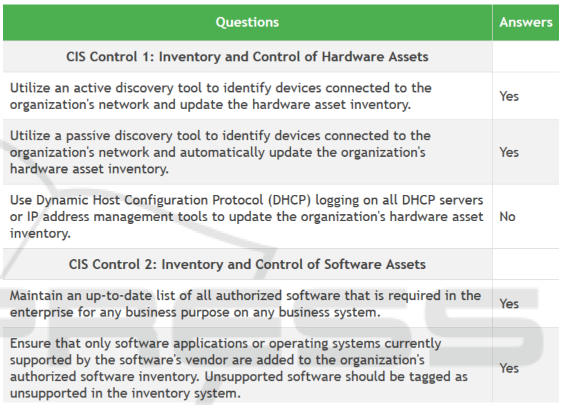
when you think about it

Figure 6: Mobile App.

The quiz can be configured with a variable number of questions and was deployed both online using (LimeSurvey, 2017) and as a mobile application (see Figure 6). 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 where initially developed for supporting a cybersecurity awareness event. The mobile app, although still in beta version due to its limited feedback, is also available on the Play Store (Ponsard, 2018)

4.5 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 (CIS, 2016) and using (LimeSurvey, 2017). 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 CIS are also considered much earlier to start growing a cybersecurity culture. The result is depicted in Figure 7 and gives a good idea of what needs to be covered against what is already done.



Questions	Answers
CIS Control 1: Inventory and Control of Hardware Assets	
Utilize an active discovery tool to identify devices connected to the organization's network and update the hardware asset inventory.	Yes
Utilize a passive discovery tool to identify devices connected to the organization's network and automatically update the organization's hardware asset inventory.	Yes
Use Dynamic Host Configuration Protocol (DHCP) logging on all DHCP servers or IP address management tools to update the organization's hardware asset 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 on any business system.	Yes
Ensure that only software applications or operating systems currently supported by the software's vendor are added to the organization's authorized software inventory. Unsupported software should be tagged as unsupported in the inventory system.	Yes

Figure 7: Self-assessment summary.

5 SOME LESSONS LEARNED

Although our campaign is still on-going, the feedback collected so far shows a pretty good level of awareness in our SMEs. During workshop sessions mixing a dozen of SMEs 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). All SMEs had been well informed about GDPR and its connection with IT security by their federation. The positive impact of the GDPR on cybersecurity was also reported, with a 50% increase in requests in some consulting companies.

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 (ECSM, 2018). The support of a wider organisation in which the SME is actively involved is really an ideal, especially if it can be organised with pairs. In our case the workshop co-organised with the construction federation was a success in terms of interactions and experience sharing. Campaigns must combine both passive channels to reach a wide audience but also active events where SMEs can actively engage. Such events should also evolve to avoid the pitfall of annual tick-box exercises that can just worsen the attitude.

So far, we did not explicitly use personae to reach the SMEs but relied on a FAQ which is regularly updated to cope with new issues. Our FAQ is mostly textual but have started to design visuals to make it more appealing, e.g. to explain some key milestones to progress in maturity.

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. A minor technical point is that for animating workshops, we preferred the mobile application over the web version because of its better usability and reliability (off-line mode).

6 CONCLUSION & NEXT STEPS

To summarise, people are a major weakness in cybersecurity, but when engaged and correctly trained, they can become the first line of defence against attackers. In this paper, we reported about our on-going experience in conducting an awareness process in the light of existing instruments. Although this report is still partial and hard to quantify, we believe our feedback can be useful for others engaged in cybersecurity awareness. On the qualitative level, our current feeling is that techniques are complementary and needs to be combined to have a good global effectiveness. Web tools and awareness events can initiate the process which can then rely on more specific tools to match the SME profile, risks and level of maturity.

Our next steps will be to set up a complete portal and refine the self-assessment with other IT experts, especially to make the transition with their work.

ACKNOWLEDGEMENTS

This research was partly supported by Digital Wallonia and the DIGITRANS project (grant nr. 7618). We thanks Infopole and the companies of the cybersecurity cluster.

REFERENCES

ANSSI (2017). SecNumacadémie. https://secnumacademie.gouv.fr.

Ashford, W. (2017). Smes more vulnerable than ever to cyber attacks, survey shows. http://bit.do/computer-weekly-SME-cybersecurity.

BBB (2017). State of cybersecurity among small businesses in north america. Better Business Bureau, http://bit.do/2017-state-of-cybersecurity.

BSI (2018). Cyber security for SMEs. https://www.bsigroup.com/en-GB/Cyber-Security/Cyber-security-for-SMEs.

CCB (2016). Cyber Security Guide for SME. http://www.ccb.belgium.be/en/guide-sme.

CIS (2016). CIS Controls V6.1. https://www.cisecurity.org/controls.

Cooper, A. (1999). *The inmates are running the asylum.* Macmillan Publishing Company Inc.

ECSM (2018). European Cyber Security Month Quiz. https://cybersecuritymonth.eu/references/quiz-demonstration.

ISF (2002). Effective security awareness. Information Security Forum.

Ki-Aries, D. and Faily, S. (2017). Persona-centred information security awareness. *Computers & Security*, 70:663 – 674.

LimeSurvey (2017). the online survey tool - open source surveys. https://www.limesurvey.org.

Lockheed Martin (2018). Are you a cybersecurity ninja or n00b? http://bit.do/lookheedmartin-quiz.

Muller, P. et al. (2015). Annual Report on European SMEs 2014/2015. European Commission.

NCSA (2018). Stay Safe Online - Cybersecurity Awareness Toolkit for SMB. National Cyber Security Alliance.

Osborn, E. et al. (2015). Business Versus Tech: Sources of the Perceived Lack of Cyber Security in SMEs. In *1st Int. Conf. on Cyber Security for Sustainable Society*.

Ponsard, C. (2018). Cybersecurity Quizz (Google Play Store). http://bit.do/QuizzCyberSecurity.

Ponsard, C., Grandclaudon, J., and Dallons, G. (2018). Towards a Cyber Security Label for SMEs: A European Perspective. In *Proc. 4th ICISSP, Funchal, Madeira*.

SafeOnWeb (2018). Test your digital health. https://campagne.safeonweb.be/en.

Sánchez, L. E. et al. (2010). Security culture in small and medium-size enterprise. In *ENTERprise Information Systems*. Springer Berlin Heidelberg.

SBDC, M. (2018). Small business, big threat. https://smallbusinessbigthreat.com.

UK Gov. (2016). Cyber essentials. https://www.cyberaware.gov.uk/cyberessentials.

UK Gov. (2018). Cyber essentials self assessment. https://www.cyberessentials.ie/self-assessment.

VDS (2017). A Brief Assessment for SMEs - Quick Check for Cyber Security. http://vds-quick-check.de.

Zurich IG (2016). Smes' cyber risk awareness is on the rise. https://www.zurich.com/en/media/news-releases/2016/2016-1123-01.