Methodology and Feedback about Systematic Cybersecurity Experts Auditing in Belgium

Christophe Ponsard[1], Jeremy Grandclaudon[1] and Nicolas Point[2]
[1]*CETIC Research Centre, Charleroi, Belgium*
[2]*Multitel Research Centre, Mons, Belgium*

Keywords: Cybersecurity, SME, Assessment, Lightweight Framework, Survey.

Abstract: Increasing the maturity of SMEs with respect to cybersecurity threats is crucial as they are less prepared and less resilient. They are also increasingly exposed and targeted by malicious actors. Providing support means ensuring an effective ecosystem is available to help companies all along the process. Resources have to be available, from raising awareness to performing audit, increasing protection and building response capabilities. In this paper, we report about the progress achieved after one year of deployment of a Belgian cybersecurity initiative focusing on SMEs. An important goal is to make sure minimal requirements will be checked and enforced by cybersecurity experts while letting them use their own methodology. We explain how the expertise is validated using an evaluation grid based on the NIST Cybersecurity framework and CIS 20 criteria directly reflecting protection priorities for SMEs. We also highlight some interesting characteristics and lessons learned in our data set of 25 experts evaluated so far.

1 INTRODUCTION

Small and Medium Enterprises (SMEs) are a strong driver of the world-wide socio-economic development. At European level, they contribute to more that half of the economic value and hire about two third of the workforce (Muller et al., 2015). Given the fast move to a digital society, Information Technology (IT) has become business critical for SMEs and needs to be protected against cybersecurity attacks. However, SMEs tend to be highly focuses on their business and less on the quality of their process and IT infrastructure. They may also lack expertise or time to be fully protected against cybersecurity threats. They may also wrongly assume their size will not attract attackers. In the past few years, the rate of attacks targeting them has increased dramatically with estimations around 60% to 70% (Keeper Security, 2018). As SMEs are also less resilient than bigger companies: more than half of the hacked SMEs do not recover and cease their activity a few month after an attack (NCSA, 2018).

The need to support SMEs in the management of cybersecurity threats is widely acknowledged. At European level, many organisations such as ENISA, SME Alliance, the European Commission, European Cybersecurity Organisation (ECSO) are devoting effort in this area. At national level, most countries have set up some form of program to raise awareness and to provide guidance as reported in our previous work (Ponsard and Grandclaudon, 2018; Ponsard et al., 2019). Examples of such initiatives are the CyberEssentials in UK (UK Gov., 2016) or the Finnish Cyber Security Certificate (FINCSC, 2018).

In Belgium, the effort is currently structuring at the two levels, depicted in Figure 1:

- *The Regional Level* is responsible for the non-certifying audits which aim at ensuring SMEs have identified key cybersecurity risks and have taken adequate measures to manage them. They are helped in this task by a pool of cybersecurity experts. In Wallonia, the driving initiative is called "Keep IT Secure" (KIS for short) and is led by Digital Wallonia (Digital Wallonia, 2018). Expertise is validated by an advisory board which checks that experts master cybersecurity fundamentals and are able to conduct assessment and improvement activities with SMEs. A funding scheme is also available through specific cybersecurity vouchers that will only support the intervention of validated experts.
- *The National Level* is concerned about providing certification based on a light certification scheme inspired by ISO27K (ISO, 2013). It under de-

Ponsard, C., Grandclaudon, J. and Point, N.
Methodology and Feedback about Systematic Cybersecurity Experts Auditing in Belgium.
DOI: 10.5220/0009190307540759
In *Proceedings of the 6th International Conference on Information Systems Security and Privacy (ICISSP 2020)*, pages 754-759
ISBN: 978-989-758-399-5; ISSN: 2184-4356

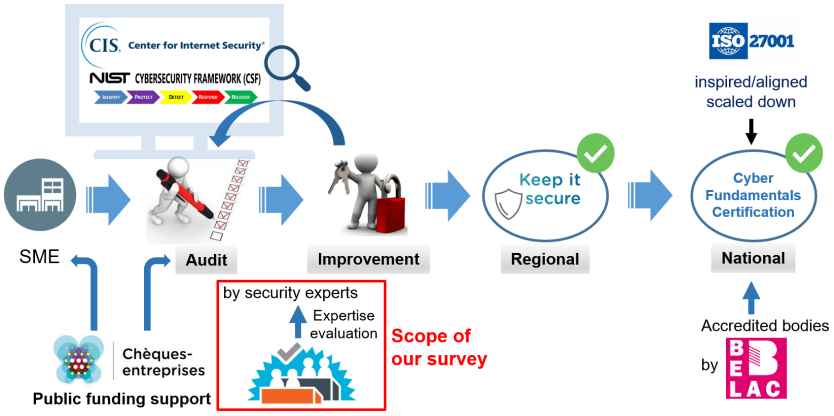

Figure 1: KIS Ecosystem in Belgium and scope of this survey.

velopment by Center for Cybersecurity Belgium which is also supporting awareness actions such as cybersecurity guide for SMEs (CCB, 2016).

The purpose of this paper is to detail how the KIS initiative is practically organised to validate that its experts are qualified to help SMEs. The aim is to be sure they have the required competencies while letting them enough freedom about the methods and tools they want to use in this process. We do not directly report here about the cybersecurity maturity level of SMEs although the required expertise is calibrated to address the threats to which they are exposed.

Our work is structured as follows. First, Section 2 describes how we designed the expert validation phase based on reference frameworks such as the NIST Cyber Security Framework (CSF) and basic security controls such as specified by the Center for Internet Security (CIS). Then Section 3 reports on our application of the resulting expert validation toolkit for the first nine months of its application. During that period, more than 25 experts have been interviewed and all the data has been recorded. Even if the process is still ongoing, we already give a first sketch analysis of key characteristics of our local ecosystem which we believe is quite representative. Our next contribution is to detail some lessons we learned so far along in Section 4. Finally, Section 5 draws some conclusions and presents our planned work.

2 EXPERT ASSESSMENT PROCESS AND TOOLKIT

Keep IT Secured emerged after a long maturing period started in 2017 and involving public authorities, research centres, a local cybersecurity cluster and end-user SMEs through specific awareness-raising events. During our elaboration process, we were inspired by other European initiatives detailed in (Ponsard and Grandclaudon, 2018).

Unlike other domains where posterior control is possible, the sensitive dimension of cybersecurity requires ensuring, prior to any service, that service providers are qualified experts w.r.t. their ability to:

- Identify and manage risks related to the various types of information held by the company especially in the SME context
- Implement adequate protection mechanisms for the various types of systems that contain and manage information

The following key abilities are required and need to be checked:

- General purpose expertise in cybersecurity and reference frameworks
- Ability to embrace all SME-specific cybersecurity issues
- Ability to carry out organisational and technical audits, according to a well-established methodology that may be their own

The criteria are based on international standards and inspired by European labels. These include the NIST CSF (NIST, 2014), the 20 key criteria of the Center for Internet Security (CIS, 2016) and similar approaches undertaken in other countries (e.g. CyberEssentials in Great Britain). These criteria cover the main steps of a cybersecurity risk management approach: identification - protection - detection - response - recovery. The precise methodology is left to the discretion of the auditor but to take into account the 20 key criteria of the CIS. The criteria are also only significant in their contextualisation in relation to the risks incurred. The capability to perform risk

assessment is also evaluated during the interview process based on case studies where basic risks and then more complex risks are progressively injected.

2.1 General Interview Process

As a reminder the interview process considered here concerns the validation of cybersecurity experts. We do not report about audits those experts will carry out later inside SMEs, once their expertise has been validated.

KIS works on a personal basis and not on a company basis. So interviews are carried out individually, even if several experts from the same organisation have applied. It is led by two specialists from the cybersecurity expert advice centre and lasts for a maximum of two hours. After having welcomed and explained the KIS framework, the expert is asked to give an overview of his professional training and experience.

KIS does not impose a methodology on the provider, but checks the coverage of fundamentals that guarantee a good mastery of cybersecurity within SMEs. To do this, a few concrete scenarios are presented and serve as support for a dynamic discussion to evaluate the following aspects:

- Identification of risks in relation to the context of the SME
- Main strategies from prevention to recovery using NIST CSF at top level
- Use of basic controls, based on a detailed checklist inspired from CIS20 but structured around NIST CSF

2.2 Checklist

The check-list is organised as a spreadsheet divided in seven main tabs. First an overview tab for filling the administrative and evaluation information, then an help task explaining the global structure and then five tabs corresponding to the five NIST CSF categories. Those tabs are easy to fill using click control and have room for comments. While an assessor is asking a question, the other is filling and checking to prepare more questions on issues that have not yet been covered by expressing them in the scope of the supporting cases. An interesting way to use it is to upload it on a collaborative platform so it can be filled collaboratively. So the sheet can efficiently help to both drive and control the interview and allows the interviewers to hop from a topic to another while keeping track of everything.

As an example the *Identify* tab is depicted in Figure 2. Each tab is composed of a main categories and then more detailed sections with checks organised by levels: basic, intermediate and advanced. As the interview progresses, basic checks are first covered and then progressively more complex ones but the discussion can also go more quickly deeper in detail on some topics and already cover intermediate and advanced topics. The coverage of all advanced topics is not mandatory and left to the interviewers.

Note that the description remains short reminders about topics to cover during the interview. Their formulation is totally generic and technology-agnostic. However the interview itself will generally introduce some concrete scenarios (see next section) but also

	A	B	C	D	E	F
1	**Identify**					
2		**Spontaneous**	**Questionned**	**Sufficient**	**Problematic**	**Remarks**
3	**Main Categories**					
4	IT Asset Management	☑	☐	☐	☐	
5	Governance	☐	☐	☑	☐	
6	Risk assessment	☑	☐	☑	☐	
7	Risk managements strategy	☐	☐	☐	☑	Missing link with SME business
8						and structure
9	**Basic**					
10	Presence of a computer inventory?	☑	☐	☐	☐	
11	The company's business is clear	☐	☑	☐	☐	
12	Vulnerable resources are identified	☑	☐	☐	☐	
13	Security policy in place?	☑	☐	☐	☐	
14	The risks to the company are identified	☐	☑	☐	☐	
15						
16	**Intermediate**					
17	The risk management process in place	☑	☐	☐	☐	
18	The company's risk level is determined	☐	☑	☐	☐	
19	Availability of a detailed software inventory	☑	☐	☐	☐	
20	The sources of information are identified and verified	☐	☐	☐	☐	Not applicable
21						
22	**Advanced**					
23	The issue of contractors is identified	☑	☐	☐	☐	
24	The measures to address risk management outsourcing are in place	☐	☑	☐	☐	

Figure 2: Global summary of the ”Identify” tab of the KIS assessment spreadsheet.

technological context. E.g. a Cloud storage may be introduced as part of the infrastructure and will trigger the need of more specific checks present in other parts of the sheet. As a result, the filling will not be linear although a global progression from basic to more advanced topics will be followed. So the sheet also ensure that no important topics are overlooked.

2.3 Supporting Scenarios

Scenarios are not described in detail here for evident reasons but are composed of two main cases: one very basic, focus on a SME with basic needs of IT infrastructure and one more specialised in order to be able to ensure a wide coverage. Each case is explored with a raising level of threats. The first case is typically inspired from a traditional domain with a limited IT support: basic network, few workstations, configuration close to domestic use. It then develops the scope of the business activities to increase its dependencies on information technology through on-line orders, transactions, more complex networks, remote access, etc. A complementary case is also used to explore more specific problems such as high availability and sensitive information, e.g. in health or logistics.

2.4 Outcome of the Assessment

Three types of outcome are possible:

- *Positive*, possibly with some points of attention: the expert is integrated in the KIS pool for three years.
- *Positive with Conditions*, i.e. with some improvement points requiring follow-up. The expert is integrated into the KIS pool but will have to undergo a control interview after one year.
- *Negative*: the expert is not allowed to integrated the KIS pool. The reasons can be technical but also the lack of ability to conduct an audit, a lack of general vision (even if the person can be very sharp on a field) or a lack of cybersecurity scope (e.g. pure GDPR consultants, see Section 4). The candidate can also be redirected to other types of services or be advised on how to improve. The candidate can retry a new interview after a minimal period to acquire the missing expertise.

3 ANALYSIS

This section reports on our analysis of 25 evaluations carried out between March and November 2019 (most of them over the past four months). The results are anonymised and presented as aggregated statistics on different dimensions of the questionnaire (considering the five NIST CSF phases and the global maturity level). We also look at the most and less problematic (type of) controls, e.g. controls that experts tend to forget despite their importance. Before going into those details the sample is characterised based on their main domain activities.

3.1 Domain-level Analysis

Our current data set is composed of 25 experts coming from 21 different companies. Most of the companies are of very small size as described in Table 1. For the smallest companies, the domains of activity closely match the (single) expert domains of expertise. Some intermediate companies are organised as network of experts focusing on cybersecurity. The bigger companies have a wider range of activities including a pool of cybersecurity experts.

Table 1: Distribution of company size.

Size	# companies
1	10
2-5	7
6-10	2
>10	2
Total	21

Table 2 presents the overall split across the main domains of activities. Its also reports about the various evaluation outcomes (either full accept, conditional accept or reject as described in Section 2). Note that some experts may have more than one expertise, so the total does not add up to our total number of experts here.

Table 2: Distribution of experts across domains.

Domain	Total	# full accept	# cond. accept	# reject
devops	7	3	3	1
cybersecurity	6	6	0	0
web developer	6	3	2	1
GDPR expert	6	4	0	2
IT audit/strategy	5	4	1	0

Interesting point is that quite a large number of devops and web developers applied for KIS but they often remain too technical. Some lack a wider organisation level perspective enabling risk analysis or simply auditing capabilities. Without too much surprise, experts focusing fully on cybersecurity were all accepted. The point with them was to make sure they adopt a broad and staged view to deal with the SME

context. Another interesting category is IT auditor and consultants in enterprise architecture. Those have very good risk assessment capabilities and are usually able to master the required level of technical expertise in cybersecurity.

3.2 Phase-level Analysis

The phase level analysis is based on the five NIST CSF phases. Table 3 provides the percentage of candidates in each of our four categories of readiness for applying some control, from fully spontaneous to totally discarded. We also provide a global maturity index for each phase which is computed using the following weighted means resulting in a perfect score of 10 (everything spontaneously checked) and a worst score of 0 (everything discarded):

$$\frac{30.\#\{spontaneous\} + 20.\#\{questioned\} + 10\#\{basic\}}{3.\#\{audited\}}$$

Table 3: Distribution of experts across domains.

Phase	Spont.	Quest.	Basic	Disc.	Score
Identify	60%	10%	23%	11%	7,4
Detect	62%	15%	22%	6%	7,9
Protect	78%	5%	15%	7%	8,6
Respond	60%	3%	21%	21%	6,9
Recover	53%	6%	24%	21%	6,5

The resulting score is the higher for the *protect* category, followed by *detect* and *identify* while later *respond* and *recovery* phases are less well investigated. Note there might be some bias due to the fact that more time tend to be spent on earlier phases during the interviews.

When digging further in the answers (not detailed here) the top five categories of controls points are related to our top two scores:

- Awareness (protect)
- Access control and identity management (protect)
- Data security (protect)
- Protection technologies (protect)
- Response to anomalies (detect)

While the bottom five categories of controls points are more mixed across categories:

- Recovery planning (recover)
- Communication (recover)
- Maintenance (protect)
- Risk management (identify)
- Response to anomalies (respond)

4 SOME LESSONS LEARNED

At this stage, we are still learning a lot from the ongoing interview process. However, we could already extract a few interesting points worth being shared.

Overall Reactions of Experts. When launching our initiative, we were a bit concerned about reactions of experts who would not pass the evaluation, especially coming from an unregulated context where self-proclaimed IT experts could start working with SMEs. In the end, in most cases, the process revealed quite smooth. Most experts without track records have actually turned down the interview request and were removed from the KIS pool. Some experts came to have a try but knowing about their limits and more eager to listen to recommendations. As the goal is to help SMES, if a good potential is detected, our goal is, of course to propose an improvement path and another evaluation can be scheduled later on. For the experts that have all the competencies, it is also rewarding as they get some recognition and they also see that some clean-up is done at the benefit of the end-user SMEs. We were also surprise with some elaborated and documented methods some experts had developed, including company awareness-raising actions for some of them.

Responsability Issue. A interesting point is to see how companies are dealing with the fact that the KIS is granted to an individual expert and not to a company. Two alternative behaviours can be observed: either a single expert is labelled for the company. This does not prevent other experts to be involved but all reports must be endorsed by the validated expert who engages it responsibility on the quality of the work delivered to the SME. Another option is to send multiple experts to the evaluation. This second option gives more visibility on the real number of practising experts. However, the process still takes some time and effort to complete so all potential experts of a company are not expected to apply for it.

The GDPR Effect. GDPR was and remains a great incentive for raising awareness about cybersecurity inside SMEs. A downside is that some consulting companies active in GDPR also position themselves on cybersecurity based on their data protection focus. However addressing GDPR is not enough to cover the whole scope of activities required for protecting SMEs from cybersecurity threats. In the end, the point revealed a bit touchy: without banning GDPR experts, they can apply provided they are able to address the full scope of a global cybersecurity audit. As it has

only a partial overlap with GDPR, a pure GDRP consultant will not pass the checking process.

Collecting Evolution Needs. The interview process was also the opportunity to get feedback from the field. Although our assessment grid was designed to fit SME maturity and was validated before starting our interview campaign, some checks proved too advanced like forensics analysis or direct cooperation with local CERT. Other checks may need more detailed breakdown like making sure the security policy matches the company purpose (after identifying both). This evolution is planned on an annual basis and will be discussed with an advisory board involving cybersecurity professors from local universities and with all the interested experts part of KIS with the support of a local cybersecurity cluster. In addition to help us improving our criteria, those meetings also help to define the path to increase the maturity level of SMEs engaged in an cybersecurity improvement process while keeping attracting news SMEs through specific awareness-raising actions. Last but not least, we expect this will also be the opportunity to share some good practices between experts.

5 CONCLUSION & NEXT STEPS

In this paper, we reported about the ongoing evaluation process of cybersecurity experts carried out using the Keep IT Secure framework at the regional level in Wallonia (Belgium). We showed how the framework is aligned with our national perspective and international standards such as NIST cybersecurity and CIS20 while also providing a path to ISO27K. Based on those strong references, we designed an audit methodology for validating the expertise of cybersecurity companies that will help end-user SMEs. The resulting evaluation grid is used in a role-playing game that allows the advise centre to check how well an expert covers the full spectrum of key activities and controls when dealing with an SME case. The process does not impose a specific methodology but follows the expert methodology. This enables to assess how effective it is and to make some recommendations.

Second, we also reported about the analysis of the interesting data set collected during our interviews. Thanks to the systematic use of our check-list, we could perform a quite interesting analysis. Although it requires some extensions both in size and scope, we could already point out interesting characteristics and some lessons learned. We believe our approach could interest other countries dealing with the problem of providing a reliable expert network to help SMEs tackle the cybersecurity threats.

Our future work is to update our analysis based on more audits. At this point an estimated 60% of active cybersecurity companies have been covered. We also plan to evolve our framework based on the collected feedback and to make it available more widely for those interested in sharing similar approaches. At a more global scale, we are working on the interconnection of our work with emerging certification scheme at the Belgian federal level (see Figure 1). We are also providing feedback at European level through specific projects like SPARTA and organisations like ECSO.

ACKNOWLEDGEMENTS

This research was partly supported by Digital Wallonia and the SPARTA H2020 project (nr. 830892). We also thank Infopole, DGO6 and companies of the Walloon cybersecurity cluster.

REFERENCES

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.

Digital Wallonia (2018). Keep IT Secure. https://www.digitalwallonia.be/keepitsecure.

FINCSC (2018). Finnish Cyber Security Certificate. https://www.fincsc.fi.

ISO (2013). Iso/iec 27001 information security management. https://www.iso.org/isoiec-27001-information-security.html.

Keeper Security (2018). 2018 State of Cybersecurity in Small and Medium Size Businesses study. https://start.keeper.io/2018-ponemon-report.

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.

NIST (2014). Cybersecurity Framework. https://www.nist.gov/cyberframework.

Ponsard, C. and Grandclaudon, J. (2018). Survey and guidelines for the design and deployment of a cyber security label for smes. In *4th Int. Conf. on Information Systems Security and Privacy (Revised Selected Papers), Funchal, Madeira, Portugal*.

Ponsard, C., Grandclaudon, J., and Bal, S. (2019). Survey and lessons learned on raising SME awareness about cybersecurity. In *5th Int. Conf. on Information Systems Security and Privacy, Prague, Czech Republic*.

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