International Journal of Standardization Research
Volume 17 • Issue 2 • July-December 2019

Cybersecurity Standardisation for SMEs:
The Stakeholders' Perspectives and a Research Agenda

Bilge Yigit Ozkan, Utrecht University, The Netherlands
https://orcid.org/0000-0001-6406-356X

Marco Spruit, Utrecht University, The Netherlands
https://orcid.org/0000-0002-9237-221X

ABSTRACT

There are various challenges regarding the development and use of cybersecurity standards for SMEs. In particular, SMEs need guidance in interpreting and implementing cybersecurity practices and adopting the standards to their specific needs. As an empirical study, the workshop Cybersecurity Standards: What Impacts and Gaps for SMEs was co-organized by the StandICT.eu and SMESEC Horizon 2020 projects with the aim of identifying cybersecurity standardisation needs and gaps for SMEs. The workshop participants were from key stakeholder groups that include policymakers, standards developing organisations, SME alliances, and cybersecurity organisations. This paper highlights the key discussions and outcomes of the workshop and presents the themes, current initiatives, and plans towards cybersecurity standardisation for SMEs. The findings from the workshop and multivocal literature searches were used to formulate an agenda for future research.

KEYWORDS

Cyberattacks, Information Security, Organisational Characteristics, SDO, Stakeholders, Workshop

INTRODUCTION

A survey in the Global Risks Report (World Economic Forum, 2018) has revealed that cyberattacks are in the top ten risks both in terms of likelihood and impact. Cyberattacks are now seen as the third most likely global risk for the world over the next ten years. According to this study, cybersecurity risks are growing, both in their prevalence and in their disruptive potential. Cyberattacks have both short term and long term economic impacts on different economic agents in terms of losses and expenses (Gañán, Ciere, & van Eeten, 2017).

Small and medium-sized enterprises (SMEs), which are the predominant form of enterprise and make up 99.8% of European enterprises in the Organisation for Economic Co-operation and Development (OECD) area (Digital SME Alliance, 2017), are ill-prepared for cyberattacks.

DOI: 10.4018/IJSR.20190701.oa1

Although there is a multitude of standards available to measure, identify and improve the cybersecurity practices at organisations, many of these are not well suited for SMEs (Manso, Rekleitis, Papazafeiropoulos, & Maritsas, 2015).

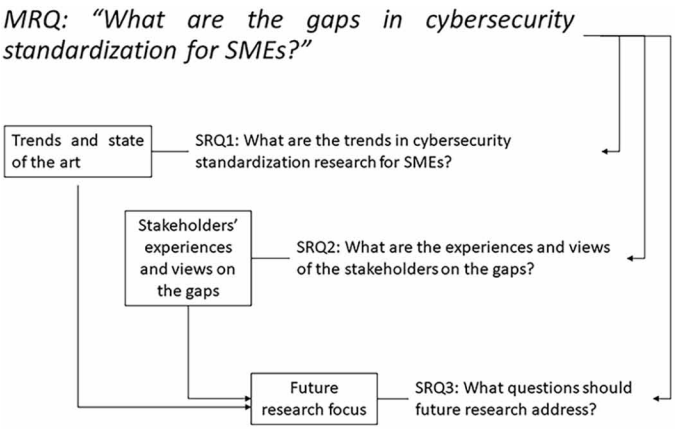
In the standardisation processes, in many cases, SMEs are dependent stakeholders, and they lack resources to properly participate in the process. SMEs typically require financial support, access to technical expertise and other types of assistance to be involved in the standardisation process (de Vries, Verheul, & Willemse, 2003). In addition, SMEs may face other barriers to benefit from standards and involvement in standardisation. Awareness of standards and the process of standardisation are two important barriers (de Vries, Blind, Mangelsdorf, & Verheul, 2009).

The goal of this research is to identify the gaps (e.g. knowledge or facilitation gaps) regarding cybersecurity standardisation for SMEs by performing a literature study, analysing the trends in the literature, describing the initiatives that address SMEs, conducting an empirical study through a workshop with applicable stakeholders, and identifying opportunities for future research. Therefore, the following main research question is put forward: "What are the gaps in cybersecurity standardisation for SMEs?"

To answer this main research question in a structured way, three sub research questions were formulated. The first sub research question examines the trends in the literature and state of the art in European level initiatives addressing cybersecurity standardisation for SMEs. The second sub research question addresses the experiences and views of the stakeholders. The third sub research question addresses the future research directions to be considered to fill the gaps.

A visual depiction of these research questions is shown in Figure 1.

Figure 1. Main research question and sub research questions



SRQ1 is addressed by performing multivocal literature searches to show the trends in the literature on cybersecurity standardisation for SMEs and the state of the art in the European landscape. The findings are presented in the Literature Study section.

SRQ2 is addressed by identifying the stakeholders in cybersecurity standardisation for SMEs and organising a workshop to gather stakeholders' views and perspectives. In that sense, given the importance of cybersecurity, SMEs' challenging situation, lack of research addressing SMEs and the diverse stakeholders, the SMESEC and StandICT.eu EU Horizon 2020 projects co-organized the "Cybersecurity Standards: What impacts and gaps for SMEs" workshop to investigate experiences, needs and gaps in cybersecurity standardisation for SMEs by bringing the key parties together. Thus,

the workshop addresses the second sub research question: "What are the experiences and views of the stakeholders on the gaps?" The workshop was held on May 24, 2019, in Brussels, Belgium.

SRQ3 is addressed by synthesising all findings from SRQ1 and SRQ2 into a focused agenda for future research.

The contribution of this paper to cybersecurity standardisation for SMEs is two-fold: on one hand, it presents the trends in the literature for cybersecurity standardisation research addressing SMEs and the experiences and views of the stakeholders for SME cybersecurity standardisation, on the other hand, it aggregates the related gaps and needs towards an agenda for the standardisation research.

The remainder of the paper is organized as follows. The Literature Study section explains the key terms for information security and cybersecurity that are used for searching the literature, presents the European landscape in SME Standardisation including cybersecurity specific initiatives, and other related literature for the study at hand. The Empirical Study section presents the design of the workshop that was co-organised by the StandICT.eu and SMESEC EU funded Horizon 2020 projects ("Workshop Cybersecurity Standards," 2019), workshop stakeholder groups and participants, information about the workshop including the structure of the workshop, workshop contributions categorised by the stakeholder groups and the key outcomes of the workshop. The gaps and the research agenda formulated from the findings are presented next. The final section provides an overview of practical impacts and concludes the paper.

LITERATURE STUDY

Since the concepts in the cybersecurity and information security domain are intertwined the authors used the terms cybersecurity and information security together for identifying the trends in literature. Albeit, it is important to note the differences between these terms. In this section, first, the respective coverage of these domains is described. Second, to address SRQ1 the literature searches that were performed to identify the trends are presented with the results. Third, findings from the grey literature are presented. This knowledge base comprises the European SME standardisation landscape including cybersecurity-specific initiatives. Finally, a review of SMEs' organisational characteristics influencing their information security (Frederik Mijnhardt, Thijs Baars, & Marco Spruit, 2016) that was particularly used to draw questions for future research to address the insights stemming from the workshop ("Workshop Cybersecurity Standards," 2019) is presented.

Information Security and Cybersecurity

Concepts in the information security and cybersecurity domain are intertwined, making things considerably more complex for untrained stakeholders. Therefore, it is important to distinguish between the scopes and goals of the two distinct fields. According to the ISO/IEC 27032–guidelines for cybersecurity–standard, information security is concerned with "the protection of confidentiality, integrity, and availability of information in general, to serve the needs of the applicable information user" (ISO/IEC, 2012). On the other hand, cybersecurity is defined as "the preservation of confidentiality, integrity and availability of information in the cyberspace". The cyberspace has several characteristics:

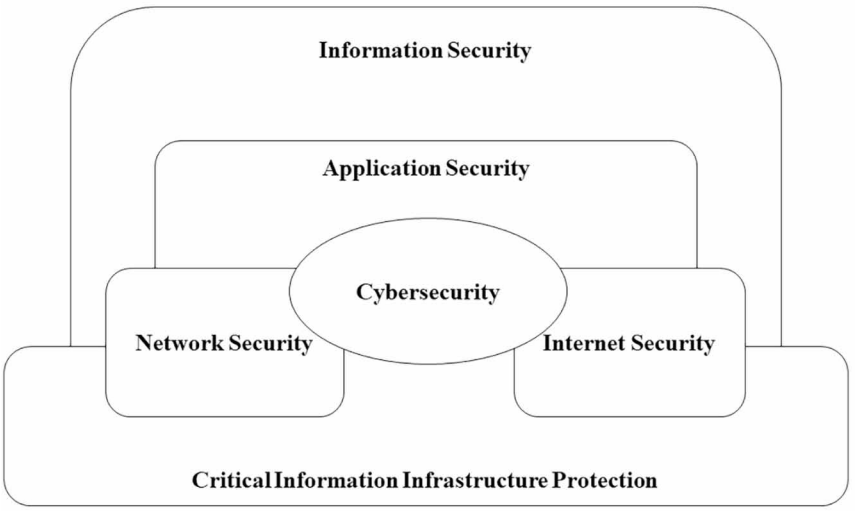
1. It is a virtual environment; the environment does not exist in any physical form;
2. It is a complex environment, which resulted from the emergence of interconnected networks (such as the internet);
3. It has multiple 'dimensions': it is also formed by the people, the organisations and the activities on a plethora of devices and networks that have a connection to the cyberspace.

The ISO/IEC 27032 standard differentiates cybersecurity and other domains of security as depicted in Figure 2 (ISO/IEC, 2012).

The ISO/IEC 27032 standard defines the relationship between cybersecurity and other domains as follows:

Cybersecurity relies on information security, application security, network security, and Internet security as fundamental building blocks…It has a unique scope requiring stakeholders to play an active role in order to maintain, if not improve the usefulness and trustworthiness of the Cyberspace. (ISO/IEC, 2012)

Figure 2. Relationship between cybersecurity and other security domains (redrawn from ISO/IEC 27032 (ISO/IEC, 2012))



Information Security and Cybersecurity Standards for SMEs

In order to help organisations and individuals to improve awareness on standardisation, certification and labelling in cybersecurity, the European Cybersecurity Organisation (ECSO) published an overview of existing cybersecurity standards and certification schemes (ECSO, 2017). Given the extensive number of domain-related standards, this document facilitates the identification of relevant standards easily.

In this state of the art syllabus document, ECSO not only focuses on the standards specific to sectors, but also the standards applicable to generic organisations. The generic organisations in this sense are the ones not associated with any particular industry vertical (e.g. energy, healthcare, and telecom). The standards applicable to generic organisations are also perfectly applicable to industry verticals but may not include the sector-specific requirements. 20 standards and schemes are listed as applicable to generic organisations in the ECSO document. Seven of them are international standards published by ISO (International Organization for Standardization). Only one of these 20 standards and schemes –the Finnish Cyber Security Certificate (FINCSC)– has been identified as addressing specifically SMEs (JAMK University of Applied Sciences, 2020). As the name implies, it is rather a certification scheme than a standard. It is based on self-assessment questionnaires to assess companies followed by the review of the findings by an accredited certification body.

To identify any standards specifically addressing SMEs published by ISO, CEN (European Committee for Standardization) and CENELEC (European Committee for Electrotechnical Standardization), we conducted searches using these organisations' search tools. We identified 3

standards only from ISO – one related with environmental management (ISO, 2019a), one related with innovation management (ISO, 2019b) and one related with human resources management (ISO, 2018)– that either supports phased implementation of a standard or provides additional guidance for SMEs. These are all recent standards; we expect that SDOs will publish more standards addressing SMEs in the future. As described in the "Cybersecurity Specific Initiatives" section of the paper, the Small Business Standards (SBS) guide –"SME Guide for the implementation of ISO IEC 27001 on Information Security Management" (SBS, Digital SME Alliance, 2018)– is under consideration for adoption by CEN-CENELEC.

In a study investigating the suitability of information systems security management standards for SMEs, the authors provide a list of 17 standards and methods (Table 2) (Barlette & Fomin, 2008). Only two of these are marked as theoretically suitable for SMEs. Despite the name of this study implies that more standards had been investigated, the ISO 27001 standard was the only focus of this study regarding information security standards.

ENISA published an overview study titled "Information security and privacy standards for SMEs", which also provides recommendations to improve the adoption of the standards (Manso et al., 2015). In Annex A of ENISA's document, a list of information security and privacy standards for SMEs is provided but with no discussion on how these standards could be adopted by SMEs.

The Digital SME Alliance has recently published a position paper titled "The EU Cybersecurity Act and the role of standards for SMEs" (The European Digital SME Alliance, 2020). This position paper presents the most important challenges for SMEs in the adoption of standards and offer recommendations to SDOs to support SMEs in their challenges. The recommendations include the following options:

Option 1: Further the evolution of existing standards.
Option 2: Develop lightweight standards or guides.
Option 3: Develop new standards specifically for SMEs.
Option 4: Combine different standards into packages tailored to SMEs.

The Digital SME alliance differentiates SMEs by their role in the digital ecosystem and states that the solutions should be tailored according to their specific needs (The European Digital SME Alliance, 2020).

Trends in the Literature

In order to investigate the publication trends (SRQ1), four different search queries were formulated (Table 1) and executed in Scopus and Web of Science (WoS) research index databases. The search scope was limited to publication title, abstract and keywords for Scopus, and topic and title for WoS.

Table 1. Literature search strings (cybersecurity, standard and SME)

Search #	Target Population	Search String
S1	The entire population of papers in cybersecurity domain	("cyber security" OR "cybersecurity" OR "information security")
S2	The sub-population that relates to Standardisation/Standards	(("cyber security" OR "cybersecurity" OR "information security") AND "standard*")
S3	The sub-population that relates to SMEs	(("cyber security" OR "cybersecurity" OR "information security") AND "SME*")
S4	The sub-population that relates to SMEs and Standardisation/Standards	(("cyber security" OR "cybersecurity" OR "information security") AND "standard*" AND "SME*")

Figure 3 presents the results from S1 and S2 respectively. The earliest year of publications found in the databases are: in Scopus, 1967 for S1 and 1985 for S2; in WoS, 1996 for S1 and 1991 for S2.

Accordingly, an increase in the number of publication over the years with an increasing trend is clearly visible (Figure 3-left). In parallel, an increase in the number of publications on cybersecurity standardisation over the years is observed however not trending as much and visible only in recent years (Figure 3-right).

Figure 4 presents the results from S3 and S4. The earliest year of publications found in the databases are: in Scopus, 1998 for S3 and 2004 for S4; in WoS, 2006 for S3 and 2007 for S4.

Figure 3. Trends in the number of research publications on cybersecurity (left) versus cybersecurity standardisation (right)

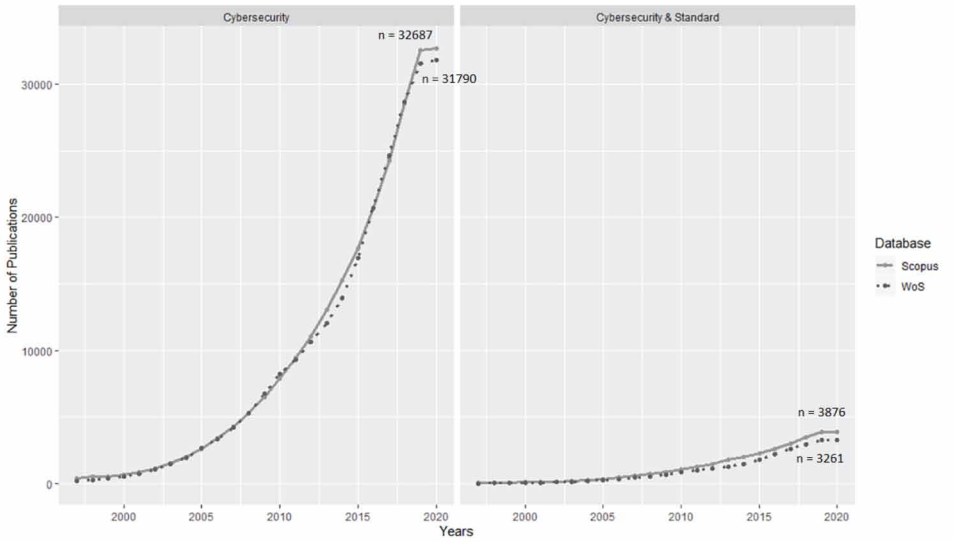
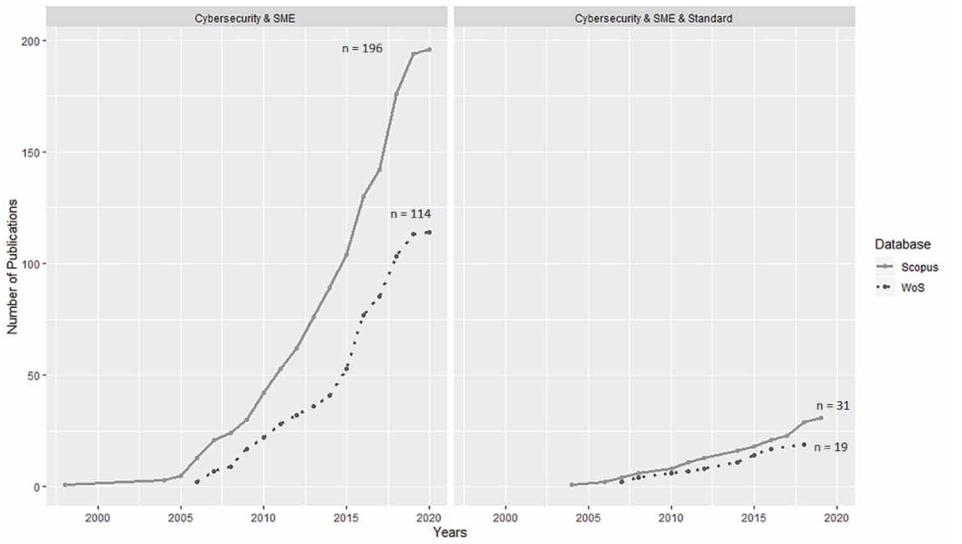


Figure 4. Trends in the number of research publications on cybersecurity and SMEs (left) versus cybersecurity, SMEs and standardisation (right)



Accordingly, security research, in general, has started to consider SMEs after 2005 with a stable trend (Figure 4-left). Among these, very few publications also consider the standardisation aspects (Figure 4-right). They also increase with a stable however lower trend. The proportion of the sub-population that considers SME in the entire security population (Figure 3-left) is less than 1 percent (the number of cybersecurity publications addressing SMEs (Figure 4-left) divided by the number of total cybersecurity publications (Figure 3-left)). Furthermore, what is clear from Figure 3 and Figure 4 is the significant difference between the number of publications on cybersecurity standardisation that addresses SMEs (Figure 4-right) and that does not (Figure 3-right).

To sum up, the evidence from the cyber- and information security publications search suggests that the research interests and outputs that address standardisation in an SME context are few and the topic has only begun to attract the attention of a few researchers in recent years.

In relation to the main research question of this study, the publications results for the right side of Figure 4 were investigated in further detail. This search resulted in 31 publications from the Scopus database and 16 publications from the WoS database. Only three of the publications were identical. Accordingly, the searches from the two databases resulted in 44 unique publications. Detailed investigation showed that, among those publications, 11 articles and 1 conference paper are not addressing SMEs. The SME abbreviation was used for other phrases such as subject matter experts in these articles. Excluding these reduces the number of relevant publications to 32. Table 2 shows

Table 2. Number of publications per publication type (cybersecurity, SME and standard)

Publication Type	Total Number of Publications	Number of Relevant Publications
Article	21	10
Book Chapter	1	1
Conference Paper	17	16
Conference Review	5	0
Total	44	27

the number of publications per publication type. As can be seen from this table, five of the resulting publications are conference review papers. Excluding these papers results in 27 relevant publications in total. Therefore, the Number of Relevant Publications column in Table 2 shows the total number of papers by excluding the publications that are not addressing SMEs and the conference review publications. The list of the relevant and non-relevant publications –presented as a bibliography– can be found in the Appendix.

From the results of the searches performed, the authors conclude that although a considerable amount of literature has been published on information security and cybersecurity standardisation, at a large extent, this literature does not address SMEs. In their paper on a standardisation research agenda, (de Vries et al., 2018) point out that the enormous number of standards (which is the case in the cybersecurity domain) represents a considerable burden for SMEs. In their paper, the authors also state that research on standards' impact on SMEs is limited. Our findings from the literature search support these arguments.

SME Standardisation and European Landscape

In this section, the state of the art with respect to four types of standardisation initiatives aimed at SMEs in European level is presented: Initiatives of Standards Developing Organisations, Initiatives of SME Organisations, Cybersecurity Specific Initiatives, and the EU Rolling out plan for ICT (Information and Communications Technology) standardisation.

Initiatives of Standards Developing Organisations

International, regional or national level Standards Developing Organisations (SDOs) have undertaken several initiatives for helping SMEs in standardisation processes. The SME Standardisation Toolkit (CEN-CENELEC, 2019c) is an example of tools provided by CEN (European Committee for Standardization) and CENELEC (European Committee for Electrotechnical Standardization) to facilitate SME involvement in standardisation. This toolkit is mainly aimed at national standardisation organisations.

Another example to support SMEs in standardisation is the interactive online educational tool (CEN-CENELEC, 2019d) which provides SMEs with a chance to learn about standardisation in a quick and easy way. This e-learning tool is available in 23 languages. Furthermore, BSI (British Standards Institution) has published a guide to standards for small businesses that emphasizes the benefits of standards.

Finally, ETSI (European Telecommunications Standards Institute) published a white paper (ETSI, 2011) on the results of a study to evaluate how to improve the participation of Small and Medium-sized Enterprises (SMEs) in ETSI standardisation. As reported by the Digital SME Alliance, *ETSI recently reviewed its internal procedures to mandate that proposers of new standards describe their relevance to SMEs. As decided by the ETSI Board in January 2020, all new standards projects at ETSI will be accompanied with a form that displays information on their impact on SMEs* (The European Digital SME Alliance, 2020). This news article announces the decision as a success story as the result of the work of SBS in the ETSI decision-making bodies.

Initiatives of SME Organisations

The European DIGITAL SME Alliance is the largest network of the small and medium-sized ICT enterprises in Europe, representing about 20,000 digital SMEs. SBS (Small Business Standards) is a non-profit organisation representing SMEs within the European Standardisation System. SBS published a user guide for European SMEs on ISO 26000 guidance on social responsibility (SBS, 2016).

Cybersecurity Specific Initiatives

With the Communication on ICT Standardisation Priorities, the European Commission (EC) proposes to focus standard-setting resources and communities on 5 priority areas: 5G, Internet of Things, cloud computing, cybersecurity and data technologies because they are essential for wider EU competitiveness (EC, 2016). Every year, the EC releases the Rolling plan on ICT Standardisation, which identifies ICT standardisation activities in support of EU policies. The 2019 plan was published in March. The rolling plan provides a unique overview of standardisation activities in the field of information and communication technologies (ICT) linked to EU legislation and policies, such as healthcare, cloud computing, intelligent transport systems, security, accessibility, Internet of Things, eGovernment, smart grids and many others (EC, 2019). In the "Cybersecurity/ Network and Information Security" section of this plan, EC defines 7 actions requested from the Standards Developing Organisations (SDOs). Among these actions, one of them directly addresses SMEs' needs as follows:

SDOs to develop a "guided" version of ISO/IEC 270xx series (information security management systems including specific activity domains) specifically addressed to SMEs, possibly coordinating with ISO/IEC JTC1 SC27 WG1 to extend the existing guidance laid out in ISO/IEC 27003. This guidance should be 100% compatible with ISO/IEC 270xx and help SMEs to practically apply it, including in scarce resource and competence scenarios. (EC, 2019)

Perfectly aligning with the abovementioned action, the Digital SME alliance and SBS have published the "SME Guide for the implementation of ISO IEC 27001 on Information Security

Management" (SBS, Digital SME Alliance, 2018). This guide is currently under consideration for adoption by CEN-CENELEC.

The European Union Agency for Network and Information Security (ENISA) is conducting security surveys and publishing dedicated cyber security guides for SMEs. ENISA published guidelines for SMEs on the security of personal data processing (European Network and Information Security Agency, 2016) and cloud security guide for SMEs (Dekker, Liveri, Europäische Union, & Agentur für Netz- und Informationssicherheit, 2015). Another publication of ENISA aims to provide a set of relevant recommendations regarding how to increase the adoption of information security and privacy standards in SMEs (Manso et al., 2015).

ECSO (the European Cyber Security Organisation) has a working group (WG4: Support to SMEs, coordination with countries and regions) to support SMEs (ECSO, 2019b).

The National Cybersecurity Centre supports the most critical organisations in the UK, the wider public sector, industry, SMEs as well as the public. The National Cybersecurity Centre operates Cyber Essentials which is an information assurance scheme that encourages organisations to adopt good practices in information security (National Cybersecurity Centre, 2017). Cyber Essentials includes an assurance framework and a simple set of security controls to protect information from threats coming from the internet. To support SMEs in adhering to the approach, the UK government has deployed a specific voucher scheme including coaching, documentation and certification.

The Information Systems Security Association (ISSA) published the ISSA 5173 standard to encourage SMEs to take steps to secure their customer's and employee's data (ISSA UK, 2018). The standard sets out a hierarchy of security controls that are considered both appropriate and affordable.

Cybersecurity Standard Gap Analysis

The challenges for SMEs regarding cybersecurity standardisation are elaborately discussed in the "Cybersecurity standard gap analysis" whitepaper (Cyberwatching.eu, 2018). This white paper was prepared by surveying the cybersecurity research, industry, public sector and user communities in order to get inputs into identifying the perceived gaps. 16% of the survey responders were SMEs. In the whitepaper, the following issues regarding SMEs are listed as recommendations:

- The cost issue for SMEs looking toward standards and cybersecurity certification must be addressed;
- SMEs must be able to access standards and related certification without breaking the bank;
- Self-assessment and other low-cost solutions need to be explored.

Organisational Characteristics Influencing SME Information Security Maturity

It is important to understand the organisational characteristics influencing SME cybersecurity or information security maturity. Based on literature review and expert evaluations (Frederik Mijnhardt et al., 2016) have identified 11 organisational characteristics (OCs) consisting of 47 measurement levels as presented in Figure 5. These OCs can be utilised as an input for developing SME specific cybersecurity standards or tailoring the existing standards for SME characteristics.

EMPIRICAL STUDY: MULTI-STAKEHOLDER WORKSHOP

To address SRQ2, the workshop "Cybersecurity Standards: What impacts and gaps for SMEs" was co-organised by the StandICT.eu and SMESEC EU funded Horizon 2020 projects.

StandICT.eu (Supporting European Experts Presence in International Standardisation Activities in ICT) is an H2020 project that addresses the need for ICT Standardisation and defines a pragmatic approach and streamlined process to reinforce EU expert presence in the international ICT standardisation scene ("About StandICT.eu," 2018). SMESEC (Protecting Small and Medium-

Figure 5. Organisational characteristics and measurement levels in CHOISS (Frederik Mijnhardt et al., 2016)

Organizational characteristic	Measurement levels
General company information	
Number of employees	0–9 employees, 10–49 employees, 50–250 employees
Organization's revenue	0–2 Million, 2–10 Million, 10–50 Million
Organization's sector	Aerospace and Defense; Agriculture and Foresting; Business Services and Consultancy; Consumer, Media, Leisure, Travel and Entertainment; Finance, Banking and Insurance; Health; IT and Telecom; Industrial Production; Energy, Utilities and Mining; Public, Education and Non-Profit; Transport, Packaging and Logistics
Degree of outsourcing	
To what degree is software development outsourced	0–25, 25–50, 50–75, 75–100%
To what degree are software and services hosted externally	0–25, 25–50, 50–75, 75–100%
Reliance on IT for running the business operations	
The organization can do business without IT support for x many hours	<10 min, 10 min to 1 h, 1–24 h, >24 h
CIA (Confidentiality, Integrity, Availability)	
The importance of Availability of the organization's critical information	Low, medium, high
The importance of Confidentiality of the organization's critical information	Low, medium, high
The importance of Integrity of the organization's critical information	Low, medium, high
Complexity of the IT environment	
The number of FTE supporting the IT environment.	0–1 FTE, 1–2.5 FTE, 2.5–5 FTE, 5–10 FTE, > 10 FTE
The organization's annual spend on IT	<1, 1–2.5, 2.5–5, 5–10, >10%

sized Enterprises digital technology through an innovative cyber-SECurity framework) is an H2020 project proposed by an international group of experts as a response to the cyber-security challenges of SMEs with limited background on cybersecurity and a restricted budget ("About SMESEC," 2017).

The workshop was hosted by CEN and CENELEC, supported by ECSO and the Digital SME Alliance, and gathered the key stakeholders described in Table 4 together. In the workshop, there were 12 talks followed by a total of 28 participants including the presenters. This section presents the design of the workshop, workshop stakeholder groups and participants, information about the workshop including the aim and the structure of the workshop. The stakeholders' contributions and the outcomes of the workshop are also presented in this section.

Set-Up

Before organising the workshop, and based on Freeman's (Freeman, 2010) definition of a stakeholder– *any group or individual who can affect or is affected by the achievement of the organization's objectives*–, the authors asked the most experienced members (in SMEs and standardisation processes) of the StandICT.eu and SMESEC consortia to identify key stakeholders for SME cybersecurity standardisation. As a result, five key stakeholder groups were identified:

1. Policymakers, influencers, regulators;
2. Standards Developing Organisations (SDOs);
3. SME Alliances;
4. Cybersecurity Organisations; and
5. EU funded research projects related to cybersecurity for SMEs and ICT standardisation.

After identifying the stakeholder groups, the organisers –the StandICT.eu and SMESEC projects– of the workshop ("Workshop Cybersecurity Standards," 2019) have informed several organisations from each stakeholder group about the aim of the workshop and invited them to participate in the workshop. The majority of the stakeholders were interested in the workshop and at least one stakeholder from each group agreed to participate. After the workshop, the authors analysed the stakeholders' contributions during the workshop. This paper categorises the findings by stakeholder groups as presented in Table 4.

Workshop Participants

The authors analysed the types of the stakeholders using the IT standardisation stakeholder typology presented in (de Vries et al., 2003) since it was specifically defined for IT standardisation processes and was illustrated by an information security management standard case study. In (Mitchell, Agle, & Wood, 1997), the authors present the attributes of stakeholders as power, legitimacy and urgency. Using these attributes, they propose a stakeholder typology based on the number of attributes possessed by the stakeholders. In the typology proposed, there are seven types of stakeholders namely, dormant, dominant, dangerous, definitive, discretionary, demanding and dependent. (de Vries et al., 2003) present the definition of these stakeholder types adapted to the standardisation processes. In the workshop, there were stakeholders of definitive, dominant, discretionary and dependent types. The definitions of these types adapted to the standardisation processes are presented in Table 3 (de Vries et al., 2003).

Table 3. Stakeholder types and definitions (de Vries et al., 2003)

Stakeholder Type	Definition
Definitive	Definitive stakeholders have the power to affect the standardisation process, they consider the standard to be important, and their involvement is indisputable.
Dominant	Like the discretionary stakeholder, the dominant stakeholder itself does not see immediate interest in participating, while its participation is considered desirable from the perspective of the standardisation process.
Discretionary	Discretionary stakeholders do not have the resources to affect the standardisation process and feel no urgent need to participate.
Dependent	The dependent stakeholders are important for the general support of a standard and they see the need to participate in the standardisation process.

Accordingly, SMEs can be categorised as either discretionary or dependent stakeholders, depending on their level of security awareness. SMEs that do see the need for information security belong to dependent stakeholder category. Dependent stakeholders in many cases lack resources to properly participate in the standardisation process. SMEs require financial support, access to technical expertise and other types of assistance to be involved in the standardisation process (de Vries et al., 2003).

The stakeholder groups and the matching workshop participants are listed in Table 4 together with their stakeholder types. In the workshop, SMEs were represented by two SME alliances as presented in Table 4. The stakeholders listed in Table 4 interact with each other, establish liaisons, coordinate and collaborate their activities in several settings. There are initiatives such as joint technical committees (CEN-CENELEC, 2019a) (“ETSI - Cyber Security,” 2019), working groups (ECSO, 2019a) (ECSO, 2019b), workshops (CEN-CENELEC, 2019b), publications (Manso et al., 2015), surveys (Cyberwatching.eu, 2018), and meetings to ensure the harmonisation of these stakeholders’ efforts for cybersecurity standardisation for SMEs.

In addition to the stakeholders given in Table 4, three ICT standardisation experts, one government representative, two independent researchers, and seven private sector members participated in the workshop.

Structure of the Workshop

The workshop comprised of a keynote, three panels and a wrap-up session that are elaborated upon as follows. The Keynote introduced the EU Cybersecurity Package and the Innovation & Research Plan

Table 4. Workshop stakeholder groups, participants and their types

Stakeholder Group	Workshop Participant Organisation	Number of Participants (per Group)	Stakeholder Type			
			Definitive	Dominant	Discretionary	Dependent
Policymakers, influencers, regulators	• European Commission (EC)	4	X	X		
Standard Developing Organisations (SDOs)	• CEN (European Committee for Standardization) • CENELEC (European Committee for Electrotechnical Standardization) • ETSI (European Telecommunications Standards Institute)	2	X			
SME Alliances	• Small Business Standards (SBS) • Digital SME Alliance	3			X	X
Cybersecurity Organisations	• European Cyber Security Organisation (ECSO)	1	X	X		
EU funded research projects related to cybersecurity for SMEs and ICT standardisation	• SMESEC.eu • StandICT.eu	5	X		X	X

towards Horizon Europe. Panel 1 set the scene of cybersecurity standardisation impacting SMEs. The panel's speakers were the key representatives from the Standard Developing Organisations (SDOs) on achievements to date and future challenges. Panel 2 gave a voice to SMEs. In this panel, there were two speakers from EU funded H2020 projects and one speaker from ECSO WG4 (Working Group 4) (ECSO, 2019b). Panel 3 provided a voice from SMEs, providing an opportunity for the SMEs to report on gaps and needs on cybersecurity standards and best practices. At the end of the workshop, a wrap-up was presented to synthesise the findings and final words could be expressed by the participants. Every stakeholder expressed their willingness to collaborate in helping SMEs with their cybersecurity standardisation challenges. The next section elaborates on the workshop sessions, organised by stakeholder groups.

Workshop Contributions Categorised by Stakeholder Groups

Policymakers, Influencers, Regulators

The EC representative gave a policy level talk and introduced the EU Cybersecurity Package and the Innovation & Research Plan towards Horizon Europe. The speaker expressed that the Cybersecurity Package will enable a more robust response to cyber-attacks by:

- Encouraging a Single Cybersecurity Market;
- Pooling and shaping research efforts in Cybersecurity;
- Fostering NIS (Network and Information Security) Directive implementation;
- Proposing a reformed ENISA;

- EU Cybersecurity Certification;
- Coordinating an emergency response.

The EC representative also addressed the key topic for SDOs as certification. According to the EC representative, for the cybersecurity domain, certification will evolve similar to the energy and aviation domains. A participant from the EC pointed out that EU funded H2020 projects have standardisation as a task and can allocate resources, on the other hand, SDOs lack resources. There is no link between these two. Some action should be taken to tighten the connection that will benefit both sides.

Standards Developing Organisations (SDOs)

The CEN - CENELEC JTC (Joint Technical Committee) 13 (CEN-CENELEC, 2019a) representative addressed the main objective of the JTC 13 as the transposition of international standards to European standards. The scope of activities of the JTC 13 is the development of standards for cybersecurity and data protection covering all aspects of the evolving information security. JTC 13 has several liaisons including JTC 8 Privacy management and ETSI TC (Technical Committee) Cyber. The current activities of JTC 13 are twofold. First, the transposition of international standards (27 standards in total) like the ISO/IEC 27K series and others such as the ISO/IEC 29100 Privacy framework, and ISO/IEC 19790 Security requirements for cryptographic modules. Second, feasibility studies include the feasibility study on Small Business Standards (SBS) ISO 27001 Guide for SMEs, lightweight evaluation methods (other than as proposed by ISO/IEC 15408), a data protection interface and data protection professional profiles. The JTC 13 representative concluded that SME needs are a strong driver to ease the knowledge and use of International and European standards.

The ETSI TC Cyber representative who gave an overview of the committee and described the diverse scope of areas they are working on. The speaker pointed out the BSI / PETRAS white paper ("Navigating and Informing the IoT Standards Landscape | BSI Group," 2019) which reports on the following:

- Opportunities and challenges that IoT (Internet of Things) SMEs and start-ups face when developing connected products;
- SME's priority areas for standardisation;
- Accessible summary of the IoT policy and standards landscape.

The ETSI TC Cyber representative addressed the ETSI technical specification 103 645 - Cyber Security for Consumer Internet of Things as the first globally-applicable industry standard on consumer IoT security (ETSI, 2019). It is agreed to transpose TS 103 645 into a European Standard (EN). A European Standard (EN) automatically becomes a national standard in each of the 34 CEN-CENELEC member countries. In addition, a test specification is being considered to sit alongside TS 103 645. The speaker informed the attendees that there is an opportunity for SMEs and ETSI members to contribute to these documents.

A CEN-CENELEC participant pointed out there is no or poor follow up for the standardisation proposals. According to the participant, a reason for this might be it is being a prolonged process.

SME Alliances

The representative from Digital SME alliance introduced the alliance that is the first European association in the ICT sector exclusively focused on SMEs. The speaker gave some figures regarding cybersecurity statistics for SMEs as follows (Mansfield, 2017):

- 43% of cyberattacks target small business;
- 14% of small businesses rate their ability to mitigate cyber risks, vulnerabilities and attacks as highly effective;

- 60% of small companies go out of business within six months after a cyberattack.

The speaker pointed out their important publication "SME Guide for the Implementation of ISO/IEC 27001 on Information Security Management" (SBS, Digital SME Alliance, 2018) which is currently under consideration for adoption by CEN-CENELEC. More ideas on cybersecurity standards for SMEs were introduced by the speaker as follows:

- Preparing a GDPR (General Data Protection Regulation) Guide for SMEs;
- Preparing a guide for SMEs on a consumer standard for IoT;
- Expanding the ISO27001 guide for SMEs (after review);
- Lightweight cyber schemes for SMEs, guide on specific IoT.

The representative from SBS joined the workshop remotely and presented the goals of SBS as to represent and defend SMEs' interests in the standardisation process at European and international levels, to raise the awareness of SMEs about the benefits of standards, and to encourage them to get involved in the standardisation process. The speaker commented that regarding the cyber domain and standardisation, all cybersecurity aspects are covered (i.e. no significant gaps), but the following issues do exist:

- There are too many standards, and many are not actionable or particularly useful (entry barrier for SMEs);
- There is a need to converge toward useful, interoperable sets of standards;
- If not freely available on-line, constantly evolving, and well-versioned, there is a risk of low practical value;
- There is a need for broad industry & society, public-private support and adoption (multi-stakeholder holistic approach);
- The speaker pointed out SBS's position at ETSI TC CYBER for translating the standards for SMEs and proposed the following options for SDOs adapting standards for SMEs:
  - Evolution – new versions with specific levels to existing standards ("maturity levels"), adapted and applicable to SMEs;
  - Lightweight standard/requirements/recommendation – amend a special section for SMEs as "minimum requirements";
  - Develop new, specific standards for SMEs;
  - Combined requirements (or "guidelines/recommendations") – a "security pack" (cyber hygiene).

Cybersecurity Organisations

The representative from ECSO WG1 Standardisation, certification, labelling and supply chain management (ECSO, 2019a) gave an overview of ECSO which has 251 member organisations among which 20-25% are SMEs. It was stated that ECSO unites and represents European cyber security industry players, as well as national public administrations, research centres, SMEs, regions, and academia. The speaker pointed out ECSO's publication, the State of the Art Syllabus (SoTA) - Overview of existing cybersecurity standards and certification schemes (ECSO, 2017) which includes 290 standards and schemes, and is currently under revision. There is currently a call for contribution to update this document. Furthermore, it is important to note that ECSO WG1 is collaborating with ETSI, CEN, CENELEC, ENISA and others.

The representative from ECSO WG4 (ECSO, 2019b) presented the strategy, objectives and achievements of their working group. ECSO WG4 focuses on the following:

- Support the development of SMEs, start-ups and high growth companies;

- Develop coordinated activities between clusters (both business-oriented and triple helix), regions and local bodies (for local implementation of solutions and educations);
- Development of East and Central EU public and private sectors dealing with cybersecurity.

The speaker introduced the ECSO SME HUB as a unique platform promoting "Cybersecurity Made in Europe" and the ECSO label as a private marketing tool fostering the claim of quality and security of European companies. It was pointed out that this label is not a certification tool, but aims to reflect three key messages: "made in Europe", "created and developed by ECSO" and "issued by a qualified organisation". The eligibility criteria to acquire this label were also presented.

EU Funded Projects Related to Cybersecurity for SMEs and ICT Standardisation

The SMESEC project's two-dimensional perspective was presented to the workshop attendees. These dimensions are the technical solution and the human and organisational context. The representative introduced the contribution opportunities for the SMESEC project to cybersecurity standardisation for SMEs by liaising and coordinating with relevant stakeholders.

In the SMESEC project, the CySME maturity model (SMESEC, 2018) is being developed as part of the framework. This maturity model will make self-assessment of cybersecurity capabilities for SMEs possible in a standards-transparent way. CySME questionnaires, which are a coherent collection of SME-specific quick scans on all SME-relevant cybersecurity focus areas with corresponding security controls and best practices from all existing cybersecurity-related standards, including ISO and ETSI, are being implemented by the CYSEC tool (Shojaifar, Fricker, & Gwerder, 2018). The CYSEC tool is also being developed as part of the SMESEC framework positioned as a self-reliant capability assessment, training and awareness platform for SMEs. The CySME maturity model (SMESEC, 2018) will help SMEs with their initiatives for self-assessing and improving cybersecurity capabilities in a standards-transparent way.

The SMESEC project aims to deliver a cybersecurity standardisation guide for SMEs that will facilitate their awareness.

The objectives of the StandICT.eu project were described as follows:

- Supporting the participation of EU experts in international ICT standardisation activities;
- Ensuring the promotion of European requirements and interests;
- Raising awareness on the advantages of adopting ICT Standards;
- Building strong motivation to businesses and SMEs, in addition to researchers, to contribute to the shaping of ICT Standards.

The StandICT.eu representative explained the tool "Standards Watch" (StandICT.eu, 2019) which monitors the status of ICT standards at the international level, mapping critical areas such as Cybersecurity, 5G, Cloud Computing, IoT, Big Data and Artificial Intelligence. The speaker also presented the latest figures, such as the number of funded applications, 154 for their first five open calls; 53 of these funded applications were related to cybersecurity.

Three StandICT.eu funding grantees presented their experiences. These three professionals fully engaged in the cybersecurity domain who showcased the European Gaps & Priorities addressed by their work with the support of the initiative.

Outcomes of the Workshop

The five most important cybersecurity standards gaps and needs identified at the workshop –along with the stakeholder group that raised the needs– can be summarised as follows:

1. SMEs need guides for implementing existing cybersecurity standards (SDOs and SME Alliances);

2. The cost of acquiring and implementing standards is a problematic issue for SMEs (SME Alliances);
3. SMEs would benefit from standards with maturity levels applicable to SMEs (SME Alliances);
4. SME-specific standards can be considered as an option to fulfil the needs of SMEs (SME Alliances);
5. EU funded research projects have standardisation as a task and can allocate resources, on the other hand, SDOs lack resources. There is no link between these two. Some action should be taken to tighten the connection that will benefit both sides (Policymakers, Influencers, Regulators).

As a result of the presentations and discussions during the workshop, the following were the additional highlights:

- CEN-CENELEC JTC13 is considering the adoption of SBS's guide for implementing ISO/IEC 27001 for SMEs;
- ETSI has recently published TS 103 645 - Cyber Security for Consumer Internet of Things impacting SMEs;
- During the workshop, ECSO announced that the new version of the SoTA syllabus document (ECSO, 2017) is being prepared and contributions are expected from the relevant parties;
- As the workshop helped establish the expectations of different stakeholders, an important proposed activity can be the contribution of the related stakeholders to the revision of the two aforementioned documents (ECSO, 2017) (ETSI, 2019) as requested by ECSO and ETSI respectively;
- In addition, the SMESEC and StandICT.eu projects had the opportunity to gather insights from the participants to steer their future works. The outcomes of the workshop and planned and ongoing work are promising in the sense that will help to move the collective efforts forward.

RESEARCH AGENDA: CYBERSECURITY STANDARDISATION FOR SMES

The top 5 cybersecurity standards gaps and needs that the authors identified below result from both the multivocal literature searches and the workshop. In order to better focus and integrate future research, the authors define corresponding research questions to address these gaps as a research agenda proposition in Table 5.

CONCLUSION

In standardisation research, prior work has emphasized the challenges and barriers for SMEs in standardisation. The importance of stakeholder identification in standardisation processes has also been pointed out before. This research set out to operationalize these observations by physically gathering the key stakeholders together in a workshop to identify their perspectives on the gaps in cybersecurity standardisation for SMEs.

This paper highlights the trends in the literature, identifies the state of the art in the European landscape, presents the key discussions and outcomes of the workshop and presents the themes, current initiatives, and plans towards cybersecurity standardisation for SMEs. Furthermore, the SMEs' position regarding cybersecurity standardisation and gaps is presented from the stakeholders' point of views.

The findings from the multivocal literature search and the workshop were formulated to identify the Top 5 gaps in cybersecurity standardisation for SMEs and to propose an agenda for future research. Further research on the posed research questions would be useful to better address SMEs in cybersecurity standardisation.

The workshop also had some practical impacts on the participants. The participants had the opportunity to hear about the current happenings and recently published documents related to cybersecurity standardisation, to discuss the cybersecurity standardisation gaps and needs for SMEs,

Table 5. Agenda for future research

Gaps and Research Questions	
Gap 1: Lack of SMEs' awareness and involvement in standardisation processes	
RQ 1.1	How can SMEs' awareness and involvement in cybersecurity standardisation be improved?
Gap 2: Lack of cybersecurity standards specifically addressing SMEs	
RQ 2.1	How can standards incorporate organisations' maturity levels?
RQ 2.2	How can SME-specific standards be developed?
RQ 2.3	How can organisational characteristics be used in developing standards specifically for SMEs?
RQ 2.4	How do SME cybersecurity requirements differ by their role in the digital ecosystem?
Gap 3: Challenges of adapting existing cybersecurity standards for SMEs	
RQ 3.1	How can maturity levels applicable to SMEs be introduced in standards?
RQ 3.2	What are the barriers for SMEs in adapting standards?
RQ 3.3	How can existing standards be adapted to SME characteristics?
RQ 3.4	How can organisational characteristics be used in adapting existing standards to SMEs?
RQ 3.5	To what extent the extensive number of cybersecurity standards raise a barrier for SME standardisation?
RQ 3.6	How can the need to converge toward useful, interoperable sets of standards be addressed?
Gap 4: Financial barriers of available standards by SMEs	
RQ 4.1	How can SMEs acquire standards and certifications at an affordable price?
RQ 4.2	To what extent do consultancy, implementation and maintenance costs influence SMEs uptake of standards and certifications?
Gap 5: Lack of co-operation between the stakeholders	
RQ 5.1	How can a direct link between EU funded research projects on cybersecurity and SDOs be established?

to hear about successful professionals' experiences working on cybersecurity standardisation, and to get in contact and network with other stakeholders. The participation, involvement and interest of the stakeholders in the workshop indicate their willingness to co-operate to address SMEs in cybersecurity standardisation.

To the best of our knowledge, this workshop was the first of its kind, focusing on cybersecurity standardisation for SMEs by bringing the related parties physically together. It would be beneficial if further workshops were organised to give especially SMEs (as the users of the standards) the opportunity to express their experiences about dealing with the challenges and their expectations regarding cybersecurity standardisation.

Although this research mainly addresses cybersecurity standardisation challenges that SMEs face, the proposed future research focus includes research questions applicable to other standardisation domains due to the generic –not cybersecurity specific– nature of some of the challenges. The literature study in this research presents SME standardisation initiatives of SDOs that are not specific to cybersecurity. The findings show that there are only a few standards that specifically address SMEs. These standards –all published by ISO– are in environmental management, innovation management and human resources management domains. ISO plays a leading role in providing SMEs with guidance on how to adapt existing standards. ETSI, with its recent board decision –to mandate that proposers of new standards describe their relevance to SMEs– has now taken another step forward to better support SME participation in standardisation processes.

ACKNOWLEDGMENT

This work was made possible with funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 740787 (SMESEC). The opinions expressed and arguments employed herein do not necessarily reflect the official views of the funding body. The authors wish to thank Philippe Cousin and Silvana Muscella for making the workshop possible. Philippe Cousin from the SMESEC project took a leading role in establishing stakeholders' involvement in the workshop and finalising the structure of the workshop. Silvana Muscella from the StandICT.eu project took a leading role in the logistics and organisation of the workshop.

REFERENCES

About SMESEC. (2017). Retrieved June 20, 2019, from https://www.smesec.eu/about.html

About StandICT.eu. (2018, March 30). Retrieved June 20, 2019, from StandICT.eu website: https://www.standict.eu/about-standicteu

Barlette, Y., & Fomin, V. V. (2008). Exploring the Suitability of IS Security Management Standards for SMEs. *Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HICSS 2008)*, 308–308. doi:10.1109/HICSS.2008.167

CEN-CENELEC. (2019a). *CEN/CLC/JTC 13*. Retrieved June 20, 2019, from https://standards.cen.eu/dyn/www/f?p=204:7:0:FSP_ORG_ID:2307986&cs=1E7D8757573B5975ED287A29293A34D6B

CEN-CENELEC. (2019b). *Cybersecurity standardization—CEN-CENELEC Workshop*. Retrieved June 20, 2019, from https://www.cencenelec.eu/news/events/Pages/EV-2019-001.aspx

CEN-CENELEC. (2019c, July 11). *SME Standardization Toolkit*. Retrieved November 7, 2019, from https://www.cencenelec.eu/sme/SMEST/Pages/default.aspx

CEN-CENELEC. (2019d, November 7). *Standards eSME*. Retrieved November 7, 2019, from http://www.standards-esme.eu/

Cyberwatching.eu. (2018, October). *Cybersecurity Standard Gaps Analysis*. Retrieved from https://cyberwatching.eu/sites/default/files/White-Paper-Cybersecurity-Standard-Gaps-Analysis_Cyberwatching.eu-October2018.pdf

de Vries, H., Blind, K., Mangelsdorf, A., & Verheul, H. (2009). *SME access to European standardization*. Retrieved from https://www.unms.sk/swift_data/source/dokumenty/technicka_normalizacia/msp/SME-AccessReport.pdf

de Vries, H., Jakobs, K., Egyedi, T. M., Eto, M., Fertig, S., Kanevskaia, O., & Scaramuzzino, G. et al. (2018). Standardization: Towards an Agenda for Research. *International Journal of Standardization Research*, *16*(1), 52–59. doi:10.4018/IJSR.2018010104

de Vries, H., Verheul, H., & Willemse, H. (2003). *Stakeholder identification in IT standardization processes*. Academic Press.

Dekker, M., Liveri, D., Europäische Union, & Agentur für Netz und Informationssicherheit. (2015). *Cloud security guide for SMEs cloud computing security risks and opportunities for SMEs*. 10.2824/508412

Digital SME Alliance. (2017, July 31). *Position Paper on European Cybersecurity Strategy: Fostering the SME ecosystem*. Retrieved from https://www.digitalsme.eu/digital/uploads/20170731-DIGITAL-SME-Cybersecurity-Position.pdf

EC. (2016, April 19). *Communication on ICT Standardisation Priorities*. Retrieved December 11, 2019, from ICT Standardisation Priorities for the Digital Single Market website: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52016DC0176&from=EN

EC. (2019, March 25). *2019 Rolling Plan for ICT Standardisation*. Retrieved from https://ec.europa.eu/docsroom/documents/34788/attachments/1/translations/en/renditions/native

ECSO. (2017). *ECSO State of the Art Syllabus v2*. Retrieved from https://www.ecs-org.eu/documents/uploads/updated-sota.pdf

ECSO. (2019a). *European Cyber Security Organisation—Work Group 1*. Retrieved June 20, 2019, from ECSO - European Cyber Security Organisation website: https://ecs-org.eu/working-groups/wg1-standardisation-certification-labelling-and-supply-chain-management

ECSO. (2019b). *European Cyber Security Organisation—Work Group 4*. Retrieved June 20, 2019, from ECSO - European Cyber Security Organisation website: https://ecs-org.eu/working-groups/wg4-support-to-smes-coordination-with-countries-and-regions

ETSI. (2011, February). *Participation of SMEs in Standardization*. Retrieved from https://www.etsi.org/images/files/ETSIWhitePapers/WP_No_6_SME_FINAL.pdf

ETSI. (2019). *ETSI TS 103 645—Cyber Security for Consumer Internet of Things*. Retrieved June 21, 2019, from https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf

ETSI - Cyber Security. (2019). Retrieved June 20, 2019, from https://www.etsi.org/committee/1393-cyber

European Network and Information Security Agency. (2016). *Guidelines for SMEs on the security of personal data processing*. ENISA.

Freeman, R. E. (2010). *Strategic Management: A Stakeholder Approach*. Cambridge University Press. doi:10.1017/CBO9781139192675

Gañán, C. H., Ciere, M., & van Eeten, M. (2017). Beyond the pretty penny: The Economic Impact of Cybercrime. *Proceedings of the 2017 New Security Paradigms Workshop*, 35–45. doi:10.1145/3171533.3171535

ISO. (2018). *ISO 30414:2018 Human resource management—Guidelines for internal and external human capital reporting*. Retrieved March 6, 2020, from ISO website: https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/06/93/69338.html

ISO. (2019a). *ISO 14005:2019 Environmental management systems—Guidelines for a flexible approach to phased implementation*. Retrieved March 6, 2020, from ISO website: https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/07/23/72333.html

ISO. (2019b). *ISO 56003:2019 Innovation management—Tools and methods for innovation partnership—Guidance.* Retrieved March 6, 2020, from ISO website: https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/06/89/68929.html

ISO/IEC. (2012). *ISO/IEC 27032:2012—Information technology—Security techniques—Guidelines for cybersecurity*. Retrieved December 14, 2017, from https://www.iso.org/standard/44375.html

ISSA UK. (2018). *ISSA UK Home Page*. Retrieved December 11, 2019, from https://www.issa-uk.org/

JAMK University of Applied Sciences. (2020). *FINCSC – Finnish Cyber Security Certificate*. Retrieved March 3, 2020, from Finnish Cyber Security Certificate website: https://www.fincsc.fi/en/services/

Mansfield, M. (2017, January 3). *Cyber Security Statistics: Numbers Small Businesses Need to Know*. Retrieved June 25, 2019, from Small Business Trends website: https://smallbiztrends.com/2017/01/cyber-security-statistics-small-business.html

Manso, C. G., Rekleitis, E., Papazafeiropoulos, F., & Maritsas, V. (2015). *Information security and privacy standards for SMEs: Recommendations to improve the adoption of information security and privacy standards in small and medium enterprises.* Retrieved from http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0215977:EN:HTML

Mijnhardt, F., Baars, T., & Spruit, M. (2016). Organizational Characteristics Influencing SME Information Security Maturity. *Journal of Computer Information Systems*, *56*(2), 106–115. doi:10.1080/08874417.2016.1117369

Mitchell, R. K., Agle, B. R., & Wood, D. J. (1997). Toward a Theory of Stakeholder Identification and Salience: Defining the Principle of Who and What Really Counts. *Academy of Management Review*, *22*(4), 853–886. doi:10.5465/amr.1997.9711022105

National Cybersecurity Centre. (2017, September 26). *National Cybersecurity Centre—CyberEssentials (UK).* Retrieved December 11, 2019, from Cyber Essentials website: https://www.cyberessentials.ncsc.gov.uk/

Navigating and Informing the IoT Standards Landscape | BSI Group. (2019). Retrieved June 21, 2019, from https://www.bsigroup.com/en-GB/navigating-and-informing-the-iot-standards-landscape/

SBS. (2016, November). *Small Business Standards User Guide for European SMEs on ISO 26000 Guidance on Social Responsibility*. Retrieved from https://www.sbs-sme.eu/sites/default/files/publications/SBS%20SME%20ISO%20User%20Guide%202016_FINAL.pdf

SBS, Digital SME Alliance. (2018). *SME Guide for the implementation of ISOIEC 27001 on information security management*. Retrieved from https://www.digitalsme.eu/digital/uploads/SME-Guide-for-the-implementation-of-ISOIEC-27001-on-information-security-management.pdf

Shojaifar, A., Fricker, S. A., & Gwerder, M. (2018). Elicitation of SME Requirements for Cybersecurity Solutions by Studying Adherence to Recommendations. *REFSQ 2018 Joint Proceedings of the Co-Located Events*. Presented at the *24th International Conference on Requirements Engineering: Foundation for Software Quality*.

SMESEC. (2018, June). *CySME Maturity Model*. Retrieved June 27, 2019, from https://www.smesec.eu/News/180610_SMESecMM_UU.html

StandICT.eu. (2019). *Standards Watch*. Retrieved June 21, 2019, from StandICT.eu website: https://www.standict.eu/standards-watch

The European Digital SME Alliance. (2020, February 7). *Standardisation Success Story: "Relevance to SMEs" becomes a priority for new ETSI standards*. Retrieved March 6, 2020, from European Digital SME Alliance website: https://www.digitalsme.eu/relevance-to-smes-becomes-a-priority-for-new-etsi-standards/

Workshop: Cybersecurity Standards: What impacts and gaps for SMEs. (2019, April 15). Retrieved June 20, 2019, from StandICT.eu website: https://www.standict.eu/events/cybersecurity-standards-what-impacts-and-gaps-smes

World Economic Forum. (2018). *The Global Risks Report*. Retrieved from http://www3.weforum.org/docs/WEF_GRR18_Report.pdf

APPENDIX

The search string S4 in Table 1 resulted in 44 unique publications from Scopus and WoS. The detailed analysis of these publications is presented in Table 2. The list of relevant publications and non-relevant publications are presented in this appendix as two separate bibliographies as follows.

- The list of relevant unique publications (27 in total) resulting from the search string S4 (Table 2):

Alebrahim, A., Hatebur, D., Fassbender, S., Goeke, L., & Côté, I. (2015). A Pattern-Based and Tool-Supported Risk Analysis Method Compliant to ISO 27001 for Cloud Systems. In Transportation Systems and Engineering: Concepts, Methodologies, Tools, and Applications (pp. 730–747). Retrieved from www.igi-global.com/article/a-pattern-based-and-tool-supported-risk-analysis-method-compliant-to-iso-27001-for-cloud-systems/123453

Bruderer, R., Villena, M., Tupia, M., & Bruzza, M. (2018). A cybersecurity model for mobile devices aimed at SMEs that use freelancers and BYOD schemes. 129–136. Retrieved from Scopus.

Chapman, D., & Smalov, L. (2004). On information security guidelines for small/medium enterprises. 3–9. Retrieved from Scopus.

Chiu, M., Lin, H. W., Nagalingam, S. V., & Lin, G. C. I. (2006). Inter-operabitity framework towards virtual integration of SMEs in the manufacturing industry. International Journal of Manufacturing Technology and Management, 9(3–4), 328–349. doi: 10.1504/IJMTM.2006.010061

Choez, C. G. P., & Llanos, F. D. C. (2018). Análisis de NIIF 9—Instrumentos Financieros desde una perspectiva industrial. Contabilidad y Negocios, 13(25), 6–19. doi: 10.18800/contabilidad.201801.001

Coles-Kemp, E., & Overill, R. (2007). The design of information security management systems for small-to-medium size enterprises. 47–54. Retrieved from Scopus.

Fagade, T. (2017). Hacking a Bridge: An Exploratory Study of Compliance-based Information Security Management in Banking Organization. 15(5), 7.

Firoiu, M., & Bacivarov, I. C. (2016). Physical and logical security risk assessment procedure for smes, according to ISO/IEC 27005:2011 and sr iso 31000:2010 standards. Quality - Access to Success, 17(152), 86–98. Retrieved from Scopus.

García-Porras, C., Huamani-Pastor, S., & Armas-Aguirre, J. (2018). Information Security Risk Management Model for Peruvian SMEs. 2018 IEEE Sciences and Humanities International Research Conference (SHIRCON), 1–5. doi: 10.1109/SHIRCON.2018.8592994

Gattiker, U. E. (2008). Early warning system for home users and small- And medium-sized enterprises: Eight lessons learned. International Journal of System of Systems Engineering, 1(1–2), 149–170. doi: 10.1504/IJSSE.2008.018136

Gillies, A. (2011). Improving the quality of information security management systems with ISO27000. The TQM Journal, 23(4), 367–376. doi: 10.1108/17542731111139455

Koumpouros, Y., & Georgoulas, A. (2019). A systematic review of mHealth funded R&D activities in EU: Trends, technologies and obstacles. Informatics for Health and Social Care, 45(2), 168–187. doi: 10.1080/17538157.2019.1656208

Lyubimov, A., Cheremushkin, D., Andreeva, N., & Shustikov, S. (2011). Information security integral engineering technique and its application in ISMS design. 585–590. doi: 10.1109/ARES.2011.121

Mangin, O., Barafort, B., Heymans, P., & Dubois, E. (2012). Designing a process reference model for information security management systems. Communications in Computer and Information Science, 290 CCIS, 129–140. doi: 10.1007/978-3-642-30439-2_12

Medve, A. (2012). Model-based framework for integrated evolution of business and IT changes: Integrated evolution of business and IT changes. 255–260. Retrieved from Scopus.

Mijnhardt, F., Baars, T., & Spruit, M. (2016). Organizational characteristics influencing sme information security maturity. Journal of Computer Information Systems, 56(2), 106–115. doi: 10.1080/08874417.2016.1117369

Muthaiyah, S., & Zaw, T. O. K. (2018). ISO/IEC 27001 implementation in SMEs: Investigation on management of information assets. Indian Journal of Public Health Research and Development, 9(12), 2631–2637. doi: 10.5958/0976-5506.2018.02112.5

Polverini, D., Ardente, F., Sanchez, I., Mathieux, F., Tecchio, P., & Beslay, L. (2018). Resource efficiency, privacy and security by design: A first experience on enterprise servers and data storage products triggered by a policy process. Computers & Security, 76, 295–310. doi: 10.1016/j.cose.2017.12.001

Ponsard, C., Grandclaudon, J., & Dallons, G. (2018). Towards a cyber security label for SMEs: A european perspective. 2018-January, 426–431. Retrieved from Scopus.

Ponsard, Christophe, & Grandclaudon, J. (2019). Survey and Guidelines for the Design and Deployment of a Cyber Security Label for SMEs. In P. Mori, S. Furnell, & O. Camp (Eds.), Information Systems Security and Privacy (pp. 240–260). doi: 10.1007/978-3-030-25109-3_13

Rizzo, C. (2010). ETSI security standardization. 3, 315–320. Retrieved from Scopus.

Rizzo, C. (2011). ETSI security standardization. 633–638. doi: 10.1109/ICRMS.2011.5979345

Sanchez, L. E., Villafranca, D., Fernandez-Medina, E., & Piattini, M. (2007). Developing a model and a tool to manage the information security in small and medium enterprises. 355–362. Retrieved from Scopus.

Sánchez, L. E., Villafranca, D., Fernández-Medina, E., & Piattini, M. (2008). Practical application of a security management maturity model for SMES based on predefined schemas. 391–398. Retrieved from Scopus.

Shojaie, B., Federrath, H., & Saberi, I. (2015). The Effects of Cultural Dimensions on the Development of an ISMS Based on the ISO 27001. 2015 10th International Conference on Availability, Reliability and Security, 159–167. doi: 10.1109/ARES.2015.25

Valdevit, T., & Mayer, N. (2010). A gap analysis tool for SMES targeting ISO/IEC 27001 compliance. 3 ISAS, 413–416. Retrieved from Scopus.

Van Akkeren, J., & Harker, D. (2003). The mobile Internet and small business: An exploratory study of needs, uses and adoption with full-adopters of technology. Journal of Research and Practice in Information Technology, 35(3), 205–219. Retrieved from http://www.jrpit.acs.org.au/jrpit/JRPITVolumes/JRPIT35/JRPIT35.3.205.pdf

- The list of non-relevant unique publications (17 in total) resulting from the search string S4 (Table 2):

6th International Conference on Software Process Improvement, CIMPS 2017. (2018). Advances in Intelligent Systems and Computing, 688, 1–304. Retrieved from Scopus.

20th Americas Conference on Information Systems, AMCIS 2014. (2014). Presented at the 20th Americas Conference on Information Systems, AMCIS 2014. Retrieved from Scopus.

Bozanic, Z., Dirsmith, M. W., & Huddart, S. (2012). The social constitution of regulation: The endogenization of insider trading laws. Accounting, Organizations and Society, 37(7), 461–481. Retrieved from https://ideas.repec.org/a/eee/aosoci/v37y2012i7p461-481.html

EmergiTech (Conference), University of Technology, M., & Institute of Electrical and Electronics Engineers. (2016). 2016 IEEE International Conference on Emerging Technologies and Innovative Business Practices for the Transformation of Societies (EmergiTech): Date, 3-6 Aug. 2016. Retrieved from https://ieeexplore.ieee.org/servlet/opac?punumber=7728913

Flores, Y., Shah, K., Lazcano, E., Hernández, M., Bishai, D., Ferris, D. G., … Morelos HPV Study Collaborators. (2002). Design and methods of the evaluation of an HPV-based cervical cancer screening strategy in Mexico: The Morelos HPV Study. Salud Publica De Mexico, 44(4), 335–344. doi: 10.1590/s0036-36342002000400007

Gervasi, O., Murgante, B., Misra, S., Borruso, G., Torre, C. M., Rocha, A. M. A. C., … Cuzzocrea, A. (2017). Computational Science and Its Applications – ICCSA 2017: 17th International Conference, Trieste, Italy, July 3-6, 2017, Proceedings. Springer.

Hallová, M., Polakovič, P., Šilerová, E., & Slováková, I. (2019, March 31). Data Protection and Security in SMEs under Enterprise Infrastructure. Retrieved March 13, 2020, from AGRIS on-line Papers in Economics and Informatics website: https://ageconsearch.umn.edu/record/294142

Hölbl, M., & Welzer, T. (2009). Two improved two-party identity-based authenticated key agreement protocols. Computer Standards & Interfaces, 31(6), 1056–1060. doi: 10.1016/j.csi.2008.09.024

Li, L., Xia, Z., Hadid, A., Jiang, X., Zhang, H., & Feng, X. (2019). Replayed Video Attack Detection Based on Motion Blur Analysis. IEEE Transactions on Information Forensics and Security, 14(9), 2246–2261. doi: 10.1109/TIFS.2019.2895212

Oreshkov, V. V., Energy, L. T., Nikolaychuk, A. V., Shevchenko, A. P., Salishchev, A. D., Gnuskov, M. V., … Region, J. T. V. (2018). Forecast for development of methods and means of Russian energy systems management. doi: 10.28999/2541-9595-2018-8-4-469-479

Ponsard, C., & Deprez, J.-C. (2018). Helping SMEs to better develop software: Experience report and challenges ahead. 213–214. doi: 10.1145/3183519.3183553

Proceedings of 12th Australian Information Security Management Conference, AISM 2014. (2014). Presented at the Proceedings of 12th Australian Information Security Management Conference, AISM 2014. Retrieved from Scopus.

Smentkowski, V. S., Ostrowski, S. G., & Keenan, M. R. (2009). A comparison of multivariate statistical analysis protocols for ToF-SIMS spectral images. Surface and Interface Analysis, 41(2), 88–96. doi: 10.1002/sia.2973

Success of a Cervical Cancer Screening Program: Trends in Incidence in Songkhla, Southern Thailand, 1989-2010, and Prediction of Future Incidences to 2030. (2014). Asian Pacific Journal of Cancer Prevention, 15(22), 10003–10008. Retrieved from http://journal.waocp.org/article_30215.html

Thapa, R. B., Matin, M. A., & Bajracharya, B. (2019). Capacity Building Approach and Application: Utilization of Earth Observation Data and Geospatial Information Technology in the Hindu Kush Himalaya. Frontiers in Environmental Science, 7. doi: 10.3389/fenvs.2019.00165

Wang, Y., Hassebrook, L. G., & Lau, D. L. (2010). Data Acquisition and Processing of 3-D Fingerprints. IEEE Transactions on Information Forensics and Security, 5(4), 750–760. doi: 10.1109/TIFS.2010.2062177

Yu, Y., Klauser, F., & Chan, G. (2009). Governing Security at the 2008 Beijing Olympics. The International Journal of the History of Sport, 26(3), 390–405. doi: 10.1080/09523360802602265

Bilge Yigit Ozkan received her MSc from Middle East Technical University in 2010. She had worked in the industry between 1996 and 2016. She had experience in diverse fields of information and computer science—information security, process improvement, technology management, etc.—during her employment. Her research focuses on cybersecurity standards and maturity models. She is currently employed as a PhD candidate at Utrecht University.

Marco Spruit is an associate professor in the Natural Language Processing group within the Information and Computing Sciences department of the Faculty of Science at Utrecht University in the Netherlands. As principle investigator in the department's Applied Data Science Lab, his research primarily focuses on Self-Service Data Science.