European DIGITAL SME Alliance

The EU Cybersecurity Act and the role of standards for SMEs

Position paper

Brussels, 14 January 2020

Introduction: The EU Cybersecurity Act at a glance

Small and medium-sized companies play an important role in providing cybersecurity solutions. A recent position paper by the European Cyber Security Organisation (ECSO) estimates that 60,000 companies—98% of which are SMEs and start-ups—are active in the EU cybersecurity market.[1] Their strength lies especially in niche markets and in disrupting markets with innovative business models. However, due to fragmentation, SMEs are often unable to scale up their operations.[2][3] Currently, companies in the Information and Communications Technology (ICT) sector need to undergo different certification processes to sell their products and services throughout the EU. Against this backdrop, the European Commission has initiated a framework for cybersecurity certification.[4]

[1] ECSO (2017), Position paper: Initial position on the EU cybersecurity package. Report prepared for the European Commission. Published October. Available at: http://www.ecs-org.eu/documents/uploads/ecso-position-paper-on-cybersecurity-package.pdf

[2] European Commission (2016), Commission signs agreement with industry on cybersecurity and steps up efforts to tackle cyber-threats. Published July. Available at: http://europa.eu/rapid/press-release_IP-16-2321_en.htm

[3] European Commission (2015), Cybersecurity industry. Published December. Available at: https://ec.europa.eu/digital-single-market/en/cybersecurity-industry

[4] European Commisison, (2017), The EU cybersecurity certification framework. Published September. Available at: https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-certification-framework

+32 2893 0235
VAT: BE0899786252
https://digitalsme.eu
office@digitalsme.eu
123 Rue du Commerce, 1000 Brussels, Belgium
EU Transparency Register: 082698126468-52

The EU Cybersecurity Act can be considered a major step forward towards the creation of a single European market for cybersecurity products and services. For the first time, it introduces a comprehensive, EU-wide framework for the certification of ICT products, services and processes. Despite being voluntary, the schemes could harmonise cybersecurity certification throughout the EU and thus eradicate existing barriers that prevent SMEs from scaling up and doing business across borders. Further, the certificates will allow customers to better understand the security features of a product or service they want to purchase, therefore contributing to greater market transparency. Each certification scheme will specify the categories of ICT products, services and processes covered, and set tailored cybersecurity requirements.[5] The requirements will likely be defined in reference to standards or technical specifications. Finally, a respective scheme will outline the type of evaluation of a product, service or process (e.g. self-assessment or third-party evaluation) and the intended level of assurance. For example, a high assurance level means that the certified product has passed the most stringent security tests.

In this position paper we examine the intersection between standards and certification schemes from the perspective of small and medium-sized enterprises (SMEs). As standards and technical specifications will likely play an important role in defining the cybersecurity requirements in the schemes, it is important to examine whether the

[5] How will the schemes be put in place and how does the Commission ensure that all relevant stakeholders are consulted? As a general mechanism, the European Commission or the European Cybersecurity Certification Group (composed by Member States) will propose the certification of a certain group of ICT products, services and processes to the European Union Agency for Cybersecurity (ENISA). ENISA will then produce a certification scheme in consultation with relevant stakeholders that will then be adopted by the Commission through implementing acts. At the same time, the Commission will prepare the 'Union rolling work programme for European Cybersecurity Certification'. The work programme defines certification priorities and is developed by the European Commission in consultation with stakeholders, e.g. members of the European Cybersecurity and Certification Group (ECCG) and ad-hoc working groups.

current standardisation frameworks and the available standards in cybersecurity are fit for SMEs.

What is at stake for Europe and small companies?

Today, SMEs are increasingly relying on networks and information systems for their business. Some of them offer digital services and their business model heavily depends on digital technologies.[6] At the same time, because of limited resources, it is harder for SMEs to recover from damages caused by a cyber-attack than for large businesses: 60% of SMEs that were victims of cyberattacks did not recover and had to shut down within six months.[7] Cybersecurity is therefore of crucial importance for the business continuity of an SME. However, this importance will only increase when industrial processes start moving online.

In the digital age, the security of complex manufacturing processes and industrial supply chains will not only depend on high cybersecurity standards in tier-1 suppliers or Original Equipment Manufacturers (OEMs), but also on the level of cybersecurity assurance in companies along the supply-chain pyramid (i.e. tier-2 or tier-3 suppliers). In many industrial processes, those tier-2 or tier-3 suppliers rely on machines that work with old operating systems. Therefore, there may be risks along the supply chain which are exacerbated when industrial processes become digital.[8] Going **digital is a major game-changer for industrial**

[6] Mazzarol, T. (2015), SMEs engagement with e-commerce, e-business and e-marketing, Small Enterprise Research, 22:1, 79-90. https://doi.org/10.1080/13215906.2015.1018400 & Enisa (2016), Information security and privacy standards for SMEs. Published June. Available at: https://www.enisa.europa.eu/publications/standardisation-for-smes

[7] SMESEC (n.d.), A lightweight cybersecurity framework for thorough protection. Available at: https://smesec.eu/index.html

[8] Iñaki Eguía Elejabarrieta, Standardisation and Certification: Insider's perspective and Industrial SME view, 23 October 2019, Brussels. Available at: https://www.digitalsme.eu/digital/uploads/I%C3%B1aki-Eguia-SME-entrepreneur-and-cybersecurity-expert.pdf

George Sharkov, Cyber Security Standardization & SMEs (Insider view), 23 October 2019. Available at: https://www.digitalsme.eu/digital/uploads/George-Sharkov-SBS-expert-at-ETSI.pdf

processes and moves the vulnerability from the physical to the cyber space. SMEs up and down the supply (or value) chain need to be taken into consideration when proposing measures aimed at increasing the level of cybersecurity assurance. SMEs might be an even easier target than large companies, since, due to a perceived lack of security, cyber criminals are increasingly looking towards them as a gateway into the supply chain.[9]

In a 2016 study,[10] European Union Agency for Cybersecurity (ENISA) concludes that despite rising concerns about information security risks, the level of SMEs' information security and privacy standard adoption in Europe is relatively low. Equally, their uptake is not largely perceived as a priority. **A lack of adoption of security solutions** is a real risk, which becomes evident when considering the very low adoption rate of some current product certification schemes: e.g. Common Criteria[11] apply to about 1,400 products worldwide. For comparison, 32,000 ISO/IEC 27001 certificates have been issued worldwide. These numbers are only a drop in the ocean compared to the approximately 190 million companies operating globally. This shows that the lack of adoption of cybersecurity standards in the market is a real problem. The lack may be due to the **high complexity and lack of adaptation of these standards** to the needs of smaller companies. Also, many SMEs are often **not aware of the importance of cybersecurity**. Therefore, most of the time, certification schemes are only

[9] Fresh Business Thinking (2016), Cybersecurity is a growing priority – don't be the weak link. Published May. Available at: http://www.freshbusinessthinking.com/cybersecurity-is-a-growing-priority-dont-be-the-weak-link/

[10] ENISA (2016). Information security and privacy standards for SMEs. Published June. Available at: https://www.enisa.europa.eu/publications/standardisation-for-smes

[11] Common Criteria (CC)—the popular reference name for "Common Criteria for Information Technology Security Evaluation"—is an internationally recognized set of guidelines (ISO 15408, supplemented by 18408), which define a common framework for evaluating security features and capabilities of Information Technology security products against functional and assurance requirements and certifying to the procurer that the process of specification, implementation and evaluation was conducted in a thorough and standardised manner. The international recognition of the certification is performed by the Arrangement on the Recognition of Common Criteria Certificates (CCRA).

used by industry, especially SMEs, when they **are a mandatory requirement to participate in procurement bids**.

At the same time, cybersecurity may sometimes support, but could also sometimes run counter to, other requirements, such as data protection or being user-friendly. Cybersecurity certifications could be disruptive as they will allow consumers with limited technical literacy to **make an informed choice about the security of a certain product, service or process**.[12] Potentially, certification could facilitate cybersecurity to a point where even untrained staff can make safe choices. At the same time, cybersecurity requirements could also lead to restrictions in the use of a device or product—or even lead to lock-down of certain ICT devices (e.g. wireless devices).

Further, new technologies are disrupting supply chains and industrial processes. For instance, artificial intelligence may in the future take autonomous decisions that can influence people's lives and wellbeing. 5G is another technology which will lift whole industrial protection chains into the digital environment—along with the substantial associated risks. The more a company becomes dependent on ICT and the more it embraces emerging technologies such as big data and IoT, the more crucial cybersecurity becomes.

Thus, the problem of cybersecurity is multifaceted, multi-layered and of a large magnitude, but solutions also need to be realistic. It is not possible to achieve full security. Proposed solutions need to be based on risk assessments, be practical and follow priorities. To sum up, in order to make the EU Cybersecurity Act and its certification schemes a success, we need to consider the following points to bridge the difficulties in achieving effective cybersecurity certification:

[12] Fabio Guasconi, Standardisation and Cybersecurity – An insiders' perspective, 23 October 2019. Available at: https://www.digitalsme.eu/digital/uploads/Fabio-Guasconi-SBS-expert-at-ISO.pdf

1) Cybersecurity standardisation and certification require a broad support by industry & society and a high level of adoption.

2) Decision-makers both in policy and business need to be aware that 100% cybersecurity is not achievable. The aim should be to reduce risks and build resilience through prevention and protection as well as through sharing information about threats and vulnerabilities.

3) Security measures may need to be balanced with usability or privacy concerns (e.g. compliance with GDPR or other confidentiality requirements).

4) Rapidly evolving new industry platforms (e.g. network functions virtualisation [NFV] and software defined networking [SDN]/5G, quantum computing, artificial intelligence/machine learning, etc.) need 'predictive' attention to avoid major risks for society.

How do we ensure that standards and certification are widely adopted? Much will depend on how the schemes will be designed and implemented. If certification schemes are too complex and their adoption too slow, the Cybersecurity Act could **run the risk of becoming yet another piece of legislation that SMEs are not even aware of and which they do not apply**. One way to address this issue is to propose easy-to-apply standards as part of the EU-wide certification schemes. However, some of the current standards are highly technical and do not provide practical solutions to SMEs. Therefore, **there is a need to think about SME-friendly standards and solutions within the framework of the EU Cybersecurity Act. Secondly, the category of 'small and medium-sized enterprises' is not homogenous, and to be effective, we believe that there needs to be a stronger analysis of the needs of different types of SMEs.**

Which solutions for which SME?

We believe that the adaptation of measures to **different types of SMEs** is key to bridge the difficulties in achieving effective cybersecurity certification. Differentiation and adaptation

to different types of SMEs is pivotal if we want to develop cybersecurity standards and define requirements that actually fit the needs of the market and are therefore more efficient in achieving the goal of increasing cybersecurity among businesses. There is a need for **greater distinction between different types of SMEs and their role in the digital ecosystem in order to make sure that solutions are tailored to them**. Therefore, we propose to distinguish between the following categories:

- **'digital enablers':** Throughout the European Union, a significant number of SMEs are involved in developing and providing digital hardware, software and services—these companies are the 'digital enablers'. In the cybersecurity industry, 'digital enablers' form the supply side, as they are active in developing and providing cybersecurity solutions.[13]
- **'digitally based' SMEs:** This second category are 'digitally based' businesses which are connected to the first category via clusters and value chains or outsourcing (including cloud-based services). These businesses do not have digital or cyber as

[13] According to a report prepared by ECSO, the European industry can be divided into three parts: high grade, low grade and mid-grade cybersecurity. "**High grade** refers to a niche market for companies originating from the defence sector. Given restrictions on public procurement, a protected and high-level European offer has been developed. The **low-grade** cybersecurity market is largely dependent on non-European companies. As the offer for the general public, Business-to-Consumer (B2C), is mainly based outside Europe, new European companies entering the market are often acquired by non-European actors. Players such as Microsoft, IBM, CISCO, Symantec are dominating this market, often offering end-to-end solutions combining the implementation of network protection strategies with governance solutions and identity access management services. The **mid-grade** European cybersecurity market refers to the protection of critical infrastructures and public authorities is quite dispersed, and SMEs play an important role here. The large majority of the thousands of European companies active in this area are SMEs having a turnover under 5 million EUR and less than 50 persons. They are highly specialised in one area and do not offer the whole range of cybersecurity solutions. These SMEs operate in specific niches in domestic markets, with low levels of internationalisation." See: ECSO (2016), European cybersecurity industry proposal for a contractual public-private partnership. Published June. Available at: http://ecs-org.eu/documents/ecs-cppp-industry-proposal.pdf

their core, but highly depend on digital solutions for their business model and main business functions. They need to be aware of compliance or cybersecurity requirements in order to be able to request them from their providers. In the cybersecurity industry, these are companies that use cybersecurity solutions to ensure continuity of their business operations (demand side).[14]

- **'digitally dependent' SMEs**: The third category of SMEs is perhaps the largest. This is the type of 'digitally dependent' or 'end user' SMEs, that use regular ICT for running their businesses. In the context of the digital economy, 'digital dependency' is rapidly increasing. This group is perhaps the one that is most in need of easily understandable & practical solutions.
- **'start-ups'**: Finally, the category of **start-ups** is a sub-group of the first or second category. Being busy with the functional development of their business models, they typically neglect (or are not aware of) requirements such as 'security by design' or 'resilience by design', which can be implemented both via technical solutions and the business processes. Under the pressure of competition and expectations to quickly scale up, security has a low priority. This category of enterprises requires specific measures and incentives to adopt security standards. They should be in the focus of governmental bodies and programs. Also, cybersecurity should be strongly

[14] "The industry in which an SME is active and the size of an SME influence their likelihood of protecting themselves against cybercriminals. Firstly, the industries, best protecting themselves against digital fraud in terms of measures taken, are: ICT and media, the industry, finance, and the professional services sector. The agricultural sector and the construction industry are the least protected sectors. Secondly, micro-enterprises (up to 10 employees) are less likely than larger SMEs (10-250 employees) to implement security measures, underlining again the factor company size." See: Interim Report on Supporting specialised skills development: Big Data, Internet of Things and Cybersecurity for SMEs, EASME/COSME/2017/007, March 2019. Available at: https://www.digitalsme.eu/digital/uploads/March-2019_Skills-for-SMEs_Interim_Report_final-version.pdf.

encouraged (even requested) by investors (so they too must be well-aware and understand the need of security compliances as digital market differentiator).

To summarise: **Differentiation is needed to tailor standards and certification schemes to different types of SMEs**. A highly specialised 'digital enabler' that provides IT security solutions will be more fit to adopt a complex IT-security standard and should assist 'digitally based' companies in doing so. 'End user' SMEs on the other hand may require secure-by-design solutions and a set of basic standards with relevant certifications they can follow to make sure they meet a basic level of cybersecurity hygiene.

Standardisation: What are the hurdles for SMEs?

Currently, the coverage of standards in cybersecurity is wide and extends to all relevant aspects of cybersecurity risks. However, while the scope of standards is broad and relevant, adoption of standards is lacking. Obstacles to **adoption of standards** relate mainly to problems of **affordability**, **adaptation to SME needs**, **awareness** and **access**.

Below, we outline the four 'A'-challenges to standards-adoption for SMEs.[15] For the analysis of the hurdles, we relied on an ENISA report of 2015.[16]

1) **Affordability: Standards are not freely available & implementation is expensive.**
   - **Free access to standards:** Standards are often only available in a paid-for version. Only few standards or specifications (i.e. those developed by ETSI or by other international standards consortia) are freely available online, well-

[15] George Sharkov, Cyber Security Standardization & SMEs (Insider view), 23 October 2019. Available at: https://www.digitalsme.eu/digital/uploads/George-Sharkov-SBS-expert-at-ETSI.pdf
Fabio Guasconi, Standardisation and Cybersecurity – An insiders' perspective, 23 October 2019. Available at: https://www.digitalsme.eu/digital/uploads/Fabio-Guasconi-SBS-expert-at-ISO.pdf

[16] ENISA (2015), Information security and privacy standards for SMEs. Recommendations to improve the adoption of information security and privacy standards in small and medium enterprises. Available at: https://www.enisa.europa.eu/publications/standardisation-for-smes/at_download/fullReport

maintained and updated. However, SMEs need access to a standard to effectively evaluate its usefulness for their business. Secondly, as a substantial part of supply/value chains, SMEs must comply with several generic and specific standards - which puts additional costs on them and may lead to a difficult situation if standards are not tailored to small companies.

- **Implementation costs of standards**: The costs of implementing standards are too high for many SMEs. Taking up a standard and applying it inside a business can be demanding in terms of financial resources, especially since SMEs often only have limited staff to take care of IT.

2) **Adaptation: Standards are not tailored to SMEs & there are no easy technical solutions or guides for implementation.**
   - **Tailoring/adapting standards**: Some standards are not very practical nor useful, nor easy to apply for SMEs. There are limited European or international standards designed for SMEs.
   - **Localisation**: (language translation and adaptation) is rare for specific technical standards.
   - **Explaining standards:** There is a lack of simple or easy cybersecurity solutions or guides. The development of more straightforward guides would also contribute to the internal capacity to apply standards.
   - **Lack of technical solutions**: There are no easy technical solutions supporting the application of standards.

3) **Awareness & internal organisational capability**
   - **Awareness about existence of standards:** Oftentimes, awareness of the existence of standards in certain areas is low.
   - **Business case**: The awareness of how standards add business value is limited.

- **Misconceptions:** There are misconceptions about the complexity of standards and unfair market regulations.
- **Internal capability and capacity**: The level of knowledge and expertise on how to apply standards to products, services or processes of smaller companies needs to be increased. Standards are often hard to understand for SMEs which do not have the inhouse expertise for translating standards into specific tasks and activities. Especially when there is a lack of clear implementation guidelines.
- **Lacking capability**: SMEs that have outsourced the ICT function may suffer from limited internal knowledge about cyber threats.

4) **Access to & participation in standardisation organisations:**
   - **Lack of resources:** SMEs do not have the resources to partake in the standardisation processes to the extent that large companies do, causing them to be severely underrepresented in standardisation bodies.
   - **Participation and influence**: Thus, the design of standards is mainly driven by large companies, which have different requirements. Participation in standardisation processes needs to be increased.

In summary, standards can be beneficial to SMEs, but only if they are easily accessible and reduce complexity to a level that is suitable to SMEs. Therefore, DIGITAL SME would like to propose a standardisation scheme that is more accessible, affordable and adapted to SMEs. As standards and technical specifications will likely play an important role in defining the cybersecurity requirements in the schemes, it is important to analyse the key hurdles for the adoption of standards by SMEs and to draw conclusions on how to overcome these hurdles.

Our recommendations: Options for standardisation bodies to adapt standards to the needs of SMEs

Together with standardisation organisations, the relevant policymakers should set the framework to **converge towards a useful, interoperable set of standards**. DIGITAL SME advocates for frameworks that put the real focus on SMEs. Are SMEs 'just mentioned' in pieces of legislation or does legislation propose concrete measures and actions to make sure SMEs are involved in the process?[17]

After having analysed the hurdles for SMEs when it comes to the standardisation system, and having categorised SMEs according to their digital maturity, DIGITAL SME would like to propose four options that could help to better adapt standards to the needs of SMEs in the short to medium-term. These options serve as recommendations to policymakers going forward, and they will have to be evaluated and combined into an overarching strategy to facilitate the adoption of standards by SMEs. The long-term goal is to increase the overall level of cybersecurity assurance.

- **Option 1**: *Further the evolution of existing standards*. The proposed way forward under this option is for standardisation bodies to develop existing standards further by including different maturity levels that match the different categories of SMEs outlined above. This would require revisiting relevant standards and amending them to allow for a greater distinction according to the actual user of the standard.
- **Option 2**: *Develop lightweight standards or guides*. Lightweight standards/requirements/recommendations are the most straightforward response to the issues. Standardisation organisations could collaborate with small-business organisations to develop 'lightweight' versions of standards for SMEs. This would firstly involve a mapping of all relevant standards, the identification of the most

[17] In order to develop such a framework, it would be helpful to assess SMEs' feedback on the implementation of 'cyber hygiene' requirements from the Directive on security of network and information systems (the 'NIS Directive'). Further, we recommend advising the standardisation bodies such as the European Telecommunications Standards Institute (ETSI) and the European Committee for Standardisation (CEN) to enrich their composition and encourage SME involvement.

'practical' ones, ideally measured by their level of adoption and usage in the business environment, and then pooling efforts into developing practical guides or standards, as has been done by DIGITAL SME on behalf of SBS in the case of the practical Guide for SMEs on ISO/IEC 27001.

- **Option 3**: *Develop new standards specifically for SMEs*. This line of action would advocate for the development of new standards building on the specific requirements of and specifically targeted at SMEs (of the different categories, as described above).
- **Option 4**: *Combine different standards into packages tailored to SMEs*. Combining standards ('packaging') would mean defining typical (perhaps sector-specific) profiles and roles (throughout the supply/value chains) rather than going in the direction of multiple new specific standards. Standardisation bodies could then outline integrated sets of harmonised standards and compliances (including lightweight versions, possibly with several options) that are easier to understand and implement. E.g. for IoT, one could develop a 'general security package' which ensures security from consumer to provider, covering devices, communications (and encryption) and services (cloud based).

As a next step, we will formulate which of these options is most suitable per different type of SME. E.g. Option 1 would allow differentiation along all SME categories. Option 2 would rather be suitable to 'end user' SMEs or 'digitally based' SMEs. Developing specific targeted actions along the options mentioned below will require further analysis.

To bridge the hurdles identified above in points 2) adaptation an 3) awareness, DIGITAL SME believes that it would be beneficial to create a 'one-stop-shop' in form of an online platform where SMEs can access simple guides and solutions tailored to their level of expertise and maturity. For instance, a company would be able to freely access a guide with 7-10 simple steps and instructions about essential cybersecurity hygiene, e.g. related to backups, network security, Windows-Updates, etc. Those guides need to be easily understandable for non-technical people when addressing 'end user' SMEs. However, the platform should

also include specific guides for different roles and more advanced levels of expertise, some of them building on available standards.

Conclusion

In this position paper we examined the intersection between standards and certification schemes from the perspective of small and medium-sized enterprises (SMEs). Cybersecurity certifications could be disruptive as they will allow consumers with limited technical literacy to **make an informed choice about the security of a certain product, service or process**. Potentially, certification could facilitate cybersecurity to a point where even untrained staff can make safe choices. As standards and technical specifications will likely play an important role in defining the cybersecurity requirements in the schemes, it is important to examine whether the current standardisation frameworks and the available standards in cybersecurity are fit for SMEs. However, much will depend on how the schemes will be designed and implemented. **There is a need to think about SME-friendly standards and solutions within the framework of the EU Cybersecurity Act.** If certification schemes are too complex and their adoption too slow, the Cybersecurity Act could run the risk of becoming yet another piece of legislation that SMEs are not even aware of and which they do not use. **Therefore, DIGITAL SME would like to propose a standardisation scheme that is more accessible, affordable and adapted to SMEs.**

However, SMEs are not a homogeneous group. Thus, **differentiation is needed to tailor standards and certification schemes to different types of SMEs**. A highly specialised 'digital enabler' that provides IT security solutions will be more fit to adopt a complex IT-security standard and should assist 'digitally based' companies in doing so. 'End user' SMEs on the other hand may require secure-by-design solutions and a set of basic standards with relevant certifications they can follow to make sure they meet a basic level of cybersecurity hygiene.

Building on this analysis, **DIGITAL SME proposes four options for the further development of standards, that could help to better adapt standards to the needs of SMEs in the short to medium-term.** These options serve as recommendations to policymakers going forward, and they will have to be evaluated and combined into an overarching strategy to facilitate the adoption of standards by SMEs. **Further, DIGITAL SME proposes a simple platform which would be a 'one-stop-shop' for practical guides on cybersecurity for SMEs. The long-term goal is to increase the overall level of cybersecurity assurance among companies in Europe, and a mix of both raising awareness and providing practical solutions is needed to achieve it.**

Main References:

Iñaki Eguía Elejabarrieta, Standardisation and Certification: Insider's perspective and Industrial SME view, 23 October 2019, available at: https://www.digitalsme.eu/digital/uploads/I%C3%B1aki-Eguia-SME-entrepreneur-and-cybersecurity-expert.pdf

George Sharkov, Cyber Security Standardization & SMEs (Insider view), 23 October 2019, available at: https://www.digitalsme.eu/digital/uploads/George-Sharkov-SBS-expert-at-ETSI.pdf

Fabio Guasconi, Standardisation and Cybersecurity – An insiders' perspective, 23 October 2019, available at: https://www.digitalsme.eu/digital/uploads/Fabio-Guasconi-SBS-expert-at-ISO.pdf

For further information on this position paper, please contact:

Ms. Annika Linck, EU Policy Manager

E-Mail: a.linck@digitalsme.eu