European
DIGITAL SME
Alliance

31 July 2017

Position Paper on

European Cybersecurity Strategy: Fostering the SME ecosystem

-

In 2013, the European Commission and the European External Action Service launched the EU Cybersecurity Strategy. Since then, cybersecurity has been one of the central topics in numerous other EU strategies, initiatives (such as Digital Single Market strategy and European Agenda on Security). However, due to the growing number of recent cybersecurity threats, as well as opportunities that it has to offer – the European Commission is about to review the EU Cybersecurity Strategy and the mandate of the European Union Agency for Network and Information Security (ENISA) in order to align it to the new EU-wide framework on cybersecurity. Commission's review is due to September, 2017.

Therefore, European DIGITAL SME Alliance, in collaboration with the European Cyber Security Organisation (ECSO)[1] has developed its Position Paper on European Cybersecurity. This paper is intended to contribute to the Commission's review – we call the European Commission to include our suggestions listed below in this paper to the EU Cybersecurity Strategy review.

It is our strong belief that European SMEs play an important role in the European cybersecurity ecosystem. This role is rather two-fold. First, cybersecurity technology is changing rapidly and only the SMEs, due to their agility, can provide the cutting-edge solutions needed to remain competitive. On the other hand, SMEs make up 99.8% of European enterprises but they are unprepared for cyberattacks. Decision makers working in these enterprises still often underestimate the threat posed by cybercrime. Moreover, the lack of competitive solutions tailored to the needs of SMEs is an important barrier to build an efficient and global security policy, and making SMEs the weak link in cyber-attacks.

This position paper provides an overview of measures that, if adopted and well implemented, would facilitate SMEs' cybersecurity ecosystem, and contribute to the

[1] This paper is mostly based on ideas and proposals from the ECSO Position Paper "Why SMEs and territorial cooperation matter for cybersecurity". DIGITAL SME largely contributed to the development of the ECSO position paper and provided the chairmanship to the relevant working group of ECSO, WG4 on SMEs, Regions and East EU countries.

effective functioning of overall European cybersecurity.

Boosting offer and demand for SME solutions

Without a structured demand, SMEs and start-ups cannot grow at rapid pace. Here, the need is for more clarity on client demand in order to better address the market (specific business plan, prioritization). On the other side, operators and end-users still lack a business model based on "return on security investments versus risks": this concern is shared also with large security providers. Thus, we suggest the following elements for boosting offer and demand:

I. European Cybersecurity SMEs HUB

Government procurement as well as large private tenders are an opportunity for European SME providers. However, SMEs rarely meet the requirements to respond to such tenders. This is because large public and private tenders typically call for a complex package of services that singles SMEs cannot provide. While SMEs' agility and flexibility allow them to offer innovative and potentially disruptive solutions in specific technologies, they normally do not specialize in other required domains, and therefore are unable to respond to a larger tender by their own.

In this context, we call for the establishment of European cybersecurity SMEs HUB. This Hub would, first of all, connect small and medium sized digital companies and foster their ad hoc cooperation on specific projects. The Hub would facilitate the establishment of new consortia or d hoc new companies as consolidation of several SMEs. It would allow SMEs to put knowledge, skills and resources together. The Hub would provide a plug-and-play kit of contractual solutions, based on which flexible consortia could emerge quickly.

Thus, the so-called 'virtual factories' would be created, significantly reducing transaction costs necessary to negotiate and agree contractual conditions among several SMEs. These services provided by the Hub would allow SMEs to take part in wider bids- both for public procurement and private, thus compete with multinational companies.

The Hub would also offer to SMEs, as well as to their associations and chambers of commerce, a competence center on domains such as governance, traceability and audit, identity access management, data security and cryptography, DRM messaging security, application security, security of infrastructure and equipment, HSM industrial network security; audit, consulting and training; operational and outsourcing services, etc

II. Make EU solutions more visible to public procurers

As it is explained above, currently SMEs are mostly incapable of participating in public tenders. In addition to that, multinational companies tend to outsource SMEs in the third countries, due to their lower costs. In order to create more favorable conditions for European SMEs, public tenders should require transparency of value chain and prefer European suppliers. That is, all the tender participants should be obliged to demonstrate where and from which companies they are buying the services. Meanwhile, the public procurers should give their preference to those tenders that use solely European products/services.

In this view, the "Made in the EU/EU SME's trusted solution" label is an option to be investigated to facilitate private procurements oriented towards European SMEs. This label could be a main differentiator stressing European qualities like data protection and high security standards. It should be seen more as a marketing tool to promote the European cybersecurity offerings on export market by increasing the visibility of SMEs.

For a creation of the label, we suggest to first of all map the existing mechanism and investigate the schema/requirement to deliver such label (i.e. in France with www.francecybersecurity.fr and in Germany " IT Security made in Germany" or "Software Made in Germany"). In addition, we suggest drafting a catalogue of EU companies specialized in cybersecurity: including the firewall solutions, companies specialized in penetration tests and other segments in accordance with the market study.

III. Development of territorial cooperation strategy

SMEs structured in clusters and/or specialised in the same sector (e.g. the energy) could share some costs on cybersecurity (e.g. training, alerting notices) and funding tailored solution (e.g. detection sensors for industrial systems) adequate to their needs and budgets. Therefore, we see the development of territorial cooperation strategy as one of the crucial elements to help SMEs having access to cybersecurity protection measures.

EU Funding for Research, Innovation and Development of Solutions that Effectively Reach the Market

There are many initiatives at EU level to support SMEs when dealing with investment issues. However, from an operational point of view, SMEs are not taking advantage of the existing funding as they are unable to handle the administrative burden of the collaboration and funding-related reporting. Therefore, we suggest developing the following actions:

I. Request of minimum participation of SMEs in Horizon 2020 projects

We argue that at least 20% of the participants of the Horizon 2020 (H2020) calls to be funded should be SMEs, start-ups or high growth companies (50+% increase in annual revenue). The requirement of 20% is also adopted as a Key Performance Indicator for the cPPP monitoring that will be prepared by ECSO on yearly basis.

II. Adoption of cascading funding mechanisms in H2020 calls on cybersecurity

European cybersecurity SMEs express an important need for increasing the number of H2020 topics that include cascade funding. It is foreseen that a cascade funding model is going to be present in almost all the other areas of the LEIT ICT Working Programme for 2018-2020. However, it is not present in cybersecurity domain. We claim that this is a big mistake as it has proven to be a very efficient mechanism for supporting companies in the adoption of new technologies. Moreover, consortium building funds should be available not only in reimbursement format but as a direct financing tool (e.g. Katana projects). Therefore, we call for the cascading funding mechanism for H2020 calls on cybersecurity.

III. Review and simplification of the SME Instrument

Due to the high level of complexity for applying and administrative burdens for SMEs, the current amount of money and the timeline are inadequate for SMEs looking to quickly go to the market. Instead of providing 1.5M€ funding, we suggest having many small projects of 50K€ to 500K€ funding at the early phases.

IV. Designing an EU model for investment

EU cybersecurity startups and SMEs face funding problems and have great difficulty in raising the necessary funds for their technological and commercial development. Several innovative companies were acquired by foreign companies, such as Stonesoft (FI) acquired by McAfee, Secusmart (DE) acquired by Blackberry or Anubis Networks (PT) bought by BitSight. In particular, SMEs need capital to be invested in marketing and business development but the EU market faces a lack of private capital risk/investors in cybersecurity domain. Therefore, we propose mapping the potential capital venture and funding investment in EU and creating a “Bid” and “Search” platform.

Marketing and Export Outside the EU (from Innovation to Market)

SMEs face limited export capability: many SMEs lack the knowledge of international markets they need to operate effectively overseas or even within the EU. Some companies have exported very successfully but even these companies would welcome better intelligence on countries, opportunities and competitor overseas. However, this information can be hard (or expensive) to acquire.

Meantime, particular niches in the domestic market are relatively small. SMEs do not have the resources to monitor the developments in their big competitors. One of the biggest problem SMEs have in their propositions is that they do not have sufficient competitive intelligence to understand where their product/service sits in the market. Moreover, SME often faces on the market competition against global giants. Finding customers and proposing SME solutions and innovation to customers outside Europe requires new type collaboration with local partners from the target market.

I. Establishment of European cybersecurity SMEs HUB supporting export campaigns

As for the internal EU market, we suggest the establishment of European cyber security SMEs HUB supporting export campaigns. This HUB should design partnerships delivering monthly Market Watching, newsletter on venture capital operations, US/ASIA industry moves in EU, and finally accelerate SMEs market presence outside the EU.

II. Analysis of SMEs export networks outside the EU

In order to support the link among SMEs outside of Europe, and thus get some important customer references outside the EU (e.g. Middle East, South Asia market), we propose carry out an analysis of SMEs export networks outside the EU with a key message for the “Made in the EU” cybersecurity industry. We also call on investigating the best practices and discuss the synergies with EEAS and DG Growth on export.

Cybersecurity solutions and certification for SME users and providers of critical services

Whereas certification is a key factor for IT security across value chains, the voluntary uptake of existing certification schemes among SMEs is insufficient. This is certainly due to cultural issues such as the lack of awareness among the smaller organisations. However, other important factors that undermine the uptake of existing certification schemes are their excessive cost and complexity. Both the financial and administrative burdens of certifications are not sufficiently proportional to the size of the companies and are, thus, perceived as excessive by SMEs.

European DIGITAL SME Alliance suggests the gradual approach on security requirements for SMEs and the proportionality criteria on verification. Given the small size and the reduced resources available for SMEs, we argue a baseline requirement level should be followed by all users and providers but based on a self-declaration schemes.

Our suggested key principles of certification for SMEs:

I. Proportionality of verification

(When required) third party verification has to follow a strict principle of proportionality. Complexity, time and cost have to be proportional to the size of the undertaking. What should count, it's not the size of the undertaking, but the size of the infrastructure/supply chain/etc. to be evaluated and the desired level of certification.

II. Reduced formalism

SMEs, especially micro-enterprises, are often organized with an informal management structure. In many cases, very small companies have little specialization of roles and functions ("everyone does everything") and the management functions are centered in one single person (e.g. the company owner). Therefore, process certifications or management system certifications should be adapted to the informal organizational set of smaller companies.

III. Need for implementation guides

Very often standards and certification schemes are written in abstract, high level language that requires companies to adapt in order suit internal needs and set up. SMEs often do not have the internal resources to understand abstract instructions and implement them in their reality. So, there is a need to develop implementation guides for SMEs providing concrete examples of use of the standards and practical instructions such as check-lists.

IV. Gradual approach and self-certification

Different requirement levels have to be foreseen, whereby companies can choose their level according to their needs. Third party certification should not be the only option available; instead the first level(s) should be restricted to self-certification scheme(s). In this regard, we should investigate the option of replacing (or integrating) third-party certification with peer to peer schemes.

V. Validity and re-certification

By the default option there should be no predetermined limit to validity duration of a certification. Limitations on the duration and/or periodic audits should be provided for only in very specific cases where there is an objective need. Re-certification or renewal, when necessary have to happen at no cost for the company, except for the auditing costs if required. The CEO of the company should sign the adoption of these limited and simple requirements. In this regard, this signature of CEO could be seen as the first level of assurance of solutions provided by the SMEs.

About the European DIGITAL SME Alliance

DIGITAL SME is the largest network ICT small and medium sized enterprises in Europe, representing about 20.000 digital SMEs across the EU. The alliance is the joint effort of 28 national and regional SME associations from EU member states and neighboring countries to put digital SME at the center of the EU agenda.

DIGITAL SME is an association formed in 2007 to express *the voice of ICT SMEs in Europe*. DIGITAL SME aims to ensure that ICT SMEs get *talked to* rather than just *talked about*. It provides a voice for digital SMEs in the policy and business arenas and is already represented in several EU expert groups and taskforces.

The European DIGITAL SME Alliance is a member of UEAPME the European Association of SMEs. The European DIGITAL SME Alliance is a founding member and co-financer of SMALL BUSINESS STANDARDS, the European Association that is mandated and co-financed by the European Commission in order to represent the interests of SMEs in standardisation according to Regulation 1025/2012. The European DIGITAL SME Alliance is a founding member of ECSO, the European Cyber Security Organisation.