SBS position on cybersecurity solutions and certification for SME users and providers of critical services

March 2018

➢ BACKGROUND

On 13 September 2017, the European Commission published a joint communication outlining their views to build a strong cybersecurity for the EU. The document underlines how the growth of the cybersecurity market in the EU – in terms of products, services and processes – is prevented by the lack of cybersecurity certification schemes recognised across the EU to build higher standards of resilience into products and to underpin EU-wide market confidence. For this reason, the European Commission is working on a proposal to set up an EU cybersecurity certification framework.

Whereas certification is a key factor for IT security across value chains, Small Business Standards (SBS) acknowledges that 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. Small businesses often perceive cyber security measures as too expensive to implement and/or admit their confusion regarding concrete implementation measures to take. There is a need to keep both the financial and administrative burdens to an acceptable level considering the size of the companies.

In order to overcome the issue, SBS 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 self-declaration schemes.

➢ Suggested key principles for certification of SMEs:

I. Proportionality of verification

Complexity, time and cost of certification have to be proportional to the level of security risk involved as well as to the size of the infrastructure/supply chain. The level of security risk being equal, third party verification of SMEs has to be proportional to the size of the undertaking.

II. Reduced formalism

SMEs, especially micro-enterprises, are often organised with an informal management structure. In many cases, very small companies have little specialisation of roles and functions ("everyone does everything") and the management functions are concentrated in one single person (e.g. the company owner). Therefore, process certifications or management system certifications should be adapted to the informal organisational 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 security levels have to be foreseen, whereby companies can choose the security level that better responds to their needs. Despite acknowledging the need for third party certification for companies providing critical services, the lower security level(s) (i.e. not those associated to the provision of critical services) should be restricted to self-certification scheme(s). In this regard, it should be investigated 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.

VI. Better use of existing standards for certification purposes

It is recommended to identify and possibly adopt European and international standards that are already available or under development which could be used for the development of certification schemes and increase trust in the EU Digital single market. Specific attention should be paid to the work of ISO and IEC which have already produced the ISO/IEC 27000 series of standards on information security and the IEC 62443 series of standards on how to implement electronically secure Industrial Automation and Control Systems. In addition to that, also the Mutual Recognition Agreement (MRA) certification schemes developed by the Senior Officers Group for Information Systems (SOG-IS) have already proven to be valid: they are already used in highly secured

environments and could constitute a valid solution for the further development of the European cybersecurity ecosystem, which mainly consists of SMEs.

VII. Need for sector-specific approaches

SBS welcomes the recommendation made by the EC in the joint communication about the need to develop sector-specific approaches for cybersecurity. The success of general cybersecurity strategies can be only achieved if these strategies are accompanied by complementary actions that consider the needs of specific sectors such as financial services, energy, transport, health, etc.