Governance framework for European standardisation

Aligning Policy, Industry and Research

V1.0

DECEMBER 2015

www.enisa.europa.eu European Union Agency For Network And Information Security

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Authors

This report has been written by an expert group formed by members of the ETSI/CEN/CENELEC Cybersecurity Coordination Group (CSCG) including ENISA. The main contributors include:

- Charles Brookson – Zeata Security Ltd
- Scott Cadzow
- Ralph Eckmaier
- Jörg Eschweiler
- Berthold Gerber
- Alessandro Guarino – UNI
- Kai Rannenberg – Goethe University Frankfurt, DIN
- Jon Shamah
- Sławomir Górniak – ENISA

Contact

For contacting the authors please use isdp@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu.

Acknowledgements

ENISA would like to thank the numerous experts from Standards Development Organisations, industry, foundations and others who reviewed this paper for their contributions.

ISBN 978-92-9204-154-0 DOI 10.2824/358519

Table of Contents

Executive Summary

In response to the European Union's Cybersecurity Strategy[1], the CSCG[2] has published a White Paper[3] with recommendations on digital security. The CSCG's recommendations underline the importance of Cybersecurity standardisation to complete the European internal market and to raise the level of Cybersecurity in Europe in general. CSCG Recommendation #1 proposes a review of the current governance framework. This document analyses the good practices within the governance framework of the European Union and proposes recommendations for stakeholders. It has been written by CSCG and ENISA experts as a response to the Recommendation #1 and forms a logical entity together with the response to the CSCG Recommendation #2, *Definition of Cybersecurity – Gaps and overlaps in standardisation*, published by ENISA at the same time.

Cybersecurity differs from other areas because the systems to which best practices (including formal guidelines and standards) are to be applied are by nature socio-technical systems, where people and technological elements are strictly intertwined. The social part of the systems comprises a plurality of actors and stakeholders. In technical domains primarily a restricted and controllable set of actors is to be found. All these different actors can have conflicting interests in protecting their security – the ongoing debate on the confidentiality of individual users of Cyberspace versus the necessities of national security is only the most striking example.

The role of standardisation and policy, in their interaction with Cyberspace and Cybersecurity is similarly complex and this is possibly best exemplified with regard to privacy legislation. From these considerations it follows that a purely technical, classical standardisation approach is likely to fail in such a domain as Cybersecurity. With people being part of the system to be secured, purely technical standards and guidelines have to be complemented by organisational, societal ones. In standardisation policy a multi-disciplinary approach would be very useful but it appears hard to achieve.

In order to avoid market fragmentation, limited take up of standards, and by consequence, failure to achieve a secure Cyberspace and the application of standardised measures for Cybersecurity, a coordinated approach is needed. The overall objective of this coordinated approach towards Cybersecurity standardisation should meet the following individual objectives, observed by all stakeholders involved:

- Cybersecurity standards should be developed through consensus among all stakeholders, including European Standardisation Organisations (ESOs), European institutions and industry;
- Cybersecurity standards should be approved under the auspices of a recognised body;
- The distribution of mandated work for the development of Cybersecurity standards should be coordinated by the recognised bodies;
- Recognised bodies should make their development work programme public and coordinate with other recognised bodies to eliminate duplication and possible overlaps.

[1] http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1667
[2] ETSI CEN CENELEC Cybersecurity Coordination Group, http://www.cencenelec.eu/standards/Sectors/DefenceSecurityPrivacy/Security/Pages/Cybersecurity.aspx
[3] Recommendations for a Strategy on European Cybersecurity Standardisation ftp://ftp.cencenelec.eu/EN/EuropeanStandardization/Sectors/DefenceSecurityPrivacy/Cybersecurity/CSCG_WhitePaper2014.pdf

Specific requirements concerning Cybersecurity standardisation outlined above, with their far-reaching consequences, call for new and more efficient modalities of interaction among the main actors – the European Standardisation Organisations, the European Commission, the industry – and other stakeholders.

1. Introduction

In the Cybersecurity strategy of the European Union, the EU reaffirms the importance of all stakeholders in the current Internet governance model and supports the multi-stakeholder governance approach. Indeed, the multi-stakeholder approach is fundamental to the development of successful standards, particularly in the area of Cybersecurity where public sector requirements are implemented to a large extent by private sector service providers.

In the field of promoting a Single Market for Cybersecurity products, the Cybersecurity strategy underlines the importance of the ETSI CEN CENELEC Cybersecurity Coordination Group (CSCG) and ENISA, by stating: 'the Commission will support the development of security standards'; 'Such work should build on the on-going standardisation work of the European Standardisation Organisations (CEN, CENELEC and ETSI), of the Cybersecurity Coordination Group (CSCG) as well as on the expertise of ENISA, the Commission and other relevant players'.

The Cybersecurity Coordination Group (CSCG) of CEN, CENELEC and ETSI is the only joint group of the three officially recognised European Standardisation Organisations with a mandate to coordinate Cybersecurity standards within their organisations. The CSCG was created in late 2011 to provide strategic advice on standardisation in the field of IT security, Network and Information Security and Cybersecurity.

In response to the European Union's Cybersecurity Strategy, the CSCG has published a White Paper with recommendations on digital security. The CSCG's recommendations underline the importance of Cybersecurity standardisation to complete the European internal market and to raise the level of Cybersecurity in Europe in general.

CSCG Recommendation #1 states:

The European Commission should mandate the CSCG to create a governance framework for the coordination of Cybersecurity standardisation within Europe. The CSCG recommends that the European Commission should consult the CSCG on all harmonisation and standardisation issues related to Cybersecurity. Within the European Cybersecurity initiative, the CSCG shall be the relevant point of contact for a cooperative network for the exchange of best practices, assisting its members in building coordinated capacity and steering the organisation of harmonised standardisation projects. The CSCG also recommends that the European Commission should establish a legal framework throughout the EU, enabling the complete and seamless implementation of harmonised and mature Cybersecurity standards.

Although the fulfilment of this recommendations in such a form would be formally impossible due to the legal framework put in place, this document analyses the good practices within the governance framework of the European Union and proposes recommendations for stakeholders.

2. Particularity of Cybersecurity

It is not easy to provide a unique definition of the term 'security'[4]. In common language technology related to security has been difficult to unequivocally identify. Linguistic barriers are present; the terms 'security', 'safety' and 'privacy' often are used in common language as synonyms. There are scoping issues too, as national security, personal security, corporate security etc. are also considered. Taking this into account in the technology domain of information security, a rough consensus has been derived around the CIA (Confidentiality, Integrity and Availability) paradigm. Thus applying this CIA paradigm we can protect a document from revealing information to an eavesdropper, we can detect if a document has been manipulated, and we can control access to a document. When scenarios are presented, the actors in the CIA paradigm are also broadly agreed by a rough consensus as Alice and Bob, who wish to exchange their documents without the adversary Eve gaining any useful information or in any way adversely impacting the activities of Alice and Bob[5].

However whilst the CIA paradigm works well in a document structured world, and can be applied with some success in multi-party transactions, it may have reached its limit as we move towards a new level of infrastructure, the internet being the representative and the most pervasive instantiation of such a change. Complementing the CIA paradigm with other attributes, such as identification and non-repudiation of documents and files appears necessary.

The public Internet and the underlying IT infrastructure (nowadays mainly operated by telecommunications companies owned by private or private-public shareholders) has become a critical infrastructure for both businesses and individual users. Growing dependence on networked digital systems has brought with it an increase in both the variety and quantity of Cyberthreats. The different methods governing secure transactions in the various Member States of the European Union sometimes make it difficult to assess the respective risks and to ensure adequate security. In a classical document based CIA paradigm the roles of Alice, Bob and Eve are relatively simple to isolate. The movement to a world where we move away from classical documents towards shared data, shared computing resources, shared networking resources and shared processing there is an increasing fuzziness in determining the role of each of Alice, Bob and Eve.

Cybersecurity is not an entity that is simple to classify. It is not the application of cryptography to encrypt a document, or to authenticate a user of a computer system. Cybersecurity as a domain looks at the security of infrastructures, devices, services and protocols, as well as security tools and techniques to ensure security. The role of a Cybersecurity expert is to offer security advice and guidance to users, manufacturers and network and infrastructure operators.

Cybersecurity may be classified as the set of techniques required to provide security assurances in Cyberspace. The characteristics of Cyberspace thus need to be examined in order to provide a true Cybersecurity framework.

One key characteristic of Cyberspace is that it is an infrastructure that is shared by all business domains, all social domains, all countries and all citizens. Increasingly the users of Cyberspace are not human but are

[4] Please refer to ENISA paper *Definition of Cybersecurity – Gaps and overlaps in standardisation*, published jointly with this one.
[5] http://www.networkworld.com/article/2318241/lan-wan/security-s-inseparable-couple.html

machines thus Cyberspace is the infrastructure that underpins the Internet of Things, Intelligent Transport, eHealth and several other applications. The end result is that Cyberspace is the critical infrastructure of all things and thus will be host to criminal and terrorist actions just as much as the host to citizens, industry and government. This key characteristic, of criminals sharing infrastructure with their victims, of governments sharing with their citizens, of nation states sharing infrastructure with the neighbours and competitors is new and distinguishes Cyberspace and Cybersecurity from previous generations.

Cybersecurity differs from other areas because the systems to which best practices (including formal guidelines and standards) are to be applied are by nature socio-technical systems, where human beings and technological elements are strictly intertwined. The social part of the systems is comprised of multiple actors and stakeholders. In technical domains primarily a restricted and controllable set of actors can be encountered. All these different actors can have conflicting interests in protecting their security – the ongoing debate on the confidentiality of individual users of Cyberspace versus the necessities of national security are only the most striking example.

The role of standardisation and policy, in their interaction with Cyberspace and Cybersecurity is similarly complex and this is possibly best exemplified with regard to privacy legislation. From these considerations it follows that a purely technical, classical standardisation approach is likely to fail in such a domain as Cybersecurity. With people being part of the system to be secured, purely technical standards and guidelines have to be complemented by organisational, societal ones. In standardisation policy a multi-disciplinary approach is an essential requirement that has yet to become accepted. Key disciplines to be involved include engineering, sciences, law, political sciences etc.

3. Objectives of coordinated approach towards Cybersecurity standardisation

The notion of a standard is derived from its definition as: '*a document, established by consensus and approved by a recognized body, that provides, for common and repeated use, rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context'* (ETSI from ISO/IEC Guide 2:1996, definition 3.2).

Parties taking part in a standardisation process and its stakeholders are described in the ENISA paper *Definition of Cybersecurity – Gaps and overlaps in standardisation*[6]. Industry has a specific role there, as industrial de-facto standards are widespread. Within the private sector, industrial interest in standardisation activities in the area of NIS tends to be driven by areas of work that are in line with the core interests of product developers or service providers (for example authentication, billing, etc.). Aligning public sector goals with standardisation priorities of the private sector remains challenging.

Where information security is concerned, there is clearly room for improvement in identifying and responding to evolving risks and technology developments. In particular, the time lag between the appearance of a new technology or technically driven business model and the availability of applicable standards is still too long.

In the coordination of the approach to standards for Cybersecurity the developers of standards should be encouraged to work to achieve consensus on technical matters in the context of recognized bodies. The overall objective of a coordinated approach towards Cybersecurity standardisation should therefore meet the following individual objectives:

- Cybersecurity standards should be developed through consensus;
- Cybersecurity standards should be approved in a recognised body;
- The distribution of mandated work for the development of Cybersecurity standards should be coordinated by the recognised bodies;
- Recognised bodies should make their development work programme public and coordinate with other recognised bodies to eliminate duplication and to minimise overlap.

Failure to achieve these objectives is likely to have a negative impact on the achievement of a secure Cyberspace (see section 2) and the application of standardised measures for Cybersecurity.

The identification of a recognised body for standardisation in the Cybersecurity domain has to remain flexible because technology development does not take place in strictly controlled environments. Disruptive technologies[7] have the capability to change markets and where such technologies change Cyberspace or the use of it, the role of recognised bodies that develop standards for such modified markets is likely to change too. In contrast, many of the current recognised bodies maintain what have

[6] ENISA paper published together with this one

[7] A disruptive technology is one that displaces an established technology and shakes up the industry or a ground-breaking product that creates a completely new industry.

been termed 'sustaining technologies'[8] but as standards are often at the leading edge of the market there is already a degree of fluidity of participants in the principal standards bodies as they seek to develop a disruptive technology (e.g. GSM[9], ITS[10]) to a sustaining technology and to bypass many of the oft-quoted problems of disruptive technologies (e.g. immaturity, low reliability, low performance).

Large scale involvement in standardisation is often a reflection of market potential of a specific product or service. The nature of Cyberspace that enables assets to be networked together both in non-real-time and real time is enabled by a relatively small set of technologies. The capabilities offered by the small set of technologies have enabled the growth of Cyberspace itself. However the Cyberspace and the economic activity it supports requires a response of comparable magnitude to enable its protection.

[8] Sustaining technology relies on incremental improvements to an already established technology.
[9] Global System for Mobile Communications
[10] Intelligent Transport System

4. Review of current governance framework

A governance framework in the discussed area is a set of rules and practices applied to assure that European Cybersecurity standardisation activities are aligned with EU strategies and that they stay on track to achieve the goals and implemented in a correct way, allowing for measuring of performance. It should make sure that stakeholders' interests are taken into account and define roles and responsibilities and procedures for proper supervision, control and information flows.

While it is important to understand how Cybersecurity frameworks can assist in IT and information security governance, and what regulatory processes are in place to affect governance, it is equally important to address the issues that inhibit Cybersecurity governance. There is a need for individual care and corporate/governmental driven Cybersecurity governance. Organizations such as businesses and governmental entities should recognize and take steps to minimize risks associated with the use of Information Technology (IT). IT governance is the involvement of all stakeholders in the management process of an organization while security governance involves the board of directors, executives and business owners. Regulatory compliance and increased risk influence IT managers to consider security as a part of their operations and dictates the development of internal governance policies. While there are several tools to assist in the process of governance, organizations have not consistently adopted these tools due to the absence of a formally worldwide adopted sanction. Additionally, factors exist that may influence the process of Cybersecurity governance and include factors such as adoption of Cybersecurity governance frameworks and organizational users understanding their role in the era of IT.

4.1 The big picture

Governance of Cyberspace in general is a complex problem, and Cybersecurity is only one of the objectives that it should achieve. It somewhat developed in an 'organic way', with relatively few controls and centralised supervision. There are limited controls on the provision of address space, on the establishment of the core DNS servers that enable much of the internet to operate, and on the allocation and ownership of TLDs. This model – it must be kept in mind – has allowed the development of the Internet as we know it today and its myriad applications, both commercial and non-commercial. Security was not a concern in the development of the technology that underpins all this but we have reached a point where its necessity, for States, corporations, and individual users alike, is obvious to all.

Information security governance – as distinct from security management – builds the accountability framework and assures the necessary oversight on risk mitigation. The process of security governance deals with aligning security strategies to the organisational strategic objectives, which in the case of nation-states are usually stated in their laws, regulations and Cybersecurity strategies and in the case of business organisations and corporations consist of their business goals. Standards have always been a fundamental tool in information security governance, and the governance of Cyberspace more generally, as they are an obvious tool to transparently build an organisational accountability structure.

Standardisation of technology – especially communications protocols – has been key to the huge development of the Internet, but historically it was not managed, or governed in accordance with a general plan or policy. The technologist that developed each brick in the Internet technological substrate voluntarily let the specification open and accessible. The TCP/IP protocol suite is a prime example: all machines today speak, or are expected to speak, IP. The masters of the IP world are the technologists of the IETF, the IESG, the IAB, and the Area Directors in the IETF's Working Groups. The IP world has much less of the political control that the older PSTN operators where numbering, naming and addressing was

often rigidly controlled through bodies such as ITU-T and global trade agreements. A major European contribution was of course the http protocol, developed at CERN, and its creators' choice of leaving its specifications open and royalty-free. The practical upshot of this is that industry is encouraged to develop 'open' markets through standards with occasionally an impetus given to market development by regional or global agreements regarding the freedom of movement of goods and services being used to promote harmonised standards. While these few examples of decentralised governance were hugely successful, they did not address security (Cybersecurity) in any way. Economic mechanisms – and political considerations – make it unthinkable to redesign the technological substrate of the Internet, security can only be retrofitted on the existing systems.

When it comes to governance of information security standardisation – which is the subject of this work and its scope – it can be argued that a purely decentralised model is not likely to work and achieve its goals. The particularities of Cybersecurity explained in the preceding chapter, especially the socio-technical nature of the systems to protect, the plurality of actors and stakeholders, and the expansion of Cyberspace – the 'IP-world' - to such systems as infrastructures and industrial plants, lead to the conclusion that regulatory efforts are needed. In the European context moreover, coordination among 28 member states with different regulation legislative systems, a certain level of EU-wide policy can be positive, also considering the goals of the Digital Single Market initiatives.

The rest of this chapter will review the current framework of information security governance in the European Union, the actors involved, and how they interact and produce standards.

4.2 European Cybersecurity Standardisation Governance

4.2.1 European Standardisation Organisations

The definition of 'European Standardisation Organisations' (ESOs) encompasses the main transnational bodies engaged in standard development and recognised also by the European Commission.

- CEN (The European Committee for Standardisation) is the ESO with the broadest scope of subjects and has a membership composed of the National Bodies. CENELEC (the European Committee for Electro-technical Standardisation) is the specialised entity under which – among other things – Cybersecurity standardisation falls. As mentioned, the constituency of CEN-CENELEC[11] is composed of National Standardisation Bodies, representing both EU and EFTA countries, and other stakeholders. The National Bodies that form the membership of CEN and CENELEC are usually also part of the ISO worldwide standardisation system and transposition of ISO work items to CEN deliverables is assured under the Vienna agreement[12], whilst IEC work items are transposed to CENELEC deliverables under the provisions of the Dresden agreement.
- ETSI (European Telecommunications Standards Institute) is also a transnational organisation, however with a narrower scope, as the acronym reveals. ETSI historically develops mainly ICT standards and among its most successful technical standards are the original GSM specifications for digital cellular networks. The constituency of ETSI[13] is quite different than CEN-CENELEC's. Industry can be directly represented as the membership is not based on national representatives. The development process is usually nimbler and more focused; the great majority of standards developed are technical in nature. ETSI is also open to non-European members, an important aspect to be considered when global application of standards is desired. There is no equivalent at

[11] http://www.cencenelec.eu
[12] http://www.iso.org/va
[13] http://www.etsi.org

ETSI for the CEN-ISO and CENELEC-IEC agreements but rather a set of co-operation agreements with other SDOs that encourage re-use of existing standards work in the ETSI work programme.

The development process inside the ESOs is based on consensus among all the stakeholders involved, although across the ESOs the stakeholders determining the suitability of a standard for publication is a function of the ESO and the deliverable type. The internal governance of the ESOs represents the first side of the wider European governance framework for Cybersecurity standardisation, the other being the interaction between ESOs and the Commission when standardisation is developed in support of policy.

Internally to each ESO a further subdivision into specialist bodies occurs and this is seen across each of a number of technology sectors that address sector specific (vertical domains) and sector independent (horizontal domains) standardisation requirements. Examples include:

- ETSI TC CYBER – Coordination group for all horizontal activity related to Cybersecurity and privacy protection; has remit and power to promulgate new technical standards and to align output of ETSI where internal conflicts exist.
- ETSI ITS WG5 – Responsible for vehicle to vehicle and vehicle to infrastructure communication security in the domain of Intelligent Transport Systems

To mitigate the risk of duplication of effort and facilitate communication between the ESOs and with the European Commission, in 2011 a coordinating body was established, the Cybersecurity Coordination Group, putting together representatives from the ESOs, the Commission, and relevant stakeholders – ENISA among them.

4.2.2 European Union Bodies

While the ESOs are completely independent in their activities regarding which standards to develop and how to do it including the timing and priorities of their activities, the EC has been interested in how standardisation could support European policy goals since the early 1980s, establishing contacts and cooperation with the standardisation organisations.

Among the Directorates Generals of the Commission, DG GROWTH (Internal Market, Industry, Entrepreneurship and SMEs) holds the main responsibility for standardisation policy in general and initiating the standardisation requests to the ESOs.

In the field of Cybersecurity however, several other DGs are involved in policy shaping:

- DG Connect (Communications Networks, Content and Technology) is responsible for the Digital Single Market;
- DG Home (Immigration and Home Affairs): Cybersecurity is one of the facets of National and European Security. DG Home is responsible for the European Agenda on Security, cybercrime and cooperates with EC3 (European Cybercrime Centre at EUROPOL[14];
- DG Justice: Cybercrime is a fast growing area of crime, one of the main threats to society and driver for development of Cybersecurity measures. Areas covered by this DG also include privacy and data protection.

[14] https://www.europol.europa.eu/ec3

4.2.3 Policy and standardisation: how the EU interacts with the ESOs

Regulation 1025/2012 is the current legal basis for the interaction between the Commission and the ESOs. It lays the basis for the development of voluntary standards in support of European legislation and policies. It also serves as the legal framework for the use of standardisation in products and services.

The Regulation affords the Commission the key role in standardisation governance, both in the planning phase and the implementation phase. The annual planning cycle results in the EU Work Programme for standardisation, in which it is explained how the Commission intends to leverage standardisation to foster legislation and polices. The implementation phase is carried out mainly via 'Standardisation Requests' (previously known as mandates) issued to the three European Standardisation Organisations. The requests are issued, following a consultation phase with relevant stakeholders and the go-ahead by the Committee on Standards, and formally via a Commission Implementing Decision. The requests can be accepted or refused by the ESOs; however they are usually accepted. Once accepted, the ESOs are bound to develop specific standardisation deliverables – most importantly European Standards – in a specified timeframe. While the adoption of the final standards is voluntary, national standardisation organisations are required to transpose the newly developed European standards into national standards, superseding if necessary previous national ones.

The standardisation process follows the principles, laid out in the Regulation. The process must be transparent and promote broad participation among stakeholders interested. Work programmes are publicly available – this does not apply however to the internal processes and documents during the development itself. Also it must be noted that while final published ETSI standards are available freely, this is not usually the case for CEN-CENELEC.

A final note on the ICT technical standards, so important in Cyberspace, and not developed usually by the recognised ESOs: the Regulation provides a mechanisms by which these standards can be referenced and incorporated into the European process. Under its article 12 a notification system for all stakeholders, (including European standardisation organisations and European stakeholder organisations) has been established.

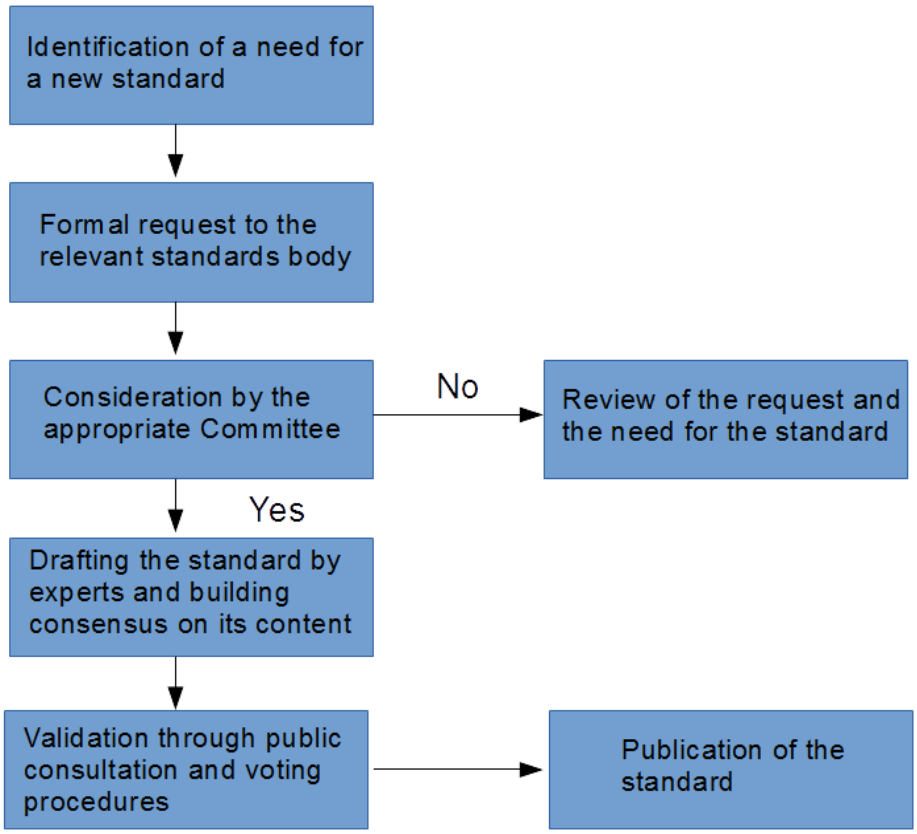

Figure 1: Development of European standards

5. Good practices in Cybersecurity standardisation

In this chapter, good practices in terms of standardisation in Cybersecurity are identified, with regard to stakeholders, and in preparation of aligning procedures.

Cybersecurity is a community effort, so one important goal is to make stakeholders interested parties in standardisation. Therefore in Section 5.1 a listing of stakeholders is given. It is also important to get the interested parties to the table, making participation possible and efficient for them. Procedures play a major role in this, so they are discussed in Section 5.2.

5.1 Stakeholders

This section gives a short description on stakeholders that should participate in standardisation activities and their typical properties. In principle all types of stakeholders may come in with 'products', which they would like to see considered in standards. Products may be commercial products or services that commercial stakeholders like to promote in the respective markets, but products can also be concepts and ideas that their originators would like to proliferate.

5.1.1 European Standardisation Organisations (ESOs)

ESOs are the main transnational bodies engaged in standard development and recognised by the European Commission. For description, please refer to Section 4.2.

Among them, CEN, the European Committee for Standardization, is an association that brings together the National Standardization Bodies of 33 European countries.

5.1.2 National standardisation/normalization bodies

National standardisation bodies are organizations (unique per country) whose tasks include coordination of national standardisation activities and participation in international bodies like CEN or ISO as representatives of the countries. Usually they don't take part in technical preparation of standards, which is performed by national technical societies.

5.1.3 Policy and administration

Policy and administration stakeholders often participate in standardisation to maintain the relation between standards and related regulation (e.g. regulation on electronic signatures), but also with less formalized guidance documents issued by the respective administrative agencies (e.g. documents on IT security baseline protection). This would especially hold for Cybersecurity expert agencies such as MS Agencies with competence on network and information security

In some cases policy and administration stakeholders participate in standardisation from the perspective of protecting their 'own' Cybersecurity, i.e. the security of their users and their infrastructure.

5.1.4 Industry and research

Some industry stakeholders participate in standardisation to maintain the relation between standards and their products and services. In this role they tend to prefer fast standardization to follow market trends and not too detailed standardisation to keep the design sovereignty with regard to their products.

Some industry stakeholders participate in standardisation, as they are major users of the respective standards and possibly related technologies and services. Often they need to protect their earlier investments and are therefore not interested in too dynamic and radical changes in standards.

Research stakeholders often participate in standardisation to contribute with new concepts and ideas to promote them and to gather feedback on them. Often they are interested in publishing their gatherings and their experiences.

5.1.5 Consumer and community

Consumers usually do not have the resources to participate in standardisation themselves. Therefore most consumer stakeholders in standardisation are representatives of consumer organisations. The situation is similar for communities. In many cases neither consumer stakeholders nor community stakeholders have major resources for this activity.

5.1.6 Education

Education stakeholders participate in standardisation for different reasons: Some standards treat education and training, so education stakeholders contribute with experiences, concepts and ideas similarly to other domain stakeholders for other reasons. In addition education is often, especially in universities, closely related to research, so for some education stakeholders combining their education and research interests makes sense and often only the combination makes a convincing case to incur the investments and costs needed for standardisation.

5.2 Procedures

Appropriate procedures play a major role in efficient delivery and uptake of ICT security standards. The set of good practices presented below provides for a good base for an appropriate governance framework.

- Preference for the existing EU approach

The current organisational frameworkis appropriate toconstitute a base for all standardisation activities within the EU. Procedures described in Section 4 are based on the legal requirements (specifically Regulation 1025/2012) and proved to be effective if correctly applied. This correct application however is crucial to ensure that standards that are developed are really needed by stakeholders and of good quality.

- Good representation from stakeholders

It is crucial to ensure good representation of stakeholders mentioned in section 5.1. in the standardisation process. As adoption of standards is in most cases a voluntary measure, lack of participation of specific entities or lack of consensus among them might result in a low uptake of specific standards.

- Transparency of procedures

Promulgation of standards should be as transparent as possible. The need of a standard should be notified to the appropriate body (i.e. appropriate DG of the European Commission), the same transparency should be applied to the process of standardisation request and further development of standards. No stakeholder should be specifically excluded from this process. History of standards creation should be available to be consulted.

- Process as open as possible to independent experts and SMEs / all interested parties

The standardisation process should not exclude independent experts and SMEs, who often cannot afford expensive trips to plenary meetings of large standardisation bodies. Appropriate means to ensure their presence in the procedures should be put in place.

- Availability of published standards

Although it is not possible to ensure availability of all standards without cost at international level (i.e. ISO standards), it is important to make sure that information about new standards is widely spread. The standards created under European framework should be 'advertised' among stakeholders even at the stage of their creation and their availability shoud be ensured.

- Bottom-up approach to creation of Cybersecurity standards

Cybersecurity standards should be created based on the needs of stakeholders. Appropriate entities (i.e. DGs of the European Commission) should collect the relevant information on the need of standardisation activities through ongoing public consultations with the industry, research and supervisory bodies.

5.3 Cybersecurity Coordination Group (CSCG)

The ETSI CEN/CENELEC Cybersecurity Coordination Group is a European-level group of standardisation experts fostered by the three European Standardisation Organisations, CEN-CENELEC and ETSI. Inside the CSGS, which holds regular periodical meetings throughout the year are represented the ESOs, the European Commission and ENISA.

CSCG is well placed to foster communications among the relevant actors, namely the ESOs and the policy level, helping on one hand the ESOs to suggest possible standardisation activities in support of European policies and interests and on the other hand to the policymakers to tap the expertise pool provided by the Cybersecurity experts, even before formalising Standardisation Request, in an ongoing collaboration. CSCG is also well-placed for coordinating efforts between the ESOs, eliminating overlapping and duplication of efforts.

6. Recommendations for stakeholders

The particularities of Cybersecurity standardisation outlined above, with their far-reaching consequences, call for new and more efficient modalities of interaction among the main actors – the European Standardisation Organisations, the European Commission – and other stakeholders.

In some areas there are standards missing; in other areas there may be the danger of overlapping work potentially leading to problems in interoperation of technical artefacts and synchronisation of standardisation initiatives

Currently interaction among ESOs and among different Work Groups working on overlapping or similar activities is almost always based on bilateral "liaisons" carried out by specific officers or experts designated inside each group and reporting periodically. Also, there is a clear lack of coordination of standardisation activities in the area of Cybersecurity. A more flexible and less rigid model of collaboration could improve communication, information sharing and efficiency.

Cybersecurity standardisation in support of European policies necessarily involves the European Commission as hub and input source for the actual standardisation development. Currently the governance framework is based on a somewhat rigid "request-response" protocol, where Standardisation Requests are directed from the EC to the ESOs which chose to fulfil it or not.

This governance modality is also quite rigid and a more nimble, continuous dialogue should yield more efficient results, both in terms of celerity and adherence to the high-level policies of the European Union and European interests more generally.

A model that could be advised consists in a coordinated approach to the development of standards. Appropriate DGs of the European Commission should collect the needs from stakeholders on a permanent basis (participation of ESOs in the process can be considered – industry initiatives initiated through ETSI, national ones through CEN/CENELEC). Standardisation requests should firstly be consulted with a coordination body, such as CSCG, which would maintain a database of standards and ongoing standardisation activities. The input from such a coordinating body would be used to justify a concrete standardisation request.

This need for nimbler, more structured communication, continuous collaboration and coordination in Cybersecurity standardisation could be satisfied by a permanent forum where the Commission (the relevant DGs), the three European Standardisation Organisations, the agencies involved – ENISA among them – are present.

The already established Cybersecurity Coordination Group could very well fulfil this role, as it involves representatives both from the National Standardisation Bodies member of CEN-CENELEC as well as from the more industry-oriented ETSI members. Moreover, the Commission is already involved, for now the GROWTH Directorate-General, as well as ENISA.

At the end of 2011, the European Multi Stakeholder Platform (MSP) on ICT standardisation[15] was set up. Based on a European Commission Decision[16] to advise on matters related to the implementation of ICT standardisation policies, it deals with: potential future ICT standardisation needs in support of European legislation, policies and public procurement; technical specifications for public procurements, developed by global ICT standards-developing organisations; cooperation between ICT standards-setting organisations; and the Rolling Plan[17], which provides a multi-annual overview of the needs for preliminary or complementary ICT standardisation activities in support of the EU policy activities. It is recommended that the CSCG should be involved in the work of MSP, as advisory body.

It is moreover recommended that a specialised Cybersecurity group be created inside the CEN-CENELEC system. A group of this kind already exists in the other ESO, ETSI.

Facilitating communications among ESOs and the EC would mean that ESOs could be much more proactive in proposing new standardisation even before the developing of formal requests. Also they would be much more involved and knowledgeable in the developing of Cybersecurity policies and so in a better position for their main activity in support of Europe. In short, a permanent forum/platform to mediate and facilitate information sharing among ESOs themselves and ESOs and the policy level would let to better and faster standard developing in support of EU policy.

There are three organisational models for coordination that can be adopted: The first model is a centralised coordination group with more authorities; the second model is a centralised focus group. The primary difference between the models is the degree of influence on the work programmes of the ESOs and thus the impact on the governance models of each ESO. The third model is a coordination group in its current status.

1. A centralised coordination group with authority to direct the cyber security standardisation activity across the ESOs would address the following concerns:
   - Weak interaction of ESOs both internally and to each other: The existing model of interaction relies upon bilateral “liaisons” carried out by specific officers or experts designated inside each group and reporting periodically. Such liaisons tend not to be able to veto or promote work in the liaised to body and the relative informality does not give any guarantee of communication, information sharing and efficiency.
   - EU governance framework reliance on a “request-response” protocol: There is no obligation on the ESOs to accept standardisation requests from external bodies and in practice any work item raised has to be raised within the specific governance structures of the particular ESO and each ESO has a different model. The Cybersecurity Coordination Group fulfils this role but augmented by alterations in the governance rules of the ESOs to accept guidance from an external group. The existing Joint Presidents Group and the Global Standards Coordination groups would then recognise the coordination body as an adjunct to the existing ESOs with special responsibility in this domain.
2. The second model is to form a centralised focus group that is maintained externally to the current ESOs as a discussion forum. Unlike the coordination group this would not require any alteration to the governance models of the ESOs but should be recognised by the Joint

[15] https://ec.europa.eu/digital-agenda/en/european-multi-stakeholder-platform-ict-standardisation
[16] https://ec.europa.eu/digital-agenda/news/commission-decision-28-november-2011-setting-european-multi-stakeholder-platform-ict
[17] https://ec.europa.eu/digital-agenda/en/rolling-plan-ict-standardisation

Presidents and Global Standards Coordination groups as a formally managed body of the EU with special expertise in the Cybersecurity domain. The purpose of a focus group should be similar to that of the coordination group but working on a series of gentleman's agreements on the distribution of standards activity in this domain. This should be considered as a more formal body that the existing CSCG but may be drawn from the same body of experts.

3. The third model is to keep the group in its current organisational shape and to address any further organisational issues after a gap analysis and an overlap analysis have shown, what work needs to be done and is needed most urgently.

ENISA

European Union Agency for Network
and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office

1 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece

Catalogue Number TP-01-15-933-EN-N

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu

ISBN: 978-92-9204-154-0
DOI: 10.2824/358519