BUSINESSEUROPE

POSITION PAPER

23rd November 2017

The proposal for a Cybersecurity Act

KEY MESSAGES

1. No one-size fits all certification scheme can apply to all connected technologies or the risks they face. The certification framework cannot pre-prescribe a list of elements to be included in each scheme.
2. Determining and developing schemes requires a bottom-up approach. ICT users and providers aligned with the EU's strategic cybersecurity interests should be formally included at the earliest stages of each candidate scheme.
3. The framework must be voluntary to try, test and understand the benefits and impact of each scheme before determining whether market access rules are required. Schemes should be dynamic to certify the ability to react to new challenges and risks.
4. Innovative businesses are increasingly exposed to practices aimed at misappropriating trade secrets and IP. More importance should be placed on exploring other policy avenues necessary to counter industrial intellectual property theft and implementing existing law. Strong encryption is crucial and should be encouraged. We should not (inadvertently) reduce the capabilities of organisations to protect their intellectual property.
5. The standards and practices behind each scheme will be crucial. Industry-led technical standards should be developed in an open, transparent and consensus-based manner to forge interoperability in cybersecurity.
6. ENISA should be granted a permanent mandate to continue supporting cybersecurity capacity building in Member States.
7. The human factor is one of the most significant causes of cyber events in terms of error and threat. The public and private sectors need to increase efforts to highlight the importance of basic cyber-hygiene, attack avoidance, incorporation of "security-by-design" and heightened vigilance in the workplace

WHAT DOES BUSINESSEUROPE AIM FOR?

Encouragement of all players in the value chain to ensure products, services and systems are cybersecure from the earliest stage of the engineering process in a dynamic way. A cybersecurity certification framework that achieves voluntary, robust, industry-relevant and affordable schemes. A one-size fits all scheme cannot apply to the multitude of Internet of Things. Europe should promote the need for general education and awareness of basic cybersecurity to minimise human error in security incidents.

Context

As the global digital revolution takes hold and proliferates into our economies, societies and governments, the potential for information to be electronically tampered with and controlled is real. According to the International Data Corporation (IDC), by 2025, almost 90% of all data created will require some level of security but less than half will be secured[1]. At the same time, the sheer number and intricacy of cyberattacks, cyber espionage and cyber sabotage has increased in recent years. Its overall economic impact rose five-fold between 2013 – 2017 and there are suggestions that this will further quadruple by 2019.[2] These attacks are often coordinated by hacktivists, criminal actors and state actors. They are directed at citizens, businesses and political institutions.

The digital single market cannot reap its full economic and societal benefits if the technologies and services it consists of are not secure. In line with ENISA's Maslow's cyber-need pyramid, the challenges faced by businesses, citizens and society are paramount.[3] There is also much to be learnt from the evidence displayed and from the information received in relation to known cybersecurity attacks. Information sharing in sector specific fora, known as ISACs (Information Sharing and Analysis Centres) are proving a highly effective way of preventing cyber-attacks from having a wider impact, for instance in the financial services sector.

That is why many businesses have (continually) invested in understanding and limiting the impact of cyberattacks as a key part of their business model. This does not only enable them to globally sell their products and services in a safe manner through complex distribution chains, but prioritising cybersecurity also enables greater system availability, protects their brands, loss of business information, investment and intellectual property.

Government, agencies, businesses and citizens all have a role to play in ensuring cyber secure conditions. The cooperation between these four facets are vital in the pursuance of safe and trusted conditions for Europe's digital economy. Without these conditions, innovative technologies such as, the Internet of Things (IoT)[4], Artificial Intelligence (AI) and the Industrial Internet will not be able to realise their great economic and societal potential.

Going forward, the EU's cybersecurity policy needs to embrace collaboration, flexibility, and robustness while fostering long-term innovation-friendly and tech-neutral progression. At the same time, high-class digital infrastructure is required for businesses to base their cybersecurity measures upon in relation to the functioning of their products or services in the digital single market.

BusinessEurope supports the Commission's intention to update ENISA's mandate and **set up a framework to identify specific cybersecurity schemes** that could meet pan European application. We **remain committed to increasing Europe's cybersecurity capacities** and **therefore propose improvements below** to negate concerns we have in relation to its objectives. The proposal should champion innovative solutions and a smooth transition to a fully digitalised economy.

[1] Data Age 2025: The Evolution of Data to Life-Critical, IDC, 2017
[2] Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, JOIN/2017/0450 final
[3] Principles and Opportunities for a renewed EU Cybersecuirty Strategy, ENISA, 2017
[4] (it takes 2 minutes for an IOT device to be attacked) Internet Security Threat Report, 22, Symantec, 2017

1. One-stop-shop for certification

In the context of connected industries, all players in the value chain should ensure their products and services are cybersecure in a dynamic manner from the earliest stage of the engineering process, thereby also promoting responsible innovation through (security-by-design). The creation of a European cybersecurity framework ("framework") could be beneficial to determine the need for certain cybersecurity certification schemes (Article 2(9)) ("schemes"). This may only lead to its desired outcome if the framework enables: specific, voluntary, dynamic, industry-relevant and affordable schemes.

Therefore, if well designed, such schemes could play an important role in increasing security of digital products, services and systems. When pan-EU schemes are not deemed beneficial fragmented national initiatives should be aided through mutual recognition. The international recognition and compatibility of such schemes should be kept in mind due to the global relevance of applicable markets.

While we support entrusting the European Commission to establish a framework for ICT products and services, we draw your attention to the fact that groups of ICT products and services will require a specific approach. Although some capabilities to react to cyber threats can be standardised, no one-size fits all framework can be attributed to the array of current and future IoT technologies and potential risks attributable to them. This requires different approaches in different economic sectors due to the way they function.

In this case, we think it would be necessary that the Regulation should take a bottom-up approach and recognise how all sectors and sizes of businesses currently understand and focus on identifying, assessing and alleviating cybersecurity risks. Then a focus on what should be achieved and how it can be designed by the European Commission in cooperation with ENISA and its like-minded industrial stakeholders.

No development can slide into a one-size fits all approach. To this end, the elements to include within Article 47 should be guiding and not pre-prescribe or direct any scheme. It should be decided on the basis of stakeholder input for each scheme at hand. For example, possibilities could include security precautions required by the consumer (eg. instructions to change passwords) but this example would not be needed if not relevant (eg. the device may not be intended for consumers or have password authentication).

The first step towards a framework must be taken through voluntary mechanisms. The benefits of each scheme should be tried and tested before any mandatory market access rules are put in place for certain products and services. Due to the potential costs of such schemes, it is important that the benefits of any market access relevant schemes are fully understood and in the first stage, take the positive and negative costs, security levels and competitiveness of participants into account before being concluded.

Still, the current proposal may already have unintended consequences of making certain schemes mandatory by default. As the proposal enables ENISA to determine schemes through referencing other Union or international standards (Article 47(1)(b)), any reference made to "state of the art" (eg. in privacy by default or design, Article 25(1) in the General Data Protection Regulation (GDPR)), could automatically warrant it mandatory in practice. While this may not be the intention of this proposal – legal certainty should prevail. The voluntary nature should also not be indirectly altered in practice through the use of public procurement. The framework should instead encourage all sectors to carry out and disseminate certification practices in relation to their specific technological areas. This would allow each scheme to relate to state of the art practices, remain tech-neutral and robust.

A strong focus on security by design and secure development practices is necessary to strengthen the cybersecurity capabilities of industry. A blanket approach to mandatorily apply a renewal of certificates every 3 years under Article 48(6) without taking the scheme at hand into consideration will not reward active and dynamic intervention in the framework as security can be eroded by new cyberattack techniques. This is the wrong direction for this framework to head in. If a scheme is “static” (eg. it certifies at a given time but doesn’t provide for continuous upgrade) it cannot effectively certify the ability of a product or service to react to new cyber-threats. Also, renewing every 3 years could create huge demands and cause unnecessary bottlenecks, turning interested applicants away. A more effective approach would be to ensure that the scheme specifies dynamically, the organisational and technical procedures the ICT provider has to put in place to effectively and timely react to new threats and challenges. In this sense, we believe that Article 46 should make reference to organisational procedures used to ensure continuous upgrade.

Yet industry input in the proposed new governance structure is currently limited. After the Commission asks ENISA to prepare a candidate scheme ENISA will consult national certification authorities grouped together in the newly established “Cybersecurity Certification Group”. Industry stakeholders (ICT users and providers) that are aligned with the EU’s strategic cybersecurity interests should also be formally included at the beginning of the process. To that end, the Cybersecurity Certification Group should be complemented by a like-minded “Industry Stakeholder Group” to offer appropriate know-how at this crucial time of decision making and should have strong relationships with international, global and European Standards organisations.

When designing such schemes, the Commission and ENISA should be aware that 100% security is not possible and should reflect that an acceptable marginal risk will exist. The assurance level scheme under Article 46 is positive in this regard. That is why the involvement of industry to define minimum levels of security requirements such as: secure identity management and the ability to patch and update IoT devices when vulnerabilities emerge, are key factors to consider. Defining requirements is typically the role of standards developing organisations and careful consideration needs be put in to the interplay between these groups. Clarity will be needed to determine whether levels within schemes are guiding for users or if they have an actual legal impact in practice

A false sense of cybersecurity should not be created through the introduction of measures to develop cybersecurity certification practices for IoT devices. To that end, the framework should strike the right balance between the need to ensure the highest level of cybersecurity and the costs that companies, in particular SMEs and start-ups, face through such schemes.

The framework will no doubt increase labelling practices in order to demonstrate voluntary compliance. The presence of a label does not guarantee ongoing security of the product. In addition, any label will only be as useful as the market surveillance that follows it. Those investing in such practices need to exist within a level playing field and not be undercut by non-bona fide actors seeking to apply labels to non-conforming technologies. This will require substantial Member State investment in order to police the market and impact assessments on the benefits of applying labels.

2. Primacy of European schemes

Fragmentation of national cybersecurity rules have proliferated and can represent single market barriers, particularly in areas where they are used to enable market access. This can make the use of complex distribution chains to process and sell highly innovative products and services across borders more difficult. Therefore, we support the

Commission's proposal that once a specific EU scheme and the related certificate is adopted, a national scheme covering the same area falls away (with the understanding that no Member State can be forced to lower its cybersecurity levels). Otherwise, a legally uncertain and confused market for these technologies would exist.

Each scheme must determine possible use of self-certification/third-party certification. Yet the Commission's proposal misses to mention the possibility of self-certification for connected products and services. In the context of the New Legislative Framework, industry has successfully demonstrated that self-certifying a wide range of products on safety and health aspects significantly elevated product safety. Therefore, independent entities within a company should be allowed to perform assessments. Enabling this possibility would provide more proportionality for suppliers applying certain security requirements, for example, it provides a measure of security for sensitive intellectual property. This would also improve the time it takes to place an operation on the market and better achieve ENISA's goal of increasing the capacities of business and improve costs, particularly for SMEs. Voluntary self-certification methods used under the New Legislative Framework for industrial products could provide inspiration to guide policy makers in this regard.

3. Consistency with other legislation

The framework or schemes it produces must be fully consistent with other European legislation (eg. the General Data Protection Regulation (GDPR) and Directive on security of network and information systems (NIS)). The GDPR will soon oblige organisations to establish and follow cybersecurity practices such as protection against loss, alteration, unauthorised disclosure and access of data. Time limited notification procedures are included, impact assessments will be required before high risk data processing can take place and demonstration of compliance is needed. The NIS Directive equips Member States with competent authorities to react and notify Cyberattacks. It has enabled greater cooperation between Member State authorities and created a culture of security across various business sectors.

In this regard, Member States and businesses continue to prepare to fully implement both the GDPR and NIS frameworks by May 2018. As businesses continue to prepare to apply its provisions fully, data breach notification procedures in both the GDPR and NIS Directive should be elaborated on to give authorities the responsibility to return notification information to businesses about cybercrime and hacktivism.

4. Standardisation

Since IoT technologies are developing and proliferating at a rapid pace, it is necessary to have sector specific standards that are developed and updated by industry. The standards and practices behind each scheme will be crucial. Identification of existing or any missing standards for certain products and services should take place before any intended scheme is approved. Therefore, as European standardisation organisations (eg. CEN/CENELEC and ETSI) have vast experience in developing technical specifications, they should be at the heart of developing cybersecurity standards which should be considered when developing these schemes.

Europe needs a strong and globally competitive industry for cybersecurity on par with other leading regions. Each scheme should remain globally relevant in the context of cybersecurity threats and practices. To facilitate interoperability (eg. to enable encryption), Europe together with its like-minded international partners should continue to build on their cooperation in developing and supporting industry-led voluntary technical standards, in an open, transparent and consensus-based manner. It should make use of international mutual recognition schemes where necessary. Europe should only divert from the globally accepted standards where a first mover advantage exists.

5. Encryption

Cybersecurity should not be weakened for national security and encryption should be promoted. With the growth of the internet, encryption has become one of the most important tools governments, companies, and individuals have to promote safety and security in the new digital age. While acknowledging the overall benefits of encryption, many governments have started pushing for the introduction of what are often called "backdoors." That is, a hidden way of bypassing the software protocols that keep communications secret, accessing only the conversations of malicious actors, while continuing to protect everyone else.

Yet backdoor proposals undermine cybersecurity. Cryptographers, like other scientists, build on each other's theory and practice. Weakening any part of encryption weakens the whole cyber security ecosystem. Cybersecurity experts from governments, academia and industry continue to prove that it is impossible to create any backdoor with a guarantee that it would never be discovered and used by malicious actors from which this proposal seeks to shut down. Compromised backdoors are a single point of failure which creates a great risk for the digital single market. Secure communications are a vital component to maintaining Europe's commercial competitiveness by enhancing our protection against industrial espionage.

6. ENISA

In order to strengthen European cybersecurity, it is necessary to establish the basic pillars on which it is based: resilience, deterrence and defence. Therefore, it is positive that the European Cybersecurity Agency (ENISA) is reviewed and granted a permanent mandate in order to continue supporting cybersecurity capacity building and coordination between Member States. Full application of the NIS Directive will also require ENISA to be entrusted with a more stable mandate in order to apply these activities in the future (eg. elaborating and implementing establishment of Analysis and Exchange Centres). Increasing public-private cooperation in this regard would be beneficial to achieve the aims of this proposal. It is also important that central coordination of its activities takes place to avoid fragmentation at national level.

While cooperation in cybersecurity through information sharing has improved, greater legal certainty for businesses when sharing that information with other public and private entities is required. This will not only improve the overall functioning of cybersecurity frameworks but trust between public and private partners. It is often the case that some businesses do not feel fully confident in sharing information about their products and services while governments and agencies do not want to share information in relation to national security. This gap needs to be bridged using better regulation principles so that knowledge sharing can enable investment and innovation in the correct areas to the benefit of more efficient cybersecurity conditions.

7. Awareness

We believe that more ambition could complement the Cybersecurity Act to solidify the security capabilities and confidence in Europe's digital economy. As just under a half of

European citizens feel that they are well informed about the risks of cybercrime[5] and 95% percent of all security incidents involve human error, the greatest vulnerability to cyberspace are citizens.[6] Therefore, we need to increase our education and awareness raising efforts to highlight the importance of cyber hygiene of connected devices. This knowledge could develop overtime. More experienced businesses in this policy area could also create dialogues and demonstrate best cybersecurity practices to less experienced businesses. As “going digital” is no longer an option but a necessity, all businesses, no matter the size, sector or region will need to be aware of cybersecurity practices that are relevant to their sector.

Even modest efforts by the Commission and Member States in this regard can make a big difference to the success of ongoing industry led efforts to invest and educate consumers on the importance of cybersecurity. They would also increase the impact of future schemes proposed through this framework. We would therefore welcome further EU and Member State initiatives aimed at improving the awareness and knowledge of cybersecurity amongst citizens.

We also remind policy makers that the cybersecurity skills gap for professionals working in the private sector is predicted to grow to 1.8 million by 2022.[7] More can be done to update Member State education systems so that the engineers, programmers, developers and after sales jobs which will be created by the explosion of IoT devices in various sectors of our societies uphold the importance of cybersecurity.

Users of IoT technologies should be encouraged to keep their devices updated for their own benefit and the benefit of cyberspace on the whole. This will require industry efforts to disseminate best practices and standards which should also be a pre-requisite for a scheme. Member States and more advanced industry players should also support smaller and medium sized businesses to aid in the information sharing and implementation of cybersecurity best practices. The EU should support businesses through adequate funding and fostering of cooperation between public and private actors (eg. Commission’s public-private partnership on cybersecurity in 2016) which is instrumental in coordinating cybersecurity resources in Europe.

8. Industrial Cyber-theft

This proposal does not address cyber-attacks aimed at businesses to protect them against cyber-theft of critical technologies, trade secrets and other confidential business information. Innovative businesses are increasingly exposed to dishonest practices aimed at misappropriating trade secrets and IP. Industrial theft of IP and trade secrets have been continuously escalating: these attacks are estimated to make up 25% of all cyber-attacks across all sectors and up to 94% of all cyberattacks in the manufacturing sector in 2016[8]. The cost of industrial IP and trade secrets theft is expected to cost between 1-2% of GDP[9] and result in a loss of competitiveness, reduced R&D investments and jobs.[10] Without effective legal and technological means for protecting IP and trade secrets across the Union, incentives to engage in innovation related cross-border activity within the internal market are undermined. These growing attacks are being motivated more and more by state funded actors. In the interest of innovation,

[5] Special Eurobarometer 423, Cyber security, Commission, 2015
[6] Cybersecurity intelligence index, IBM, 2014
[7] Global Information Security Workforce Study, Frost & Sullivan, 2017
[8] Data Breach Investigations Report 10th Edition, Verizon, 2017
[9] Net Losses: Estimating the Global Cost of Cybercrime, Economic impact of cybercrime II, Center for Strategic and International Studies, 2014
[10] Trade Secret Report: Economic Impact of Trade Secret Theft, CREATe – PwC, 2014

effective ex-ante/pre-emptive policy responses need to be considered in all possible EU policy avenues. Member States should also fully implement the trade secrets Directive in this regard.[11]

In order to develop our capacities to deter and prevent state funded cyber espionage, the Commission should launch a study to determine what legal options exist to deter states engaged in supporting, enabling, tolerating or neglecting the prevention of cyber-attacks or cyber-intrusions. Expensive defensive measures will never be fully effective without accompanying strategy to deter potential hostile actors than investing in expensive defensive measures.

* * *

[11] Directive (EU) 2016/943