EU Cyber Security Package
Position Paper

Introduction

ISACA, a global, independent, non-profit association that serves nearly 140,000 information and cyber security, audit, risk and technology governance professionals, many of whom live and work within the European Union (EU), welcomes the opportunity to share its position on the new EU Cyber Security Package, including the proposal for a Regulation on ENISA and on Information and Communication Technology (ICT) cyber security certification (EU Cyber Security Act).

President Juncker's State of the Union address and the publication of the package begins an EU-wide discussion on the level of security needed to protect EU business and citizens and to build trust in the digital single market. ISACA welcomes and fully supports the strong political push for cyber security. Further, the organisation seeks to be an expert participant in the discussion.

In recent years, traditional information security has entered the cyberage, with increased amounts of information being available from a wide range of everyday devices and more organisations having online sales channels, information security has needed to keep pace and evolve to include cyber security. Organisations have therefore been challenged by the emergence of cybercrime and cyberwarfare, which are growing rapidly. Security breaches have evolved from opportunistic attacks by individual perpetrators to targeted attacks that are often attributed to organised crime or hostile acts between nation states. Moreover, new technologies are changing the cyber landscape. Growing digital connectivity brings enormous opportunities but also exposes the economy and society to rising threats and risks related to the Internet of Things (IoT) devices, systems and services. To mitigate these risks, Europe needs to substantially improve its approach to cyber security.

The present paper provides ISACA's perspectives on selected elements of the EU Cyber Security Package, with particular emphases on the role of the European Union Agency for Network and Information Security (ENISA); the proposed cyber security certification framework; and certain aspects of the Joint Communication "Resilience, Deterrence and Defence."

The role of ENISA

A coherent response to emerging cyber security needs in Europe requires the existence of a genuine central cyber security agency with a clear mission and strategy. ENISA is the only EU-level body with extensive experience and knowledge base in the field of cyber security. However, so far, the fixed-term mandate has been a limiting factor in defining the Agency's long-term strategy and – more importantly – in attracting highly specialised cyber security experts. Consequently, **ISACA welcomes**

the intention to strengthen ENISA's role and responsibilities through a permanent and broader mandate. Increased financial and human resources allocated to ENISA are a necessary prerequisite for effective execution of the Agency's current and future tasks, including those foreseen in the context of the future framework for certification. **In addition to a larger number of permanent employees, the Agency should also have a list of external consultants with particular expertise who could be consulted as needed for specific issues**.

Increased cooperation with stakeholders is an important aspect of ENISA's enhanced mandate. **ISACA strongly supports the establishment of the Permanent Stakeholders' Group** whose role is to advise the Agency on its activities, including the Agency's work programme. In addition to representatives of public authorities, the industry and consumer organisations, the **Group should also include representatives of recognised professional organisations, particularly those who are able provide a global perspective.** This is particularly important as cyber threats have no borders and individual professionals are key to build cyber resilience. Moreover, ISACA believes that the Group's term of office should be longer than the proposed two and-a-half years. The selection, formation and establishment of the Group's working practices is a lengthy process that may take up to one year. Therefore, **to ensure continuity and stability of the Group, the term of office should be at least four years.**

ICT cyber security certification

ISACA strongly supports the objective of the Regulation, which is to make the cyber security certification more attractive and less expensive for businesses. **A harmonised approach and mutual recognition of certificates is fundamental to increase resilience and solve the present fragmentation challenge.**

The current co-existence of multiple schemes and standards for security certification results in a significant burden for the industry; therefore, it is crucial to ensure that the future EU certification framework be fit for purpose. In ISACA's view, **rather than creating new cyber security schemes, European cyber security certification should attest that ICT products and services are certified in accordance with globally recognised standards.** The creation of completely new cyber security schemes would increase the cost for ICT companies, which in the end would be paid by customers. This would also increase the time needed for the development of new products and services. Given the borderless nature of the digital environment and cyber threats, it is essential that ENISA leverage globally recognised standards, guidance and best practices when developing future certification schemes, and engages in close cooperation with international partners in the standardisation process.

It is equally important to **ensure that the process of preparing future candidate schemes is maximally open and transparent, and it takes into account the needs of the broad range of users.** Given the considerable impact that the future schemes will have on the economy and society, this process must involve not only national public authorities but also the representatives of different industry sectors and professional organisations.

ISACA believes **that the Regulation should also define the timelines for schemes to become effective following their adoption**. Considering the current state of cyber security and people's mindset, ISACA believes that **the voluntary nature of certification schemes is appropriate at this stage.** Certification can become an important source of competitive advantage and the market will regulate it by creating stronger demand for certified ICT products and services. The willingness to purchase certified equipment could be further increased by acknowledging that using equipment certified in accordance with the level of risk by organisations is considered "prudent" and could serve to reduce the fines these organisations would need to pay in case of breaches. Mandatory certification might be needed in the future but only for a limited group of products with high security risks, such as critical infrastructure and electronic health.

ISACA believes that **the security objectives defined in the proposed Regulation should also cover user-friendliness (usability) and simplicity** to clarify that the user does not require formal training to use the security solution. **This is particularly important for private users who should also be encouraged to use certified equipment, as this could bring significant advances in security.** It is challenging to put a price tag on the prevention of an incident. However, according to the 2017 Ponemon Institute Cost of Data Breach study[1], the average consolidated total cost of a data breach was more than 3M Euro. That's not to mention the reputational damage to the organisation, which can be unimaginable.

Moreover, the **security objectives should be aligned with provisions of the GDPR**, especially with regard to personally identifiable information (PII). Finally, it should be ensured that **cyber security will follow the complete development life cycle and that change management of products and services will take into account cyber security in order to avoid creating new vulnerabilities.**

ISACA agrees with the proposed validity period for certificates, which is maximum three years. This is an optimal period after which products should be recertified. The criteria for determining specific assurance levels should be further clarified. The requirements for each level should be also clearly defined.

Under the proposed Regulation, the monitoring, supervisory and enforcement tasks lie with the Member States. Each Member State will have to provide for one certification supervisory authority, which will then look at the compliance of various conformity assessment bodies. Such a process

[1] 2017 Ponemon Cost of Data Breach Study

might be complicated and could lead to different criteria and procedures followed by conformity assessment bodies in various Member States. ISACA believes **there should be one central body responsible for monitoring all conformity assessment bodies to ensure that all of them function in the same way following the same procedures.**

EU cyber skills base

The Joint Communication "Resilience, Deterrence and Defence: Building strong cyber security for the EU" sets out an updated ambitious EU cyber security strategy. ISACA welcomes the emphasis put in the Communication on education, cyber hygiene and awareness. Cyber resilience needs a strong boost not only in terms of infrastructure but also human resources. The European Commission rightly notes that a large share of cyber security incidents are due to technical failures without malicious intent or due to some type of human error. The insufficient awareness of cyber-threats of employees and poor cyber hygiene practices contribute to increased vulnerability of companies to cyber threats. The EU, therefore, should have a high focus on improving security skills at all levels of society--business and public sector.

Building a strong EU cyber skills base is one of the objectives set out in the Communication, and **ISACA staunchly supports the call on industry to step up cyber security-related training for organisations' staff**. Addressing the cyber security skills gap is a major challenge that has been at the heart of ISACA's activities. In ISACA's 2017 State of Cyber Security Research report, fewer than half of the organisations responding were confident in their teams' abilities to handle anything beyond simple cyber incidents.[2] ISACA will build upon these efforts even more in 2018, when we will launch a tool for organisations to measure their cyber security capabilities on a continual and evolving basis. It is ISACA's belief that such 'evolvable' tools are necessary to protect enterprises large and small in the face of an ever-shifting threat landscape.

Conclusions

ISACA would welcome the opportunity to work with the EU decision makers throughout the legislative process leading to the adoption of the EU Cyber Security Act and stands ready to assist the efforts to identify the needs for future certification schemes. ISACA also will provide practical guidance materials for its members to facilitate compliance with the requirements set by the future EU framework.

[2] ISACA 2017 State of Cyber security

Summary

The role of ENISA

- ISACA welcomes the intention to strengthen ENISA’s role and responsibilities through a permanent and broader mandate.
- The Permanent Stakeholder Group should include representatives of recognised professional organisations, particularly those who are able provide a global perspective.
- In order to ensure the necessary continuity and stability of the Permanent Stakeholder Group, the term of office should be at least four years.

ICT cyber security certification

- ISACA strongly supports enhanced cyber security and a harmonised EU approach to certification.
- The certification schemes must adhere to globally recognised standards. Creating completely new schemes will lead to delays and additional costs for businesses and, ultimately, consumers.
- The process of preparing future candidate schemes must not only involve national public authorities but also various sectors of industry and professional societies.
- The voluntary nature of certification schemes is appropriate at this stage.
- The security objectives of the future schemes should include simplicity – this is important for private users who should be encouraged to use certified equipment.
- Cyber security should be reflected in the complete development life cycle and change management of products and services.
- The Regulation should define timelines for schemes to become effective, to avoid unjustified delays.
- To avoid fragmentation, there should be one central body responsible for monitoring all conformity assessment bodies to ensure that all of them function in the same way following the same procedures.

EU cyber skills base

- ISACA staunchly supports the need to boost cyber security skills at all levels, business and public sector. Addressing the cyber security skills gap is a major challenge that has been at the heart of ISACA’s activities.

About ISACA

Nearing its 50th year, ISACA® (isaca.org) is a global association helping individuals and enterprises achieve the positive potential of technology. Today's world is powered by technology, and ISACA equips professionals with the knowledge, credentials, education and community to advance their careers and transform their organisations. ISACA leverages the expertise of its more than 140,000 members in information and cyber security, governance, assurance, risk and innovation, as well as its enterprise performance subsidiary, CMMI® Institute, to help advance innovation through technology. ISACA has a presence in more than 188 countries, including more than 215 chapters and offices in both the United States and China.

ISACA Headquarters: 3701 Algonquin Road, Suite 1010, Rolling Meadows, Illinois, 60008 USA
Web: **www.isaca.org**

Contact:
Tara Wisniewski - twisniewski@isaca.org
Jen Gremmels - jgremmels@isaca.org