European Round Table
for Industry

# ERT Position on Cybersecurity

# Introduction

## For the European economy to flourish, business and consumers need to take full advantage of the opportunities offered by new technologies.

The successful uptake of services like cloud computing, artificial intelligence, automated and autonomous driving, e-health, smart grid technology, factories of the future and many other new applications depends on users trusting the security of this increasingly digitised world. They need to feel confident that their data and privacy is protected.

New technologies as well as greater interworking across them is introducing new complexity. These changes can create new vulnerabilities or magnify existing weaknesses, making them more exploitable through cyber-attacks. As we get more connected, the risks could multiply. Also, as the volume, sophistication and persistence of attacks has increased, the public mood and government reaction to cyber-attacks have varied from sector to sector, state to state and crisis to crisis. This has led to the fractious debate and fragmented regulatory framework we encounter today.

Industry and policymakers acknowledge the importance of protecting digital technologies and the benefits of a strongly coordinated approach to cybersecurity policy in Europe and beyond. Mutual recognition of the shared need for cybersecurity should serve to facilitate some common standards and behaviours.

ERT Members welcome the recent legislative initiatives such as the NIS Directive, the Cybersecurity Act, and more recently the European Commission recommendation on 5G security leading to the definition of a toolbox. Those initiatives will enable the EU to continue to strengthen the EU's resilience and security capabilities across our society.

We are open to cooperating with governments and policymakers to ensure Europe delivers on these initiatives. ERT has analysed the cyber defence maturity trend related to European companies and developed the following recommendations.

# ERT recommendations to strengthen cybersecurity in Europe and globally

### a) Governments should coordinate with industry to facilitate detection of and response to cybersecurity incidents:

- **Governments are responsible and need to have adequate means at their disposal to protect civil society and businesses against foreign state cyber-attacks.** The rate of cyber-attacks by state actors against civil society is continuously rising and governments need to do more to protect and deter such activity. It is unreasonable and undesirable to expect the private sector to be the primary security provider. The pay-out ratio from conducting such activities needs to change to decrease the incentives and stem the increasing trend.
- **We need global in-depth robustness and resilience in our societies to sustained cyber-attacks.** There is no getting around the need for companies in Europe and around the world to boost and maintain to the appropriate level their security by design and internal measures when delivering products and services. To be prepared for attacks, industry should encourage decision makers (notably in medium and small size enterprises) to improve their cybersecurity capabilities. For example:
  - To have proper contracts to support the appropriate product and service robustness with partners and providers proportionate with their possible risks for their customers and society.
  - To keep up with preventative and recovery basics.
  - To access and to benefit from government available threat intelligence to improve prevention and detection of state-sponsored attacks.

Industry should also encourage cybersecurity players to develop and deploy new tools to protect our data economy and keep pace with the complexity of digital technology that underpins it, for example: security of AI-based decisions, security of automation and orchestration of services & security of autonomous transportation services.

Political support on national, regional and global levels can help industries in their fight against cybercrime and strengthen their due diligence and societal strategies.

- **Policymakers should facilitate and promote newly adopted and ongoing initiatives at EU level to enable a secure and resilient society.** At the same time keeping at the forefront the need for state-of-the-art security when implementing technology to enable a truly digital and sovereign EU. In this respect, we welcome the recently adopted texts at EU level. The regulatory framework that follows must re-enforce guiding principles that are technology neutral as the pace of technological change outpaces detailed regulation and legislation very rapidly.
- **Avoid fragmentation by encouraging the horizontal cross-domain consistency of cybersecurity measures (including certifications), to avoid possible variability of requirements across industries for the same transversal products or categories of products.**

There is significant tension between some national postures and the transnational nature of digital technology particularly in public digital services. Many jurisdictions still have different regulations and approaches towards cybersecurity. Ultimately this leads to different requirements that cause product vendors to manage several versions of the same product, and forces multinational companies to manage several different architectures. This is inefficient on a European, and a-fortiori on a global scale. There are opportunities for companies to provide services once and deliver them to many, but government requirements for the legal domains of their state can lead to local service provision or data storage that can restrict the architecture choices for industry.

We welcome the ongoing work by the European Commission together with the European Union Agency for Cybersecurity (ENISA), Member States and industry stakeholders to develop a common coordinated approach to avoid fragmentation and hence strengthen the EU's principles of trust and resilience in the digital single market.

We encourage the European Commission to promote coordination between the Directorate Generals in the development of security requirements for the proposed changes to the Radio Equipment Directive, General Product Safety Directive and the Machinery Directive and an aligned approach towards harmonised standards for the implementation of security requirements.

- **International cooperation & standardisation: The EU and its Member States should strive for a co-ordinated European voice and greater investment in pressing for international consensus and transparency, which ultimately underpins industry driven baseline standards and certification schemes.**
    - Use the available tools enshrined in the NIS Directive or the Cybersecurity Act to strengthen cooperation at EU level and exchanges with industry.
    - Use the Stakeholder Cybersecurity Certification Group to intensify exchanges between the European Commission and industry to harmonise and foster common risk analysis approaches, to identify security objectives and reflect industrial reality in security requirements.
    - Promote multilateral collaborations in regulation and standardisation to set a level playing field matching the global reach of the World Trade Organization (WTO), including development of global standards and principles for cybersecurity e.g. in the International Telecommunication Union (ITU), G7 and G20 and inclusion into Free Trade Agreements (FTAs).
    - Inspired by the Budapest Convention on Cybercrime, ERT is open to working with partners from politics and industry to establish international rules on responsible behaviour in dealing with cybercrime.
    - In alignment with industry, policymakers should adopt European or International third-party certification schemes wherever appropriate, for example certification of critical infrastructure applications and critical Internet of Things (IoT) solutions where lives and limbs are at stake.
    - Adopt risk-based decisions on security requirements, based on evidence or objective criteria and following a robust impact assessment of the measures on the entire value chain.
- **Awareness-raising:** Governments should provide standardised cybersecurity information to raise awareness and transparency to their citizens and businesses. Cybersecurity information should include insights and information relating to cyber incidents & breaches where appropriate and necessary.
- **Public procurement:** Public administrations should lead by example by integrating cybersecurity requirements into their public procurement specifications.
- **Education:** Dedicated cybersecurity courses should be included in school curricula – as degree courses in universities, professional education and trainings – in order to lead the transformation of skills and job profiles needed for the future. This includes having professionals in all fields that understand cybersecurity risks and requirements. Digital and cybersecurity upskilling of our workforces and all EU citizens will be key to ensuring a resilient and secure, but digitally savvy, society.
- **Public-private dialogue:** Industry is committed to foster the public-private dialogue to enhance trust in the digital economy. ERT stands ready to engage with governments, citizens and other key stakeholders in the cybersecurity debate to support confidence in the adoption of Information and Communication Technology (ICT) applications and solutions.

### b) ERT Members believe that companies should embrace the following principles:

- **Ownership of cyber and IT security:** Companies should anchor the responsibility for cybersecurity at the highest organisational levels by designating specific Chief Information Security Officers (CISOs) with clear responsibility for cybersecurity assurance in all businesses and corporate areas. And to develop and deploy the cybersecurity strategy and culture across the organisation, coordinated by the CISO. They should establish board level oversight and clear measures and targets as well as the right mindset throughout organisations – "It is everyone's task". Benchmarks should be set for checking the effectiveness of actions in cybersecurity strategies and information sharing.

- **User-centricity:** Companies should serve as a trusted partner throughout a reasonable lifecycle, providing products, systems, and services as well as guidance based on the customer's cybersecurity needs and risks. They should simplify and reduce the security responsibilities that users and customers have to assume.

- **Security by design, security by default & security monitoring:** Companies should adopt the highest appropriate level of security and data protection and ensure that it is preconfigured into the design and monitored during the entire lifetime of products and services, across functionalities, processes, technologies, architectures, and business models. Cybersecurity standards should be embedded into business processes and organisational goals.

- **The commitment to build leading capabilities in cybersecurity:** Meeting stringent security requirements for achieving confidentiality, authenticity, integrity, secure lifecycle management and availability objectives.

- **Identity and access management:** Connected devices must have secure identities and safeguarding measures that only allow authorised users and devices to use them.

- **Encryption:** Connected devices and communications networks must ensure confidentiality for data storage and transmission purposes wherever appropriate. Encryption has a role to play to ensure confidentiality and should be promoted.

- **Continuous protection:** Companies must offer updates, upgrades and patches throughout a clearly communicated reasonable lifecycle for their products, systems, and services via a secure update mechanism.

- **Holistic approach:** Security requirements need to be considered in a holistic and joint fashion that consider dependencies at standard, product, deployment and operation level, to ensure security enhancements materialise.

- **Claiming responsibility throughout the digital supply chain:** Companies must establish a risk-based comprehensive approach for enabling cyber resilience across all the relevant value chains, including IoT. The framework must enable transparent cyber risk management via collaborative, adaptable and assured means:

  - **Collaborative –** cyber resilience governance framework across the full supply chain. Incident response and business continuity plans have to be extended beyond the company's boundaries.

  - **Adaptable –** products and processes need to be reviewed (as the nature of the cyber threats evolve), encouraging willing market players to pioneer stronger security, over time.

  - **Assured –** independent third-party certification where appropriate. Independent certifications for security-relevant processes or security-relevant technical solutions can help to reduce the risk of cybersecurity incidents, especially where life and limb are at risk. Critical infrastructure and critical IoT solutions (e.g. autonomous cars, collaborative robots) will be increasingly exposed to cybersecurity threats. Based on the recent Cybersecurity Act and other regulations, European public authorities should in public private partnerships work on new certification schemes that leverage on existing and relevant European and international schemes, unless security requirements are already established and audited via Notified Bodies, e.g. for Medical Devices Manufacturers via the Medical Device Regulation.

# Conclusion

## Growing cybersecurity risks will place constraints on the future development of Europe.

Governments, citizens and industry all have a role to play in managing risks and building the required cybersecurity capabilities for the Digital Single Market, thereby providing a framework of trust. To strengthen cybersecurity, governments as well as EU institutions and ENISA will need to work with industry and all relevant stakeholders to develop baseline security and coordination requirements. There is an important read-across to social acceptance of digital transformation that calls for a straightforward and open conversation with the public about the cultural and behavioural changes ahead. International, cross-industry and public-private collaboration is paramount to ensure system resiliency.

ERT

The European Round Table for Industry (ERT) is a forum that brings together around 55 Chief Executives and Chairs of major multinational companies of European parentage, covering a wide range of industrial and technological sectors. ERT strives for a strong, open and competitive Europe as a driver for inclusive growth and sustainable prosperity. Companies of ERT Members are situated throughout Europe, with combined revenues exceeding €2 trillion, providing around 5 million direct jobs worldwide - of which half are in Europe - and sustaining millions of indirect jobs. They invest more than €60 billion annually in R&D, largely in Europe.

+32 2 534 31 00 www.ert.eu
contact@ert.eu @ert_eu

Boulevard Brand Whitlocklaan 165
1200 Brussels, Belgium

Position paper released in February 2020