Balancing digital transformation and cybersecurity policies

Policy brief on Cybersecurity: more investment and better skills

Cybersecurity is defined in the report as "all the safeguards and measures adopted to defend information systems and their users against unauthorised access, attack and damage to ensure the confidentiality, integrity and availability of data"

Digital Transformation + Online interactions → Exposure to cyber threats and digital crimes

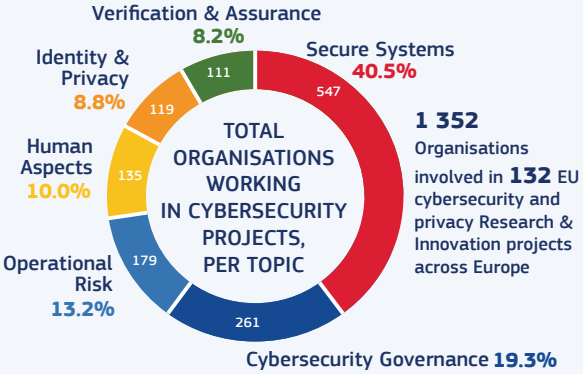
There has been an increase in cybersecurity threats. Since **2018**:

- There has been an **11%** increase of digital breaches
- Phishing has become the most prevalent cyberthreat, with more than 320 000 victims in around 150 countries

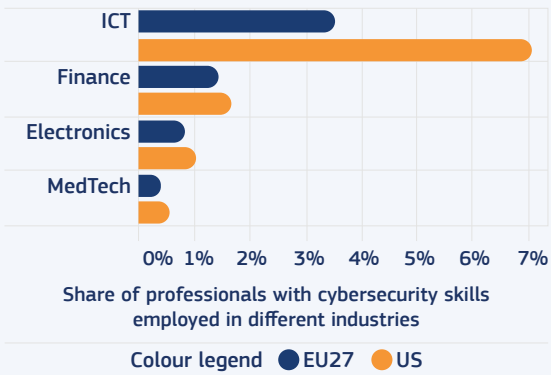
Due to this increase, cybersecurity and privacy are areas of major policy concern. In the report entitled **Shaping Europe's Digital Future**, the Council of the European Union underlined the importance of cybersecurity as **"... a key component for a digitalised Single Market, as it ensures trust in digital technology and the digital transformation process."**

The EU27 needs to invest more into cybersecurity research, technologies and skills

- Produces cybersecurity technologies with unique expertise and a strong research community in **postquantum cryptography**
- Leads in secure implementation of **cryptographic algorithms** in hardware and software of cybersecurity technologies
- Between **2013-2017**, the EU27 owns 23% of the world's patent applications in digital security technologies
- Currently behind the US in terms of **patent applications** and cybersecurity spending and investment



The EU is continuing to heavily spend and invest in multiple cybersecurity areas, including "Secure Systems" and "Cybersecurity Governance". The main challenge for the European cybersecurity industry is that the biggest players and service providers are non-European.



There is a shortage and mismatch in terms of quality of professionals with cybersecurity skills in Europe. Currently, the US has a higher share of cybersecurity professionals than the EU27 across all investigated industries, indicating a high skill gap in cybersecurity and a lower uptake of these technologies across Europe.

For more information, read the full Policy Brief on Cybersecurity: more investment and better skills here:
https://ati.ec.europa.eu/reports/policy-briefs/cybersecurity-more-investment-and-better-skills

The European Commission has taken steps to enhance cybersecurity capabilities and stimulate a stronger cybersecurity industry

EU Cybersecurity Strategy

- Boost EU-level cooperation, knowledge and capacity
- Encourage the emergence of SMEs in cybersecurity
- Strengthen EU industrial capabilities and partnership
- Protect critical infrastructure

European Cybersecurity Act

- Entered into force on June 2019
- Established an EU framework for cybersecurity certification
- Boosts the cybersecurity of online services and consumer devices

There are currently gaps in the national and European level cybersecurity strategies, such as a lack of necessary capabilities, skills and infrastructure, to defend institutions against:

- New cyber challenges
- Skills shortages in cybersecurity
- Lack of entrepreneurship
- Funding gaps, i.e. in the growth phase of SMEs

To support national governments in their cybersecurity strategies, a **common vision for "Cybersecurity in Europe by 2030"** was developed to aid in formulating, prioritising and coordinating recommendations for actions around cybersecurity across Europe.

About the Advanced Technologies for Industry (ATI) project

The ATI project – funded by the European Commission – supports the **implementation** of Europe's new growth strategy with a systematic monitoring of **technological trends** and reliable, **up-to-date data** on advanced technologies.

The **Policy Briefs** analyse national and regional policy measures focused on a specific policy challenge, technological area or mode of implementation and explore policy tools that have been designed and implemented with the aim of fostering the generation and uptake of advanced technologies. The reports provide a comparative analysis of some of the most relevant national and regional examples on the policy landscape in the EU. They highlight the lessons learnt based on existing policy evaluations, monitoring or any other learning process and will present both good practices and potentially the bad ones. In the case of novel policy initiatives, they focus on the key challenges in the design process.

For more information, read the full Policy Brief on Cybersecurity: more investment and better skills here:
https://ati.ec.europa.eu/reports/policy-briefs/cybersecurity-more-investment-and-better-skills

Publications Office of the European Union

PDF: ISBN 978-92-9460-576-4 doi: 10.2826/778094 EA-02-21-484-EN-N