DIGITALEUROPE

THE DOWNLOAD

DIGITALEUROPE's concise policy brief on the hottest tech topics.

In this edition:

TAMING THE CYBER STORM WHILST EMPOWERING EUROPEAN BUSINESSES TO THRIVE

What do we think?

Cybersecurity must be a top priority for the EU. As we digitalise our economy, it is vital that we keep governments, businesses and citizens safe online.

Legislation can be an essential part of that process, but it can harm our interests if not done well. It's all about ensuring an effective and coherent implementation across the EU. Companies have been grappling with a complex web of new EU cybersecurity legislation. In the past five years alone, the EU has put forward at least eight laws impacting cybersecurity.

Compliance costs for companies are estimated to be at least €60.2 billion.[1] If we want businesses in Europe to build strong cybersecurity whilst remaining competitive, we must simplify and harmonise our cyber rules instead of creating more laws.

We call for a focus on implementing existing legislation, alignment with other regions, dedicated funding to support compliance and a more collaborative approach with industry.

What does it mean for a company to be 'cyber-secure'?

Cybercrime cost the global economy over $8.15 trillion at the end of 2023, almost triple the figure of 2020.[2] Companies must protect their services and customers from digital threats such as phishing and malware attacks. They have to apply technical and organisational measures, ranging from encryption to complex processes responding to hacks.

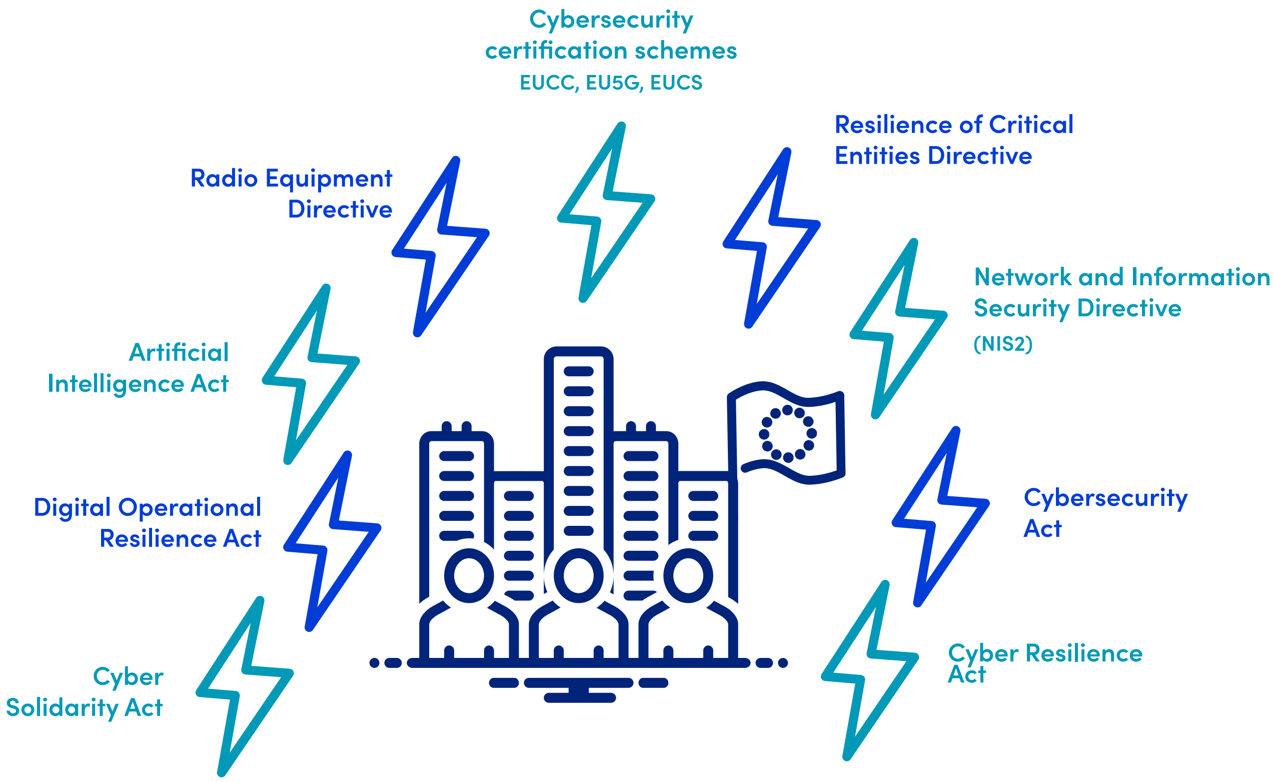
For instance, in finance, cybersecurity teams focus on securing transactions, preventing fraud and protecting customer data. In healthcare they must protect patient data, medical devices and hospital networks.

[1] Based on Frontier Economics, Assessing the economic impact of EU initiatives on cybersecurity, available at https://www.frontier-economics.com/media/izyk5rgz/assessing-the-economic-cost-of-eu-initiatives-on-cybersecurity.pdf, and the European Commission's Cyber Resilience Act impact assessment (SWD(2022) 283 final).

[2] Statista, 'Estimated cost of cybercrime worldwide 2018-2029,' available at https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide.

State of play

A complex web of new cybersecurity legislation



Cybersecurity certification schemes
EUCC, EU5G, EUCS

Resilience of Critical Entities Directive

Radio Equipment Directive

Network and Information Security Directive
(NIS2)

Artificial Intelligence Act

Digital Operational Resilience Act

Cybersecurity Act

Cyber Solidarity Act

Cyber Resilience Act

Russia’s aggression against Ukraine has increased the threat level, which pushed the EU to create new rules to boost cyber resilience. The success of these measures depends on ensuring that businesses of all sizes can handle the complex and often costly web of legislation.

What challenges are we facing?

- **Who's in charge?** There are multiple EU and national cyber bodies with overlapping responsibilities. Finding guidance becomes an impossible task.
- **Too much reporting:** Multiple reporting is using up scarce company resources. For instance, in finance, a single cybersecurity incident may have to be reported at least four times to different authorities.[3]
- **Not enough skills:** Europe faces a shortage of 260,000 to 500,000 cybersecurity professionals.[4] Increased cyber regulation is straining the limited talent available.
- **Hiring lawyers, not cyber experts:** Complying with the revised Network and Information Security Directive (NIS2) and the Cyber Resilience Act (CRA) alone will cost industry a combined €60.2 billion.[5] This is money that should instead be invested in training and hiring cyber experts, or future innovations and markets.

Europe faces a shortage of **260,000 to 500,000** cybersecurity professionals

[3] See DIGITALEUROPE, The Single Market love story: 10 digital actions to save the 30-year marriage, available at https://cdn.digitaleurope.org/uploads/2024/02/DIGITAL-EUROPE-THE-SINGLE-MARKET-LOVE-STORY-FINAL-WEB.pdf.

[4] Communication on the Cybersecurity Skills Gap, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52023DC0207.

[5] Based on Frontier Economics and European Commission data. See 'Assessing the Economic Impact of EU Initiatives on Cybersecurity' and the Cyber Resilience Act's Impact Assessment, respectively.

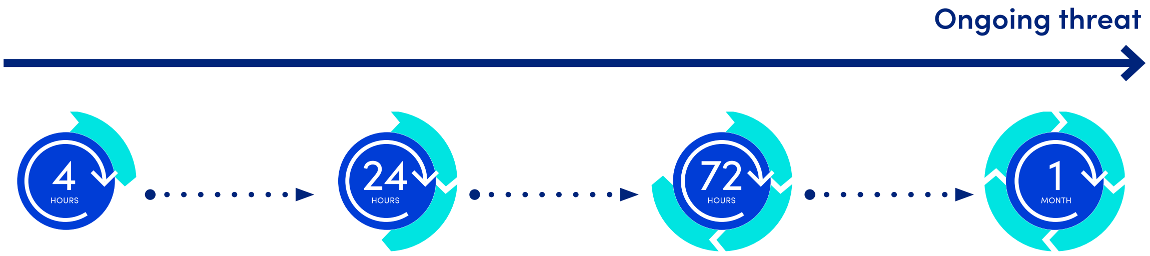
What should the EU do?

- **Implement, not reinvent:** We should properly enforce the cybersecurity laws already in place, rather than create new ones. New rules should only be introduced if they make it easier for companies to comply.
- **Report once:** We should launch a Single Reporting Act to cut down on the number of reports businesses have to file, supporting the Commission's goal of reducing red tape by 25%.
- **Single points of contact:** Each Member State should establish central points of contact for reporting. This would simplify processes and reduce confusion caused by too many different authorities involved.
- **Partners:** We should use the existing 100 standards, and work towards mutual recognition of cybersecurity requirements with other regions.
- **More EU budget for cyber:** Programmes like Digital Europe need more funding to help businesses comply, as is the case in some Member States. In addition, specific funding could provide toolkits and templates to make compliance less costly.

Case study

When a company faces a cybersecurity incident that puts private data at risk, its immediate focus is to contain the threat and recover. But it must not only manage the crisis. The company must do so whilst respecting different EU laws – overwhelming even the most prepared teams.

A bank, for example, must determine whether a breach qualifies as a reportable incident under not only NIS2 and the CRA, but also DORA and the GDPR. Each regulation has its own set of rules, including for when the clock starts ticking.



1. **Notify the financial regulator**
   Under DORA.
2. **Send a notification to national cybersecurity authorities**
   Under NIS2 and CRA.
3. **Submit report to the supervisory authority**
   Under GDPR, and affected data as per CRA and NIS2.
4. **Submit final reports to revelant authorities**
   Under DORA and NIS2. CRA requires this 14 days after corrections.

Managing all these deadlines and formats stretches legal, compliance and IT teams thin. Smaller companies, without enough resources, struggle even more.

For regulators, these overlapping notifications can lead to information overload. Companies, in the meantime, are left juggling reports instead of focusing on resolving incidents – where their attention should be to make Europe more cyber secure. Rather than making companies spend resources on excessive reporting, the EU and ENISA should proactively invest in private-public cybersecurity efforts, such as the EU Cybersecurity Reserve.[6]

[6] As included in the Cyber Solidarity Act.

DIGITALEUROPE

DIGITALEUROPE is the leading trade association representing digitally transforming industries in Europe. We stand for a regulatory environment that enables European businesses and citizens to prosper from digital technologies.

We wish Europe to grow, attract, and sustain the world's best digital talents and technology companies. Together with our members, we shape the industry policy positions on all relevant legislative matters and contribute to the development and implementation of relevant EU policies, as well as international policies that have an impact on Europe's digital economy.

Our membership represents over 45,000 businesses who operate and invest in Europe. It includes 113 corporations which are global leaders in their field of activity, as well as 41 national trade associations from across Europe.

FOR MORE INFORMATION, PLEASE CONTACT:

Rita Jonušaitė
Senior Manager for Cybersecurity & Cloud
rita.jonusaite@digitaleurope.org

Sid Hollman
Policy Officer for Cybersecurity
& Digital Infrastructure
sid.hollman@digitaleurope.org

www.digitaleurope.org

@DIGITALEUROPE

@digitaleurope_org

DIGITALEUROPE

@DIGITALEUROPEvideo