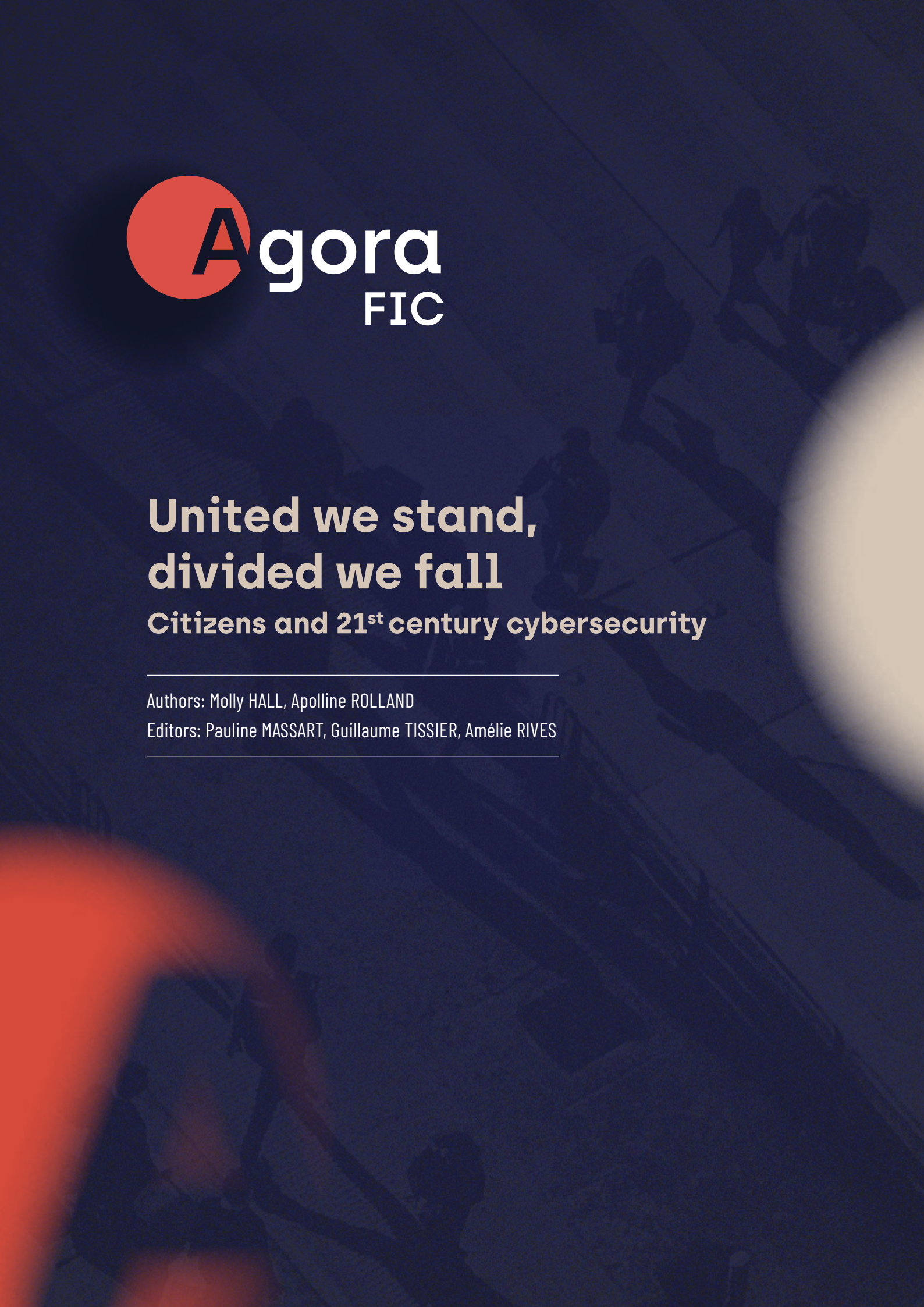


United we stand, divided we fall

Citizens and 21st century cybersecurity

Authors: Molly HALL, Apolline ROLLAND
Editors: Pauline MASSART, Guillaume TISSIER, Amélie RIVES

TABLE OF CONTENT

Acknowledgements 1

Executive Summary 2

INTRODUCTION 6

WHERE DOES THE BUCK STOP? PROTECTING CITIZENS' ONLINE SAFETY 8

THE EUROPEAN UNION APPROACH 8

CYBERSECURITY 8

Network and Information Security Directive - NIS (2016) 8

Cybersecurity Act (2019) 12

Cyber Resilience Act (in process) 13

DATA PROTECTION 14

GDPR (2016) 14

THE GOVERNMENTAL APPROACH 14

PROTECTING CRITICAL INFRASTRUCTURE 14

United States of America 15

Israel 15

How does the protection of critical infrastructure in Europe compare to Israel and the US? 16

PROTECTING DATA AND PRIVACY 18

How is citizen privacy protected outside the EU? 18

THE PRIVATE SECTOR APPROACH 18

DON'T BE A FOOL: USE THE PROPER TOOL! EMPOWERING CITIZENS FOR ONLINE SAFETY 21

AN OUNCE OF PREVENTION IS WORTH A POUND OF CURE 21

National governments 22

Industry 23

Civil society organisations 24

DON'T PANIC! RESPONSES TO CYBER-ATTACKS 25

Government 26

Private sector 27

Civil society organisations 27

FOREWARNED IS FOREARMED: INCREASING CYBERSECURITY AWARENESS 28

THE WAY FORWARD: RECOMMENDATIONS 32

REFERENCES 36

Agora FIC

About

The FIC Agora is the strategic reflection platform of the International Cybersecurity Forum. Its objective is to contribute to the public debate on the major issues of trust and digital security throughout the year.

This high-level platform was prompted by the need for elected officials, public decision-makers, private and public sector managers and academics to exchange and debate on cyber threats, public policies (resilience, the fight against cybercrime, digital diplomacy, industrial policy, training, etc.) and the major societal challenges brought about by technological disruption.

Because responses to cybersecurity issues require close coordination between the territorial, national and European levels, the Agora conducts its work both in Paris and in Brussels. In order to adapt to the sensitivity of the subjects dealt with, it also offers different frameworks for exchange and dissemination, both restricted and open.

agora-fic.com

Avisa Partners

BELGIUM
Boulevard du Régent 35,
1000 Brussels

FRANCE
17, avenue Hoche,
75008 Paris

Contact:
agora@forum-fic.com

NOVEMBER 2022

Executive Summary

The increase in cyber-attacks seems never-ending, in line with our societies' accelerating digitalisation, boosted among others by teleworking during the COVID19 pandemic. While numerous government and industry initiatives have focused on improving online safety, the empowerment of citizens online has often been neglected. Citizens remain the weakest link in cybersecurity. It is urgent to put them at the heart of cybersecurity efforts.

How can citizens be better protected in a changing online landscape? Who is responsible for protecting citizens, and how can they be empowered to become the strongest rather than the weakest link?

This paper by the FIC Agora takes an in-depth look at what cybersecurity players are doing to protect citizens online, from the EU's cybersecurity regulatory frameworks to the national policies of major cybersecurity powers, to trending industry solutions. It delves into the role citizens have to play in improving their own cybersecurity, how to empower them and with what tools to prevent and respond to cyber-attacks.

This paper also tackles the issue of awareness: if citizens are unaware of the risks or how to respond to them, they can never be fully cyber-secure. It is essential to improve cybersecurity awareness to offer citizens a chance to become less vulnerable online.

The FIC Agora surveyed over 1,000 European citizens to understand their awareness of cybersecurity issues and their experience of cybersecurity attacks.

The results are clear: while plenty of online security initiatives are available to industry, citizens are often left behind. Serious effort is needed in Europe to improve cybersecurity awareness to empower citizens to ensure their online safety.

This paper offers 12 recommendations to put citizens at the heart of cybersecurity efforts as part of a whole-of-society approach. Governments, businesses and citizens themselves all have a role to play in collectively improving cybersecurity.

EDUCATION & AWARENESS

1

Fund cybersecurity education programmes in schools. Gen Z, despite being digital natives, has some of the weakest cybersecurity practices of any generation currently in the workforce[1]. This trend is likely to continue unless cybersecurity training begins at an earlier age. Age-appropriate and inclusive cybersecurity education should be a part of the regular school curriculum. Funding could come from public-private partnerships, as the private sector has a responsibility to ensure that its future customers can use its products safely.

2

Establish lifelong learning cybersecurity programmes at the community level. With the rapid development of new technologies, cybersecurity best practices continue to evolve. More opportunities must be created at the community level to ensure that citizens, throughout their lives, can keep up with cybersecurity regulations, tips, and solutions. Such programmes could be funded by local and regional authorities, where necessary via public-private partnerships.

3

Take awareness campaigns beyond education and into adoption. As the EU celebrates its 10th Cybersecurity Awareness Month, the next step must be to ensure that citizens are not only aware of cybersecurity best practices, but actually adopt and implement solutions. Authorities should leverage the momentum around Cybersecurity Month to encourage users to update their passwords, enable automatic updates, or use antivirus software.

1. The Generational Gap in Cybersecurity and Privacy, Weir, URL.

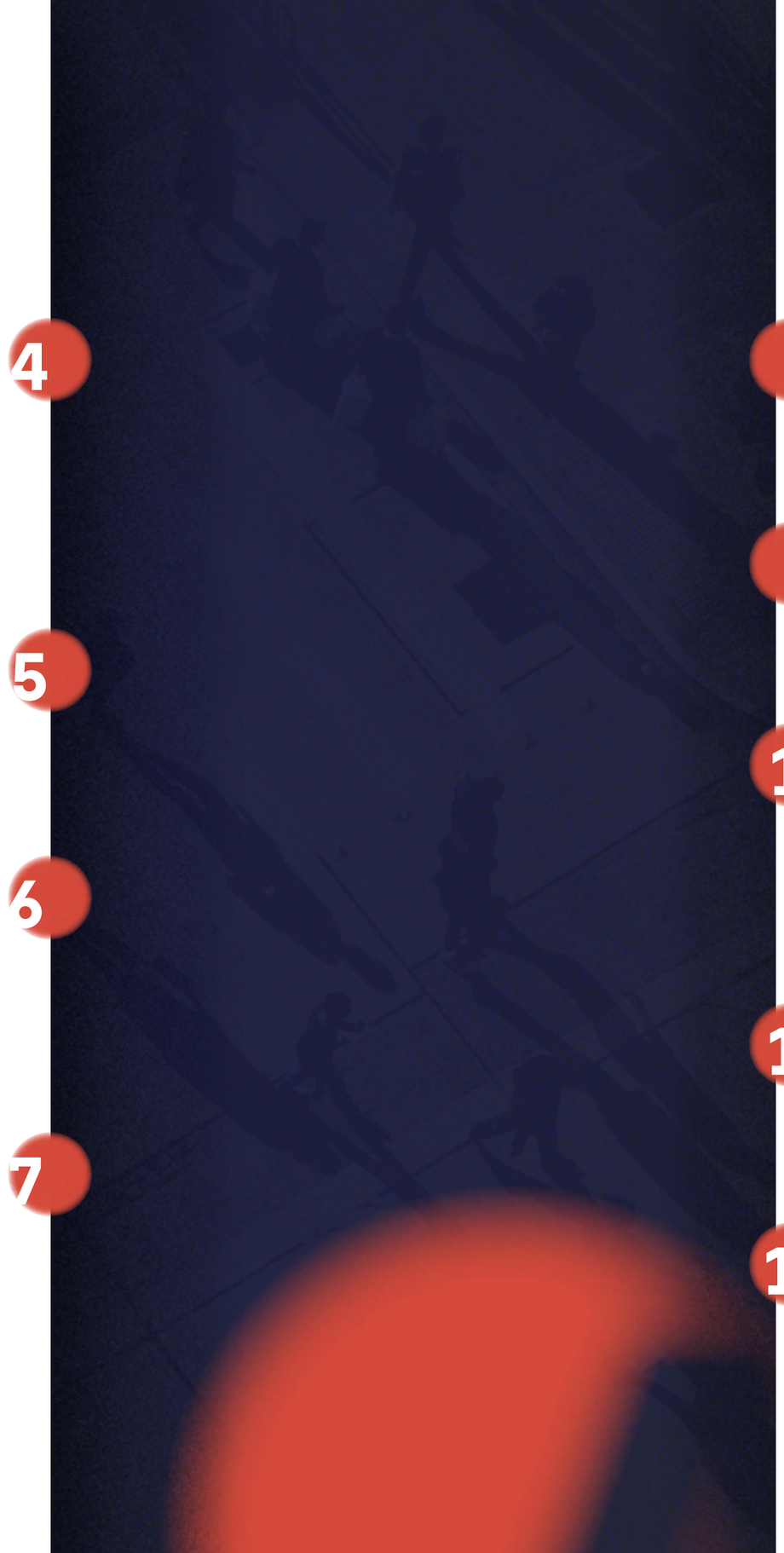
SUPPORT TO CITIZENS

Launch cyber toolkits for citizens. Some national cybersecurity agencies offer useful toolkits which provide citizens with the right tools to stay safe online, as in Belgium or the UK. Cyber toolkits for citizens should include quizzes to help citizens identify phishing attacks and other attacks, offer advice and solutions on what to do if data or accounts are compromised, and indicate where to find further information. The toolkits should be action-oriented, with easy-to-follow steps and easy-to-implement solutions.

Create and promote measures to ensure high cybersecurity standards in all products. Recent developments such as the EU certification schemes or Cyber Resilience Act are important first steps towards this. Further measures will need to be developed to match the evolution of technology and products and ensure that they continue to comply with high standards.

Require digital service providers to increase transparency about their security and privacy practices. Digital service providers, including internet service providers, have some discretion as to what information they can collect and store and what they can do with it, especially if they operate outside the EU. Citizens must be able to trust that when they connect to the internet and use technologies, they are safe. These providers should thus be more transparent about their privacy and security practices.

Create a Cyberscore. Based on the Nutriscore model, a Cyberscore should be developed to offer a multi-coloured label to assess the level of cybersecurity of the product. This could provide an easily readable indication to citizens about the safety of a product and to allow them to make well-informed purchases.



POLICY & OUTREACH

Develop an e-social contract. The development of an e-social contract could help to improve digital trust and encourage shared responsibility online. The terms of such a contract should be defined in consultation with all relevant stakeholders, including governments, industry, civil society organisations and citizens.

Adopt and implement the Cyber Resilience Act and future regulations expediently. Member States have different transposition and implementation processes for EU regulations, which can result in uneven implementation. This can put citizens at risk. Member States should implement EU cybersecurity policies swiftly.

Improve threat information sharing between governments, industry and citizens. Relevant government agencies should continue to inform industry of new threats and trends, but also directly inform citizens. Belgium, for example, offers a cyber newsletter which informs citizens of cybersecurity threats, similarly to severe weather threats. This practice should be broadened across the EU, and would go a long way to both improve citizens' awareness of cyberthreats and ultimately lead them to up their protection.

Provide funding to support stakeholders to comply with legislation and the introduction of new standards. The development of cybersecurity certification schemes and the introduction of new standards often represents a financial burden on product providers and consumers. Funding should be made available to allow stakeholders to keep up and comply with legislative requirements.

Promote a local approach to implementing cybersecurity strategies. Local authorities are the closest to citizens and have a key role to play in involving the latter in cybersecurity efforts. Local authorities must be empowered by EU, national and regional authorities for that "last-mile" communication to citizens.

INTRODUCTION

The European Union (EU) has fully embraced its "Digital Decade" geared towards the full digitalisation of its Member States by 2030. The precondition to a safe digital society is the cybersecurity of both organisations and citizens.

The COVID-19 pandemic significantly sped up Europe's digitalisation. It brought with it a significant increase in cyberattacks of 81%. The war in Ukraine pushed cybersecurity firmly up the agenda, with Russia's hybrid warfare tactics.

How can citizens be better protected in this changing landscape? Who is responsible for protecting citizens, and how can the latter be empowered to become the strongest rather than the weakest links?

The EU has developed a strong security and privacy regulatory landscape. From the 2016 General Data Protection Regulation (GDPR) to the most recent Cyber Resilience Act (2022), the EU is setting global standards for guaranteeing citizens' online security, data, privacy.

Efforts to create a secure digital environment go beyond the EU regulatory framework, encompassing contributions from Member states, industry, and civil society. Yet despite cybersecurity regulations, tools and initiatives, **there remains a gap in governments' and individuals' approach to cybersecurity.** An exclusive survey conducted by FIC on **European citizens' cybersecurity awareness** in France, Germany, the UK, Italy and Poland revealed that 51% had experienced a cyber-attack, yet two-thirds of respondents had never seen a cybersecurity awareness campaign[2]. These results reveal a clear disconnect and a need for citizen-centric cybersecurity frameworks.

Cybersecurity is the *sine qua non* condition of European digital sovereignty, and citizens hold the key to cybersecurity. Some EU member states have recognised this and put in place extensive awareness programmes and citizen-centric tools designed to help individuals improve their cybersecurity. But this approach is far from universal and governmental awareness-raising programmes are not enough. Industry too must play a greater role in ensuring citizens' cybersecurity and privacy. Only a comprehensive, strategic vision centred on the citizen can enable them to take greater control of their cybersecurity.

To develop such a vision, it is first necessary to understand what the EU, Member States, industry, and civil society organisations do to protect citizens. This paper examines existing regulatory frameworks, cybersecurity trends, specific initiatives and tools and analyses how citizens perceive cybersecurity and their ability to protect themselves online. It offers a series of recommendations to place citizens at the heart of national and European cybersecurity strategies.

2. OpinionWay survey for the FIC conducted in September 2022, URL.

HAVE YOU EVER BEEN THE VICTIM OF ANY OF THE FOLLOWING CYBER-ATTACKS?

	FRANCE	GERMANY	UNITED KINGDOM	ITALY	POLAND
Has already suffered at least one attack	**48%**	**49%**	**51%**	**57%**	**51%**
An online scam such as phishing	12% 29%	11% 31%	15% 32%	24% 47%	8% 28%
Online harassment	3% 10%	9% 25%	12% 26%	5% 15%	8% 27%
Theft of personal data	4% 18%	8% 24%	8% 25%	3% 18%	3% 18%
Cyber-extortion	5% 14%	7% 22%	5% 17%	3% 14%	7% 20%
Theft of banking information	3% 17%	7% 21%	7% 17%	- 9%	2% 13%

The survey was conducted by Opinion Way for the FIC from August 26 to September 5, 2022, URL

Yes, several times

Subtotal Yes

51%
of respondents have already been victims of a cyber-attack

WHERE DOES THE BUCK STOP? PROTECTING CITIZENS' ONLINE SAFETY

Cybersecurity regulatory frameworks have tended to focus on the protection of governments and critical infrastructure. In the European Union, these policies are national and supranational in nature, which complicates the regulatory environment and can be a burden for businesses and citizens.

THE EUROPEAN UNION APPROACH

Cybersecurity protection and resilience are at the top of the EU's digital policy agenda. The EU has strived to strengthen its regulatory framework since 2013[3]. This framework rests on several key regulations, which encompass:

- **Cybersecurity:** regulations governing the protection of networks and systems, and
- **Data protection:** regulations governing the protection of personal data.

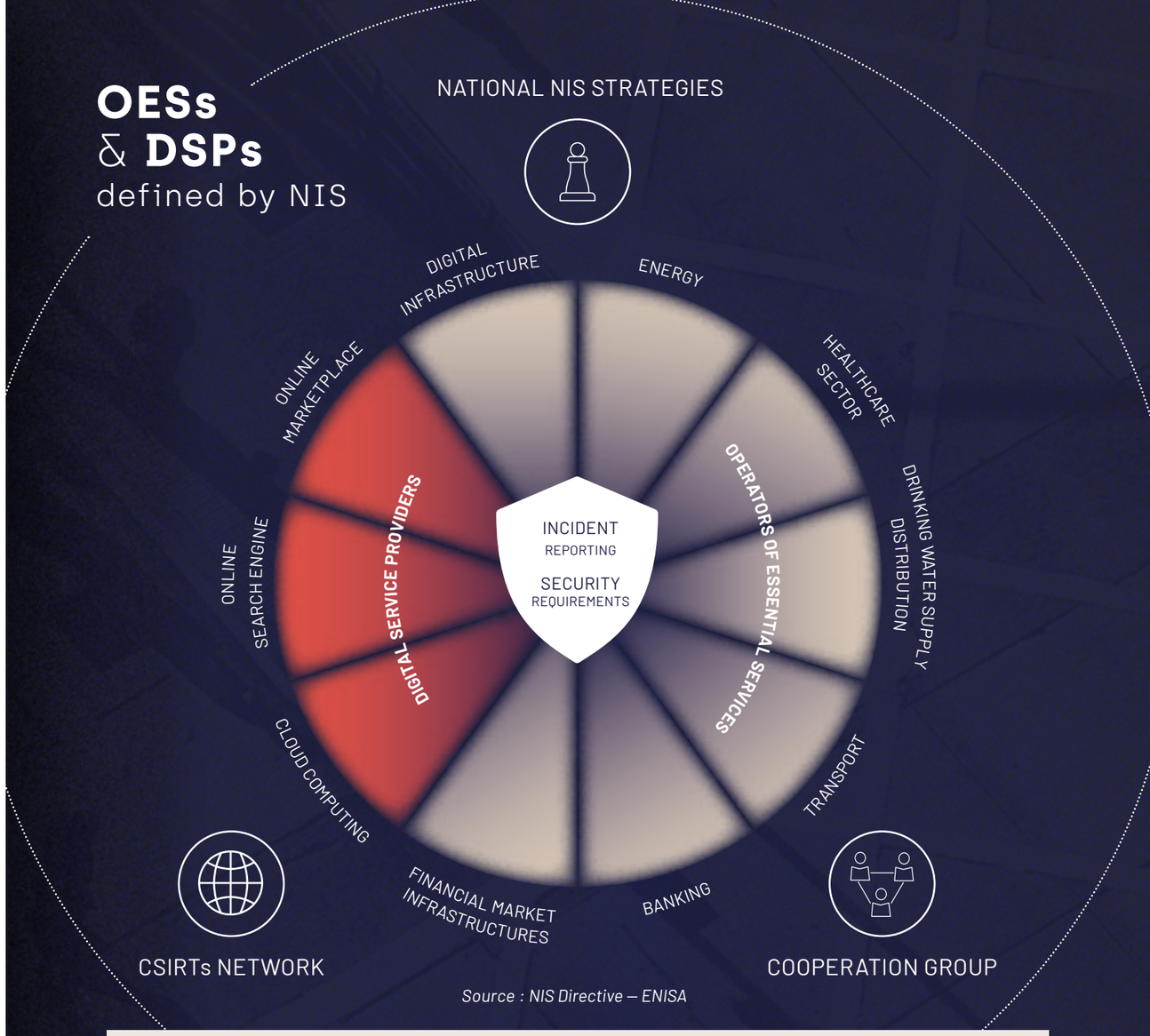
CYBERSECURITY

NETWORK AND INFORMATION SECURITY DIRECTIVE

NIS
[2016]

The 2016 Network and Information Security (NIS) Directive[4] is the first European regulation to enforce a minimum level of cybersecurity in the EU to improve the overall cyber resilience of EU Member States (MS)[5]. It requires Member States to develop a cybersecurity strategy, be adequately equipped to deal with cyber threats, establish a national cybersecurity authority and appoint a national CSIRT[6]. The NIS Directive also aims to strengthen cooperation between Member States with the creation of the NIS Cooperation Group and the network of CSIRTs, and to promote a culture of cybersecurity in critical infrastructure sectors. Specifically, the NIS Directive distinguishes between **'operators of essential services' (OESs) and 'digital service providers' (DSPs).**

3. The European Cybersecurity Market, Enterprises Ireland, URL.
4. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, URL.
5. Ibid
6. Computer emergency response team: a group of experts responsible for managing computer security incidents.



Source : NIS Directive – ENISA

Under the NIS, OESs and DSPs must:

- **Secure their network and information systems** by adopting technical and organisational measures appropriate to the risk
- **Ensure continuity of service** by taking appropriate measures to prevent and minimise the impact of security incidents
- **Notify the competent national authority of any security incident** that has a significant impact on the continuity of essential services provided[7] [8].

MS were responsible for determining what constitutes an OES in their country, which led to differing national interpretations[9] and to a fragmentation in the European market[10].

7. There is no specific EU directive regarding incident reporting threshold, each Member States implement here its guidelines to national OESs & DSPs.
8. The EU NIS Directive, IT Governance, URL.
9. Briefing on the NIS2 Directive: A high common level of cybersecurity in the EU, Negreiro, URL.
10. NIS Directive, IT Governance, URL.

SECOND NETWORK AND INFORMATION SECURITY DIRECTIVE

NIS2

(2022)

The proposal for the NIS2 Directive (2020)[11] was motivated by the increase in the number of cyber-attacks, a growing digital interconnection in the EU and beyond and to better reflect the reality of essential digital services[12]. The NIS2 was introduced to clarify and broaden the scope of the first NIS. NIS2 codifies a regime of obligations and sanctions for essential services providers, expands the number of public and private organisations which must improve their security levels, addresses supply chain security, streamlines reporting obligations, and introduces stricter enforcement requirements and oversight[13].

NIS2 replaces OESs and DSPs with two new categories: **'essential' entities** and **'important' entities**[14]. Essential entities include the OESs covered by the first NIS (energy, transport, banking, finance, market infrastructure, health, drinking water and digital infrastructure) and additionally entities in the wastewater, public administration (such as cloud and data centre providers, Internet exchange point providers, top-level domain name registries) and space sectors[15]. Important entities correspond to operators in the postal and courier services, waste management, chemical manufacturing, production and distribution, food production, processing and distribution, and digital suppliers (such as providers of social networks and service platforms, online marketplaces and search engines) sectors[16].

11. Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, URL.
12. Briefing on the NIS2 Directive: A high common level of cybersecurity in the EU, Negreiro, URL.
13. Ibid
14. Cybersecurity in the EU – Why we need NIS2 and what changes does it mean for the tech sector?, EURACTIV, URL.
15. EU Country Commercial Guide - Cyber Security, International Trade Administration, URL.
16. Ibid

COMPARING NIS AND NIS2 DIRECTIVES

	NIS (2016)	NIS (2022)
Objectives	> Increase the overall level of cybersecurity and cyber resilience in the EU > Harmonise the level of cybersecurity between MS by ensuring a minimum level of cybersecurity > Ensure that MS and companies are properly equipped to deal with cyber threats > Strengthen cooperation between MS in the field of cyber security > Promote an EU-wide culture of cybersecurity in selected critical sectors providing essential services	> Strengthen cyber resilience across the EU by extending the scope of the Directive in terms of sectors and businesses covered and by limiting fragmentation due to differences in interpretation between MS > Reduce inconsistencies and fragmentation to improve and strengthen harmonisation, security and incident reporting requirements, monitoring and MS cyber security capabilities > Improve cooperation and information sharing
Designation of entities	'Operators of essential services' (OESs) 'Digital service providers' (DSPs)	'Essential entities' 'Important entities'
Sectors covered	**OESs:** Digital infrastructure, energy, healthcare sector, drinking water supply and distribution, transport, banking, financial market infrastructures **DSPs:** Cloud computing, online marketplace, online search engines	**Essential entities:** Existing OES (energy, transport, banking, finance, market infrastructure, health, drinking water and digital infrastructure sectors) + wastewater, public administration (such as cloud and data centre providers, Internet exchange point providers, top-level domain name registries) and space sectors **Important entities:** Postal and courier services, waste management, chemical manufacturing, production and distribution, food production, processing and distribution, and digital suppliers (such as providers of social networks and service platforms, online marketplaces and search engines)
Outcomes	Establishment of cybersecurity strategies, national cybersecurity authorities and CSIRTs in EUMS Improvement of overall level of cybersecurity in the EU Establishment of NIS Cooperation Group and Network of CSIRT	*Foreseen:* Improved harmonisation in interpretation and implementation of directive, reduction of fragmentation Improved level of cybersecurity and cyber resilience of the EU Improved information-sharing and cooperation among MS Strengthening of existing group and network and establishment of the EU-CyCLONE network to support coordination and management of large-scale incidents[17]
Negative impact	Fragmentation due to differences in national interpretation of the directives[18]. (Eg: differences in classification of OES MS) Lack of effective supervision and enforcement regime[19] Limited information sharing among MS[20]	*Foreseen:* Unequal implementation of first NIS means uneven playing field for implementation of NIS2 New obligations will burden organisations unless the new NIS is combined with effective support

The NIS2 is set to be adopted by the European Parliament in October 2022, with the transposition into national law of the Member States to take place in 2024[21].

17. Briefing on the NIS2 Directive: A high common level of cybersecurity in the EU, Negreiro, URL.
18. Ibid
19. Ibid
20. Ibid
21. Review of the Directive on security of network and information systems, European Parliament Legislative Train, URL.

CYBERSECURITY ACT

[2019]

The EU Cybersecurity Act[22] was adopted in 2019 to support and advance the provisions of the 2016 NIS Directive. The Cybersecurity Act creates a legal framework for the EU's Digital Single Market (DSM), to remove existing barriers between Member States in the digital sector and encourage transborder business transactions[23]. It strengthens the mandate of the European Union Agency for Cybersecurity (ENISA) and introduces a mechanism for a European cybersecurity certification framework for information and communication technology (ICT) products, services and processes, defined as[24]:

ICT PRODUCT

An element or a group of elements of a network or information system

ICT SERVICE

A service consisting fully or mainly in the transmission, storing, retrieving or processing of information by means of network and information systems

ICT PROCESS

A set of activities performed to design, develop, deliver or maintain an ICT product or ICT service.

The European Cybersecurity Certification Framework issues certifications recognised throughout the EU, allowing ICT products, services and processes to be certified only once for the entire European market[25]. These certifications provide a minimum level of cybersecurity protection for ICT solutions and aim to promote trust in EU cybersecurity solutions. Certifications are issued by National Cybersecurity Certification Authorities (NCCAs) appointed by MS to oversee the compliance of the certificates[26].

For the time being, certification of ICT products, services and processes remains voluntary[27] but could become mandatory for high-risk ICT products, services and processes by 2023[28].

Three EU certification schemes are currently under development:

- **Common Criteria-based European candidate cybersecurity certification scheme (EUCC):** based on the existing Common Criteria international scheme, the Common Methodology for Information Technology Security Evaluation, and the corresponding standards ISO/IEC 15408 and ISO/IEC 18045[29]. A first version was delivered to the European Commission in May 2021 but remains to be approved to be effective[30].
- **European Cybersecurity Certification Scheme for Cloud Services (EUCS):** the scheme is still being developed following public consultations which ended in February 2021. There currently remains robust discussions on the text of the scheme among Member States, particularly with regards to the sovereignty requirements which would prevent and limit possible interference by non-EU Member States with certified cloud services[31][32][33].
- **European 5G Cybersecurity Certification (EU5G):** the scheme is still under development. An Ad Hoc Working Group (AHWG)[34] - a group of stakeholders led by ENISA to share their expertise and help create certification schemes - was established in October 2021 to elaborate the scheme[35].

22. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing regulation (EU) no 526/2013 (Cybersecurity Act), URL.
23. The European Cybersecurity Market, Enterprises Ireland, URL
24. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing regulation (EU) no 526/2013 (Cybersecurity Act), URL.
25. The EU Cybersecurity Act, European Commission, URL.
26. EU Cybersecurity Certification - FAQ, ENISA, URL.
27. Understanding the EU Cybersecurity Act and Its Effect on Businesses Dunkelberger, URL.
28. The European Cybersecurity Act, EUROSMART, URL.
29. Cybersecurity Certification: Candidate EUCC Scheme V1.1.1, ENISA, URL.
30. Public Consultation on the draft Candidate EUCC Scheme, ENISA, URL.
31. Consultation on the draft of the candidate Certification Scheme on Cloud Services (EUCS) - Closed, ENISA, URL.
32. Germany calls for political discussion on EU's cloud certification scheme, Bertuzzi, URL.
33. Sovereignty requirements remain in cloud certification scheme despite backlash, Kabelka, URL.
34. Ad-hoc Working Group calls, ENISA, URL.
35. Ad-Hoc Working Group 03 - on 5G Cybersecurity Certification, ENISA, URL.

CYBER RESILIENCE ACT

[IN PROCESS]

The Cyber Resilience Act, introduced in September 2022, is the latest piece of regulation to complete the European cybersecurity legislative arsenal[36].

The aim of the Cyber Resilience Act is to establish common standards for cybersecurity products, to harmonise policies and further strengthen the EU's normative cybersecurity power[37]. The Cyber Resilience Act will provide rules and obligations for manufacturers and vendors to meet market needs and protect consumers[38], through the introduction of provisions on conformity assessment or on market surveillance, for instance[39].

The objectives of the European Commission are threefold[40]:

1. Enhance and ensure a consistently high level of cybersecurity of digital products and ancillary services
2. Enable users to match the security properties of such products against their needs, including by enhancing the transparency of cybersecurity features to protect users from insecure digital products and ancillary services, and incentivise vendors to offer more secure products, thus increasing the trust in the digital single market
3. Improve the functioning of the internal market by levelling the playing field for vendors of digital products and ancillary services.

The proposed Cyber Resilience Act would guarantee:

1. Harmonised rules when bringing to market products or software with a digital component
2. A framework of cybersecurity requirements governing the planning, design, development and maintenance of such products, with obligations to be met at every stage of the value chain
3. An obligation to provide duty of care for the entire lifecycle of such products[41].

The EU Council and European Parliament are yet to deliberate. After adoption, Member States will have 24 months to transpose the regulation into national legislation.

36. Cyber Resilience Act, European Commission, URL.
37. The new European Cyber Resilience Act, European Parliament Train Schedule, URL.
38. Cyber resilience act - new cybersecurity rules for digital products and ancillary services, European Commission, URL.
39. Ibid
40. Ibid
41. EU Cyber Resilience Act, European Commission, URL.

IMPACTS OF EUROPEAN CYBERSECURITY REGULATIONS ON THE PROTECTION OF EU CITIZENS

EU cybersecurity regulations may not be aimed directly at citizens, but they have a direct positive impact on their protection. EU regulations raise the general level of cybersecurity in Member States and ensure a minimum level of security in solutions used by citizens. The NIS and NIS2 Directives, for example, secure the critical infrastructure which provides essential services to European citizens, while European certifications ensure the safety of products used by citizens.

DATA PROTECTION

GDPR

[2016]

In 2016, the EU adopted one of the most comprehensive data protection and privacy regulations in the world. The General Data Protection Regulation (GDPR)[42] strengthens individuals' rights and control over their personal data by imposing obligations on organisations, wherever they are located, when targeting or collecting data on individuals in the EU. The GDPR introduces provisions and requirements related to the processing of individuals' personal data and imposes significant fines on organisations which fail to meet privacy and security standards[43]. The GDPR has been a source of inspiration for the governance of personal data around the world and demonstrates the EU's normative power and its ability to set and promote international standards in line with its values.

THE GOVERNMENTAL APPROACH

Governments have a duty to protect their citizens, including in cyberspace. National regulatory frameworks directly impact how citizens navigate online environments and aim to protect populations from both state-sponsored and criminal cyber threats. Most country-level regulations however prioritise the protection of essential organisations over citizens in the belief that if these businesses are secure, citizens will be protected.

PROTECTING CRITICAL INFRASTRUCTURE

The protection of essential organisations and critical infrastructure important to ensure that citizens' data is protected and that they can operate online safely. EU regulations define the responsibilities of essential services, but what is the state of play beyond the EU, in a globally connected world? Some countries have amended existing regulations to define essential services and digital service providers, while others have adopted new legislation to define cybersecurity and reporting requirements, making it complex for providers to understand their obligations and for citizens to understand levels of protection. In most countries, citizens are absent from policies. The United States and Israel offer interesting comparative case-studies to the EU landscape.

IMPACT OF GDPR
ON THE PROTECTION OF EU CITIZENS

One of the most visible impacts of the GDPR is the requirement to store any data collected in the EU and to limit unauthorised transfer or use of that data. 65% of respondents to the FIC survey believe their data is safe when stored in the EU[44]. This is in stark contrast to the US, where 85% of respondents to an Ipsos survey in 2022 said they were concerned about the security and privacy of the data they share online[45]. The GDPR has undoubtedly played a role in making European citizens more secure online by setting high standards for privacy protection. The adoption of regulations modelled on the GDPR beyond the EU is a testament to Europe's normative power and its ability to promote data subject rights globally.

42. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/ec (General Data Protection Regulation), URL.
43. What is GDPR, the EU's new data protection law?, GDPR.EU, URL.
44. OpinionWay survey for the FIC conducted in September 2022, URL.
45. A majority of Americans are concerned about the safety and privacy of their personal data, Ipsos, URL.

UNITED STATES OF AMERICA

In the U.S., the Cybersecurity and Infrastructure Security Agency (CISA) within the Department of Homeland Security is responsible for setting cybersecurity policy[46]. CISA not only secures the federal government's online domains but also coordinates and sets policy for the security of essential services. In this role, CISA focuses strongly on working with private sector partners to ensure that any regulations or recommendations are feasible and business-friendly in a way that strengthens their cyber resilience but does not place an undue burden on businesses.

Beyond this, the U.S. regulatory landscape is still largely developing. Several recent policies help define the cybersecurity obligations of essential and digital service providers. Most notably, the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)[47] establishes robust reporting requirements. However, the specific requirements must still go through the public rulemaking process. Some pushback from industry against additional regulations can be expected during the process, which could result in exceptions or the weakening of the requirements. The final rule may not be available until 2025.

ISRAEL

Israel is globally recognised as a leader in technology and cybersecurity. Its regulatory landscape is nearly as complex in the U.S., in part because of how cybersecurity responsibilities are split between different government bodies. The primary cybersecurity regulatory body is the Israel National Cyber Directorate (INCD), responsible for the protection of essential services. The INCD was established in 2018 with the merging of the National Cyber Security Authority (NCSA), which was the operative body for cyber protection, and the National Cyber Bureau (INCB), which was responsible for policies and the cyber force build-up[48].

Critical infrastructure protection has been a cybersecurity priority for Israel for nearly 30 years. The government passed Special Resolution B/84 in 2003[49], which defines critical infrastructure and mandates such organisations to have dedicated IT-security personnel[50]. In addition, Israel has two other key laws defining the cybersecurity regulatory framework, including the 1995 Computer Law (amended in 2012) and the 2018 Privacy Protection Regulations (Data Security) 5777-2017. Together, these define requirements for protecting critical infrastructure similar to those of the EU's NIS Directive.

46. Cybersecurity, CISA, URL.
47. PUBLIC LAW 117-103—MAR. 15, 2022, American Congress, URL.
48. Cyber force refers to the responsibility to develop a national cyber defence. See more here.
49. Israel Defense Forces and National Cyber Defense, Tabansky, URL.
50. Critical infrastructure sectors in Israel include the 11 sectors defined in the NIS Directive plus the following: Food Supply and Distribution, Government, Public Safety, and Law Enforcement.

HOW DOES THE PROTECTION OF CRITICAL INFRASTRUCTURE IN EUROPE COMPARE TO ISRAEL AND THE US[51]?

Israel makes a clear distinction between the roles of civilian agencies and the military in protecting Israeli cyber space. Furthermore, the Israeli government is well aware of the need to protect individual liberties and has prioritised that since the Snowden leaks of 2013[52].

The American regulatory system is both more complex and less stringent than the EU's, in large part because of the federal system. This not only requires a whole-of-government response to address cybersecurity, but also a whole-of-nation response, including support and implementation at local levels.

Some industry sector-specific reporting requirements precede federal requirements, and companies may face state-level obligations in addition to federal ones[53]. While it is clear which organisations fall under the "critical infrastructure" designation[54], the regulatory framework remains opaque as specific obligations to protect critical infrastructure and their customers' data are not firmly defined. Current regulations allow for the development of digital profiles of citizens, which are regularly sold to digital advertisers, leaving data vulnerable to hackers.

51. This report compares Israeli and American regulations to the NIS, NIS2 having yet to come into force.

52. Israel Defense Forces and National Cyber Defense, Tabansky, URL.

53. One example is the 2014 Federal Information Security Modernization Act (FISMA).

54. Critical infrastructure organisations in the US are defined as follows: see here.

COMPARING CYBERSECURITY
IN THE EU, THE U.S. AND ISRAEL

FACTOR	EU NIS	US FRAMEWORK	ISRAEL FRAMEWORK
Incident response – CERT/CSIRT	Requires Member States to be appropriately equipped. For example, with a Computer Security Incident Response Team (CSIRT) and a competent national NIS authority.	Federal Information Security Modernization Act of 2014 (FISMA 2014) codifies the US-CERT as a function of DHS.	Resolution 2444, *Advancing the National Preparedness for Cyber Defense* establishes the National Cyber Security Agency (NCSA) which is charged with maintaining Israel's CERT.
Cooperation	Ensures cooperation among Member States by setting up a Cooperation Group to support and facilitate strategic cooperation and the exchange of information.	The Cybersecurity and Infrastructure Security Agency Act of 2018 makes cooperation and information sharing a core duty of CISA. The Executive Order on Improving the Nation's Cybersecurity (2021) increases information sharing between federal IT service providers (contractors) and impacted government agencies.	No official regulation for cooperation. But Israel prioritises multi-stakeholder cybersecurity cooperation among government, academia, and private sector entities. This can be seen through the CyberSpark Initiative that helped transform Be'er Sheva into a major cyber centre.
Critical infrastructure identification and classification	Imposes targeted organisations to take appropriate security measures and notify serious incidents to the relevant national authority.	Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) sets reporting requirements; final rules still in development. Computer Security Incident Notification Requirements for Banking Organisations and Their Bank Service Providers (2021) sets reporting requirements for the banking sector.	Privacy Protection Regulation (Data Security) determines that owners of databases designated within an "intermediate" or "high" tier of security are required to notify data breaches to the PPA (Israel's Privacy Protection Act, which is implemented by the Privacy Protection Regulation).
Purposes	Prevents risks and ensures security of network and information systems.	The Federal Information Systems Modernization Act (FISMA) 2014 establishes CISA's central role in the security of the information and information systems of federal, executive-branch, and civilian agencies. There is no private-sector equivalent policy to date. CISA is responsible for information sharing with the private sector and is responsible for the cybersecurity of critical infrastructure.	Privacy Protection Regulation (Data Security) requires anyone who owns, manages or maintains a database containing personal data to implement various information security practices, including registering the database, maintaining security controls, and adhering to other regulations.

PROTECTING DATA AND PRIVACY

> **The GDPR has had far reaching impacts on better data privacy protection globally**

The inclusion of the right to privacy in the European Convention on Human Rights sets the foundation for a citizen's right to digital privacy in the EU. The GDPR enshrines this right throughout the European Union, extending the requirement to protect user data to all companies operating in the EU, even if located elsewhere. The GDPR has had far reaching impacts on better data privacy protection globally[55]. The variety of approaches to privacy regulation outside the EU can be confusing for users however.

HOW IS CITIZEN PRIVACY PROTECTED OUTSIDE THE EU?

Regulatory frameworks on data protection and privacy around the globe differ widely[56]. Some countries have modelled their laws on the GDPR, using the GDPR's eight core user rights[57]:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

Israel and Canada stand out as strong on cybersecurity, but appear comparatively weaker on citizens' privacy. Israel only confirms the rights to access, correct, and delete one's information. Canada goes slightly further by also allowing for the right to restrict processing. Yet neither confirms the right to data portability, sets an age limit on consent in national privacy legislation, nor provides any rights not to be subject to fully automated decisions.

The United States also stands out in that no single privacy policy exists at the federal level. Some policies in place address personal health information[58], personal banking information[59], and the online privacy of children[60]. But for the most part, privacy protections have been enacted at the state level. California, Colorado, Utah, and Virginia have adopted and are in the process of implementing privacy acts similar to the GDPR, including generally the same protections for individual data privacy rights. But because of a fractured privacy framework[61], US companies have been slow to adopt measures, and data privacy remains secondary to business interests.

THE PRIVATE SECTOR APPROACH

The cyber threat landscape has expanded drastically and citizens have limited options to control what data they share and limit their vulnerability online. Manufacturers and providers have a responsibility to design products and services with citizens' security and privacy in mind.

Smart devices have brought about a new layer of vulnerability. Smart watches, fitness trackers, doorbells, speakers or virtual assistants can lead to loss of data, including passwords or images. This data can be used to compromise interconnected devices or could be sold to criminal actors. In addition, citizens often share more data than they realised and may unknowingly give their consent for the manufacturer or service provider to sell the data. This can create an unwanted public profile of a person, which can be manipulated and misused.

There is however a growing consensus on best practices and solutions to improve the protection of users and citizens.

55. What is GDPR, the EU's new data protection law?, GDPR.EU, URL.
56. Global Comprehensive Privacy Law Mapping Chart, IAPP, URL.
57. What is GDPR, the EU's new data protection law?, GDPR.EU, URL.
58. Your rights under HIPAA, US Department of Health & Human Services, URL.
59. The Right to Financial Privacy Act, EPIC, URL
60. Children's Online Privacy Protection Rule («COPPA»), US Federal Trade Commission, URL.
61. Divided we fall: Why fragmented global privacy regulation won't work, Kieran, URL.

SECURITY

PROBLEM

In today's world of remote work, reliance on cloud computing, and professional use of personal devices, traditional means of securing IT systems (e.g. via a company VPN or firewall) is no longer enough. The "security perimeter" has shifted.

BEST PRACTICE

ZERO TRUST ARCHITECTURE[62]: Zero trust architecture (ZTA) shifts the focus away from static perimeters around physical networks toward users, assets, and resources, mitigating the risk of decentralised data. It is built on the principles of «zero trust», which means that it is conceived to prevent data breaches by limiting internal lateral movements[63]. Access is more granularly enforced: even if internal users have access to the data environment, they may not have access to sensitive data.

SECURITY

PROBLEM

Security has long been an afterthought in the design of software and hardware. This leads to weaker products which are more vulnerable to attacks and breaches.

BEST PRACTICE

SECURITY BY DESIGN: This practice implies manufacturers integrating security features into both software and hardware from the beginning. In essence, security by design should follow these general principles[64].

- The context should be established to determine all the elements that compose the system, so defensive measures have no blind spots.
- The system should be designed to make compromise difficult. Manufacturers must also make disruption difficult, by designing a system that is resilient to denial-of-service (DoS) attacks and usage spikes. The system should be designed to facilitate the detection of compromise and to identify suspicious activity as it occurs.
- The system must be designed in such a way that, if an attacker manages to gain a foothold, the impact of the compromise is reduced.

Apple has for example developed security-focused hardware which follows the principle of supporting limited and discretely defined functions to minimise the attack surface[65]. Apple couples hardware with system security which ensures the system and data are not vulnerable during upgrades.

Citizens are the weakest link in cybersecurity, and security by design can go a long way to improving their protection.

SECURITY & PRIVACY

PROBLEM

Too much personal information and valuable data is stored in plaintext, making it easier for hackers to steal, use or sell data after breaches.

BEST PRACTICE

DATA ENCRYPTION & SANDBOXING: Encryption can make it harder for hackers to access data after a breach, while sandboxing the data limits access to data. Encryption is critical, particularly with many devices now using personally identifiable information (PII) including biometrics. Sandboxing data implies the implementation of select permissions which limits who can access what data, limiting exposure in case of a cyberattack.

While citizens may not need to understand the details of encryption or sandboxing, they should be made aware of the added-value of these practices to their security.

SECURITY & PRIVACY

PROBLEM

Many IoT devices have default passwords and citizens may not know that they need to change these. Weak passwords continue to be the number one way to access and steal data.

BEST PRACTICE

UNIQUE PASSWORDS AND MULTI-FACTOR AUTHENTICATION (MFA): Industry could improve citizens' protection by removing default passwords on devices and requiring that unique passwords are used. MFA adds an extra layer of security which makes it harder for an attacker to access an account or a device.

62. Le modèle Zero Trust, ANSSI, URL.
63. Zero Trust Architecture, Rose et al., URL
64. Secure design principles, UK National Cyber Security Centre (NCSC), URL.
65. Hardware security overview, Apple, URL.

PRIVACY

PROBLEM

Companies collect and use citizens' data for purposes other than strictly necessary, including selling or leveraging it for marketing purposes.

BEST PRACTICE

GDPR[65] & CITIZEN-CENTRIC PRIVACY POLICIES: Complying with GDPR implies:

- Ensuring the "right to be forgotten", meaning that citizens can control their data and request that it be deleted
- Storing data only in countries that have implemented GDPR, and therefore respect the right not to sell the citizen's data.

For citizens, a weaker privacy policy means their data is used often without their knowledge, in turn leading to a risk of exposure to data theft. Citizens can use GDPR-compliant VPN services, which are less likely to log unnecessary information and which will limit the information that their ISP can collect. But VPNs can add an additional cost and burden to citizens.

For social media specifically, platforms like Facebook have instituted some additional privacy controls for citizens, but they are complicated, hard to access, and there remains mistrust that the platform will limit tracking and respect the rights of citizens.

PRIVACY

PROBLEM

For too long, data privacy has been a secondary concern in the development of information systems. This has led to weak privacy practices and solutions that are retrofitted to the technology.

BEST PRACTICE

PRIVACY BY DESIGN AND BY DEFAULT: Just like security by design, privacy by design means that privacy protection is taken into account from the design stage of IT systems and procedures. It ensures for instance that products are GDPR-compliant and that data subjects' rights are protected.

Privacy by default implies that any entity processing personal data ensures that it is not processed unnecessarily. For example, a social media's default setting should make sure that no more information than strictly necessary is collected, shared or displayed. This protects citizens by ensuring that even when sharing PII or other valuable information, only the minimum is tracked, stored, or shared.

PROTECTING CITIZENS:
IS THE EUROPEAN UNION DOING ENOUGH?

European citizens may not be directly at the heart of the current EU and Member States' cybersecurity regulations, but they are safer and their rights are better protected than elsewhere in the world. While industry protections have improved, it is clear that more security can be built into devices and services which citizens use in their daily lives. The Cyber Resilience Act could be a good first step in guaranteeing the provision of an extra layer of protection. However, additional regulations will likely represent a significant compliance and financial burden for companies, and support should be made available to ensure rapid implementation.

66. Complete guide to GDPR compliance, GDPR.EU, URL.

DON'T BE A FOOL USE THE PROPER TOOL! EMPOWERING CITIZENS FOR ONLINE SAFETY

Despite a regulatory framework that has traditionally focused on governments and organisations, numerous initiatives have been launched to put citizens at the heart of cybersecurity.

The responsibility for cybersecurity cannot solely rest on governments and businesses. Citizens must play an active role in protecting and securing their own data and protect themselves from cyber-attacks. Should they fall victim to a cyber-attack, citizens should know what mitigation and response measures are available. Unfortunately, only one in three respondents of a recent FIC poll could recall seeing or hearing about a cybersecurity awareness campaign, meaning that most are likely unaware of the resources available to them to improve their cyber posture[67].

There is in fact a plethora of government, civil society and private-sector initiatives designed to help build a digitally secure society. These initiatives can be broken into two broad categories:

- **Prevention:** initiatives designed to help users prepare for and prevent a cyber-attack or data breach, and
- **Mitigation & response:** initiatives which help users respond and act in the event of a cyber-attack.

AN OUNCE OF PREVENTION IS WORTH A POUND OF CURE

The old adage "an ounce of prevention is worth a pound of cure" is true in cybersecurity. Most governments offer programmes to help train, inform, and protect citizens online. This is in addition to support they offer to businesses and critical infrastructure operators and owners.

67. OpinionWay survey for the FIC conducted in September 2022, URL.

NATIONAL GOVERNMENTS

Below is a selection of country-level government initiatives which seek to empower citizens.

FRANCE	BELGIUM	SPAIN	UNITED KINGDOM	USA
Awareness				
Hack Academy: A public interest initiative supported by ANSSI and the Ministry of the Interior which uses humour to train users on everyday cyber risks and how to protect against them.	**Cyber Security KIT:** This toolkit, created by the Cyber Security Coalition and the Centre for Cybersecurity Belgium, seeks to raise awareness in cybersecurity for SME's and other organisations	**Internet Security 4 Kids (IS4K):** This child-focused site by INCIBE and the Ministry of Economic Affairs and Digital Transformation and other partners has everything parents need to help keep their kids safe online. That includes guides (parental controls, online bullying, etc.), tools (quizzes and games), and more.	**Cyber Aware:** Advice on how to stay secure online from the UK's National Cyber Security Centre. Walks users through making their digital services more secure.	**Cybersecurity Awareness Program:** A national public awareness effort aimed at increasing the understanding of cyber threats and empowering the American public to be safer and more secure online.
Trainings				
CyberEdu: A training initiative launched by ANSSI, which aims to strengthen the consideration of digital security in all French higher education courses in computer science in order to build a more cyber aware society.		**Free Online Cybersecurity Courses:** Spain's INCIBE offers free cybersecurity courses for freelancers and micro businesses, and provides materials for teachers and parents. They also publish privacy and online security guides.		
Games				
	SafeonWeb.Be: One-stop cyber hub to find resources, tools, and more to help prevent cyber-attacks, and on what to do after a hack. Safeonweb also includes quizzes and checklists.	**Ciberemprende:** This programme by INCIBE seeks to attract innovative talent in cybersecurity by holding a competition of entrepreneurial ideas and projects in the seed phase to help them to develop their business ideas or projects.	**CyberSprinters:** A digital game for 7–11-year-olds which can be played on phones, tablets and desktops, and is supported by activities for educational practitioners. Parents and carers can also try the CyberSprinter puzzles with their children at home.	**President's Cup Cyber Challenge:** CISA leads and hosts the President's Cup to identify, recognise, and reward the best cyber talent across the US. Challenges are based on real-world situations from the National Initiative for Cybersecurity Education (NICE) framework to expand cyber skills through fun and creative tests.
Others				
ANSSI Security Visa: Lets users know when a product or service has been rigorously tested and approved by ANSSI	**SafeonWeb App:** The CCB has developed an app that lets users register their home networks and receive notifications if a threat has been detected. Users can also receive regular news updates that inform about general cyber threats in Belgium.		**Active Cyber Defence (ACD) Hub:** The ACD programme aims to reduce the damage caused by cyber-attacks by providing eligible users with tools and services that protect them against a range of attacks.	

INDUSTRY

Cybersecurity and technology companies have developed cybersecurity initiatives for their users, often as part of corporate social responsibility programmes. Some also offer free products (example: Bitwarden). Corporate initiatives tend to focus on training the next generation of cybersecurity professionals but also offer opportunities for those looking to change careers or learn new skills. Examples include:

TRAINING

- Orange CyberDefense #SuperCoders[68]: Orange organises workshops for children ages 9-14 to introduce them to coding. Through this programme, children learn the basics of coding, safe internet practices and how to act responsibly in the digital space.
- Samsung Solve for Tomorrow[69]: This STEM contest for middle and high school students in the U.S. encourages participants to solve problems in their communities using technology. This programme drives community engagement and encourages investment in STEM education to help build a stronger workforce for the future. Students also receive a foundational education in technology, which includes cyber best practices.
- Microsoft Philanthropies Technology Education and Literacy in Schools (TEALS)[70]: This programme builds sustainable computer science programmes in underserved high schools by helping teachers learn to teach computer science. In addition, Microsoft focuses on providing digital literacy training and providing digital and technology skills to help people excluded from the digital economy gain jobs and improve their livelihoods.
- Samsung Innovation Campus[71]: The Samsung Innovation Campus provides ICT education to students and unemployed youth. Along with core competencies such as AI, IoT, Big Data, Coding and Programming, the programme trains participants on a range of soft skills to foster talented youth who will go on to shape our future society.

TRAINING - WOMEN & MINORITIES

- Orange CyberDefense Women's Digital Centres programme[72]: This programme has developed "Digital Centres" in Europe and Africa to train women without qualifications or a job. Training lasts six months to one year, teaching vital skills like mathematics, writing, using computers and tablets, software and the internet. This programme helps fight the gender gap in tech and creates more digitally savvy citizens.
- Capgemini Digital Inclusion Programme[73]: This programme seeks to build a bridge between technology and society and works closely with NGOs, social innovation organisations and clients across four main streams: (1) Digital Literacy, (2) Digital Academy, (3) Tech4Positive Futures and (4) Advocacy & Thought Leadership. To support Digital Literacy, Capgemini provides access to devices and teaches digitally uninformed users basic digital skills to foster digital autonomy. This also helps users learn basic cybersecurity practices, like good password management.
- Google "Code with Google"[74]: Google's flagship programme expands computer science education among underserved communities.

ACCESSIBILITY

- Google Supporting "Newswise"[75]: Google is working with Newswise to provide media literacy training to young people to help them discern online misinformation, distinguish real versus fake sources of information, making them less likely to click on spam links and put their data at risk.
- Google Career Certificates[76]: Google supports online training programmes for job-ready skills in high-growth career fields such as Data Analytics, Digital Marketing & E-commerce, IT Support, Project Management, and UX Design. These are publicly available on Coursera.org, and help train participants in fields like IT Support and Data Analytics to learn data privacy and security skills.

In addition to the company-led programmes, some cybersecurity industry associations have launched initiatives related to awareness, youth training and gender parity. The European Cybersecurity Organisation (ECSO)[77] for example supports a variety of training and awareness programmes, including their Youth4Cyber initiative. This initiative seeks to raise the level of cyber hygiene and to stimulate an interest for cybersecurity careers in European youth through age-specific modules that can be tailored to the youth's needs and interests. Industry associations tend to concentrate their efforts on business-oriented initiatives that benefit their memberships.

68. #SuperCoders: Corporate Social Responsibility, Orange, URL.
69. Thriving together: Samsung CSR US, URL.
70. TEAL Program, Microsoft, URL.
71. Cultivate key human resources who will lead the 4th Industrial Revolution, Samsung, URL.
72. The Women's Digital Centres programme: actively supporting women's empowerment, Fondation Orange, URL.
73. Capgemini - Social, Capgemini, URL.
74. Code with Google, Google, URL.
75. Philanthropic initiatives for local communities, Google, URL.
76. Google Career Certificates, Google, URL.
77. European Cyber Security Organisation (ECSO) - About, ECSO, URL.

CIVIL SOCIETY ORGANISATIONS

A growing number of civil society organisations offer tools and initiatives to help users protect themselves against cyber threats.

These include, among others:

- ***Global Cyber Alliance (GCA):*** GCA offers various cybersecurity toolkits to make it easy to find and implement cybersecurity controls to help organisations and citizens defend themselves against cyber threats and provides trainings to help citizens improve their digital security and privacy. In addition, it has published a guide to implementing DMARC (Domain-based Message Authentication, Reporting and Conformance), available in 18 languages. GCA also has launched Quad9, a free service users can install to block access to malicious websites, helping to protect users from inadvertently exposing their data.
- ***National Cybersecurity Alliance:*** NCA offers several resources for users to improve their cybersecurity. They publish guides on everything from passwords and password managers to phishing and how to detect viruses on personal computer. NCA also provides training and career advice for those in the cybersecurity field, helping to build the cyber workforce in an attempt to address the growing gap of cyber professionals.
- ***Cyber Peace Institute:*** The Cyber Peace Institute offers cybersecurity solutions to non-profits to help protect them against cyber threats, for instance in the healthcare sector. CPI publishes the Cyber Incident Tracker (CIT) #HEALTH, to help identify and track the growing cyber threats to healthcare organisations.
- ***Center for Internet Security (CIS):*** CIS is best known for publishing the 18 Critical Security Controls®. These controls are generally designed to protect businesses, but some can be implemented by individuals to better protect their home systems and their personal data. The controls are best practices developed by a consortium of industry, academia, and government experts.

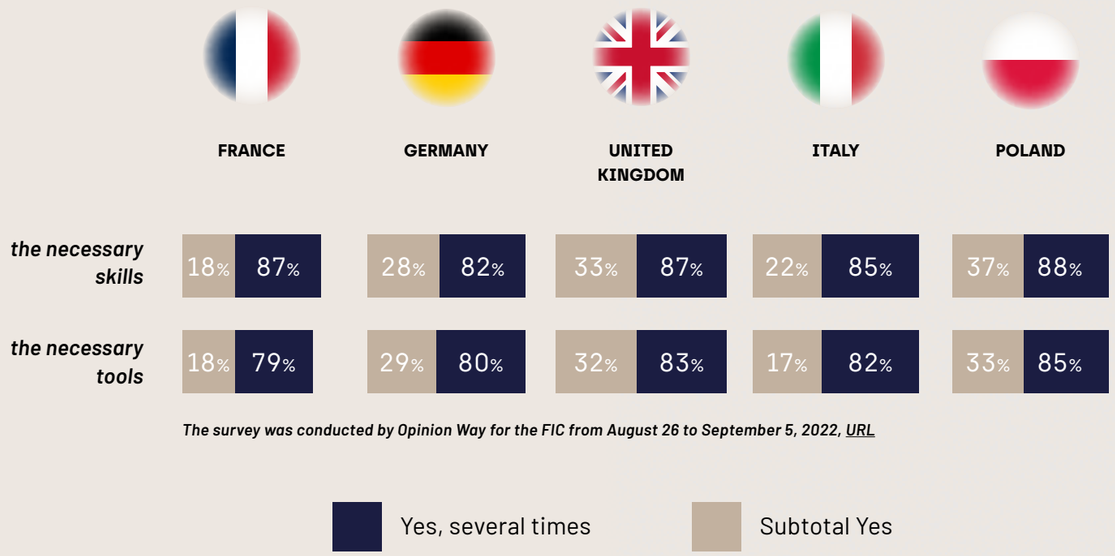
HELPING CITIZENS PREVENT CYBER-ATTACKS

- Between government, industry, and civil society organisations, numerous tools are available to protect citizens from cyber-attacks.
- Industry has focused on helping citizens secure their devices, but could do more to create products designed to be secure.
- Industry is helping foster the next generation of IT professionals, and additional partnerships with governments and civil society organisations could add to these efforts.

DON'T PANIC! RESPONSES TO CYBER-ATTACKS

AS REVEALED BY AN EXCLUSIVE SURVEY BY FIC, USERS GENERALLY FEEL THEY HAVE THE TOOLS AND SKILLS TO SECURE THEMSELVES ONLINE AND PREVENT A CYBER-ATTACK[78].

IN ORDER TO ENSURE YOUR ONLINE SAFETY, DO YOU HAVE...?



The survey was conducted by Opinion Way for the FIC from August 26 to September 5, 2022, URL

They are however less confident about what to do upon discovering that their information (passwords, identification numbers, other PII) may have been compromised. Organisations, especially in the private sector, remain reluctant to admit to data breaches and may as a result be slow to notify regulators and their customers, making it that much more difficult for citizens to react with appropriate measures. Some guidance and initiatives are available to support citizens, mostly from governments and civil society organisations.

78. OpinionWay survey for the FIC conducted in September 2022, URL.

GOVERNMENTS

Below is a selection of country-level government initiatives which seek to empower citizens.

FRANCE

Cybermalveillance Website & Diagnostic Tool: The Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) (French National Cybersecurity Agency) set up a website for citizens to learn about cyber-attacks and determine if they have been a victim. Users can answer a series of questions to describe the problem then are offered personalised recommendations for how to rectify the situation. The tool can also recommend specialised local service providers approved by Cybermalveillance.gouv.fr if necessary.

BELGIUM

As a part of the **SafeonWeb** online portal, the Centre for Cyber Security Belgium has a "First Aid" section designed to help citizens facing specific problems. Users can check if their data has been stolen and receive guidance on next steps, find information to reduce the amount of spam and phishing emails they receive, and obtain guidance on what to do in case of a virus, among others.

SWEDEN

Sweden offers several user-friendly guides on what to do in the event of specific hacks or cyber-attacks, through the website **www.sakerhetskollen.se**. These guides walk users through common signs that their information or system may have been compromised and provide step-by-step instructions for what to do next and how to rectify the situation.

AUSTALIA

Australia offers help to find the right support based on the type of cyber-attack via **www.cyber.gov.au**. In addition to guides and instructions to recover accounts or what to do after personal data has been compromised, they offer an easy, **2-minute quiz** to help identify if a user has been hacked. The quiz concludes with detailed advice on the next steps to take.

PRIVATE SECTOR

Numerous private-sector actors offer paying services to support citizens in their response to cyber-attacks or data breaches. The rapid growth in such offers can make it hard to distinguish reputable services and businesses. The EU cybersecurity certification scheme will be critical to help citizens know which products and services to trust. In the meantime, national cybersecurity certifications schemes can be a useful guide. France's ANSSI "Security Visa"[79] for example, qualifies and verifies security solutions through rigorous third-party testing.

CIVIL SOCIETY ORGANISATIONS

- ***National Cybersecurity Alliance:*** NCA offers information on how to report cybercrime, what to do in the event of a hack, and how to begin fixing the problem.
- ***Have I Been Pwned (HIBP):*** This website helps users identify if their email address or phone number has been compromised as part of a data breach.
- ***Forum of Incident Response and Security Teams (FIRST):*** FIRST is a consortium of security and incident response teams for information-sharing and global policy and regulation development. They offer a Victim Notification service in case of a data breach.
  Users can register their IP address(es) and autonomous system numbers (ASN) to receive an automatic notification in case of a breach. While intended for system managers, the system is open to all and could provide a solution for early alerts about cyber threats, enabling a faster response.

A LACK OF RESOURCES FOR RESPONDING TO CYBER-ATTACKS

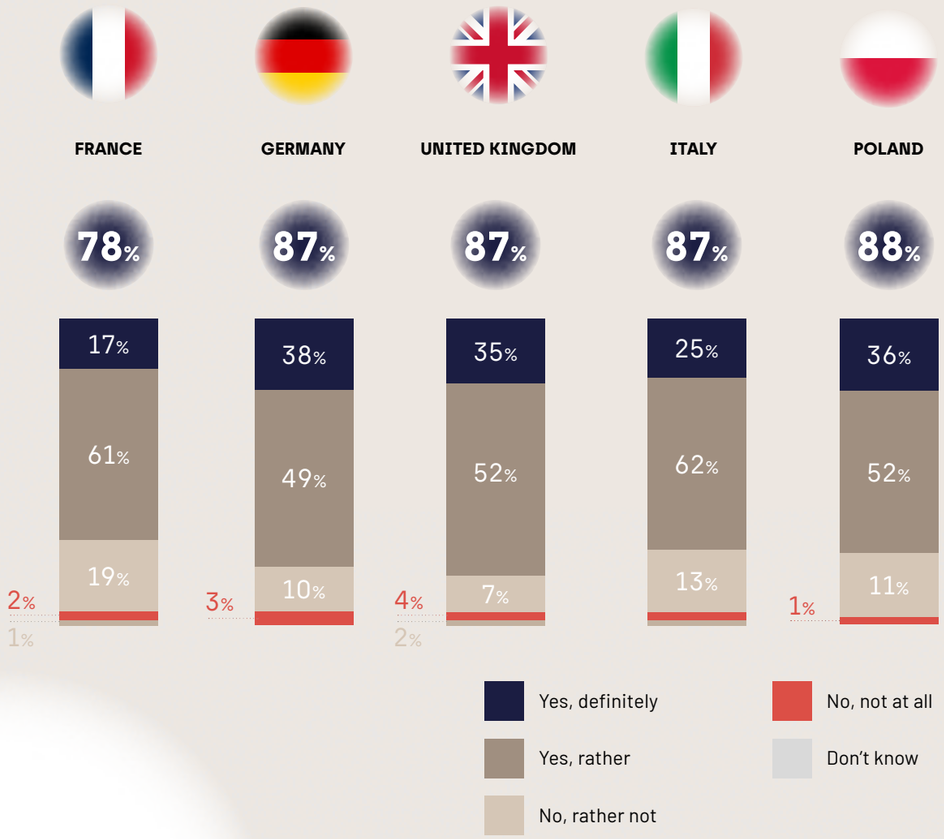
- **There remains a clear opportunity for governments, industry, and civil society organisations to provide solutions for users if they fall victim to a cyber-attack.**
- **Governments are leading the way with helplines and trusted resources, but more can be done to help citizens become aware of and use these services.**

79. Security Visa, ANSSI, URL.

FOREWARNED IS FOREARMED: INCREASING CYBERSECURITY AWARENESS

The regulatory environment has evolved rapidly and is starting to look at cybersecurity for all. Initiatives and solutions by governments, industry, and civil society organisations address multiple aspects of cybersecurity and offer citizens solutions to the most common problems. It therefore makes sense that an overwhelming number of users, 85% of respondents in a recent FIC poll, feel safe online[80].

IN GENERAL, DO YOU FEEL SAFE WHEN YOU USE YOUR DIGITAL TOOLS (MOBILE PHONE, COMPUTER, WEBCAM, CONNECTED OBJECTS…)?



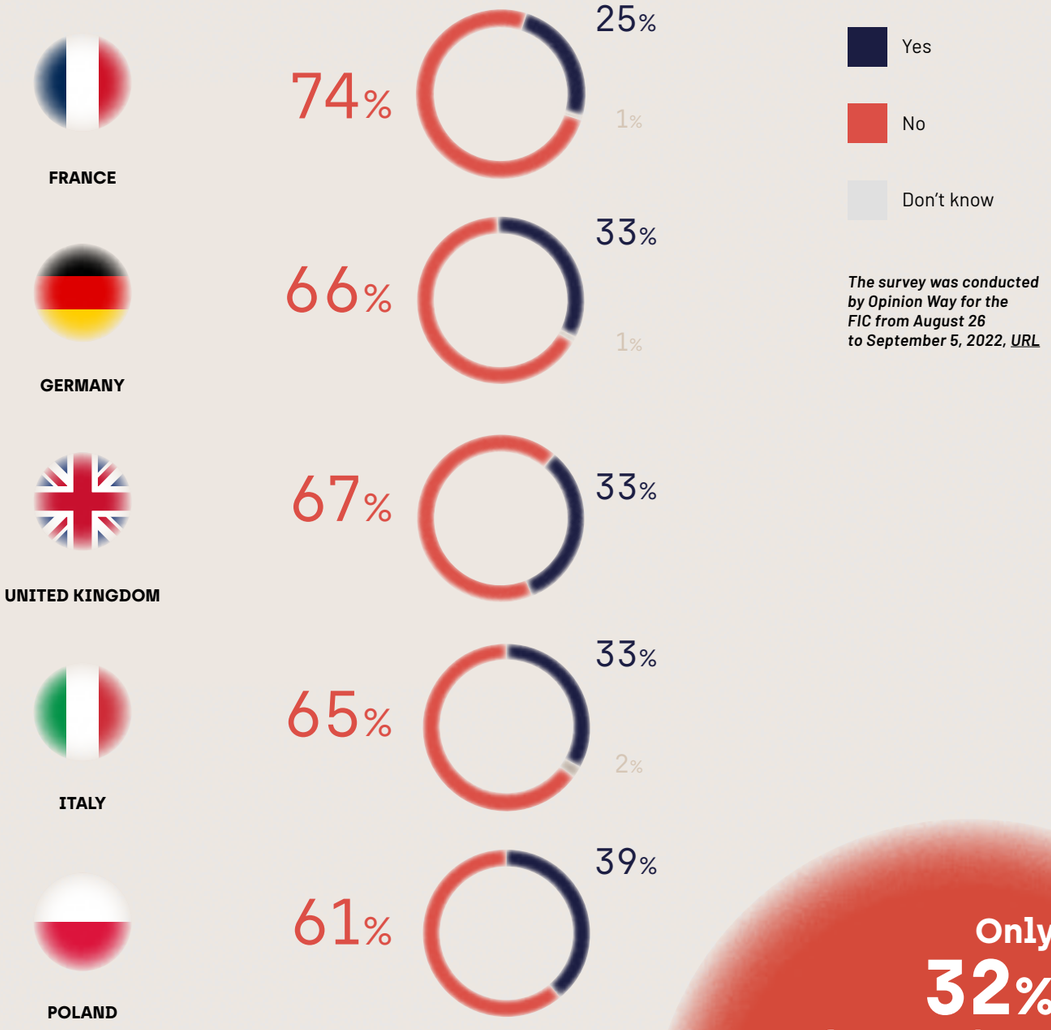
85% yes **14% no**

80. OpinionWay survey for the FIC conducted in September 2022, URL.

But with one in two users having been the victim of malicious cyber acts, how safe are citizens really?

Interviews with experts in the field reveal a gap between citizens' perceptions and the reality. Survey respondents may feel safe online in part because anyone answering an online poll may be more tech savvy than the average citizen. The survey also showed that only one in three respondents could recall a cybersecurity awareness campaign, meaning they could also be unaware of the vulnerabilities posed by their devices and services.

DO YOU REMEMBER EVER SEEING A CYBERSECURITY AWARENESS CAMPAIGN?



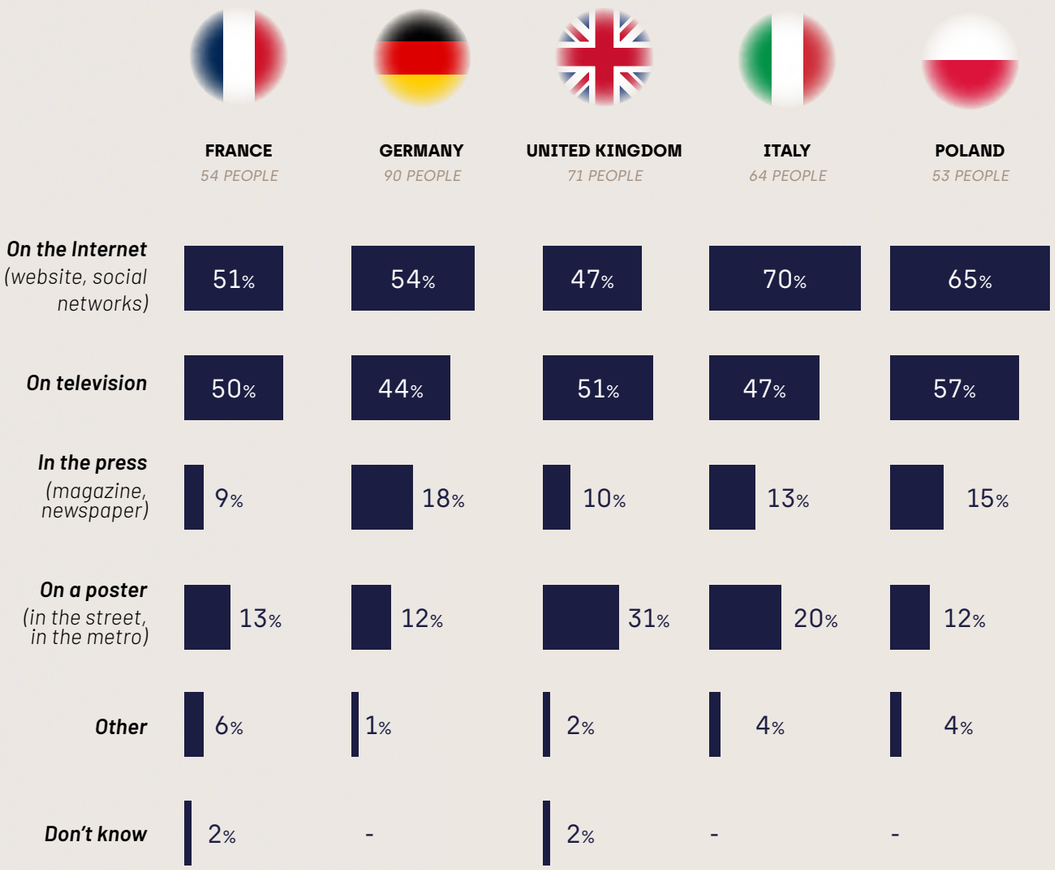
The survey was conducted by Opinion Way for the FIC from August 26 to September 5, 2022, URL

Only 32% of respondents remember a cybersecurity awareness campaign.

81. OpinionWay survey for the FIC conducted in September 2022, URL.

WHERE DO YOU REMEMBER SEEING A CYBERSECURITY AWARENESS CAMPAIGN?

QUESTION ASKED ONLY TO THOSE WHO REMEMBER HAVING SEEN A CYBERSECURITY AWARENESS CAMPAGIN, I.E. 32% OF THE SAMPLE. MULTIPLE ANSWERS POSSIBLE - TOTAL GREATER THAN 100%.



The survey was conducted by Opinion Way for the FIC from August 26 to September 5, 2022

This lack of awareness reveals that citizens are not fully aware of the indirect consequences that attacks on collective infrastructure can have on themselves. This awareness gap also points to a discrepancy in safety perceptions at home compared to at work. Users may not be as concerned about their personal devices, but with work and personal life blending with fewer separations between electronic devices, the risks increase.

The lack of cybersecurity awareness is a well-known issue. National cybersecurity agencies have taken the lead on wide-ranging cybersecurity awareness campaigns, often in partnership with private sector and civil society organisations. These campaigns tend to focus on educating the public about cyber hygiene best practices, phishing and other threats, and advertising free resources.

A flagship event for cybersecurity awareness, October was designated as Cybersecurity Awareness Month[82]. This initiative began in 2004 as a result of a collaboration between the US Department of Homeland Security and the US National Cyber Security Alliance to raise awareness of the importance of cybersecurity[83]. Since then, the practice has become popular and October is recognised as Cybersecurity Month in many countries. During this month, good cybersecurity practices are highlighted by private and public entities to inform and encourage citizens to protect themselves online. In the EU, the initiative is celebrating its 10 years of existence this October 2022, supported by ENISA, the European Commission and the Member States themselves[84].

European national cybersecurity agencies also use the Cybersecurity Awareness Month of October as a reminder of good cybersecurity practices to the general public. In addition, they run awareness campaigns throughout the year. Some national best practices particularly stand out:

- Belgium: The CCB participates in the effort to improve the public's knowledge of key cyber issues. CCB focuses on using humour to spread their key messages, such through this video. More content can be found here: https://www.safeonweb.be/en/campaign-material
- France: Like the CCB, France uses humour and quirkiness to spread messages. These campaigns help citizens become more familiar with the information hub https://www.cybermalveillance.gouv.fr/. Full awareness kit information is available here: https://www.cybermalveillance.gouv.fr/tous-nos-contenus/kit-de-sensibilisation.
- USA: Cybersecurity Awareness Month has existed in the US since 2004, with varying themes. In 2022, CISA is emphasising the role of the user in cybersecurity, encouraging individuals to get involved in protecting themselves. The full campaign is available here: https://www.cisa.gov/cybersecurity-awareness-month.

In addition to these government-based campaigns, civil society and non-profit organisations often partner with governments and industry to run awareness campaigns to help users protect themselves better.

82. European Cybersecurity Month, URL.
83. Cybersecurity awareness month, CISA, URL.
84. European Cybersecurity Month, URL.

THE WAY FORWARD:
RECOMMENDATIONS

Putting citizens at the heart of cybersecurity efforts requires a whole-of-society approach. Governments, businesses, and citizens themselves have a role to play to collectively improve cybersecurity through the protection and the empowerment of citizens. The FIC Agora offers 12 recommendations to encourage a more people-centric cybersecurity.

EDUCATION & AWARENESS

1

Fund cybersecurity education programmes in schools. Gen Z, despite being digital natives, has some of the weakest cybersecurity practices of any generation currently in the workforce[85]. This trend is likely to continue unless cybersecurity training begins at an earlier age. Age-appropriate and inclusive cybersecurity education should be a part of the regular school curriculum. Funding could come from public-private partnerships, as the private sector has a responsibility to ensure that its future customers can use its products safely.

2

Establish lifelong learning cybersecurity programmes at the community level. With the rapid development of new technologies, cybersecurity best practices continue to evolve. More opportunities must be created at the community level to ensure that citizens, throughout their lives, can keep up with cybersecurity regulations, tips, and solutions. Such programmes could be funded by local and regional authorities, where necessary via public-private partnerships.

3

Take awareness campaigns beyond education and into adoption. As the EU celebrates its 10th Cybersecurity Awareness Month, the next step must be to ensure that citizens are not only aware of cybersecurity best practices, but actually adopt and implement solutions. Authorities should leverage the momentum around Cybersecurity Month to encourage users to update their passwords, enable automatic updates, or use antivirus software.

85. The Generational Gap in Cybersecurity and Privacy, Weir, URL.

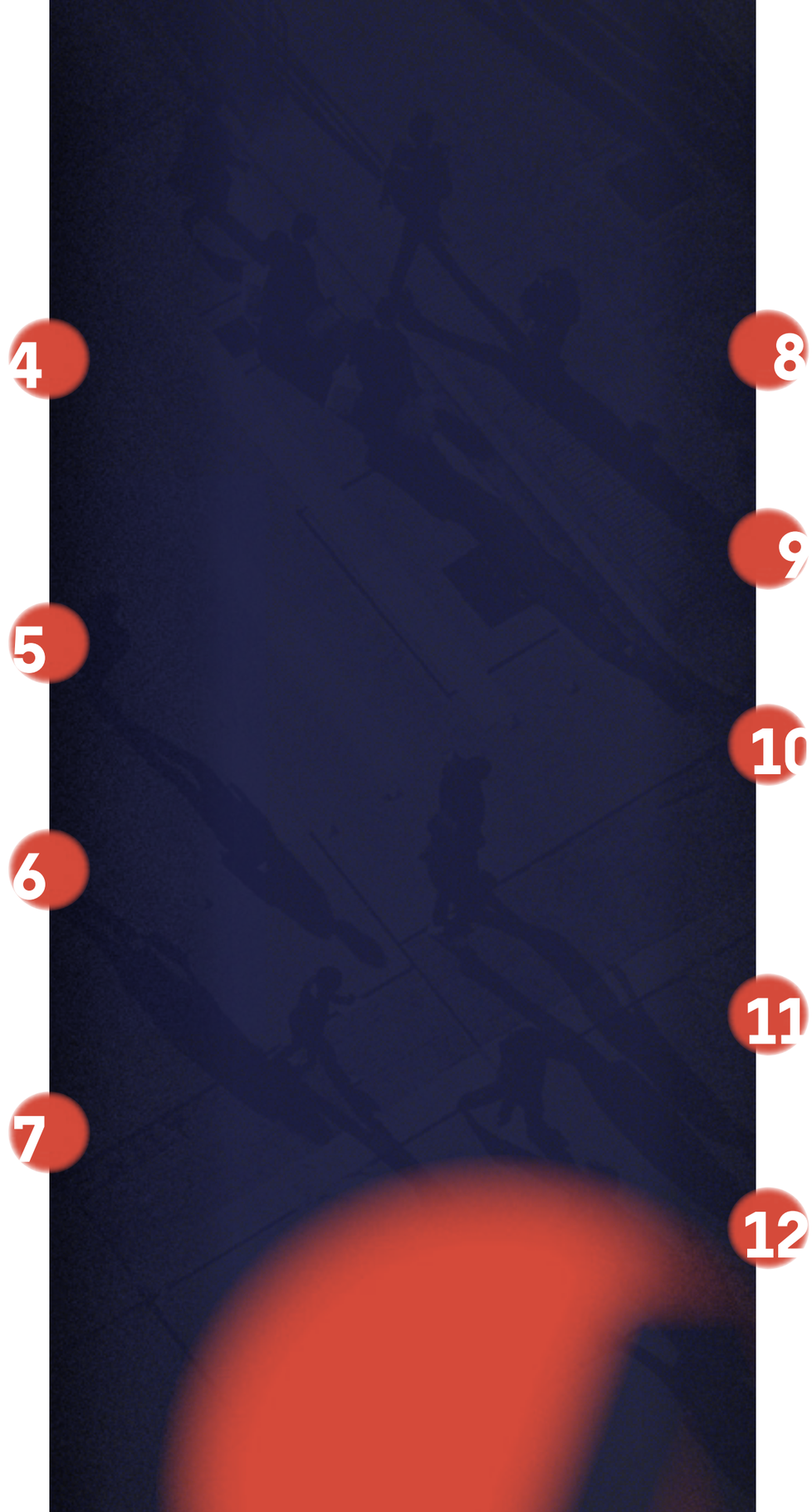
SUPPORT TO CITIZENS

Launch cyber toolkits for citizens. Some national cybersecurity agencies offer useful toolkits which provide citizens with the right tools to stay safe online, as in Belgium or the UK. Cyber toolkits for citizens should include quizzes to help citizens identify phishing attacks and other attacks, offer advice and solutions on what to do if data or accounts are compromised, and indicate where to find further information. The toolkits should be action-oriented, with easy-to-follow steps and easy-to-implement solutions.

Create and promote measures to ensure high cybersecurity standards in all products. Recent developments such as the EU certification schemes or Cyber Resilience Act are important first steps towards this. Further measures will need to be developed to match the evolution of technology and products and ensure that they continue to comply with high standards.

Require digital service providers to increase transparency about their security and privacy practices. Digital service providers, including internet service providers, have some discretion as to what information they can collect and store and what they can do with it, especially if they operate outside the EU. Citizens must be able to trust that when they connect to the internet and use technologies, they are safe. These providers should thus be more transparent about their privacy and security practices.

Create a Cyberscore. Based on the Nutriscore model, a Cyberscore should be developed to offer a multi-coloured label to assess the level of cybersecurity of the product. This could provide an easily readable indication to citizens about the safety of a product and to allow them to make well-informed purchases.



POLICY & OUTREACH

Develop an e-social contract. The development of an e-social contract could help to improve digital trust and encourage shared responsibility online. The terms of such a contract should be defined in consultation with all relevant stakeholders, including governments, industry, civil society organisations and citizens.

Adopt and implement the Cyber Resilience Act and future regulations expediently. Member States have different transposition and implementation processes for EU regulations, which can result in uneven implementation. This can put citizens at risk. Member States should implement EU cybersecurity policies swiftly.

Improve threat information sharing between governments, industry and citizens. Relevant government agencies should continue to inform industry of new threats and trends, but also directly inform citizens. Belgium, for example, offers a cyber newsletter which informs citizens of cybersecurity threats, similarly to severe weather threats. This practice should be broadened across the EU, and would go a long way to both improve citizens' awareness of cyberthreats and ultimately lead them to up their protection.

Provide funding to support stakeholders to comply with legislation and the introduction of new standards. The development of cybersecurity certification schemes and the introduction of new standards often represents a financial burden on product providers and consumers. Funding should be made available to allow stakeholders to keep up and comply with legislative requirements.

Promote a local approach to implementing cybersecurity strategies. Local authorities are the closest to citizens and have a key role to play in involving the latter in cybersecu rity efforts. Local authorities must be empowered by EU, national and regional authorities for that "last-mile" communication to citizens.

REFERENCES

#SuperCoders: Corporate Social Responsibility, Orange, URL.

A majority of Americans are concerned about the safety and privacy of their personal data, Ipsos, URL.

Ad-Hoc Working Group 03 - on 5G Cybersecurity Certification, ENISA, URL.

Ad-hoc Working Group calls, ENISA, URL.

Briefing on the NIS2 Directive: A high common level of cybersecurity in the EU, Negreiro, URL.

Capgemini - Social, Capgemini, URL.

Children's Online Privacy Protection Rule («COPPA»), US Federal Trade Commission, URL.

Code with Google, Google, URL.

Complete guide to GDPR compliance, GDPR.EU, URL.

Consultation on the draft of the candidate Certification Scheme on Cloud Services (EUCS) - Closed, ENISA, URL.

Critical infrastructure sectors in Israel include the 11 sectors defined in the NIS Directive plus the following: Food Supply and Distribution, Government, Public Safety, and Law Enforcement.

Cultivate key human resources who will lead the 4th Industrial Revolution, Samsung, URL.

Cyber force refers to the responsibility to develop a national cyber defence. See more here.

Cyber resilience act – new cybersecurity rules for digital products and ancillary services, European Commission, URL.

Cyber Resilience Act, European Commission, URL.

Cybersecurity awareness month, CISA, URL.

Cybersecurity Certification: Candidate EUCC Scheme V1.1.1, ENISA, URL.

Cybersecurity in the EU – Why we need NIS2 and what changes does it mean for the tech sector?, EURACTIV, URL.

Cybersecurity, CISA, URL.

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, URL.

Divided we fall: Why fragmented global privacy regulation won't work, Kieran, URL.

EU Country Commercial Guide - Cyber Security, International Trade Administration, URL.

EU Cyber Resilience Act, European Commission, URL.

EU Cybersecurity Certification - FAQ, ENISA, URL.

European Cyber Security Organisation (ECSO) - About, ECSO, URL.

European Cybersecurity Month, URL.

Federal Information Security Modernization Act (FISMA), CISA, URL.

Germany calls for political discussion on EU's cloud certification scheme, Bertuzzi, URL.

Global Comprehensive Privacy Law Mapping Chart, IAPP, URL.

Google Career Certificates, Google, URL.

Hardware security overview, Apple, URL.

Israel Defense Forces and National Cyber Defense, Tabansky, URL.

Le modèle Zero Trust, ANSSI, URL.

NIS Directive, IT Governance, URL.

OpinionWay survey for the FIC conducted in September 2022, URL.

Philanthropic initiatives for local communities, Google, URL.

Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, URL.

Public Consultation on the draft Candidate EUCC Scheme, ENISA, URL.

PUBLIC LAW 117–103—MAR. 15, 2022, American Congress, URL.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/ec (General Data Protection Regulation), URL.

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing regulation (EU) no 526/2013 (Cybersecurity Act), URL.

Review of the Directive on security of network and information systems, European Parliament Legislative Train, URL.

Secure design principles, UK National Cyber Security Centre (NCSC), URL.

Security Visa, ANSSI, URL.

Sovereignty requirements remain in cloud certification scheme despite backlash, Kabelka, URL.

TEAL Program, Microsoft, URL.

The EU Cybersecurity Act, European Commission, URL.

The EU NIS Directive, IT Governance, URL.

The European Cybersecurity Act, EUROSMART, URL.

The European Cybersecurity Market, Enterprises Ireland, URL

The new European Cyber Resilience Act, European Parliament Train Schedule, URL.

The Right to Financial Privacy Act, EPIC, URL.

The Women's Digital Centres programme: actively supporting women's empowerment, Fondation Orange, URL.

Thriving together: Samsung CSR US, URL.

Understanding the EU Cybersecurity Act and Its Effect on Businesses, Dunkelberger, URL.

What is GDPR, the EU's new data protection law?, GDPR.EU, URL.

Your rights under HIPAA, US Department of Health & Human Services, URL.

Zero Trust Architecture, Rose et al., URL

ACKNOWLEDGEMENTS

The FIC Agora team would like to thank Phédra Clouner, Deputy Director of the Centre for Cybersecurity in Belgium and member of the FIC Advisory Board, Phil Reitinger, Chief Executive Officer of the Global Cyber Alliance, as well as Camille Monlouis-Félicité for their valuable contributions to this white paper.

Agora FIC

Ask not what the internet can do for you - ask what you can do for the internet.

Next event...

FIC EUROPE

LILLE, FRANCE
APRIL 5-7, 2023