EUROPEAN UNION AGENCY
FOR CYBERSECURITY

RAISING AWARENESS OF CYBERSECURITY

A Key Element of National Cybersecurity Strategies

NOVEMBER 2021

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost the resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

CONTACT

To contact the authors, please use: info@enisa.europa.eu
For media enquiries about this paper, please use: press@enisa.europa.eu

AUTHORS

European Union Agency for Cybersecurity (ENISA), e-Governance Academy (EGA)

EDITORS

Anna Sarri, Cybersecurity Officer in Capacity Building Unit, ENISA

Radu Arcus, Cybersecurity Expert in Capacity Building Unit, ENISA

ACKNOWLEDGEMENTS

Special thanks the Estonian e-Governance Academy for supporting ENISA in the tasks related to the development of this report and in specific Merle Maigre, Radu Serano, Mari Tomingas and Alena Labanava. This study was conducted under the ENISA FWC F-CO2-21-T01.

ENISA would like to thank and acknowledge all the experts that took part and provided valuable input for this report.

LEGAL NOTICE

COPYRIGHT NOTICE

ISBN 978-92-9204-544-9, DOI 10.2824/363629

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Although cybersecurity is one of the most important challenges faced by governments today, public awareness remains limited. Almost everybody has heard of cybersecurity and its importance; however, the behaviour of citizens does not always reflect a high level of awareness. Cybersecurity is essential for individuals and for public and non-public organisations, yet observing security practices often proves to be difficult.

This report seeks to assist EU Member States in further building their cybersecurity capacities by analysing best practices on raising citizens' awareness of cybersecurity. It offers recommendations about ways for better communicating cybersecurity.

The need for cybersecurity awareness and skills is becoming increasingly urgent due to our dependence on Information and Communication Technology (ICT) across all aspects of our society. Recent technological advances and the introduction of smart devices have forced both government and private organisations to create awareness of cyber threats and cybersecurity.

The coronavirus pandemic has further complicated the cyber threat landscape. In March 2020, the COVID-19 pandemic led to social distancing measures and travel restrictions. The global effort to slow down infection rates caused a rapid shift to remote working. In a short amount of time, IT security professionals had to respond to the challenges introduced by working from home arrangements, such as enterprise data movements whenever employees use their home Internet to access cloud-based apps, corporate software, videoconferencing, and file sharing.[1] Even though the hardware and software solutions may have been in place to secure the organisation's data, there were often no established policies to help employees through the jungle of threats and vulnerabilities they were to face when moving their workplace out of the traditional office environment.[2]

With a lack of appropriate guidelines, training and cybersecurity awareness, adapting to such a 'digital by default' normal is difficult, and remote workers may inadvertently act in ways that expose the business to cyber threats. Frequently reported examples of these kinds of mistakes are connecting work devices to public Wi-Fi networks, sharing corporate devices with family members without authorisation, connecting work devices to personal equipment without permission and using personal devices to access work applications and downloading unauthorised applications contrary to organisational policies. All such frequent habits increase the risk of data exposure.

In short, communication about cybersecurity issues is a complicated endeavour. In this report, we have collected information and evaluated the intensity, regularity and diversity of different cybersecurity awareness practices and processes in EU Member States. We present ways in which Member States have achieved better cybersecurity awareness in society and have incorporated cybersecurity awareness into their national cybersecurity strategies (NCSS). In addition, we provide recommendations in the following four areas: building capacities for cybersecurity awareness, regular assessments of trends and challenges, measuring cybersecurity behaviour and planning cybersecurity awareness campaigns.

[1] ENISA Threat Landscape "The Year in Review. From January 2019 to April 2020", ETL2020 – A year in review, https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/etl-review-folder/etl-2020-the-year-in-review/view

[2] NATO CCDCOE Recent Cyber Events: Considerations for Military and National Security Decision Makers, No 10 / May 2021, https://ccdcoe.org/uploads/2021/05/Recent-Cyber-Events-10_May-2021.pdf

1. INTRODUCTION

1.1 AIM, SCOPE AND OBJECTIVES

The aim of this work on cybersecurity awareness raising was first to analyse the ability of EU Member States to build their national capacities to raise citizens' awareness regarding cybersecurity issues. Then, based on the results of an analysis of best practices on raising citizens' awareness of cybersecurity, this work aims to assist EU Member States in further building their cybersecurity capacities. This report offers recommendations about ways to better communicate cybersecurity. The study covers the practices of EU Member States from 2018 until 2021.

The specific objectives of this study were to:

- Analyse existing methods for raising cybersecurity awareness at a national level.
- Identify stakeholders and their roles in the organisation associated with implementing and monitoring awareness raising activities.
- Identify EU Member States' good practices on how to organise, measure effectiveness and ensure appropriate outreach of the awareness raising activities.
- Identify a set of metrics before designing awareness raising activities in order to follow up on effectiveness and reach out both in the short- and long-term perspective.
- Identify the behavioural aspects that may influence awareness campaigns.
- Highlight challenges and lessons learnt from the design of such activities.
- Propose recommendations for improving awareness in society, considering all the above elements.

1.2 APPROACH AND METHODOLOGY

This report proposes recommendations to increase the effectiveness of national awareness raising activities, based on the research into existing NCSS, interviewing stakeholders involved in cybersecurity awareness raising in Member States, and identifying good practices, challenges and lessons learnt.

The intensity, regularity and diversity of different cybersecurity awareness practices and processes in EU Member States has been evaluated based on collected information. Throughout the study, we have examined the following indicators:

- The amount and sequence of information provided to citizens on cyber threats and on cybersecurity by national authorities.
- The level of accessibility of threat-related information provided by national authorities to the society.
- Quantitative data and metrics for monitoring public cybersecurity behaviour.

Additionally, the connection between quantitative metrics and operational perspectives in carrying out possible awareness campaigns is analysed. The work is based on a substantial analysis of Member States' awareness campaign methodologies, including carrying out their planning processes, the way they meet challenges and how they measure success and impact.

Based on a pre-defined questionnaire, 20 structured interviews were conducted with the relevant national authorities during May–July 2021. The collected evidence was synthesised to identify overarching patterns, the perceived quality of awareness raising activities and the campaign's success in achieving the specified goals and objectives. The evaluation of the

awareness raising activities was based on the analytical data gathered from desktop research, interviews with subject matter Member State authorities and questionnaire results

Figure 1: List of countries and primary institutions interviewed for this project

Country	Institution
Belgium	Centre for Cybersecurity Belgium
Croatia	National Computer Emergency Response Team (CERT)
Czech Republic	National Cyber and Information Security and Agency
Denmark	National Agency for Digitisation
Estonia	Information System Authority, Ministry of Economic Affairs and Communications
Finland	Digital and Population Data Services Agency
Germany	Federal Office for Information Security (BSI – *Bundesamt für Sicherheit in der Informationstechnik*)
Ireland	Cybersecurity Policy Division, Department of Environment, Climate and Communications
Italy	Presidency of the Council of Ministers[3]
Latvia	National Computer Emergency Response Team (CERT)
Luxembourg	Ministry of State, High Commission for National Protection
Malta	National Cybersecurity Coordination Centre
The Netherlands	Ministry of Justice and Safety
Norway	Ministry of Justice and Public Security
Poland	Department of Cybersecurity, Chancellery of the Prime Minister
Portugal	National Cybersecurity Centre
Romania	National Cyber Security Directorate (DNSC)[4]
Slovakia	National Security Authority
Slovenia	Government Information Security Office
Sweden	Civil Contingencies Agency

To see the detailed questionnaire used, please refer to Annex A. For a full list of EU MS country data (central coordinator, list of campaigns, links), refer to Annex B.

1.3 TARGET AUDIENCE

The target audience of this report is public organisations engaged with cybersecurity awareness raising at a national level, national competent cybersecurity authorities, information technology (IT) security professionals, and other target groups who have organised or attended the European Cybersecurity Month and/or other public cybersecurity awareness raising events. Furthermore, the report targets policymakers who are aiming to improve the security awareness

[3] In August 2021, the National Cybersecurity Agency (NCA) was established, responsible for the development of a national cybersecurity culture in Italy.
[4] The name was changed from National Computer Emergency Response Team (CERT) in September 2021.

of society, professionals and, more generally, IT end-users. The report could also prove useful to the different stakeholders in the international development community, who provide assistance in cybersecurity.

1.4 DEFINITIONS

Cybersecurity	Preservation of confidentiality, integrity and availability of information in the cyberspace.[5]
Cybersecurity awareness	Level of appreciation, understanding or knowledge of cybersecurity aspects. Such aspects include cognizance of cyber risks and threats, but also appropriate protection measures.[6] We maintain that awareness is not training; the purpose of awareness presentations is simply to focus attention on security. Awareness presentations are intended to allow individuals to recognise IT security concerns and respond accordingly.[7] Through awareness raising, individual and corporate users can learn how to behave in the online world and protect themselves from potential risks and threats.[8]
Good practices	Activities that have been shown to work well and proven to succeed in achieving objectives and could be recommended as a model. They are activities oriented towards providing guidance to the different stakeholders.

We define cybersecurity awareness as the level of appreciation, understanding or knowledge of cybersecurity aspects.

1.5 STRUCTURE

The report is divided into five parts. Firstly, it provides definitions and describes the methodologies followed in the development of this report. Secondly, an overview of building national capacities towards national cybersecurity awareness is provided, showcasing best practices from a number of EU Member States. Then, the importance of periodic assessments of cybersecurity trends and challenges is presented, followed by an analysis of the collection metrics used to measure the behavioural aspects of cybersecurity. In the fifth chapter, an examination of the actual cybersecurity awareness campaigns conducted in practice is provided. Each chapter has an outline of overarching patterns, followed by good practices from selected Member States and a conclusion. The last chapter provides a number of recommendations to increase the effectiveness of national awareness raising activities.

[5] ISO/IEC 27032:2012
[6] Nurse J.R.C. (2021) Cybersecurity Awareness. In: Jajodia S., Samarati P., Yung M. (eds) Encyclopedia of Cryptography, Security and Privacy. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-27739-91596-1
[7] US NIST Special Publication (800-16), https://csrc.nist.gov/publications/detail/sp/800-16/final
[8] https://www.enisa.europa.eu/topics/cybersecurity-education

2. BUILDING CAPACITIES TO RAISE CYBERSECURITY AWARENESS

In 2020, ENISA published a national capabilities assessment framework[9] that aims to provide Member States with a self-assessment of their level of maturity. To achieve this goal, it enables the assessment of NCSS objectives, such as raising user awareness by providing KPIs on five maturity levels. The aim of the framework is to help EU Member States enhance and build cybersecurity capabilities both at strategic and operational levels.

The purpose of the study was to provide an overview and analysis of EU Member States' capacities to raise cybersecurity awareness among their general population through the organisation of national activities and plans. The results of interviews with and surveys completed by experts who conduct awareness building in Member States highlight the different approaches that countries follow to support cybersecurity awareness in the context of their NCSS.

Desk research and interviews revealed that Member States with a cybersecurity strategy which includes a clear vision about national cybersecurity awareness raising are in a stronger starting position when building their cybersecurity capacities. Member States are on even firmer ground if the objective of society-level cybersecurity awareness in their national cybersecurity strategies is supported by concrete measures, tasks, and deliverables specified in the strategy implementation plan.

Throughout the years, the importance of cybersecurity awareness raising has been recognised in the NCSS of Member States. While earlier strategies sometimes addressed the issue superficially or declaratively, there is now an evident trend to describe the aims of awareness raising as well as relevant activities in more detail.

A number of Member States claim that more efficient awareness raising is conducted when there exists a clearly defined national agency coordinating or overseeing cybersecurity awareness efforts. However, there were some successful cases of horizontally spread tasks, such as in Finland, Luxembourg and the Netherlands, where the activities are carried out by a number of different ministries and agencies. The underlying factor to ensure accountability and progress was identified as all parties involved having a clear understanding of their respective roles and responsibilities.

The majority of countries studied recognise the importance of close interagency cooperation in conducting awareness raising activities. The interviews with EU Member States also verified a need for public and private actors to engage together at national and regional levels for efficiency in raising awareness. Ensuring cybersecurity requires synergistic actions in the legal, organisational, technical and educational areas.

Despite acknowledging the need for joint engagement, guaranteeing the ongoing budget required remains challenging. This stems from the fact that resources are allocated by government entity, rather than by task or objective. Only three Member States out of twenty

[9] https://www.enisa.europa.eu/publications/national-capabilities-assessment-framework

could confirm that established and regular national funding for cybersecurity awareness activities is guaranteed. For some Member States, European Union funds are used for such activities.

Regarding cooperation between the relevant cybersecurity agencies and the media, Belgium, Czech Republic, Finland, Luxembourg and Slovakia demonstrate good practice on how to maintain constructive connections with the media and create an open atmosphere that enables the provision of more information to journalists.

2.1 NCSS WITH A CLEAR VISION ABOUT AWARENESS

Cybersecurity awareness raising is more likely to be successful when the corresponding vision is spelled out in the NCSS to help all stakeholders understand what is at stake and why cybersecurity awareness raising is needed (context), what is to be accomplished (objectives), as well as what is it about and to whom it applies (scope). The clearer the vision, the easier it is for key stakeholders to ensure a comprehensive, consistent and coherent approach. A clear vision also facilitates coordination, cooperation and implementation.[10]

Desk research and an analysis of surveys and interviews revealed the following good practices of selected EU Member States:

Croatia is currently updating its NCSS. Awareness raising is embedded in three areas: electronic communication, critical information infrastructure and cybercrime. The Croatian national Computer Emergency Response Team (CERT-HR) which implements cybersecurity awareness raising activities, is a department within the Croatian Academic and Research Network with a separate strategy (2019–2022)[11] that prioritises digital transformation of the educational system and cybersecurity awareness raising as part of that.

The NCSS of the **Czech Republic** 2021–2025[12] was published in December 2020, with a separate chapter titled "Resilient Society 4.0" addressing education and awareness raising of the overall population.

The **Estonian** NCSS 2019–2022[13] along with the Estonian Cybersecurity Act (2018) task the Estonian Information System Authority to raise awareness among citizens, to prevent cybersecurity incidents and to notify citizens about possible threats.

The **Finnish** Cybersecurity Strategy from 2019[14] focuses, inter alia, on the need to increase public cybersecurity competence: "Finnish society needs cybersecurity competence both in public administration and in the business community. … At the national level, it must be ensured that everyone has sufficient capacity to operate safely in a digital environment."[15] In addition, the Government Resolution on digital security in the public sector aims to improve the digital security skills and awareness of public sector staff as well as the personnel of business and non-governmental organisations.

The awareness raising objectives of the **Latvian** Cybersecurity Strategy 2019–2022[16] focus on building an information society that include raising cybersecurity awareness amongst teachers, students, governmental employees, and society in general by promoting safe use of hardware,

[10] https://www.itu.int/pub/D-STR-CYB_GUIDE.01-2018
[11] https://www.carnet.hr/en/
[12] https://www.nukib.cz/en/cyber-security/strategy-action-plan/
[13] https://www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf
[14] https://julkaisut.valtioneuvosto.fi/handle/10024/162265
[15] https://turvallisuuskomitea.fi/wp-content/uploads/2019/10/Kyberturvallisuusstrategia_A4_ENG_WEB_031019.pdf
[16] https://www.mod.gov.lv/en/nozares-politika/cybersecurity

software and the Internet. These objectives are divided into specific tasks that are assigned to various institutions.

Luxembourg's upcoming NCSS IV (2021–2025) approaches the issue of awareness raising from the perspective of "Building trust in the digital world and protection of human rights online". Amongst various strategy objectives, cybersecurity education and vocational training focuses on awareness raising. An action plan of the strategy defines concrete tasks and deliverables.

Malta's 2016 NCSS[17] has six goals, one of which is "cybersecurity awareness and education". With this goal, Malta aims to target academia, the public and private sector and citizens to "sensitize" awareness, knowledge as well as capabilities and expertise in cybersecurity. Specific measures under this goal include a "Strategic, target-oriented national awareness and advice campaign" and "Encouragement of 'cyber hygiene' and personal responsibility".

For the first time, **Norway** in 2019 launched a separate National Strategy for Cybersecurity Competence,[18] because competence and knowledge about cyber threats, vulnerable areas, and effective measures are a precondition for the ability to protect digital systems against cyber incidents. Developed by the Norwegian Ministry of Justice and Public Security and the Ministry of Education and Research, the Competence Strategy addresses cybersecurity from the perspective of a general *challenge* to society. While drafting the strategy, the ministries were in close dialogue with both universities and research funding agencies to guarantee an open and inclusive process. They also involved stakeholders from the public and private sector. The goal of the strategy is to improve cybersecurity competence in accord with the needs of society. The strategy sets out conditions for long-term competence building, encompassing national capacity building in the fields of research, development and education, and measures designed to raise awareness in the business community and among the general public.

Poland's Cybersecurity Strategy for 2019–2024 has as its main objective to increase the level of resilience to cyber threats and to strengthen data protection. It includes the issues of raising awareness in cybersecurity.

Portugal's latest Cybersecurity Strategy 2019–2023[19] expands on cybersecurity awareness under a special axis called "*prevention, education and awareness*" which foresees a number of specific action points such as, for example, to promote robust and cross-cutting cybersecurity training programs for all organisations and the average citizen, to strengthen cyberspace security skills and knowledge in education and to promote digital education and literacy.

Slovakia's Cybersecurity Strategy 2021–2025[20] prioritises a well-educated public and well-educated professionals. It includes not only reference to regulations but also practical activities, such as risk management, detection and cybersecurity incident handling, system recovery, education, dissemination of security awareness and, last but not least, research and development of cybersecurity tools and processes.

For the National Strategy and its objectives to be feasible, specific tasks and activities must be identified, together with clear responsibilities. To this end, the Government of Slovakia adopted in July 2021 an Action Plan for the implementation of the National Cyber Security Strategy for 2021 to 2025, which defines specific tasks and activities, identifies responsible entities and also time horizons for fulfilling individual tasks and activities. The aim of the Action Plan is to create a

[17] https://cybersecurity.gov.mt/wp-content/uploads/2018/09/Mita-_Malta-Cyber-Security-Strategy-Book.pdf
[18] https://www.regjeringen.no/no/dokumenter/nasjonal-strategi-for-digital-sikkerhetskompetanse/id2627189/
[19] https://www.cncs.gov.pt/docs/cncs-ensc-2019-2023.pdf
[20] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Slovakia

[1] Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

comprehensive schedule of tasks and activities in the field of cybersecurity for the next five years.

Slovenia is working on a new version of its NCSS that is expected to be ready by June 2022. The current version, the 2016 NCSS[21] does address cybersecurity awareness raising. Furthermore, the 2018 Information Security Act[22] provides a legal basis for awareness-raising activities. It gives the mandates for the awareness-raising tasks to the Government Information Security Office.

In conclusion, Member States with a NCSS that includes a clear vision about national cybersecurity awareness raising are in a stronger starting position when building their cybersecurity capacities. They are on even firmer ground if the objective of the society-level cybersecurity awareness in their NCSS is further supported with concrete measures, tasks and deliverables specified in the strategy implementation plan. Throughout years, the importance of cybersecurity awareness raising has been recognised in cybersecurity strategies. While earlier strategies sometimes addressed the issue superficially or declaratively, there is now an evident trend to describe the aims of the awareness raising as well as relevant activities in more detail.

2.2 COORDINATION OF AWARENESS ACTIVITIES AND INTERAGENCY COOPERATION

In a number of Member States –11 Member States out of the 20 observed – cybersecurity awareness raising activities are coordinated by a single, competent authority. This dedicated and competent cybersecurity authority is a leading entity that provides direction, coordinates actions, and monitors the implementation of cybersecurity awareness activities. The lead agency also identifies an initial set of stakeholders to be involved in the development and implementation of the awareness activities, clarifies the roles of different stakeholders and outlines how they should collaborate in order to manage expectations throughout the process.

In turn, these entities are responsible and accountable for the implementation of each specific initiative assigned to them and are expected to coordinate their efforts with other relevant stakeholders as part of the implementation process.

An example of a coordination mechanism would be conducting periodic meetings with all relevant stakeholders for a joint review of action plans. An example of a cooperation mechanism would be the creation of an intra-sectoral task force to address a particular issue.

Desk research and interviews revealed that coordination models vary country by country.

In **Belgium**, the central coordinator is the Centre for Cybersecurity Belgium (CCB). The CCB works with the Cybersecurity Coalition, a national cooperation that brings together representatives of the private, academic and administration sectors. The Cybersecurity Coalition has created a task force on awareness raising which collaborates with the CCB. They prepare materials together and encourage partners to use them all year around.

In **Czech Republic**, the National Cybersecurity Centre is the executive section of the National Cyber and Information Security and Agency. Amongst other tasks, the National Cybersecurity Centre oversees awareness and educational activities concerning cybersecurity. Nevertheless, it is the responsibility of every organisation's management to raise the cybersecurity awareness of their employees.

The **Estonian** Information System Authority is the coordinator of cybersecurity awareness raising in Estonia. It gathers data to assess the level of awareness, analyses incident statistics

[21] https://www.gov.si/assets/ministrstva/MJU/DID/Cyber_Security_Strategy_Slovenia.pdf
[22] http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO7707

and organises activities based on the collected data. Under the coordination of the Information System Authority, multiple actors are engaged in awareness raising. For example, the police have online "Web-Constables" – police officers who respond to notifications and letters submitted by people via the internet and train children as well as adults about issues of internet security. PhD candidates specialising in cybersecurity at the Tallinn University of Technology work with children in the schools. The Information System Authority also cooperates with civil society organisations like the Estonian Union for Child Welfare that targets activities towards children. Communication companies run their own campaigns, for example, Telia has conducted a campaign for kids countering cyberbullying.

Finland has a distributed model instead of a centralised agency that is responsible for everything related to cyberspace. There are a number of different agencies that work in different areas. The Finnish Cybersecurity Strategy (2019) explains this as follows: "National cybersecurity will be built in cooperation among the authorities, the business community, organisations and citizens, when everyone can contribute to our shared cybersecurity. Each individual is therefore an important cybersecurity actor who can improve cybersecurity through his or her actions on a daily basis and thus impact his or her own cybersecurity and that of others." In the appendix to the publication Digital Security in the Public Sector,[23] the responsibilities of different agencies in relation to cybersecurity are described.

In **Germany**, the Federal Office for Information Security shapes information security in digitalisation through prevention, detection and response for government, business, and society. The document that guides national cybersecurity awareness raising is the "Act on the Federal Office for Information Security".[24] Since 2018, a separate citizens' awareness unit team "Cybersecurity for citizens and society" has existed in the Federal Office for Information Security.

In **Italy**, the Law Decree n. 82 of 14 June 2021, converted into Law n. 109 on 4 August 2021, established the National Cybersecurity Agency (NCA) which also carries out activities related to the communication and promotion of cybersecurity awareness to contribute to the development of a national culture. The Agency includes the National Cybersecurity Cell (NCSC) – an inter-ministerial body meant for coordinating preventive measures and reacting to national cybersecurity crises – that replaced the one operating within the Security Intelligence Department (DIS).[25]

Ireland has established a cybersecurity education working group within the National Council for the Curriculum and Assessment, Computer and Education Society of Ireland (which is a group of teachers at elementary, middle, and high-school levels) and Cyber Ireland.

In **Latvia**, CERT.LV is tasked with informing the society of cyber threats, but they do not play a single leading role and are not the main coordinator among all the institutions for cybersecurity awareness campaigns. The Ministry of Environmental Protection and Regional Development, for example, is responsible for organising events during European Digital Week.

Luxembourg has no single dedicated agency for the coordination of awareness raising. The inter-ministerial cyber prevention and cybersecurity committee is responsible for ensuring

[23] https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/162265/VM_2020_45.pdf?sequence=1&isAllowed=y
[24] https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/BSI/BSI_Act_BSIG.pdf?__blob=publicationFile&v=1
[25] The national cybersecurity ecosystem in Italy was reshaped with the entry into force of the Law Decree n. 82 of 14 June 2021, which created the National Cybersecurity Agency (NCA). To the extent that awareness raising is part of preventive activities, the National Cybersecurity Cell provides this coordination. The NCSC is chaired by the NCA director general, it includes the Prime Minister's Military Counsellor, representatives from the Intelligence community (DIS, AISE and AISI), the Civil Protection Department, as well as from the Ministries represented in the Cybersecurity inter-ministerial Committee (Ministry of Foreign Affairs, Ministry of Internal Affairs, Ministry of Justice, Ministry of Defence, Ministry of Economy and Finance, Ministry of Economic Development, Ministry of Technological Innovation and Digital Transition, Ministry of Sustainable Infrastructures and Mobility, Ministry for Ecological Transition and the Ministry of University and Research).
[1] Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

national coordination in the field of cyber prevention and cybersecurity and as such also at a high level for awareness raising. The High Commission for National Protection is in charge of coordinating the drafting and implementation of the NCSS. The "Bee Secure" government initiative is operated by the National Youth Service and the Kanner-Jugendtelefon, in partnership with Securitymadein.lu,[26] the Grand-Ducal Police and the Public Prosecutor's Office. The ministries involved are the Ministry of National Education, Children and Youth, the Ministry of the Economy and the Ministry of Family and Integration. Other key players include the National Institute for Public Administration that raises awareness among civil servants. Thanks to its field experience and its established network of partners, "Bee Secure" is able to contribute in a concrete way to the empowerment of the user.

In 2016, the **Malta** Information and Technology Agency (MITA) was assigned the mandate to coordinate and oversee citizens' cybersecurity awareness and education, and the Cyber Security Malta campaign was launched. MITA cooperates with other stakeholders in the framework of the National Cybersecurity Committee which also includes the Police, the Armed Forces, the Critical Infrastructure Directorate, the Communications Authority, the Financial Services Authority, the Gaming Authority and the Digital Innovation Authority.

In the **Netherlands**, various ministries have their own policy for cybersecurity awareness raising. Overall, the Ministry of Security and Justice is responsible for cybersecurity measures concerning civilians, the Ministry of Economics is responsible for cybersecurity awareness raising among companies and entrepreneurs, and the Office and Ministry of Security and Justice deal with municipalities and vital infrastructure. The latter engage in awareness raising activities to prevent citizens and organisations from becoming victims. They cooperate with the police and several private sector players such as Google, Facebook, Microsoft and telecommunication companies.

In **Norway**, NorSIS is a national coordinator for the European Cybersecurity Month. NorSIS is an independent body that works in collaboration with public sector, institutions, partly financed by the Ministry of Justice and Public Security. Its main target groups are the general population, as well as small and medium enterprises. In the future its activities will be targeted mostly at private citizens. NorSIS partners with traditional media, the Safer Internet Centre and other partners depending on the scope of activities, e.g. the National Data Protection Agency, the Norwegian Cyber Security Centre and the Norwegian Digitalisation Agency. The Centre organises and provides guidance, advice, case handling and other services free of charge to the population. The Norwegian National Security Authority is a cross-sectoral professional and supervisory authority within the protective security services in Norway.

In **Poland**, in 2020, the Ministry of Digital Affairs was reorganised and incorporated into the chancellery of the Prime Minister. The role of the Minister of Digital Affairs is performed by the Prime Minister, and the former Minister of Digital Affairs has taken on the role of Secretary of State. The Department of Cybersecurity in the Chancellery of the Prime Minister focuses on the development of the content, guidance and recommendations. Overall, awareness raising activities in Poland are conducted by the Computer Security Incident Response Team (CSIRT) of the National Research Institute (NASK) that deals with a wider audience like academia, the education sector, the transportation sector, and local administration. The National Research Institute is promoting the safe use of new technologies and the Internet, providing materials and best practices for educating society on cybersecurity. The Polish Ministry of Defence Computer Security Incident Response Team is sometimes also engaged in awareness raising by running phishing awareness campaigns and providing recommendations.

[26] Security madein.lu is an economic interest group owned by the state of the Grand Duchy of Luxembourg and local governments, see https://securitymadein.lu/agency/

[1] Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

An example of public-private cooperation in Poland is the Cybersecurity Cooperation Program,[27] a non-commercial public-private partnership for the National Cybersecurity System where parties exchange experiences in order to, inter alia, increase the security of digital processes, products and services. The cooperation agreement covers such areas as: information, education, training and testing as well as certification with particular emphasis on raising competencies in the field of awareness of threats and attack methods in cyberspace.

In **Romania**, the National Cyber Security Directorate (DNSC) as the national competent authority for the cybersecurity of networks and information systems has the responsibility of the cybersecurity awareness activities. In this role, DNSC frequently delivers awareness materials for all types of users both on its website and on social media channels. DNSC fulfils the function of alerting of issues, prevention, awareness and training.

In **Slovakia**, according to the Cybersecurity Act, the National Security Authority is responsible for awareness raising and for preparing legislation in the field of cybersecurity. The Cybersecurity Competence and Certification Centre within SK-CERT determines the education programs for building security awareness and professional training. The NSA in Slovakia has good relationships across the cybersecurity community. They cooperate with the police when it comes to raising awareness about cybercrime, as well as with academia (e.g. Technical University in Žilina, the Academy of the Police Forces and other universities). Cooperation discussion also involves the Slovakian Academy of Sciences. In the future, increased collaboration is also planned with the Slovakian Cybersecurity Association.

In **Slovenia**, the Government Information Security Office is the national competent authority and raising public awareness of information security is one of their tasks. The Government Information Security Office coordinates training, exercises and education in the field of information security and is responsible for raising public awareness of information security. The interagency cooperation includes the national CERT, the police, the cybersecurity section of the Slovenian Chamber of Commerce, Telecommunications companies (TELCOs Telekom Slovenia and A1) and the Slovenian Bank Association. The national CERT runs an awareness-raising programme Safe on internet, and a consortium of the Faculty of Social Sciences, some non-governmental organisations, the Academic and Research Network of Slovenia (ARNES) and the Police runs an awareness-raising programme Safer Internet. The Slovenian Bank Association cooperates with the national CERT.

To sum up, several Member States demonstrate that successful awareness raising is conducted when there is a clear national agency coordinating or overseeing citizens' cybersecurity awareness activities. However, there were some successful cases of horizontally spread tasks, such as Finland, Luxembourg and the Netherlands. To ensure accountability and progress, the parties involved should have a clear understanding of their respective roles and responsibilities.

Furthermore, all Member States recognise the importance of close interagency cooperation for awareness raising activities. According to the interviews, for successful cybersecurity awareness raising, there's a need for public and private actors engaged together in cybersecurity awareness raising activities at a national and regional level. Ensuring cybersecurity requires synergistic actions in the legal, organisational, technical and educational areas as well as cooperation between public administration and the private sector.

[27] https://www.gov.pl/web/cyfryzacja/program-wspolpracy-w-cyberbezpieczenstwie-pwcyber--partnerstwo-publiczno-prywatne-na-rzecz-krajowego-systemu-cyberbezpieczenstwa

2.3 RESOURCE ALLOCATION

Sufficient, consistent and continuous funding provides the foundations for an effective national cybersecurity posture. For an efficient implementation of cybersecurity awareness raising activities, Member States should allocate necessary human and financial resources.

Desk research, analysis of surveys and interviews revealed the following good practices based on selected EU Member States:

In **Croatia**, the national CERT as a part of the Croatian Academic and Research Network uses European funding for cybersecurity awareness campaigns. The last campaign was co-financed by the EU programme "Connecting Europe Facility" under the action Grow CERT.

In **Czech Republic**, cybersecurity awareness raising activities are financed from an annual budget that is based on strategic documents and priorities.

In **Luxembourg**, entities engaged in awareness raising manage their regular annual budgets allocated to cybersecurity awareness raising campaigns and ongoing initiatives. If necessary, extraordinary annual financing requirements needed for the implementation of awareness building objectives of the most recent strategy are defined and negotiated.

In **Norway**, the grants from the Ministry of Justice and Public Security, make up about half of the annual budget of NorSIS. This allocation is meant to cover cybersecurity awareness raising activities towards citizens such as the national cybersecurity month, public information campaigns etc.

Guaranteeing a stable stream of funding continues to be challenging. However, Member States with an NCSS and implementation plans that make reference to cybersecurity awareness raising were in a somewhat stronger position to ensure necessary funding.

For a stable stream of funding, the lead coordinating authority works with the owners of the specific initiatives to understand what resources (human resources, expertise and funding needs) are required to accomplish the work, and then identifies and secures the required resources in accordance with administrative financial structures of the country.

More generally, it is relevant to keep in mind that resources are defined beyond the terms of money (i.e. dedicated budget); they also include people, material, as well as the relationships and partnerships and continued political commitment and leadership required for successful execution.

2.4 COOPERATION WITH MEDIA

Developments in ICT have exposed the media to cybersecurity threats and frauds. Content security is also at stake: misinformation is a growing threat that damages the confidence the public has in the media. As the audience is now getting information through multiple platforms, they don't know how to be sure a piece of news comes from a respected media outlet. In addition, piracy is damaging legitimate service provider revenues and legitimate service providers won't be able to afford to provide high quality services if they continue to lose consumers to piracy.

Media plays a key role in democracies around the world, acting as a watchdog of the state and informing citizens about the decisions that affect their everyday life. The media also plays an important role in raising public awareness of cybersecurity as an amplifier of public messages and a reminder of the importance of good cybersecurity practices. Cooperation with the media also raises awareness across the society of the increasing cybersecurity risks.

Desk research, analysis of surveys and interviews revealed the following good practices based on selected EU Member States:

The Centre for Cybersecurity **Belgium** (CCB) has compiled a document called "ABC of the CCB"[28] with 42 most asked questions and answers regularly disseminated to journalists writing about cybersecurity.

The Czech Republic aims to have one person in every bigger newsroom covering cybersecurity topics. In the case of cyber incidents, these points of contacts will prove useful in knowing, for example, what phishing is and they can spread this information further.

In **Finland**, during elections, special media programs are aired where about half a dozen well-respected journalists dive deep into cybersecurity matters. In 2018, a public-private partnership initiative in Finland called Mediapooli published a book titled *Editor's Encryption Guide* (*Toimittajan Salausopas*)[29] which is a "cyber textbook for journalists" that includes guidance for journalists on how to protect their sources from cyberattacks.

In **Latvia**, before some major events like elections, CERT-LV organises media briefs.

Slovakia, since January 2021, supports a monthly cybersecurity addition in the newspaper *Hospodárske noviny*. This is an attachment with articles and interviews with professionals from the National Cybersecurity Centre and relevant institutions.

To conclude, cooperation between the relevant cybersecurity agencies and the media in Belgium, Czech Republic, Finland, Luxembourg and Slovakia demonstrates ways in which to maintain constructive connections with the media and enable regular practices that provide journalists with more relevant and timely information about cybersecurity threats and risks.

[28] https://ccb.belgium.be/sites/default/files/ABC_CCB_A5_NL.pdf
[29] https://www.mediapooli.fi/wp-content/uploads/sites/3/2020/10/toimittajan-salausopas.pdf

3. REGULAR ASSESSMENTS OF CYBERSECURITY TRENDS AND CHALLENGES

In the interview process of this study, we collected information about whether EU Member States regularly provide their citizens with cybersecurity situational awareness data and information such as assessments, analyses and reports of the threat environment, aside from daily cyber threat overviews. We focused on assessments with the purpose of raising citizens' awareness through analysis of evolving threats and providing practical advice. These publications help citizens to realise how the malicious use of "bits and bytes" in cyberattacks can have spill-over effects on everyday life.

Traditionally, cybersecurity threat information products are technical in nature, for example, the information about vulnerabilities in certain ICT products is typically published on the information channels of the CERT/CSIRT teams.[30] Such information prepared for expert groups is not intended for and remains incomprehensible for the wider, non-technical audiences such as the general public or managers of organisations. Therefore, it is important that the national cyber authorities seek to address the wider public as their audience as well.

Desk research, analysis of surveys and interviews revealed the following good practices based on selected EU Member States:

The **Czech** National Cyber and Information Security Agency publishes annual reports on the state of cybersecurity and publishes the trends of the previous year, based on the information provided by around 200 critical infrastructure institutions.[31] It also shares cybersecurity warnings and recommendations for the general public, such as protecting home devices during the COVID-19 pandemic.

The **Estonian** Information Systems Authority publishes monthly, quarterly and annual cybersecurity assessments.[32] The publication of the annual report is always a media event and news is generated in various media channels based on the report. In addition, the Information Systems Authority publishes threat alerts intended for the general public and security guidelines and advisories for both experts and end users. The Estonian Internal Security Service and Foreign Intelligence Service both publish annual assessments that have a separate chapter on cybersecurity covering the intelligence angle of cyber threats.

The **Finnish** Transport and Communications Agency National Cybersecurity Centre publishes a monthly Cyber Weather report[33] along with an annual report. The Cyber Weather report provides an update on the key information security incidents and phenomena of the month. This is an overview of cybersecurity trends and cyber incidents in the past month. The Cyber Weather news items are assigned one of three categories: calm, worrying or serious. The report is divided into sections about data breaches and leaks, scams and phishing, malware and vulnerabilities, automation, network performance and spying. When relevant, the Transport and

[30] For example, see https://www.cert.europa.eu/cert/filteredition/en/CERT-LatestNews.html
[31] https://www.nukib.cz/en/infoservis-en/publications-reports/
[32] https://www.ria.ee/en/information-system-authority/publications.html
[33] https://www.kyberturvallisuuskeskus.fi/en/ncsc-news/cyber-weather
[1] Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

Communications Agency National Cybersecurity Centre also issues urgent security alerts and vulnerability notifications that draw the attention of citizens.

The Federal Office for Information Security in **Germany** annually publishes "The state of IT security in Germany", usually in autumn.[34] It contains information about cyber threats concerning general users, however, the key focus is on enterprises and the government. The Citizen Awareness Unit in the Federal Office for Information Security uses this report to extract information which is of special interest to general users and translates it to a more illustrative and easy-to-understand communication style. For example, they may use a series of infographics to summarise the most important cybersecurity threats for general users (like phishing, ransomware etc.).[35] In addition, the Federal Office publishes guidelines and various technical papers on a variety of cybersecurity topics throughout the year. In 2020, for example, they issued several guidelines related to the COVID-19 pandemic, such as recommendations for a secure home office and secure online shopping. Focus topics also included strong passwords and two-factor authentication to appropriately protect important data stored in online accounts.

Ireland's Department of Environment, Climate and Communications in 2020 issued via their website over 30 advisories about ransomware attacks on the healthcare sector.

Latvia's CERT.LV provides public reports annually and quarterly, as well as monthly statistics on their web page. Following the Finnish example, once a month, the Latvian national CERT publishes a detailed cyber weather report about past cyber incidents in Latvia on social media. This has been going on for over a year and it has become very popular. Some people comment that this is the only weather forecast they read. The Cyber Weather report is divided into five segments: scams and phishing, malware and vulnerabilities, IoT, data breaches and data leaks, and network performance. If everything is fine, the weather is sunny, if there are a few incidents – it is raining, and if there are a lot of incidents or big financial losses – it is a thunderstorm.

In **the Netherlands,** the National Cyber Security Centre (NCSC) actively publishes high quality regular assessments, such as the Cyber Security Assessment Netherlands compiled in collaboration with the National Coordinator for Security and Counterterrorism. The Cyber Security Assessment Netherlands 2021 provides insight into threats, interests and resilience in relation to cyber security and the effect these factors have on national security.[36] To increase the digital resilience of companies and organisations, the NCSC has also written the Guide to Cyber Security Measures,[37] which lists eight measures every organisation should take to help counter cyberattacks. Examples of these measures are logging of server data, implementing a password policy, making backups and encrypting information.

In **Norway**, NorSIS has a particular emphasis on collecting, organising, and disseminating knowledge about cybersecurity information that matters to the target audience. They publish a threat report once a year, targeted at SMBs, at the request of the Ministry of Justice and public Security. They also conduct an annual survey on the state of cybersecurity culture within the population. The main target group for NorSIS is private and public sector organisations. Their activities are targeted at small and medium-sized private enterprises, local government authorities and the general public. Also, the Military Intelligence Service and the Norwegian Cyber Security Centre publish annual reports that give overviews of various threat scenarios, including cyber space.

[34] https://www.bsi.bund.de/EN/Service-Navi/Publications/SecuritySituation/SecuritySituation_node.html
[35] https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/verbraucherinnen-und-verbraucher_node.html
[36] https://english.ncsc.nl/; https://english.ncsc.nl/topics/cybersecurity-assessment-netherlands
[37] https://english.ncsc.nl/topics/cybersecurity-assessment-netherlands/documents/publications/2021/august/4/guide-to-cyber-security-measures
[1] Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

In **Poland**, the CSIRT of the National Research Institute publishes an annual report titled "The safety landscape of the Polish internet"[38] that includes cybersecurity threat statistics, as well as annual reports regarding Dyzurnet.pl team activities[39]. The Dyzurnet.pl team is a point of contact that has been functioning within the framework of the National Research Institute since 2005. The team responds to anonymous reports received from Internet users about potentially illegal material, mainly related to sexual abuse of children. Additionally, information about cyber threats, expert analyses, and recommendations are also published on the governmental web-portal managed by the Cybersecurity Department of the Chancellery of the Prime Minister.[40]

In **Romania**, the National Cyber Security Directorate provides cybersecurity bulletins weekly, and an annual report about its comprehensive cybersecurity activity.

The **Slovakian** National Cybersecurity Centre SK-CERT provides cybersecurity bulletins once a week and security warnings on ad-hoc basis. Once a year they provide an annual cybersecurity report.

In **Slovenia**, the Government Information Security Office twice a year prepares reports on cyber incidents and attacks, and the national SI-CERT prepares annual reports on cybersecurity. Based on the threat environment, SI-CERT also publishes regular updates on cybersecurity threats and prepares awareness-raising materials.

Finally, providing regular analysis and reports of the threat environment is an important step towards higher cybersecurity awareness. Regular publication of cybersecurity trends and challenges is important because it promotes public discussion about the possible impact cyberattacks can have not only on the particular information systems targeted, but also on national security as a whole.

Regular and accessible assessments also help citizens to realise how each person can contribute to a better protected cyberspace. Effective cybersecurity can only be achieved via a comprehensive approach – an effort that requires a contribution from everyone.

Rendering information about cybersecurity trends and challenges accessible and comprehensible to a non-technical audience enables outreach to wider audiences, including the general public and decision-makers and decision-shapers at political, organisational and societal levels.

Regular publication of cybersecurity trends and challenges is important because it promotes public discussion about the possible impact cyberattacks can have not only on the particular information systems targeted, but also on national security as a whole.

[38] https://en.nask.pl/eng/reports/reports/3835,CERT-2019-Report-PL.html
[39] https://en.dyzurnet.pl/publications
[40] https://www.gov.pl/web/baza-wiedzy/aktualnosci

4. MEASURING CYBERSECURITY BEHAVIOUR

Organisations cannot control their data, but they can control what they care about, meaning what kind of data they care to measure. Good data scientists know that analysing data is the easy part. The key is deciding what data matters.

Gathering data and statistics from public surveys and establishing metrics about the cybersecurity behavioural aspects is a crucial part of successful awareness raising. Quantitative measurement of cybersecurity provides background on cybersecurity thinking and behavioural patterns of people, which gives important guidance for awareness raising activities, in particular during the preparation phase of cybersecurity awareness campaigns.

The lack of common practice for measurement methodology presents us with uncertainties regarding what the relevant indicators for cybersecurity culture really are. Motivation to establish metrics for cybersecurity culture includes providing solid comprehension on how the population relates to the inevitable digitalisation of their society. General information on how citizens perceive digital risks, their attitudes and knowledge can help to provide better direction for choosing measures for protecting the digital environment.

The EU regularly measures the attitudes of Europeans regarding cybersecurity, culminating in a Special Eurobarometer survey conducted to understand the awareness of its citizens, and their respective experiences and perceptions of cybersecurity. It brings together the results of the public opinion surveys regarding cybersecurity in the 27 European Union Member States.

National agencies responsible for cybersecurity awareness raising should use public polls and work in close cooperation with national statistics offices to identify, understand and incorporate the opinions of the wide target audience. Collecting relevant data provides an opportunity to get to know the target group and this helps in deciding what kind of information the target audience needs to improve their skills and knowledge about cybersecurity. It is also useful to analyse cyber incident data to better understand what societal groups have been hurt the most and subsequently analyse what are the best risk mitigation measures.

Desk research, analysis of surveys and interviews revealed the following good practices based on selected EU Member States:

Belgium Safeonweb.be includes a Digital Health Index[41] which is a quick test to determine whether the respondent's digital health needs a boost. The index consists of 15 questions concerning software updates, data back-ups, attacks like phishing, the proper of use anti-virus software and passwords.

CERT-**Croatia** admits that more time and funding is needed for good quantitative research. While they do not conduct surveys, they use other available data, such as the EU kids online

[41] https://www.safeonweb.be/en/digital-health-index

survey and data from member institutions of the national research and education network of Croatia.

The **Czech** National Cyber and Information Security and Agency realised during the analysis process that they lacked statistical data for the analytical part of the awareness raising plan and initiated close cooperation with the Statistics Office in 2021.

The **Estonian** State Information Authority acknowledges that using polls is challenging but extremely useful. The authority uses data from Statistics Estonia, as well as from Eurobarometer. It highly values its cooperation with Statistics Estonia. Following the example of Eurobarometer, the two authorities cooperate and some cybersecurity-related questions have been added to the annual questionnaire of Statistics Estonia, such as what people do online to ensure cybersecurity (using stronger passwords, using different passwords for different websites, cautiously check emails with attachments etc.) In short, Estonia successfully optimised their efforts to be relevant to target audiences via identification of the main areas that need attention through data gathering from Eurobarometer and Statistics Estonia.

Since November 2020, the **Finnish** Digital Agency has a personnel barometer for digital security[42] that consists of questions related to competence and training of digital services / devices from a security perspective, as well as inquiries about what people fear online and what kind of threats people regard as significant. The barometer measures people's trust in their own organisation, public administration and/or private companies to securely handle their data, including personal data. It also asks about the impact the COVID-19 pandemic has had on the work and leisure time of the respondents. Finland also conducts regular organisational polls regarding information security. During 2017–2018, more than 100 organisations and more than 20,000 persons answered over 40 questions regarding training, competence and the threat landscape. The survey will be repeated again in 2022.

In **Germany**, the unit for citizen awareness of the Federal Office for Information Security in cooperation with the police conducts an annual *Digitalbarometer*[43] survey with 2000 participants covering qualitative and quantitative aspects of cybersecurity looking at four areas: behavioural aspects on acquiring information about IT security; personal experience with cybercrime; brand knowledge of the Federal Office for Information Security; and an annual focus topic (previous examples include phishing and home office security). Based on the data from this survey in 2019, BSI expanded their materials on emergency cases. For example, they created leaflets with explanations of what to do in an emergency situation, if a person becomes a victim of fraud, for example.

Another study on cybersecurity behaviour in Germany is the "DIVSI Milieu Study on Trust and Security on the Internet" conducted in 2018 by an independent institute.[44] The study focuses on how people in Germany relate to risks in cyberspace. The central findings of the study form a very broad basis that can be used to identify measures designed to enhance trust and security on the Internet. The study concluded that people's behaviour on the Internet and their attitudes toward trust and security can be divided into seven user types based on their security awareness and usage of information technology (self-assessment). Whereas one user type is more likely to be interested in entertainment topics, another user type is interested in news. This made it possible to position the cybersecurity awareness campaigns accordingly to reach each user type in their habitat.

Latvia does not use broad public surveys on regular basis but has used polls before the launch of national cybersecurity campaigns to set the baseline. Polling before the campaign has been

[42] https://dvv.fi/-/digiturvabarometri-2-2021
[43] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Digitalbarometer/Digitalbarometer-ProPK-BSI_2020.html
[44] https://www.divsi.de/projekte/unterthemen/milieus/index.html ; https://www.divsi.de/wp-content/uploads/2018/11/DIVSI-U25-Studie-euphorie.pdf.

conducted by a marketing agency as part of the campaign, using questions developed by CERT-LV, such as "Have you been a victim of cybercrime?", "How often do you use a computer?. After the campaign the questions were "Have you seen the ads?", "Where did you see the ads?", "Did you like them?. Alternatively, several interagency meetings were organised before a campaign with key public and private cybersecurity players, where statistics and information were shared with the goal to identify causes and potential solutions. One lesson learnt is the need to measure the change in people's behaviour, not only whether people have seen the ads. This is challenging, as the effect is not immediate and behavioural changes can take years to be established.

Luxembourg is currently evaluating the opportunity to implement a more systematic approach to evaluating cybersecurity awareness raising requirements and monitoring the effects of awareness raising campaigns in the context of their most recent NCSS.

In **Norway**, NorSIS publishes an annual survey about cybersecurity[45] where they include a wide variety of indicators in order to explore them further in the analysis of the data collected. Norway conducted a comprehensive pilot study in 2015 based on questions seeking to find out, "What characterises the Norwegian cybersecurity culture?", "To what degree does cybersecurity education influence the Norwegian population's cybersecurity behaviour or awareness?", "How does the Norwegian population relate and react to cyber risks?", "To what degree does the individual take responsibility for the safety and security of the cyberspace?".

As a result of the study[46], NorSIS found a strong correlation between an interest in technology and cybersecurity practices. The study concluded that the Norwegian government should take greater responsibility for cybersecurity education, especially for the young, the old and the unemployed. Another survey in 2017 discovered that young people did not get enough organised lessons on cybersecurity compared to employed people. Therefore, based on capability gaps revealed by the same study, NorSIS prepared materials for students, parents and teachers and marketed them in collaboration with a local county, the Directorate of Education and Training and other partners. NorSIS promotes these resources whenever thematically relevant, for example, on Safer Internet Day.

In **Poland**, the Minister of Digital Affairs together with the National Research Institute regularly conducts a quantitative survey called "Monitoring the results of the campaigns for the dissemination of the benefits of using digital technologies". The survey covers selected aspects of cybersecurity and awareness of various types of threats but also studies which security measures are used by citizens on the Internet. The survey was conducted in 2018 and 2020 and will be held again in 2022. Results from the survey are used to plan communication activities in campaigns. In addition, all available sources of information such as police, CSIRT statistics and research carried out by private or public organisations have been considered when planning the awareness campaigns.

Romania currently does not have a system of metrics and, thus, measures, the activity on the social media of the National Cyber Security Directorate (DNSC). They are engaged in a program of improving their management that is supported by the EU funds. One of the topics in this program is measuring the satisfaction of people using their services. Thus, there are plans to prepare feedback questionnaires for individuals, private enterprises and public agencies in the near future.

In **Slovakia,** national SK-CERT prepares different statistics and reports for its partners as well as the for the public. These are constantly supplemented and expanded as SK-CERT's information resources grow. Three basic groups of statistics are currently being prepared: an

[45] https://norsis.no/wp-content/uploads/2016/09/The-Norwegian-Cybersecurity-culture-web.pdf
[46] Ibid.

overview of detected events (events, alarms) and resolved incidents over time; automatically generated statistics on various areas of the primarily Slovak Internet (Slovak IP address range); and ad-hoc reports and statistics. Some of these statistics are published in the Annual report on Cyber Security in the Slovak Republic.

The **Slovenian** SI-CERT and the Government Information Security Office are planning public awareness campaigns based on incident data from the national CERT and data from the Statistics Office published once a year. For example, in 2019 in Slovenia many people were targeted with love scams from Africa with the scammers pretending to be soldiers on a mission. SI-CERT designed a targeted media campaign, after which the number of incidents declined. Another example demonstrates how in 2020, e-commerce grew due to the pandemic, along with an increase in scams in this field. SI-CERT ran a campaign on e-commerce scams and later a campaign about scams related to cryptocurrencies. The campaigns were based on incident data and established an understanding of the threat landscape.

In **Sweden**, the Civil Contingencies Agency has since 2019 been conducting surveys about people's cybersecurity competencies. Annual surveys enable them to compare behavioural patterns. In 2020, the survey included additional questions about the COVID-19 situation, but the main part of it remained unchanged.

In conclusion, collecting quantitative data on cybersecurity behaviour (including via public surveys and statistics) across the whole of society provides useful and necessary insight for planning more targeted and effective awareness raising activities, thus facilitating more successful outcomes.

Existing regular public opinion surveys such as the Eurobarometer can serve as a useful starting point for nations striving to connect data with awareness raising activities. In addition to data from Eurobarometer, drawing on systematically collected aggregate data from national CERTs and the law enforcement agencies about cyber incidents and cybercrimes can highlight trends and be used to build situational awareness. That data, in turn, helps to identify and tailor the awareness campaigns.

An important success factor in raising citizens' awareness is to connect the operational and societal perspectives of awareness raising. The best way to combine those perspectives is to make the governmental entities that are responsible for the operational perspective also responsible for raising cybersecurity awareness, such as has been done in the case of the Federal Office for Information Security in Germany, the Information System Authority in Estonia or the Centre for Information Security in Norway.

Using public polls and fostering close cooperation with national statistics offices helps to better identify, understand and reach specific target audiences.

Using **public polls** and **fostering close cooperation** with national statistics offices helps to better identify, understand and reach specific target audiences.

5. PLANNING FOR CYBERSECURITY AWARENESS CAMPAIGNS

To identify good practices for planning cybersecurity awareness campaigns, we studied the following questions:

- What are the best ways to reach target audiences?
- What were the goals and objectives that these cybersecurity awareness campaigns aspired to achieve?
- How did they identify target audiences?
- What were the specific topics covered by the campaigns?
- How did they connect the messages to the target groups?

5.1 MAIN CHALLENGES AND LESSONS LEARNT ABOUT EFFECTIVE CAMPAIGNING

Changing people's attitude takes time so it is important to have strategic patience. It is useful to keep in mind that it took ten years to make people use seatbelts in cars. Cybersecurity awareness campaigns also require a careful balance to both highlight threats that are present in cyberspace, while at the same time establishing capacity to keep personal data safe and maintain trust in digital services.

It is important to identify all target groups to ensure no-one gets left behind. Some target groups, however, may be notoriously difficult to reach, such as the elderly, as well as people with lower education and socioeconomic wellbeing. Regarding finding the right ways to approach various audiences in the general public, Member States underline the significance of using a variety of different channels, such as games, videos, seminars and social media. Note that to effectively engage with users on various social media platforms such as Facebook, Twitter and Instagram may require further knowledge about content creation.

Moreover, lack of resources remains a challenge. There should be a whole-society approach towards cybersecurity, but often, there are not enough resources to address every group, which limits the scope of outreach. To overcome the problem, attempts to cooperate with different entities who are willing to help amplify the cybersecurity awareness raising content in their communities can be helpful.

Throughout the campaign, Member States underline the usefulness of defining key performance indicators, as well as conducting market research before and during each media campaign to measure the marketing effectiveness. In addition, regular monitoring reports show the development of the campaign effects online and in social media networks.

It is worth noting that Member States generally recognise the usefulness of the European Cybersecurity Month as an amplifier of cybersecurity awareness activities.

Desk research, analysis of surveys and interviews revealed the following good practice regarding planning awareness campaigns from select EU Member States:

The Centre for Cybersecurity in **Belgium** organises tenders for a three-year contract period to guarantee continuity in creative concept and visual style. The On Safe on Web website Belgium gathers links to commonly used websites like Facebook and Amazon that redirect users to the pages on those sites where people can set up the two-factor authentication. Before the COVID-19 pandemic, a federal awareness raising truck drove around the country to meet people in small towns. These meetings revealed that some people knew shockingly little about cybersecurity. In order to reach the widest audience, the Safe on Web website is intentionally kept simple.

Croatia links awareness activities outside campaigns to a particular day, for example: Safer Internet Day, Password Day, Consumer Rights Day, or Data Protection Day. When developing a communication strategy and the creative concept of the campaign, the goal was not to create fear, but rather to try to impact the way people think and behave. The message "Think how you use personal data on the Internet" was based on the profile of an average overly confident and naïve user who does not care too much about online safety. This is where the name "Great Croatian Naives" comes from. Seven profiles of cybercrime victims were created with central topics including safe passwords, phishing sites, personal data, scams, ID theft etc.

The **Czech Republic** developed mandatory courses addressing cybersecurity threats for civil servants for the 2022 EU Council Presidency of the Czech Republic. These courses can be adjusted for other sectors such as healthcare, police, education and other civil servants. A special outreach was organised for the elderly based on a study of 500 senior people, which illustrated their online activity. Under the cybersecurity Framework Educational Program, Czech schools organised cybersecurity campaigns promoting the topic among high-school students and their teachers.

Estonia's Information System Authority admits that finding resources for conducting polls is challenging. When running a campaign and organising a procurement for partners, the Estonian authority asks a procurement partner to conduct either quantitative or qualitative research about a particular target group. For example, when organising a campaign for the elderly, the procurement partner conducted an online poll asking how citizens behaved online and discovered that people under 55 were much more aware of best practices for secure online behaviour than those over 55. The discovery resulted in the 2019 campaign focusing on the elderly. In 2020, the data from Statistics Estonia showed that 2–3% of enterprises experienced cyber incidents, but small and medium-sized businesses did not know how to deal with them, because of their insufficient IT and information security practices. An awareness campaign for small and medium enterprises followed. During that campaign, prior work with a focus group of Russian and Estonian speaking entrepreneurs revealed that knowledge about how to deal with insider threats was essential for entrepreneurs.

In **Finland**, a recent campaign focus has been on new kinds of threats related to the use of social media services and fraud phone calls, SMSs, email messages and web-services. In 2020, in a spontaneous pop-up campaign mode, a cybersecurity expert from the Digital and Population Data Services Agency (DVV) recorded a Microsoft technical scam call and exposed it on his personal LinkedIn and Twitter pages. Within a few days, the recorded scam call became one of the major news items and an estimated 1.5 to 2 million people learnt about it. Another occasion that attracted media attention was the March 2021 Facebook data breach which exposed the data of 1.2 million Finnish users. Over one million people learnt about the event. A combination of social media and traditional media seems to be the best way to get the attention of the Finnish public. Unfortunately, mostly negative news attracts the media attention.

Germany selected five topics after an analysis of the publicly assessable studies, surveys and reports. The main framing campaign (published in March 2021) started raising awareness of five main topics in general: Home Office, Smart Home (Smart TV), Social Media, Gaming, and Online-Shopping. Each advertisement shows the main message to the audience in a hashtag

slogan format (e.g. #einfachaBSIchern "#simplysecured") and is linked to the Federal Office for Information Security (BSI) website. Each topic has its own teaser page to allow people who are more interested to look for further information.

Ireland is working on developing national curriculum courses for children between the ages of 12 and 15, such as a computer science course, coding and digital media literacy. One of the three key aspects is cybersecurity hygiene. The goal is to attract young people from both genders and from diverse social backgrounds with the goal of encouraging them to study more science, technology, engineering and mathematics.

Italy launched an awareness campaign about ransomware targeting CISOs and IT administrators and consisting of guidelines detailing mitigation measures and in-depth analysis about ransomware attacks: Netwalker and Egregor. Furthermore, during the cybersecurity attacks related to Solarwinds and Microsoft Exchange, the Italian National CyberSecurity Cell (NCSC) and the CSIRT Italia launched a specific awareness campaign on their website, as well as set in motion point-to-point alerts containing updates, mitigations and best practices for the users of Facebook, Microsoft and Solarwinds. More recently, as a consequence of ransomware attacks, the CSIRT Italia published additional guidance and published a dedicated section on their website containing all the relevant documentation.

In **Norway**, one of the largest campaigns was prepared in parallel to drafting the NCSS, when a group with experts from both the public and private sector brainstormed to come up with the ten most important basic pieces advice about cybersecurity to give all companies in Norway. A recent survey has shown the advice had a large impact on the audiences that received it.

The government in **Poland**, to counter the problem of kids' online abuse and YouTube showing highly violent content, swearing, heavy drinking and other inappropriate behaviour to children, produced a campaign for parents titled "Do Not Lose Your Child Online". They launched it before a summer vacation, because it was noted that during the summer holidays, kids were often left alone to browse in the net. The government also alerted parents about the inappropriate type of content and encouraged them to use solutions from Google and Microsoft for parental controls. A dedicated guide to be "Be Safe on Social Media" was published which gave details of how to configure security settings to help keep children safe. Another campaign for kids in Poland was "Be From a Different Fairy Tale" which targeted toddlers going to primary school with their first tablets and consisted of customised movies related to fairy tales like Frozen, Red Hat, Gold Fish along with messages and movies for parents teaching them to introduce the content to their kids.

Portugal had a campaign for raising the cybersecurity awareness of girls. It was meant to reduce the gender gap in cybersecurity awareness and to motivate girls to study that field. It was hard to find the best approach to reach these women and girls. In the future, Instagram could be a possible channel. Underlining specific content for awareness and training, like password use, available contacts after a cyberattack, and ICT security policies in organisations works better than promoting fear and highlighting risks. Via feedback from quality assessment surveys after training if was found that citizens were eager to have more technical and practical knowledge about cybersecurity.[47]

In **Romania**, the most recent outstanding campaign from 2021 was the National Antifraud Campaign, organised by the National Cyber Security Directorate (DNSC) in collaboration with the Romanian Police and the Romanian National Banks Association. It involved a mock attack and explaining to regular users how the attacks work and how to avoid them. It was targeted

[47] For a list for of cybersecurity awareness campaigns in Portugal, see https://www.cncs.gov.pt/docs/relatorio-sociedade2020-observatoriociberseguranca-cncs-1.pdf, p. 106.

towards all credit cards users, because the DNSC observes a lot of criminal activities related to extracting money from credit cards.

In **Slovakia,** the Cyber Security Competence and Certification Centre is responsible for organising training, educational events and security awareness campaigns. The Competence Centre, together with SK-CERT and the NSA, participates in the preparation of events aimed at raising awareness in the cybersecurity space. Such events include the ITAPA, a large conference on digitisation and new technologies, the annual GLOBSEC security conference etc.

In conclusion, to achieve successful cybersecurity awareness campaigns, public communication and marketing experts should be involved for appropriate message framing. Message framing is the strategy for communicating a complex societal problem in such a way that the main arguments are clearly understandable and cannot be easily challenged.

The EU-wide practice of organising campaigns during the European Cybersecurity month of October is a good practice but it is not sufficient. The awareness raising activities and campaigns to engage EU residents should be carried out throughout the year.

6. RECOMMENDATIONS

This report proposes recommendations to increase the effectiveness of national awareness raising activities, based on the research of existing NCSS, and from information provided by identified stakeholders who were interviewed for this study. This report provides good practices, challenges, lessons learnt and a set of recommendations for further improvement.

The recommendations are divided into four areas:

(1) building capacities for cybersecurity awareness,

(2) regular assessments of cybersecurity trends and challenges,

(3) measuring cybersecurity behaviour, and

(4) planning for cybersecurity awareness campaigns.

6.1 BUILDING CAPACITIES FOR CYBERSECURITY AWARENESS

- Develop within the NCSS a clear vision for national cybersecurity awareness raising, assigning clear roles and responsibilities to the different stakeholders involved. This will help in developing further national cybersecurity capacities and establish a better outlook on the topic.

- Develop specified concrete measures, tasks, and deliverables to address the objective of society's cybersecurity awareness within the implementation plan of the NCSS. This will help to establish a firmer foundation to achieve success in raising awareness.

- Back the mission and mandate of the entities involved in the building of cybersecurity awareness with legal acts, where possible. This will help in justifying actions and addressing any practical details that might be vague and unclear.

- Consider assigning the central coordination role for awareness raising activities to a single institution. This can be helpful, however, there are also some successful exceptions that represent a horizontal spread of tasks. It can be concluded that ensuring accountability and progress requires that all parties involved should have a clear understanding of their respective roles and responsibilities, which can be more straightforward to achieve with central coordination but does not exclude horizontal governance models.

- Engage public and private actors together in awareness raising activities both at a national and regional level to ensure synergistic actions in all areas: legal, organisational, technical and educational, as well as cooperation between public administration and the private sector. This can help to achieve efficient cybersecurity awareness raising campaigns.

- Cover awareness-raising objectives by financing. This is an important factor for the successful implementation of public awareness activities. Sufficient, consistent and continuous funding provides the foundations for an effective national cybersecurity posture.

6.2 REGULAR ASSESSMENTS OF CYBERSECURITY TRENDS AND CHALLENGES

- Provide regular analysis and reports of the threat environment. This is an important step towards higher awareness. Regular analysis and reports aim to inform citizens and ICT experts, decision-makers and society in general, to create cybersecurity awareness. They promote common understanding of threats and foster the concept of cybersecurity being a joint contribution, requiring efforts at state, organisational and individual level.

- Render information about cybersecurity trends and challenges that will be accessible and comprehensible to a non-technical audience. This will enable outreach to wider audiences including decision-makers and decision-shapers at political, organisational and societal levels.

6.3 MEASURING CYBERSECURITY BEHAVIOUR

- Collect quantitative data across the whole of society on cybersecurity behaviour. Quantitative measurement of cybersecurity provides background on the cybersecurity thinking and behavioural patterns of people. This gives important guidance for awareness raising activities. Public surveys and statistics can provide useful and necessary insights for planning more targeted and effective awareness raising activities facilitating successful outcomes.

- Utilise existing regular EU-wide public opinion cybersecurity surveys, such as the Eurobarometer, as a helpful starting point for nations striving to connect data with awareness raising activities. Eurobarometer is the polling instrument used by EU institutions and agencies to regularly monitor the state of public opinion in Europe on attitudes on subjects of political or social nature. The aim of the Eurobarometer is to provide quality and relevant data for experts in public opinion and the general public alike. Eurobarometer data on cybersecurity reveals what concerns Europeans have about internet interactions. It uncovers whether concern about security issues has made people change the way they use the Internet. The combination of the wide range of topics covered, the regularity of publications and the geographical coverage makes the Eurobarometer a unique source of knowledge about what Europeans think.

- Draw on systematically collected aggregated data from national CERTs and law enforcement agencies about cyber incidents and cybercrimes to help identify trends and to build situational awareness. That data, in turn, helps to better understand which specific societal groups have been hurt the most and subsequently determine the best risk mitigation measures to use. It also helps to target and tailor the awareness campaigns.

- Use public polls and foster close cooperation with national statistics offices to better identify, understand and reach target audiences. Understanding how people perceive risks is critical to create effective awareness campaigns. Collecting relevant data provides a basis to get to know the target group and decide what kind of information the target audience needs to improve their skills and knowledge about cybersecurity.

6.4 PLANNING FOR CYBERSECURITY AWARENESS CAMPAIGNS

- Involve public communications and marketing experts for appropriate message framing, that is, in the strategy of communicating a complex societal problem in such a way that the main arguments are clearly understandable and cannot be easily challenged. Professional message framing in cybersecurity awareness campaigns helps to build a greater understanding of cybersecurity communication to address human factors in cybersecurity. This can assist in creating successful cybersecurity awareness campaigns.

- To release awareness campaigns during the European Cybersecurity month of October, an EU-wide practice, is a good practice but that alone is not sufficient. The awareness raising activities and campaigns to engage EU citizens should be carried out throughout the year in every Member State. This is important as improving information security practices and promoting a sustainable society requires efforts that extend beyond one month per year.

7. BIBLIOGRAPHY

BSI Act of 14 August 2009 (Federal Law Gazette I p. 2821) last amended by Article 1 of the *Act of 23 June 2017* (Federal Law Gazette I p. 1885)

Center for Cyber Security Belgium, *Het ABC van Het CCB – Cyberveiligheidsjargon in 42 Antwoorden*, 2020

CNCS, *Estratégia Nacional de Segurança do Ciberespaço 2019–2023*, 2019

ENISA, Threat Landscape report, *From January 2019 to April 2020. The Year in Review*, 2020

Informative Statement Cybersecurity Strategy of Latvia 2019–2022, Riga, 2019

ISO/IEC 27032:2012, *Information technology – Security techniques – Guidelines for cybersecurity*, 2012

ENISA, NCSS Good Practice Guide, 2016

ENISA, National Capabilities Assessment Framework, 2020

ITU, Guide to developing a national cybersecurity strategy – Strategic engagement in cybersecurity, 2018

Justis- og beredskapsdepartementet, Kunnskapsdepartementet, *Nasjonal strategi for digital sikkerhetskompetanse*, 2019

Ministry for Competitiveness and Digital, Maritime and Services Economy, *Malta Cyber Security Strategy 2016*

Ministry of Economic Affairs and Communications, *2019–2022 Cybersecurity strategy – Republic of Estonia*

Ministry of Finance, *Digital Security in the Public Sector – Public Sector ICT*, Helsinki, 2020

National Security Authority, *The National Cybersecurity Strategy 2021–2025*, Bratislava, 2021

NATO CCDCOE, *Recent Cyber Events: Considerations for Military and National Security Decision Makers*, No 10, 2021

NorSIS (Norwegian Centre for Information Security), The Norwegian Cyber Security Culture, 2016

NÚKIB, *National Cyber Security Strategy of the Czech Republic*

Nurse J.R.C., Cybersecurity Awareness, In: Jajodia S., Samarati P., Yung M. (eds) *Encyclopedia of Cryptography, Security and Privacy*. Springer, Berlin, Heidelberg, 2021

Republic of Slovenia, *Cyber Security Strategy – Establishing a System to Ensure a High Level of Cyber Security*

Republic of Slovenia, *Zakon o informacijski varnosti (Information Security Act)*, 2018

Secretariat of the Security Committee, *Finland's Cyber Security Strategy 2019*, 2019

US NIST CSRC, *SP 800-16 Information Technology Security Training Requirements: a Role- and Performance-Based Model*, 1998

Wedenborg, F. *Toimittajan Salausopas (Editor's Encryption Guide)*, 2018

ANNEX A: QUESTIONNAIRE

1. NATIONAL FRAMEWORK FOR IMPROVING CITIZENS' CYBERSECURITY AWARENESS

The purpose of this part of the questionnaire is to provide an understanding about EU Member States' structured plans to raise cybersecurity awareness among its general population.

1.1. Does your country have a national cybersecurity strategy/policy that addresses the objective of cybersecurity awareness raising? (Please indicate a reference to the strategy and relevant strategy objectives.) Are these objectives further specified with concrete measures, tasks and deliverables in the strategy implementation plan? Are these objectives covered with financing?

Please provide your answer in writing:

1.2. Do other strategy/policy/legal documents guide national cybersecurity awareness-raising activities?

Please provide your answer in writing:

1.3. Is there a national agency coordinating and/or overseeing citizens' cybersecurity awareness? Please describe its tasks relating to cybersecurity awareness raising.

Please provide your answer in writing:

1.4. What other public and private actors are engaged with cybersecurity awareness raising on a national level? Or on a regional level? Please tick all that apply.

☐ Law enforcement agencies

☐ Educational institutions

☐ Professional public-private IT associations

☐ Civil society organisations

☐ Telecommunications companies

☐ Banks

☐ Other (please specify)

Comments:

2. REGULAR ASSESSMENTS OF CYBERSECURITY TRENDS AND CHALLENGES

The purpose of this part of the questionnaire is to take stock of regular activities of national cyber authorities in publishing assessments of cybersecurity trends and challenges seeking to address the wider public as their audience with the purpose to raise citizens' awareness of cyber threats, to analyse evolving threats and provide practical advice.

2.1. Aside from daily cyber threat overviews, do you regularly provide cybersecurity situational awareness data and information to your citizens (i.e. assessments, analysis and reports of threat environment)? Please explain.

Regularity (Please tick all that apply):

☐ Monthly

☐ Quarterly

☐ Annual

☐ Other (please specify)

Please provide your answer in writing:

2.2. Are there target groups you specifically focus such awareness activities on (e.g. with tailored information)? What are these target groups? How do you identify these target groups?

Target groups (Please tick all that apply):

☐ Children

☐ Youth

☐ Parents

☐ Elderly

☐ Small and medium-size enterprises (SMEs)

☐ Healthcare sector

☐ Other (please specify)

Please comment:

2.3. What channel of communication of cyber threats to the public has proven to be particularly useful?

Please provide your answer in writing:

2.4. Do you have any special cooperation framework with or training programme for journalists?

Please provide your answer in writing:

3. METRICS ON CYBERSECURITY BEHAVIOUR

The purpose of this part of the questionnaire is to understand what data matters for EU Member States when they prepare for cybersecurity awareness campaigns. It provides an understanding about if and how the EU Member States are gathering metrics about cybersecurity behavioural aspects. This is relevant, because it provides an important background on the cybersecurity thinking and behavioural patterns of people. Metrics are what you measure. You can't control your data, but you do control what you care about. And what you measure is what you manage. [48]

3.1. Other than Eurobarometer, do you measure public cybersecurity behavioural aspects as a basis for conducting campaigns on cyber awareness?

Please provide your answer in writing:

3.2. Do you use quantitative or qualitative methods for that? Please indicate means/channels, target groups and regularity of such polling. For example, are you conducting polls on the needs, key concerns, interests and prior information security knowledge of the people?

Please provide your answer in writing:

3.3. What aspects of collecting quantitative and qualitative data about the cybersecurity behaviour of people has proven to be particularly useful in conducting cybersecurity awareness raising campaigns? What was most challenging?

Please provide your answer in writing:

[48] https://hbr.org/2013/03/know-the-difference-between-yo

4. PUBLIC CYBERSECURITY AWARENESS CAMPAIGNS

The purpose of this part of the questionnaire is to identify best practices about cybersecurity awareness campaigns.

4.1. Other than Cybersecurity Month, which recent cybersecurity awareness campaigns carried out in your country would you consider most significant? Please indicate campaign name, time, organising entity, target groups, and format.

Please provide your answer in writing:

4.2. What were the goals and objectives that these cybersecurity awareness campaigns aspired to achieve?

Please provide your answer in writing:

4.3. How were the target audiences identified?

Please provide your answer in writing:

4.4. What were the specific topics covered by the campaign? How did you choose the content for the campaign? How did you connect messages with the target groups?

Please provide your answer in writing:

4.5 How do you evaluate the effectiveness of these campaigns? How much and what kind of measuring of the target group awareness took place before and after the awareness campaign?

Please provide your answer in writing:

4.6. Did you establish metrics to better identify lessons learned? What metrics proved most effective in measuring the success of information security awareness activities?

Please provide your answer in writing:

4.7. What were the main lessons learned from the successful awareness campaigns?

Please provide your answer in writing:

ANNEX B: MEMBER STATES DATA ON AWARENESS CAMPAIGNS

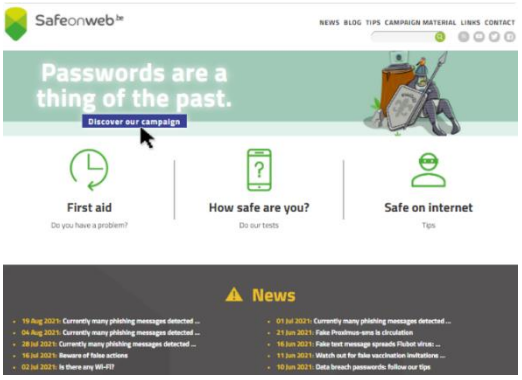
B.1 BELGIUM

Institution Interviewed: Centre for Cyber Security Belgium

General framework: Cyber Security Strategy – Belgium – Securing Cyberspace – 2012

Metrics on cybersecurity behaviour: Statbel – Four Belgian enterprises out of five use ICT security measures – 2019

Regular cybersecurity assessments published by: Centre for Cyber Security Belgium and Federal Computer Emergency Response Team



Existing cybersecurity awareness campaign(s):

Safe on Web

- It is managed by the Centre for Cyber Security Belgium.
- Every two years they do a campaign about phishing (2017, 2019 and 2021).
- In 2018, the campaign was about backups and updates.
- In 2020 the campaign was about two-factor authentication.

Greatest challenge(s) relative to cybersecurity awareness:

- Administration (e.g. agreements and MoUs);
- Complex backend of efforts;
- Multilingualism (i.e. campaigns are in four languages: Dutch, French, German and English) and the difficulty in finding local alliances with Flemish and German speakers.

Main lesson(s) learnt (to be shared with other Member States):

- Have a lot of partners.
- Learn your target audience: what, why and how they behave.
- Encourage people to do something concrete. Campaigns should be practical. "Static" content is not very efficient.
- Keep your messages simple and positive. Use humour.
- Don't scare people. Empower them with the tools to be safe online.
- Repeat your messages.

B.2 CROATIA

Institution Interviewed: National Computer Emergency Response Team (CERT)

General framework: National Cyber Security Strategy – 2015 (in Croatian)

Regular cybersecurity assessments published by: National CERT

Existing cybersecurity awareness campaign(s): Great Croatian Naives

- National campaign "2019 Great Croatian Naives", possible thanks to the Connecting Europe Facility funding.
- It used TV, Facebook, Twitter, YouTube and web banners were placed on youth portals.
- It presented 30-second movies, which were seen by 44.21% of the population within 1.5 months.

Greatest challenge(s) relative to cybersecurity awareness:

- Finding a simple and original message.

Main lesson(s) learnt (to be shared with other Member States):

- Keep it short, simple, original and understandable.
- Prepare interactive materials (i.e. quizzes, games, questionnaires etc.)

B.3 CZECH REPUBLIC

Institution Interviewed: National Cyber and Information Security Agency

General framework: National Cyber Security Strategy of the Czech Republic for the period from 2021 to 2025

Metrics on cybersecurity behaviour: Czech Statistical Office – Information Society in Figures – 2021

Regular cybersecurity assessments published by: National Cyber and Information Security Agency

Existing cybersecurity awareness campaign(s):

E-Bezpečí (E-Safety)

Bezpečně na netu (Safely on the Net)

Festivalu bezpečného internetu (Safe Internet Festival)

- Coordinated by the National Cyber and Information Security Agency;
- Engages multiple organisations from the private and non-profit sector;
- Activities include webinars, videos, competitions etc.

Greatest challenge(s) relative to cybersecurity awareness:

- Interagency understanding is important, as every agency has its own agenda.
- The attitudes of people, since many do not see cybersecurity as a problem, or they think that somebody else is doing cybersecurity for them.

Main lesson(s) learnt (to be shared with other Member States):

- More effort should be put into recruitment campaigns; there is a need for more cybersecurity experts, as well as lawyers.
- It is important to go out and talk to people.
- There should be a whole-of-society approach to cybersecurity.

B.4 DENMARK

Institution Interviewed: Danish Agency for Digitisation

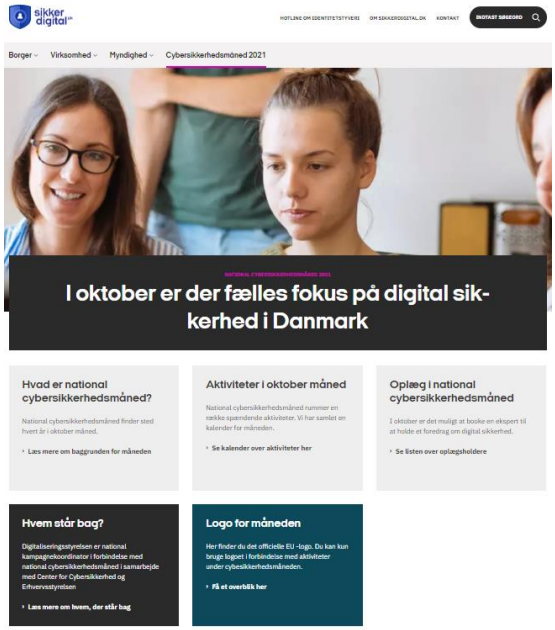
General framework: Danish Cyber and Information Security Strategy 2018-2021

Regular cybersecurity assessments published by: The Centre for Cyber Security (CFCS)

Existing cybersecurity awareness campaign(s):

Industriens Fond Cyber Effort

European Cyber Security Month



- They were coordinated by Sikker Digital (Secure Digital).
- Prior to the big campaign in October, smaller campaigns are held (in 2021 they focused on ID theft, strong passwords, fraud in gaming).
- This year, the campaign has been always-on (non-stop for the whole year).

Greatest challenge(s) relative to cybersecurity awareness:

- Budget, you need a huge budget for advertising;
- Cybersecurity is not something that is in people's minds; they respond to it only if it becomes a headache.

Main lesson(s) learnt (to be shared with other Member States):

- Use behaviour-engaging content, humour and irony; if you use engaging content people will remember.
- Using YouTube has been effective.

B.5 ESTONIA

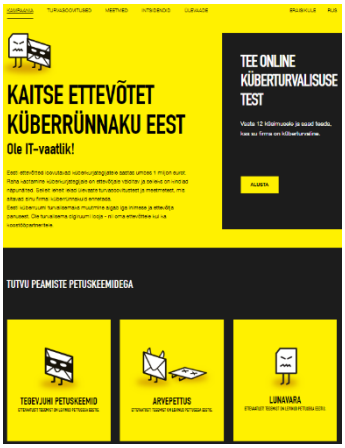
Institution Interviewed: Information System Authority (RIA)

General framework: Cybersecurity Strategy 2019–2022

Metrics on cybersecurity behaviour published by: Statistics Estonia

Regular cybersecurity assessments published by: Information System Authority (RIA)

Existing cybersecurity awareness campaign(s):



Ole IT-vaatlik! (Be IT-Conscious!)

- IT is managed by the RIA.
- In the last two years, two large-scale campaigns were implemented; both campaigns used the same slogan "SecureIT" and they started in September and lasted until November.
- The 2019 campaign targeted people over 55 years old and their family and friends; the 2020 campaign targeted micro, small and medium business leaders.

Greatest challenge(s) relative to cybersecurity awareness:

- Finding a consistent stream of budget;
- Identifying target groups.

Main lesson(s) learnt (to be shared with other Member States):

- If things are written in the Strategy, it is easier to get funding for them.
- People who work in sectors other than IT (such as those selling tires or growing food, for example) need a lot more attention.
- The most important target groups are usually those who are the most difficult to approach, and you need to go where your target audience is.

B.6 FINLAND

Institution Interviewed: Digital and Population Data Services Agency

General framework: Finland's Cyber Security Strategy 2019

Regular cybersecurity assessments published by: National Cyber Security Centre

Existing cybersecurity awareness campaign(s):

- In Finland, there is no centralised agency that is responsible for everything related to cyberspace; and since there is no central organisation for awareness raising, other public and private organisations are responsible for training and awareness.
- There aren't many national campaigns, but many smaller activities are going on simultaneously.

CYBERDI

Huijarit kuriin! (Scammers Disciplined!)

Greatest challenge(s) relative to cybersecurity awareness:

- It is difficult to find the right ways to approach the citizens.

Main lesson(s) learnt (to be shared with other Member States):

- We need to have different voices to reach a wider audience.
- We have to have games, videos, seminars and other different media because different people like to learn in different ways.

B.7 FRANCE

General framework: French National Digital Security Strategy – 2015

Regular cybersecurity assessments published by: CERT-FR

Existing cybersecurity awareness campaign(s):

Cybermalveillance

EDUCNUM

B.8 GERMANY

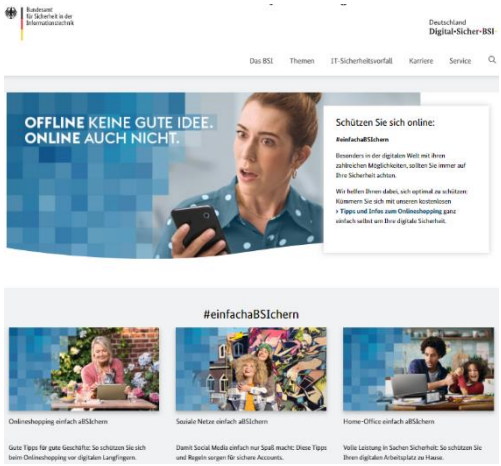
Institution Interviewed: Federal Office for Information Security (BSI)

General framework: Cyber Security Strategy for Germany 2016 (in German)

Metrics on cybersecurity behaviour published by: Federal Statistical Office, DSiN Security Index 2020

Regular cybersecurity assessments published by: Federal Office for Information Security (BIS)

Existing cybersecurity awareness campaign(s):



#einfachaBSIchern (#simplysecured)

- It is managed by the Federal Office for Information Security (BSI) and the Federal Ministry of Interior, Building and Community (BMI).
- It uses a mix of marketing measurements like Out-of-Home, Digital and Social Media Ads as well as radio ads to increase awareness about cybersecurity and information for citizens.
- The campaign aims to reach all citizens in Germany, especially the audience that is generally not at all or very little self-aware of the importance for self-help and self-protection using digital appliances.

Greatest challenge(s) relative to cybersecurity awareness:

- Within marketing activities it is difficult to judge the effectiveness of out-of-home and print advertisements, as it is uncertain how many people really see these ads; also both kind of advertisements need a high media budget for a nationwide reach.
- Keeping information and messages on complex issues of cybersecurity very easy to understand for consumers is challenging.

Main lesson(s) learnt (to be shared with other Member States):

- Send positive messages to emphasise that everyone can to improve their cybersecurity skills with some easy steps. Make a niche topic more interesting with a humorous approach.

- When planning marketing activities:
  - Use very short video ads to capture the user's attention.

- Focus on digital advertisements and plan out-of-home, print and radio ads selectively according to certain topics or phases of the campaign, to diversify your marketing approach.
- Continue to observe the metrics throughout the years to see the development and to adjust the campaign(s) where necessary.

B.9 IRELAND

Institution Interviewed: Cyber Security Policy Division, Department of Environment, Climate and Communications

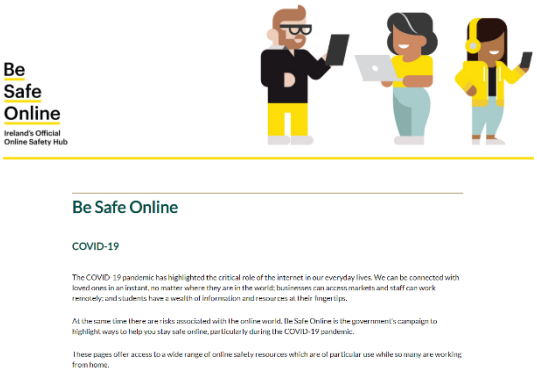
General framework: National Cyber Security Strategy 2019–2024

Metrics on cybersecurity behaviour published by: Central Statistics Office

Regular cybersecurity assessments published by: National Cyber Security Centre (NCSC)

Existing cybersecurity awareness campaign(s):

- Ireland takes an informal approach and the campaigns are not structured. For example, a 'working from home' themed campaign evolved based on political needs, the interests of the CSIRT, the competencies of the NCSC.
- There are volunteer groups, private sector interests and private CSIRTs that attempt to get the message out there.



Webwise.ie

Be Safe Online

- A governmental initiative that aligns and brings together cross-government activities in a single site.
- It includes a wide range of topics, for example, alerts parents to the problem of child exploitation, appropriate use of online tools by teenagers, how to effectively secure your account or personal device, among others.

Greatest challenge(s) relative to cybersecurity awareness:

- Existing scepticism as to whether awareness campaigns are really changing behaviour; it's a question about if we should address this through education, through employers or private advocates.

B.10 ITALY

Institution Interviewed: Presidency of the Council of Ministers[49]

General framework: National Strategic Framework for Cyberspace Security – 2013, 2017 Cybersecurity Action Plan

Metrics on cybersecurity behaviour: National Institute of Statistics – Cittadini e ICT (Citizens and ICT) - 2019

[49] In August 2021, the National Cybersecurity Agency (NCA) was established in Italy, responsible for the development of a national cybersecurity culture.

Regular cybersecurity assessments published by: CSIRT Italy, CERT-AGID (CERT of the Italy Digital Agency)

Existing cybersecurity awareness campaign(s):

Generazioni Connesse (Connected Generations)

Be Aware. Be Digital.

- Created by the Security Intelligence Department, in cooperation with national public television.
- It includes a mobile game to engage the youth; in the game Cybercity Chronicles, the player experiences different kinds of cyberattacks and learns how to deal with them.

Greatest challenge(s) relative to cybersecurity awareness:

- Defining messages: cyberspace provides a lot of opportunities as well as risks, and a balance must be found when creating cybersecurity awareness messages.

Main lesson(s) learnt (to be shared with other Member States):

- It is important to create the right message for the audience, and to keep it simple and not go into too much detail so people can understand the technical concepts.
- It is not enough only to pass on information, it is necessary to get people engaged emotionally.

B.11 LATVIA

Institution Interviewed: National Computer Emergency Response Team (CERT)

General framework: National Cyber Security Strategy 2019–2022 (in Latvian)

Metrics on cybersecurity behaviour published by: Official Statistics Portal

Regular cybersecurity assessments published by: CERT.LV

Existing cybersecurity awareness campaign(s):

Drošs Internets (Safe Internet)

Mana Drošiba (My Safety)

Neuzķeries! Esi gudrāks par krāpniekiem! (Don't get caught! Be smarter than fraudster!)

Latvia "Cyber security in the workplace"

- Presented on the Esidrošs (Self-confident) site which is maintained by the CERT.LV.
- It includes four informative videos and a digital handbook.
- It used outdoor ads, social media (using the assistance of three known influencers) and information in news portals to encourage people to watch the videos and open the handbook.

European Digital Week

- Organised by the Ministry of Environmental Protection and Regional Development of the Republic of Latvia and Latvian Information and Communications technology association (LIKTA);
- Targets enterprises and the general public.

Esi reāls (Be real)

- Organised by the Consumer Rights Protection Centre;
- Targets users of social networks.

Greatest challenge(s) relative to cybersecurity awareness:

- How to best address and reach the society;
- How to be a good organiser of an awareness raising campaign.

Main lesson(s) learnt (to be shared with other Member States):

- People are not interested in education about prevention, they respond more to the scary and dangerous things, i.e. real-time warnings about real threats.
- People may understand the message and like it, but at the same time they may not change their behaviour, at least not immediately; getting people to behave securely online can also require a lot of time.
- Our statistics showed that peak interest was during the first week of a campaign; several short campaigns in different seasons might be preferrable to month-long campaigns.

B.12 LITHUANIA

General framework: National Cyber Security Strategy – 2018 (downloadable document, in Lithuanian)

Metrics on cybersecurity behaviour published by: Official Statistics Portal

Regular cybersecurity assessments published by: Ministry of National Defense

Existing cybersecurity awareness campaign(s):

Sustiprink Imuniteta (Boost Immunity)

Draugiškas Internetas (Safer Internet)

Esaugumas (Security)

B.13 LUXEMBOURG

Institution Interviewed: Ministry of State, High Commission for National Protection

General framework: National Cyber Security Strategy 2018–2020, Cyber Defense Strategy 2021

Regular cybersecurity assessments published by: GOVCERT.LU

Existing cybersecurity awareness campaign(s):

Smart and Secure

- A combined project of EIG SECURITY MADEIN.lu with its department CASES.lu (Cyberworld Awareness and Security Enhancement Services), ANSSI.lu (Agence Nationale de la Sécurité des Systèmes d'Information), SIGI.lu (Syndicat Intercommunal de Gestion Informatique), POST Luxembourg and the Representation of the European Commission in Luxembourg.
- Its topic was on information security risks related to the Internet of Things (IoT).

Greatest challenge(s) relative to cybersecurity awareness:

- In today's world, people are overwhelmed with information and it becomes more and more difficult to attract their attention.
- Cyberattacks are becoming more sophisticated and targeted and even well aware people may easily fall victim.

Main lesson(s) learnt (to be shared with other Member States):

- The messages should be short, simple and clear.
- It is important to grab attention and awake interest.
- Try to target specific audiences using channels and devices they favour.
- Facebook and Twitter work well.
- Today, it no longer makes sense to try to reach people by paper flyers.

B.14 MALTA

Institution Interviewed: National Cyber Security Coordination Centre, MITA

General framework: Malta Cyber Security Strategy 2016

Existing cybersecurity awareness campaign(s):

Cyber Security Malta

Be Smart Online!

Greatest challenge(s) relative to cybersecurity awareness:

- Lack of personnel specialising in this domain and the diverse target groups to which awareness and education needs to be delivered.

Main lesson(s) learnt (to be shared with other Member States):

- Keep it simple; have one message and get directly to the point.
- Use drama; kids learn better through it.
- Focus on one topic at a time.
- Engage personalities and influencers relevant to the target audience.

B.15 THE NETHERLANDS

Institution Interviewed: Ministry of Justice and Security

General framework: National Cyber Security Agenda 2018

Metrics on cybersecurity behaviour: Safe Online 2020 survey, Statistics Netherlands

Regular cybersecurity assessments published by: National Cyber Security Centre

Existing cybersecurity awareness campaign(s):

Safe Internet

Safe Banking

Don't make it too easy for them

Eerst checken dan klikken (Check first, then click)

- An initiative of the Ministry of Justice and Security, with private sector partners.
- It aims to draw the attention of all Dutch people to the danger of phishing.

Greatest challenge(s) relative to cybersecurity awareness:

- Problems develop rapidly and you can't wait to take measures to address them if there is a problem now.

Main lesson(s) learnt (to be shared with other Member States):

- You have to focus on a specific topic; you can do so with the assistance of all your partners.

B.16 NORWAY

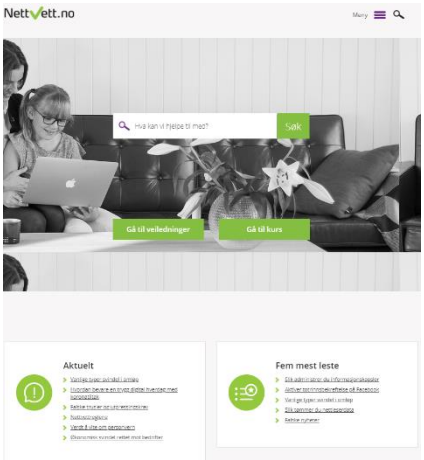
Institution Interviewed: Ministry of Justice and Public Safety

General framework: National Cyber Security Strategy for Norway – 2019

Metrics on cybersecurity behaviour: Statistics Norway – The Internet survey - 2019

Regular cybersecurity assessments published by: Norwegian National Security Authority

Existing cybersecurity awareness campaign(s):



DIGDIR (Directorate for Digitalisation)

NettVett.no

- The website run by NorSIS and was developed in collaboration with the National Security Authority and the National Telecom Authority.
- It contains advice and e-courses on a range of topics.

Greatest challenge(s) relative to cybersecurity awareness:

- Reaching out to a wider population.

Main lesson(s) learnt (to be shared with other Member States):

- Use humour and do not always be too serious.
- Broad collaboration and using several channels of communication helps to reach a wider audience.
- We try to speak not about what you 'shouldn't do' but, instead, what you 'should do'. The goal is to not create fear nor intimidate people.

B.17 POLAND

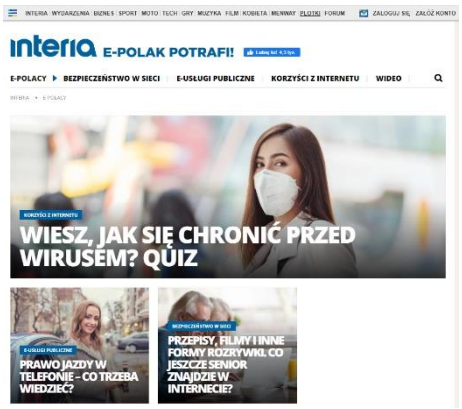
Institution Interviewed: Department of Cybersecurity, Chancellery of the Prime Minister

General framework: National Cyber Security Strategy 2019–2024 (in Polish)

Metrics on cybersecurity behaviour: Statistics Poland – Information Society in Poland in 2020 report

Regular cybersecurity assessments published by: CERT NASK (National Research Institute), GOV CSIRT

Existing cybersecurity awareness campaign(s):



Dyżurnet

Safer Internet

e-Polak potrafi! (ePole can!)

- Interia, in cooperation with the Ministry of Digitization and the National Research Institute (NASK), explains how modern technologies can change and facilitate our everyday life.
- The main campaign is carried out in four areas: e-services, web safety, programming and quality of life.
- Actions are addressed to specific targeted groups: all citizens, Internet users, seniors, children and parents.

Greatest challenge(s) relative to cybersecurity awareness:

- The problem appears to be in moving from awareness to execution; practicality and implementation are always challenges.

Main lesson(s) learnt (to be shared with other Member States):

- Repeat campaigns at least six times.
- People like short messages.

B.18 PORTUGAL

Institution Interviewed: National Cybersecurity Centre

General framework: National Cyberspace Security Strategy 2019–2023 (in Portuguese)

Metrics on cybersecurity behaviour: Statistics Portugal – Information and knowledge society – household survey – 2020

Regular cybersecurity assessments published by: National Cybersecurity Centre

Existing cybersecurity awareness campaign(s):

Safer Internet Centre

Greatest challenge(s) relative to cybersecurity awareness:

- Reaching new target audiences;
- Adapting content from one tool/platform to another;
- Cooperation with all the relevant stakeholders.

Main lesson(s) learnt (to be shared with other Member States):

- Use different approaches and different instruments to increase the effect of the campaign; people explore various issues in various ways.
- Our personnel have different backgrounds: literature, music, journalism; this helps us to see problems from different perspectives.
- Develop low cost, innovative and scalable ideas.
- Have a whole-of-society approach.

B.19 ROMANIA

Institution Interviewed: National Cyber Security Directorate (DNSC)

General framework: Cyber Security Strategy of Romania

Regular cybersecurity assessments published by: National Cyber Security Directorate (DNSC)

Existing cybersecurity awareness campaign(s):

National Cyber Security Directorate (DNSC)

- Among other responsibilities, the DNSC conducts awareness campaigns.
- Some of the current topics include spam (fake technical support), malware and cybercrime prevention.
- They also coordinate the European Cyber Security Month.

Greatest challenge(s) relative to cybersecurity awareness:

- Lack of personnel engaging in awareness raising;
- Limited budget for launching campaigns;
- Making decisionmakers understand the importance of cybersecurity and the necessity of awareness raising.

Main lesson(s) learnt (to be shared with other Member States):

- Be proactive; launch a campaign quickly after you identify a threat.
- Messages should be clear, simple, but at the same time meaningful.
- Design the campaign in a way that encourages people to learn.

B.20 SLOVAKIA

Institution Interviewed: National Security Authority

General framework: The National Cybersecurity Strategy 2021–2025

Regular cybersecurity assessments published by: National Security Authority

Existing cybersecurity awareness campaign(s):

SK-CERT

Zodpovedne.sk (Responsibly)

Greatest challenge(s) relative to cybersecurity awareness:

- How to centralise public awareness raising;
- How to get other agencies engaged in awareness raising;
- How to develop a plan for spreading security awareness in the field of cybersecurity;
- How to organise and conduct cybersecurity awareness campaigns.

Main lesson(s) learnt (to be shared with other Member States):

- You need to address the public in a simple way; technical terms about vulnerabilities do not work, but pictures work well. We also use examples so that people who don't have relevant experience can understand our messages.
- Get the input of stakeholders who are big players in cybersecurity.

B.21 SLOVENIA

Institution Interviewed: Government Information Security Office (URSIV)

General framework: Cyber Security Strategy – 2016

Metrics on cybersecurity behaviour: Statistical Office of the Republic of Slovenia – Internet security during the first wave of the COVID-19 epidemic

Regular cybersecurity assessments published by: Government Information Security Office (URSIV)

Existing cybersecurity awareness campaign(s):

- https://safe.si/ Intended for awareness-raising of children, parents, teachers and social workers, the project is partially funded by URSIV. The programme is being implemented by a consortium made up of the Faculty of Social Sciences, some non-governmental organisations, the Academic and Research Network of Slovenia (ARNES) and the Police.
- The programme provides children, teenagers, parents, teachers and social workers with knowledge and tools to guide, empower and help children and teenagers in the digital world.

Greatest challenge(s) relative to cybersecurity awareness:

- Cooperation with more organisations;
- Lack of human resources.

Main lesson(s) learnt (to be shared with other Member States):

- Use different channels of communication.
- Cooperate more with all the parties involved (Ministry of Education, NGOs etc.).

B.22 SPAIN

General framework: National Cybersecurity Strategy 2019

Metrics on cybersecurity behaviour: National Statistics Institute Survey 2020

Regular cybersecurity assessments published by: CCN-CERT

Existing cybersecurity awareness campaign(s):

IS4K Internet Segura For Kids (Safe Internet For Kids)

OSI Oficina de Seguridad del Internauta (Internet User Security Office)

B.23 SWEDEN

Institution Interviewed: Swedish Civil Contingencies Agency (MSB)

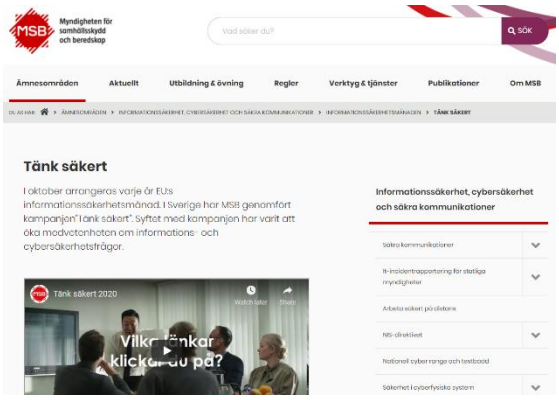
General framework: A National Cyber Security Strategy – 2017

Metrics on cybersecurity behaviour: Statistics Sweden – ICT usage in households and by individuals – 2020

Regular cybersecurity assessments published by: Swedish Civil Contingencies Agency (MSB)

Existing cybersecurity awareness campaign(s):

Tänk säkert (Think Safe)



- Implemented by the MSB with the collaboration of public, private and interested organisations that also want to contribute to increased awareness and knowledge in society;
- Aimed at private individuals and businesses with up to ten employees where privacy and entrepreneurship are closely linked;
- The purpose is to be able to take measures to become more securely connected through solid, clear and concrete tips.

Greatest challenge(s) relative to cybersecurity awareness:

- ENISA's awareness messages have often come too late for us; we would like to start the process earlier in order to prepare materials and resources.

Main lesson(s) learnt (to be shared with other Member States):

- Work with partners and engage leaders, who will in turn engage their colleagues.
- Be patient when trying to change people's behaviour; the same message may have to be repeated year after year.

TP-09-21-493-EN-N

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost the resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14, Chalandri 15231, Attiki, Greece

Heraklion Office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN 978-92-9204-544-9
doi: 10.2824/363629