Proposal No. 830929
Call H2020-SU-ICT-03-2018

Project start: 1 February 2019
Project duration: 42 months

Cyber Security for Europe

D9.11

SME cybersecurity awareness program 2

Document Identification	
Due date	31th January 2021
Submission date	18th May 2021
Revision	1.0

Related WP	WP9	Dissemination Level	PU
Lead Participant	NTNU	Lead Author	Sunil Chaudhary
Contributing Beneficiaries	NTNU, TDL	Related Deliverables	D9.6, D9.17

Abstract: This report presents sources of cybersecurity awareness resources and materials that can be useful for SMEs. The sources of these materials can be broadly categorised into

(1) European agencies and organisations
(2) EU-funded and national projects,
(3) National organisations of EEA countries and the UK,
(4) European trade associations and federations and
(5) International US-based companies offering information security and cybersecurity training and awareness resources.

Most of the listed sources are from European agencies and organisations, which have prepared awareness materials to meet the needs of European industry and enterprises. The awareness materials from the first three source categories are generally available for free or after registration. The fourth source category provides awareness resources and materials to members only and the fifth source category charges for awareness resources and materials with few exceptions that are available for free.

This document is issued within the CyberSec4Europe project. This project has received funding from the European Union's Horizon 2020 Programme under grant agreement no. 830929. This document and its content are the property of the CyberSec4Europe Consortium. All rights relevant to this document are determined by the applicable laws. Access to this document does not grant any right or license on the document or its contents. This document or its contents are not to be used or treated in any manner inconsistent with the rights or interests of the CyberSec4Europe Consortium and are not to be disclosed externally without prior written consent from the CyberSec4Europe Partners. Each CyberSec4Europe Partner may use this document in conformity with the CyberSec4Europe Consortium Grant Agreement provisions and the Consortium Agreement.

The information in this document is provided as is, and no warranty is given or implied that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

Executive Summary

In D9.6 we presented a systematic literature review of past studies on cybersecurity awareness across SMEs within the EU. One of the findings of that report is that, due to budget constraints, many SMEs depend on freely available awareness materials. In this report, we have presented the sources of numerous cybersecurity awareness materials and resources that SMEs can utilise to raise awareness internally.

The elicited sources of awareness materials are broadly classified into:

1. European agencies and organisations
2. EU-funded and national projects
3. National organisations of EEA countries and the UK
4. European trade associations and federations
5. International US-based companies that offer information security and cybersecurity training and awareness resources

To identify the first three source categories, we visited and explored the websites of 16 European institutions and bodies, 51 European agencies, 246 EU-funded and national projects, and various national bodies (mentioned in the cybersecurity national strategy) that are responsible for cybersecurity in 30 EEA countries and the UK to know if they distribute any cybersecurity awareness material resources. In the case of the fourth category, we visited and explored the websites of 296 European trade associations and federations. We conducted similar operations to various international US-based companies that offer information security and cybersecurity training and awareness resources to identify the fifth source category. The awareness materials from these sources mainly cover

1. cybersecurity threats and risks including new emerging and evolving ones,
2. good practices and cyber hygiene,
3. EU cybersecurity regulations and standards,
4. security mechanisms and assessment guidelines and frameworks,
5. ICT and security requirements,
6. cybersecurity tools and resources from third parties, and
7. cybersecurity certifications.

We observed that the first three source categories mostly produce and distribute awareness materials that can be used during the implementation phase of a cybersecurity awareness programme. Only a few of them disseminate cybersecurity awareness assessment tools that can be used during both the pre- and post-implementation phases of a cybersecurity awareness programme. Moreover, they largely depend on log data (e.g., download and visit logs) to monitor the popularity of their awareness materials. They do not have any integrated functionality to get direct feedback from the users of the awareness material. More importantly, very few of them have awareness materials using communication channels like games and simulations, more engaging and intuitive media for cybersecurity awareness. Except for the awareness materials from the EEA national organisations, others have simply performed a translation and not localisation of the awareness materials. The fourth category distributes awareness materials only to members, and there is a membership fee. The fifth category distributes only basic awareness materials. For more advanced awareness materials, SMEs have to pay for them. Further, the fifth category has utilised more diverse communication channels for cybersecurity awareness and has an abundance of awareness materials on more emerging and evolving cyber threats and risks including those that originated due to COVID-19.

Last but not least, the awareness materials from the elicited sources may not exactly fit the needs and context of an SME. Therefore, before using them, an SME must clarify what topics are relevant to its organisation, and what communication channels meet its culture and infrastructure. It is recommended to use more than one type of awareness material for every cyber threat and risk. This will improve both the reachability and touchability of a cybersecurity awareness programme.

Document information

Contributors

Name	Partner
Sunil Chaudhary	NTNU
Vasileios Gkioulos	NTNU
David Goodman	TDL

Reviewers

Name	Partner
Panayiotis Kotzanikolaou	UPRC
Jozef Vyskoc	VaF
Christine Jamieson	TDL

History

Version	Date	Authors	Comment
0.01	2020-07-20	Sunil Chaudhary	1st Draft
0.02	2021-01-28	Sunil Chaudhary	2nd Draft
0.03	2021-01-31	Sunil Chaudhary	3rd Draft
0.04	2021-03-14	Sunil Chaudhary	4th Draft
0.05	2021-03-19	Sunil Chaudhary	5th Draft
0.06	2021-04-15	Sunil Chaudhary	6th Draft
0.07	2021-04-27	Sunil Chaudhary	7th Draft
1.00	2021-05-07	David Goodman, Christine Jamieson	Ready for submission
1.00	2021-05-18	Ahad Niknia	Final check, preparation and submission process

Table of Contents

List of Tables

List of Acronyms

C	**CERT**	Computer Emergency Response Team
	CSIRT	Computer Security Incident Response Team
E	**ECSM**	European Cyber Security Month
	ECSO	European Cyber Security Organisation
	EEA	European Economic Area
	EMSA	European Maritime Safety Agency
	ENISA	European Union Agency for Cybersecurity
	EU	European Union
	EUROPOL	European Union Agency for Law Enforcement Cooperation
G	**GDPR**	General Data Protection Regulation
I	**ISP**	Internet Service Provider
	IT	Information Technology
M	**ME**	Micro Enterprise
	MOOC	Massive Open Online Course
N	**NCSC**	National Computer Security Centre
	NSA	National Security Agency
S	**SME**	Small and Medium Sized Enterprise
U	**UK**	United Kingdom
W	**WG**	Working Group

1 SMEs and Cybersecurity

Small and medium-sized enterprises (SMEs) are defined as individual firms that have a staff headcount less than 250 and have either an annual turnover less than or equal to 50 million EUR, or an annual balance sheet total less than equal to 43 million EUR [1]. They account for the majority of businesses worldwide and are therefore important contributors to job creation, innovation, and global economic development. SMEs represent about 90% of businesses and more than 50% of employment worldwide [2]; and similarly, in the European Union, 99% of enterprises are SMEs which provide two-thirds of private sector employment [3]. In 2018, there were over 25 million SMEs in the European Union (EU)-28, employing 100 million people, of which 93% were micro-SMEs, defined as having 10 or less employees [4].

SMEs have a very different profile as compared with large enterprises in terms of their work environment and organisational structure, management, and culture. Many micro-SMEs suffer financial and resource constraints [5] [6] [7], practise informal management with centralised decision making, have multi-tasking employees with possibly low adherence to established procedures and standards [8], and deploy a centralised programme management model for cybersecurity awareness (i.e., centralised policy, strategy, and implementation of cybersecurity awareness) [9]. Due to their limited size and growth needs, SMEs are forced to change plans and strategies much faster than large organisations. Moreover, in response to pressure for innovation and quality [5], they have to exploit new technologies and business opportunities that their large counterparts may choose not to. But the main problem is that they integrate emerging technologies and work practices into their business without an adequate assessment from a cybersecurity perspective [10]. Many SMEs integrate new technologies without understanding the risks they will invite, and how this impacts the overall cybersecurity hygiene of the organisation. Obviously, new technologies and work practices bring significant opportunities and competitive advantages, but they also introduce new cybersecurity risks. Such flexibility or agililty help SMEs position themselves at the *productivity frontier* [11] and also offer an opportunity to establish themselves amongst the leading innovative enterprises: however, it also makes them more vulnerable to cyber attacks.

In recent years, cyber attacks targeting SMEs have become more prevalent; around 77% of cyber attacks target SMEs [12]. SMEs may severely underestimate cybersecurity risks and vulnerabilities and not regard them as a strategic component in their business planning, despite the fact that they are a real and growing phenomenon. The CxOs, owners or decision-makers can often be dismissive of the cyber risks and vulnerabilities, and it’s a common misconception that cyber criminals prefer large organisations over SMEs: thus, cybersecurity is less critical for SMEs and worth ignoring [10] [13] [14]. Nonetheless, SMEs can be relatively more lucrative for cyber criminals since it requires only a minimal effort to attack them and can result in a substantial cumulative payoff. Moreover, SMEs that do business with large enterprises are attacked by cyber criminals, utilising them as a stepping stone to reach the large enterprise [7]. Hence, the stakes are high for SMEs who cannot afford to have their security compromised. Particularly for small enterprises that cannot withstand a major cyber attack, reputation damage, business losses and penalties levied after a cyber attack may drive a small business to bankruptcy.

To make matters worse, due to budgetary and resource constraints, many SMEs are unable to afford up-to-date security defences (e.g., security technology, established standards and practices, and cybersecurity training and awareness) and similarly are unable to hire people with relevant knowledge and expertise [10] to maintain a standard cybersecurity posture that is crucial to meet the pace of ever-evolving cybersecurity challenges. Even among SMEs which could afford cybersecurity measures, many allocate inadequate budgets and resources for the purpose. As a matter of fact, this underinvestment in cybersecurity is not just limited to SMEs, but equally prevalent in other enterprises. Its root cause may lie in the wrong mindset among financial decision-makers, who perceive cybersecurity as a well defined problem that can be solved in one step rather than as an ongoing problem [15]. Many decision-makers believe that placing a sophisticated cyber defence or complying with a security framework can be a silver bullet for cybersecurity, thus consider cybersecurity investments as being mainly for building an infrastructure [15]. This is further exacerbated by the nature of cybersecurity programmes, which directly neither generate revenue nor reduce costs [16], whilst having to compete for resources with other aspects directly tied to revenue enhancement and cost reduction. In such a situation, the attitude of cybersecurity executives and professionals plays an important role in the decision-making of resource allocation for cybersecurity [17]. Yet, an inadequate budget or resource for cybersecurity also implies that the cybersecurity executives and professionals failed to clearly express and convey the message on the benefit and competitive advantage of cybersecurity to the financial decision-makers in a language and format they understand. Added to which, the dynamic nature of cybersecurity has made estimating a practically adequate budget for cybersecurity a challenging task. This is evident from the enterprises which increase their cybersecurity investments but still fall short of budget due to an increase in risks and threats with respect to the rise in investment [17].

Thus, SMEs, which form the backbone of the Europan and global economy, need to be prepared for cyber risks and threats. And in order to do so, the provided cybersecurity solutions should be affordable.

2 Cybersecurity Awareness for SMEs

There is a wide range of organisations, for example, European agencies and organisations, EU funded projects, national organisations, and private companies, already producing and distributing a multiplicity of cybersecurity awareness programmes and resource materials that have burgeoned over the last few years. Many of these organisations produce and distribute awareness materials specifically for SMEs. Considering the challenges of budget and resource constraints, it would be advantageous for SMEs to utilise these freely available cybersecurity awareness resource materials [6]. Therefore, the main objective of this report is to collect the sources of cybersecurity awareness resource materials that are affordable and more importantly can be utilised by SMEs. But let us be clear that this is not a complete list of such awareness materials. There can be other sources at international, regional, and national levels that are not included in this report. In that case, SMEs and other interested parties are advised to use their own discretion to determine whether those awareness materials best fit their needs and accordingly take a decision whether or not to use them.

In addition, we analysed the awareness materials mainly from the following perspectives:

(a) What types of cybersecurity awareness materials are available for SMEs?
(b) In which phase of cybersecurity awareness (pre-implementation, implementation, and post-implementation) can the awareness materials be used?
(c) How easy is it for SMEs to access the awareness materials?
(d) Is there a cost for the awareness materials?

Along with that, we also touched on the following important points:

(e) Do publishers have download stats or features to know how many people have accessed the materials?
(f) What challenges do they encounter in delivery mechanisms/communication channels?
(g) Where are the gaps and what aspects of cybersecurity awareness programs are missing?

Questions (a)-(d) provide sources from where SMEs can get cybersecurity awareness materials and resources; whereas questions (e)-(g) suggest what these sources can do at a minimum to improve the accessibility and quality of the awareness materials. The suggestions are completely based on the analysis performed in the awareness materials uploaded on the website and the way they have been presented.

While collecting these sources, priority has been given to the awareness material resources that are prepared and distributed by the European organisations and projects. Among 72 listed sources of awareness materials, five are European agencies and organisations, ten are EU-funded and national projects, 38 are national organisations of the European Economic Area (EEA) countries and the United Kingdom (UK), and 11 are European trade associations and federations. We believe that information in this report would contribute to the uptake of these awareness materials by SMEs and presumably also improve the cybersecurity awareness situation in SMEs.

3 Data Collection and Analysis

In Tables 1,2,3, 4, & 5, unless specified otherwise, all the awareness materials are available for free to everyone, often without the need for registration to access them. Many listed sources do not produce and distribute cybersecurity awareness materials specific to SMEs but to organisations in general. Still, these sources have been included because they are still relevant to SMEs, and more importantly, the awareness materials are available for free, so even resource constrained SMEs could potentially utilise and benefit from them.

3.1 European Agencies and Organisations

From the website content of 16 European institutions and bodies and 51 European agencies listed in the EU weblink [18], we found five European agencies and organisations listed in Table 1 that provide materials on cybersecurity awareness. Some useful weblinks of these European agencies and organisations, from where SMEs can access awareness materials free of cost or after registering, are provided in Annex A: European Agencies & Organisations. The awareness materials from EMSA require authentication and can be accessed only by its beneficiaries. It is hassle-free to download and use the available awareness materials. It requires basic computer and Internet skills to utilise (e.g., browse website, download files, play videos, install screensaver, and register to a website) to use the awareness materials.

The awareness materials are available in various forms (i.e., using different delivery channels mentioned in Table 1) and target to raise awareness mainly on:

- Cybersecurity threats and risks including new emerging and evolving ones
- Good practices and cyber hygiene
- EU cybersecurity regulations and standards
- Cybersecurity certifications

Most of these awareness materials are designed for the implementation phase of a cybersecurity awareness programme. However, the reports and position papers from ENISA, ECSO and the European Digital SME Alliance can be useful for planning and designing a cybersecurity awareness programme. Moreover, the cybersecurity assessment tools distributed by the European Digital SME Alliance are useful for determining the level of cybersecurity awareness in an organisation before and after the implementation of a cybersecurity awareness programme.

The awareness materials produced and distributed by these organisations are generally limited to learning how to ‘identify’, ‘detect’, and ‘protect’ from cyber attacks with a few exceptions. Some of EUROPOL’s awareness materials also cover how to ‘respond’ and ‘recover’ when an organisation has suffered a cyber attack or data breach. For example, it distributes instructions and tools to recover from ransomware attacks and makes recommendations on how to act if a potential cyber attack or data breach has happened.

All the organisations are active and periodically publish awareness materials on existential cybersecurity risks and threats and reflect the current state of cybersecurity knowledge.

Although the awareness materials from ENISA and EUROPOL are in different EU languages, they have only their text translated and miss greater localisation, which goes beyond text translation.

Organisation	Scope	Events & Training	Tools & Media	Risks and Threats
European Union Agency for Cybersecurity (ENISA) [19] produces and distributes cybersecurity awareness materials and organises cybersecurity awareness programmes.	General	European Cybersecurity Month (ECSM), an annual campaign dedicated to promoting cybersecurity among EU citizens and organisations, is supported by ENISA. Organises various cybersecurity awareness workshops and training, and other events.	Disseminates awareness messaging/information using different media, e.g. • Video clips • Posters for organisations • Illustrations • Screen savers • Training courses • Awareness quizzes • Threat landscape reports (include incidents and mitigations in brief) • Reports (containing, e.g., cybersecurity awareness framework, cybersecurity awareness evaluation, and others) In many materials, the awareness information is short and succinct, generally in a single sentence. Some of the awareness materials are available in different European languages as well as English.	Various cybersecurity best practices and cyber hygiene for organisations. Cyber risks and threats including new emerging and evolving ones relevant and prevalent to organisations. Cybersecurity awareness framework. Cybersecurity awareness key performance indicators and measuring methods.
European Union Agency for Law Enforcement Cooperation (EUROPOL) [20] produces and distributes cybersecurity awareness materials for organisations.	General	"EUROPOL-APWG Symposium on Global Cybersecurity Awareness" is organised by EUROPOL in collaboration with the Anti-Phishing Working Group (APWG).	Disseminates awareness messaging/information using different media, e.g. • Infographics • Posters • Videos • Comics • Brochures • Website with prevention advice for ransomware attacks Awareness information is presented in more detail. It does not simply explain what the problem is but also how to identify it and its potential protections and mitigations. Moreover, recommendations on cyber hygiene clearly mention whom they are meant for.	Various cybersecurity best practices and cyber hygiene for organisations. Cyber risks and threats including new emerging and evolving ones relevant and prevalent to different sectors of organisations.

			The awareness materials are available in various European languages including English.	
European Maritime Safety Agency (EMSA) [21] distributes cybersecurity awareness courses designed for the maritime industry.	Maritime	“European Conference on Transport Cybersecurity” is organised by EMSA in cooperation with other European agencies and organisations. Offer cybersecurity awareness course with video lectures.	Disseminates awareness messaging/ information using video lectures. The materials are offered to only the EMSA beneficiaries.	Covers cybersecurity issues specific to the maritime industry.
European Cyber Security Organisation (ECSO) [22] has a working group (WG5: Education, Training, Awareness, Cyber Ranges) for cybersecurity awareness. It produces materials for cybersecurity awareness that include professional purposes.	General	Sponsors events for cybersecurity awareness.	Disseminates awareness messaging/ information through different media, e.g. • Presentations and • Position papers (cybersecurity awareness concept design processes) WG5 has a cybersecurity awareness calendar, and every month it produces awareness materials on a theme (i..e, cyber risk, and threat).	Cyber risks and threats including new emerging and evolving ones relevant and prevalent to organisations. Sector-specific awareness materials. Cybersecurity certifications awareness.
European Digital SME Alliance [23] has a work package called “Cyber & Data” that includes cybersecurity for SMEs.	SMEs	Disseminates news on cybersecurity awareness tools, reports, events, standards, and others useful for SMEs.	Disseminates awareness messaging/ information using position papers. The WG publishes position papers on cybersecurity for SMEs. Moreover, it distributes free tools for cybersecurity and awareness assessment for SMEs.	Awareness information on the EU Cybersecurity Act and Standards for SMEs. Tools for cybersecurity awareness assessment for SMEs.

Table 1: List of European agencies and organisations that produce or/and distribute cybersecurity awareness materials for organisations and SMEs

Some important factors which could potentially improve the overall usability of these awareness materials are:

- Except for feedback on some workshops, webinars, and training, we did not find any feedback functionality (e.g., a hyperlink for feedback) integrated into other awareness materials. Indeed, webpage visits, materials download logs, and registrations can give an idea of the popularity of the awareness materials but it is insufficient to understand how useful the provided materials were to the end-users or companies.
- Only EUROPOL has provided a feature or plugin to share the awareness materials on social media platforms and send them through email. This feature to ease the dissemination is important to improve the visibility of awareness materials.
- Many of the awareness materials do not provide complete awareness information, for instance, they should not merely be limited to "*what to do*" after encountering a cyber threat but also include briefly "*how to do it in the right way*".

3.2 EU Funded and National Projects

Of the 246 EU-funded and national projects listed in the cyberwatching.eu "R & I Project Hub" [24], we primarily focused on the projects that are still active (or running) and have working groups for cybersecurity awareness for SMEs. After this first level of screening, we reviewed the website contents of all the active projects and a few inactive projects that we presumed could still be relevant for SMEs. Based on the two-level screenings, we found ten projects listed in Table 2 which produce and/or distribute cybersecurity awareness materials for SMEs. In Annex B: EU Funded and National Projects, there are some useful weblinks of these EU-funded and national projects, from where SMEs can access now or in the near future (for running projects) the awareness materials free of cost or after registering. Some materials from SMESEC are made available privately to users contacting the project[1]. Similarly, Cyber-MAR offers reports and training but requires prior authentication. Awareness training courses are offered by Cyberwiser.eu for a fee. Some of the awareness materials by cyberwatching.eu are accessible only to registered users.

In general, it requires basic computer and Internet skills to access the awareness materials. Taking awareness quizzes and using assessment tools (again available in the form of a questionnaire) can be accessed in a browser and are simple to use.

Like European agencies and organisations, these projects also produce and distribute awareness materials in various forms mentioned in Table 2 mainly targeting the raising of SME and supply chain awareness on:

- Cyber threats and risks relevant to SMEs
- Cybersecurity best practices and cyber hygiene
- Compliance with EU cybersecurity policies, laws, and regulations for SMEs
- Cybersecurity standards and certifications for SMEs

Moreover, these projects seem to equally emphasise awareness materials that can be used to assess the cybersecurity awareness level of an organisation. Tools produced or distributed by cyberwatching.eu, SMESEC, GEIGER, and SecureHospitals can be useful for the cybersecurity awareness assessment of the organisations before and after a cybersecurity awareness programme to measure its outcome. Moreover,

[1] SMESEC finished in May 2020 and has effectively continued through the GEIGER project.

their deliverables with different frameworks and models can be helpful in planning and designing a cybersecurity awareness programme. Additionally, some projects have utilised more intuitive and engaging techniques like literary graphic and gaming competitions (DOGANA), quizzes (SMESEC), and simulation (Cyberwiser.eu), which are found to improve the effectiveness of cybersecurity awareness.

In addition to ‘identification’, ‘detection’, and ‘protection’ actions, their deliverable reports and other materials also discuss ‘response and ‘recovery’ actions that need to be taken if a cyber attack or data breach has occurred.

Except for the three projects, DOGANA (completed August 2018), SMESEC (completed May 2020), and FORTIKA (completed May 2020), all the others are ongoing. These completed projects have several awareness materials that cover the existential cyber risks and threats and so can be relevant to SMEs and micro-SMEs.

Some important factors which will potentially improve the overall usability of these awareness materials are:

- DOGANA and FORTIKA have produced awareness materials in multiple European languages. Once again, the awareness materials have relied mostly on translation rather than localisation.
- The awareness materials produced by these projects do not ask for feedback from end-users. Indeed, determined end-users can provide email feedback to the project but how many will attempt that is questionable. Integrating a feedback section or functionality, for example, a weblink in posters and leaflets and a comment section in blogs and articles can be a practical way to get feedback from the end-users.
- Except for cyberwatching.eu, other projects have a feature (or plugin) on their event webpage to share on social media platforms and/or send through email. This feature helps to contribute to the diffusion of the information.

Project Name	Scope	Events & Training	Tools & Media	Risks and Threats
cyberwatching.eu [25] is an online hub for research and innovation in the field of cybersecurity and privacy in Europe.	General and SMEs	Organises cybersecurity awareness workshops and events for SMEs.	Distributes various awareness assessment tools to SMEs, e.g. • GDPR Temperature Tool • Cybersecurity Self Assessment for SMEs • Cyberwatching Information Notice Tool • Cyberwatching Cyber Risk Temperature Tool Disseminates awareness messaging/ information to SMEs using different media, e.g. • Brochures • Cybersecurity guide (for SMEs) • Tools and quizzes for SMEs • Deliverables and technical reports by various organisations, e.g., ENISA, Cisco, NCSC & NSA, and EUROPOL	Various cybersecurity best practices and cyber hygiene for SMEs. Cybersecurity issues to organisations, more specific to SMEs. Compliance with EU policy, regulations, and laws.
Cyberwiser.eu [26] distributes cybersecurity awareness tools from Cyberwatching.eu	General and SMEs	Organises and sponsors various events like cybersecurity webinars, training, and hackathon (use simulation to generate real-time attacks). Offers cybersecurity training courses to organisations including SMEs for a fee.	Distributes different awareness assessment tools and quizzes to SMEs (tools from Cyberwatching.eu). Disseminates awareness messaging/ information using different media, e.g. • Reports • Cybersecurity courses • Awareness assessment tools and quizzes • Blog articles (review of the key opinions, practices, and policy decisions as well as a guide to interesting technology development relevant to cybersecurity awareness and training)	Various cybersecurity best practices and cyber hygiene for SMEs. Cybersecurity issues to organisations, more specific to SMEs. Compliance with EU regulations. EU national cybersecurity strategies. Training courses range from awareness to risk analysis and evaluation.
SMESEC [27] produced a unified cybersecurity solution for SMEs.	SMEs	Provides interactive training courses and material. (Securityaware.me). Open to the public or made available privately to users contacting and registering to the project. Registration is free of cost.	Offers different tools related to cybersecurity awareness, e.g. • Vulnerability Discovery & Resolution Tools • Definition & Recommendation Tools • Threat Protection & Response Tools • Lessons from Testing & Validation Disseminates awareness messaging/ information using different media, e.g.	Various cybersecurity best practices and cyber hygiene for SMEs. Cybersecurity issues including emerging and evolving ones are relevant to SMEs. Cybersecurity standardisation.

		Organises various cybersecurity seminars, workshops, and other events.	• Reports (with framework) • Awareness and training tutorials • Tools and quizzes	
GEIGER [28] aims to develop a solution that will allow SMEs to become aware of their risks related to data protection, privacy, and cybersecurity.	SMEs and MEs	Organises workshops and events to raise awareness of cybersecurity and SMEs' priorities and practices. Cybersecurity awareness training for SMEs. Aims to develop a standardised learning programme called "Certified Security Defenders". Posts awareness content to mark cybersecurity month.	Offers Geiger cybersecurity counter (a solution that can be used on the web or smartphone to dynamically show the level of current risks for the company) Disseminates awareness messaging/ information using different media, e.g. • Reports on various aspects of cybersecurity awareness for SMEs • Tools for SMEs to fight cyber attacks • Cybersecurity awareness training	Data breach, privacy, and various cyber risks and threats relevant to SMEs. Standardisation of cybersecurity learning programme for SMEs.
Cyber-MAR [29] aims for cyber preparedness actions for a holistic approach and awareness raising in the MARitime logistics supply chain	Maritime	Offers training (only to authorised users) on cybersecurity issues specific to the maritime logistics value supply chain to increase the cyber awareness level of associated actors.	Disseminates awareness messaging/ information using different media, e.g. • Reports • Cybersecurity awareness training	Awareness information and training on issues specific to maritime logistics value supply chain.
SecureHospitals [30] aims to ameliorate cybersecurity awareness and training across healthcare organisations in Europe.	Healthcare	Aims to organise workshops, webinars, and a Massive Open Online Course (MOOC) to disseminate and raise the cybersecurity awareness of healthcare organisations in Europe.	Plans to offer different tools related to cybersecurity awareness, such as: • Wizard Tool helps to prepare individual training curriculum. • Aims to create Open Information and Awareness Hub for healthcare organisations in Europe. Disseminates awareness messaging/ information using different media, e.g. • Deliverables reports • Courses and training materials by registration • Wizard Tool	Cybersecurity practices across healthcare organisations. Cybersecurity threats and risks specific to healthcare organisations.
DOGANA [31] delivered toolsets to detect and prevent social engineering	General	Organised various literary graphic and gaming competitions to raise	Toolsets to detect and prevent social engineering cyber attacks and phishing.	Social engineering cyber attacks and phishing.

cyber attacks and phishing.		awareness on social engineering and phishing.	Disseminates awareness messaging/ information using different media, e.g. • Deliverable reports • Literary graphics (e.g., comics, storytelling) and word games. Literary graphics and games are available in other European languages. • Blog articles	
FORTIKA [32] aimed to provide cybersecurity solutions to SMEs.	SMEs	Organised cybersecurity training and workshops, and European Cybersecurity Challenge.	Disseminates awareness messaging/ information using different media, e.g. • Deliverable reports (access granted to confidential reports only to the consortium and the Commission Services) • Flyers (some flyers are available in other European languages.) • White papers • Videos • User stories	EU cybersecurity legal and policy requirements for SMEs. Cybersecurity threats and risks relevant for SMEs.
CyberSec4Europe [33] has a Task in WP9 dedicated to cybersecurity awareness for SMEs.	SMEs	Organises cybersecurity awareness seminars, workshops, and other events. Disseminates information about cybersecurity awareness and training events through its social media.	Disseminates awareness messaging/ information using different media, e.g. • Deliverables (framework, recommendations, and other necessary information required in cybersecurity awareness for SMEs) • Blog articles	Cybersecurity threats and risks to SMEs and the supply chain. EU regulations for SMEs and the supply chain. Cybersecurity standards and certifications.
PUZZLE [34] aims to develop efficient processing of information and the establishment of an online collaboration and knowledge sharing platform.	SMEs and MEs	Organises cybersecurity webinars and inform about other cybersecurity events relevant to SMEs and MEs.	Intends to provide a tool and platform for data monitoring, processing, and visualisation tool and knowledge-sharing that will be useful for raising cybersecurity awareness. • Blog articles • Infographics (threat landscape) • Newsletter (requires registration) • Innovation contest (to inspire start-ups and vendors to get innovative in cybersecurity)	Cybsercurity threats and risks relevant to SMEs and MEs. Privacy and data protection GDPR clauses and legislation

Table 2: List of EU funded and National Projects that produce and distribute cybersecurity awareness materials for organisations and SMEs

3.3 National Organisations from the EEA Countries and the United Kingdom

Here we have identified the national organisations from 30 EEA countries and the UK responsible for cybersecurity awareness to SMEs and other organisations. The final list is given in Table 3. In order to do this, initially, we collected all national bodies responsible for cybersecurity in 31 countries from the *national strategies* mentioned in the hyperlink https://www.cyberwiser.eu/cartography [35]. Each country has multiple organisations responsible for cybersecurity but not all of them are accountable for cybersecurity awareness. This was followed by verifying whether national bodies are responsible for or play a role in the cybersecurity awareness of organisations and SMEs in their respective countries. Some useful weblinks of the National Organisations of EEA countries and the UK from where SMEs can access the awareness materials free of cost are provided in Annex C: National Organisations in the EEA and the UK.

National Organisation	Country	Description
Cyber Security Austria (CSA) [36]	Austria	Cyber Security Austria is a non-profit, independent, and non-partisan association with the aim to address security issues. It promotes security awareness in Austria. It makes blog posts to raise cybersecurity awareness. It has made some posts specific to SMEs and other organisations.
Cyber Security Coalition (CSC) [37] Centre for Cyber security Belgium (CCB) [38] Safeonweb [39]	Belgium	The Cyber Security Coalition is a partnership between players from the academic world, public authorities, and the private sector in the fight against cybercrime in Belgium. It provides assessment tools to raise awareness in cybersecurity (i.e., cyber threats and hygiene) and EU regulations for SMEs and other organisations. The Centre for Cyber Security Belgium is the central authority for cybersecurity in Belgium. Its main role is to implement the national cybersecurity policy incorporation with all relevant Belgian government departments that also includes informing and raising awareness among users on information and communication systems. It provides assessment tools and reports (with cybersecurity guidelines) to raise awareness in cybersecurity and EU regulations for SMEs and other organisations. Safeonweb is an initiative of the Centre for Cyber Security Belgium that aims to raise cybersecurity awareness in Belgium. The website contains awareness materials for Belgian citizens. It provides awareness materials in different forms, e.g., • News and blog posts • Security tips (e.g., remedial tips, online tests, preventive tips) • Campaign materials (e.g., banners, posters, leaflets, and videos) • Some campaign materials (e.g., PowerPoint presentation, texts, and human resource related) are provided on email request.
Computer Emergency Response Team Bulgaria (CERT.BG) [40]	Bulgaria	The Computer Emergency Response Team Bulgaria is the National Computer Security Incidents Response Team. It also promotes good practices and provides advice on various network and information security issues in the form of blog posts.
CARNet's National Computer Emergency Response Team (CERT.HR) [41]	Croatia	The national CERT is a department within the Croatian Academic and Research Network (CARNet). It is the national body for prevention from cyber threats and protection of the security of public information systems in the Republic of Croatia. It provides awareness materials in different forms, e.g.,

		• Documents (with security tips) • Presentations (for awareness programme) • Malicious contents (threat wise) instructions • Brochures • Tips and instructions • Useful links to third-party portals
Cyprus Cybercrime Centre of Excellence (3CE) [42]	Cyprus	The Cyprus Cybercrime Centre of Excellence is co-funded by the Prevention of and Fight against Crime Programme of the European Union. It provides short-term, highly focused, and specialised training seminars on cybercrime-related issues for public and private sector participants.
National Cyber and Information Security Agency (NCISA) [43] The National Computer Security Incident Response Team of the Czech Republic (CSIRT.CZ)	Czech Republic	The National Cyber and Information Security Agency is the central administrative body for cybersecurity in the Czech Republic. It cooperates with the private sector and it also raises general awareness of NCISA's activities. It publishes awareness information on the website and also includes a video explaining the message in texts. The National CSIRT of the Czech Republic cooperates with Czech businesses and provides security services to them including education and tutoring. It designs cybersecurity exercises and also guides others in designing them.
Danish Centre for Cyber Security (CFCS) [44]	Denmark	The Danish Centre for Cyber Security is the national information technology (IT) security authority, network security service, and national centre of excellence within cybersecurity. It informs and advises on preventive measures and issues guidelines and recommendations to Danish public authorities and private companies. It publishes reports helpful for the cyber threat assessment in an organisation and security guidance for cybersecurity.
Republic of Estonia Information System Authority (RIA) [45]	Estonia	The State Information System Board is a national competence centre that shapes and secures the foundations of the Estonian information society. CERT-EE is also a part of RIA. It publishes reports on national security guidelines, security assessment questionnaires, and translation versions of third-party reports. These reports can be useful resources to create awareness content.
Finnish Transport and Communication Agency National Cyber Securiy Centre (TRAFICOM) [46]	Finland	The Finnish Transport and Communication Agency National Cyber Security Centre is the national cybersecurity centre (NCSC). It includes the NCSC-FI's CERT responsible for disseminating information on information security matters in Finland. It provides security instructions for organisations and professionals.
The National Cybersecurity Agency of France (ANSSI) [47]	France	The National Cybersecurity Agency of France is the national authority for cyberspace and network and information security. It regularly reports best practices and recommendations to different stakeholders including SMEs and other organisations. It provides awareness materials in different forms, e.g., • Infographics, posters, paper toys, animated gifs, reports, social media posts, and videos (security basic precautions) • Videos, infographics, guides, posters, simulations, web docs, awareness kits, tools (privacy and security regulations) • Reports (security good practices)
Federal Office for Information Security (BSI) [48]	Germany	The Federal Office for Information Security is the German upper-level federal agency in charge of managing computer and communication security for the German government. The CERT-BUND, the national accredited CERT for Germany, is also its part. One of its tasks is to raising awareness of the public

		and the economy on IT and Internet security. It publishes reports on different cybersecurity issues that can be helpful for awareness content design.
Hellenic Computer Security Incident Response Team (CSIRT) [49]	Greece	The Hellenic Computer Security Incident Response Team (CSIRT) is the nation's flagship cyber defence, incident response, and operational integration centre. It provides cybersecurity guides and recommendations in the website posts for SMEs to raise their awareness.
Gov Computer Emergency Response Team Hungary (GovCERT) [50] Hun Computer Emergency Response Team (HunCERT) [51]	Hungary	The GovCERT is a part of the National Cyber Defence Institute. It is responsible for information security awareness campaigns. The HunCERT is a non-accredited CERT. It is run by the support of the Internet Service Providers (ISP) and targets Internet Service Providers Council members in Hungary. One of its goals is to increase security awareness. It publishes security standards and recommendations.
Computer Emergency Response Team-Iceland (CERT-IS) [52]	Iceland	The Computer Emergency Response Team of Iceland acts as a national point-of-contact for cybersecurity incidents. It is responsible for cybersecurity awareness in Iceland. It publishes security alerts and organises awareness programmes in collaboration with third parties, e.g., SANS Institute.
Irish Reporting and Information Security Service (IRISS) [53]	Ireland	The Irish Reporting and Information Security Service is Ireland's first CERT to provide services to all users within Ireland. It provides guidelines and best practices techniques on how to prevent security incidents and how best to respond in the event such as incident occurs to individuals and organisations.
Computer Security Incident Response Team-Italia (CSIRT Italia) [54]	Italy	The Computer Security Incident Response Team-Italia is established at the Department of Information Security (DIS), a department of the Presidency of the Council of Ministers of Italy. It is responsible for raising awareness and helping to prevent and coordinate cyber incidents on a large scale. It publishes cybersecurity news and organises awareness campaigns.
Information Technology Security Incident Response Institution, Republic of Latvia (CERT.LV) [55]	Latvia	CERT.LV operates under the Latvian Ministry of Defence and is regulated by the Information Technology Security Law. All services are free of charge including 24x7 assistance in incident handling, co-ordination of incident handling (with other CSIRTs and local authorities), vulnerability analysis, artefact analysis, assistance in implementation of proactive defence against attacks, IT securuty related events, and awareness raising activities.
National Cyber Security Centre of Lithuania (NKSC) [56]	Lithuania	The National Cyber Security Centre at the Ministry of National Defence is the main Lithuanian cybersecurity institution. It is responsible for spreading the ideas of cybersecurity awareness. It publishes guides (in pdf) for different cybersecurity issues.
Computer Emergency Response Team, Luxembourg (GOVCERT.LU) [57]	Luxembourg	The Computer Emergency Response Team of the Government of the Grand Duchy of Luxembourg oversees raising the awareness of public and private sectors of the risks involved and means of protection. It publishes awareness messages on their website, and notifies organisations about cyber threats.
Cyber Security Malta [58]	Malta	The Cyber Security Malta is part of Malta's national cyber security strategy. One of its key goals is a nationwide cyber security awareness campaign for the Malta Information Technology Agency (MITA). It provides awareness materials in different forms, e.g., posters and videos,
National Cyber Security Centrum (NCSC) [59]	Netherlands	The National Cyber Security Centrum incorporates the Dutch Computer Emergency Response Team (CERT). It is also responsible for cybersecurity

		awareness. It makes website posts on various cyber threats and risks to raise the awareness of organisations.
Norwegian National Security Authority (NSM) [60] The Norwegian Centre for Information Security (NorSIS) [61]	Norway	The Norwegian National Cyber Security Centre (NCSC) and Norwegian Computer Emergency Response Team (NorCERT) are parts of NSM. NSM publishes advice and guidance for personnel security. NorSIS is an independent organisation and partner to the Norwegian Government that works to create a safe digital society by raising security awareness. It organises various awareness events including coordination of the Coordinates National Security Month.
Computer Emergency Response Team Polska (CERT.PL) [62]	Poland	The Computer Emergency Response Team Polska is responsible for informational and educational activities, aimed at raising awareness in relation to IT security through a blog, Facebook, and Twitter. It publishes cybersecurity awareness leaflets in collaboration with SANS Institute.
Centro Nacional de Cibersegurança (CNCS) [63]	Portugal	The Centro Nacional de Cibersegurança is the national authority for cybersecurity in Portugal. Computer Security Incident Response Portugal (CERT.PT) is also a part of CNCS. It is responsible for promoting training and awareness actions in the country. It publishes cybersecurity awareness materials in different forms, e.g., posters, newsletters, and guides.
Cyber Security Research Centre (CSSIR Or SRI) [64] Centrul Național de Răspuns la Incidente de Securitate Cibernetică (CERT-RO) [65]	Romania	The Cyber Security Research Centre is the cybersecurity research centre of Romania that has a responsibility to raise awareness of cyber vulnerabilities and risk factors with an impact on institutional and national security. It organises awareness conferences, colloquia, workshops, lectures, and training. The Computer Emergency Response Team Romania is the national CERT of Romania that produces and distributes awareness materials to companies. It publishes awareness posters, videos, posters, posts (on a website) and organises workshops and cyber exercises.
Computer Security Incident Response Team Slovakia (CSIRT.SK) [66]	Slovakia	The Computer Security Incident Response Team Slovakia is the national CERT of Slovakia that also contributes to awareness rising in certain areas of information security. It alerts about cyber threats, provides assessment tests (e.g., phishing assessment), and guides on security best practices.
Slovenian Computer Emergency Response Team (SI-CERT) [67]	Slovenia	The Slovenian Computer Emergency Response Team is a designated national computer security incident response team (CSIRT). It keeps up-to-date information on cyber threats and other related information through the news section of its website.
The Spanish National Cybersecurity Institute- Computer Emergency Response Team (INCIB-CERT) [68] Centro Criptológico Nacional Computer Emergency Response Team (CCN-CERT) [69]	Spain	The Spanish National Cybersecurity Institute Computer Emergency Response Team is the national accredited CSIRT for security and industry. It produces and distributes awareness materials for companies in the forms, e.g., reports and webinars. The Centro Criptológico Nacional Computer Emergency Response Team is the national alert and reporting system for public administration, company and organisation of strategic interest. It also offers awareness services to companies.
Computer Emergency Response Team Sweden (CERT-SE) [70]	Sweden	The Computer Emergency Response Team Sweden is the national CERT of Sweden and it sends alert messages to registered users and produces some awareness materials for companies.

SWITCH's Computer Emergency Response Team (SWITCH-CERT) [71]	Switzerland	The SWITCH's Computer Emergency Response Team is the national CERT of Switzerland that along with other functions also produces awareness materials for companies. It has a weblink for awareness purposes. It also suggests games, books, movies, and other fun ways to use for raising cybersecurity awareness.
The National Cyber Security Centre (NCSC) [72]	United Kingdom	The National Cyber Security Centre is a government organisation that encourages behavioural changes for businesses on protection in cyberspace. It has a weblink dedicated to raising cybersecurity awareness of SMEs. It also provides security advice and guidance on cybersecurity-related topics.

Table 3: List of national organiasations of EEA countries and the UK responsible for cybersecurity awareness

In most countries, their Computer Emergency Response Team (CERT) has been found to be responsible for the cybersecurity awareness of citizens and organisations. These national bodies have targeted:

- Cyber threats and risks relevant to organisations
- Cybersecurity best practices and cyber hygiene
- Response actions after a cybersecurity incident is detected
- Compliance with national and EU cybersecurity policies, laws, and regulations for organisations
- Cybersecurity standards and certifications for organisations

Some countries have business sector-specific national bodies responsible for cybersecurity awareness. These bodies prioritise the need of that sector.

Based on the content on their website, we observed that the organisations listed in Table 3 regularly update their awareness materials to incorporate the evolving cyber threat landscape and advancements in technology. This also implies that the awareness materials produced and distributed by them are more likely to be relevant to SMEs and other types of organisation.

Interestingly, these organisations seem to depend on diversified forms of awareness materials, e.g., blogs, newsletters, posters, infographics, blog posts, videos, animated gifs, assessment tools, and others. However, we did not find them utilising more engaging and intuitive media like computer games and simulations for cybersecurity awareness. Also their materials are useful mostly during the implementation phase of a cybersecurity awareness programme. Only a few of them appear to distribute cybersecurity assessment tools that are useful before and after the implementation phase of a cybersecurity awareness programme to raise the awareness level in the organisation. Additionally, most of them have targeted organisations in general, and not specifically to SMEs. Cybersecurity organisations from the UK (i.e., National Cyber Security Centre), Belgium (i.e., Cyber Security Coalition, and Centre for Cyber Security), France (i.e., National Cybersecurity Agency of France), and Greece (i.e., Hellenic Computer Security Incident Response Team) distribute awareness materials designed specifically for SMEs.

In addition to ‘identification’, ‘detection’, and ‘protection’ actions, the awareness materials also discuss ‘response and ‘recovery’ actions that need to be taken if a cyber attack or data breach has occurred.

Finally, many of these organisations are dependent mostly on log data (e.g., download and view counts) to measure the popularity of the distributed awareness materials. Some organisations have integrated a feature to share awareness content on social media platforms. The Cyber Security Coalition from Belgium has asked for feedback on its awareness tools from end-users. Similarly, the Republic of Estonia Information System Authority has asked for feedback on its awareness content. Continuous feedback from end-users is important to understand the weaknesses in awareness content quality and delivery channels and help in future planning, update, and enhancement of awareness materials.

Since each national body has produced the awareness materials for a specific country, the awareness materials can be considered to be localised to that nation.

3.4 European Trade Associations and Federations

Amidst the vast number of trade associations and federations in Europe, we have considered only 296 of them for this study. They are from the two lists maintained by the Association of Accredited Public Policy Advocates to the European Union (AALEP), which are:

- Top industry associations in the EU [73]
- Top 200 EU trade associations [74]

These listed organisations offer cybersecurity awareness resources and materials only to members, and for membership, they charge a fee. Moreover, each organisation belongs to a particular sector and provides awareness materials suitable to a particular sector and industry. Some useful weblinks of the European trade associations and federations from where SMEs and organisations can access the awareness materials are provided in Annex D: European Trade Associations and Federations.

Organisation	Scope	Description of Materials / Programmes
Federation of Small Businesses (FSB) UK [75]	SMEs	The Federation of Small Businesses UK offers cyber protection (includes data protection and cybersecurity advice and awareness) to member SMEs in the UK. It has a helpline service for member SMEs. Along with that, it also produces and distributes materials to raise cybersecurity awareness of SMEs in different forms, e.g., articles and videos.
The Software Alliance (BSA) [76]	Software	The BSA Compliance Solutions partners with key stakeholders to raise cybersecurity awareness of its members and their customers. It targets the risk of using unlicensed and counterfeit software (e.g., malware incursions, ransomware attacks, and other critical security threats) and the benefits of software asset management. Along with that, it produces and distributes reports that can be useful for the cybersecurity awareness of software companies.
The Association of the Swedish Engineering Industries (Teknikföretagen) [77]	Engineering & Industrial Manufacturing	The Association of the Swedish Engineering Industries provides digitisation and cybersecurity services (including cybersecurity awareness) to its members in Sweden. Occasionally, it also produces and distributes materials to raising cybersecurity awareness in different forms, e.g., podcasts, reports, and videos.
Investment Company Institute (ICI Global) [78]	Finance	The Investment Company Institute offers reference tools and resources to help members address cyber threats and develop sound cybersecurity risk management programmes. It also publishes cybersecurity awareness articles in its website's Viewpoint section. These articles can be filtered by selecting Cybersecurity from the "Search by Topic" dropdown.
Europe's Distribution System Operators (E.DSO) [79]	Electricity Distribution (Smart Grid)	Europe's Distribution System Operators and its partners organise cybersecurity events for member organisations.
The Luxembourg Banker's Association (ABBL) [80]	Banks and Financial intermediaries	The Luxembourg Banker's Association organizes cybersecurity events for its members. It raises the cybersecurity awareness of its members through articles and by referring to the awareness materials from third parties like ENISA and EUROPOL that are relevant to the banking sector.

Association of Mutual Insurers and Insurance Cooperatives in Europe (AMICE) [81]	Insurance for SMEs	The Association of Mutual Insurers and Insurance Cooperatives in Europe organizes workshops on GDPR and data protection for its members.
GSMA [82]	Mobile and IoT	The GSMA organises cybersecurity events and distributes other resources, e.g., threat landscape, cybersecurity guidelines and frameworks, and related articles to raise the cybersecurity awareness of member organisations.
Confederation of British Industry (CBI) [83]	General	The Confederation of British Industry organises events and provides resources to members (include SMEs) to raise their cybersecurity awareness.
Insurance Europe [84]	Finance	The Insurance Europe publishes reports on GDPR and cyber risks for the insurer and the insured.
European Banking Federation (EBF) [85]	Banking and Finance	The European Banking Federation organises cybersecurity events, publishes reports, and interviews on cybersecurity issues relevant to the banking sector in Europe.

Table 4: List of European trade associations and federations that provide cybersecurity awareness materials to members

These European trade associations and federations have targeted:

- Cyber risks and threats relevant to their particular sector or industry
- Cybersecurity best practices and cyber hygiene
- Cybersecurity mechanisms, assessment guidelines, and frameworks for their sector or industry
- International and regional regulations and standardisations
- Cybersecurity incident reportings
- Cybersecurity requirements specific to their sector or industry
- Cybersecurity tools and references of third parties resources useful to their sector or industry

Their websites are active and found to be regularly updated with discussions on existential cyber risks and threats including emerging and evolving ones.

To raise the cybersecurity awareness of members, these organisations mostly use events, reports, and articles. Most awareness materials required user authentication to access them. Some articles and reports that are open for everyone include a feature to share on social media or send through email.

In addition to ‘identification’, ‘detection’, and ‘protection’ actions, the awareness materials also discuss ‘response and ‘recovery’ actions that need to be taken if a cyber attack or data breach has occurred.

3.5 International US-based Companies

Since the number of private organisations that produce cybersecurity awareness materials is vast in numbers, we have listed only a few of them which specifically offer cybersecurity awareness services and resources. More importantly, these listed organisations offer some awareness materials free of cost. Some European organisations collaborate with these organisations to prepare cybersecurity awareness materials, for example, CERT Poland and CERT Iceland collaborate with SANS Institute, and CERT Latvia collaborates with STOP.THINK.CONNECT. Similarly, CyberReady and InfoSec Institute offer awareness materials in different European languages. Then, Proofpoint partners with companies such as Atos, Capgemini, Deloitte, Orange, Telefonica, and Cognizant that operate in Europe. KnowBe4 and Global Knowledge have offices in European countries.

Some useful weblinks of the Private Organisations from where SMEs can access the awareness materials free of cost are provided in Annex E: Private Organisations. To access these awareness materials, often they require users to register.

Companies	Description of Materials /Programmes
SANS Institute [86]	SANS Institute is a US company that provides cybersecurity awareness training and products mostly for a fee. It also provides some basic awareness materials free of cost, e.g., • Posters • Newsletter • Blog articles
InfoSec Institute [87]	InfoSec Institute is a US-based technology training company that provides cybersecurity awareness training and products for a fee. It also provides some awareness resources free of cost and after registration, e.g., • Awareness assessment tools • Videos (YouTube blog) • Podcast • Training videos • Webinars
Cyber Safe Work [88]	It is a website that provides various types of cybersecurity awareness materials free of cost, e.g., • Posters • Quizzes • Newsletter • Assessment questionnaier • Blog
STOP.THINK. CONNECT [89]	STOP. THINK. CONNECT is the global online safety awareness campaign to help all digital citizens stay safer and more secure online. It is a coalition of private companies, non-profits and US government organisations, led by the National Cyber Security Alliance. It provides awareness materials available free of cost, e.g., • Tips & advice • Blog • Campaigns
Proofpoint [90]	Proofpoint is an international US-based enterprise security company. It provides some awareness materials free of cost, e.g., • Webinar • Podcast • Free kit
CybeReady [91]	CybeReady is a private US company that offers cybersecurity training and solutions for Autonomous Cyber Security Awareness. It provides some awareness materials free of cost, e.g., • Playbook • Leaflet

KnowBe4 [92]	KnowBe4 is a private US company that offers cybersecurity training and offers an integrated platform for security awareness training combined with simulated phishing attacks. It provides some awareness materials free of cost, e.g., • Awareness assessment tool
Global Knowledge [93]	Global Knowledge Training is an international US-based IT and professional training company. It provides some awareness materials free of cost, e.g., • Posters

Table 5: List of private organisations that provide some cybersecurity awareness materials free of cost

These companies offer some basic cybersecurity awareness materials for free. Most of these freely available awareness materials can be accessed after registration. The awareness materials are in English (with exceptions from CybeReady and InfoSec Institute that offer awareness materials in other European languages).

These companies offer awareness materials in diversified forms, most of which can be accessed for a fee. Among the freely available awareness materials, most do not include an immediate feedback feature; for example, InfoSec Institute's YouTube channel for cybersecurity awareness has a feedback section just underneath where it has received a large number of feedback from the end-users.

Most of the awareness materials have a feature that allows them to be shared on social media and send them through email.

4 Conclusions and Future Work

There are many organisations that produce and distribute a wide range of cybersecurity awareness materials free of cost. In this report, we have elicited such sources from where SMEs can download and use freely available cybersecurity awareness materials. These sources are mainly categorised into

1. European agencies and organisations,
2. EU-funded and national projects,
3. National organisations of EEA countries and the UK,
4. European trade associations and federations, and
5. International US-based companies that offer cybersecurity awareness and training.

Many of the materials may not exactly fit the business needs, organisational culture, and IT infrastructure of a particular SME, which may require tailoring the materials to fit the needs and context of the business. The awareness materials should be accessible, suitable for the user's circumstance and situations or conditions, communication strategies and techniques that suit the preference of the users, interactive and innovative to engage the audiences, and be inclusive so that no subset of the audience feels left out. Moreover, they should include tracking capabilities like self-assessment and feedback that can help to verify whether people are actually learning, and also facilitate interested users to participate and contribute to the future improvement of the awareness programme.

It is suggested that SMEs should use multiple forms of awareness materials that can fulfil the needs of diverse users and business contexts [6] [94]. The availability of awareness materials in different forms helps address a larger audience with different learning needs and preferences [95]; for example, someone with no interest in reading can utilise cybersecurity awareness materials available in the form of videos, games or simulations. Moreover, people can easily acclimate to the cybersecurity awareness materials, if always provided in the same form, thus reducing their effectiveness. Hence, using multiple channels also ensures that people are exposed to the same information multiple times but in different ways.

Future activities include conducting interviews with a selection of SME associations with a focus on the end-user experience, in order to understand the multiple channels they currently use, their efficacy and where the gaps in provision are. Given the huge amount of material available, we want to make a good qualitiatvie assessment on the reach of this resource and effort and how effective it is in getting the job done. We also plan to approach a heterogeneous set of SMEs that ideally lie across two or three vertical sectors, and are from more than one EU Member State. These interviews will investigate:

- how SME employees learn about the technical, legal and financial ramifications of cybersecurity preparedness
- where SMEs get cybersecurity information from
- who or what persuaded the SMEs to invest in developing cybersecurity awareness
- which intermediaries are best placed to reach out to constituent groups of SMEs to engage in cybersecurity awareness training
- what lessons can be learned from recent health messaging campaigns around COVID-19 and homeworking in terms of reaching a large and varied demographic

5 References

[1] European Commission, “What is an SME?,” *Europen Commission*, 2020, https://ec.europa.eu/growth/smes/sme-definition_en

[2] The World Bank, “Small and medium enterprises (SMEs) finance,” *The World Bank*, 2019, https://www.worldbank.org/en/topic/smefinance

[3] D. Clark, “Number of small and medium-sized enterprises (SMEs) the European Union in 2018,” *Statista*, 2019, https://www.statista.com/statistics/878412/number-of-smes-in-europe-by-size/

[4] P. Muller et al., "Annual report on European SMEs 2018/2019: Research & development and innivation by SMEs," European Commission, November 2019, https://op.europa.eu/en/publication-detail/-/publication/cadb8188-35b4-11ea-ba6e-01aa75ed71a1/language-en

[5] N. Farvaque et al., “Guide for training in SMEs,” *European Commission DG Employment, Social Affairs and Inclusion*, June 2009, https://ec.europa.eu/social/BlobServlet?docId=3074&langId=en

[6] M. Bada, A.M. Sasse, J.R.C. Nurse, “Cyber security awareness campaigns: Why do they fail to change behaviour?,” in *International Conference on Cyber Security for Sustainable Society*, Coventry, UK, 2015.

[7] L. A. Aguilar, “The need for greater focus on the cybersecurity challenges facing small and midsize businesses,” *U.S. Securities and Exchange Commission*, 2015, https://www.sec.gov/news/statement/cybersecurity-challenges-for-small-midsize-businesses.html

[8] C. Ponsard, J. Grandclaudon and G. Dallons, “Towards a cyber security label for SMEs: A European perspective,” in *4th International Conference on Information Systems Security and Privacy*, Funchal, Madeira, Portugal, 24-26 January 2018.

[9] M. Wilson & J. Hash, “Building an information technology security awareness and training program,” NIST Special Publication 800-50", *National Institute of Standards and Technology*, 2003, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-50.pdf

[10] R. Crouan et al., “Supporting specialised skills development: Big data, Internet of Things and cybersecurity for SMEs,” *European Commission*, 2019, https://www.digitalsme.eu/digital/uploads/March-2019_Skills-for-SMEs_Interim_Report_final-version.pdf

[11] OECD, “Strengthening SMEs and enterpreneurship for productivity and inclusive growth: Key issue paper,” in *OECD SME Ministerial Conference* , 22-23 February 2018, https://www.oecd.org/cfe/smes/ministerial/documents/2018-SME-Ministerial-Conference-Key-Issues.pdf

[12] Fireeye, “Stopping cyber crime against small and midsize enterprises,” Fireeye Inc., https://www.fireeye.com/offers/stop-cyber-crime-against-small-medium-enterprises.html, 2020

[13] S. Dojkovski, S. Lichtenstein, and M. Warren, “Challenges in fostering an information security culture in Australian small and medium sized enterprises,” in *European Conference on Information Warfare and Security*, Helsinki, Finland, 2006.

[14] T. Kurpjuhn, “The SME security challenge,” *Computer Fradu & Security*, vol. 2015, no. 3, pp. 5-7, 2015.

[15] A. Blau, "The behavioural economics of why executives underinvest in cybersecurity," *Harvard Business Review*. Available: https://hbr.org/2017/06/the-behavioral-economics-of-why-executives-underinvest-in-cybersecurity, 07 June 2017.

[16] R. Baskerville, "Risk analysis: an interpretive feasibility tool in justifying information systems security," *European Journal of Information Systems*, Bd. 1, Nr. 2, pp. 121-130, 1991.

[17] N.M. Menon & M.T.Siponen, "Executives' commitment to information security: Interaction between the preferred subordinate influence aproach (PISA) and proposal characteristics," *The DATABASE for Advances in Information Systems*, Bd. 51, Nr. 2, pp. 36-53, May 2020.

[18] European Union, https://europa.eu/european-union/contact/institutions-bodies_en

[19] ENISA, https://www.enisa.europa.eu/

[20] EUROPOL, https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides

[21] EMSA, http://www.emsa.europa.eu/contact/advanced-search/item/3477-cybersec.html

[22] ECSO, https://ecs-org.eu/working-groups/wg5-education-training-awareness-cyber-ranges

[23] European Digital SME Alliance, https://www.digitalsme.eu/working-groups/

[24] Cyberwatching.eu, https://www.cyberwatching.eu/projects

[25] Cyberwatching.eu, https://www.cyberwatching.eu/about-us

[26] Cyberwiser.eu, https://www.cyberwiser.eu/about-cyberwisereu

[27] SMESEC, https://www.smesec.eu/opencall.html

[28] Geiger, https://project.cyber-geiger.eu/about.html

[29] Cyber-MAR, https://www.cyber-mar.eu/material-hub/

[30] SecureHospitals, https://project.securehospitals.eu/

[31] DOGANA, https://www.dogana-project.eu/

[32] FORTIKA , https://fortika-project.eu/

[33] CyberSec4Europe, https://cybersec4europe.eu/about/

[34] PUZZLE, https://puzzle-h2020.com/

[35] Cyberwiser.eu, https://www.cyberwiser.eu/cartography

[36] Cyber Security Austria, https://www.cybersecurityaustria.at/index.php/verein/ziele

[37] Cyber Security Coalition, https://www.cybersecuritycoalition.be/

[38] Centre for Cyber Security Belgium, https://ccb.belgium.be/en

[39] Safeonweb, https://www.safeonweb.be/en

[40] CERT Bulgaria, https://www.govcert.bg

[41] CARNet, https://www.cert.hr/en/home-page/

[42] Cyprus Cybercrime Center of Excellence , http://www.3ce.cy/en/
[This website is currently unavailable]

[43] National Cyber and Information Security Agency, https://www.nukib.cz/en/

[44] CFCS, https://cfcs.dk/en/

[45] Republic of Estonia Information System Authority, https://www.ria.ee/en/information-system-authority/publications.html

[46] Finnish Transport and Communication Agency National Cyber Securiy Center, https://www.kyberturvallisuuskeskus.fi/en/

[47] The National Cybersecurity Agency of France , https://www.ssi.gouv.fr/en/cybersecurity-in-france/the-national-cybersecurity-agency-of-france/

[48] Federal Office for Information Security , https://www.bsi.bund.de/EN/Home/home_node.html

[49] Hellenic Computer Security Incident Response Team, https://csirt.cd.mil.gr/

[50] GovCERT-Hungary, https://nki.gov.hu/

[51] HunCERT. Hungary, https://www.cert.hu/a-hun-cert-csoportrol

[52] Computer Emergency Response Team-Iceland , https://www.cert.is/

[53] Irish Reporting and Information Security Service , https://www.iriss.ie/challenge.html

[54] Computer Security Incident Response Team-Italia, https://csirt.gov.it/

[55] Information Technology Security Incident Response Institution, Republic of Latvia , https://cert.lv/en

[56] National Cyber Security Centre of Lithuania , https://www.nksc.lt/naujienos/psl_1.html

[57] Computer Emergency Response Team, Luxembourg, https://www.govcert.lu/en/

[58] Cyber Security Malta, https://cybersecurity.gov.mt/

[59] National Cyber Security Centrum, https://www.ncsc.nl/“.

[60] Norwegian National Security Authority, https://nsm.no/about-nsm/about-the-norwegian-national-security-authority/

[61] NorSIS, https://norsis.no/english/

[62] Computre Emergency Response Team Polska, https://www.cert.pl/en/

[63] Centro Nacional de Cibersegurança Portugal, https://www.cncs.gov.pt/en/

[64] Serviciul Roman De Informații, https://www.sri.ro/en

[65] Centrul Național de Răspuns la Incidente de Securitate Cibernetică, https://www.cert.ro/

[66] Computer Security Incident Response Team Slovakia, https://www.csirt.gov.sk/

[67] Slovenian Computer Emergency Response Team, https://www.cert.si/en/about-si-cert/

[68] The Spanish National Cybersecurity Institute Computer Emergency Response Team , https://www.incibe.es/en

[69] Centro Criptológico Nacional Computer Emergency Response Team, https://www.ccn-cert.cni.es/

[70] Computer Emergency Response Team Sweden, https://www.cert.se/om-cert-se

[71] SWITCH's Computer Emergency Response Team, https://www.switch.ch/security/

[72] The National Cyber Security Center, https://www.ncsc.gov.uk/

[73] Association of Accredited Public Policy Advocates to the European Union , "Top industry associations in the EU", http://www.aalep.eu/top-industry-associations-eu

[74] Association of Accredited Public Policy Advocates to the European Union , "Top 200 EU trade associations," http://www.aalep.eu/top-industry-associations-eu

[75] Federation of Small Businesses UK, https://www.fsb.org.uk/

[76] The Software Alliance, https://www.bsa.org/

[77] The Association of the Swedish Engineering Industries, https://www.teknikforetagen.se/

[78] Investment Company Institute, https://www.ici.org/

[79] Europe's Distribution System Operators, https://www.edsoforsmartgrids.eu/

[80] The Luxembourg Banker's Association, https://www.abbl.lu/

[81] Association of Mutual Insurers and Insurance Cooperatives in Europe, https://www.amice-eu.org/M2M_events.aspx

[82] GSMA, https://www.gsma.com/

[83] Confederation of British Industry, https://www.cbi.org.uk/

[84] Insurance Europe, https://www.insuranceeurope.eu/

[85] European Banking Federation, https://www.ebf.eu/

[86] SANS Institute, https://www.sans.org/security-awareness-training

[87] InfoSec Institute, https://www.infosecinstitute.com/

[88] Cyber Safe Work, https://cybersafework.com/

[89] STOP THINK CONNECT, https://www.stopthinkconnect.org/

[90] Proofpoint, https://www.proofpoint.com/us

[91] CybeReady, https://cybeready.com/?utm_medium=cpc&utm_source=google.com&utm_campaign=security-awareness-ukhttps://www.zeguro.com/blog/32-free-cybersecurity-training-resources-for-smbs

[92] KnowBe4, https://www.knowbe4.com/?__hstc=32281505.ad5f8c92bd245451b79524d15c190ab5.1615733579933.1615733579933.1615733579933.1&__hssc=32281505.2.1615733579933&__hsfp=3071844639

[93] Global Knowledge, https://www.globalknowledge.com/us-en/#gref

[94] U. Gattiker, "Can an early warning system for home users and SMEs make a difference? A field study," in *International Workshop on Critical Information Infrastructures Security*, Samos Island, Greece, 2006.

[95] M. Pattinson et al., “Adapting cyber security training to your employees,” in *12th International Symposium on Human Aspects of Information Security & Assurance*, Dundee, Scotland, UK, 2018.

Annex A: European Agencies & Organisations

European Agencies & Organisations	Source Types	Useful Links
ENISA	Repository	https://www.enisa.europa.eu/media/multimedia/material https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/technical-operational#building https://www.enisa.europa.eu/publications#c5=2011&c5=2021&c5=false&c2=publicationDate&reversed=on&b_start=0
	COVID-19 related materials	https://www.enisa.europa.eu/topics/wfh-covid19?tab=details
	Cybersecurity month	https://cybersecuritymonth.eu/resources?perPage=10&reqPage=1&searchText=&sortOrder=descending
	Training courses	https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/training-courses
	Awareness raising quizzes templates	https://www.enisa.europa.eu/publications/archive/ar-quizzes-templates-en/at_download/fullReport
	Upcoming workshops	https://www.enisa.europa.eu/events#b_start=0
EUROPOL	Repository	https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides
	Ransomware awareness	https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/no-more-ransom-do-you-need-help-unlocking-your-digital-life https://www.nomoreransom.org/en/prevention-advice.html
	Symposium	https://digital-strategy.ec.europa.eu/en/events/first-europol-apwg-symposium-cybersecurity-new-date
	COVID-19 related materials	https://www.europol.europa.eu/activities-services/staying-safe-during-covid-19-what-you-need-to-know
EMSA	Repository	http://www.emsa.europa.eu/we-do/safety/maritime-security/item/3477-cybersec.html
	Conference	http://www.emsa.europa.eu/newsroom/latest-news/item/3441-cooperation-to-raise-cybersecurity-awareness-across-transport-modes.html
ECSO	Repository	https://ecs-org.eu/working-groups/wg5-education-training-awareness-cyber-ranges https://ecs-org.eu/publications

European Digital SME Alliance	Repository	https://www.digitalsme.eu/policy/ https://www.digitalsme.eu/cybersecurity-and-data-protection/ https://www.digitalsme.eu/cyberwatching-eu-tools-and-services-for-cybersecurity-novices-for-leading-innovators/

Table 6: Useful hyperlinks from the websites of European agencies and organisations

Annex B: EU Funded and National Projects

Projects	Source Types	Useful Links
cyberwatching.eu	Repository	https://www.cyberwatching.eu/smes-guides (registered users only) https://www.cyberwatching.eu/about/deliverables
	Tools	https://www.cyberwatching.eu/gdpr-temperature-tool-new-free-resource-european-smes-understand-their-risk-gdpr-related-sanctions https://www.cyberwatching.eu/cybersecurity-best-practices-smes-assessment https://www.cyberwatching.eu/cyberwatching-information-notice-tool https://www.cyberwatching.eu/cyberwatching-cyber-risk-temperature-tool
	Events and workshops	https://www.cyberwatching.eu/webinar https://www.cyberwatching.eu/news-events/events https://www.cyberwatching.eu/cyberwatching-eu-events
Cyberwiser.eu	Repository	https://www.cyberwiser.eu/ https://www.cyberwiser.eu/deliverables https://www.cyberwiser.eu/reports
	Tools	https://www.cyberwiser.eu/
	Training courses	https://www.cyberwiser.eu/courses-comparison
	Market watch	https://www.cyberwiser.eu/skills-watch https://www.cyberwiser.eu/technology-watch
	Events and workshops	https://www.cyberwiser.eu/newsletters https://www.cyberwiser.eu/webinars
	EU national strategies	https://www.cyberwiser.eu/cartography
SMESEC	Repository	https://www.smesec.eu/framework.html https://www.smesec.eu/deliverables.html
	Tools and quizes	https://docs.google.com/forms/d/e/1FAIpQLSdDjbakXjSRtIUPqoZRYaKcmlObsG8In6i4In6RvnPhPyE6Kw/viewform https://www.smesec.eu/smequiz.html
	Events and workshops materials	https://www.smesec.eu/events.html
GEIGER	Repository	https://project.cyber-geiger.eu/deliverables.html

	Tool and learning programme	https://project.cyber-geiger.eu/
	Workshops and events	https://project.cyber-geiger.eu/news.html
Cyber-MAR	Repository	https://www.cyber-mar.eu/material-hub/ https://www.cyber-mar.eu/trainings/
SecureHospitals	Repository	https://project.securehospitals.eu/deliverables/
	Workshops, events, and registration	https://project.securehospitals.eu/media-centre/
DOGANA	Repository	https://www.dogana-project.eu/index.php https://www.dogana-project.eu/index.php/publications/deliverables
	Toolsets	https://www.dogana-project.eu/index.php/project-toolset
	Materials from competition	https://www.dogana-project.eu/index.php/social-engineering-blog/contest-finalists
FORTIKA	Repository	https://fortika-project.eu/public-deliverables https://fortika-project.eu/confidential-deliverables https://fortika-project.eu/content/media
	Training	https://fortika-project.eu/content/training-material
	White papers	https://fortika-project.eu/content/white-papers
	User stories	https://fortika-project.eu/content/user-stories
CyberSec4Europe	Repository	https://cybersec4europe.eu/publications/deliverables/
	News and events	https://cybersec4europe.eu/events/broadcasts-and-webinars/
PUZZLE	Repository	https://puzzle-h2020.com/news-and-blog/

Table 7: Useful hyperlinks from the websites of EU-funded and national projects

Annex C: National Organisations in the EEA and the UK

National Organisations	Website cybersecurity section	Useful Links
Cyber Security Austria	Blog	https://www.cybersecurityaustria.at/index.php/blog/2017/
Cyber Security Coalition Belgium Centre for Cyber Security Belgium SafeonWeb	Tools	https://www.cybersecuritycoalition.be/tools/
	Sectors	https://ccb.belgium.be/en/work
	Entire website	https://www.safeonweb.be/en
Bulgarian Computer Security Incidents Response Team	Advices	https://www.govcert.bg/EN/NAW/SysPages/AllAdvices.aspx
CARNet's National Computer Emergency Response Team, Republic of Croatia	Knowledge base	https://www.cert.hr/HrNaiva
Cyprus Cybercrime Centre of Excellence	Dissemination	http://www.3ce.cy/en/
National Cyber and Information Security Agency Computer Security Incident Response Team Czech Republic	How to use the Internet	https://www.jaknainternet.cz/
	Exercise types	https://www.nukib.cz/en/cyber-security/exercises/exercise-types/
Danish Centre for Cyber Security	Threat assessments, guidance	https://cfcs.dk/en/about-us/about-cfcs/
Republic of Estonia Information Security Authority	Office-instructions	https://www.ria.ee/et/ametist/juhendid.html#kuberturvalisus
Finnish Transport and Communication Agency National Cyber Securiy Centre	NCSC news-instructions and guides	https://www.kyberturvallisuuskeskus.fi/en/ncsc-news/instructions-and-guides/instructions-and-guides-organisations-and-companies https://www.kyberturvallisuuskeskus.fi/en/ncsc-news/instructions-and-guides/instructions-and-manuals-cyber-security-professionals
The National Cybersecurity Agency of France	Basic precautions	https://www.ssi.gouv.fr/entreprise/precautions-elementaires/
	Regulations	https://www.ssi.gouv.fr/entreprise/reglementation/
	Good practices	https://www.ssi.gouv.fr/entreprise/bonnes-pratiques/
	Publications	https://www.ssi.gouv.fr/en/publications/

Federal Office for Information Security, Germany	Topics	https://www.bsi.bund.de/EN/Home/home_node.html
Hellenic Computer Security Incident Response Team	Small and medium businesses	https://csirt.cd.mil.gr/small-medium-businesses/
Hun Computer Emergency Response Team Hungary	Service providers-knowledge base	https://www.cert.hu/tudasbazis
Computer Emergency Response Team-Iceland	Um vefinn	https://www.cert.is/um-vefinn/frettir/
Irish Reporting and Information Security Service	Misc-breach guidance portal	https://www.iriss.ie/breach-portal.html
Computer Security Incident Response Team-Italia	News	https://csirt.gov.it/contenuti
Information Technology Security Incident Response Institution, Republic of Latvia	Entire website	https://www.esidross.lv/2017/03/10/apstajies-padoma-piesledzies/
National Cyber Security Centre Lithuania	Rekomendacijos	https://www.nksc.lt/rekomendacijos.html
Computer Emergency Response Team, Luxembourg	Services-phishing	https://www.govcert.lu/de/phishing/
Cyber Security Malta	Security guide-security tips	https://cybersecurity.gov.mt/category/security-tips/
Nationaal Cyber Security Centrum Netherlands	Cybersecurity topics	https://www.ncsc.nl/
The Norwegian Centre for Information Security	Publikasjoner	https://norsis.no/publikasjoner/
Computer Emergency Response Team Polska	OUCH!	https://www.cert.pl/ouch/
Centro Nacional de Cibersegurança Portugal	Recursos-boas práticas	https://www.cncs.gov.pt/recursos/boas-praticas/
	Recursos-newsletters	https://www.cncs.gov.pt/recursos/newsletters/
Cyber Security Research Centre	What do we do-awareness	https://www.sri.ro/awareness (access to awarness programme by registration)
	Alerte	https://www.cert.ro/tag/alerte

Centrul Național de Răspuns la Incidente de Securitate Cibernetică	Conștientizare	https://www.cert.ro/doc/ghid https://www.cert.ro/pagini/campania-anti-malware-mobil https://www.cert.ro/pagini/campania-prevenire-criminalitate-informatica https://www.cert.ro/pagini/constientizare-inselaciuni-cu-suport-tehnic-fals https://www.cert.ro/pagini/informatii-generale-despre-nis https://www.cert.ro/pagini/CVD https://www.cert.ro/tag/ECSM
Computer Security Incident Response Team Slovakia	Bezpečnostná študovňa	https://www.csirt.gov.sk/bezpecnostna-studovna-879.html
Slovenian Computer Emergency Response Team	News	https://www.cert.si/en/category/news/
The Spanish National Cybersecurity Institute-Computer Emergency Response Team Centro Criptológico Nacional Computer Emergency Response Team	Publications-guide	https://www.incibe-cert.es/en/publications
	Publications-webinars	https://www.incibe-cert.es/en/webinars
	Guides	https://www.ccn-cert.cni.es/en/guides.html
Computer Emergency Response Team Sweden	Nyheter	https://www.cert.se/
SWITCH's Computer Emergency Response Team	Website	https://www.switch.ch/saferinternet/
	SWITCH security awareness adventures	https://www.switch.ch/security/info/switch-security-awareness-adventures/
The National Cyber Security Centre United Kingdom	Information for small & medium sized organisations	https://www.ncsc.gov.uk/section/information-for/small-medium-sized-organisations
	Advice and guidance - all topics	https://www.ncsc.gov.uk/section/advice-guidance/all-topics

Table 8: Useful hyperlinks from the websites of national organisations in the EEA and the UK

Annex D: European Trade Associations and Federations

European Organisations	Website Section	Useful Links
Trust in Digital Life	Publications	GDPR for SMEs in English, French, German, Italian and Spanish https://trustindigitallife.eu/wp-content/uploads/GDPR-for-SMEs.pdf https://trustindigitallife.eu/wp-content/uploads/RGPD-pour-les-PMEs-FR.pdf https://trustindigitallife.eu/wp-content/uploads/RGPD-per-le-PMIs-IT.pdf https://trustindigitallife.eu/wp-content/uploads/RGPD-para-PYMEs-ES.pdf
Federation of Small Businesses UK	Join us – membership - FSB protection	https://www.fsb.org.uk/join-us/membership/cyber-protection.html
	Resource library	https://www.fsb.org.uk/resource-library.html?q=cyber+security https://www.fsb.org.uk/resources-page/how-to-protect-your-business-against-cyber-attacks.html https://www.fsb.org.uk/resources-page/how-to-respond-to-a-cyber-security-incident.html
	Events	https://www.fsb.org.uk/event-calendar/protecting-your-northern-ireland-business-from-cyber-crime-attacks-with-free-services.html
	Cybersecurity basics	https://www.fsb.org.uk/cyber.html
The Software Alliance	Compliance solutions	https://bsacompliancesolutions.org/education-awareness/
	Reports	https://www.bsa.org/reports
The Association of the Swedish Engineering Industries	Podcasts	https://www.teknikforetagen.se/nyhetscenter/podcast/40-foretaget-som-blev-utsatt-for-cyberangrepp/ https://www.teknikforetagen.se/nyhetscenter/podcast/41-cyberhotet-mot-sverige---hur-ser-hotbilden-ut/ https://www.teknikforetagen.se/nyhetscenter/podcast/39-sa-skyddar-du-dig-mot-natbedragerier/
	Fokusområden-digitalisering och cybersäkerhet	https://www.teknikforetagen.se/fokusomraden/digitalisering-och-cybersakerhet/
Investment Company Institute	News and resources - viewpoints - cybersecurity	https://www.ici.org/viewpoints

	Fund operations - technology, cyber and BCP	https://www.ici.org/ops/tech
Europe’s Distribution System Operators	Events	https://www.edsoforsmartgrids.eu/events/
The Luxembourg Banker’s Association	News	https://www.abbl.lu/2020/10/28/conference-cybersecurity-mitigating-risk-during-and-after-covid-19-key-take-aways/
		https://www.abbl.lu/2020/12/04/strong-customer-authentication-what-why-when-2/ https://www.abbl.lu/2020/10/08/cybersecurity-week-2020/ https://www.abbl.lu/2020/09/29/ict-and-security-requirements-for-regulated-entities-key-insights/ https://www.abbl.lu/2020/07/29/no-more-ransom-helping-victims-fighting-back-against-hackers/
	Client information	https://www.abbl.lu/topic/safe-banking/ https://www.abbl.lu/topic/phishing-smishing-vishing/
Association of Mutual Insurers and Insurance Cooperatives in Europe	Events	https://www.amice-eu.org/M2M_events.aspx
GSMA	What we do - IoT security	https://www.gsma.com/iot/iot-security/
	News	https://www.gsma.com/newsroom/resources/covid-19-mobile-cyber-security-fraud-threat-observations-and-incidents/
	What we do - mobile for development	https://www.gsma.com/mobilefordevelopment/blog/cybersecurity-a-governance-framework-for-mobile-money-providers/
	What we do - working groups	https://www.gsma.com/aboutus/workinggroups/benefits
Confederation of British Industry	Search (cyber security)	https://www.cbi.org.uk/search/?term=Cyber%20security&sort=&page=1
Insurance Europe	Positions - data protection, cyber risk, digitalisation	https://www.insuranceeurope.eu/data-protection https://www.insuranceeurope.eu/cyber-risk https://www.insuranceeurope.eu/digitalisation
European Banking Federation	Priorities - innovation & cybersecurity	https://www.ebf.eu/priorities/innovation-cybersecurity/cybersecurity/
	Search ‘cyber security’	https://www.ebf.eu/?s=cyber+security

Table 9: Useful hyperlinks from the websites of European trade associations and federations

Annex E: International US-based Companies

Companies	Website Section	Useful Links
SANS Institute	Resources - posters	https://www.sans.org/security-awareness-training/resources/posters
	Resources - OUCH! newsletter	https://www.sans.org/security-awareness-training/ouch-newsletter
	Resources - blog	https://www.sans.org/security-awareness-training/blog
InfoSec Institute	Resources - free tools	https://www.infosecinstitute.com/resource-center/?_resource_type=type-tool
	Resources – blog - YouTube	https://www.youtube.com/channel/UC4TAjYDpNggDwictUA180LA
	Resources - cyber work - cyber work podcast	https://www.infosecinstitute.com/podcast/
	Resources - cyber work - cyber work applied	https://www.infosecinstitute.com/learn/ (Requires registration)
	Resources - webinars	https://www.infosecinstitute.com/resource-center/?_resource_type=type-video (Requires registration)
	Infosec IQ training and awareness content library	https://www.infosecinstitute.com/iq/content-library/?_content_library_language=english
Cyber Safe Work	Entire website	https://cybersafework.com/
STOP.THINK. CONNECT	Entire website	https://www.stopthinkconnect.org/
Proofpoint	Resources	https://www.proofpoint.com/us/resources (Requires registration)
CyberReady	Resources - playbook	https://cybeready.com/resource-center/playbook (Require registration)
	Resources - leaflet	https://cybeready.com/ciso-toolkit
KnowBe4	Free tools	https://www.knowbe4.com/ (Requires registration)
Global Knowledge	Posters	https://www.globalknowledge.com/us-en/topics/cybersecurity/cybersecurity-awareness-posters/#gref

Table 10: Useful hyperlinks from the websites of international companies with free awareness materials