Cyber MSME

Cybersecurity for Micro, Small & Medium Enterprises

Training module title:

European landscape for cybersecurity: policies and support strategies

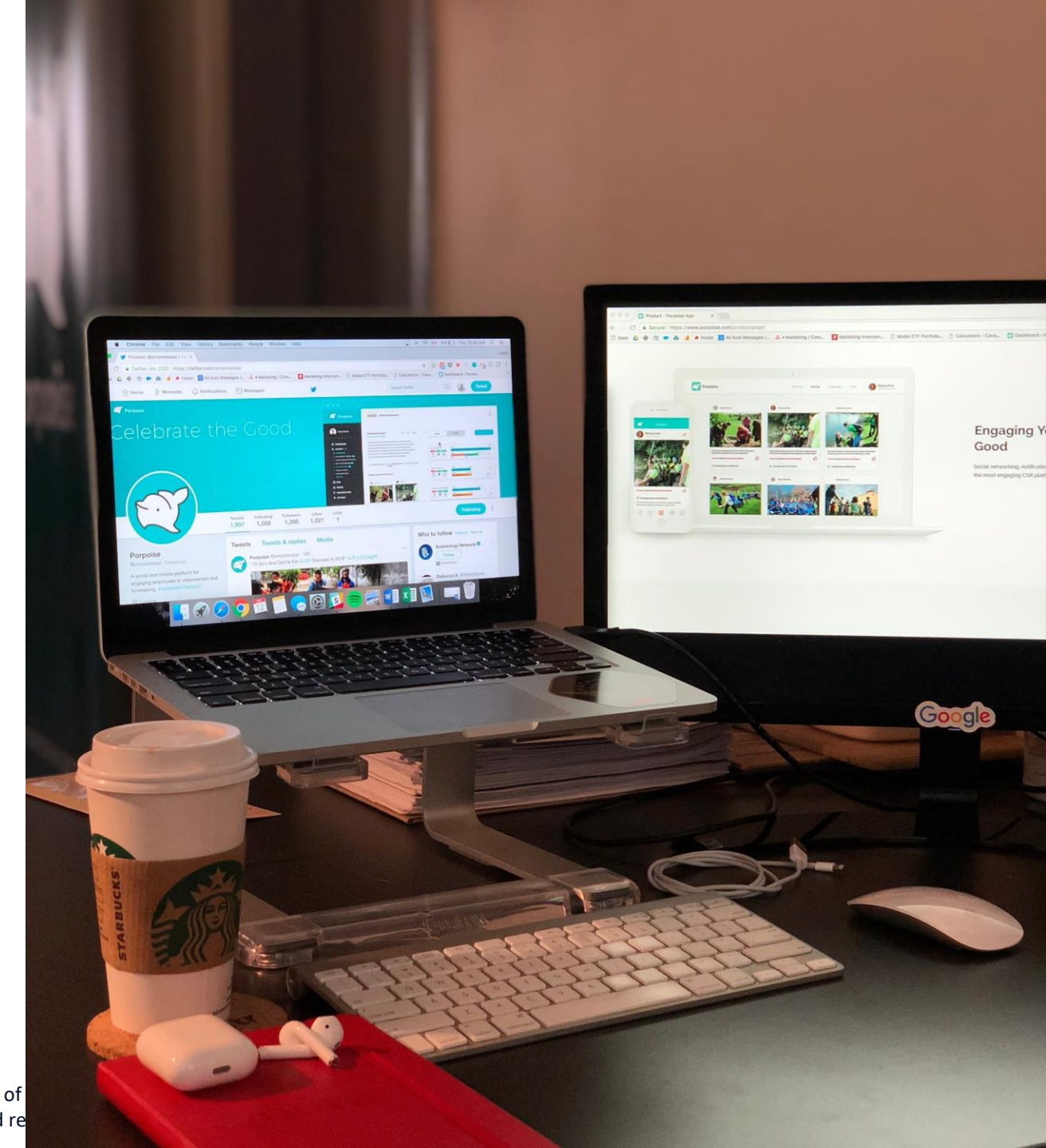
By IHF asbl

Erasmus+

Objectives and Goals:

The aim of this module is to mainstream and showcase what are the current and future horizons for cybersecurity at EU level in terms of policies and programmes, strategies and legislations.

We want also to provide an overview on institutional setting of relevance (i.e. what is ENISA and what do they do?) and supporting networks. This module is conceived as a comprehensive handout of all information that are useful to understand how cybersecurity challenges are tackled by EU Institutions and nurture awareness on further available opportunities (financial aid, training, etc.) coming from EU institutional settings.



Erasmus+

The European Commission's support for the production of
only of the authors, and the Commission cannot be held re

Index

Unit 1: The Key players for EU cybersecurity

Introduction

The content of this training module is really intended to be a road-map for users on the EU ecosystems of cybersecurity in terms of latest trends and dynamics, support mechanisms, useful resources (report, training material, etc.).

This is to provide learners robust and reliable references in case they wish to deepen their understanding of cybersecurity from a broader perspective that takes into consideration the many facets of the phenomenon.

In other words, we indicate learners trustworthy info points that they can look into to get a more comprehensive understanding of cybersecurity for their businesses, rather than consulting general web sources…

Unit 1: The Key players for EU cybersecurity

Section 1.1: ENISA – European Union Agency for Cybersecurity

Established in 2004 by the EU regulation 460/2004 (repealed by Regulation (EU) No 526/2013), ENISA is one of the many agencies of the European Union and it is tasked with the important responsibility to foster an EU-wide culture of IT security, digital proficiency, cyber-resilience and cyber-readiness.

The information and security network that the agency contributes to is designed for the benefits of EU societies as a whole, with reference to citizens, businesses, public sector and labour market.

Since its formal establishment, and following the Cybersecurity Act, ENISA's role is to assist the European Commission, Member States and the EU communities in embracing and adopting the newest cybersecurity standards in view of present and future threats.

Unit 1: The Key players for EU cybersecurity

Section 1.2: ENISA – organisation and constituent bodies

As per Regulation (EU) 2019/881, ENISA is composed by the following bodies:

- **Management Board**: it ensures the agency's compliance with its statue and founding regulation
- **Executive Board:** it represent the decision-making body and instructs the management board on decisions to be adopted
- **Executive Director**: the ED manages the agency and he/she's responsible for his/her duties independently
- **National Liaison Officers Networks:** the NLOs bridges and mediate the communication between the agency and each member state
- **Advisory Group:** it includes an external group of experts that sustains ENISA in the planning and development of work programmes, STKH management and strategic objectives
- **Ad hoc working groups:** the ED selects external experts to tackle specific scientific/technical matters (i.e., draft and consolidation of a multinational scale assessment)

Unit 1: The Key players for EU cybersecurity

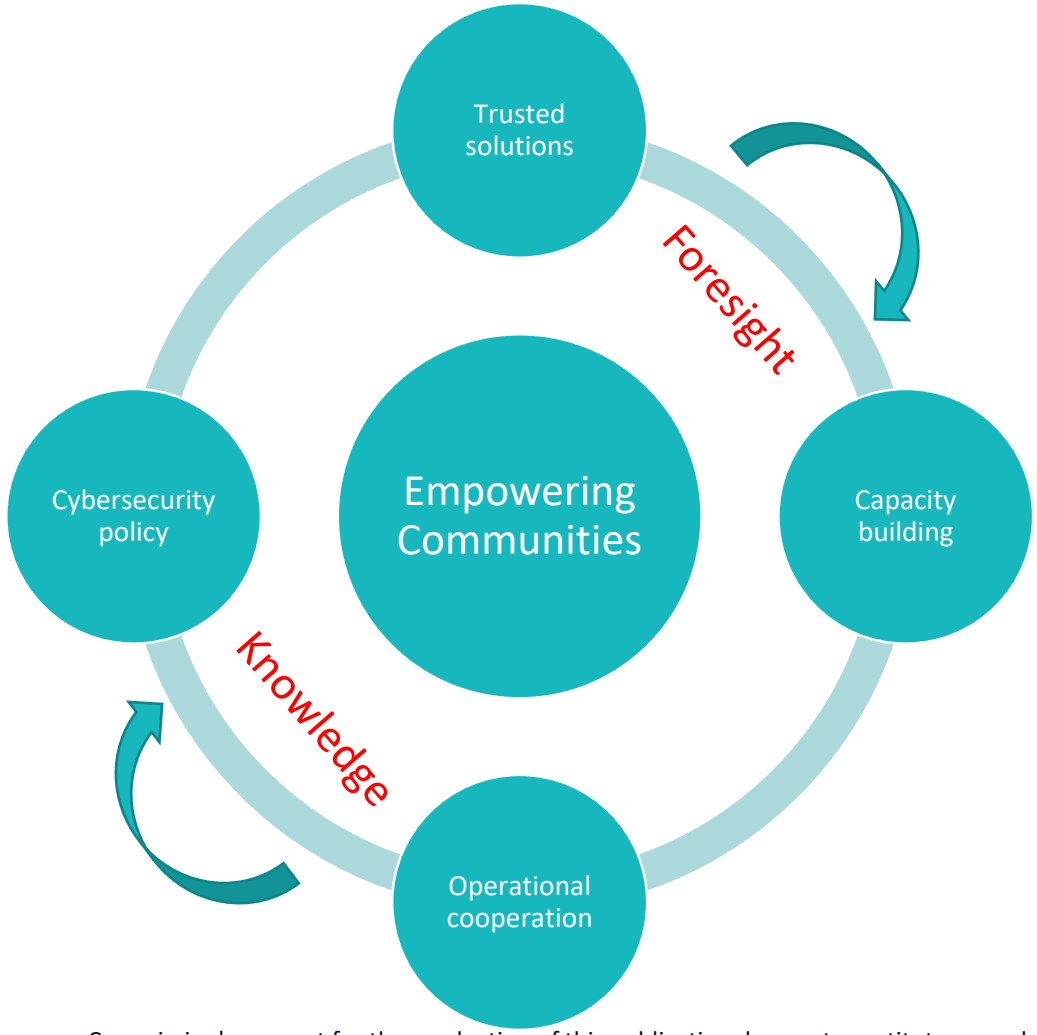
Section 1.3: ENISA – areas of interest

ENISA's areas of interest are many, but they can be essentially broken-down into 7 main clusters of activities:

- **Empowering Communities** – ENISA brings together national and international STKH that are of relevance for cybersecurity and enhances their synergies so as to upscale more easily new cybersecurity models
- **Cybersecurity policy** – ENISA provides for evidence-based qualitative and quantitative phenomena that can better inform new policies on IT, innovation and development
- **Operational Cooperation** – ENISA strengthen the axis between the many socio-economic actors that can have an impact (or are impacted by) new ground breaking development in the domain of ICT, and most importantly, cybersecurity.
- **Capacity Building** – ENISA provides for user friendly and intuitive on cybersecurity at free disposal for all citizens, and/or private businesses
- **Trusted Solutions** – ENISA monitors and evaluates new digital products and services tackling cybersecurity solutions for societies, markets and economies
- **Foresight** – ENISA contributes to develop new mitigations strategies the exposure of EU societies and economies to cyberthreats
- **Knowledge** – ENISA represent a vibrant hub for professionals and experts to exchange best practices

Unit 1: The Key players for EU cybersecurity

Section 1.3: ENISA – areas of interest: visual representation



Erasmus+

Unit 1: The Key players for EU cybersecurity

Section 1.4: why you should care about ENISA?

As a formal representative of the private sector, why should you even bother with ENISA?

- First or all, if there is any new horizon in the landscape of cybersecurity, ENISA will represent your most comprehensive source of information. No other platform has many resources as ENISA to get a better “grasp” on cybersecurity-related phenomenon at EU level
- In second stance, ENISA provides for users (i.e., business owners) a large set of resources to strengthen and foster their comprehension of cybersecurity and their own cyber-resilience/awareness/responsiveness such as crisis simulation, tools and training materials, reports and studies

Please, take your time to explore the platform and familiarize with all available resources.

Unit 1: The Key players for EU cybersecurity

Section 1.5: ESCO – European Cybersecurtiy Organisation

The European Cybersecurity Organization (ESCO) is among the top EU stakeholders in the domain of IT security and cyber-readiness. The main goal of the organization remains to promote an EU-ecosystem devoted to foster research and awareness in the domain of cybersecurity.

- ESCO is a privileged partner of both the European Commission and ENISA, bridging private an public institutions operating at international and national level
- ESCO supports the implementation of key cybersecurity strategies aimed at sustain the “cyber-transition” of public and private organizations
- ESCO assists EU bodies and agencies in developing new policies and recommendations that find application at national level

Erasmus+

Unit 1: The Key players for EU cybersecurity

Section 1.6: ESCO's areas of interest

ESCO's areas of interest are allocated to specific working groups (WG):

- **WG1 – Standardization, certification and supply chain management**
- **WG2 – Market deployment, investments and international collaboration**
- **WG3 – Cyber resilience of economy, infrastructures and services**
- **WG4 – Support to SMEs, coordination with countries and regions**
- **WG5 – Education, training, awareness and cyber ranges**
- **WG6 – SRIA and cybersecurity technologies**

More in general, ESCO tackles all transversal domains of references to help the emergence of a robust EU-spread cybersecurity culture.

Unit 1: The Key players for EU cybersecurity

Section 1.7: further support material from ESCO

Each WG is responsible for the publication and promotion of an extensive number of reports providing for numerous useful information.

ESCO's analysis are robust and reliable, users can access them for free and gain some really useful insights and the many different interest areas tackled by ESCO.

Please, feel free to navigate the Publications section as well as all the other activities carried out by the organization.

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Unit 2: EU policies and programmes for cybersecurity

Section 2.1: EU cybersecurtiy strategy

On December 2020, the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy launched the new EU's Cybersecurity Strategy for the Digital Decade (2019-2024).

The strategy represent a key component of three other EU long-term priorities (Shaping Europe's Digital Future, the Recovery Plan for Europe and the EU Security Union Strategy) responding to the need of fostering technological readiness and competitiveness of EU societies and economies.

EU's cyber resilience is at the very core of the new cybersecurity strategy and allows EU's Member States to adopt, embrace and implement new performance standards to guarantee a safe digital environment for their citizens and businesses. The strategy rests on three key pillars: **resilience**, **operational capacity**, **international cooperation**

Erasmus+

Unit 2: EU policies and programmes for cybersecurity

Section 2.1: EU cybersecurtiy strategy – RESILIENCE

Resilience, technological sovereignty and leadership is the very first strand of the new cybersecurity strategy.

With that, the European Commission wants to promote new quality standards for the security of IT networks of critical national infrastructures and services such as financial and public health systems.

Of particular interest is the education and training dimension as under this pillar the European Commission foreseen dedicated support measures to SMEs and private organisations such as:

- Research and innovation
- Workforce upskilling
- Nurturing of new cybersecurity talents

Erasmus+

Unit 2: EU policies and programmes for cybersecurity

Section 2.1: EU cybersecurtiy strategy – OPERATIONAL CAPACITY

By operational capacity we mean the adequacy and effectiveness of EU's Members States in assessing, preventing/discouraging and responding to cyberthreats.

In that sense, both the European Commission and the High Representatives remarks with particular emphasis the primary objective to safeguard from malicious attacks all critical infrastructures of modern societies and ones impacting of democratic processes, supply chains infrastructures, etc.

New transnational capacity building programmes are also encouraged among Member States as one of those instrumental means to build a new EU cyber ecosystem.

Unit 2: EU policies and programmes for cybersecurity

Section 2.1: EU cybersecurtiy strategy – INTERNATIONAL COOPERATION

A renewed strategy on cybersecurity will be tackled and implemented in cooperation with international stakeholders in view of a global stability.

The European Commission plans to intensify the dialogue with third countries and large international organizations that can be of paramount support to establish a global community-centered agenda for IT security.

These groups of interest will represent the institutional partners of the European Commission throughout this unprecedented 7-year programming of actions and support means.

Erasmus+

Unit 2: EU policies and programmes for cybersecurity

Section 2.2: the NIS Directive

The NIS directive is one of the most important piece of legislation regulating for a high common level of cybersecurity and information system across the European Union.

Adopted in 2016, the directive gives each Member State certain degrees of “autonomy” for its application at national level, in consideration of specific circumstances and contextual factors.

Citizens can monitor the status of implementation of the directive by consulting the state-of-play of its transposition.

Unit 2: EU policies and programmes for cybersecurity

Section 2.2: the pillars of NIS directive

- **NATIONAL CAPABILITIES**

EU's Members States are required to develop certain standards of cybersecurity performance in terms both of capabilities and support networks (i.e., National CSIRT - Computer Security Incident Response Team).

- **CROSS-BORDER COLLABORATION**

EU's Member States are required to establish robust and long-term institutional collaborations with external parties of interest such as CSIRTs and the NIS cooperation group – of which ENISA is a part of.

- **NATIONAL SUPERVISION OF CRITICAL SECTORS**

EU's Member States are required to perform in-depth ex-post and ex-ante supervision of the cyber-readiness of critical services and infrastructures.

Unit 2: EU policies and programmes for cybersecurity

Section 2.2: the NIS2 directive

At the beginning of 2021, the European Commission launched the proposal to revise the NIS directive as a way to address concretely the new wave of cyberthreats that impacted global markets and societies in the last few years.

Cyber-attacks, besides being among the fastest-growing form of crime worldwide, are also growing in scale, cost and sophistication. The latest forecast is that global ransomware damage costs would reach US$20 billion by 2021, 57 times more their amount in 2015 […] *Given the growing number and cost of cyber-attacks, spending on information security is also increasing worldwide. The global security market is currently worth around US$150 billion, a figure that many predict will rise to US$208 billion in 2023 and US$400 billion in 2026.*
Source: European Parliament, the NIS2 directive

At the moment, the NIS2 directive is going through the ordinary policy making process of EU institutions (an on-going revision of carried out by influential groups of interest and policy makers).

Unit 2: EU policies and programmes for cybersecurity

Section 2.3: Shaping Europe's digital future

The EU's strategic programme for the 2019-2024 period includes six main priorities (i.e., "pillars"):

- A European Green Deal
- A Europe fit for the digital age
- An economy that work for people
- A stronger Europe in the world
- Promoting our European way of life
- A new push for European democracy

Specific sub-actions are envisioned for each one of these pillars, cybersecurity falls under A Europe fit for the digital age for both pillar's strands: Shaping Europe's digital future and Europe's Digital Decade: digital targets for 2030.

Erasmus+

Unit 2: EU policies and programmes for cybersecurity

Section 2.4: Support for research and innovation

Research, innovation and IT development in the field of cybersecurity is a top concern of the Horizon Europe programme for the period 2021-2027 – the largest EU programme for research and innovation with a total budget of €95.5 billion

Cybersecurity falls under the cluster of Civil Security for Society, along with disaster-resilient societies, protection & security. Projects under this strand of co-financing are expected to meet one (or more) of the following impacts (pp. 114-115 of the guide):

- Strengthened EU cybersecurity capacities and European Union sovereignty in digital technologies
- More resilient digital infrastructures, systems and processes
- Increased software, hardware and supply chain security
- Secured disruptive technologies
- Smart and quantifiable security assurance and certification shared across the EU
- Reinforced awareness and a common cyber security management and culture

Unit 2: EU policies and programmes for cybersecurity

Section 2.5: Support for capacity building

Cybersecurity represents a major area of interest of the DIGITAL Europe Programme.

The programme tackles both the need of new and technologically advanced infrastructures, skill-gaps and human development of professionals deployed in the sector. Concrete objectives are as follows:

- advanced cybersecurity equipment, tools and infrastructures, together with Member States
- knowledge, capacity and skills related to cybersecurity, best practices
- deployment of effective cybersecurity solutions, paying special attention to public authorities and SMEs
- capabilities within Member States and the private sector in support of the NIS Directive
- resilience, risk-awareness, at least basics levels of cybersecurity
- enhancing synergies and coordination between stakeholders and policy makers

Source: Cybersecurity in the DIGITAL Europe programme – Operational Objectives

Summing up

Key takeaways

- ENISA – EU agency tasked with the role to foster an EU-wide culture of IT security, digital proficiency, cyber-resilience and cyber-readiness
- ESCO – EU key player tasked with the role to promote an EU-ecosystem devoted to foster research and awareness in the domain of cybersecurity
- EU cybersecurity strategy, three key pillars: resilience, operational capacity, international cooperation
- NIS directive, three key pillars: national capabilities, cross-border collaboration, national supervision of critical sectors
- Research and innovation: Horizon EUROPE Capacity building: Digital EUROPE

Erasmus+

Thank you

for your attention!

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.