



# Cybersecurity for SMEs

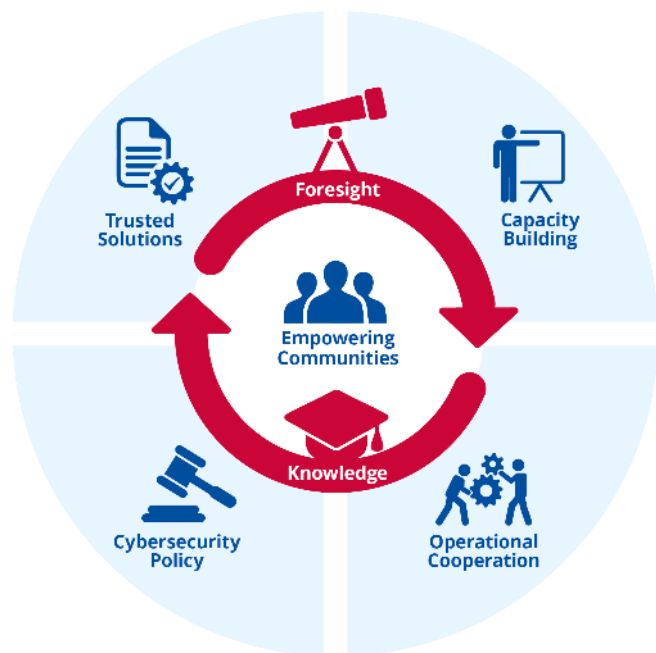
3 | 10 | 2024

**Evangelos Kantas – ENISA**

**Anna Sarri - ENISA**

**Awareness Raising & Education Team**

# ABOUT ENISA



About 150 staff - steadily growing

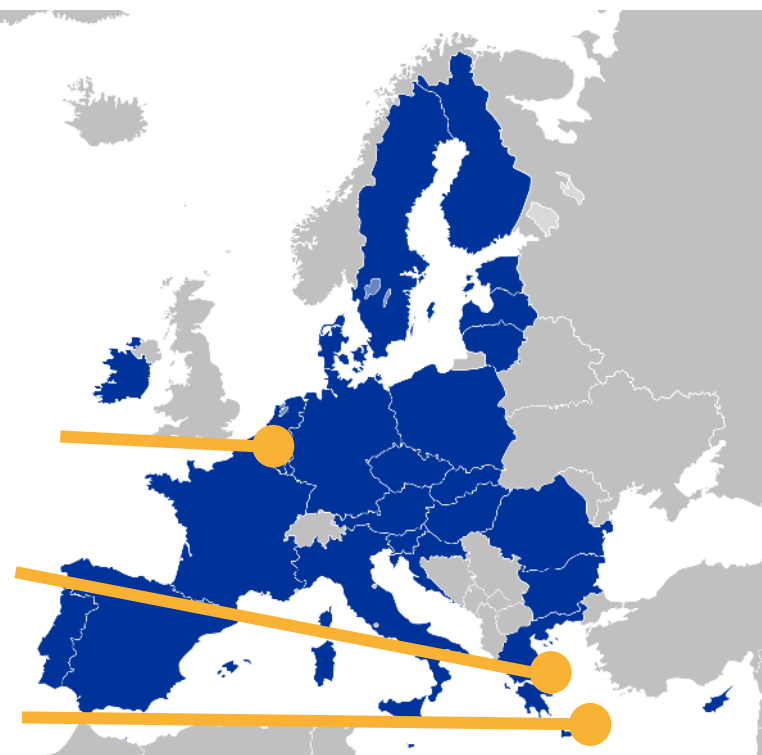
4 units doing cybersecurity work

- Operational collaboration (Cyclone, CSIRT network)
- Cyber exercises, challenges, trainings (Cyber Europe)
- Certification and standardization (EU schemes)
- Policy unit (including EECC, eIDAS, NISD, 5G, eID wallets, critical sectors)

New office in Brussels

Headquarters in Athens

Small office in Heraklion



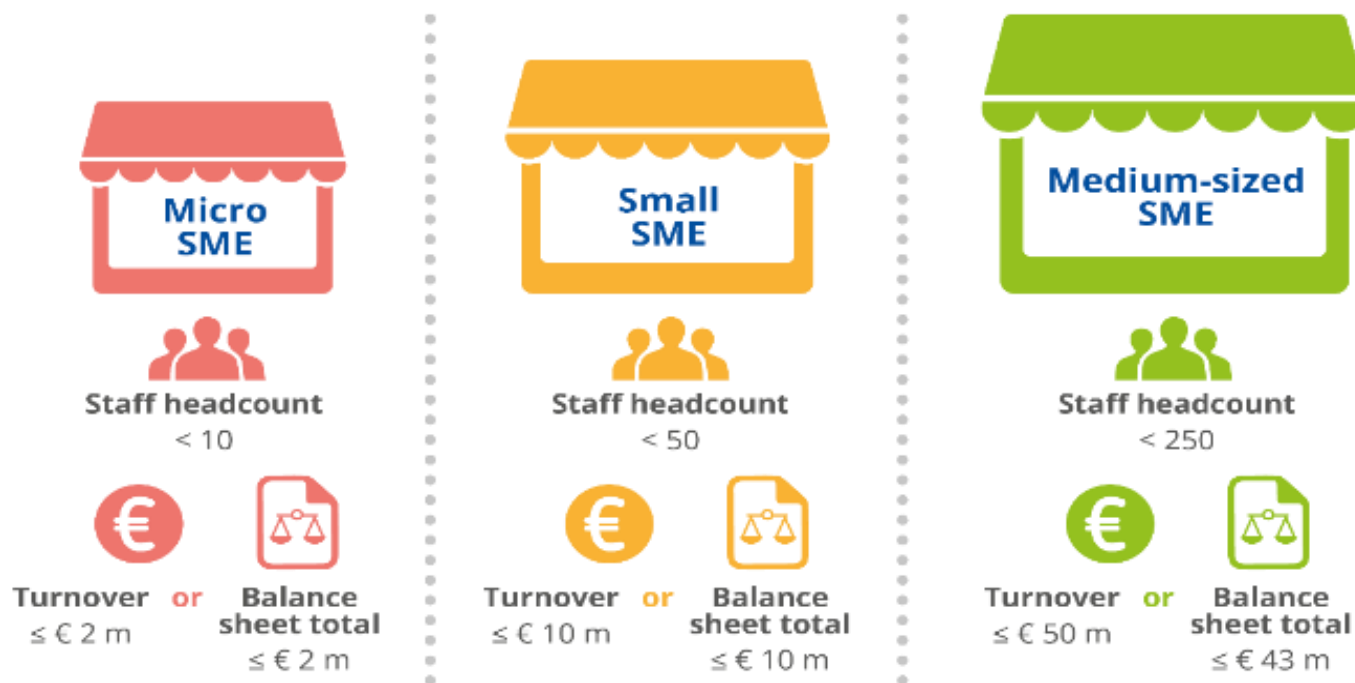
# SMES LANDSCAPE

99%

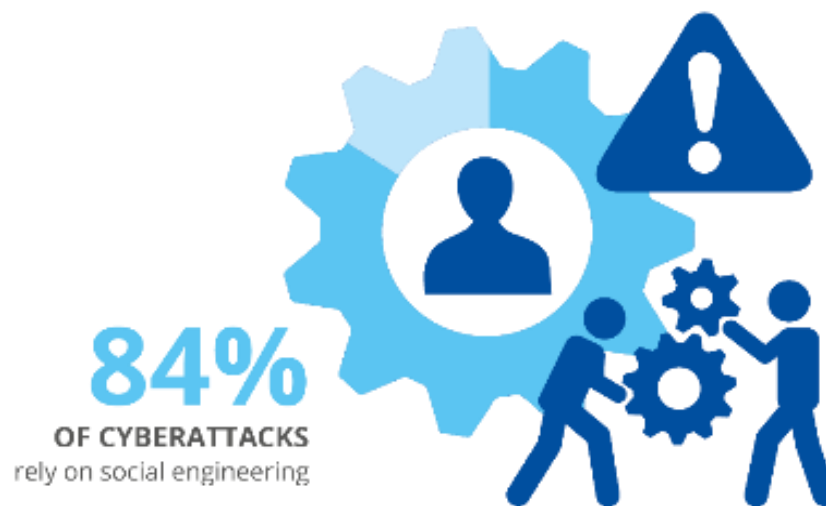
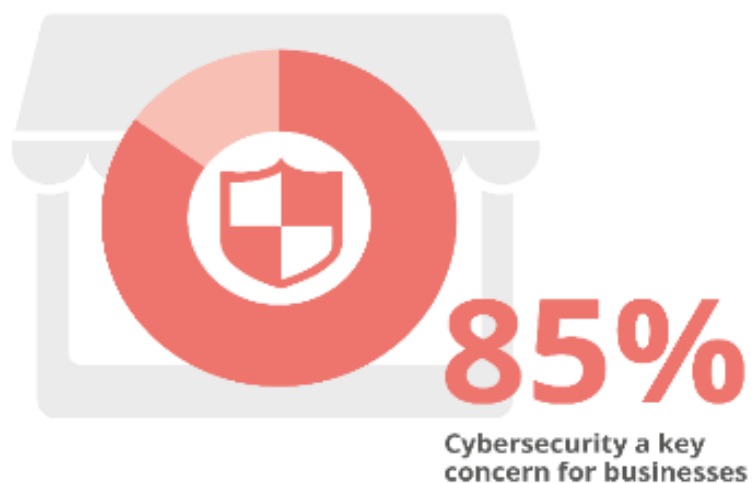
Of businesses in the EU are SMEs

93%

Of SMEs in the EU are micro.



# CYBERSECURITY CONCERNS



**41%**  
Phishing



**40%**  
Web based attack



**39%**  
General malware



**19%**  
Malicious insider



**12%**  
Denial of service



**11%**  
Social engineering



**7%**  
Compromised/  
stolen device



# TECHNOLOGY USAGE

Figure 8: Use of Cloud

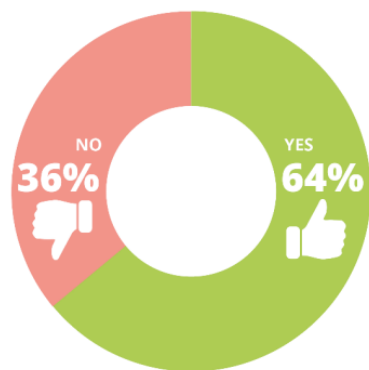
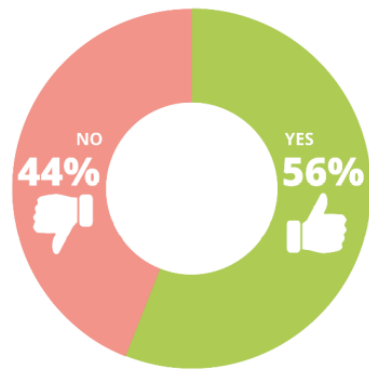


Figure 9: Use of Remote Access



LESS THAN  
**30%**  
OF THE PARTICIPANTS

- Removable media management
- ISMS
- Security Officer
- Incident response structure
- Business continuity and Disaster recovery plan
- Cyber/ Information

MORE THAN  
**70%**  
OF THE PARTICIPANTS

- Backup
- Antivirus
- Firewall
- Systematic updating of software

# CHALLENGES

- Low cybersecurity awareness of the personnel,
- Inadequate protection of critical and sensitive information,
- Lack of budget,
- Lack of ICT cybersecurity specialists,
- Lack of suitable cybersecurity guidelines specific to SMEs,
- Shadow IT, i.e. shift of ICT environment out of SME's control,
- Low management support.
- Compliance with CS legislation



# NIS DIRECTIVE IN A NUTSHELL – 3 PILLARS

## National capabilities

### National capabilities

- National CSIRT
- National authorities
- National cybersecurity strategy
- National cyber crisis management framework

## EU collaboration

### EU Collaboration

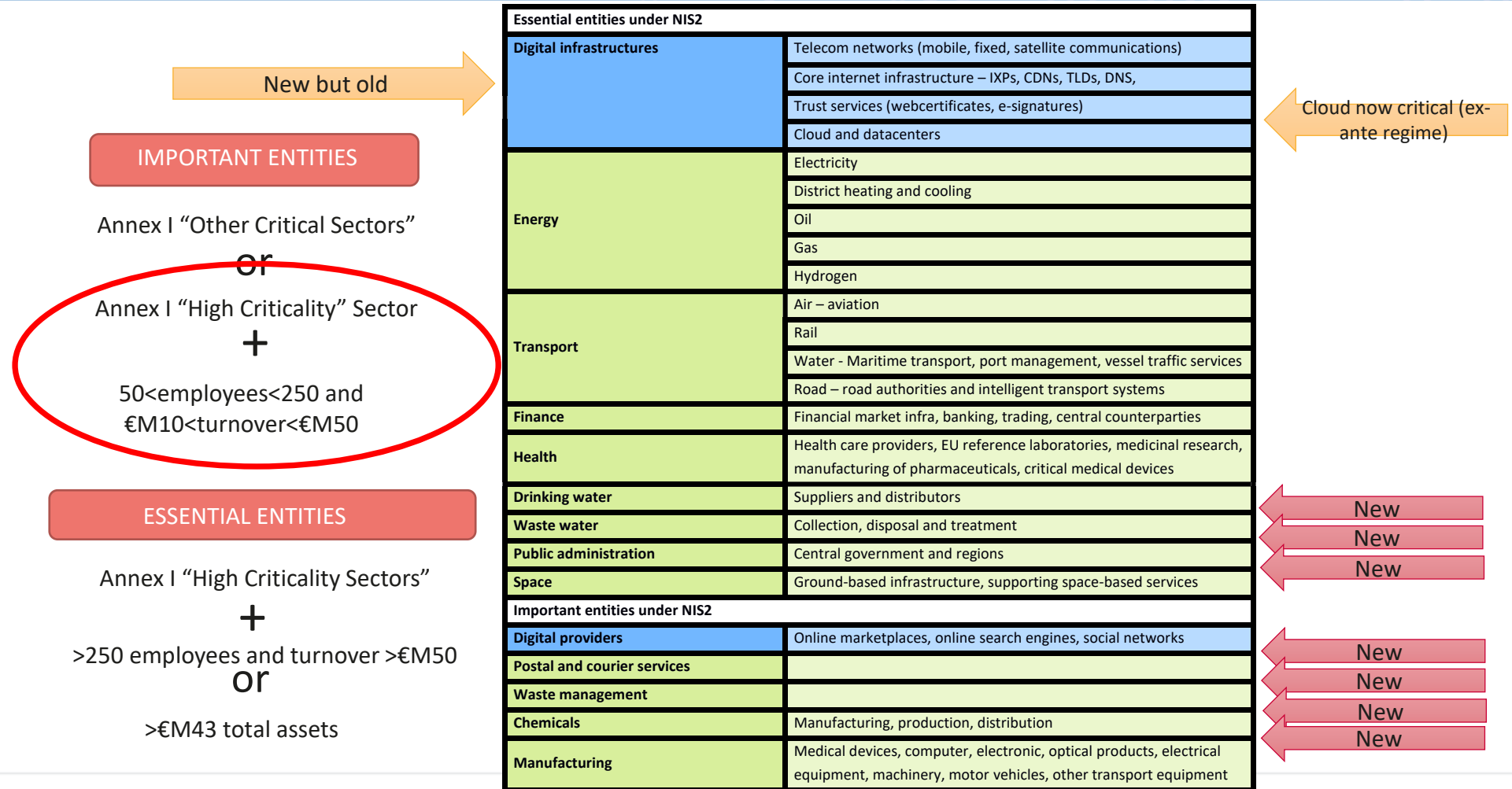
- NIS Cooperation group – strategic collaboration
- EU CSIRTs network - technical collaboration
- EU Cyclone – cyber crisis management coordination
- Coordinated supply chain risk assessments

## Supervision of critical sectors

### Supervision of critical sectors

- Security measures - risk-based
- Incident reporting - large incidents

# NIS2 DIRECTIVE – SECTORS

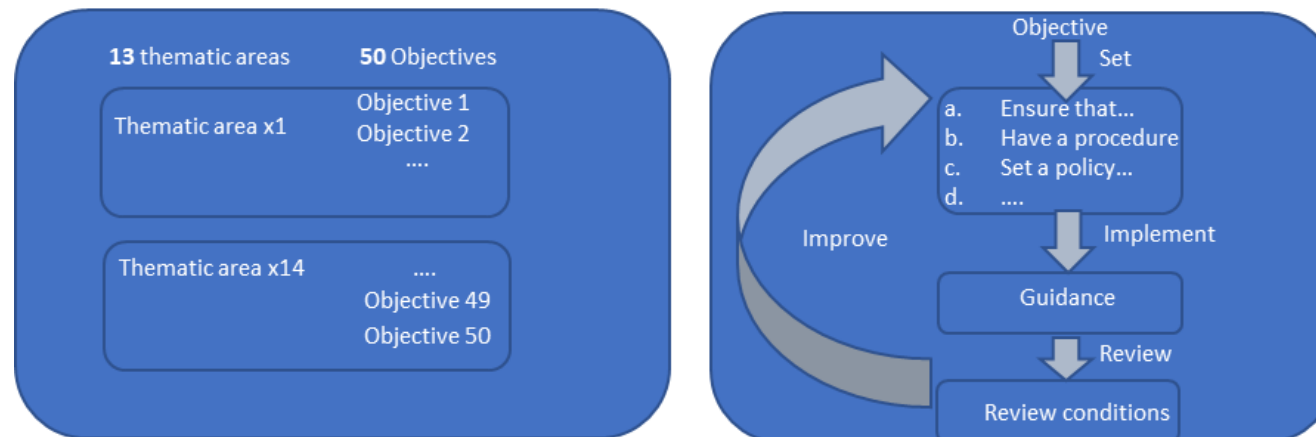


# NIS2 DIRECTIVE – SUPERVISION

	Essential Entities	Important Entities
Summary of Key Similarities and Differences	<p>Obligated to report significant cybersecurity incidents to national authorities.</p> <p>Regular audits and compliance checks ex ante and ex post</p> <p>Required to implement robust risk management measures and ensure high levels of cybersecurity resilience.</p>	<p>Obligated to report significant cybersecurity incidents to national authorities.</p> <p>Compliance checks and audits are conducted ex post only</p> <p>Required to implement appropriate risk management measures and ensure cybersecurity resilience.</p>

# NIS2 SECURITY MEASURES

- ENISA has developed a security framework
  - Developed with the Member States in the NIS Cooperation Group
  - Consulting with several sectorial groups (for instance telecoms)
  - Used by the Commission for the implementing acts
- Mapping to industry standards
  - NIST CSF Framework, ISO 27001/2, ETSI EN 319 401, IEC 62443 family



## Governance areas

1. Top management commitment & accountability
2. Network & information security policy
3. Risk management policy
4. Asset management
5. Human resources security
6. Basic cyber hygiene practices & Security training
7. Supply chain security
8. Access control
9. Security in network and information systems acquisition, development & maintenance
10. Cryptography
11. Incident handling
12. Business continuity & crisis management
13. Environmental and physical security

# INCIDENT REPORTING (ART. 23)

**2 elements that are both to be considered when it comes to defining incidents:**

- Event compromising:
  - Availability
  - Authenticity
  - Integrity
  - Confidentiality
- Event having impact on:
  - Stored, transmitted or processed data
  - Services offered by, or accessible via, network and information systems
  - An event is defined as an incident when it covers any combination of the elements above.

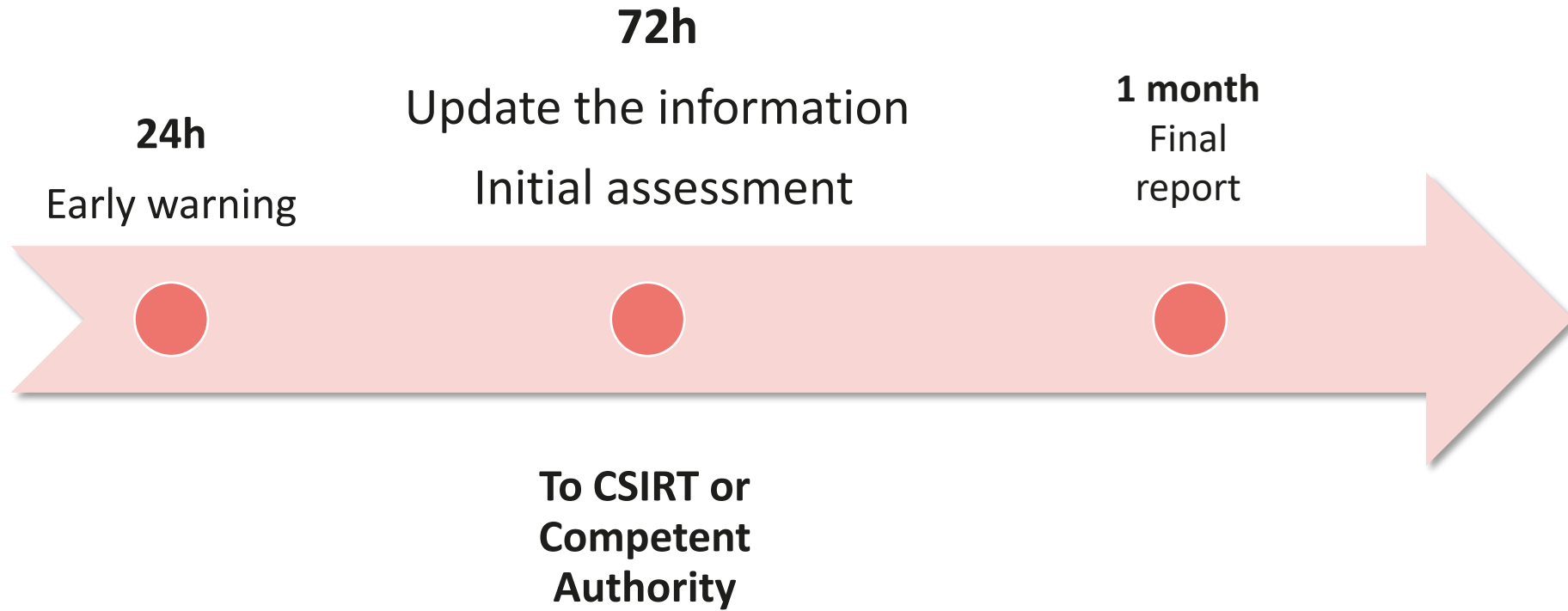
*An incident shall be considered to be significant if:*

***(a) it has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned;***

***(b) it has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage***

# INCIDENT REPORTING

## Notification of significant incidents



# SUPPORTING THE SMEs

**CYBERSECURITY FOR SMES**  
Challenges and Recommendations  
JUNE 2021

**Reports**

**Cybersecurity Maturity Assessment for Small and Medium Enterprises**

This tool helps Small and Medium-sized business enhance their cybersecurity maturity level and provide them with an adaptive progressive plan to handle cybersecurity risks.

**Tools**

**3 reasons to assess you company's cybersecurity maturity**

- Cybersecurity evaluation**  
Understand what is your cybersecurity maturity level and compare with similar businesses
- Personalised plan**  
Get a tailor-made improvement action plan adapted to the needs of your business
- Top security**  
Use our online secure tool to increase your cybersecurity level with our recommended action plan

**3 key areas to assess for your business**

- People**  
Assess whether your employees are prepared to face cyber threats
- Technology**  
Understand your technology and how to implement best cybersecurity practices
- Processes**  
Ensure that your organisation has the right processes in place to deal with cybersecurity risks

**Events**

**Κυβερνοασφάλεια για Μικρομεσαίες Επιχειρήσεις**

Συμβουλές, κατευθυντήριες γραμμές και εύχρηστα εργαλεία με στόχο την αύξηση της ασφάλειας στον κυβερνοχώρο για μικρούς & μεσαίους οργανισμούς

ENISA, Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια

**ΔΕΘ - Περίπτερο 10**  
**Δευτέρα 12 Σεπτεμβρίου 2022**  
**ΩΡΑ: 19.00-20.00**

**12 STEPS TO SECURING YOUR BUSINESS**

**Leaflets**

**CYBER 4.0 CYBERSECURITY COMPETENCE CENTER**

JOIN TO ALL NEWSLETTER

**Cybersecurity for SMEs - The EU scenario and the Italian perspective**

ENISA, ECCO

10 NOVEMBRE 2021

**Webinars**



**PUZZLE**

# ENISA ACTIONS

## Dedicated web tool



Cybersecurity doesn't necessarily have to be costly for SMEs to implement and maintain. There are several measures that can be implemented, without the company having to invest a large amount.

## Videos <https://tinyurl.com/2j7rmaj4>



A graphic for a podcast titled 'Ransomware campaigns targeting SMEs'. It features the ENISA logo and a list of participants and a moderator. The participants are: Anna Sarri (Cybersecurity Officer, EU Agency for Cybersecurity (ENISA)), Marijn Schuurblers (Head of Operations in Europe's Cybercrime Centre (EC3)), Brian Honan (CEO of BH Consulting and founder of the first Irish Computer Emergency Response Team (CERT)), and Ifigenia Lella (Cybersecurity Officer, EU Agency for Cybersecurity (ENISA)).

## Link to the podcast:

[https://www.youtube.com/watch?v=eSuBRO\\_rawU](https://www.youtube.com/watch?v=eSuBRO_rawU)

## Campaigns

An infographic titled 'ARE U SME FRIENDLY? In the shoes of an SME Director'. It contains several questions and answers related to cybersecurity for SMEs. The questions include: 'AM I ABLE TO COMPLY WITH OUR CUSTOMER'S CYBERSECURITY REQUIREMENTS?', 'HOME OFFICE IS THE NEW NORM FOR OUR BUSINESS. WHAT IMPACT ON OUR COMPANY'S SECURITY?', 'IS THE CURRENT CYBERSECURITY OFFERING SUITED FOR OUR COMPANY (IN ITS BUDGET)?', 'WHY SHALL I CARE FOR CYBERSECURITY SPACE (OUR SOURCES MANAGEMENT AND SUPPORT TO A THIRD PARTY)?', 'WHO CAN ACCESS OUR EMAILS, DOCUMENTS AND THE DIFFERENT COMPUTERS?', 'ARE THERE CYBERSECURITY RULES (AND REGULATIONS) THAT APPLY TO MY COMPANY?', 'HOW CAN I PROTECT OUR COMPANY FROM RANSOMWARE ATTACKS AND HOW TO ENSURE BUSINESS CONTINUITY SHALL WE GET INFECTED?', 'WHO CAN ATTACK OUR COMPANY? WHY WOULD A CYBERCRIMINAL GET INTERESTED IN OUR COMPANY?', 'SHALL I FEAR THE CLOUD MIGRATION AND MORE BROADLY OUR COMPANY'S DIGITAL TRANSFORMATION?'. At the bottom, it says 'Ask for our Cybersecurity guide for SMEs' and features a small image of a guide.

# HEALTHCARE SECTOR CAMPAIGN

## Cyber Health Week 2022

Welcome to the official page of the Cybersecurity Healthcare Week 2022!



**6 - 12 JUNE IS**  
 Cybersecurity Healthcare Week 2022  
 #CyberHealthWeek  
 #BoostYourCyberVitals

Join us for CyberHealthWeek  
 #BoostYourCyberVitals

### Ensure the continuity of clinical services – Information availability:

Make your healthcare organisation resilient to cyber incidents



In other words, make sure your clinical services are always available and patients have continuous access to them!

But, how?

By having a recovery plan that will help you:

- Respond swiftly
- Deliver services in abnormal circumstances
- Quickly get back to business as usual


A cyberlip a day keeps the hackers away!

#BoostYourCyberVitals

## Don't take the bite!

Immunise yourself from phishing infections!



### THE THREAT

Fraudulent attempts to steal user data are usually launched through e-mail, appearing to be sent from a reputable source, with the intention of persuading the user to open a malicious attachment or follow a fraudulent link.

### SOME PHISHING FACTS

**OVERALL OVERVIEW**  
 Number of phishing attacks has **TRIPLED** since last time early 2020. Phishing attacks hit an **ALL TIME HIGH** in 2021. Phishing accounts for **90%** of data breaches.

**HEALTHCARE SECTOR OVERVIEW**  
 Cyberattacks on healthcare sector saw a **71%** increase in 2021.

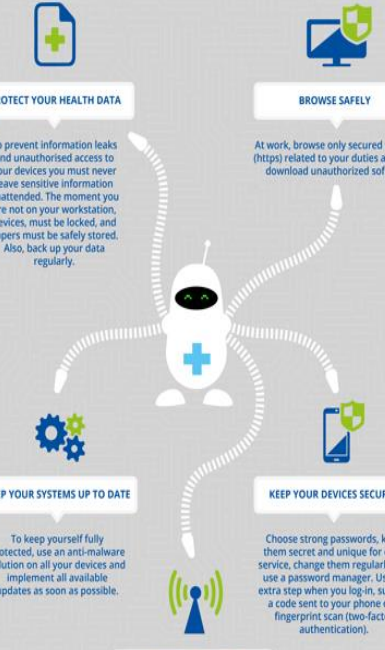
### PHISHING MADE IT TO THE RANKS

Phishing is found as the most common significant security incident and the most common initial point of compromise.

Good news is I have a prescription for phishing immunity.

Let's make some checks looking for a pathogen pattern!

Cyber-hygiene: a set of simple routines to minimise the risk of cyberthreats and information leaks.



#### PROTECT YOUR HEALTH DATA

To prevent information leaks and unauthorised access to your devices you must never leave sensitive information unattended. The moment you are not on your workstation, devices, must be locked, and papers must be safely stored. Also, back up your data regularly.

#### BROWSE SAFELY

At work, browse only secured websites (https) related to your duties and never download unauthorised software.

#### KEEP YOUR SYSTEMS UP TO DATE

To keep yourself fully protected, use an anti-malware solution on all your devices and implement all available updates as soon as possible.

#### KEEP YOUR DEVICES SECURED

Choose strong passwords, keep them secret and unique for each service, change them regularly and use a password manager. Use an extra step when you log-in, such as a code sent to your phone or a fingerprint scan (two-factor authentication).

#### CONNECT SAFELY OVER PUBLIC WI-FI

Avoid connecting to public Wi-Fi networks. If you have no choice, verify the network, keep your antivirus enabled, avoid entering credentials or performing financial transactions and ask the IT personnel for Access through VPN.

#BoostYourCyberVitals



# CYBERSECURITY MATURITY ASSESSMENT (CMA)

Home > Cybersecurity Maturity Assessment for Small and Medium Enterprises

## Cybersecurity Maturity Assessment for Small and Medium Enterprises



This tool helps Small and Medium-sized business enhance their cybersecurity maturity level and provide them with an adaptive progressive plan to handle cybersecurity risks.

[Start the assessment >>](#)

### 3 reasons to assess you company's cyber security maturity



#### Cybersecurity evaluation

Understand what is your cybersecurity maturity level and compare with similar businesses



#### Personalized plan

Get a tailored improvement action plan adapted to the needs of your business



#### Top security

Use our online secure tool to increase your cybersecurity level with our recommended action plan

### 3 key areas to assess for your business



#### People

Assess whether your employees are prepared to face cyber threats



#### Technology

Understand your technology and how to implement best cybersecurity practices




#### Processes

Ensure that your organisation has the right processes in place to deal with cybersecurity risks

# CMA - MODULES

An official website of the European Union How do you know? ▾



Search for resources, tools, publications and more 🔍 English (en)

TOPICS ▾ PUBLICATIONS TOOLS NEWS EVENTS ABOUT ▾ WORK WITH ENISA ▾ CONTACT

Home > Tools > Cybersecurity Maturity Assessment for Small and Medium Enterprises

## Cybersecurity Maturity Assessment for Small and Medium Enterprises

- Modules
- Business Profile
- Maturity Level
- Improvement action plan
- Benchmark
- Log out

### Self-Assessment Modules

Please follow our step-by-step approach to complete your assessment


- Business Profile**  
Complete or update your business profile
- Maturity Level**  
Answer questionnaire to assess your maturity level
- Improvement action plan**  
Get a tailored plan to increase your maturity level
- Benchmark**  
Get access to you benchmark and compare with other business of the same profile





# CMA - BENCHMARK

An official website of the European Union How do you know? ▾



enisa  
EUROPEAN UNION AGENCY FOR CYBERSECURITY

Search for resources, tools, publications and more 🔍 English (en)

TOPICS ▾ PUBLICATIONS TOOLS NEWS EVENTS ABOUT ▾ WORK WITH ENISA ▾ CONTACT

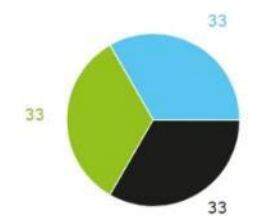
Home > Tools > Cybersecurity Maturity Assessment for Small and Medium Enterprises

## Cybersecurity Maturity Assessment for Small and Medium Enterprises

- Modules
- Business Profile
- Maturity Level
- Improvement action plan
- Benchmark
- Log out

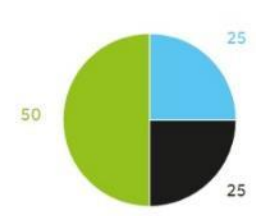
### Compare your business maturity level with similar companies within Europe

#### Companies with the same budget



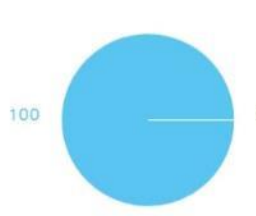
Maturity Level	Count
Foundation	33
Advanced	33
Expert	33

#### Companies with same size



Maturity Level	Count
Foundation	25
Advanced	50
Expert	25

#### Companies in the same country



Maturity Level	Count
Foundation	100
Advanced	0
Expert	0

# THE WAY FORWARD

## NEXT STEPS

- Measure the maturity of SMEs and analyze further challenges they face
- NIS2 awareness campaigns

**Sectors and entities under NIS2**

The NIS 2 directive identifies several sectors that are considered essential for the functioning of the economy and society. These sectors are classified into two main categories: High Criticality Sectors and Other Critical Sectors.

High Criticality Sectors								
Energy	Transport	Banking	Financial Market Infrastructures	Health	Drinking Water Supply and Distribution	Digital Infrastructure	Public Administration	Space

**Other Critical Sectors**

Postal and Courier Services	Waste Management	Chemical Industry	Food Production and Distribution	Manufacturing of Critical Products	Digital Providers

**Sectors and entities under NIS2**

The NIS 2 directive identifies several sectors that are considered essential for the functioning of the economy and society. These sectors are classified into two main categories: High Criticality Sectors and Other Critical Sectors.

Entities within the identified sectors are categorized into two main groups:

Entities	Essential Entities	Important Entities
	Entities from the High Criticality Sectors having either >250 employees and turnover >€M50 or >€M43 total assets	Entities from Other Critical Sectors or entities from High Criticality Sectors having 50 < employees < 250 and €M10 < turnover < €M50

Member states can identify additional entities as essential, addressing specific national needs and contexts, ensuring that all critical infrastructure and services are adequately protected.

Summary of Key Similarities and Differences	Essential Entities	Important Entities
	<ul style="list-style-type: none"> <li>Obligated to report significant cybersecurity incidents to national authorities.</li> <li>Regular audits and compliance checks ex ante and ex post</li> <li>Required to implement robust risk management measures and ensure high levels of cybersecurity resilience.</li> </ul>	<ul style="list-style-type: none"> <li>Obligated to report significant cybersecurity incidents to national authorities.</li> <li>Compliance checks and audits are conducted ex post only</li> <li>Required to implement appropriate risk management measures and ensure cybersecurity resilience.</li> </ul>

# THE WAY FORWARD

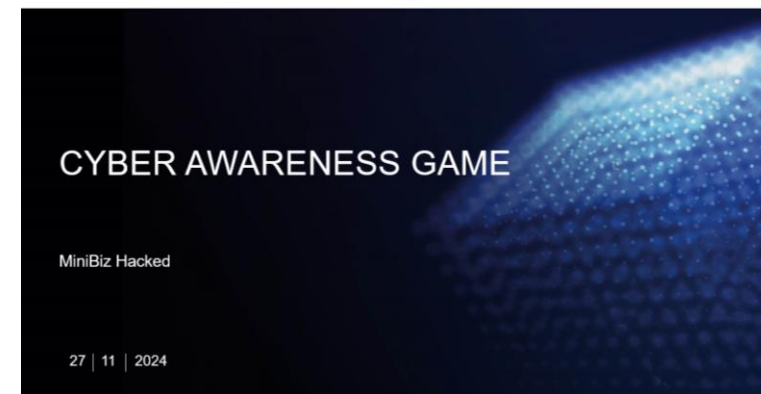
➤ AR-in-a-Box for SMEs!

NEXT  
STEPS

AR-IN-A-BOX  
SMEs Edition



AR-IN-A-BOX



BE PREPARED REDUCE THE IMPACT

*for SMEs*



# THANK YOU FOR YOUR ATTENTION

Agamemnonos 14, Chalandri 15231  
Attiki, Greece



 [info@enisa.europa.eu](mailto:info@enisa.europa.eu)

 [www.enisa.europa.eu](http://www.enisa.europa.eu)

