EUROPEAN UNION AGENCY
FOR CYBERSECURITY

# CYBERSECURITY AWARENESS: INSIGHTS FROM ENISA

# CYBERSECURITY FOR SMEs

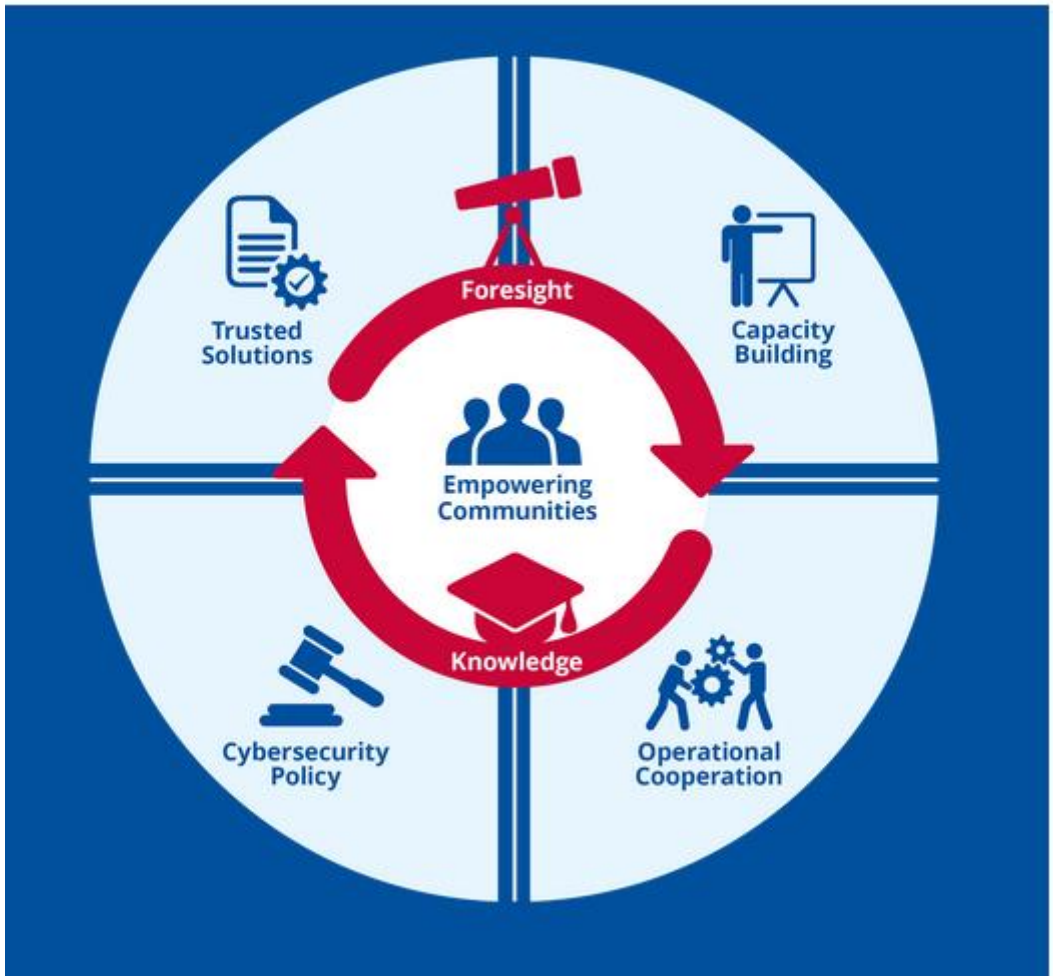

**Anna Sarri**

**Cybersecurity Officer**

**Capacity Building Unit**


**7 December 2021**

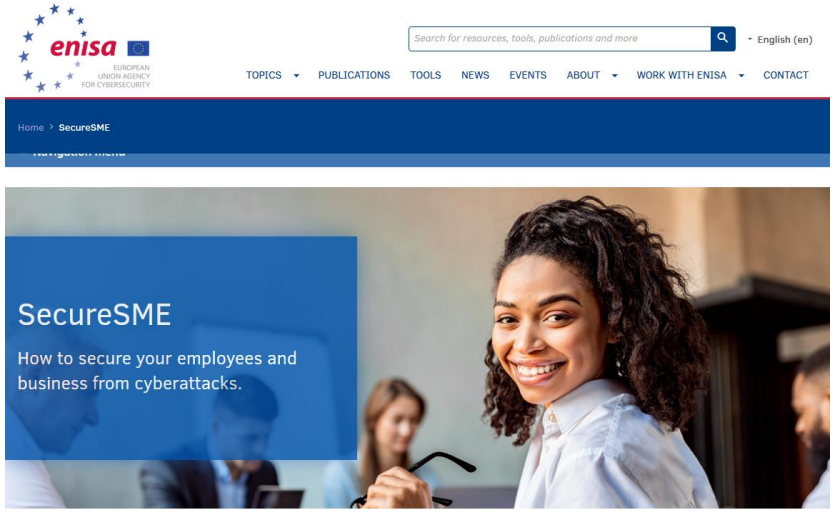
# ABOUT ENISA


Trusted Solutions
Foresight
Capacity Building
Empowering Communities
Knowledge
Cybersecurity Policy
Operational Cooperation

# SUPPORTING SMES

1


3




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.

2


4


*Awareness campaign at FIC*

# OVERALL SCOPE

THE EU CYBERSECURITY AGENCY

*In the situation of the COVID19 pandemic, ENISA analysed the ability of EU SMEs to cope with cybersecurity issues in a crisis by identifying cybersecurity challenges and determining advice and good practices, as well as proposals for actions towards Member States to support SMEs improve their cybersecurity posture.*

# METHODOLOGY

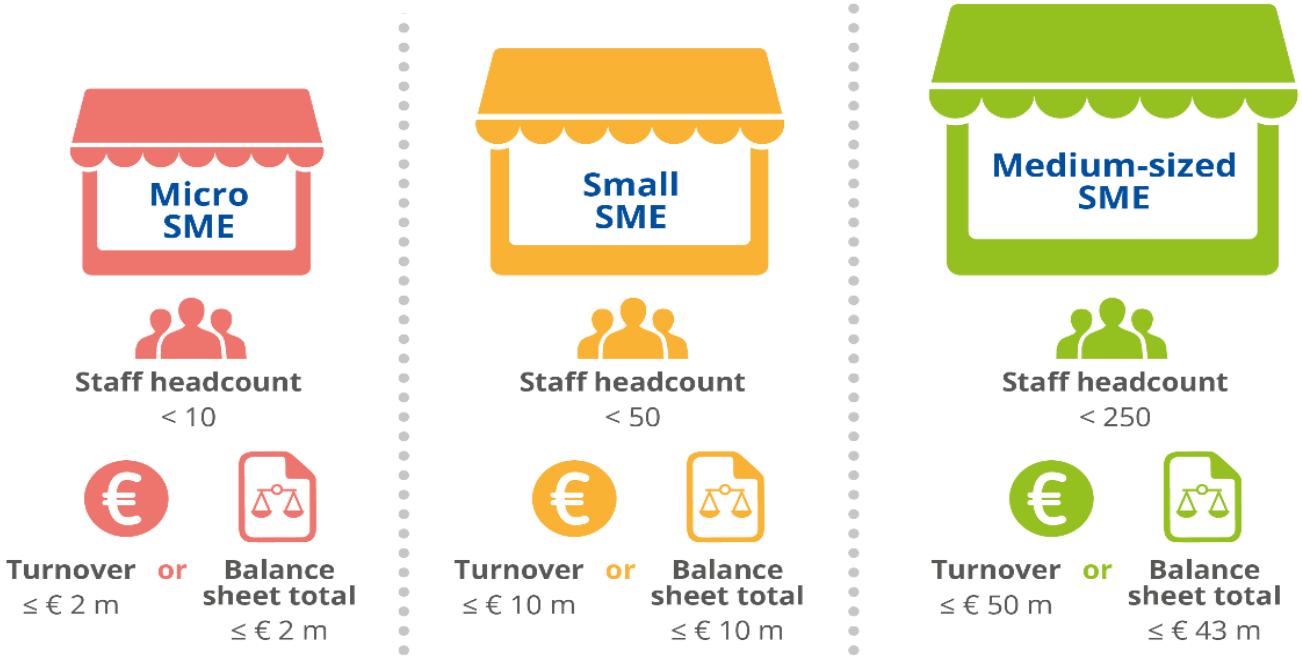
# BACKGROUND

**99%**

**of all businesses in Europe are SMEs.**

**93%**

**of all enterprises in Europe are micro SMEs.**

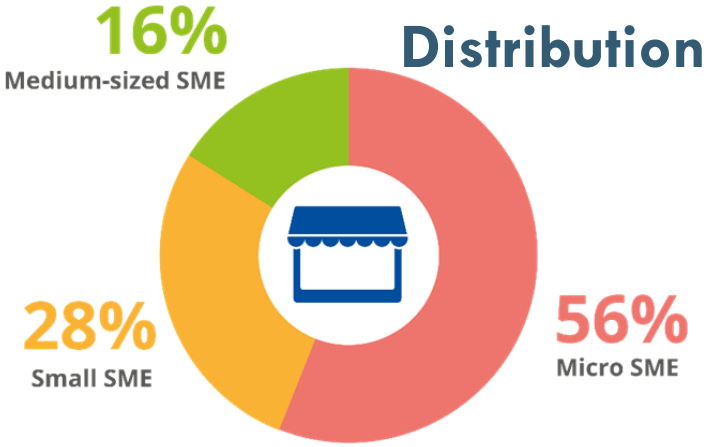


# KEY FINDINGS

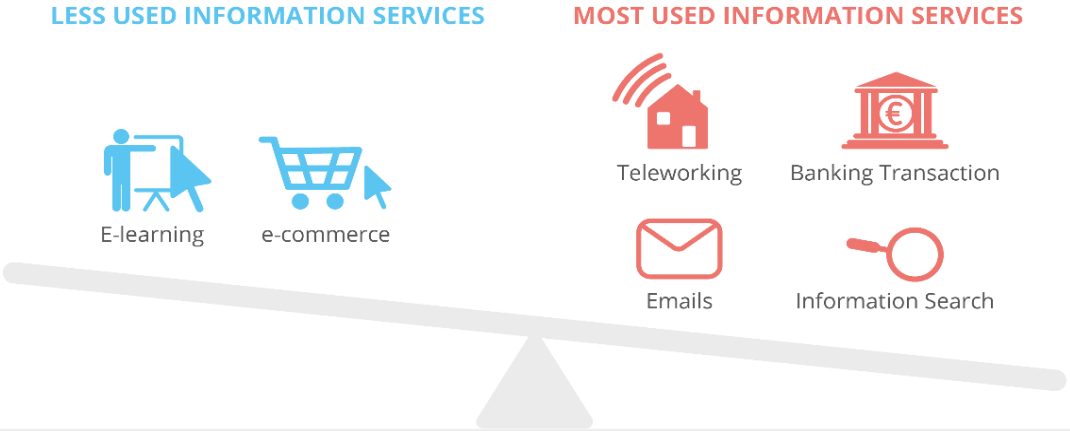
## Study Participants

- ~250 SMEs
- 25 EU MS

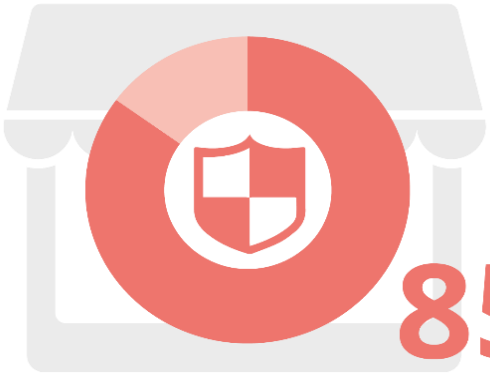
## Distribution




## Increased dependency on ICT



# KEY FINDINGS



**85%**

**Cybersecurity a key concern for businesses**

**84%**

**OF CYBERATTACKS**
rely on social engineering

**41%** Phising

**40%** Web based attack

**39%** General malware

**19%** Malicious insider

**12%** Denial of service

**11%** Social engineering

**7%** Compromised/ stolen device

# KEY FINDINGS

**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

# USE CASE SCENARIOS & LESSONS LEARNT 1/3

## RANSOMWARE ATTACK

- Company Type : IT Software Service Provider
- Company Size : < 50 employees
- Breach Type : Ransomware attack

## LESSONS LEARNT

- **Backups are an effective method to recover from a ransomware attack**
- **Strong password policy & employee awareness**
- **If using RDP for remote access ensure it is secured**

# USE CASE SCENARIOS & LESSONS LEARNT 2/3

## STOLEN LAPTOP

- Company Type : Legal Firm
- Company Size : <25 employees
- Breach Type : Laptop stolen containing sensitive client data

## LESSONS LEARNT

- **Need to know principle for accessing sensitive data**
- **Ensure all portable devices are encrypted**
- **Provide security awareness to staff on the risks of portable devices and how to protect them**

# USE CASE SCENARIOS & LESSONS LEARNT 3/3

## CEO FRAUD

- Company Type : Technology Company
- Company Size : <75 employees
- Breach Type : CEO Fraud

## LESSONS LEARNT

- **Ensure all staff, especially those in privileged role such as finance, follow written processes and procedures.**
- **Ensure management will not discipline staff for when they do follow proper processes and procedures**
- **Provide company systems for staff to communicate securely**

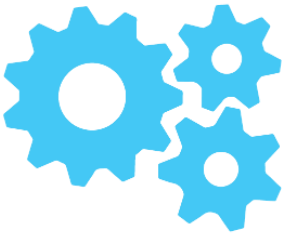
# CHALLENGES

- 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 work in ICT environment out of SME's control,
- low management support.

# RECOMMENDATIONS FOR SMES

**People**

- Responsibility
- Employee buy-in
- Employee awareness
- Cybersecurity Training
- Cybersecurity Policies
- Third Party Management



**Process**

- Cybersecurity Audits
- Incident Planning & Response
- Passwords
- Software Patches
- Data Protection

**Technology**

- Network Security
- Anti-Virus
- Email and Web Protection
- Encryption
- Security Monitoring
- Physical Security
- Secure Backups

# CHECKLISTS

| Check Item | Description | Answer |
|---|---|---|
| **Responsibility** | Does a director, or equivalent, have responsibility for cybersecurity? | |
| **Employee Buy-in** | Have all members of staff given written acknowledgement that they have read, understood and accepted the information security policy? | |
| **Employee awareness** | Do all users on your computer systems receive regular training on their security responsibilities on how to identify and deal with various security threats? Ensure that staff are aware of, and can verify, all contact points and communication channels | |
| **Cybersecurity Training** | Do staff members with specific security responsibilities receive proper and regular training to support their role? | |
| **Cybersecurity Policies** | Have you a documented security policy, with associated operating procedures, signed off and fully supported by senior management? | |
| **Third Party Management** | Does senior management authorise third party access to confidential and/or commercially sensitive information pending completion of appropriate confidentiality forms? | |

# EU AND NATIONAL LEVEL RECOMMENDATIONS

Promote Cybersecurity

Provide Targeted Guidelines

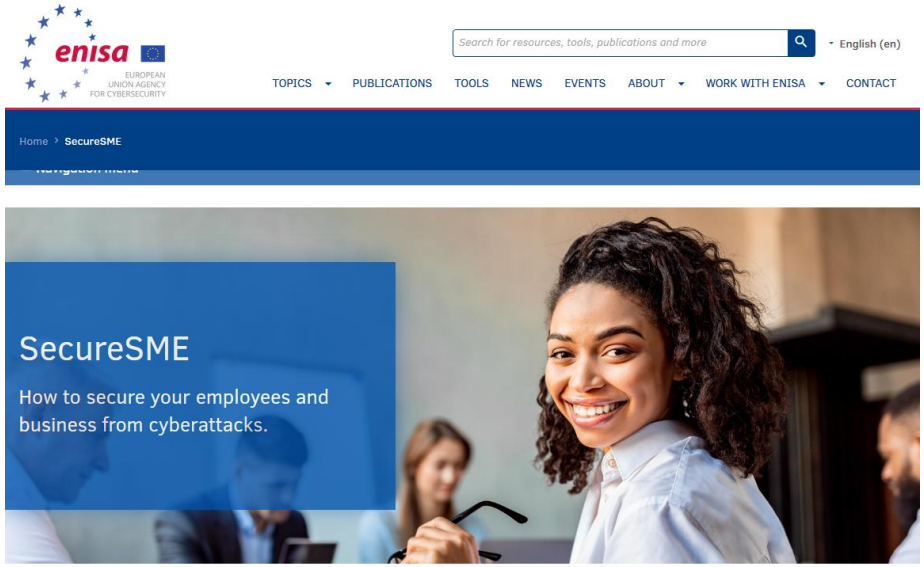
Create SME Focused Standards

Bolster Use of Risk Management Frameworks

Make Cybersecurity Affordable

Promote the creation of ISACs

# TOOLS




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.

**enisa.europa.eu/securesme**


**enisa.europa.eu/publications/cybersecurity-guide-for-smes**

# NEXT YEAR'S WORK

**Scope: Support SMEs to understand their cybersecurity posture towards risks and threats and help them improve.**

**Objective: Development of an online self-assessment to measure SMEs maturity and provide instructions for improvement.**

**+ Awareness campaign**

# THANK YOU FOR YOUR ATTENTION

**European Union Agency for Cybersecurity**
Agamemnonos 14, Chalandri 152 31
Attiki, Greece

+30 28 14 40 9711

info@enisa.europa.eu

www.enisa.europa.eu