



EUROPEAN UNION AGENCY  
FOR CYBERSECURITY

# CYBERSECURITY IN HEALTH: THREATS, CHALLENGES AND ENISA'S CONTRIBUTION

Maria Papaphilippou  
Cybersecurity Officer

EHFCN/AIM joint event

12 | 12 | 2024

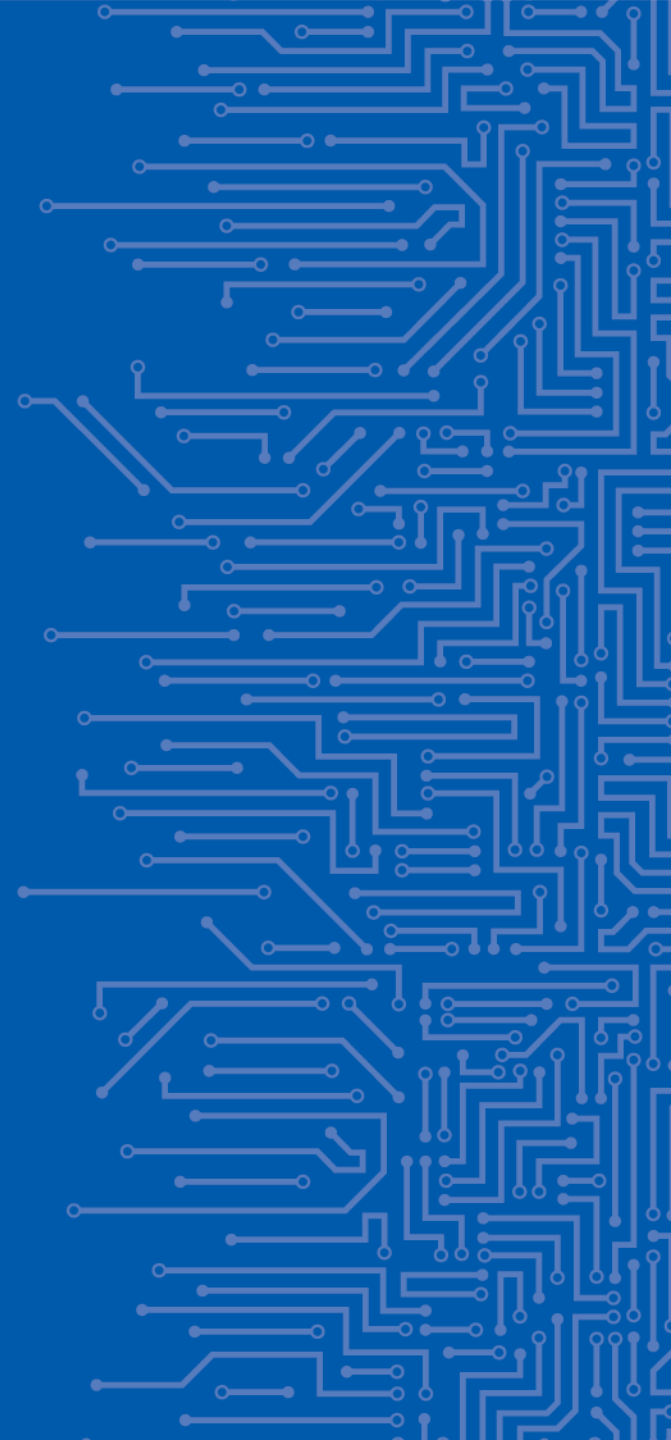


# AGENDA

1. Cybersecurity threat landscape for the health sector
2. ENISA's contribution in the health sector

1

# CYBERSECURITY THREAT LANDSCAPE FOR THE HEALTH SECTOR





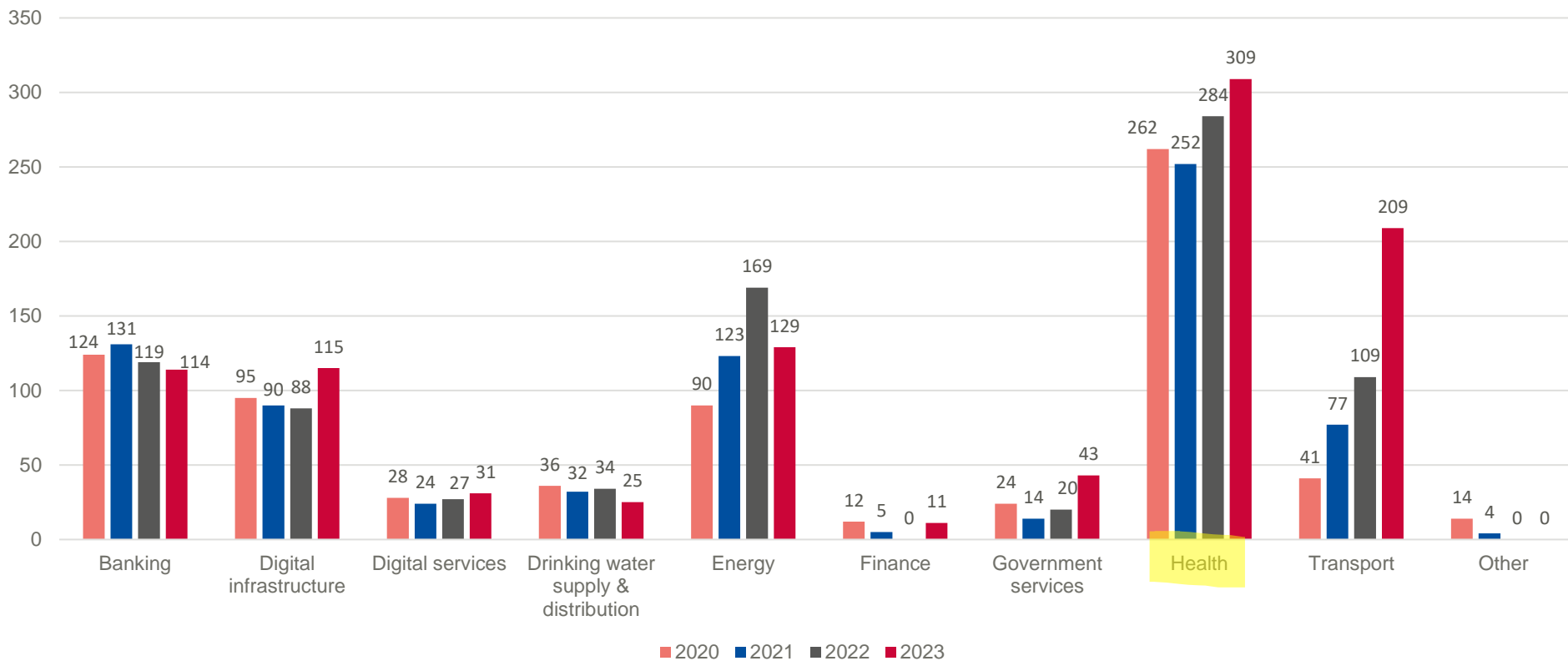
# CYBERESECURITY CHALLENGES IN HEALTH

- Ransomware attacks
- Increase in data breaches
- Supply chain attacks
- Low cybersecurity maturity
- Lack of security awareness
- Legacy systems
- Shortage in cybersecurity skills

# NIS INCIDENT REPORTING



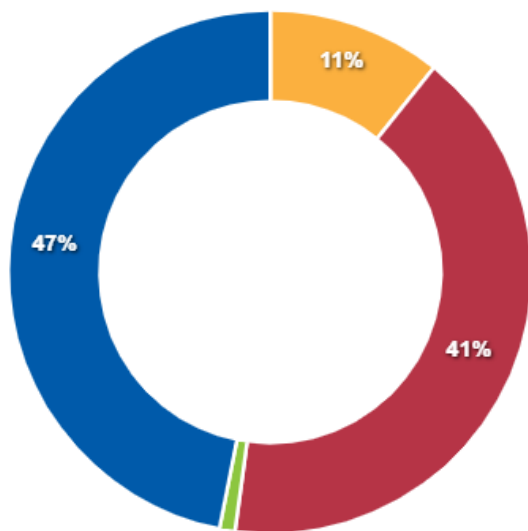
## Number of incidents per sector per year



# NIS INCIDENT REPORTING (2)

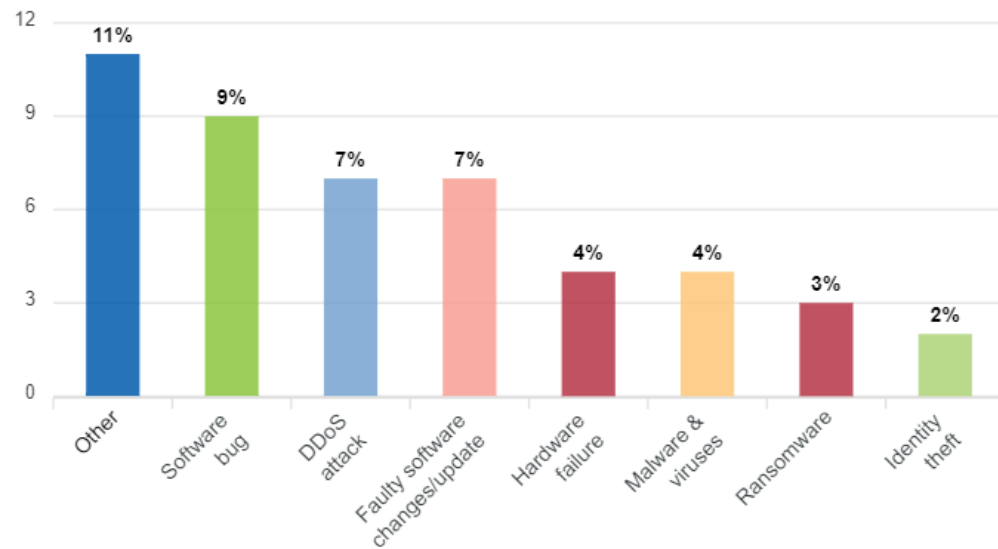


## Nature of the incident (%)



● Human errors: 11% ● Malicious actions: 41% ● Natural phenomena: 1%  
● System failures: 47%

## Technical causes (%)



# ENISA THREAT LANDSCAPE (ETL): HEALTH SECTOR

- **Data:**

- Jan 2021 - Mar 2023
- open source information

- **Scope:**

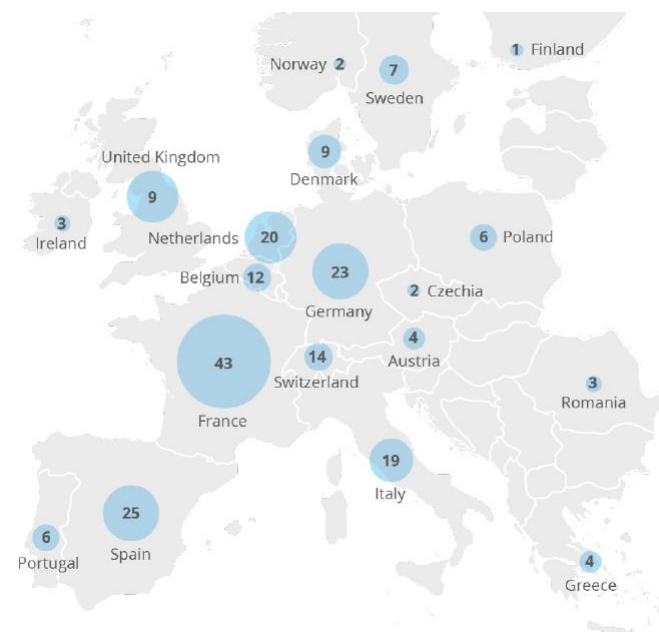
- EU
- Entities under NIS

- **Sample:**

- 215 incidents in the EU

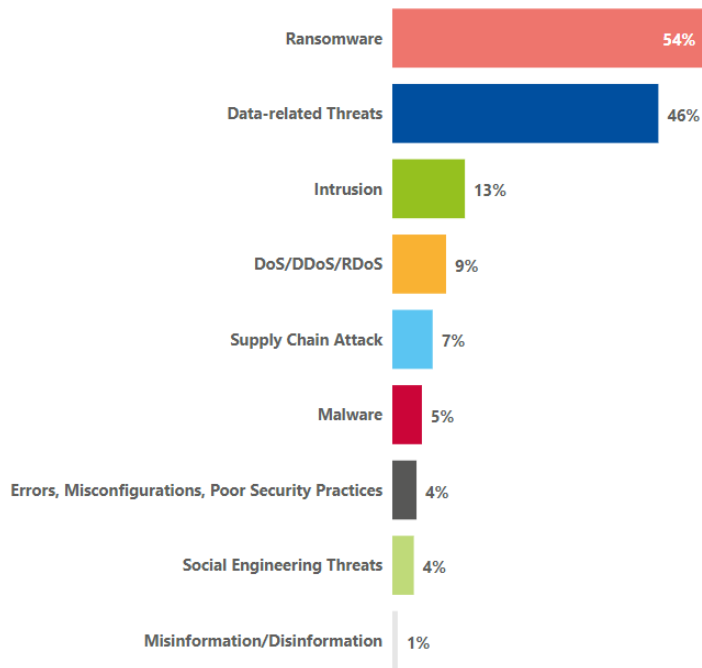
- **Analysis:**

- Observed activity (incidents)
- Prime threats
- Actors and motivation
- Targets
- Impact type
- Affected countries
- Trends

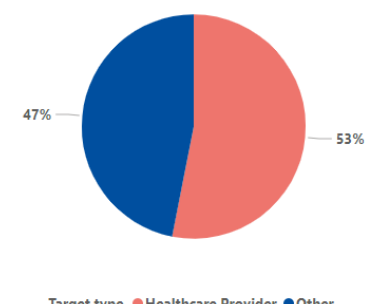
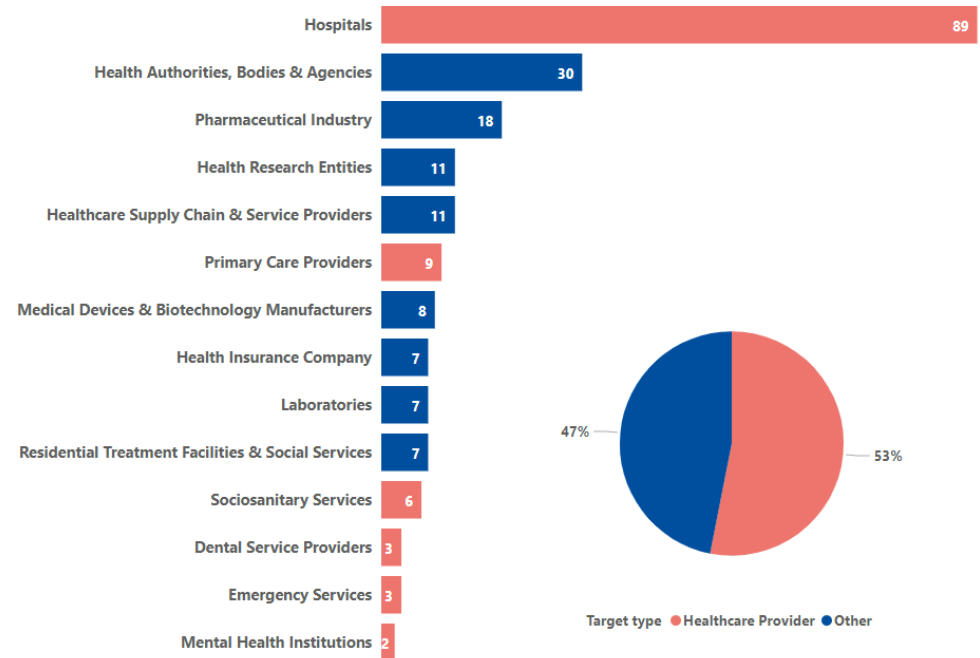


# ETL HEALTH SECTOR: THREATS AND ENTITIES AFFECTED

Threats in health sector (Jan 2021 - Mar 2023)



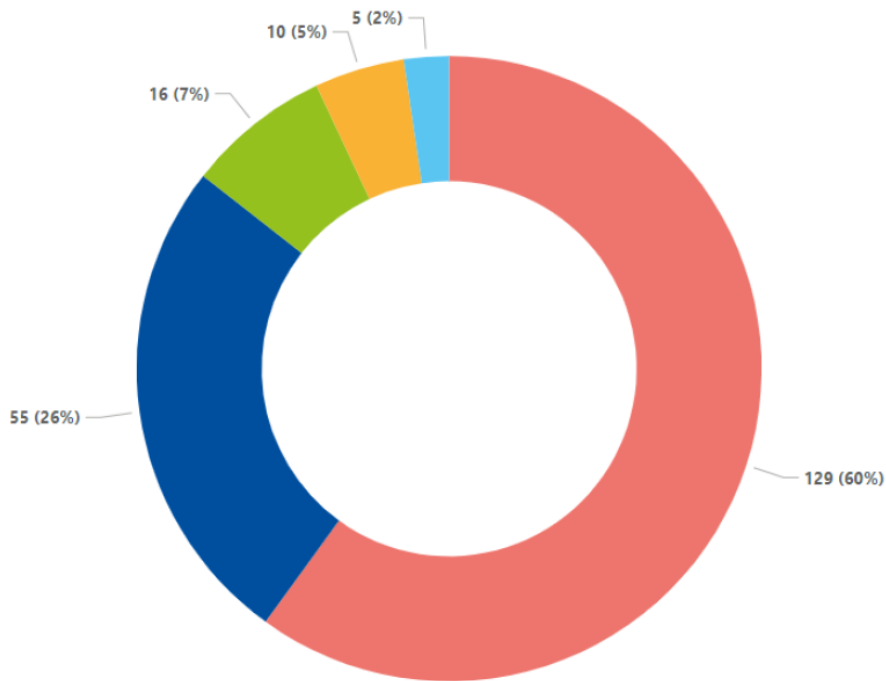
Number of incidents per entity type (targets)





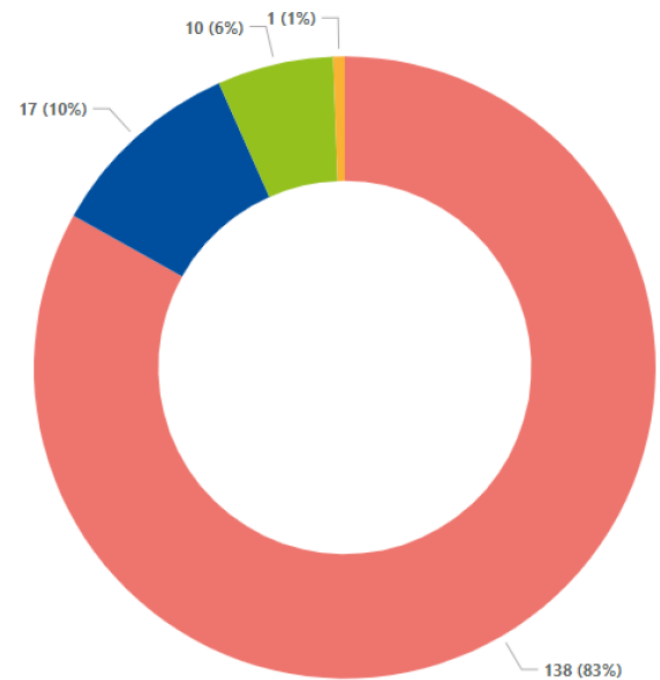
# ETL HEALTH SECTOR: THREAT ACTORS

## Actor types



Actors ● Cybercriminal ● Unknown ● Hactivist ● Insider (non malicious) ● Insider

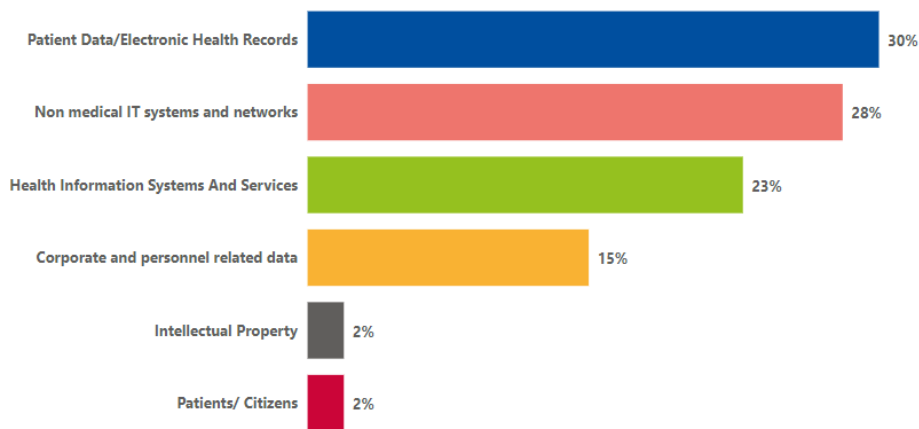
## Motivation



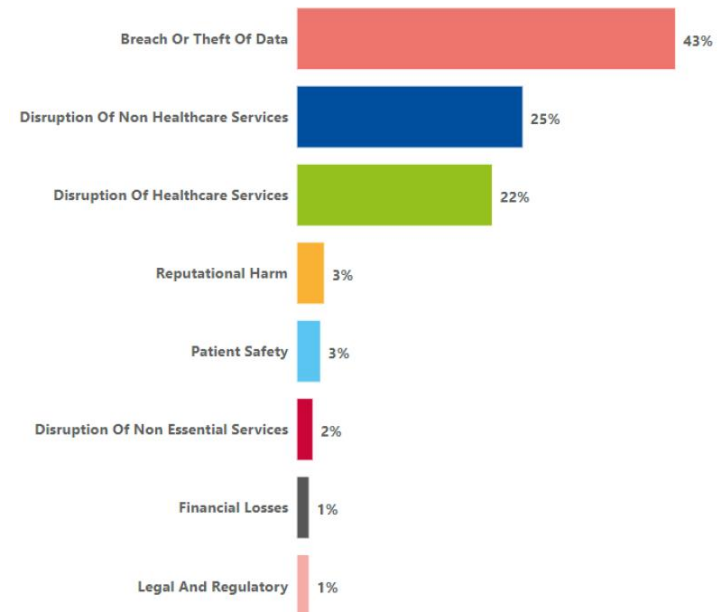
Motivation ● Financial Gain ● Ideological ● Other ● Espionage

# ETL HEALTH SECTOR: IMPACT

## Affected assets

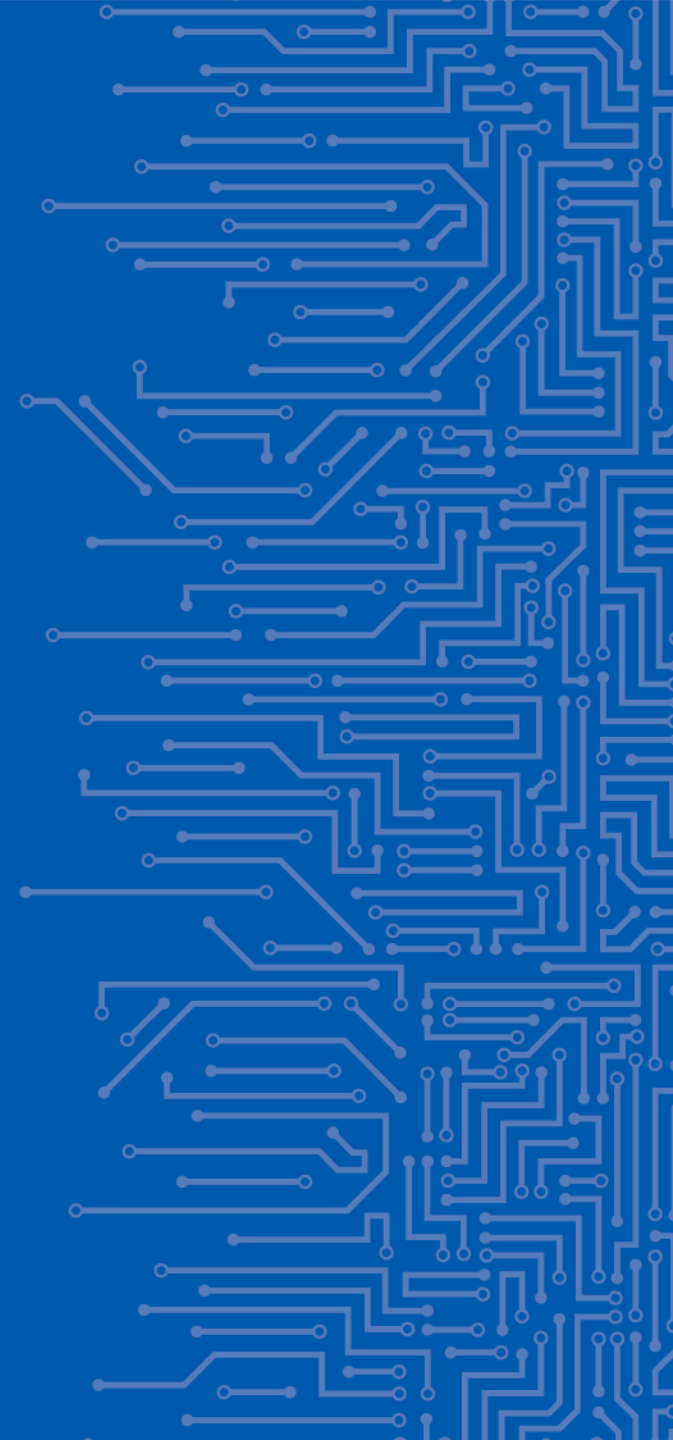


## Consequences



2

# ENISA'S CONTRIBUTION IN THE HEALTH SECTOR



# 2022 NIS INVESTMENTS REPORT

## Deep dive in health:

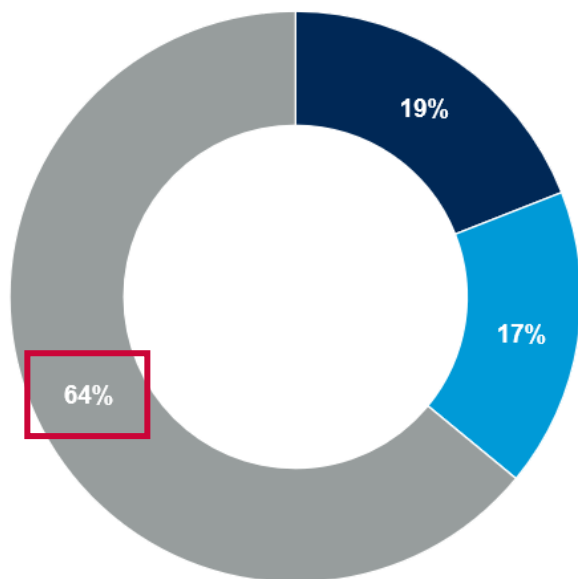
- 1080 OES/DSP
- 189 health OES
- 27 EU MS

## Additional questions on:

- medical devices
- cloud
- awareness

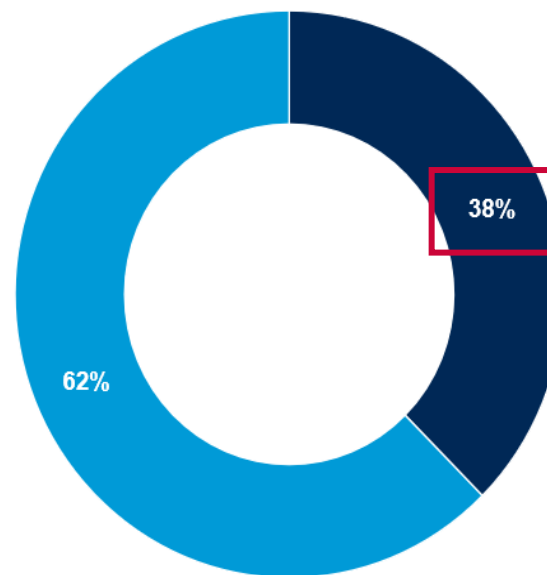


# MEDICAL DEVICE SECURITY



Connected medical devices in health

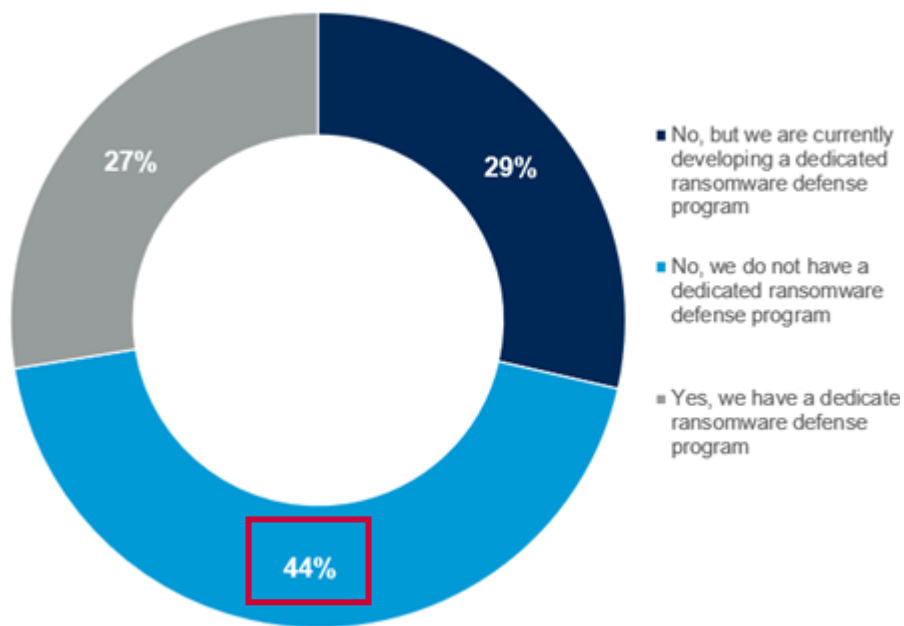
- No, but we are planning to deploy connected medical devices in 2022
- No, we are not planning to deploy connected medical devices in the short term
- Yes, we are already using connected medical devices



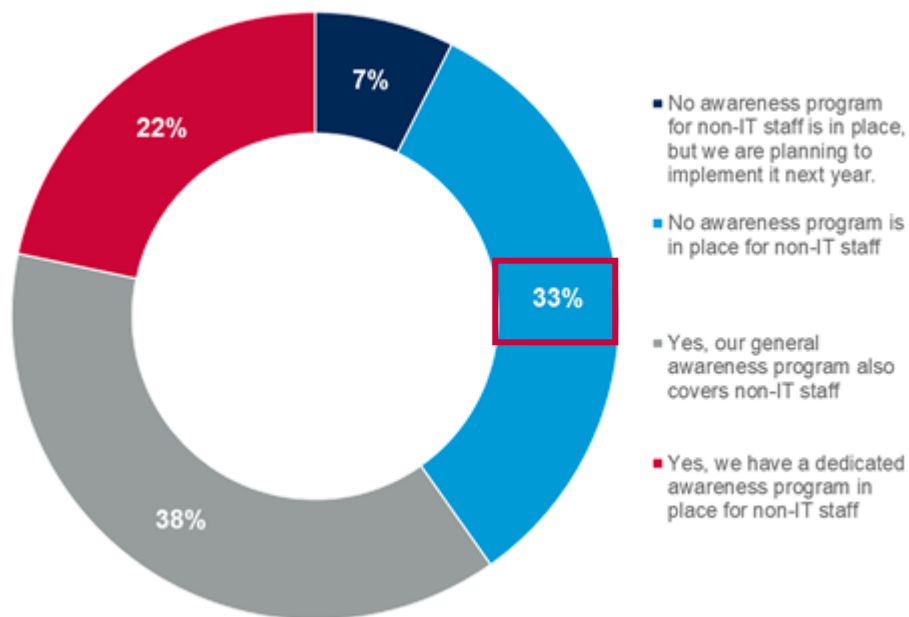
Security solutions for medical devices

- No, we do not have deployed any security solutions for medical devices
- Yes, we have deployed security solutions specific for medical devices

# PROTECTION AGAINST RANSOMWARE



Ransomware defense programs



Awareness raising for non-IT staff

# ENGINEERING PERSONAL DATA SHARING

- Engineering for privacy preserving data sharing
- Use cases in health
- Challenges and solutions

<https://www.enisa.europa.eu/publications/engineering-personal-data-sharing>



# OTHER ENISA REPORTS

November 2016



February 2020



January 2021





# ANNUAL EHEALTH SECURITY CONFERENCE

9<sup>th</sup> ENISA eHealth  
Security Conference

Empowering  
healthcare  
through  
cybersecurity

November 6th 2024 | Budapest



<https://www.enisa.europa.eu/events/9th-enisa-ehealth-security-conference>



- Chaired by Z-CERT (NL)
- Membership free of charge, travel and accommodation expenses by members
- Targeting healthcare providers and CERTs/CSIRTs
- Secretary: **EH-ISAC@Z-CERT.NL**

# CYBER EUROPE 2022



- Every 2 years
- Focus on one sector
- Series of simulated cybersecurity incidents
- Escalation to an EU level crisis
- Findings in the after action report

<https://www.enisa.europa.eu/news/enisa-news/cyber-europe-2022-testing-the-resilience-of-the-european-healthcare-sector>  
<https://www.enisa.europa.eu/publications/cyber-europe-2022-after-action-report>

# AWARENESS RAISING CAMPAIGN FOR HEALTH

## Cyber Health Week 2022

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



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 critical services are always available and patients have continuous access to them

By having a recovery plan that will help you:

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

A cyber day keeps the hackers away!

#BoostYourCyberVitals

### Don't take the bite!

Immunise yourself from phishing infections!

**THE THREAT**

A fraudulent attempt to steal user data and account credentials 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 2019 from early 2020. Phishing attacks hit on **ALL** 28 EU member states in 2021. Phishing accounts for **90%** of data breaches.

**HEALTHCARE SECTOR OVERVIEW**

Cyberattacks on healthcare sector saw a 77% 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 there's a prescription for phishing immunity.

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

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

<https://www.enisa.europa.eu/topics/cybersecurity-education/awareness-campaigns/boostyourcybervitals>

# AR-IN-A-BOX

A DIY guide for designing a custom cyber-awareness program



<https://www.enisa.europa.eu/topics/cybersecurity-education/awareness-raising-in-a-box>

# KEY TAKEAWAYS

- Cybersecurity threat landscape influenced by unstable **geopolitics, disinformation and sophistication**.
- The health sector is **critical** and must be protected.
- **Cybersecurity investments** to ensure resilience of critical EU infrastructure.
- **Awareness at board level** will improve maturity and drive cybersecurity investments.
- **Staff awareness/training** is key, especially for medical / clinical staff.
- Several EU regulatory developments requiring **cooperation and support** by Member States and private sector.
- **Information sharing** and increased **cooperation** is crucial.

# THANK YOU FOR YOUR ATTENTION

**European Union Agency for Cybersecurity**

Agamemnonos 14, Chalandri 15231

Attiki, Greece

 +30 28 14 40 9711

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

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

