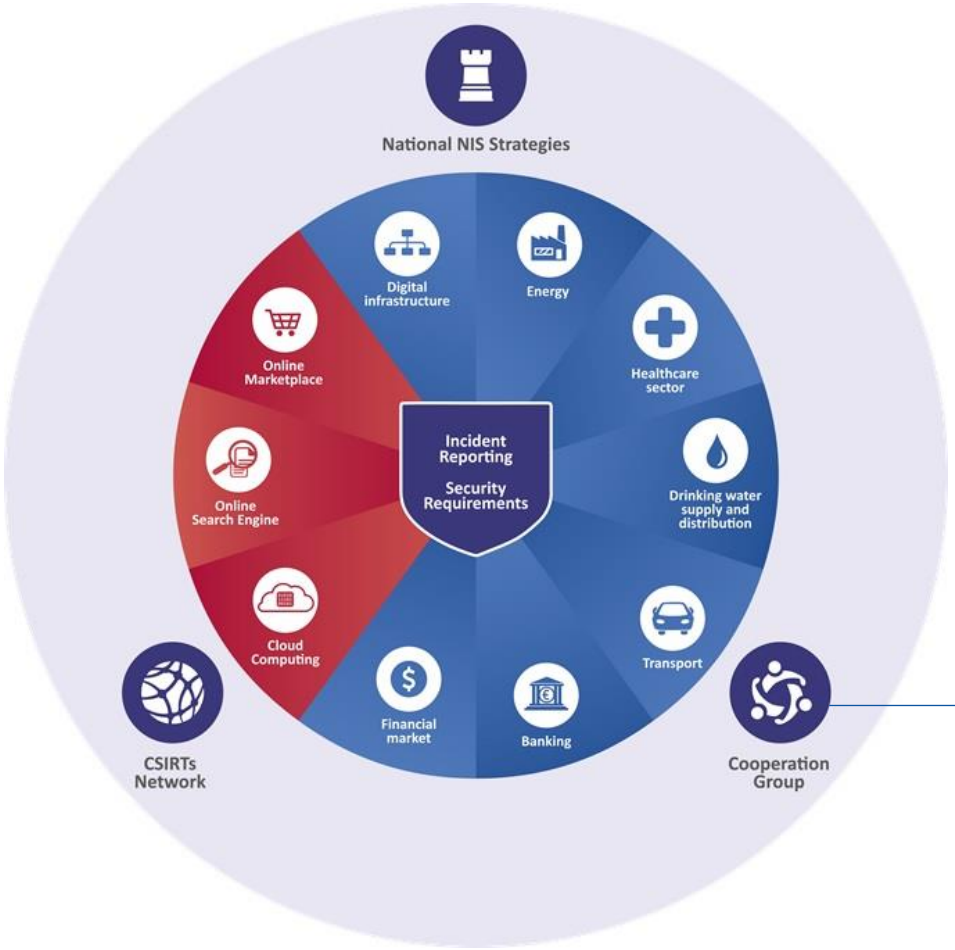
EUROPEAN UNION AGENCY
FOR CYBERSECURITY

EU HEALTH SECTOR: A EUROPEAN PERSPECTIVE

19 | 11 | 2024

THE NIS DIRECTIVE



- First EU law to introduce baseline cybersecurity requirements
- NIS2 into force in January 2023
- 21 months for national transposition

Work Stream on Health (led by PT, DK, RO, HU)

MEDICAL DEVICES REGULATION

- Aim: ensure that medical devices are safe and effective, and patients are protected from harm.
- Medical software could be considered as medical devices.
- IT Security requirements pre-market and post-market.
- Cybersecurity vulnerabilities and incident reporting for medical devices.

OTHER REGULATORY REQUIREMENTS

European Commission

Medical Devices Regulation

EU MDR

EU Cyber Resilience Act

For safer & more secure digital products

EU AI Act

Proposal for a

Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts

2021/0106 (COD)

European Commission

European Commission

EUROPEAN HEALTH DATA SPACE

#EUDigitalHealth

APRIL 2024

EU HEALTH ACTION PLAN

- Commission President announced a EU Health Action Plan
- Cybersecurity of hospitals and healthcare providers.
- Led by the Commission, supported by ENISA.
- Stakeholder groups are being consulted to gather ideas.

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ENISA THREAT LANDSCAPE: HEALTH SECTOR

19 | 11 | 2024

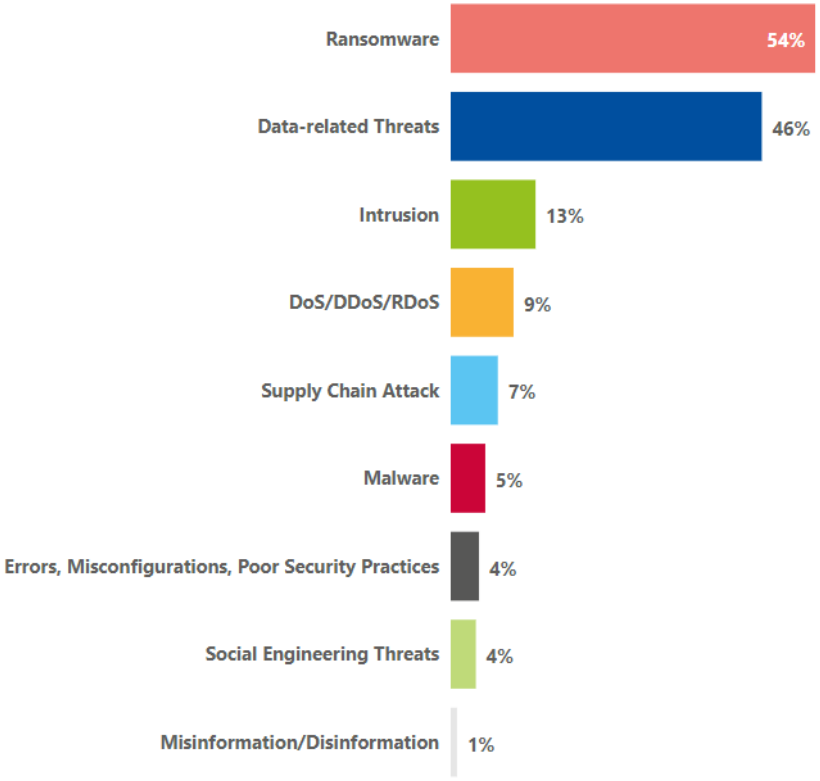
ENISA THREAT LANDSCAPE (ETL): HEALTH SECTOR

- **Objective:** bring insights into cyber threats targeting the European health sector.
- **Data:** Open source information
- **Scope**: EU, entities under NIS Directive
- **Analysis includes:**
  - Observed activity (incidents)
  - Prime threats
  - Actors and motivation
  - Targets
  - Impact type
  - Affected countries
  - Trends

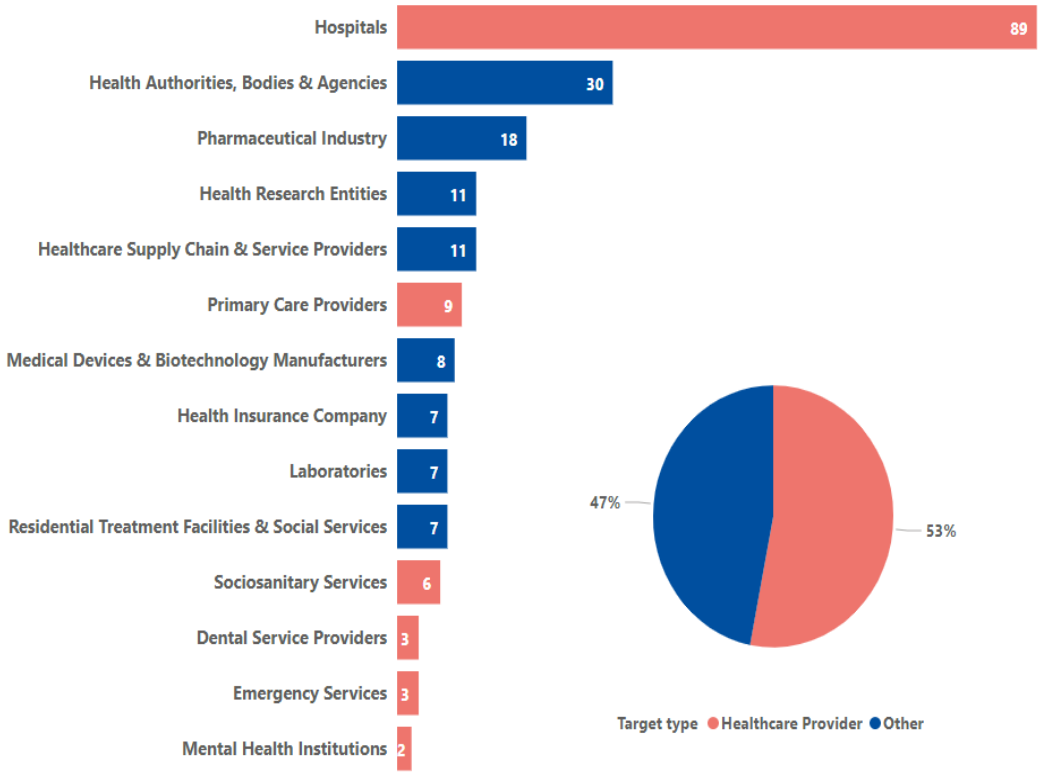
HEALTH SECTOR: THREATS AND ENTITIES AFFECTED

- The threat level for the healthcare sector in EU is **substantial.** This is based on a significant number of threats and incidents, resulting mainly in unauthorized disclosure of patients' data and disruption of medical services.

Threats in health sector

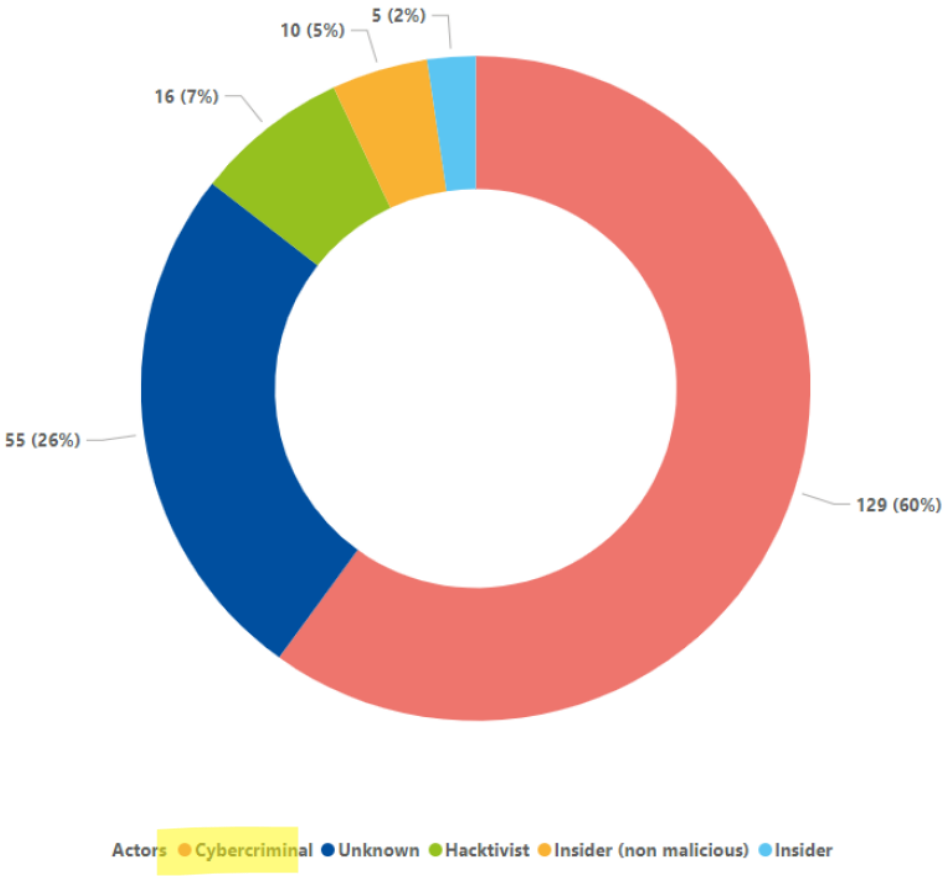


Number of incidents per entity type (targets)

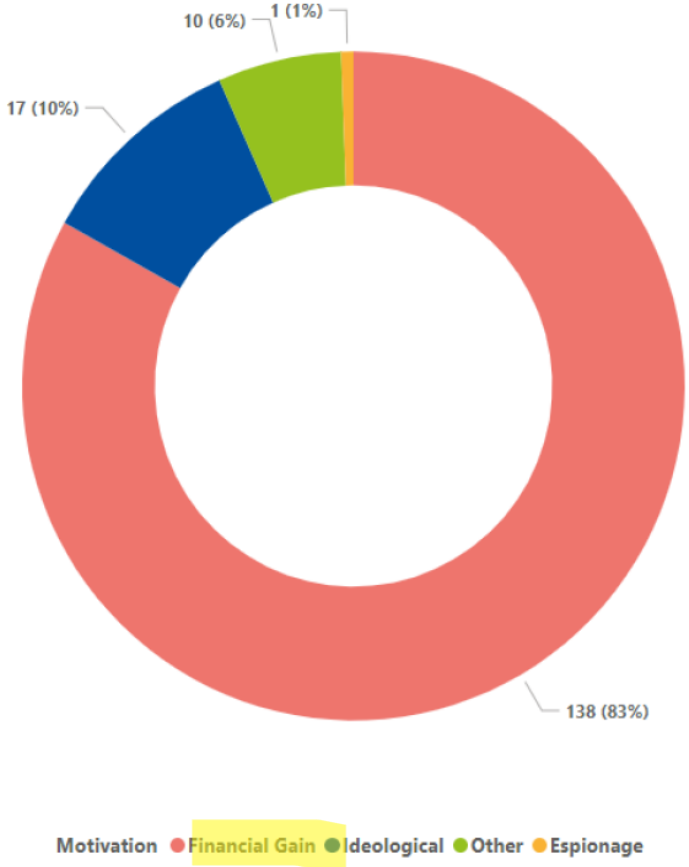


HEALTH SECTOR: THREAT ACTORS

Actor types

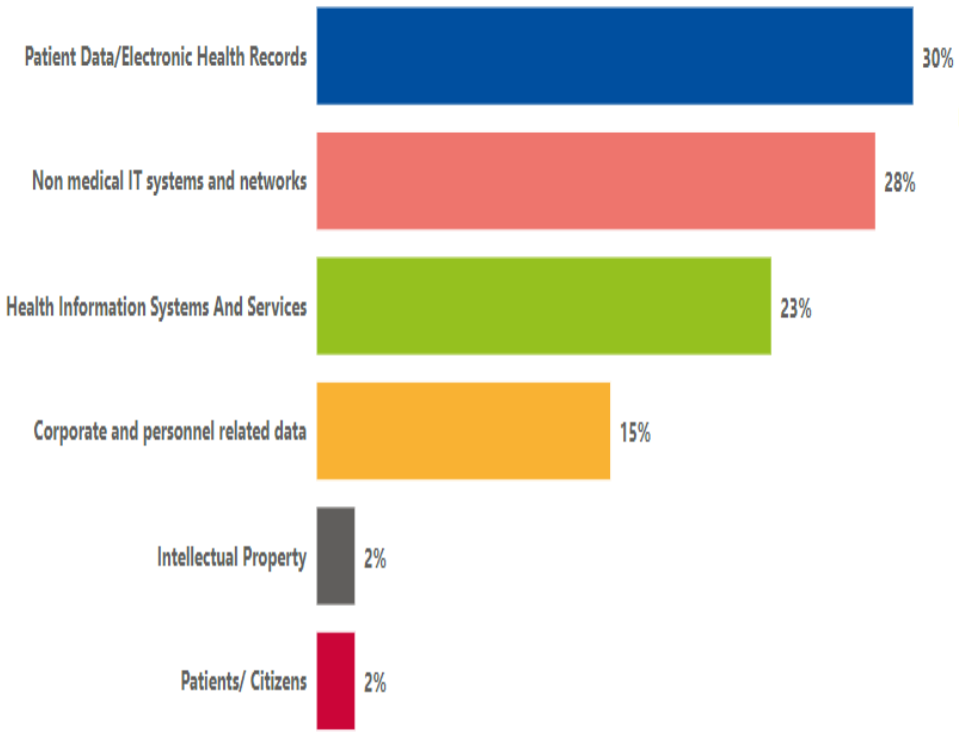


Motivation

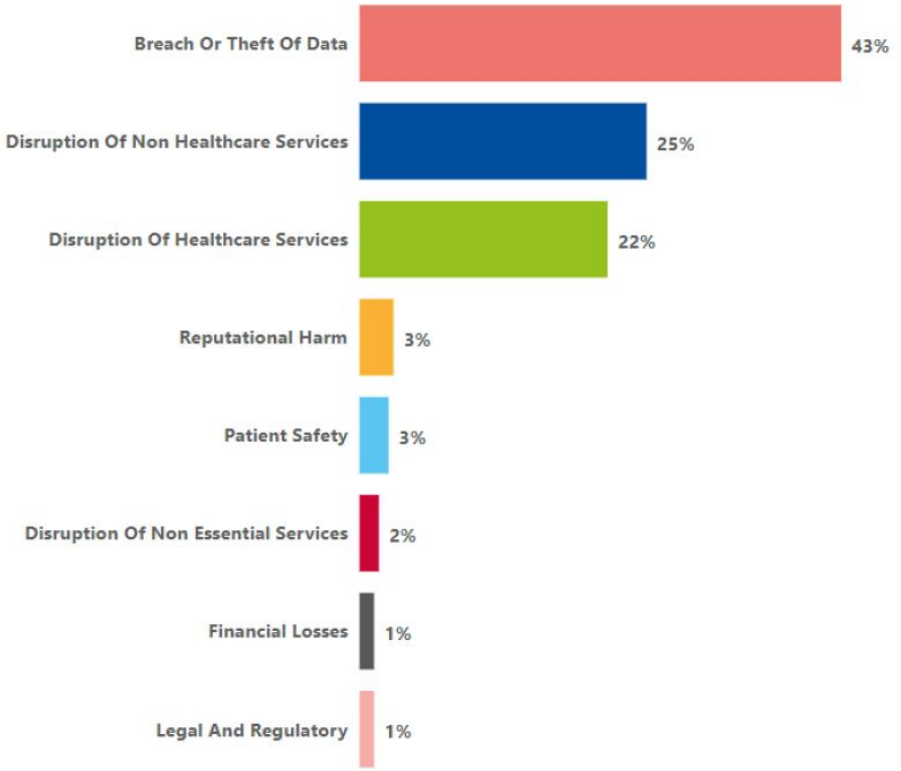


HEALTH SECTOR: IMPACT

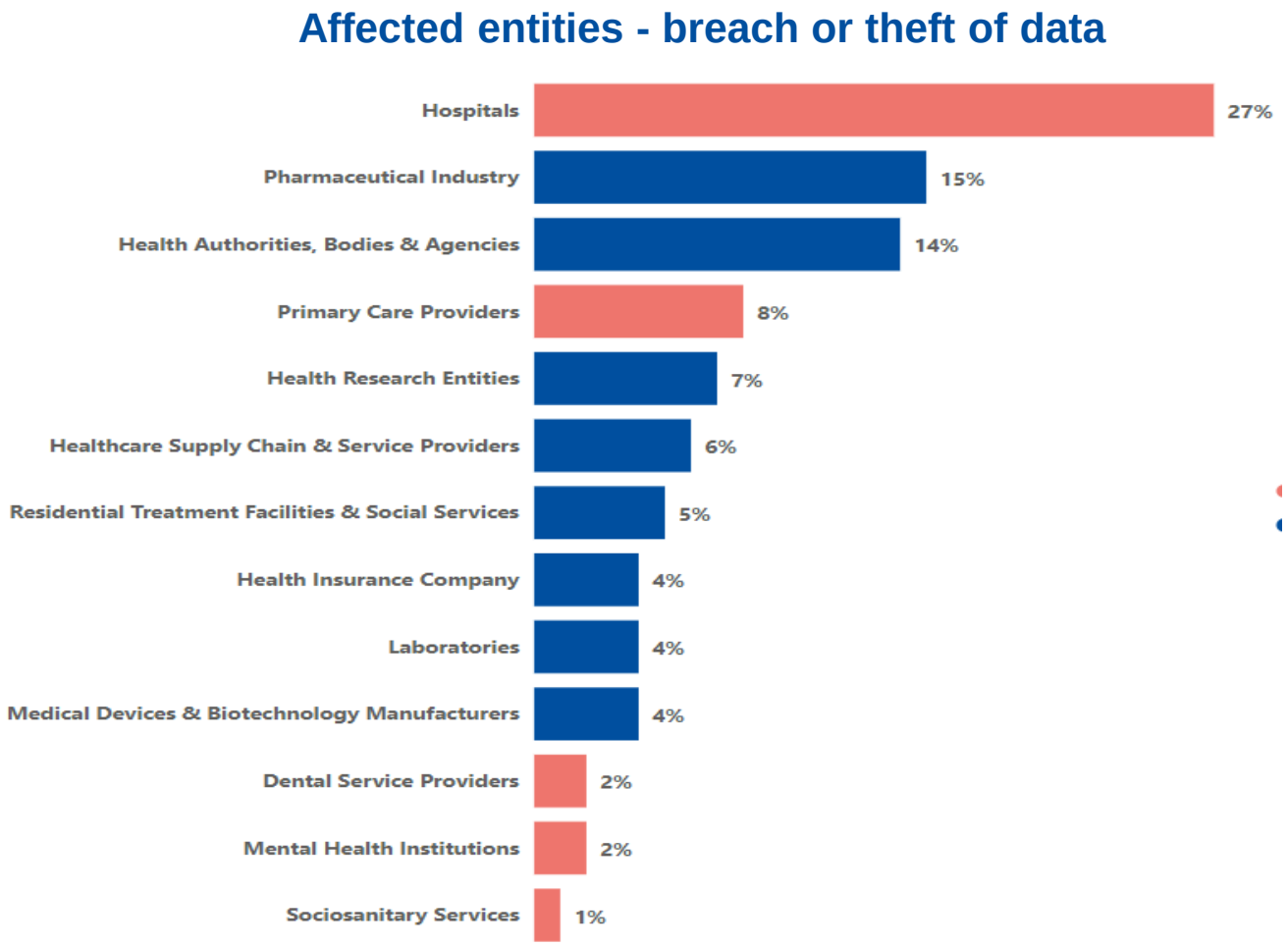
Affected assets



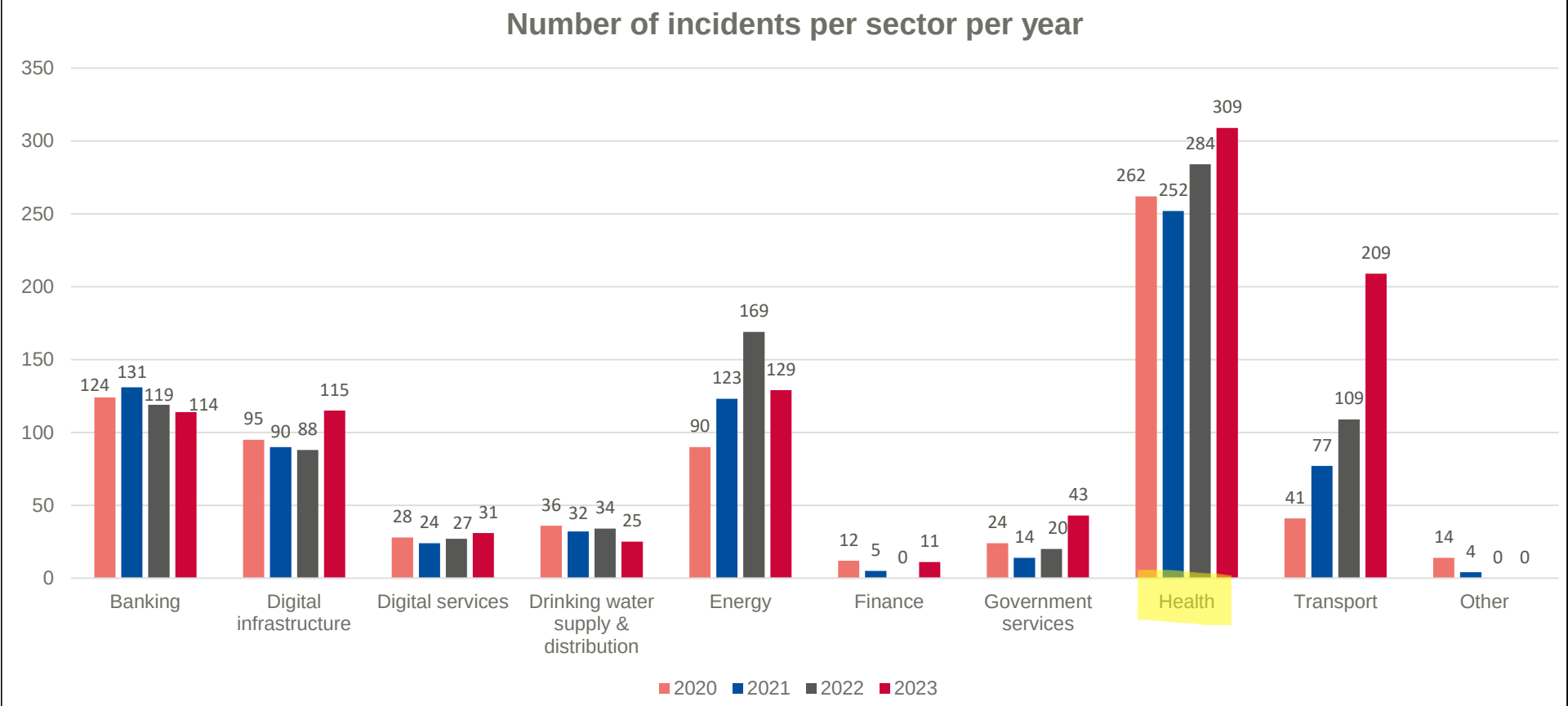
Consequences



HEALTH SECTOR: IMPACT (2)



NIS INCIDENT REPORTING



RANSOMWARE INCIDENTS - EU

Pinned Tweet

HSE Ireland
@HSELive

There is a significant ransomware attack on the HSE IT systems. We have taken the precaution of shutting down all our our IT systems in order to protect them from this attack and to allow us fully assess the situation with our own security partners.

1:28 AM · May 14, 2021 · Twitter for iPhone

732 Retweets **341** Quote Tweets **1,548** Likes

Hospital in Brussels latest victim in spate of European healthcare cyberattacks

A university hospital in Brussels has become the latest institution targeted in a spate of cyberattacks against European hospitals.

Hackers demand $10 million from Paris hospital after ransomware attack

Czech hospital hit by cyberattack while in the midst of a COVID-19 outbreak

One of the Czech Republic's biggest COVID-19 testing laboratories hit by mysterious cyberattack.

Advanced cyber-attack: NHS doctors' paperwork piles up

30 August

Doctors say it could take months to process mounting piles of medical paperwork caused by a continuing cyber-attack on an NHS supplier.

Ransomware Attack Knocks 100 Romanian Hospitals Offline

Romanian hospitals turn to pen and paper after ransomware attack on centralized healthcare management system.

HEALTH SECTOR: KEY TRENDS

- **Ransomware** one of the prime threats in health, coupled with a data breach or data theft.
- **Ransomware threat actors** driven by financial gain caused substantial impact.
- 46% of the incidents relate to **threats against the data** of health organisations (data breaches /leaks).
- The pandemic caused **patient data leaks** from Covid-19 related systems or testing laboratories on multiple occasions and in multiple countries.
- Increase of **DDoS attacks** against hospitals and health authorities in early 2023.
- Attacks on **supply chain and service providers** caused disruptions or losses to organisations in the sector.
- Healthcare organisations are reluctant to **publicly acknowledge** impact on patient safety.

KEY CYBERESECURITY CHALLENGES

- Coping with the increase in **data breaches and ransomware**
- **Vulnerabilities** in medical devices and their potential effect on patient safety and privacy
- **Supply chain** attacks
- **Low** cybersecurity **maturity**
- **Lack** of security **awareness**
- Legacy systems
- Shortage in cybersecurity skills

2022 NIS INVESTMENTS REPORT

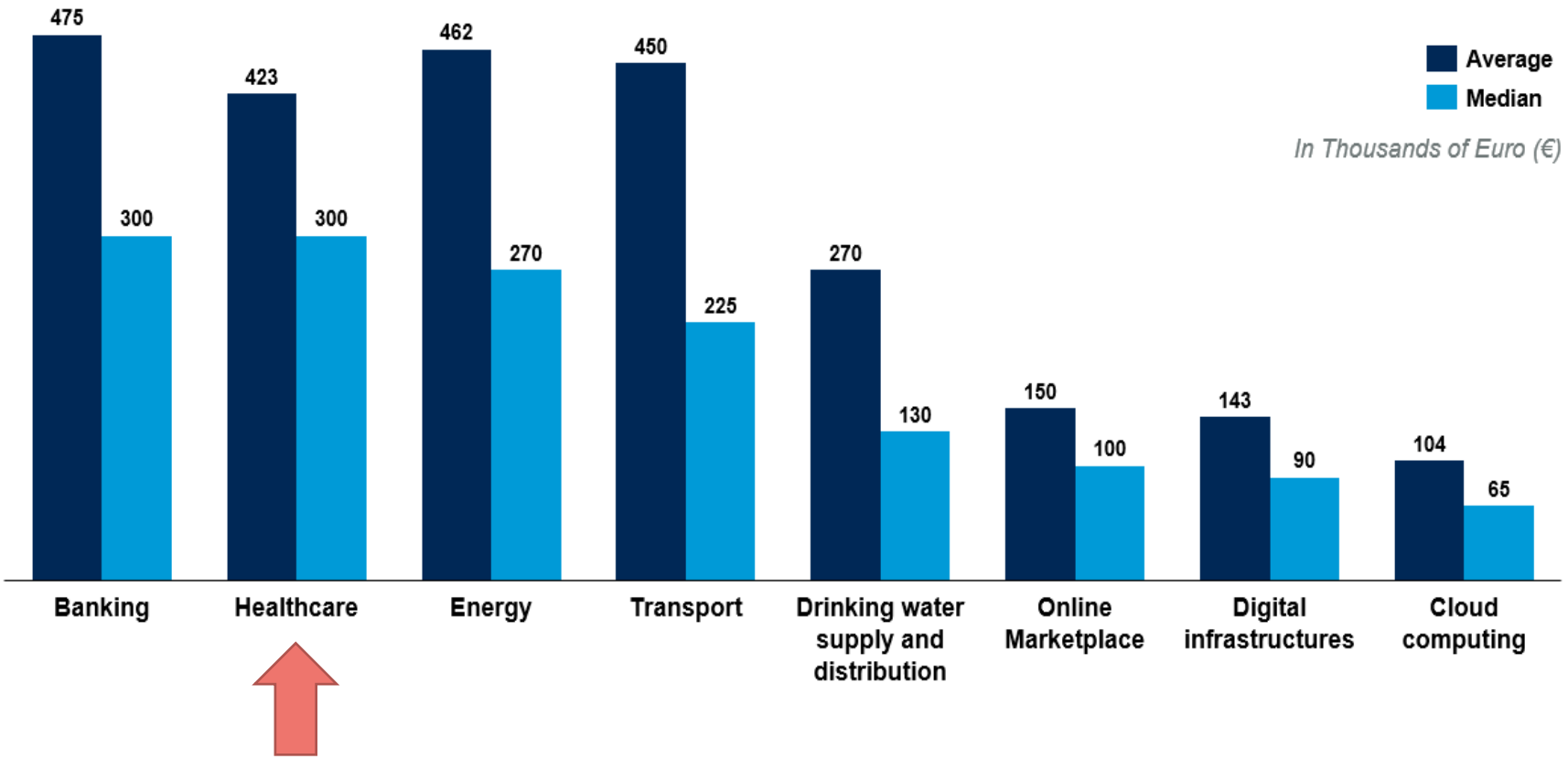
Deep dive in health:

- 189 health operators surveyed in 27 EU MS

Key findings:

- Only 27% of operators has a dedicated ransomware defence program
- 60% of operators has provided awareness training to non-IT staff
- 58% of operators uses a digital health platform running on a specific cloud platform

2022 NIS INVESTMENT REPORT: ESTIMATED COST OF MAJOR SECURITY INCIDENTS PER SECTOR



KEY RECOMMENDATIONS

- Use encryption and store sensitive data off-system to reduce the risk of unauthorized disclosure and data collection from attackers.
- Ensure that backups are offline so they are unreachable by the ransomware groups and cannot be wiped or encrypted.
- Perform regular risk assessments to understand the potential risks and threats unique to healthcare organizations.
- Implement a patch management policy to timely fix vulnerabilities on (legacy) systems and applications, hence minimizing risks exposure.
- Train users to report and identify suspicious notifications and emails. This would help mitigate the risk of successful phishing and ransomware attacks.
- Involve CISOs into all projects with an IT dimension and encourage collaboration between cybersecurity, IT and medical staff.

THANK YOU FOR YOUR ATTENTION

Agamemnonos 14, Chalandri
15231
Attiki, Greece

ENISA Threat Landscape:
Health Sector

etl@enisa.europa.eu

www.enisa.europa.eu