enisa

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ENISA THREAT LANDSCAPE (ETL): HEALTH SECTOR

Albert Haro

CISO

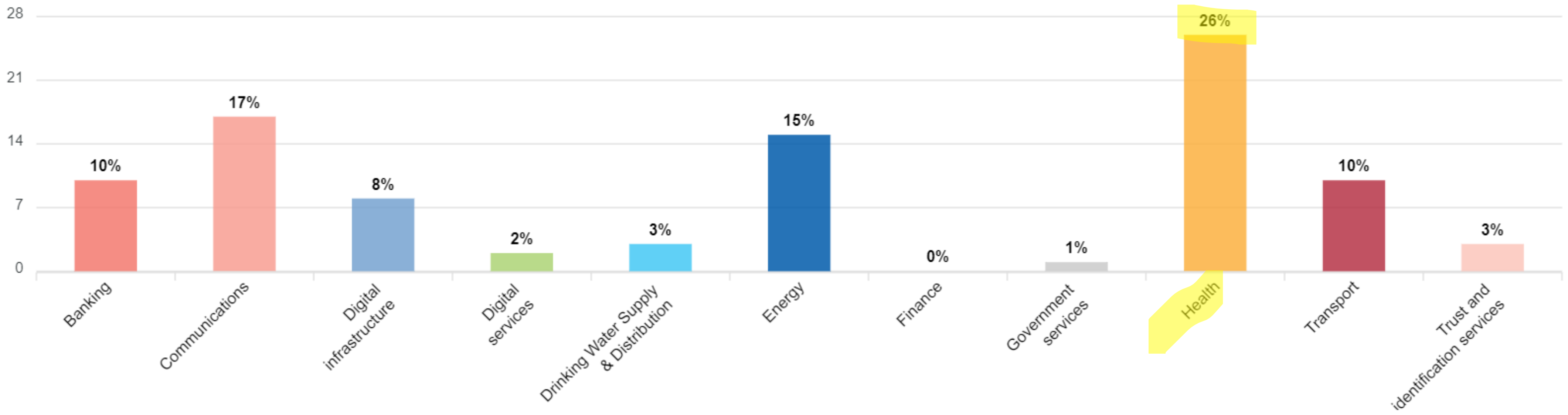
Cybersecurity Agency of Catalonia

8th ENISA eHealth Security Conference

20 | 09 | 2023

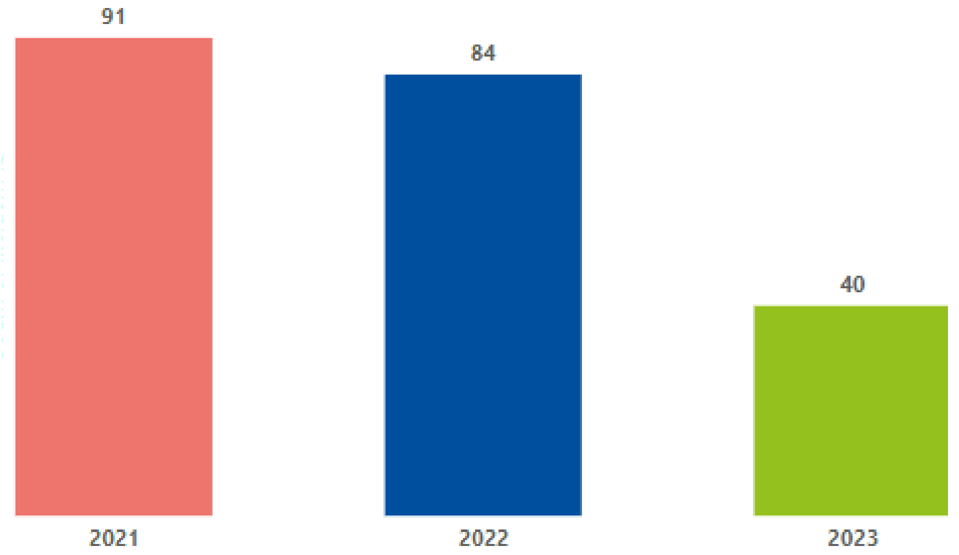
NIS INCIDENT REPORTING

Impact per sector (%)



ENISA THREAT LANDSCAPE (ETL): HEALTH SECTOR

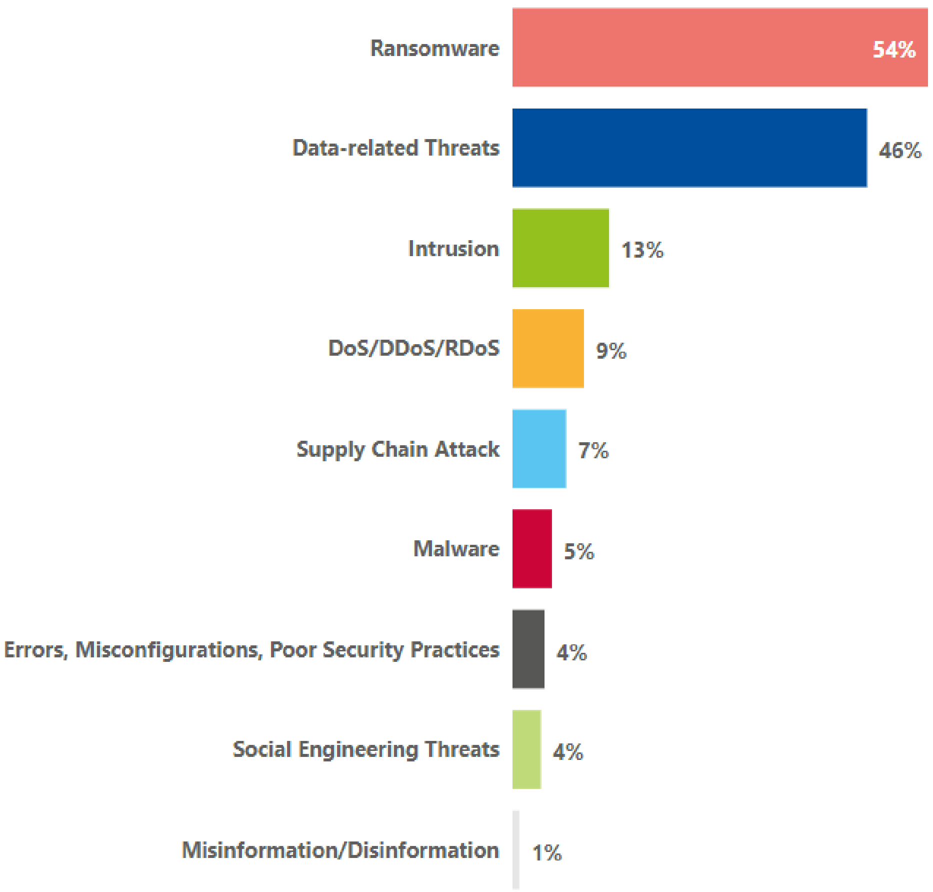
Incidents observed per year (2021, 2022, Q1 2023)



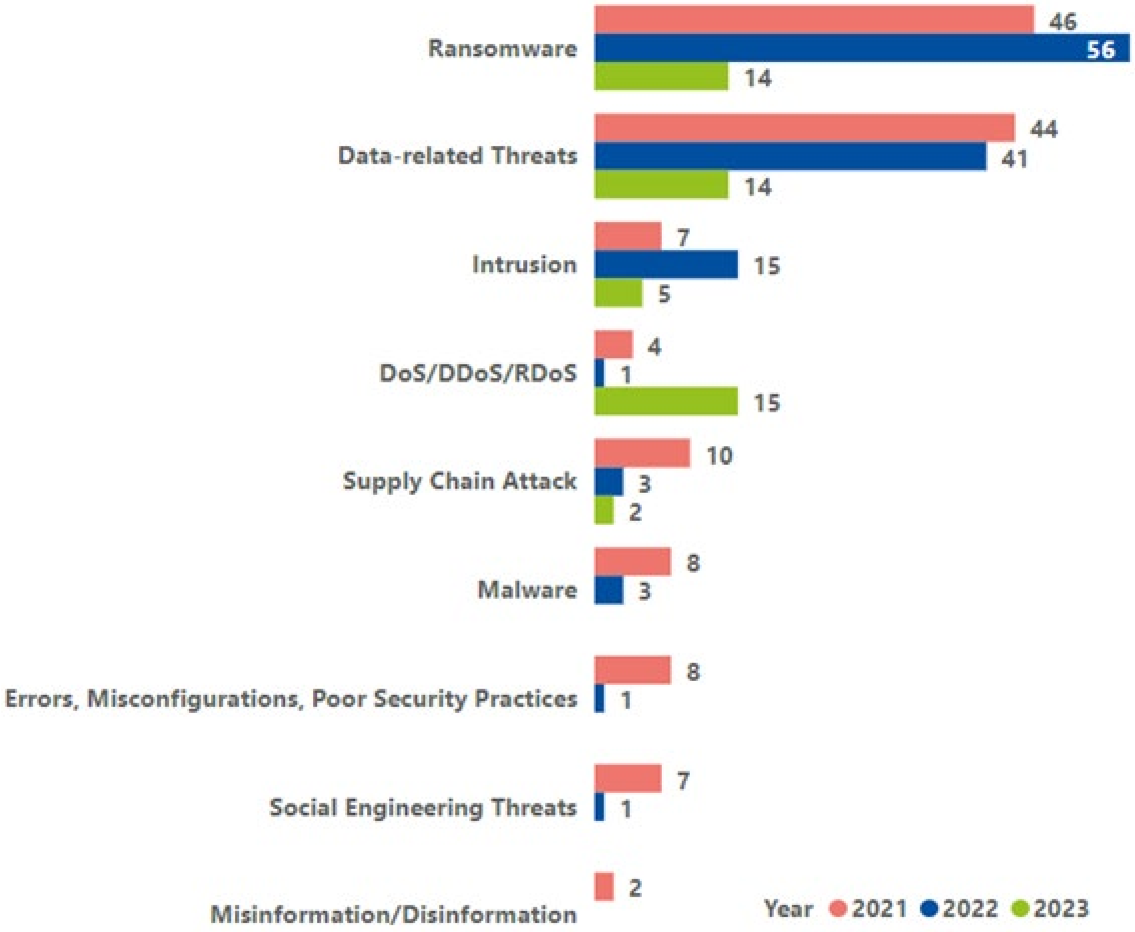
- January 2021 to March 2023
- Analysis of the incidents concluded in May 2023
- 215 publicly reported incidents in the EU and neighbouring countries

ETL: HEALTH THREATS

Threats in health sector (2021-2023)

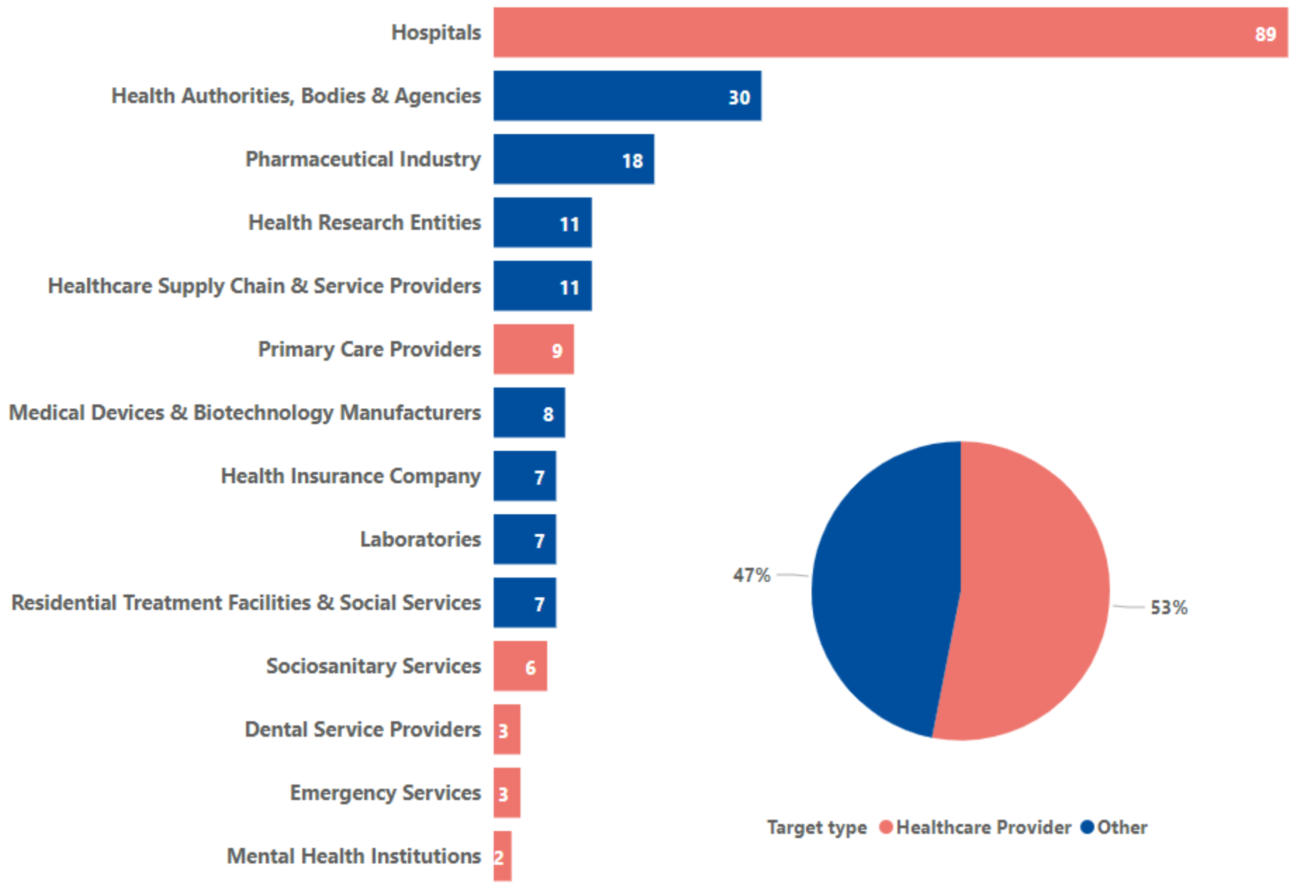


Threats per year

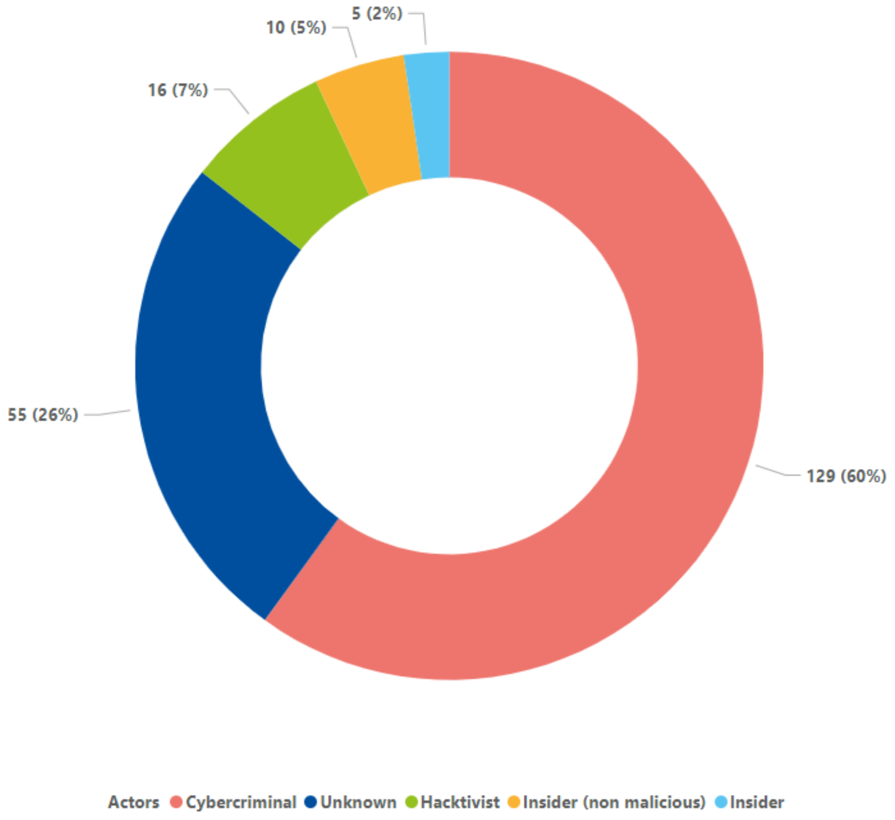


ETL: ENTITY AND ACTOR TYPES

Number of incidents per entity type

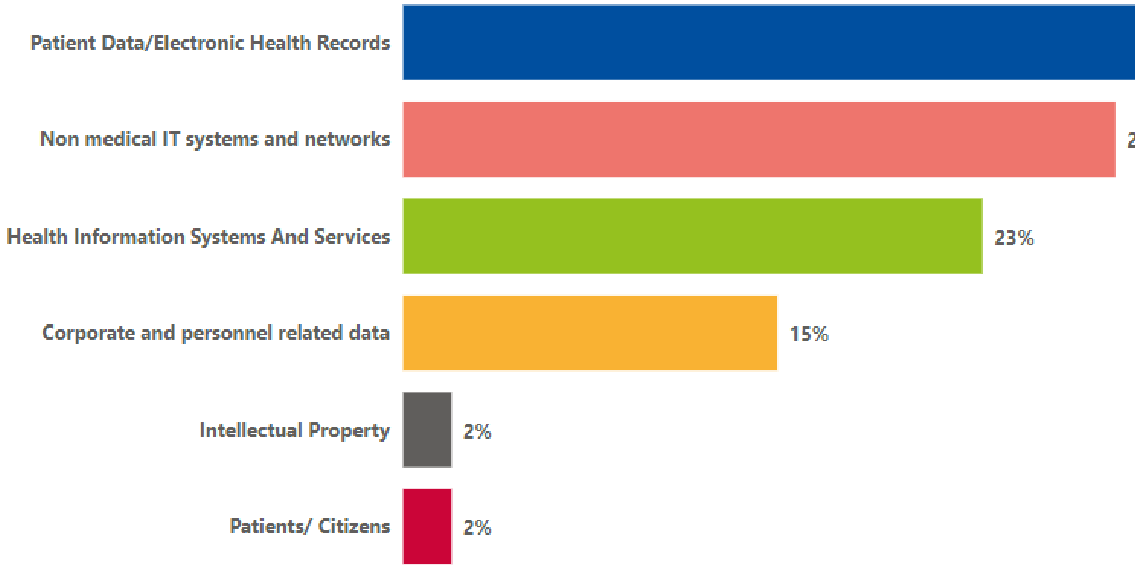


Actor types

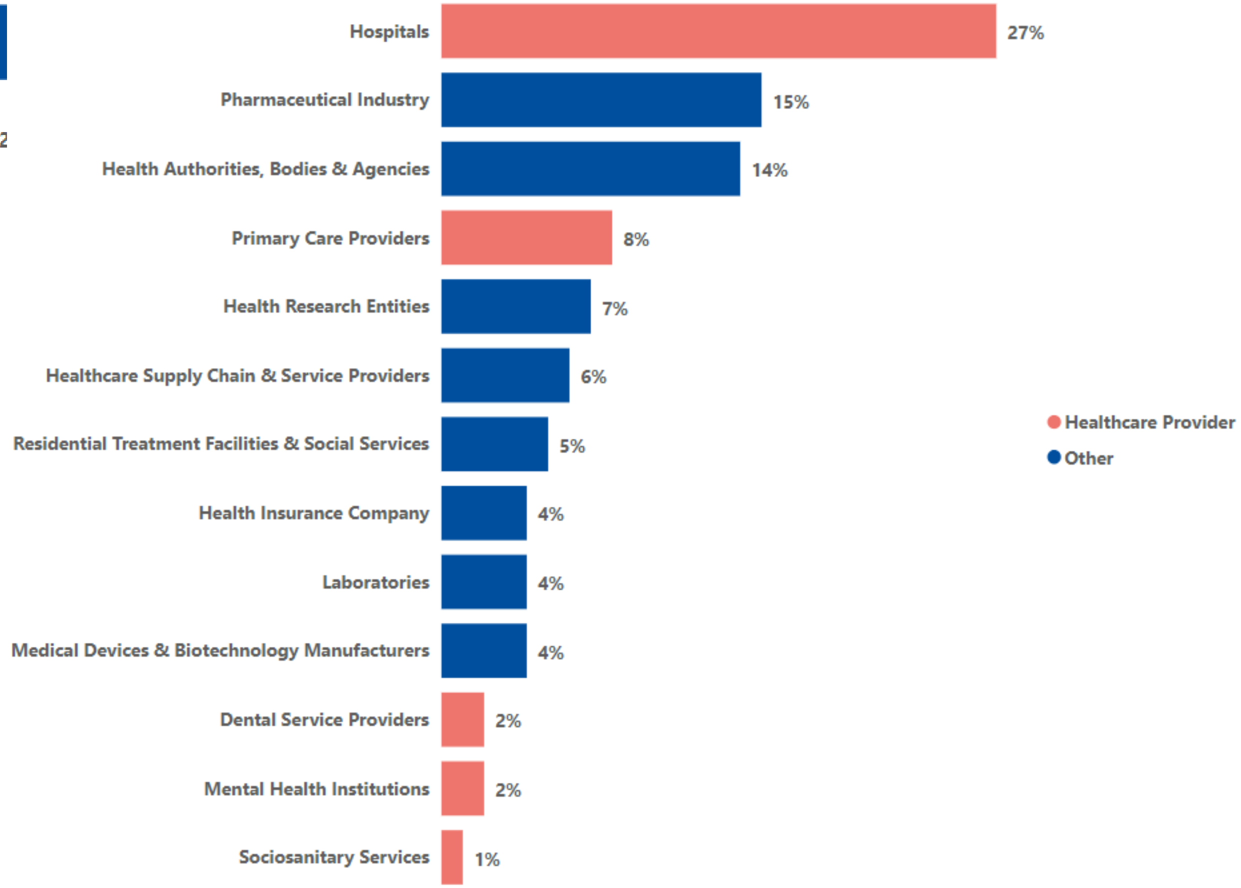


ETL: HEALTH ASSETS AND ENTITIES AFFECTED

Affected assets

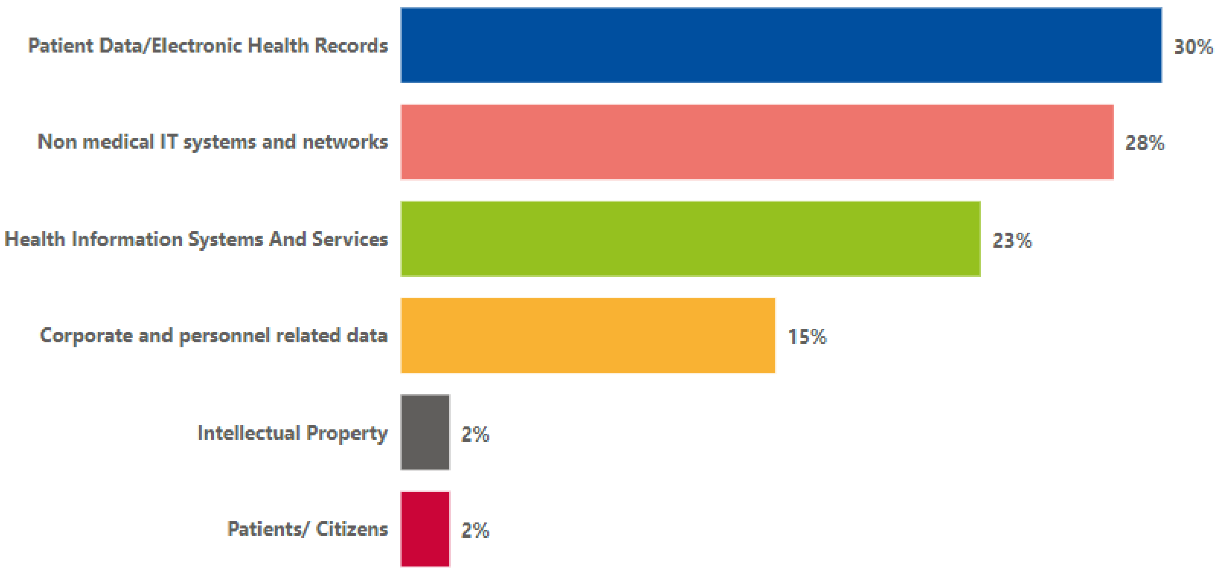


Affected entities - breach or theft of data

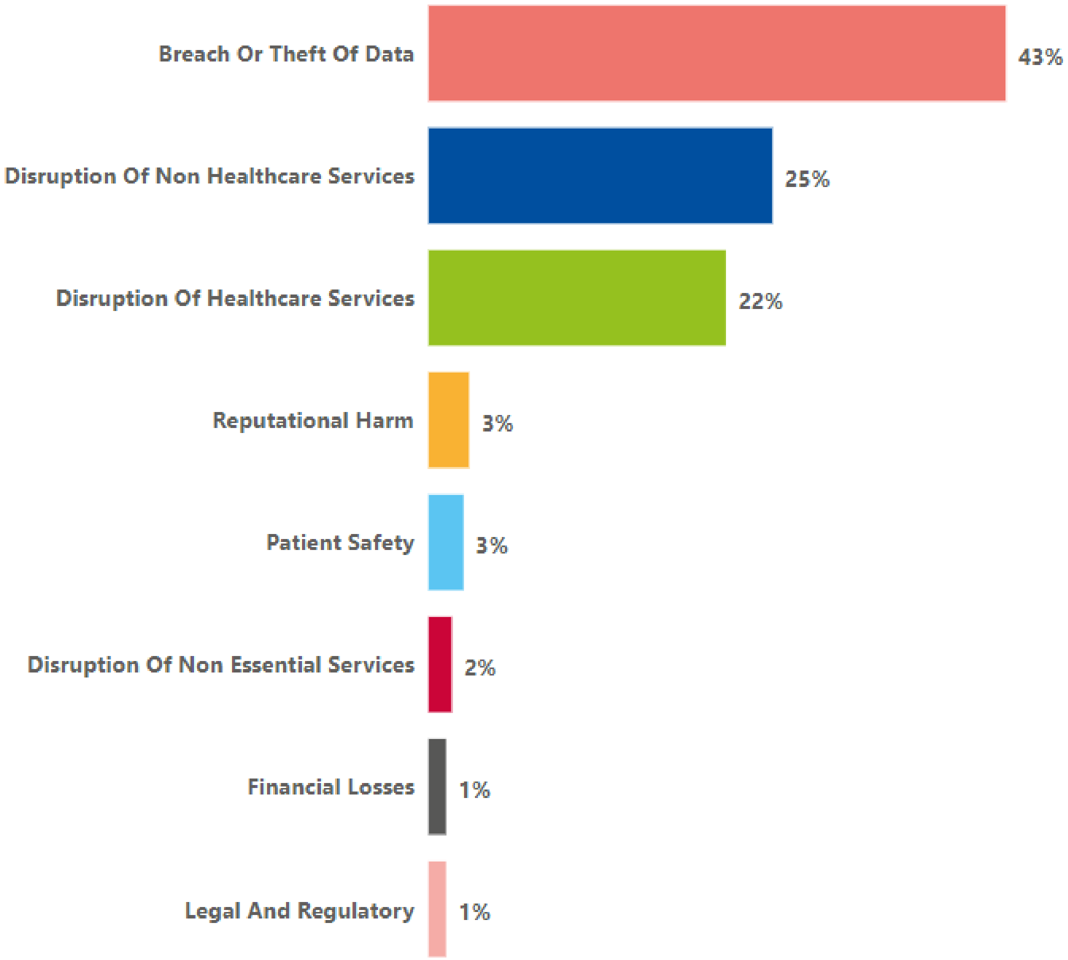


ETL: HEALTH IMPACT

Affected assets



Consequences



ETL: HEALTH FINDINGS

- **Ransomware** is one of the prime threats in the health sector (54%).
- **46% of incidents** resulted from **threats against the data** of health organisations (data breaches, data leaks).
- **Cybercriminals** had the heaviest impact on the sector, in particular ransomware threat actors driven by financial gain (53%).
- The **pandemic caused data leakage** of patient data from Covid-19 related systems or testing laboratories on multiple occasions and in multiple countries.
- Increase in **DDoS attacks against hospitals and health authorities** in early 2023.
- Attacks on **healthcare supply chain and service providers** caused disruptions or losses to organisations in the health sector (7%).
- **Delays in treatment, cancelled operations** or diversion to other facilities can impact both patients and healthcare professionals.

ETL: HEALTH CHALLENGES

- **Vulnerabilities** in medical devices.
- **Rapid evolution** of healthcare systems and medical devices.
- Patients whose sensitive health data have been stolen may face **extortion** after a data breach.
- Only 27% of organisations surveyed in the health sector have a dedicated **ransomware defence programme** and 40% of the organisations surveyed have no **security awareness programme** for non-IT staff.
- 95% of the health organisations surveys face challenges when performing **risk assessments**, while 46% have never performed a risk analysis.
- Challenges in **data collection** and underreporting.

ETL: HEALTH RECOMMENDATIONS

- **Offline encrypted backups** of mission critical data.
- **Awareness raising and training** programmes for healthcare professionals.
- Regular **vulnerability scanning**.
- Regular **patches and updates** on software and operating systems.
- Good practices for **authentication methods** for remote access.
- Basic **cyber incident response plans** to ensure that patient care is not affected.
- **Commitment of senior management** is key - NIS2 introduces liabilities for top management.
- Additional resources for mitigation controls:
  - ENISA Threat Landscape 2022
  - NIS CG report on “Threats and risk management in the health sector”

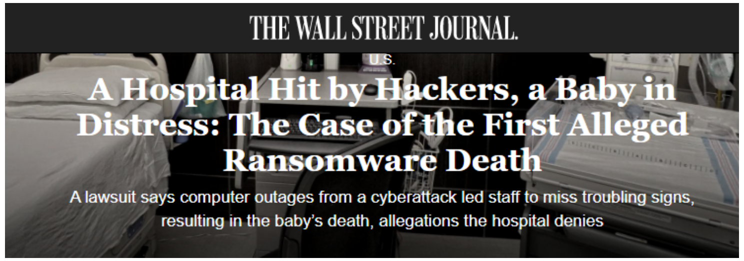
SOME RELEVANT RANSOMWARE INCIDENTS

Conti cyber attack on the HSE

Independent Post Incident Review

Commissioned by the HSE Board in conjunction with the CEO and Executive Management Team

03 December 2021

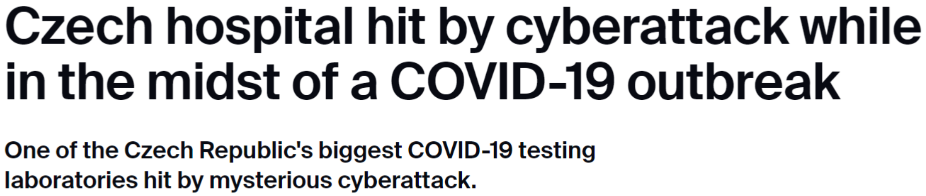


THE WALL STREET JOURNAL.

U.S.

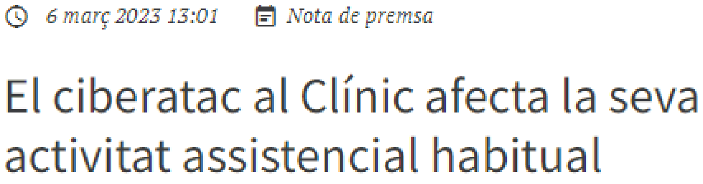
A Hospital Hit by Hackers, a Baby in Distress: The Case of the First Alleged Ransomware Death

A lawsuit says computer outages from a cyberattack led staff to miss troubling signs, resulting in the baby's death, allegations the hospital denies



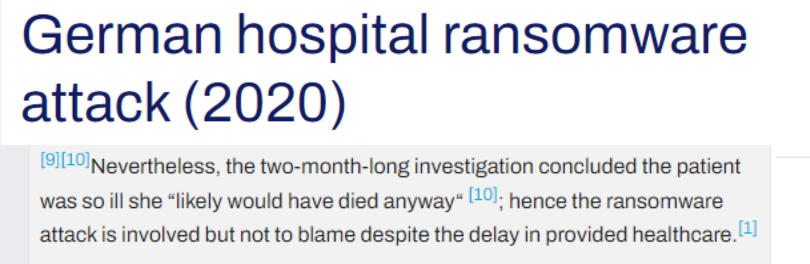
Czech hospital hit by cyberattack while in the midst of a COVID-19 outbreak

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



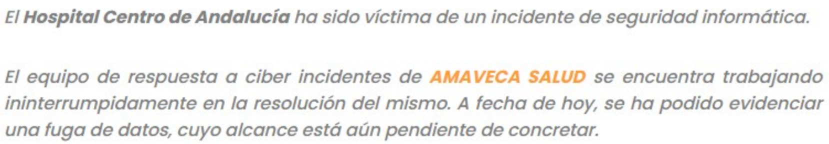
6 març 2023 13:01 Nota de premsa

El ciberatac al Clínic afecta la seva activitat assistencial habitual



German hospital ransomware attack (2020)

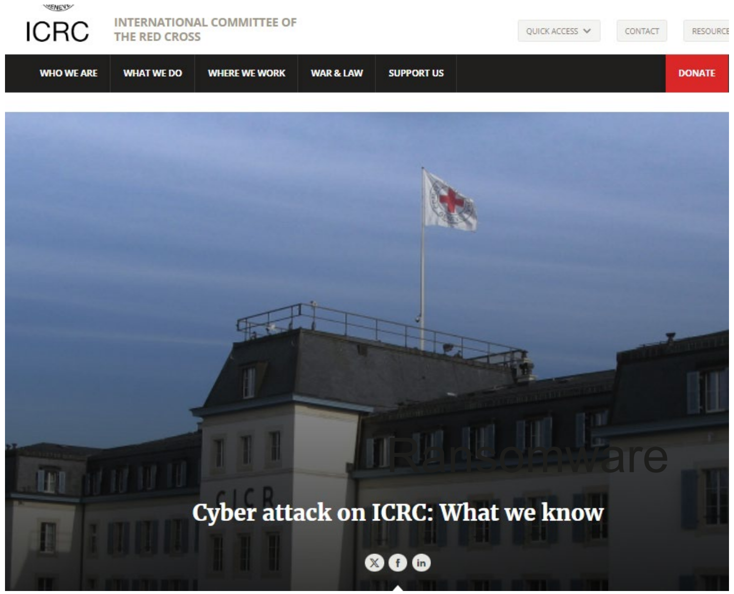
[9][10]Nevertheless, the two-month-long investigation concluded the patient was so ill she “likely would have died anyway“ [10]; hence the ransomware attack is involved but not to blame despite the delay in provided healthcare.[1]



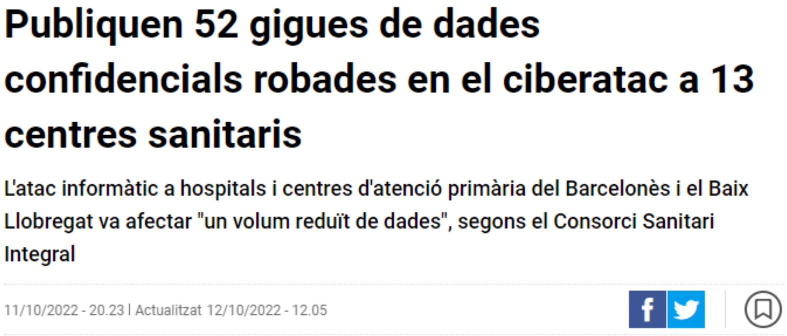
*El **Hospital Centro de Andalucía** ha sido víctima de un incidente de seguridad informática.*

*El equipo de respuesta a ciber incidentes de **AMAVECA SALUD** se encuentra trabajando ininterrumpidamente en la resolución del mismo. A fecha de hoy, se ha podido evidenciar una fuga de datos, cuyo alcance está aún pendiente de concretar.*

SOME RELEVANT DATA RELATED INCIDENTS



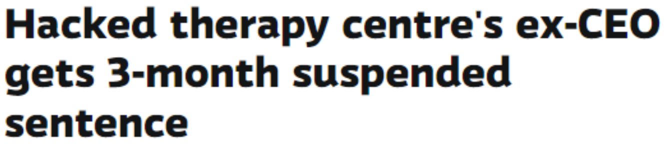
Cyber attack on ICRC: What we know



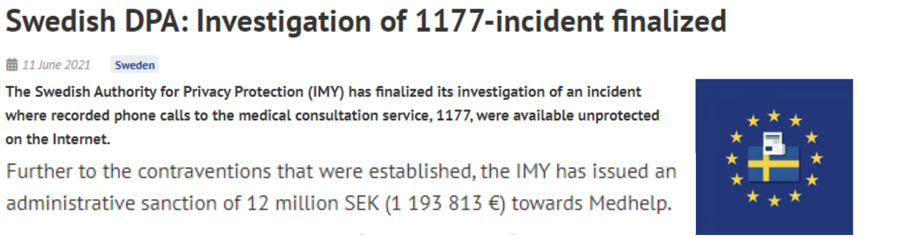
Publiquen 52 gigues de dades confidencials robades en el ciberatac a 13 centres sanitaris

L'atac informàtic a hospitals i centres d'atenció primària del Barcelonès i el Baix Llobregat va afectar "un volum reduït de dades", segons el Consorci Sanitari Integral

11/10/2022 - 20.23 | Actualitzat 12/10/2022 - 12.05



Hacked therapy centre's ex-CEO gets 3-month suspended sentence

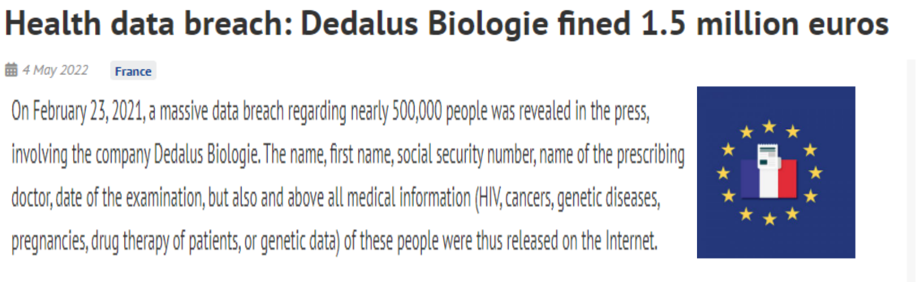


Swedish DPA: Investigation of 1177-incident finalized

11 June 2021 Sweden

The Swedish Authority for Privacy Protection (IMY) has finalized its investigation of an incident where recorded phone calls to the medical consultation service, 1177, were available unprotected on the Internet.

Further to the contraventions that were established, the IMY has issued an administrative sanction of 12 million SEK (1 193 813 €) towards Medhelp.



Health data breach: Dedalus Biologie fined 1.5 million euros

4 May 2022 France

On February 23, 2021, a massive data breach regarding nearly 500,000 people was revealed in the press, involving the company Dedalus Biologie. The name, first name, social security number, name of the prescribing doctor, date of the examination, but also and above all medical information (HIV, cancers, genetic diseases, pregnancies, drug therapy of patients, or genetic data) of these people were thus released on the Internet.

THANK YOU FOR YOUR ATTENTION

Albert Haro Abad.

☎ +34 647 333 256

✉ aharo@ciberseguretat.cat