

SERVIZIO SANITARIO REGIONALE  
EMILIA-ROMAGNA  
Azienda Unità Sanitaria Locale di Reggio Emilia  
IRCCS Istituto in tecnologie avanzate e modelli assistenziali in oncologia



2025  
EEMEA  
SCIENTIFIC  
SEMINARS

16<sup>th</sup> Advanced  
Hemostasis Seminar  
October 14-15, 2025 • Vilnius

# Cybersecurity in Healthcare Institutions and the Laboratory



Marco Foracchia





SERVIZIO SANITARIO REGIONALE  
EMILIA-ROMAGNA  
Azienda Unità Sanitaria Locale di Reggio Emilia  
IRCCS Istituto in tecnologie avanzate e modelli assistenziali in oncologia



Marco Foracchia – who is this guy ?

## Chief Information Officer

**10 years experience in the private medical IT sector**

**>10 years experience in the public sector**

**Currently managing IT systems in 1 Oncology Research Hospital and a network of 5 hospitals**



**Member of the HIMSS Italian Community Committee**



**KLAS International Advisory Board**



ASSOCIAZIONE ITALIANA | SISTEMI INFORMATIVI IN SANITÀ



**President AISIS (Italian Association of Healthcare Information Systems Professionals) Italian CHIME Chapter**

**Biomedical Engineer !**





SERVIZIO SANITARIO REGIONALE  
EMILIA-ROMAGNA  
Azienda Unità Sanitaria Locale di Reggio Emilia  
IRCCS Istituto in tecnologie avanzate e modelli assistenziali in oncologia



# Reggio Emilia Local Health Authority



80.000  
Hospitalizations



140.000  
First Aid  
accesses



8.000.000  
Clinics  
accesses



6  
Hospitals  
(1600 beds)



6800  
Employees  
(1000  
Doctors)



IRCCS (Translational  
Research Center) in  
Oncology



SERVIZIO SANITARIO REGIONALE  
EMILIA-ROMAGNA  
Azienda Unità Sanitaria Locale di Reggio Emilia  
IRCCS Istituto in tecnologie avanzate e modelli assistenziali in oncologia



Goal of this presentation

## 1. Terrorize you



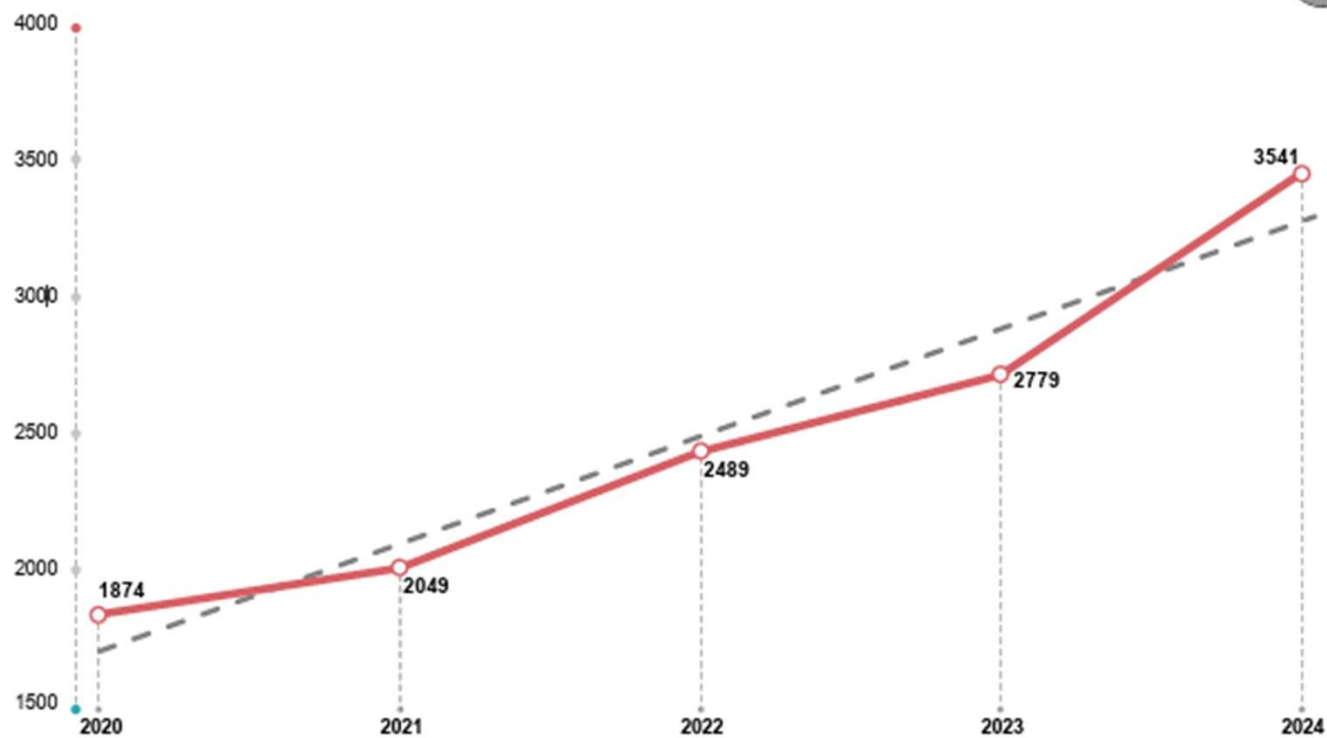
## 2. Make you feel guilty



## 3. Help you understand how we can live better together...

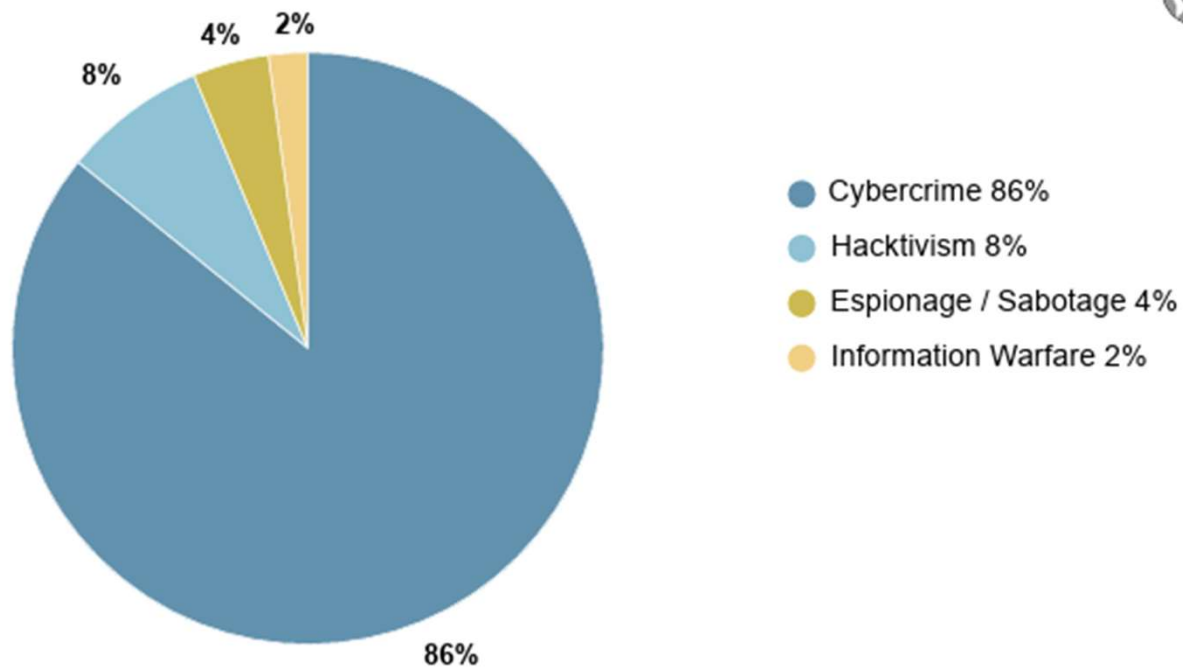


# Cybersecurity Incidents 2020-2024



© Clusit - Rapporto 2025 sulla Cybersecurity

## Attack Type - 2024

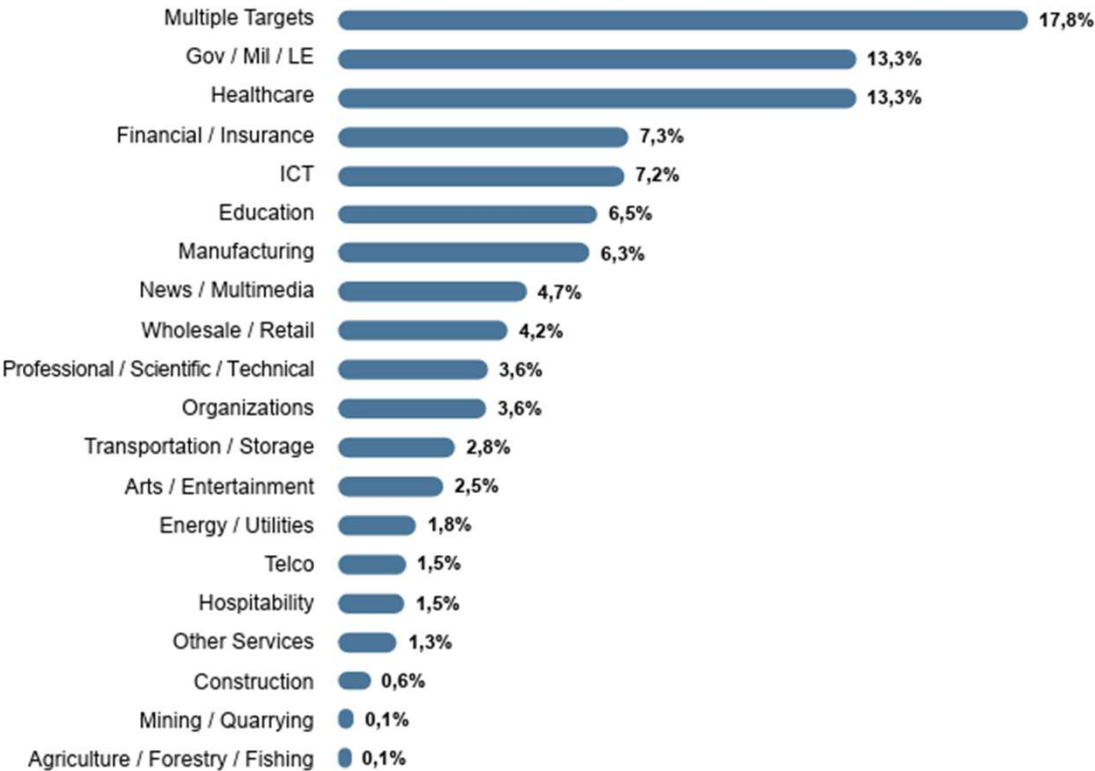


© Clusit - Rapporto 2025 sulla Cybersecurity



# Who do they attack most frequently ?

## Attacked Industries/Sectors 2024



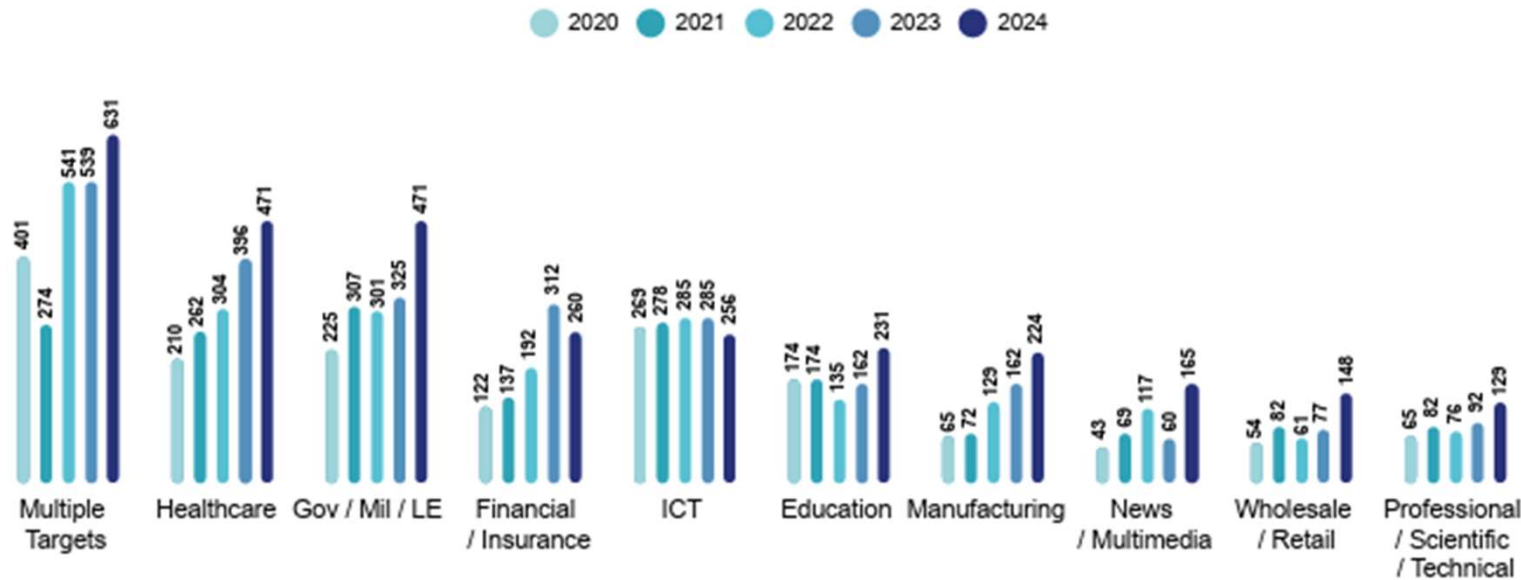
© Clusit - Rapporto 2025 sulla Cybersecurity

# Who do they attack most frequently ?

## Attacked Industries/Sectors 2020 - 2024



**18,9 %**  
growth of  
cyberattacks to  
Healthcare in 2024



© Clusit - Rapporto 2025 sulla Cybersecurity

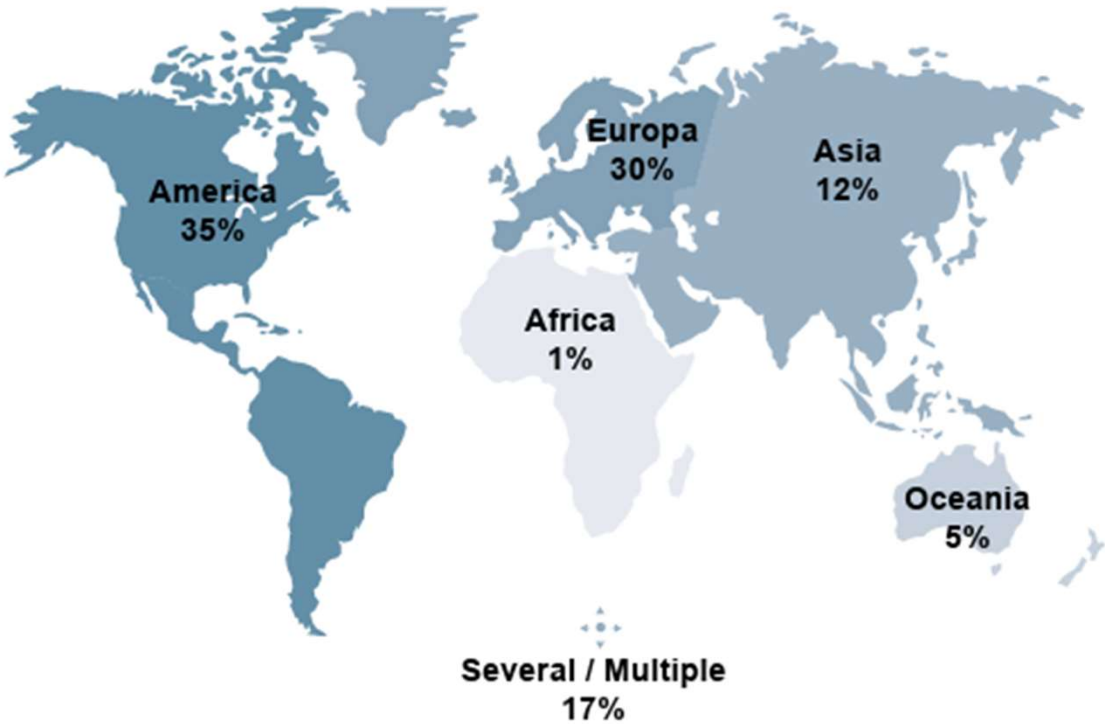


# Attacks Geography - 2024



**2 out of 3**  
Attacks in  
Europe and  
Americas

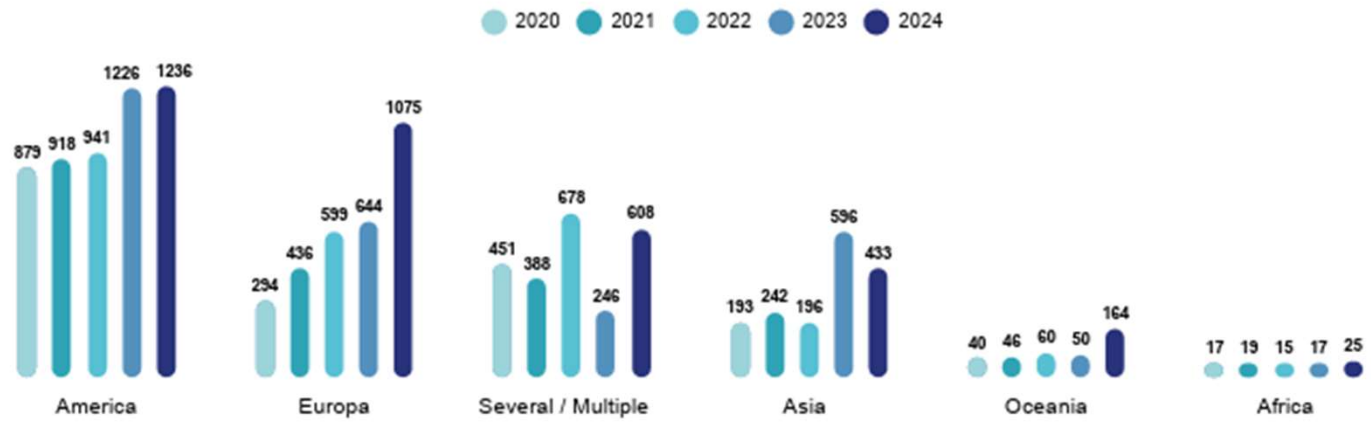
**+67%**  
attacks in  
Europe



© Clusit - Rapporto 2025 sulla Cybersecurity

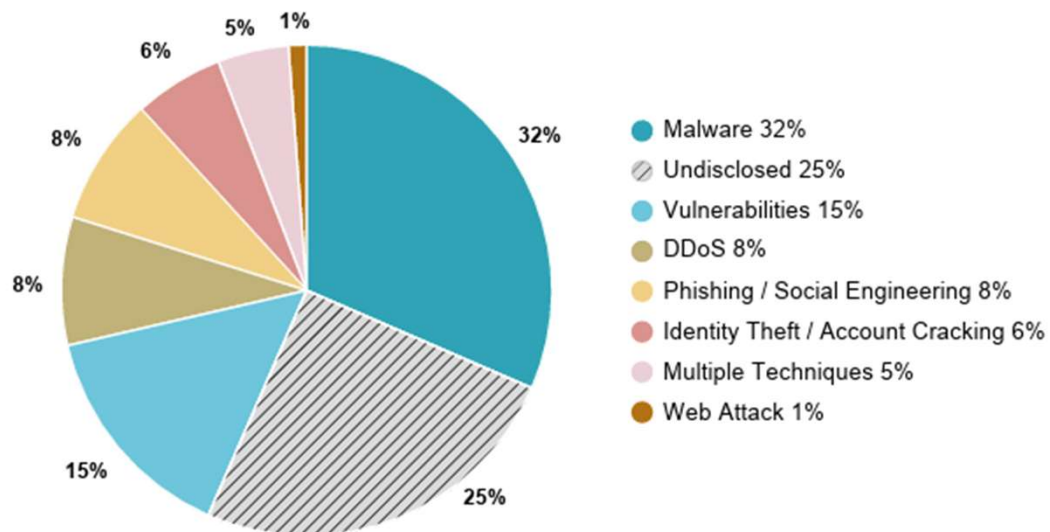


# Attacks Geography – 2020-2024



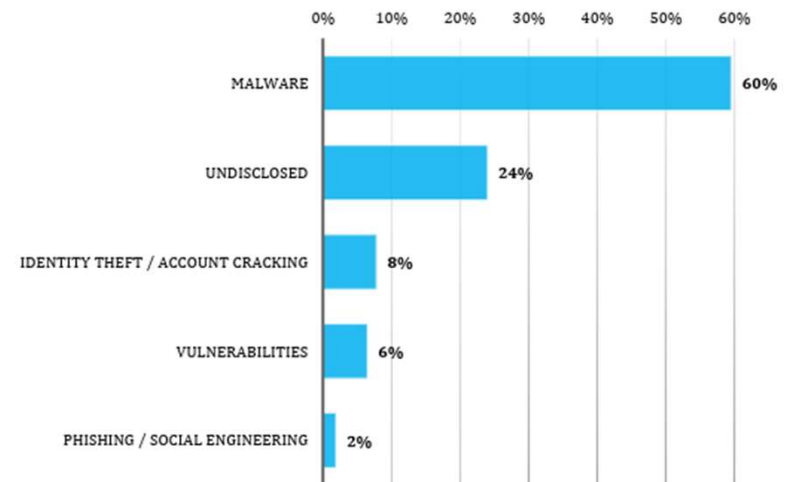
© Clusit - Rapporto 2025 sulla Cybersecurity

## Attack Type –2024



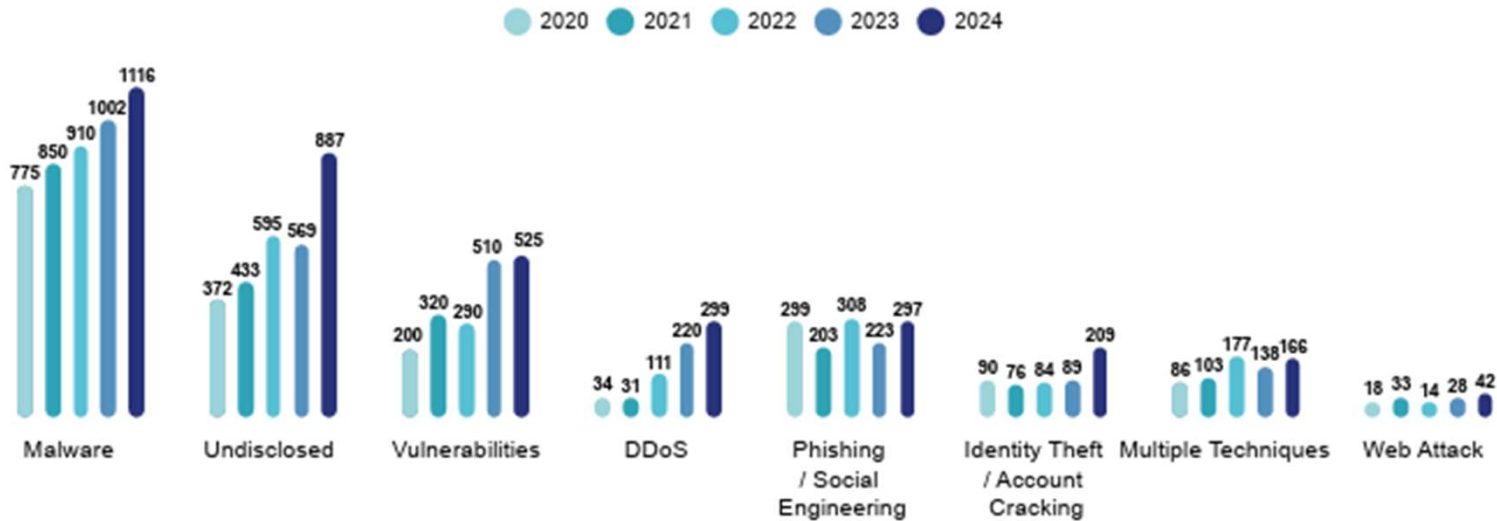
© Clusit - Rapporto 2025 sulla Cybersecurity

## Attack Type in Healthcare – 2024



© Hackmanac Global Cyber Attacks Report 2025

# Attack Type – 2020-2024



© Clusit - Rapporto 2025 sulla Cybersecurity

**SEVERITY** refers to the impact level of a cybersecurity incident on an organization or society.

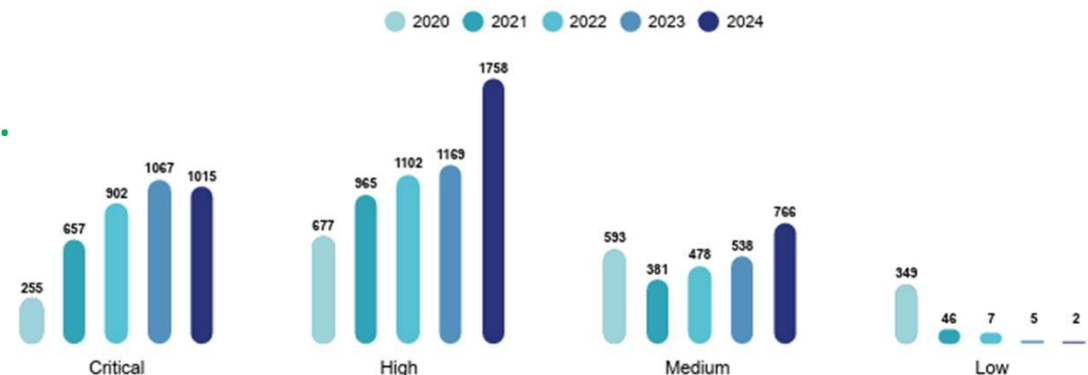
**Critical impact:** Incidents with extremely serious consequences, such as prolonged disruption of essential services, major financial losses, large-scale compromise of sensitive data, or systemic effects.

**High impact:** Significant damage, though not systemic. This includes substantial financial losses, reputational harm, or compromise of important business data.

**Medium impact:** Incidents causing moderate disruptions or losses that are still relevant to the organization.

**Low impact:** Incidents with minimal or negligible consequences. These are now almost absent in the analyzed sample.

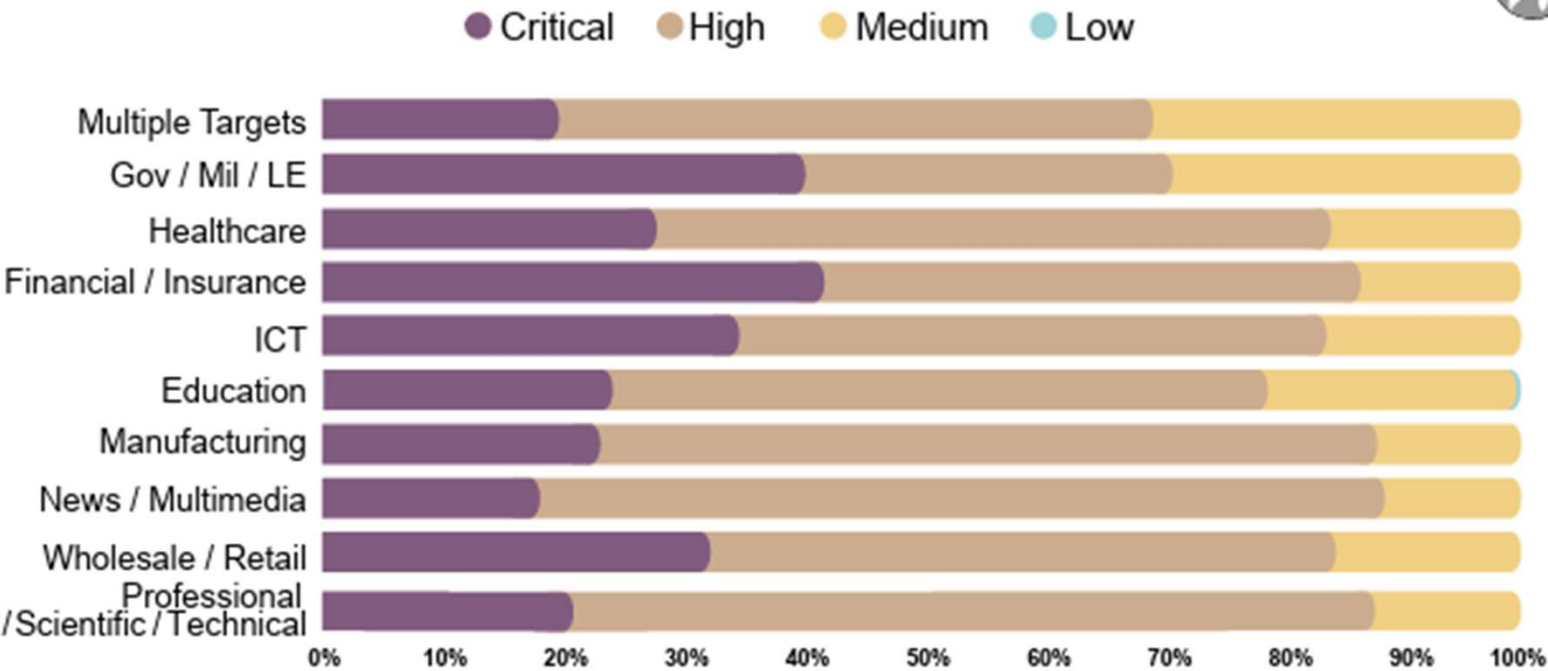
## Attack Severity – 2020-2024



Clusit - Rapporto 2025 sulla Cybersecurity



# Attack Severity per Sector– 2024



© Clusit - Rapporto 2025 sulla Cybersecurity

why



**Regulation (EU) 2016/679**  
of the European Parliament and of the  
Council of 27 April 2016

how



**Network & Information Security Directive (NIS2)**  
December 14, 2022  
(Member states had time until October 17, 2024)





# Loss / Compromission of Data



# Disruption of Service

Organizational mission (and regulatory mandate) cannot be fulfilled



## Value of Healthcare Data

**Highly sensitive data:** contain personal, medical, insurance, and financial information (name, ID number, diagnoses, reports, prescriptions, test results, etc.).

**Difficult to change:** unlike credit cards, a healthcare identity cannot be “deactivated” or replaced.

**Profitable black market:** on the dark web, a complete medical record can be worth 10 to 100 times more than a stolen credit card

**Malicious uses:** insurance fraud, extortion, medical identity theft, or personalized phishing campaigns.





# Vulnerabilities of Healthcare Systems

**Outdated infrastructure:** many hospitals still use old, often unpatchable software and devices.

**Connected medical devices (IoMT):** infusion pumps, monitors, CT scanners, etc., connected to networks but with poor security measures.

**Poor network segmentation:** an infection can quickly spread from a clinical workstation to critical systems.

**Limited cybersecurity resources:** IT budgets are often smaller than in other high-risk sectors.





## Immediate Impact and Leverage for Ransom

Critical, non-stoppable services: blocking a hospital or diagnostic lab can put lives at risk.

High pressure to pay: in ransomware attacks, the urgent need to restore operations often leads victims to pay the ransom.

Media impact: attacks on hospitals draw major public attention, useful for criminal groups seeking visibility or political pressure.



**MEDIA IMPACT  
OF HEALTH  
INFORMATION  
SYSTEM DOWNTIME**





SERVIZIO SANITARIO REGIONALE  
EMILIA-ROMAGNA  
Azienda Unità Sanitaria Locale di Reggio Emilia  
IRCCS Istituto in tecnologie avanzate e modelli assistenziali in oncologia



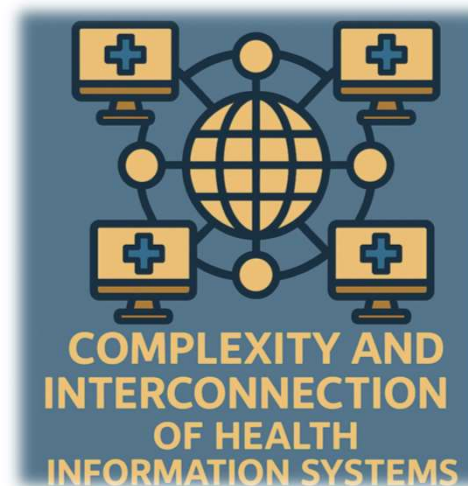
## Why are they Attacking Us ? Complexity

# Organizational Complexity and Interconnection

Multiple actors: hospitals, health authorities, labs, general practitioners, pharmacies, insurers, external providers — all interconnected and sharing data.

Rapid adoption of digital technologies: telemedicine, cloud services, and electronic health records often implemented without sufficient security.

Third-party dependencies: software vendors, maintenance contractors, cloud or diagnostic providers are common vectors for indirect attacks (supply chain attacks).





SERVIZIO SANITARIO REGIONALE  
EMILIA-ROMAGNA  
Azienda Unità Sanitaria Locale di Reggio Emilia  
IRCCS Istituto in tecnologie avanzate e modelli assistenziali in oncologia



## What are the causes ? Visibility

### Visibility - Geopolitical or Ideological Motivations

**Cyberwarfare:** healthcare structures may be targeted in hybrid warfare contexts (e.g., Ukraine).

**Hacktivism:** ideological groups may attack healthcare institutions for ethical or political reasons (vaccines, abortion, privacy, etc.).



**GEOPOLITICAL AND  
IDEOLOGICAL  
VISIBILITY  
OF HEALTH  
INFORMATION SYSTEMS**



## What are the causes ? Medical and InVitro Devices



1. Obsolete or Unsupported Operating Systems
2. Non-Upgradable Software and Unpatchable Firmware
3. Default Passwords or Weak Credentials
4. Unencrypted Communications
5. Insecure Remote Accessibility
6. Supply Chain Vulnerabilities
7. Lack of Network Segmentation
8. Risk of Operational Manipulation



SERVIZIO SANITARIO REGIONALE  
EMILIA-ROMAGNA  
Azienda Unità Sanitaria Locale di Reggio Emilia  
IRCCS Istituto in tecnologie avanzate e modelli assistenziali in oncologia



What are the causes ?

Complex digital ecosystem – Supply Chain

External Maintenance  
Provider

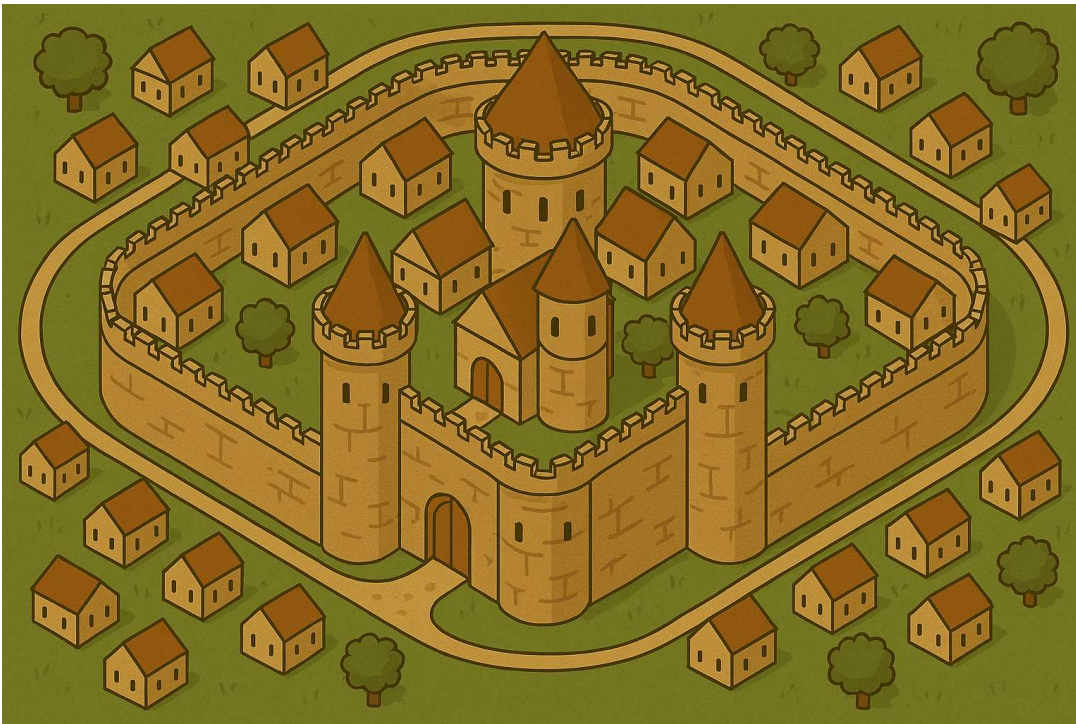
Operating System  
Manufacturer

Software Solution  
Manufacturer

External Quality  
Control Provider

LIS Integration  
Provider





## Not one system – many systems

*AUSL Reggio Emilia:  
220 IT systems  
>600 connected devices*

## Not one manufacturer/vendor – many manufacturers/vendors (with diverse technological background and level)

*AUSL Reggio Emilia:  
>400 manufacturers*

## Not all within the same scope/control (e.g. home care ! Outpatient outposts)

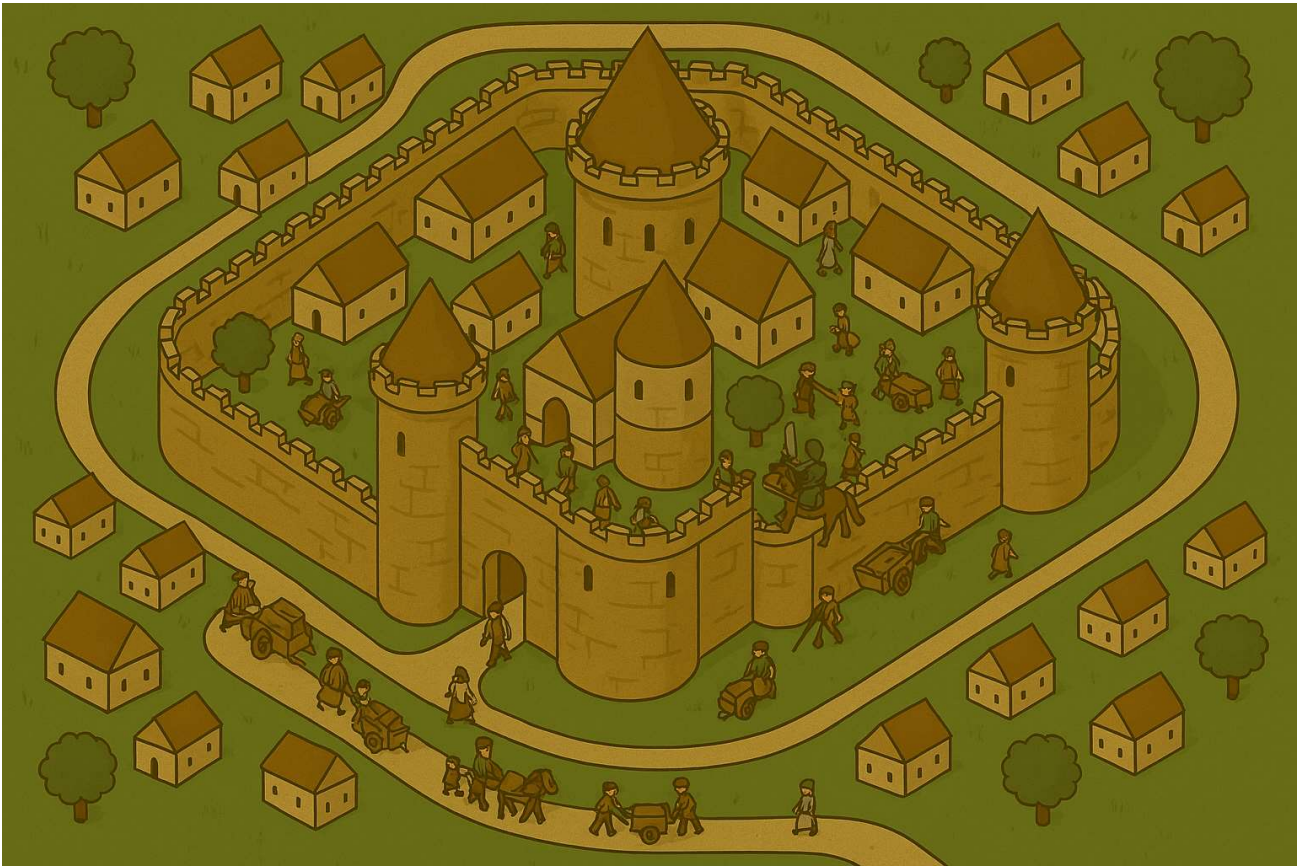
*AUSL Reggio Emilia:  
>200 network sites  
>300 connected external networks  
>300 external mobile clinical connections*



SERVIZIO SANITARIO REGIONALE  
EMILIA-ROMAGNA  
Azienda Unità Sanitaria Locale di Reggio Emilia  
IRCCS Istituto in tecnologie avanzate e modelli assistenziali in oncologia

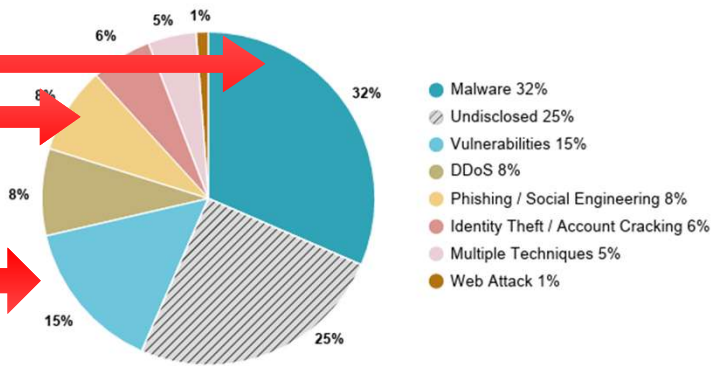


Today... an open ecosystem !





# Who has to fight the battle ?



© Clusit - Rapporto 2025 sulla Cybersecurity



SERVIZIO SANITARIO REGIONALE  
EMILIA-ROMAGNA  
Azienda Unità Sanitaria Locale di Reggio Emilia  
IRCCS Istituto in tecnologie avanzate e modelli assistenziali in oncologia



EMRAM 6  
HIMSS SOLUTION

Cybersecurity in Healthcare in the good old days...  
Isolation !

**... isolation and rigid use-cases !**



Palmanova, Italy





SERVIZIO SANITARIO REGIONALE  
EMILIA-ROMAGNA  
Azienda Unità Sanitaria Locale di Reggio Emilia  
IRCCS Istituto in tecnologie avanzate e modelli assistenziali in oncologia



## Cybersecurity in Healthcare in today world... Segmentation

**Segmentation  
requires  
mapping of processes  
and access limitation**





## Antimalware - Monitoring and Management



Client-based monitoring  
Server-based monitoring  
Network-based monitoring



### XDR – Extended Detection and Response

A unified security solution that integrates data from multiple sources (endpoints, networks, servers, cloud workloads) to provide centralized threat detection, investigation, and response.

### EDR – Endpoint Detection and Response

Focuses on detecting, investigating, and responding to threats on endpoint devices (like computers and servers). It provides visibility into endpoint activity and helps contain and remediate attacks.

### NDR – Network Detection and Response

Monitors network traffic to detect suspicious behavior and threats. It uses techniques like behavioral analytics and machine learning to identify anomalies and respond to network-based attacks.

### SIEM – Security Information and Event Management

Collects and analyzes log data from across an organization's IT infrastructure to detect threats, ensure compliance, and support incident response. It provides real-time monitoring and historical analysis.



But.. Most of the dangers come from inside !

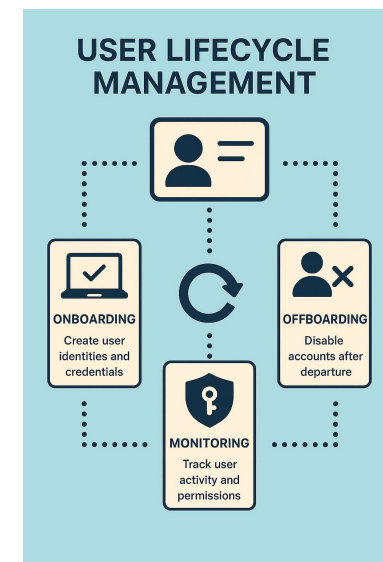
## Awareness of possible human weak-points



## Multi Factor Authentication

## Minimal Permissions

## Users lifecycle management





## Basic cyber hygiene practices and security training

As part of the cybersecurity risk management measures required by NIS2, entities must implement **security training programs for their staff**. This includes ensuring that personnel are aware of cyber threats, know how to respond to incidents, and follow best practices in cyber hygiene.





SERVIZIO SANITARIO REGIONALE  
EMILIA-ROMAGNA  
Azienda Unità Sanitaria Locale di Reggio Emilia  
IRCCS Istituto in tecnologie avanzate e modelli assistenziali in oncologia



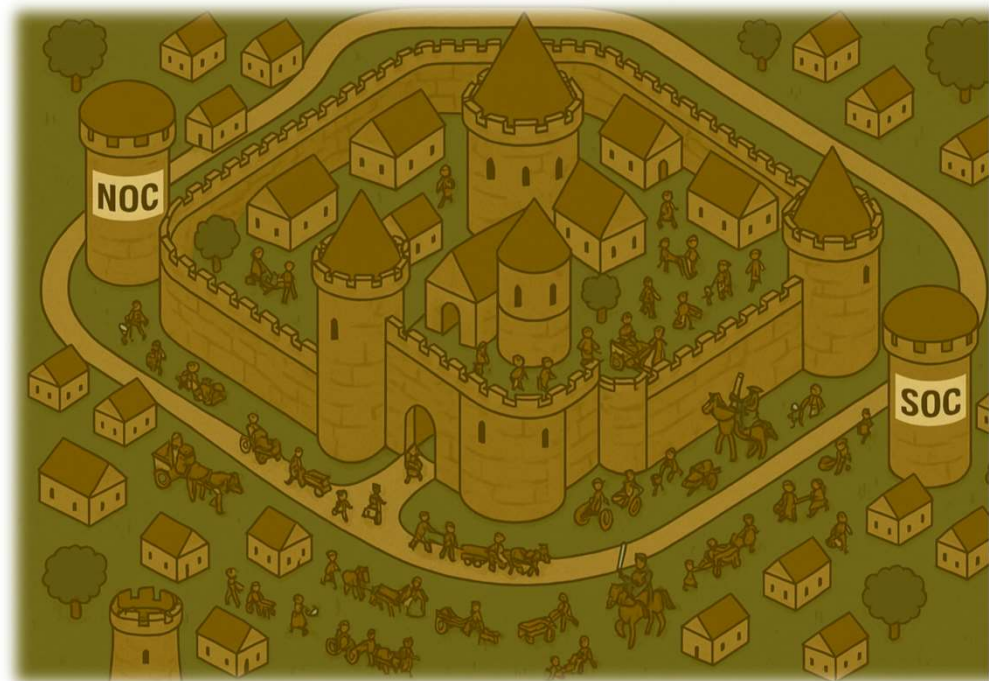
Some help..  
NOC and SOC

# Network Operations Center Security Operations Center

## Monitoring of:

- Abnormal network traffic / behavior
- Indicators of Compromise

## Fast Response





## First step: awareness of possible weak-points



**Vulnerability Assessment**



**Penetration Test**



From this step a **Cybersecurity Development Plan** is drafted and implemented

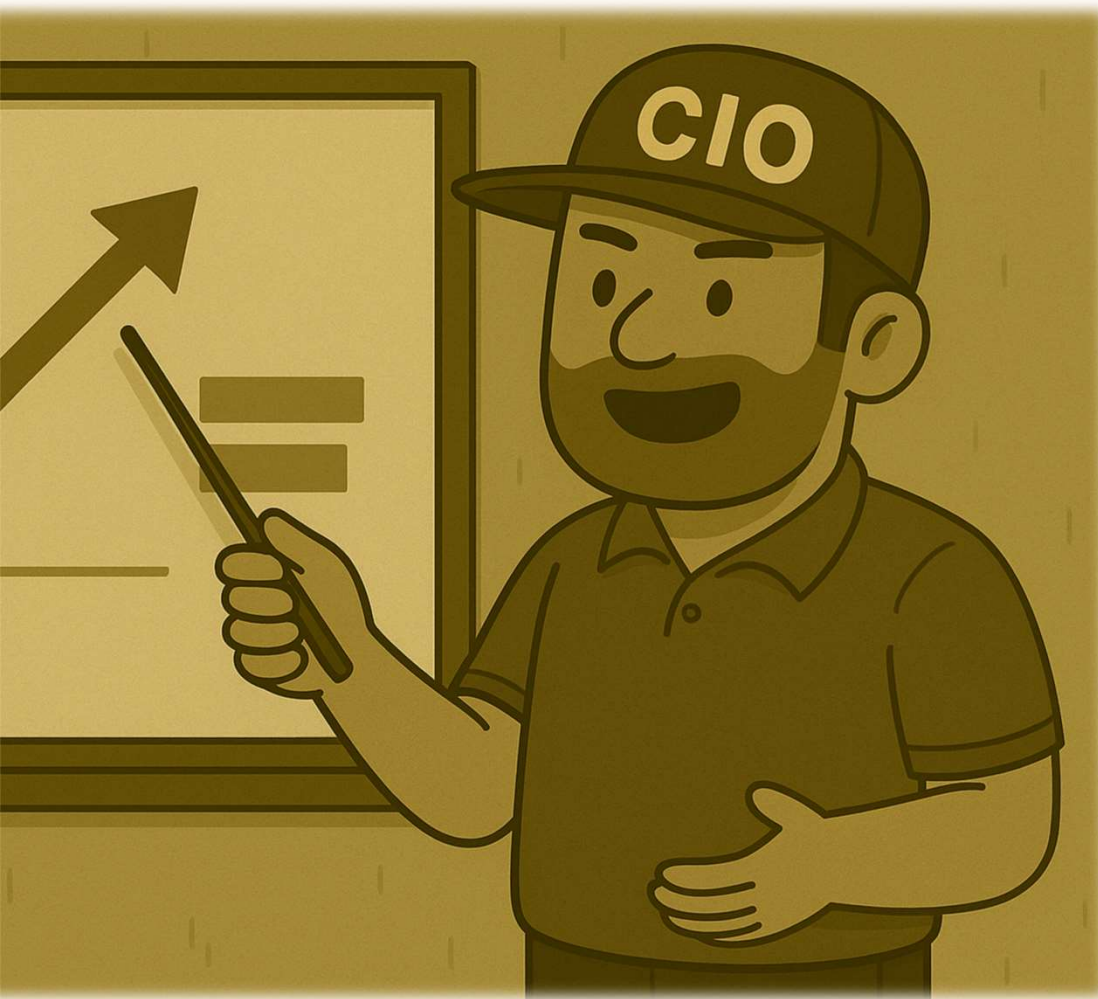


... and be ready to fight the battle !

**What to detect**  
**How to report it**  
**What to do immediately**  
**(Immediate/Fase Response)**

**Contingency Plan**





**We are a relevant target for cyber-criminals**

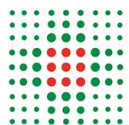
**Cybersecurity is a growing issue**

**Issue is NOT ONLY loss of data**

**We cannot close everything**

**Everybody has to actively pursue cyber-security measures**

**We have to be ready !**



SERVIZIO SANITARIO REGIONALE  
EMILIA-ROMAGNA  
Azienda Unità Sanitaria Locale di Reggio Emilia  
IRCCS Istituto in tecnologie avanzate e modelli assistenziali in oncologia



Thank you  
Any questions ?

つづく