

SURVEY ANALYSIS



CISO's Challenges & Priorities: Health



This document is the result of an **EU-wide survey** of **+100 contributions** of CISOs or equivalent, from a wide range of sectors.

It proposes both a **deep dive sector** by sector analysis and a set of **cross-sector recommendations**.

[READ THE REPORT](#)

⚠️ Top cyber threats in the health sector

- DDoS Attacks
- Obsolescence, vulnerability Management
- Phishing
- Data Leakage, (Patient) Data Loss
- Malware, Ransomware

🚶 Top cyber challenges in the health sector

- **Low funding priority** - Cybersecurity is a luxury for the health sector
- Lack of **qualified staff**
- **Big dimensions** of the organisations and the **big geographic distribution** of the infrastructure
- Boards do not know the importance of cyber threats.



In-company & Governance Challenges / Priorities for CISOs

🔍 Focal point 1

Certification

- **Certification is not considered a priority** or a good representation of the organisation's cybersecurity state.
- **Cyber ranges** or technical exercises are not widely used in the sector at all.
- CISOs must have the ability to **make long-term plans, adapting good practices and methodologies** of managing risks and of security of information to the particularities of their organisation.

🔍 Focal point 2

Code of Conduct for CISOs

- The priority is to **implement a good governance** in the sector and therefore ensure that a CISO position exists.
- CISO must **align cybersecurity with the objectives and priorities of the organisation**, create and design security policies and norms to be followed across the entire organisation.
- Clear and measurable cybersecurity objectives should be assigned to all employees

🔍 Focal point 3

Board of Directors

- Boards do **not have enough knowledge of cyber threats** and consequences.
- Boards prioritise budgets targeting the health of patients and associated needs with **no room left to invest in cybersecurity**.
- Boards should have **mandatory annual cybersecurity and IT-related training**
- Create **cybersecurity & IT departments** under the CISO management.

🔍 Focal point 4

Information sharing

- Step by step approach: starting with the need to **create healthcare security teams to facilitate information sharing** and create a **portal or tool where information could be accessible**.
- Implement an **ISAC** with the establishment of a single point of contact and bottom-up information sharing.
- Build trust and **ensure information sharing between public and private sectors**.

🔍 Focal point 5

Procurement

- **Performance, cost, maintenance, system integration, and source/provider** are the main criteria for procurement
- **Importance to rely on validated European solutions and standards** related to the communication between healthcare devices and the sharing of medical information.



Cooperation Challenges / Priorities for CISOs



Further reading from ECSO

ECSO Sector Report **Healthcare sector report: Cybersecurity for the healthcare sector**