SURVEY ANALYSIS

CISO's Challenges & Priorities: Energy

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 energy sector

- Social engineering attacks
- Ransomware
- Technological complexity
- Insider threat
- Data breaches

Top cyber challenges in the energy sector

- Lack of cybersecurity culture **and awareness**
- Insufficient budget allocation by Boards **for in-company** awareness and **training programmes.**
- Lack of cybersecurity skilled staff
- Challenges of **network and technology complexities** for ICT security network framework

In-company & Governance Challenges / Priorities for CISOs

Focal point 1

Certification

- Companies favour a **risk-based approach** rather than a **certification-based approach** with internal audits, vulnerability assessments, pen testing for a continuous evaluation of risk levels
- Companies prefer a **certified process** over **certified components**
- CISOs are **not always involved in the certification process** of their company

Focal point 2

Code of Conduct for CISOs

- Set **mandatory minimums for compliance rules**.
- **Clear allocation of cybersecurity roles and responsabilities** in companies under the CISO leadership.

Focal point 3

Board of Directors

- **Insufficient investments** in cybersecurity
- Low level of Boards **awareness of cybersecurity threats and consequences.**.
- Lack of clear understanding in business terms why **cybersecurity can be a business enabler** and not a detractor.
- CISOs must learn to **report in business-like terms** to ensure that risks are quantified and investments justified.

Cooperation Challenges / Priorities for CISOs

Focal point 4

Information sharing

- CISOs need to start working together and exchange expertise, possibly through the creation of a **European forum and CISO information channel**.
- CISOs could use a **specialised platform with strong authentication architecture** for an in-depth exchange of information
- Increase of **collaboration between OES, Law Enforcement Agencies, the national authorities, and the EU**.

Focal point 5

Procurement

- Main criteria are: **cost/cost-benefit, performance, trusted source of origin, necessity and guarantee of quality from other organisations**
- Importance to use **EU certified solutions** for the **trusted management of sensitive data**.
- European solutions and services are preferred for **sovereignty, autonomy, availability of customer support, and necessity for regular updates**.

Further reading from ECSO

ECSO Sector Report
Energy networks and smart grids: Cybersecurity for the energy sector

ECS
EUROPEAN CYBER SECURITY ORGANISATION