A snapshot of Cybersecurity in the EU

A Eurelectric short paper

November 2024

eurelectric
powering people

In summary,

- **Cyberattacks are on the rise**. In the energy sector, a doubling was observed from 2020 to 2022. Countries in the EU are more frequently becoming the target of these attacks, and the majority of global attacks are currently performed by Russian actors.

- **The EU energy sector invests more in information security than other sectors**, but it must continue to grow in accordance with its extensive IT systems. **Across sectors, the EU invests less than North America and the Asia Pacific in information security investments.**

- **The EU has a multitude of legislative dossiers and institutions in place** on cybersecurity, with as many as seven dossiers proposed or reviewed in the last EU mandate.

- **Moving forward, the EU should: ensure consistent and harmonised implementation, foster a skilled cybersecurity workforce, facilitate the necessary investments and promote collaboration.**

Eurelectric represents the interests of the electricity industry in Europe. Our work covers all major issues affecting our sector. Our members represent the electricity industry in over 30 European countries.

We cover the entire industry from electricity generation and markets to distribution networks and customer issues. We also have affiliates active on several other continents and business associates from a wide variety of sectors with a direct interest in the electricity industry.

We stand for

The vision of the European power sector is to enable and sustain:
- A vibrant competitive European economy, reliably powered by clean, carbon-neutral energy
- A smart, energy efficient and truly sustainable society for all citizens of Europe

We are committed to lead a cost-effective energy transition by:

investing in clean power generation and transition-enabling solutions, to reduce emissions and actively pursue efforts to become carbon-neutral well before mid-century, taking into account different starting points and commercial availability of key transition technologies;

transforming the energy system to make it more responsive, resilient and efficient. This includes increased use of renewable energy, digitalisation, demand side response and reinforcement of grids so they can function as platforms and enablers for customers, cities and communities;

accelerating the energy transition in other economic sectors by offering competitive electricity as a transformation tool for transport, heating and industry;

embedding sustainability in all parts of our value chain and take measures to support the transformation of existing assets towards a zero carbon society;

innovating to discover the cutting-edge business models and develop the breakthrough technologies that are indispensable to allow our industry to lead this transition.

Dépôt légal: D/2024/12.105/28

WG Sustainable Network Technology
SGTF EG2 Eurelectric representatives

Contact:
Jessica GARCIA, Advisor - Distribution & Market Facilitation –
Jgarcia@eurelectric.org

Cybersecurity Snapshot

Electricity infrastructure stands as one of society's most critical sectors, requiring continuous functioning and stable operations. The need to maintain a secure sector is key, as a worst-case scenario outcome from an attack could lead to blackouts, causing widespread disruptions and significant societal issues. The digital transition along with decentralisation and international geopolitical tensions has, among other factors, brought the World Economic Forum to recently consider cyber insecurity identify cyber insecurity as the **fourth most severe risk** in the coming two years[1].

Cyberattacks are increasingly being used as a modern type of warfare. In Ukraine, the digital attacks have been complemented by simultaneous missile attacks, causing severe effects for civilians (Wired, 2023). The increase of malicious attacks from government supported hacker groups has not been limited to Ukraine. Globally, the attacks of Russian origin amounted to 61 percent of all recorded attacks in 2023 (Thales, 2023).

The frequency of cyberattacks has been escalating swiftly in the last years. The IEA has estimated **the attacks to have more than doubled between 2020 and 2022,** with a record of 1101 weekly attacks globally towards utilities in 2022.

Out of all geographical targets, the EU countries rose from 9,8 percent to 46,5 percent during six months in 2023 (Le Monde, 2023). More than 20 successful cyber-attacks took place towards European energy utilities during 2022 (EnergiCERT, 2022). The publicly available data is not comprehensive due to the sensitivity of the topic. To illustrate the potential impact of a successful cyberattack, in 2023, Russian attackers carried out the largest known cyberattack on Danish critical infrastructure, gaining access to the systems of 22 energy companies (SektorCERT, 2023).

Since 2022, according to EnergiCERT, the energy sector' cyber security centre, have counted the following:

48

Publicly known attacks against European energy and supply companies

31

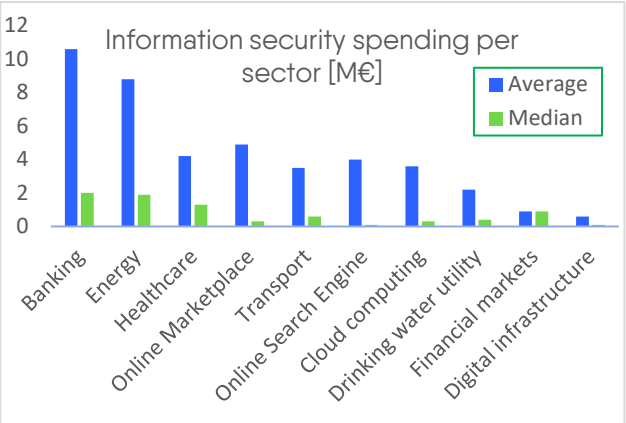
Ransomware attacks 13 out of them include data theft

15

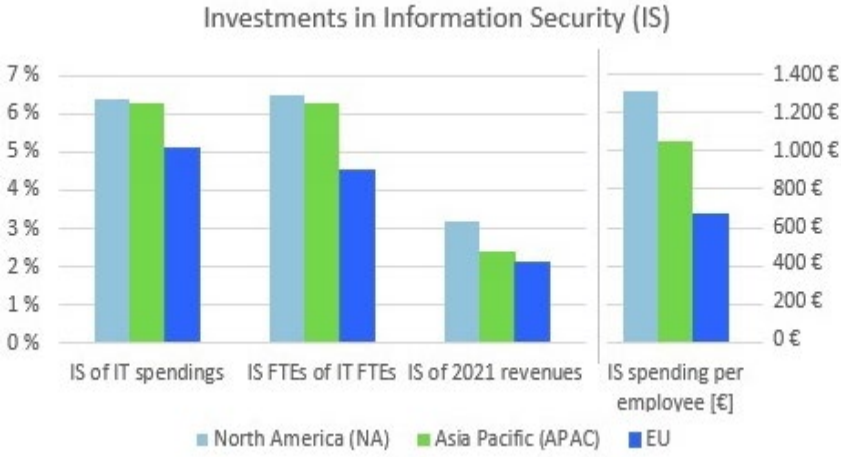
Attacks that affected operational technology (OT) of networks

[1] Top 3 are 1) misinformation and disinformation, 2) extreme weather events 3) societal polarisation, Global Risk Report 2024, WEF

Europe's cybersecurity agency ENISA recently highlighted that the **EU energy sector, in par with the banking sector, is investing more funds in information security measures** than sectors such as healthcare, transport and drinking water utilities (see figure).



However, globally and across sectors, EU is investing less in information security in comparison to North America and Asia Pacific. The figure below showcases different measurements of investments in four different categories.



For instance, out of the FTEs allocated to information security out of the total FTEs in IT, the EU earmarks only 4,5 percent in comparison to North America and Asia Pacific earmarking 6,5 and 6,3 percent respectively.

Data sourced from ENISA, NIS INVESTMENTS Cybersecurity Policy Assessment, p. 9 (2023).

A Eurelectric report found that **Distribution System Operators (DSOs) demonstrate the highest level of digital maturity in cybersecurity measures compared to other aspects of their digital transformation efforts** (2024). As the digitalisation journey continues, the cybersecurity efforts will need to increase.

Enhancing our ICT systems requires not only increased investments but also a proficient and skilled workforce. In 2022, the European Commission estimated the shortage of cybersecurity professionals in all sectors in the EU ranged between 260,000 and 500,000, while the EU's cybersecurity workforce needs were estimated at 883,000 professionals.

Regulation

There is an extensive amount of legislation and certification schemes relevant to ensuring a protected power sector. Mainly, legislation is set out on the EU level. The main and first cross-sectoral legislation is the **Directive on security of Network and Information System (NIS Directive)** which was adopted in 2016. It aims to achieve a high common standard of network and information security across all EU Member States. The NIS Directive has been recently updated (NIS 2), with changes entering into force in 2023, and mandating national transposition by Oct 2024.

During the past EU legislative term, several pieces of cybersecurity legislation for the EU were published or proposed. Some of which will bring large numbers of entities into the regulatory scope of national authorities. This will require considerable effort for compliance. The main regulation can be summarised as the amendments to the **Cybersecurity Act, the Cyber Resilience act (CRA), partly the Cyber Solidarity Act (CSA) and the network code on cyber security (NCCS)**.

Initiated	Legislation	Description	Status
Amendment Proposed April **2023**	The EU Cybersecurity act	Amendment introduced certification framework for ICT products, services and processes	In force, Review by June 2029
Proposed April **2023**	EU Cyber Solidarity Act	For EU institutions to increase attack response	Awaiting publication in Official Journal
Proposed Sept **2022**	Cyber Resilience Act	Requirements for hardware and software	Awaiting publication in Official Journal
Proposed Dec **2020**	NIS2 Directive The directive on security of network and information systems	Cross-sectoral legislation, for cyber and resilience	In force, applicable Oct 2024. Review by Oct 2027
Proposed June **2019**	The Network Code on Cybersecurity	Rules on preparedness, response and reporting for the electricity sector	In force June 2024, several guidelines awaited.
Proposed 2016	Risk-preparedness in the electricity sector	Rules for MS cooperation preventing, preparing for, and managing electricity crises.	In force June 2019. Review by Sept 2025

Governance

There are as many as 12 enforcement mechanisms and agencies involved in ensuring cybersecurity across Europe*. That could be regrouped into three subcategories: EU institutions, advisory bodies and networks of Member States.

Among the EU institutions, there are four main entities with varying tasks. **The European Union Agency for Cybersecurity, ENISA**, is the EU agency dedicated to achieving a high common level of cybersecurity across Europe. For the EU bodies and agencies, **CERT-EU** ensures emergency responses. **The European Cybersecurity Competence Centre, ECCC,** is an executive agency aiming to increase cybersecurity capacities and competitiveness. **The European Defence Agency (EDA),** is the agency working with the Unions' overall defence, including cyber resilience.

In addition to the abovementioned institutions, there are four advisory bodies and four different networks of Member States working with cybersecurity on EU-level.

In the intersecting field of energy and cyber, The European Commission has a so-called **Smart Energy Expert Group, SEEG**, whose mission is to accelerate the digitalisation of the energy system. The expert group was formally created under the digitalisation of the energy Action Plan. The subgroup under the SEEG called Working Group Cybersecurity will provide recommendations and guidance to the Commission on cybersecurity for energy systems. This encompasses evaluating the ramifications of new legislative initiatives in the field and exploring how best to address related challenges.

** The 12 are: CERT-EU, European Cybersecurity Competence Centre (ECCC), European Defence Agency (EDA), EU Agency for Cybersecurity (ENISA), European Cyber Shield, European Cybersecurity Certification Group (ECCG), Interinstitutional Cybersecurity Board (IICB), NIS cooperation group, Interinstitutitonal Information Security Coordination group, Network of National Coordination Centres, CSIRTs network, EU CyCLONe*

eurelectric
powering people

Moving forward, we recommend following:

1. Allow the electricity sector time to fully implement the nearly completed regulatory framework before introducing new regulations. Propose regulatory improvements only when regulatory action is the sole solution, after validation of non-overlapping with another current regulation.

The electricity sector is becoming increasingly vital for Europe, as evidenced by the rising number of cybersecurity regulations focused on it. The sector now needs time to fully implement the new framework. Regulations should only be developed or changed in case of a specific need that the sector does not cover and cannot implement alone. In a few years, the feedback will allow for improvements in this framework. For now, it is important to promote these regulations and implement the corresponding measures.

2. Recognising escalating threats by fostering a skilled workforce and facilitating essential investments

The cybersecurity industry requires a boost in its skilled workforce to effectively address evolving threats. Eurelectric welcomes the implemented Skills Academy to address this issue. Moreover, there is an urgent need to enable the necessary investments that will empower the industry to effectively cope with the heightened risk landscape. **The national regulatory frameworks must acknowledge and adequately reward the increased costs** arising from cybersecurity measures and compliance of all cyber legislations.

3. Continuing to put cybersecurity at the top of the agenda by improving collaboration

We welcome the NIS 2 directive and network code on cyber which will facilitate this collaboration and exchange. Ensuring security and working proactively is an essential task for all parts of the value chain in the power sector and across the continent. A chain is as strong as its weakest link, which is why the European power sector advocates for EU-wide cooperation and coherent legislation, **that needs to be implemented and coordinated in an efficient way by the MS**.

Energy transformation, meaning both energy transition and electrification of new uses, will lead to major investments across the sector. These investments must include cybersecurity by design with stable regulations and standards. To support this, we welcome the finalisation of the Cyber Resilience Act.

To further enhance collaboration, a mapping of the different EU enforcement mechanisms and agencies should be conducted to clarify the different roles that each body plays. The EU has established many new advising bodies to support the implementation of new legislation.

Union of the Electricity Industry - Eurelectric aisbl
Boulevard de l'Impératrice, 66 – bte 2 - 1000 Brussels, Belgium
Tel: + 32 2 515 10 00 - VAT: BE 0462 679 112 • www.eurelectric.org
EU Transparency Register number: 4271427696-87