WEBINAR ON

DATA PROTECTION FOR POWER UTILITIES

Organised By

GSEF Global Smart Energy Federation

APUA ASEA

12th April, 2023

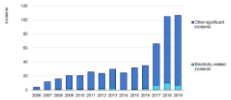
Speaker : Alexis RECHAIN, Str@tec-arc

INTRODUCTION

- The energy sector, and in particular the Utilities sub-sector, is composed **of infrastructure considered "vital"**. It provides access to a range of **essential services**, from health care to banking to transportation. A secure supply of electricity is therefore **of paramount importance** for States and citizens.
- **Digitalization offers many advantages** for the new environment of energy (and electric) systems and for consumers: **improved efficiency, cost savings and reduced downtime** ...
- **The significant increase in connected devices and distributed energy resources** – such as distributed generation, smart metering, behind-the-meter storage – is **expanding the potential surface of cyberattacks on electrical systems**. Increased connectivity and automation throughout the electrical system could also make them **more vulnerable** to cyberattacks.
- **Are we prepared? Are our data and systems safe?**

CONTEXT

- The African Union has adopted in 2014 the Malabo convention on cyber security and personal data protection, but it is yet to come into force as less than 15 countries have ratified it.
- The International Energy Agency's (IEA) 2020 report, "Power systems in transition", lists the **major cyberattacks** of the period 2006 – 2019, highlighting those that targeted the energy sector, which are **increasingly frequent**.



- Representatives of the energy sector are **more worried about the risks of cyberattacks than before Russia's invasion of Ukraine**, according to DNV “Cyber Priority – The state of cyber security in the energy sector” report (2022), which suveyed 948 energy professionals in 98 countries.
- In South Africa, in 2019, ESKOM faced a Trojan attack while Power City was the victim of a ransomware, shutting down the access to its prepaid system
- In Mali, in 2023, hackers have stolen 2 To of personal data from a bank in Mali, including personal data from VIPs. While some of the Senegalese TELCO regulator’s data were stolen in 2022, including personal data..

PRESENTATION

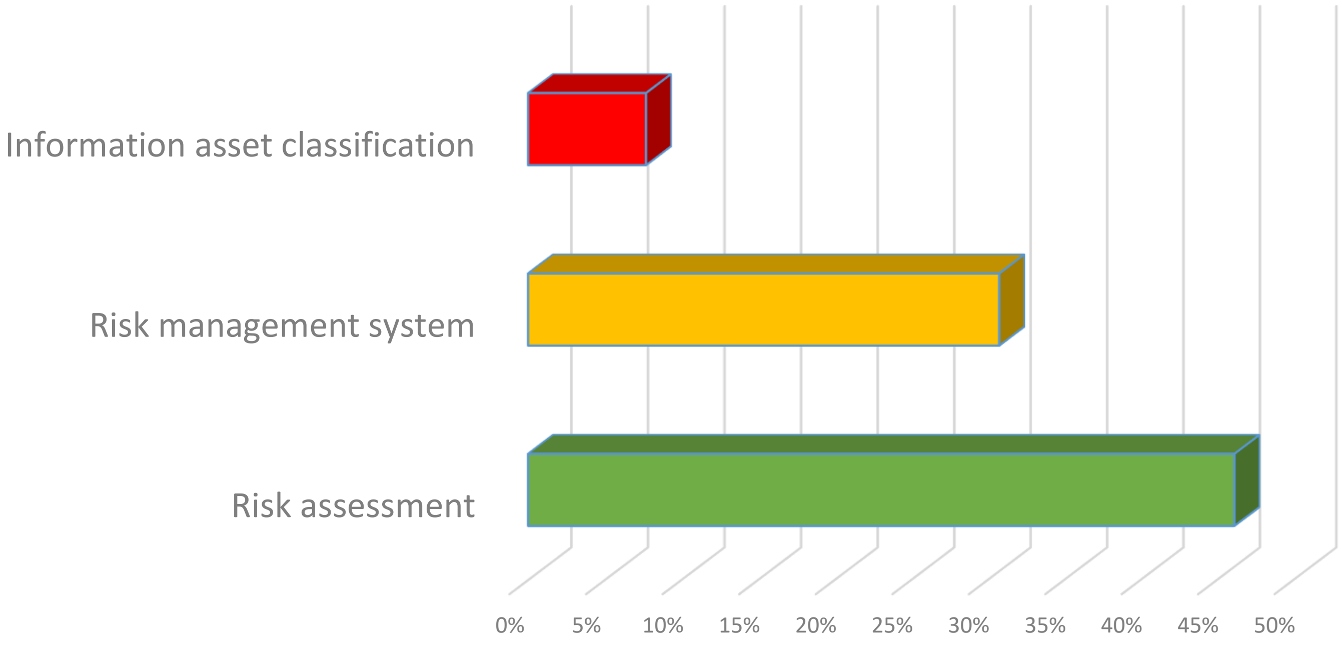
- **What about APUA members?**
- ***84.6%*** *of APUA member companies surveyed have* ***already suffered a cyber attack****. Nearly 40% say they are attacked* ***several times a year*** *!*
- ***46.15%*** *have already* ***lost data*** *due to a computer attack.*
- 53.85% claim to have an Information Security Management System (ISMS) but **only 7.7% of the sample is certified against ISO 27001.**
- 61.54% say they carry out security audits regularly but the **last audit dates back on average to ... 2018 !!!**
- 69.23% say they have a cybersecurity awareness and training program but **only 15.4% have an automated platform** for this type of activity.
- 38.5%: the percentage of companies with a **specific teleworking policy and security measures**

PRESENTATION

- **Allocated resources are limited**
- 69.3% of companies spend **less than 300 kEUR per year** on information security for an average turnover of 713 million EUR => 0.04%
- 2.08: the average number **of resources dedicated to information security**
- 2.08 resources on average = 1 **engineer** (but only 1 in 2 specialized in information security) **+ 1 IT technician**
- **Only 24.4% of** resources hold a **ISO 27001 certificate** (Foundation, Lead Implementer, Lead Auditor)
- 46.2% of companies spend **less than EUR 7,500 per year** on training IT and/or information security officers.
- 69.2% of companies spend **less than EUR 7,500 per year** on cybersecurity awareness and training for all agents.

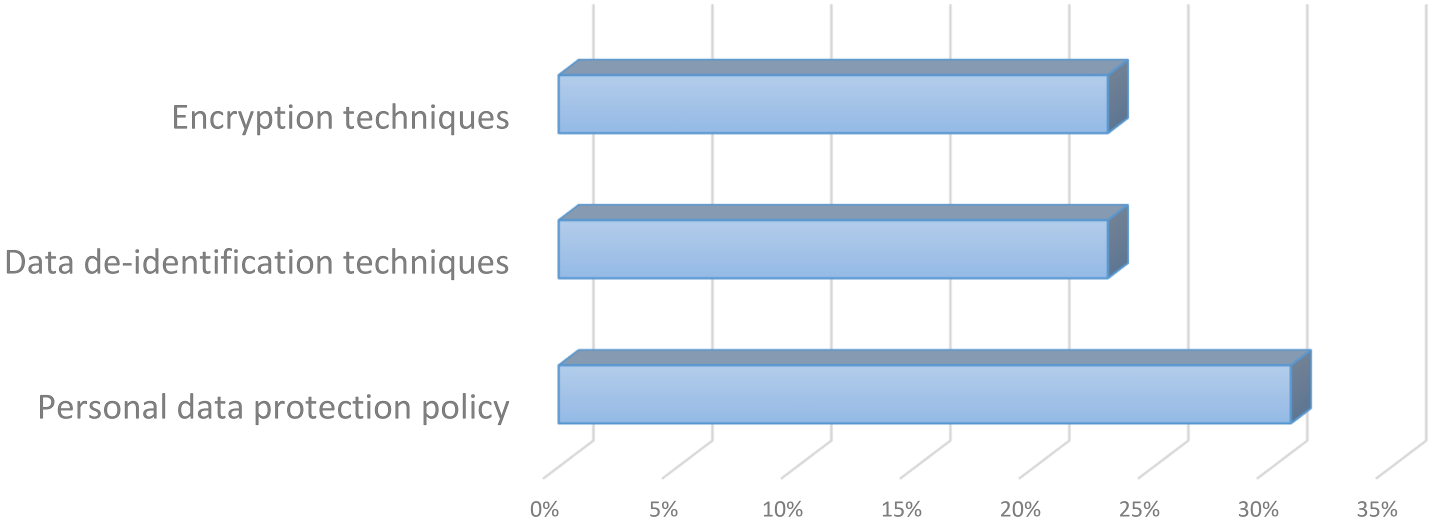
PRESENTATION

- **Risk management**
- While 46.2% of companies conduct an information security risk assessment, **only 30.7% have a risk management system and less than 8% have classified their information assets.**



PRESENTATION

- **Data protection**
- Only**30.8% of companies have developed a personal data protection policy and less than a quarter use data de-identification or encryption techniques,** while all use personal identifiers (e.g. telephone number, account number).
- Respondents rate their **level of competence in the application of personal data regulations at 5/10**.



KEY TAKEAWAYS/ RECOMMENDATIONS

- APUA member companies, like most companies in Africa, are making significant efforts in terms of digitalization, with a view to facilitating the user experience and improving operational efficiency. In doing so, they significantly increase their exposure area and related cybersecurity risks. The survey suggests member firms likely underestimate cybersecurity and data protection risks and must:

1. strengthen the skills of the actors in data protection and the fight against cyberattacks as well as the managerial organization for a better management of the cybersecurity risk;
2. In particular, improve the understanding of IT stakeholders regarding the industrial environment (OT/SCADA) in which they operate;
3. dedicate more financial resources to data protection and the fight against cyberattacks;
4. strengthen the involvement and leadership of leaders on these issues;
5. strengthen their cooperation and regularly share their experiences on this theme.

MOVING FORWARD

- APUA is developing services and projects to support its members in tackling information security and data protection issues:

1. Setting up an observatory on cybersecurity and data protection issues with an annual survey to monitor progress, incidents and trends;
2. Conducting sensitization activities towards the top management of its members on information security and data protection issues.
3. Developing specific curricula on information security and data protection through the African Network of Centers of Excellence in Electricity (ANCEE) and setting up an e-learning platform.
4. Setting up a task force to provide technical assistance services to members in order to improve information security and data protection management
5. Discussing with Technical and Financial Partners the development of a CSIRT network to provide assistance to its members in case of cybersecurity incidents

THANK YOU

For queries email at arechain@stratec-arc.com