PART D: Presentation of the 2nd Annual APUA Cybersecurity Survey for Utilities

Session Contents

- Results from the 2nd annual APUA cybersecurity survey for Utilities (2023)

Speaker:

Alexis RECHAIN

CEO Str@tec-arc

Introduction

Cybersecurity has a rising significance considering the use of ICTs for all aspects of Utilities daily business. Computer attacks and digital scams have increased alarmingly during these times of uncertainty.

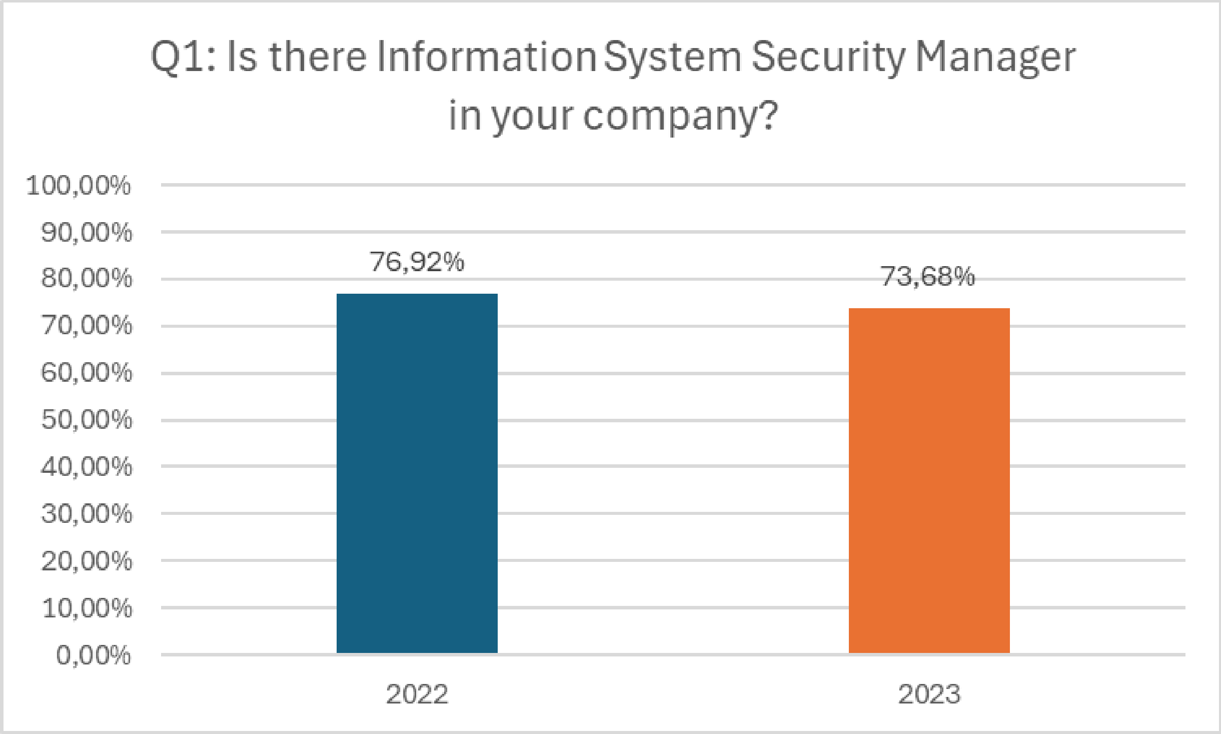
Electricity companies, members of APUA, on the other hand, are engaged in digital transformation efforts to improve user services and performance. By becoming electricity companies 2.0, they are more exposed to the threats of cyberspace.

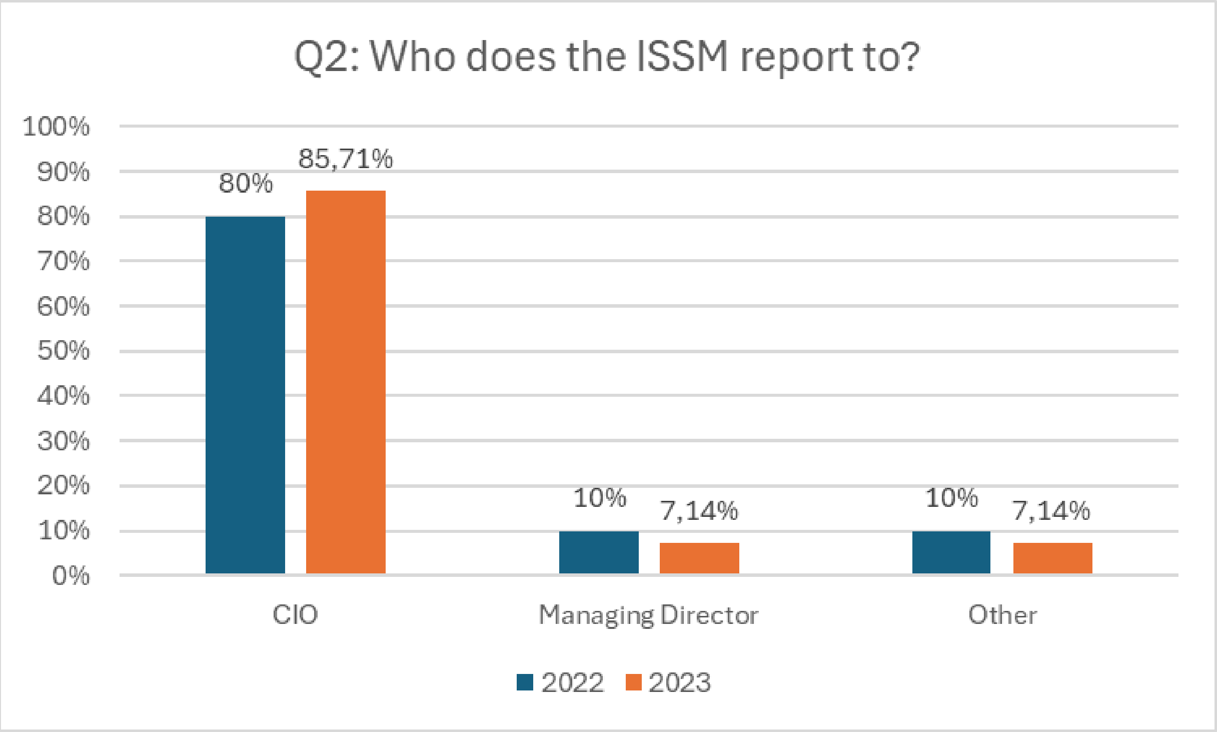
It is therefore becoming crucial for organizations to have frameworks in place to govern data protection and IT/OT systems. Putting in place adequate security and trust solutions is therefore one of the main challenges that must be addressed.

In 2022, APUA has organized its first survey on Cybersecurity issues for the Utilities. The presentation of the results of the 2nd survey aims at showing the evolution of both preparedness and threats amongst APUA members in 2023. The survey was conducted from Nov. 2023 till Jan. 2024. 20 companies (36% of members) shared their information, compared to 14 (25%) for the first survey.

So let’s share some of the results …

Are we better prepared or organized?

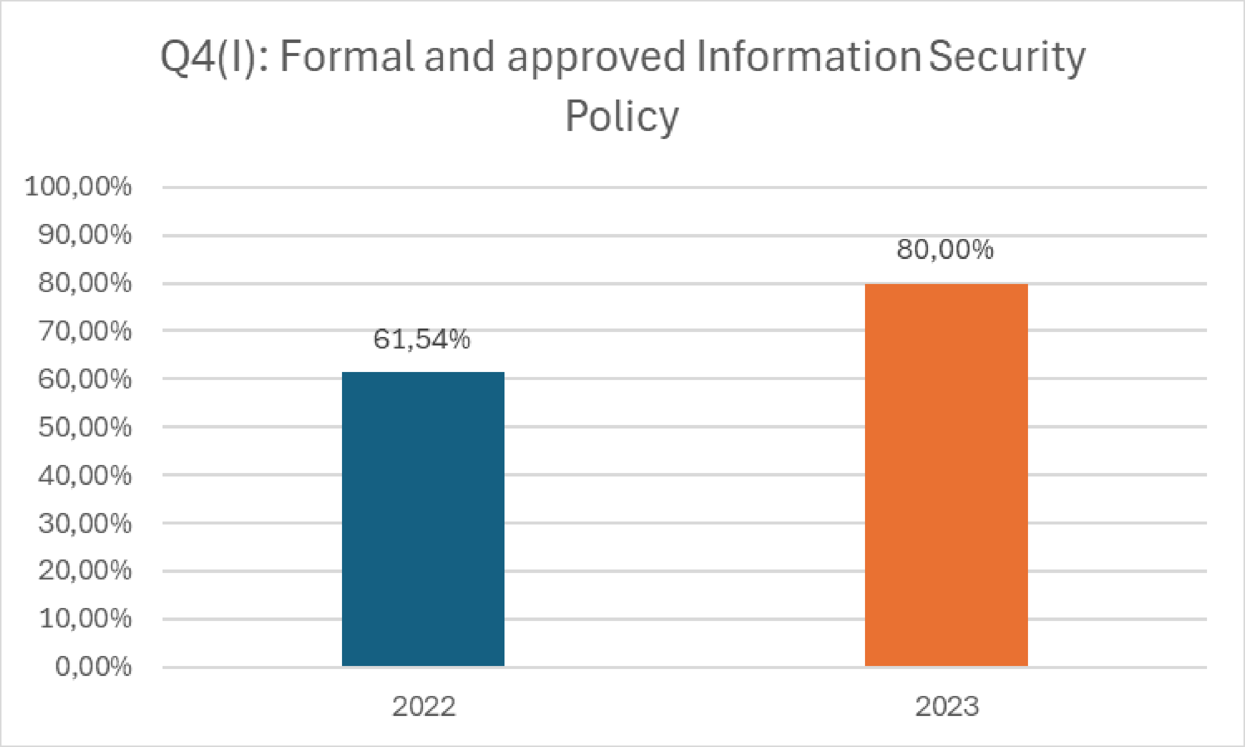


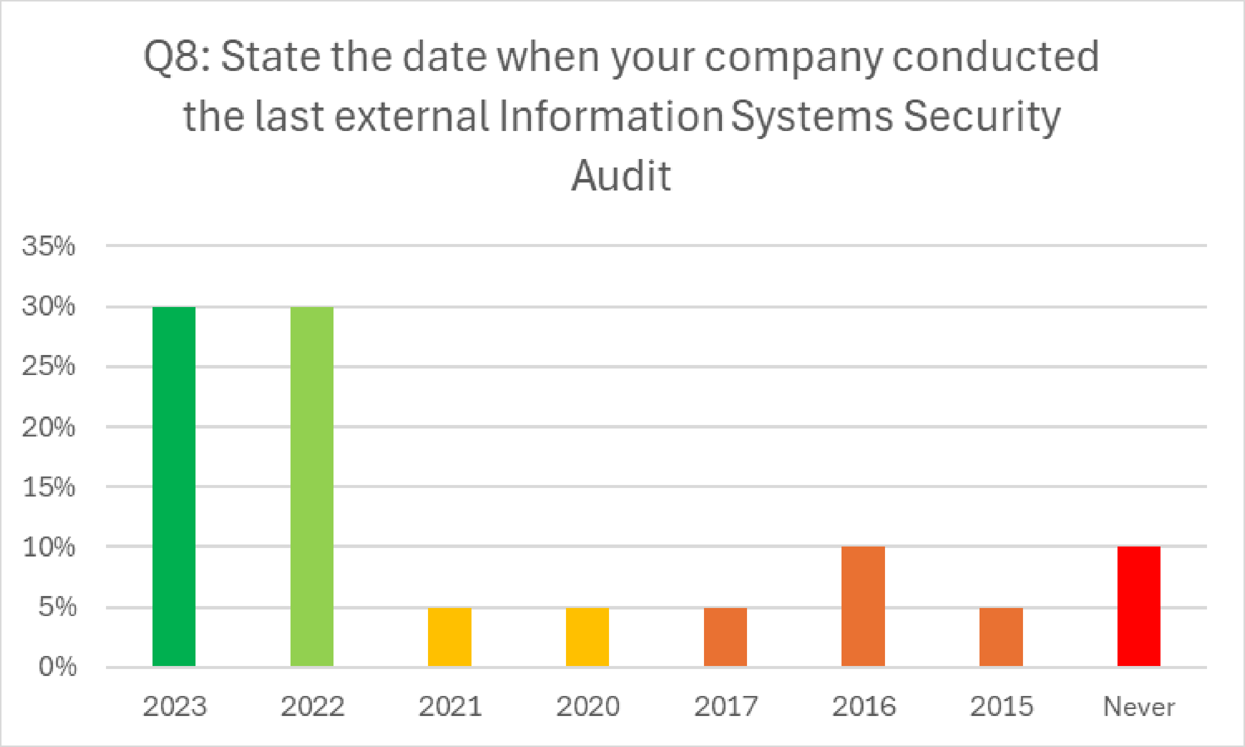


85,7% of the Information Security Officers report to the Chief Information Officer.

Is it the good level?

Are we better prepared or organized?

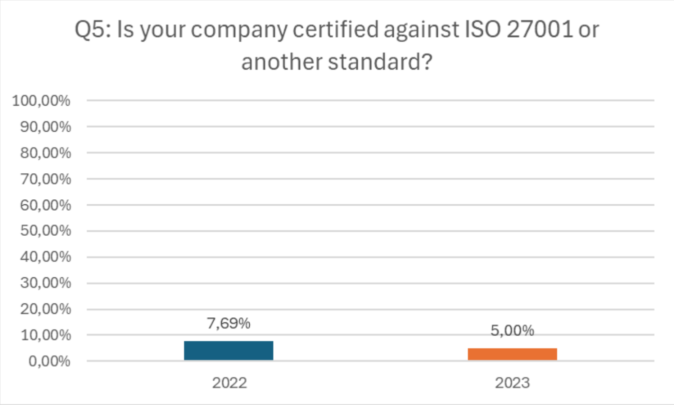




More members have an Information Security Policy.

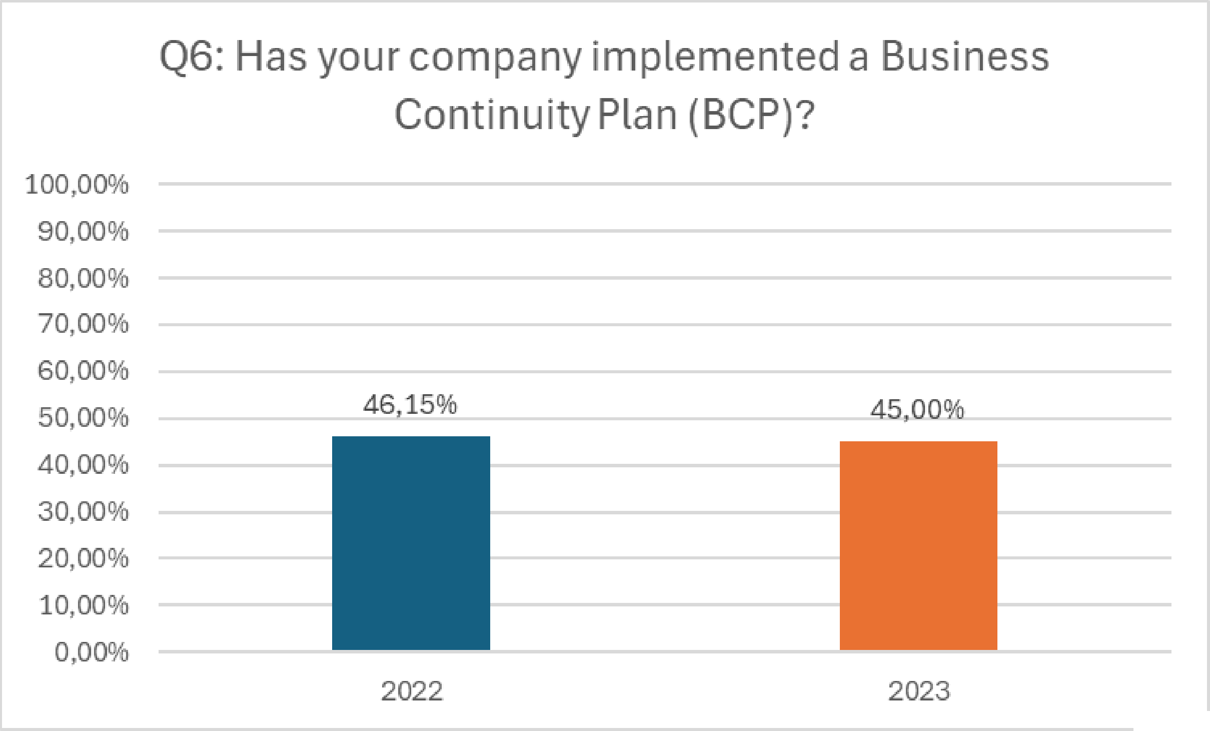
But the ISMS is still to be sanctioned by a certification.

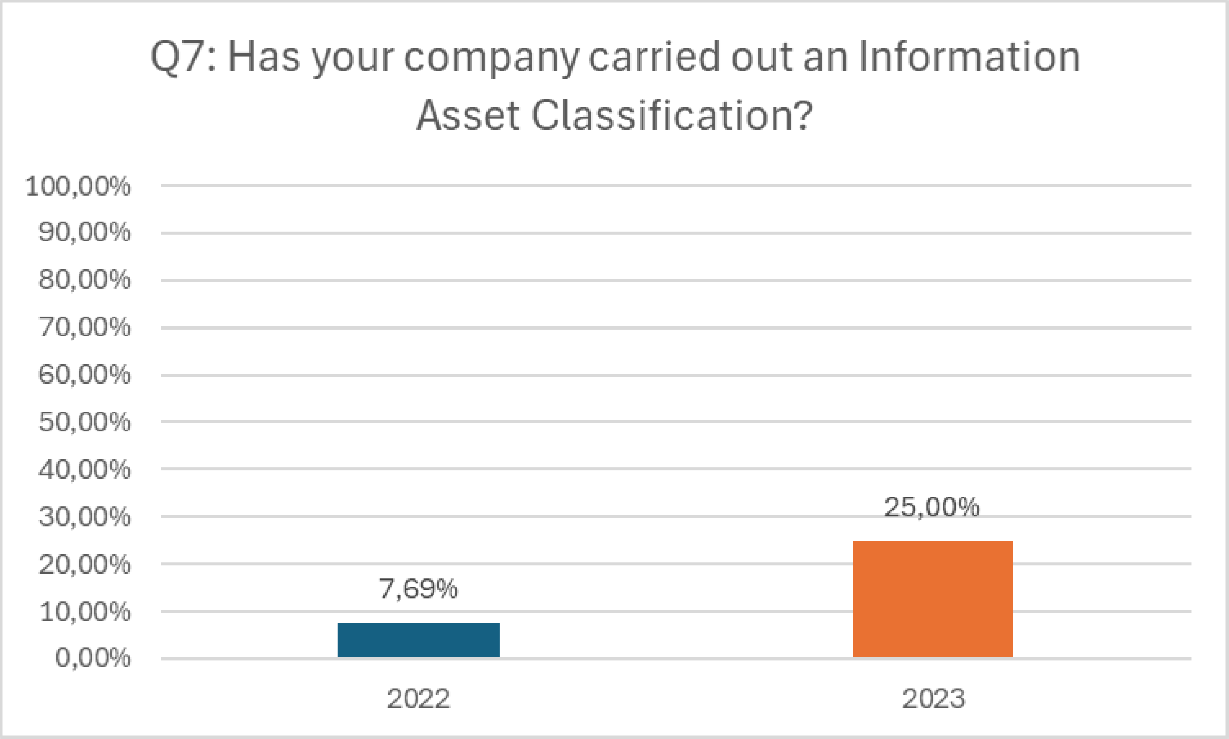
And audits are not performed on a regular basis (≠ policy?).



Are we better prepared or organized?

What if?

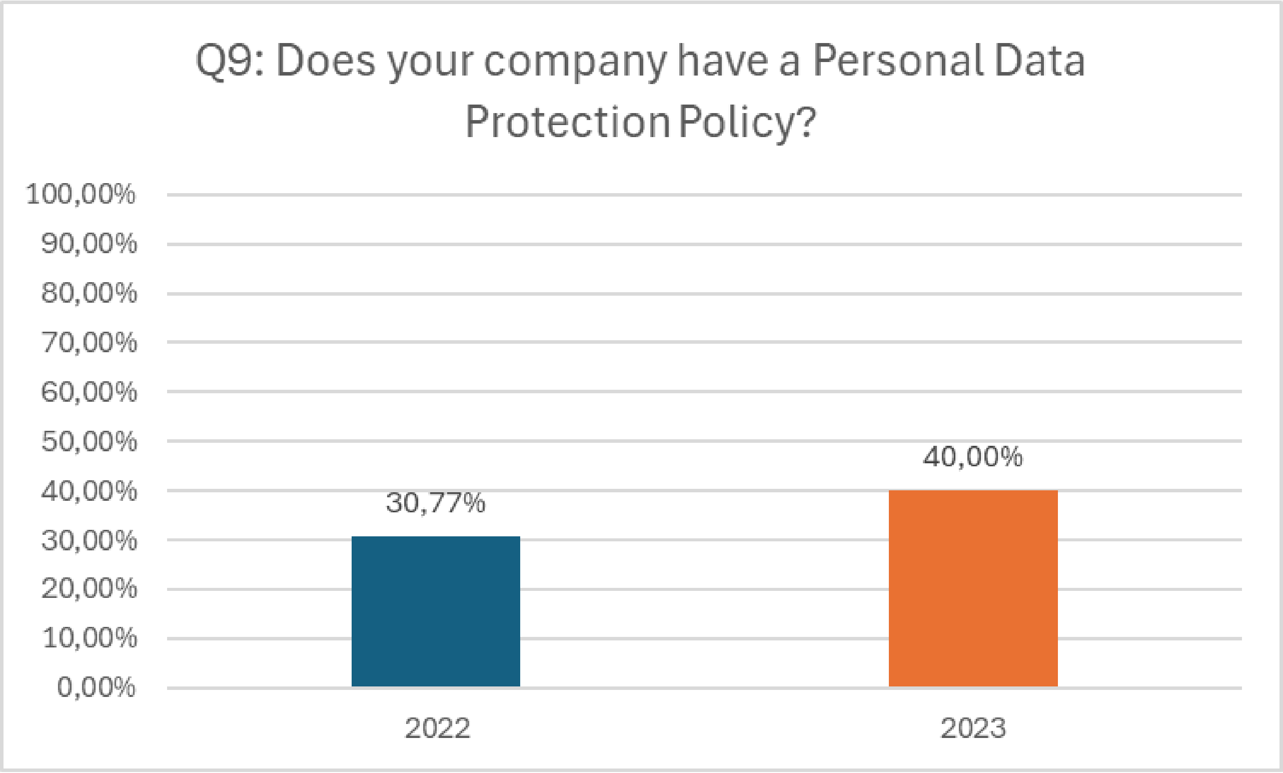




37,5% of members have experienced a major incident on their IT system for more than 12 hours. In 33% of cases, it happened several times during the year.

Knowledge of Information Assets has increased. Yet, to improve

Are we better prepared or organized?

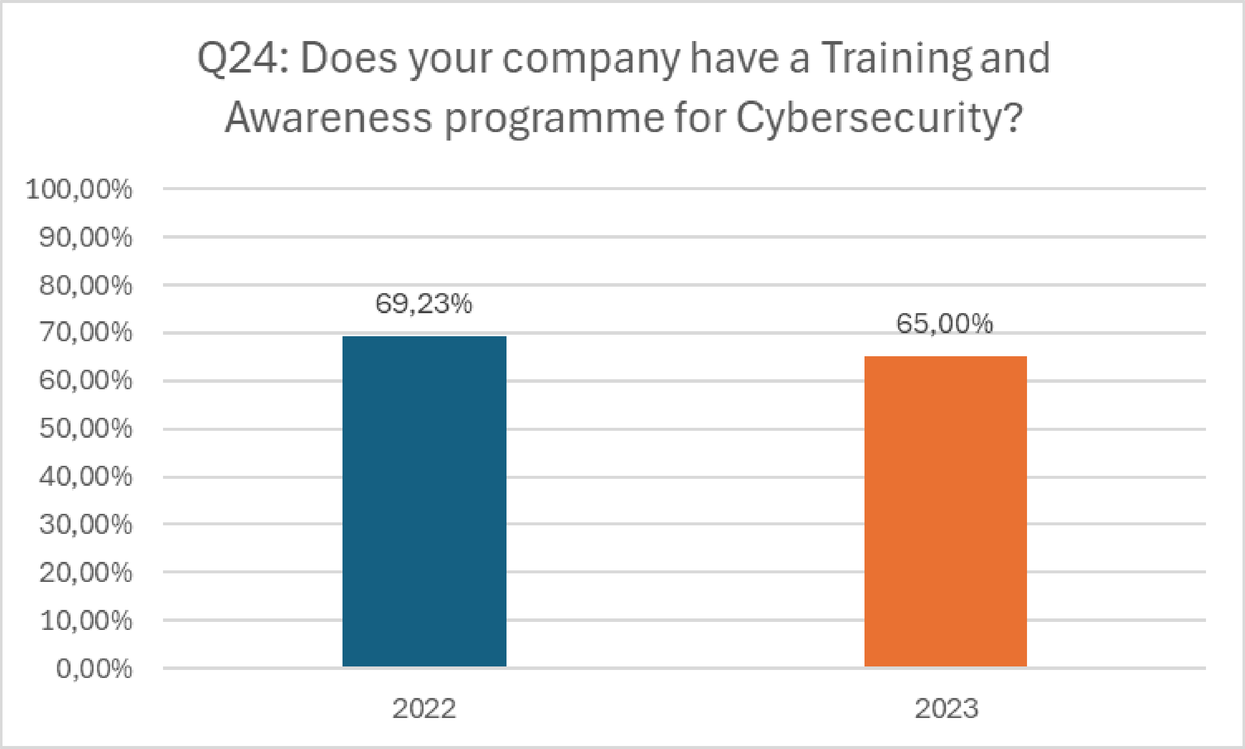


40% of members now have a DP

50% use protection techniques

- Encryption
- Pseudonymization
- Anonymization
- …

Are we better prepared or organized?



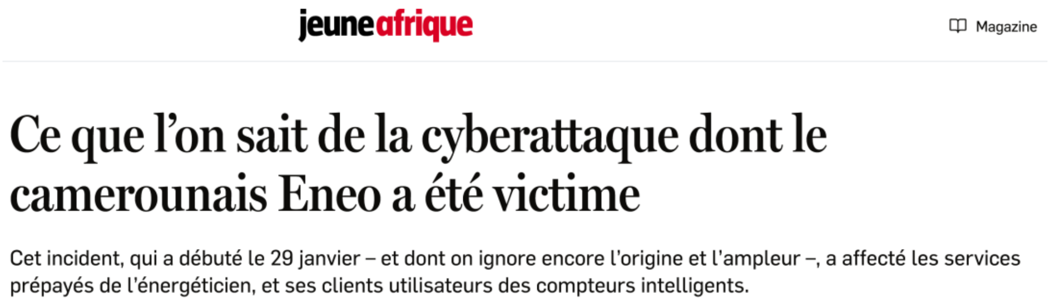
Stable, but we have to do more efforts

65% of members forecast an increase in the training budget

Remember: people (we) are the “weak link” in the cybersecurity fight.

How real is the threat?

Breaking news !!!

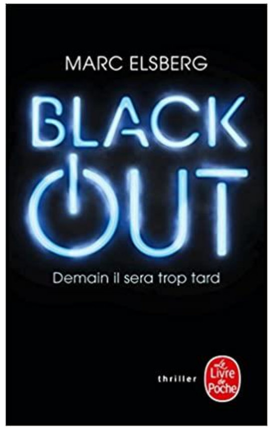


jeuneafrique

Magazine

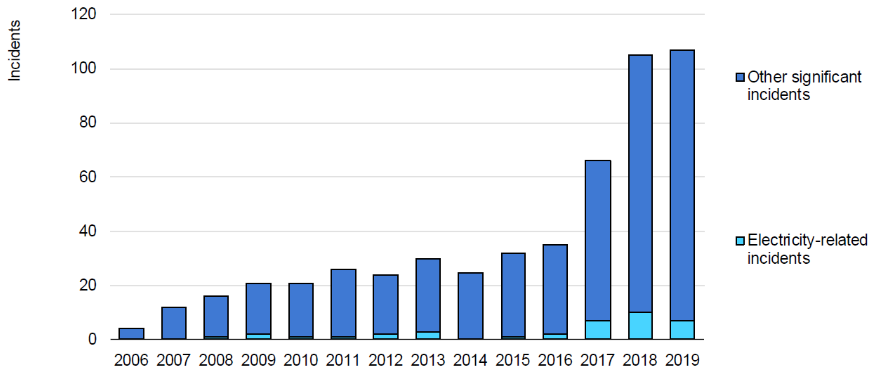
Ce que l'on sait de la cyberattaque dont le camerounais Eneo a été victime

Cet incident, qui a débuté le 29 janvier – et dont on ignore encore l'origine et l'ampleur –, a affecté les services prépayés de l'énergéticien, et ses clients utilisateurs des compteurs intelligents.



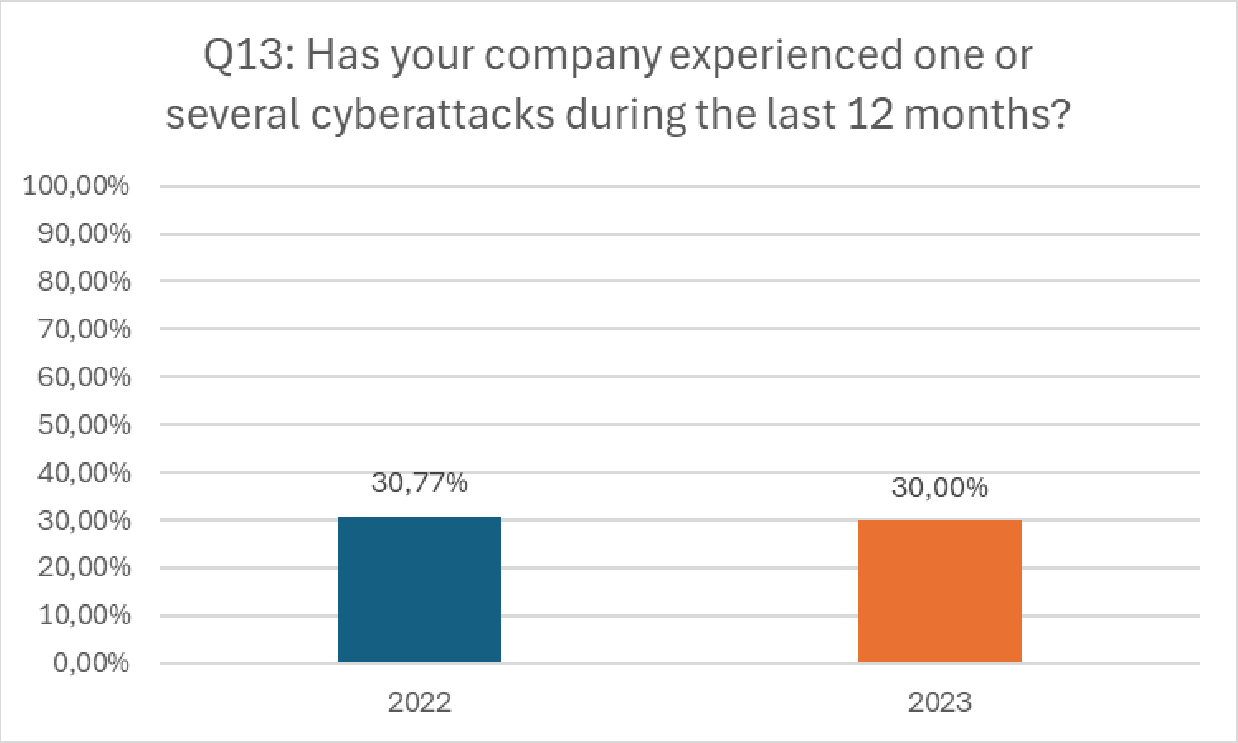
https://www.darkreading.com/cyberattacks-data-breaches

- 31/01/2024 Fulton County Suffers Power Outages as Cyberattack Continues
- 30/01/2024 'Cactus' Ransomware Strikes Schneider Electric
- 30/01/2024 Feds Reportedly Try to Disrupt 'Volt Typhoon' Attack Infrastructure



iea
International Energy Agency
Power systems in transition
Challenges and opportunities ahead for electricity security

How real is the threat?



From 7 attacks in the last 12 months

to …

26 000 000 (mostly viruses, worms …)

Phishing, malware, ransomware on

50% of members attacked have lost

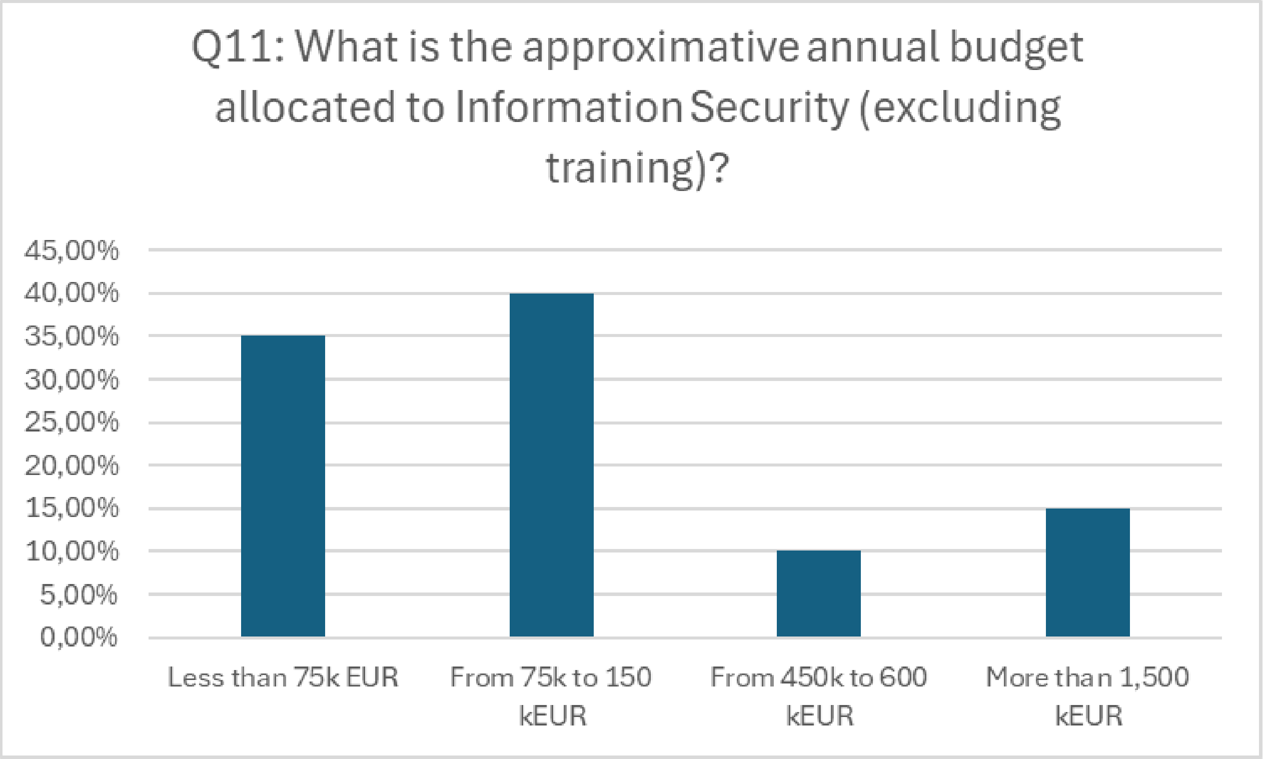
In one case, several times

An interesting question: what do we call "an attack"?

How real is the threat?

- 5% of members have suffered an attack on their ICS/SCADA systems, causing an interruption of service between 6 and 12 hours.

Let’s talk about money for a minute



An average budget of 371 kEUR

Only 0,07% of company’s turn-over

Yet, better than 0,04% in 2022

80% forecast an increase of budget

Another interesting question: what are the costs of incidents?

Key Takeaways / Recommendations

1. The threat is real

2. We are getting prepared … but too slowly. We could be short of time against hackers.

3. Our Boards & CEOs need to understand that more money has to be put on the table

4. Cybersecurity efforts must be made within an enterprise governance framework

5. APUA needs you to respond to surveys in order to better understand the threat and develop more accurate services

Thank you

Any questions?

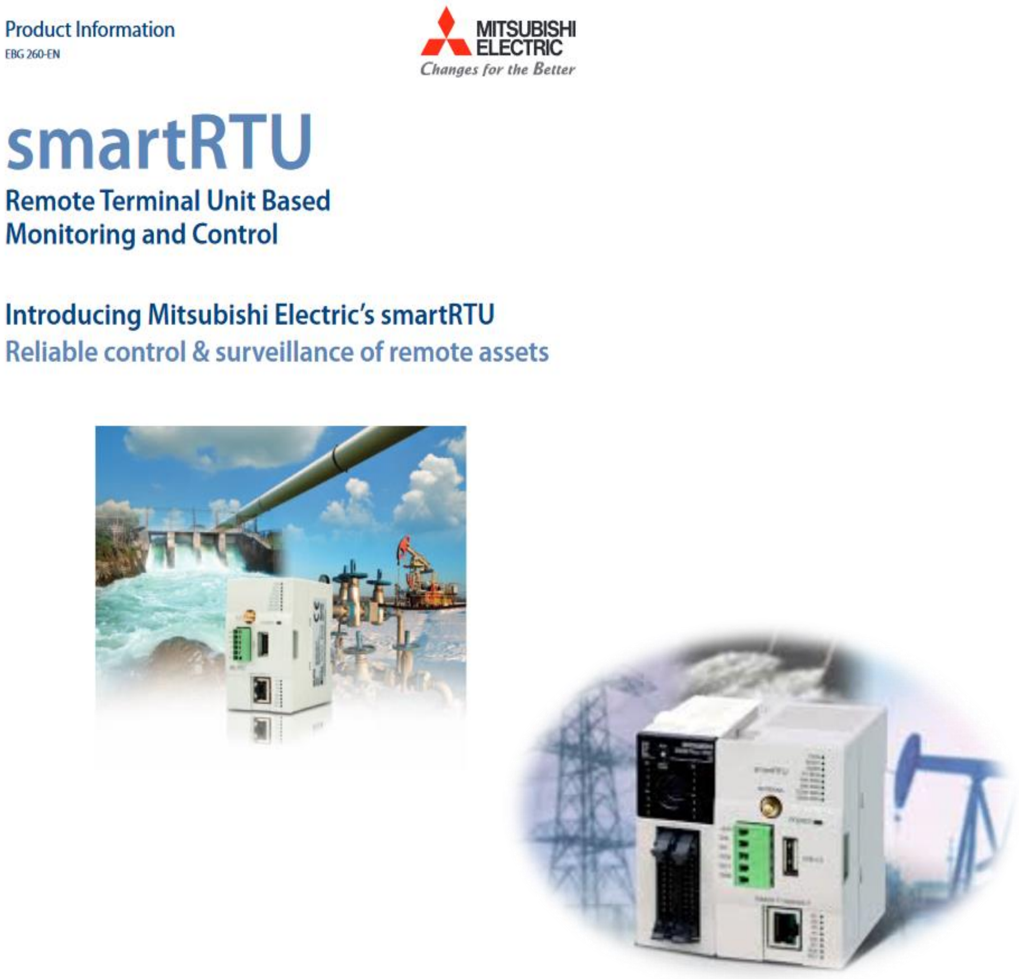
Alexis RECHAIN

Str@tec-arc

arechain@stratec-arc.com

Annex slide

Vulnerability notices



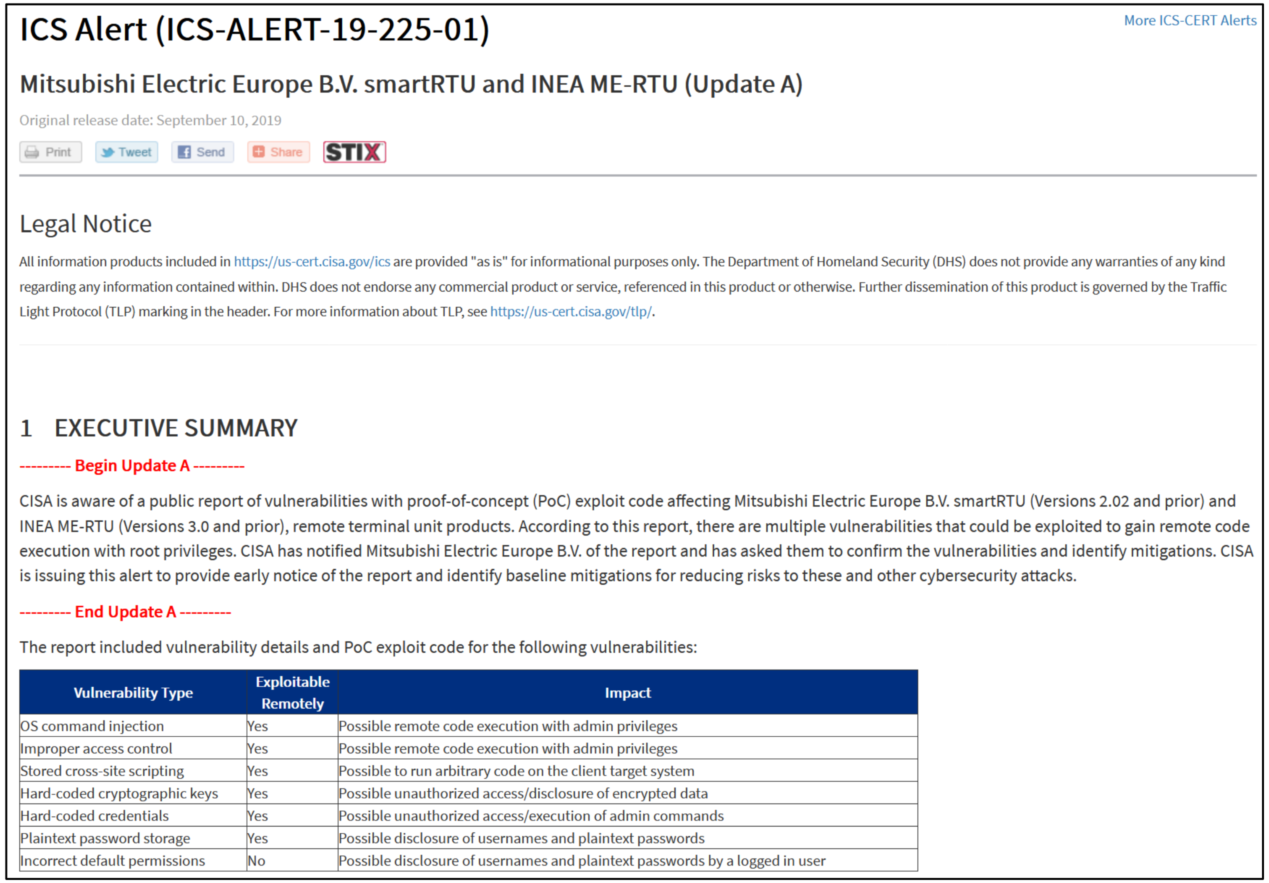
Product Information
EBG 260-EN

MITSUBISHI ELECTRIC
Changes for the Better

smartRTU

Remote Terminal Unit Based Monitoring and Control

Introducing Mitsubishi Electric's smartRTU
Reliable control & surveillance of remote assets



ICS Alert (ICS-ALERT-19-225-01)

Mitsubishi Electric Europe B.V. smartRTU and INEA ME-RTU (Update A)

Original release date: September 10, 2019

Legal Notice

All information products included in https://us-cert.cisa.gov/ics are provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. DHS does not endorse any commercial product or service, referenced in this product or otherwise. Further dissemination of this product is governed by the Traffic Light Protocol (TLP) marking in the header. For more information about TLP, see https://us-cert.cisa.gov/tlp/.

1 EXECUTIVE SUMMARY

--------- **Begin Update A** ---------

CISA is aware of a public report of vulnerabilities with proof-of-concept (PoC) exploit code affecting Mitsubishi Electric Europe B.V. smartRTU (Versions 2.02 and prior) and INEA ME-RTU (Versions 3.0 and prior), remote terminal unit products. According to this report, there are multiple vulnerabilities that could be exploited to gain remote code execution with root privileges. CISA has notified Mitsubishi Electric Europe B.V. of the report and has asked them to confirm the vulnerabilities and identify mitigations. CISA is issuing this alert to provide early notice of the report and identify baseline mitigations for reducing risks to these and other cybersecurity attacks.

--------- **End Update A** ---------

The report included vulnerability details and PoC exploit code for the following vulnerabilities:

Vulnerability Type	Exploitable Remotely	Impact
OS command injection	Yes	Possible remote code execution with admin privileges
Improper access control	Yes	Possible remote code execution with admin privileges
Stored cross-site scripting	Yes	Possible to run arbitrary code on the client target system
Hard-coded cryptographic keys	Yes	Possible unauthorized access/disclosure of encrypted data
Hard-coded credentials	Yes	Possible unauthorized access/execution of admin commands
Plaintext password storage	Yes	Possible disclosure of usernames and plaintext passwords
Incorrect default permissions	No	Possible disclosure of usernames and plaintext passwords by a logged in user

Annex slide

- Cybersecurity & Infrastructure Security Agency (CISA) – Alerts & Advisories

https://www.cisa.gov/news-events/cybersecurity-advisories?f%5B0%5D=advisory_type%3A95

- CVE Mitre - https://cve.mitre.org/

- CVE Details - https://www.cvedetails.com/

- SHODAN - https://www.shodan.io/