Cyber Attacks and electrical Grids.

Problem Statement Recap

- Problem statement: There is a growing threat of cyber-attacks on energy grids, which exploits specific vulnerabilities within the system.
- Causes include:

  - outdated systems and technology.

  - untrained or lack of cybersec staff.

  -

Roles Recap:

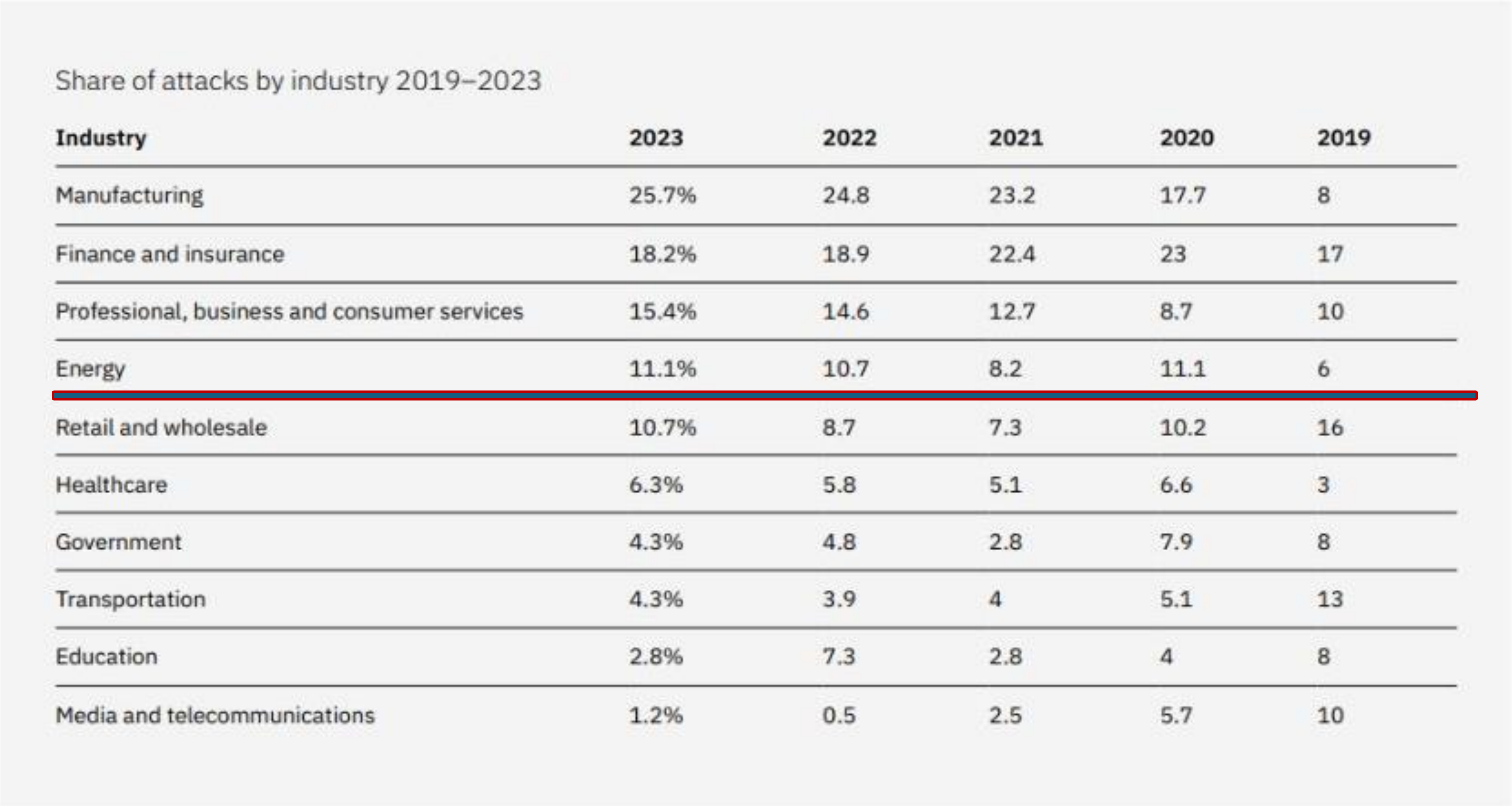
- **Ahmed:** responsible for analyzing recent cyber attack trends targeting energy grids globally and assess their potential impact on local systems.
- **Shreeji**: responsible for examining incident response strategies and crisis management protocols specific to cyber incidents affecting energy utilities.
- **Shola:** responsible for exploring technologies like advanced intrusion detection systems (IDS), anomaly detection, and secure communication protocols relevant to energy grid cybersecurity.
- **Divyansh:** responsible for investigating specific vulnerabilities and entry points exploited by cyber adversaries targeting energy infrastructure.
- **Ankita:** responsible for studying best practices and standards for securing energy grids, including guidelines from organizations such as NERC and DOE.

What we found: Cyber Attack Trends

When it comes to trends regarding cyber-attack trends on energy grids:

- Energy organizations, including electric utilities and oil and gas companies, were the fourth most attacked industry, representing 11.1% of attacks.
- Malware was the most common action on objective observed, representing 43% of cases, with ransomware cases accounting for 22% of attacks. The use of legitimate tools for malicious purposes was the second most observed action on objective, accounting for 36% of incidents and server access incidents followed at 21%.
- Data theft and leak accounted for the top impact on energy organizations at 33% of observed cases, followed by digital currency mining and extortion tying for 22% of incidents each.

- The exploitation of public-facing applications was the top initial infection vector, representing half of the cases, followed by the use of valid local accounts at 38% and replication through removable media in 13% of cases.
- Europe experienced the highest percentage of incidents within the energy sector at 43%, followed by North America at 22%, Latin America at 14% and the Middle East and Africa and Asia-Pacific at 11% each.



Share of attacks by industry 2019–2023

Industry	2023	2022	2021	2020	2019
Manufacturing	25.7%	24.8	23.2	17.7	8
Finance and insurance	18.2%	18.9	22.4	23	17
Professional, business and consumer services	15.4%	14.6	12.7	8.7	10
Energy	11.1%	10.7	8.2	11.1	6
Retail and wholesale	10.7%	8.7	7.3	10.2	16
Healthcare	6.3%	5.8	5.1	6.6	3
Government	4.3%	4.8	2.8	7.9	8
Transportation	4.3%	3.9	4	5.1	13
Education	2.8%	7.3	2.8	4	8
Media and telecommunications	1.2%	0.5	2.5	5.7	10

Solution/Conclusion:

Sources

- X-Force Threat Intelligence Index 2024 Contents. (n.d.). https://www.ibm.com/downloads/cas/L0GKXDWJ
-