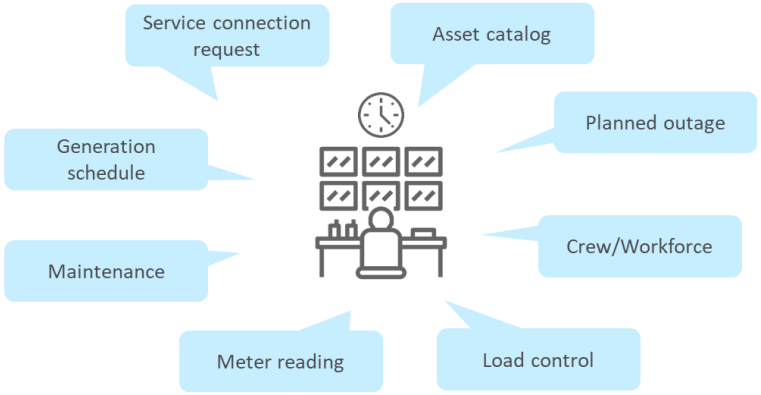
Importance of Cyber-Security for Increasingly Digital Distribution Utilities

Sebastian Lehnhoff, OFFIS

Digital Distribution Utilities

Transformation opportunities

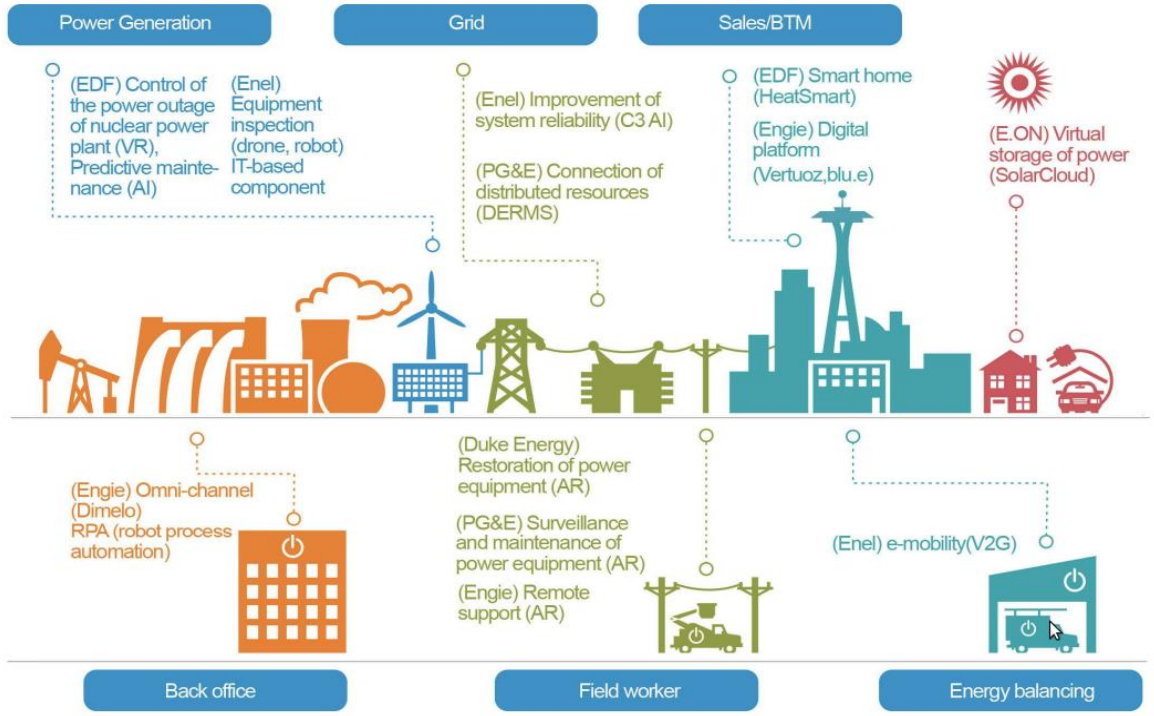
- Decentralization in the power system creates opportunities
  - More data exchange between systems from many different actors
  - Emerging new business models
- Turning point digitalization: from energy distribution to data business
  - Focus on data as a core engine of business
  - Data-based value creation process
  - Machine learning, artificial intelligence, IoT
- Management of decentralized energy resources (DERs)



Digital Distribution Utilities

Transformation challenges

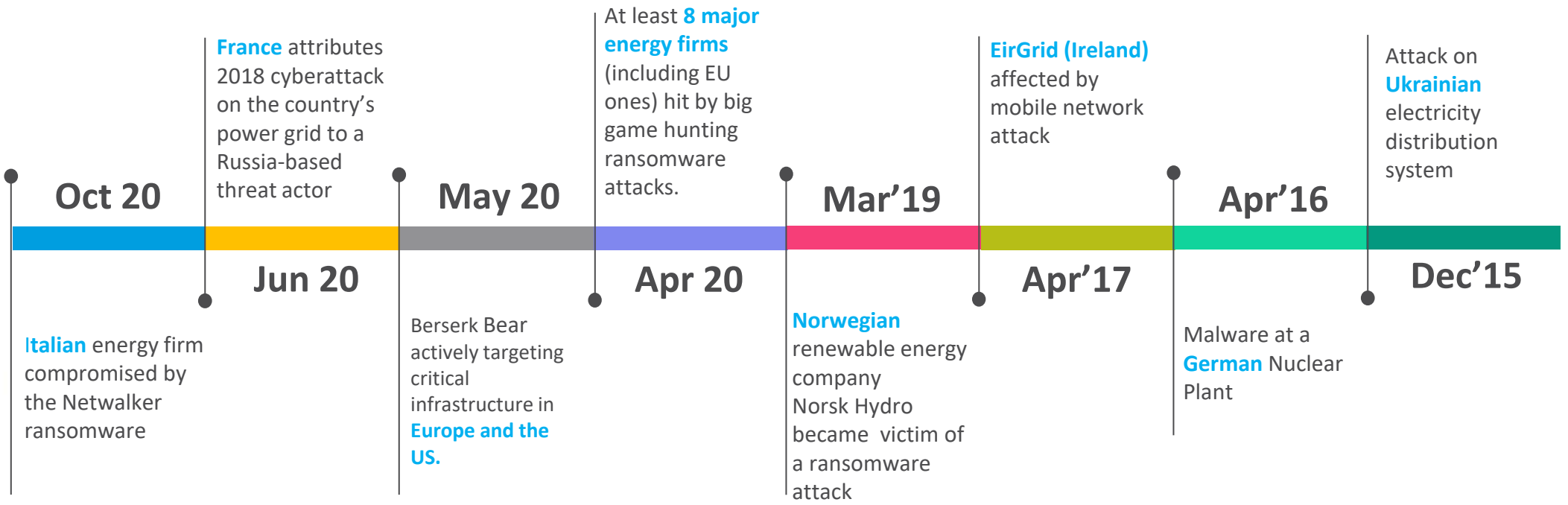
- Restructuring of the energy system, including
  - many smaller plants – system critical as a whole
  - competition and new business models
  - networking through digitalization
- Digitalization trends, including
  - Growing IT and OT convergence
  - higher complexity hardware and software
- Mitigating cyber vulnerabilities require
  - Regulation and incentives
  - Cyber-security awareness and culture



Source: McKinsey & Company, Reorganized by adding utility case, ISGAN 09/21

Cyber-Attacks on Power Systems

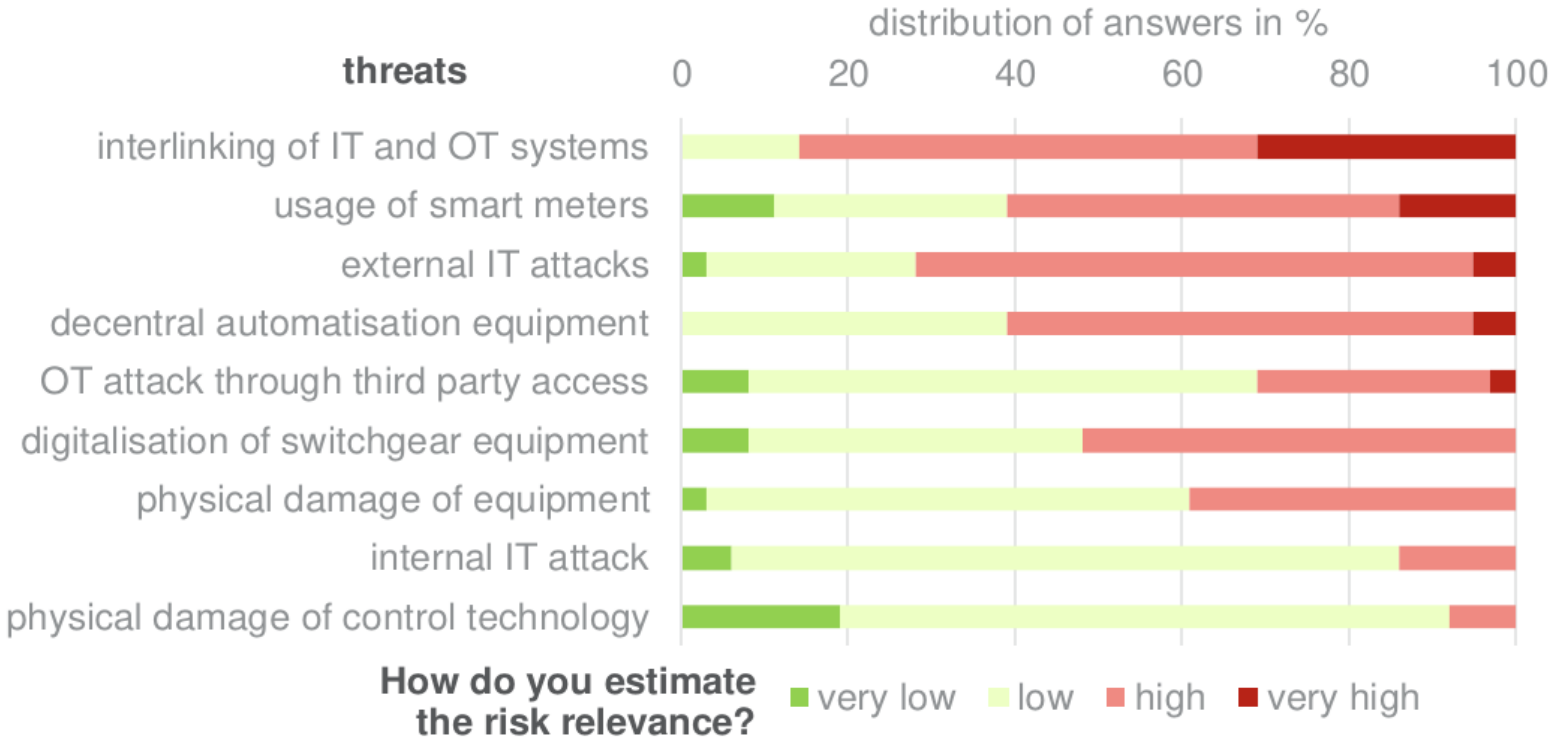
- In recent years, there have been multiple cyber-attacks (reported) in Europe
  - severe impact in terms of economic losses and physical damages
  - Cyber-security strategies and countermeasures are urgently needed for protecting the power system



Source: Computer Emergency Response Team for the EU Institutions (CERT-EU)

Cyber-Security

- Threats
  - Cyber-security strategies are required to avoid cyber-attacks and reduce the severity of its risk



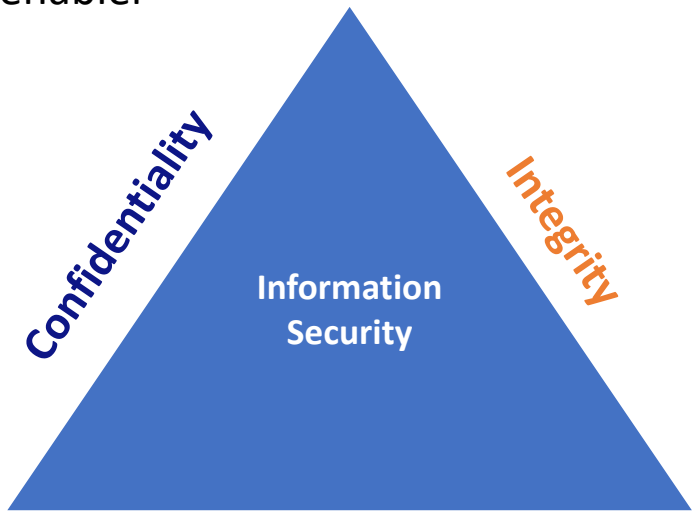
Source: ecoys 2018

Cyber-Security

- Countermeasures following the CIA triad
  - Cyber-security is not business „versus“ costs
  - But should be seen as business „enabler“

Man-in-the-Middle, Stuxnet, Phishing campaign, SQL injection attack, Side-channel- attack, escalate privilege, AES Cache-Timing Attack

Countermeasures
Access Management
Training / Awareness



False data injection, Load Altering attack, Phishing campaign, Tampering

Countermeasures
Data Encryption / Hashing
Training / Awareness

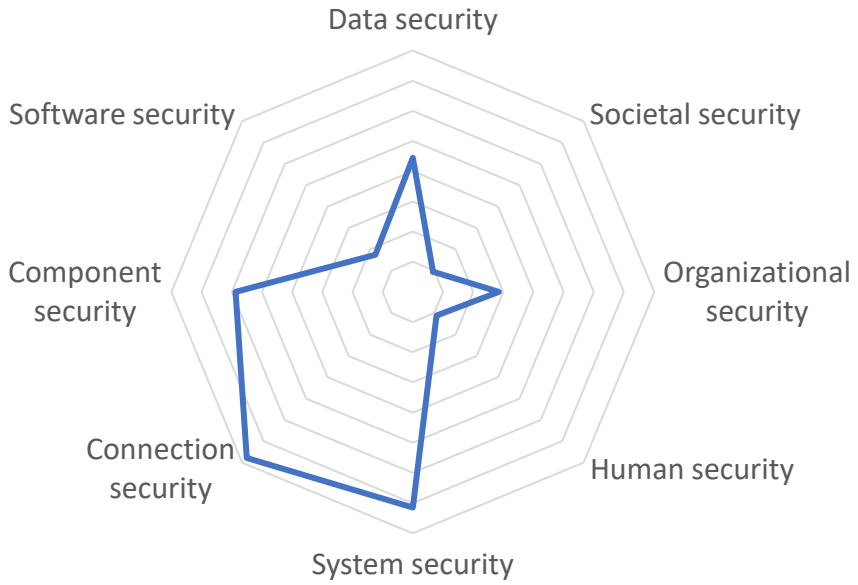
DoS/DDoS, Ransomware, Blocking attack, Escalate privilege, AES Cache-Timing Attack, Buffer overflow

Countermeasures
Redundancy / Backup
Separation of IT / OT

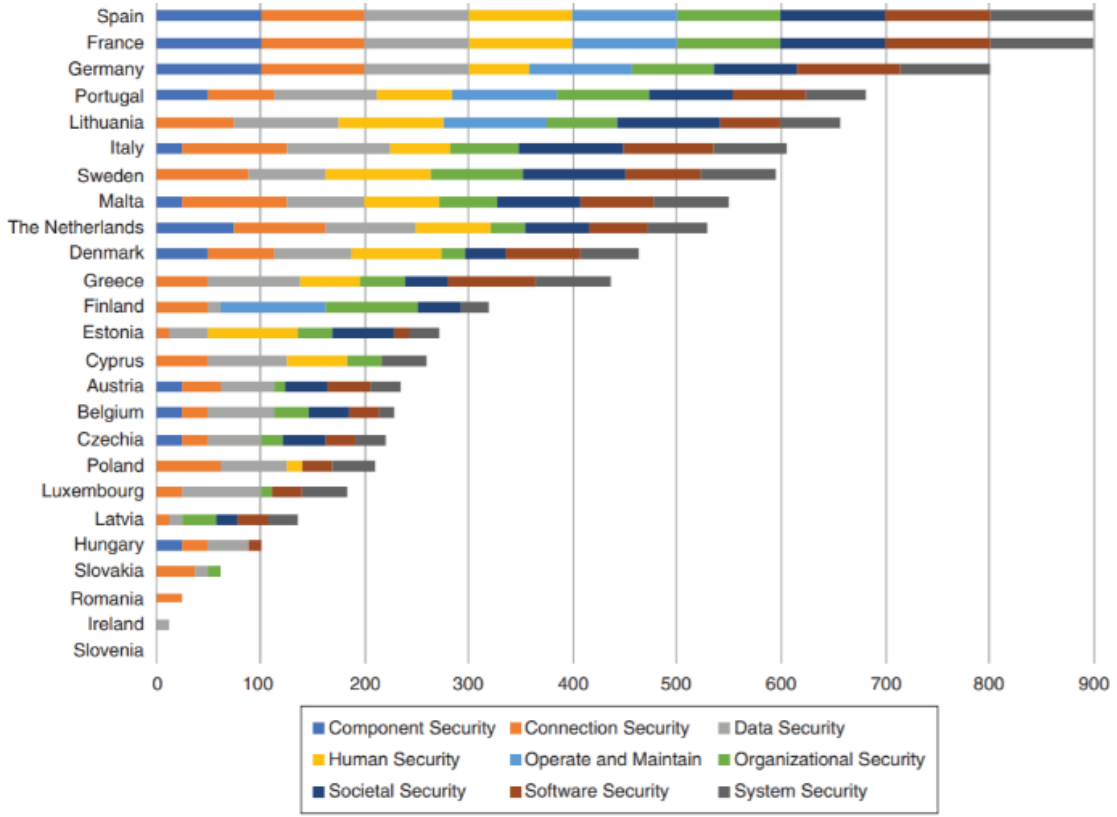
"*You can't have a ransomware attack on your IT network and not have it affect the OT network unless it's like one machine*“ Tom Alrich, Security Consultant, 2021

Cyber-Security

- Education is key for mitigation of threats
  - 3 out of 8 cyber-security educational domains covered and only focus on „IT“ security
  - BUT still lacking „soft-skills cyber-security“



Source: B. Siemers et al., "Modern Trends and Skill Gaps of Cyber Security in Smart Grid: Invited Paper," IEEE EUROCON 2021



Source: N. Dragoni, A. Lluch Lafuente, F. Massacci and A. Schlichtkrull, "Are We Preparing Students to Build Security In? A Survey of European Cybersecurity in Higher Education Programs [Education]

Key Takeaways/ Recommendations

- Cyber-vulnerabilities have risen significantly in power systems
- Complexity of infrastructure increases
  - Legacy devices are being exposed to outside systems
  - Intelligent devices with different functionality
- High demand for cyber-security workforces
  - Regulation and incentives (budget) for active cyber-security policy and action plans, i.e. testbed, training
  - Building cyber-security culture for a broader audience of IT and non-IT practitioners
- Cross-functional collaboration is needed
  - Information exchange between academic institutions, industry, government, and electric utilities
  - Enhancing trust and sharing proof of practice in the event of cyber-security attacks

References

- OFFIS Institute for Information Technology: https://www.offis.de
- European Security Agency: https://www.enisa.eu
- SotACS: State of the Art in CS and SmartGrid Edu: https://doi.org/10.1109/EUROCON52738.2021.9535627
- CCRSG: European Cybersecurity Education Project: https://www.offis.de/offis/publikation/modern-trends-and-skill-gaps-of-cyber-security-in-smart-grid.html
- IDUNN: https://www.idunnproject.eu/
- DKE: https://www.dke.de/de/arbeitsfelder/cybersecurity
- BDI: https://bdi.eu/themenfelder/digitalisierung/cybersicherheit-und-wirtschaftsschutz/#
- Cloudsec: https://cloudsek.com/whitepapers_reports/abysmal-state-of-global-critical-infrastructure-security/
- Central Electric Authority: https://cea.nic.in

Prof. Dr. Sebastian Lehnhoff

Chairman of the Board

OFFIS
Escherweg 2
26121 Oldenburg
Tel: +49 441 9722-0
e-mail: lehnhoff(at)offis.de
More info: www.offis.de