UCL

Exploring the Security Culture of Operational Technology Companies

The Role of External Consultancy in Overcoming Organisational Barriers

Stefanos Evripidou, Uchenna Ani, Steve Hailes, and Jeremy Watson
University College London, University of Keele

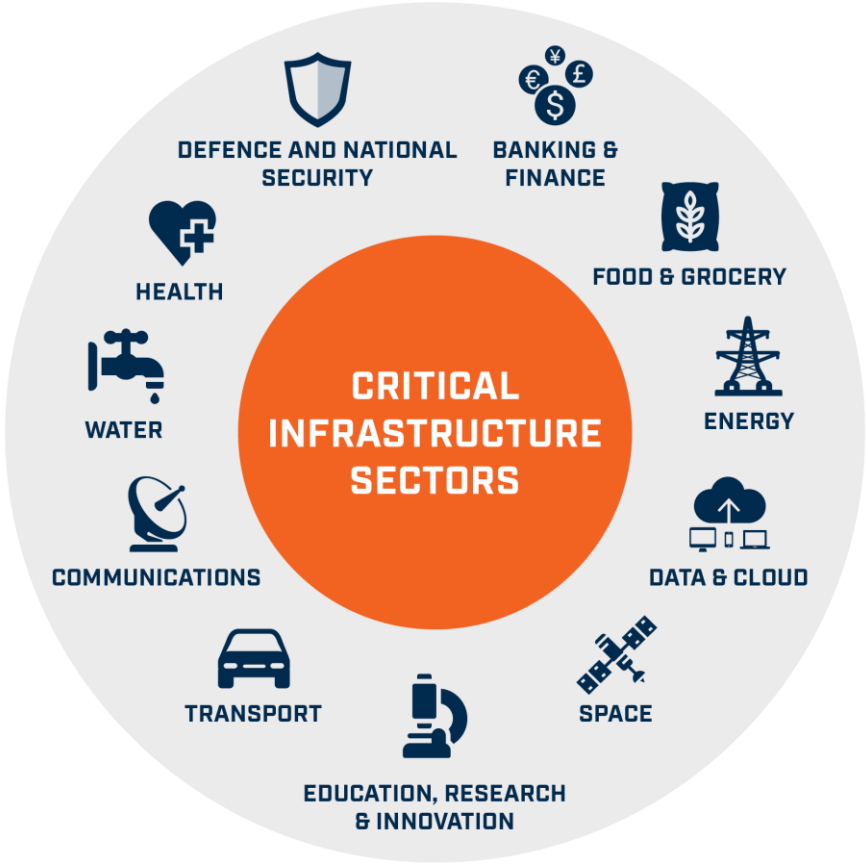
Operational Technology (OT)

"Hardware and software that detects or causes a change, through the direct monitoring and/or control of industrial equipment, assets, processes and events." (Gartner, 2019)

	Operational Technology (OT)	Information Technology (IT)
Priorities	Safety, Reliability, Availability (SRA)	Confidentiality, Integrity, Availability (CIA)
Component Lifecycle	Decades	Typically < 5 years
Communication Protocols	Various proprietary/ industrial protocols (e.g. Modbus)	Ethernet/IP
Impact of cyberattacks	Physical (environmental, human) and financial	Generally financial

OT Companies

- Increased Digitilisation (Industry 4.0)
  - Increased security risk
- Often operate critical infrastructure
  - Network and Information Systems (NIS) Regulation
- Physical impact
  - Colonial Pipeline - May 2022
  - Strong culture of safety

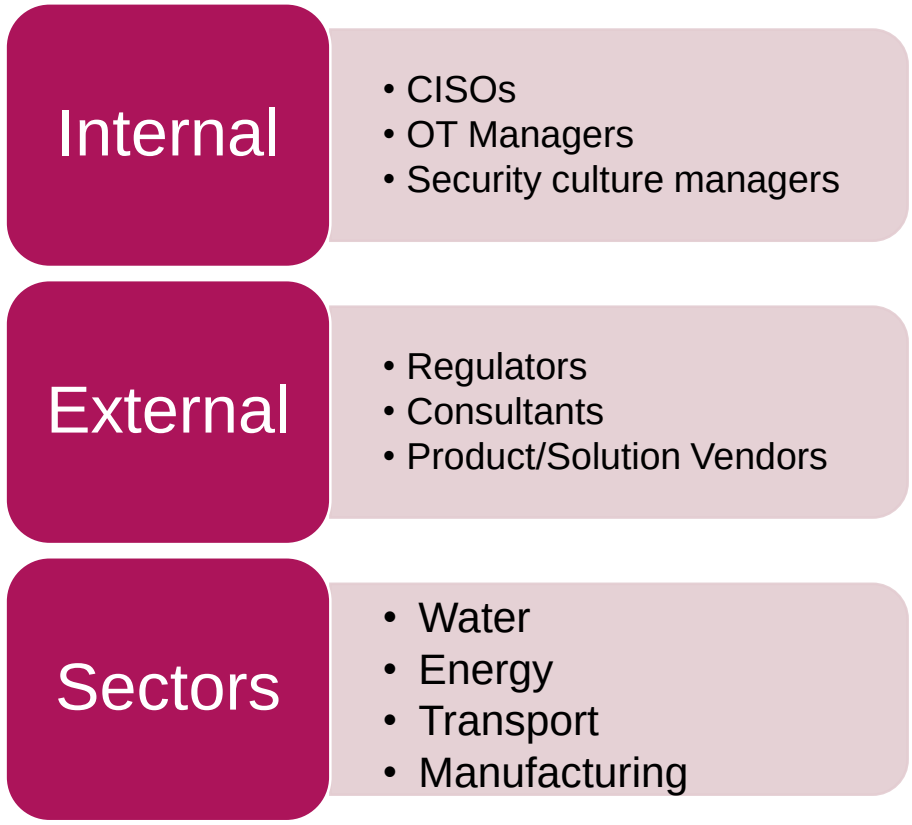


RQ: How is security culture developed in companies that use OT?

1. What are the greatest organisational and human barriers?
2. How do security consultants and security solution vendors contribute to overcoming these barriers?

Methodology

- 33 interviews from 25 companies
- Theoretical Sampling – Expanded scope
- Thematic analysis (Braun & Clarke, 2006)



Barrier I – Governance

- *“First thing you have to work out is who's doing what and who does the company think is running their OT security.”*

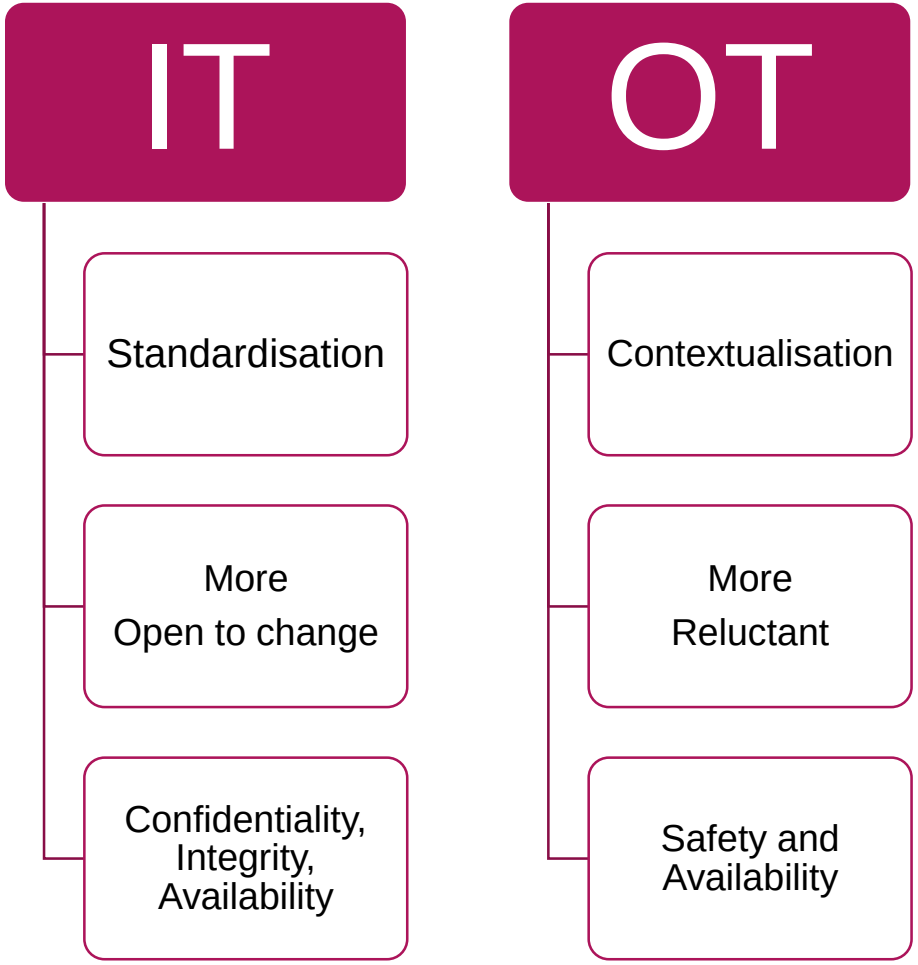
- IT and operations/engineering functions
- Reporting lines
- Competing interests
- Budget allocation

Barriers II & III

- Lack of knowledge and expertise
  - Tacit operational experience vs Security expertise
  - How does one become an OT security expert?

- Lack of communication
  - *“If you talk to the IT department, they don't have any expertise in OT and they don't really talk to the engineering department because the engineering department doesn't want to talk to IT people.”*

Different security “mindsets”



External stakeholders - Consultants and Vendors

- Technology implementors, policy designers - Governance
- Raising awareness, sharing knowledge - Knowledge expertise
- Mediators between functions - Communication

- How do companies absorb that and turn it to a strong organisational security culture?

Conclusions

- Consultants and vendors do have a role to play
  - At a key early phase in OT companies' cybersecurity journey
- Governance, Expertise and Communications are common problems
  - Underlying technology is different, complicating things
- Future work
  - Other stakeholder groups
  - User populations: Operational technology personnel

Thank you for listening!

- Any questions?
- For any queries or collaboration contact
- stefanos.evripidou.16@ucl.ac.uk
- References

- Braun, V., Clarke, V., 2006. Using thematic analysis in psychology. Qualitative Research in Psychology 3, 77–101. https://doi.org/10.1191/1478088706qp063oa
- ‘Definition of Operational Technology (OT) - Gartner Information Technology Glossary’, 2019