Norwegian Centre for Research-based Innovation

NORCICS

SFI Norwegian Centre for Cybersecurity in Critical Sectors

Sustainable socio-technical cybersecurity capabilities

A multi-method study of Norwegian municipalities

Research questions:

How can municipalities build sustainable cybersecurity capabilities with sufficent structural, technological and human support to perform the expected security tasks from major security frameworks?

What are significant barriers and opportunities for building these capabilities

- Related to the socio-technical dimensions of each capability
- Sourcing choices

Further: How does the municipalities approach sensing, seizing and transformative capabilities for cybersecurity?

Methodology:

- Document analysis of relevant cybersecurity frameworks
- Delphi-based card sorting study
- Semi-structured Interviews of cybersecurity practicioners

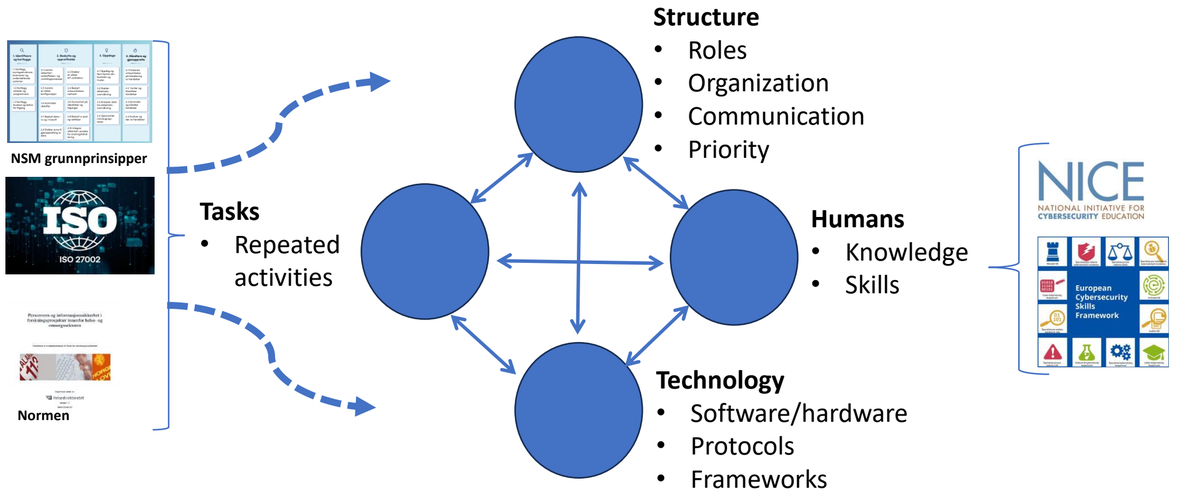
Document analysis

- Structured document analysis with coding for 4 categories:
  - Task, Structure, Technology, Human
- 3 Cybersecurity frameworks
  - NSM ICT Principles
  - ISO 27002
  - Norwegian Code of Conduct for information security and data protection in the healthcare and care services
- Synthesized to 71 tasks with related technology, structure and human considerations

Modified delphi card sorting study and semi-structured interviews

- Qualitative and quantitative data
- Practitioner´s perspectives and co-creation

From frameworks to capabilities



Document analysis and data extraction

Task

Activities with a sustained impact on human resource requirements. Often framed as processes with specific inputs and outputs or formulated with an active language, such as “do”, “perform”. Not one-time-activities, such as “establish policy for…”

Structure

The organization's systems of roles, responsibilities, communication channels, and how activities are organized and directed. Descriptions of roles and responsibilities, communication channels such as reporting lines, formal meeting points, cross-functional teams and committees, forums, and other similar mechanisms

Humans

Skills and competencies in line with the NIST NICE frameworks understanding of cybersecurity role descriptions. Specific requirements around qualifications, skills, and knowledge related to cybersecurity tasks. Exclude general information security skills and awareness training

Technology

Technology that supports tasks related to the capability, such as cybersecurity tools for detection and response, vulnerability management, identity and access management. May also include broader technological artifacts such as security frameworks, security baseline standards, and protocols.