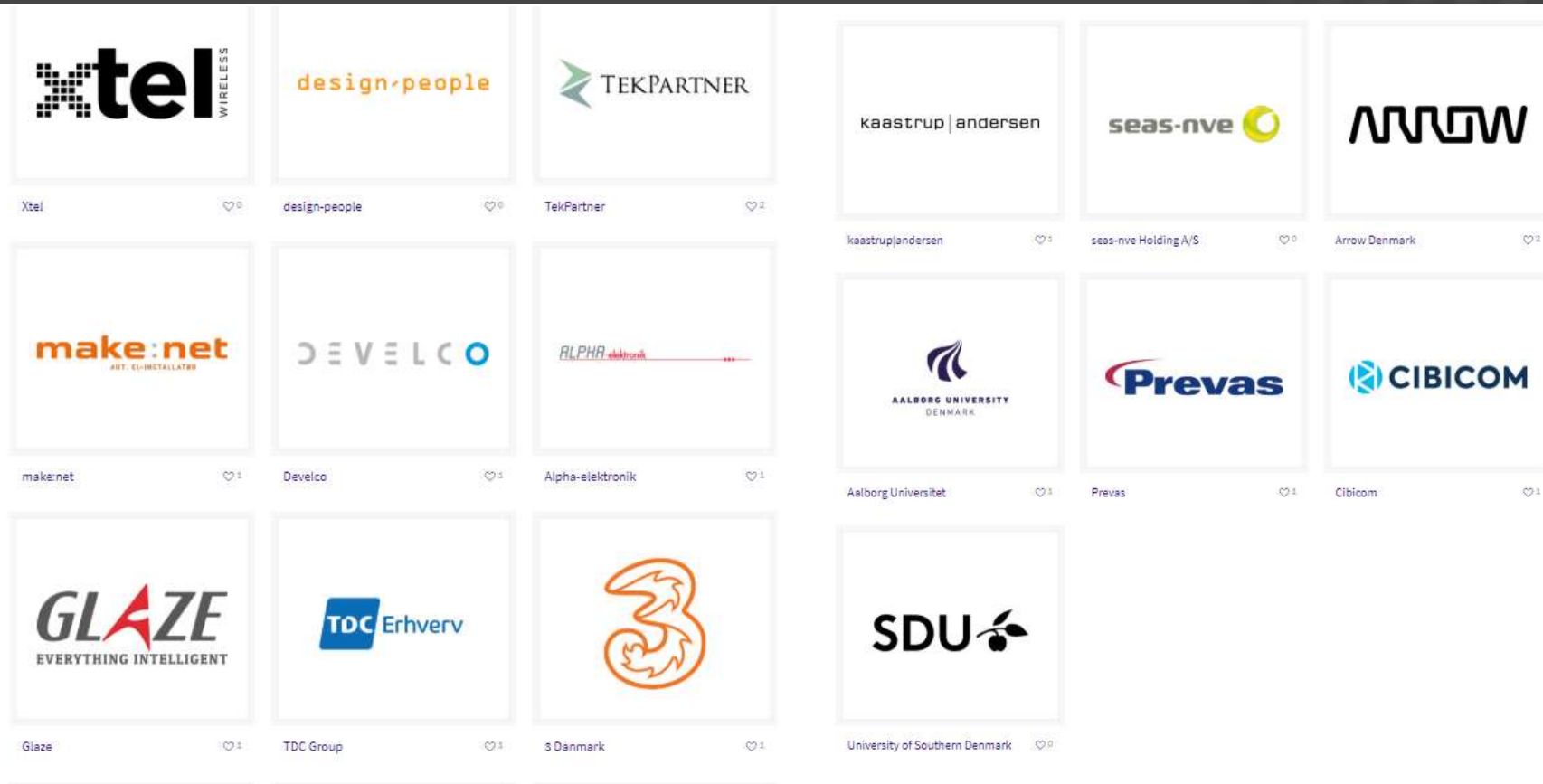


# NORDIC IOT CENTRE



Nordic IoT Centre



# SMART CITY CLUSTER DENMARK

- Smart cities are rapidly emerging
- In 2050 2 out of 3 will be living in megacities
- 33.600 new jobs in Denmark in 2025



Nordic IoT Centre



# CIDI

- Maturity study: IoT security of Danish industry companies
- Next step: Improve this by working with 20 case companies.



IT UNIVERSITY OF CPH

Nordic IoT Centre



## Bliv skarp på IoT-sikkerheden i dine produkter



CYBERSECURE IOT IN DANISH INDUSTRY

**INDUSTRIENS  
FOND** FREMMER DANSK  
KONKURRENCEEVNE  
The Danish Industry Foundation

# PROCESS

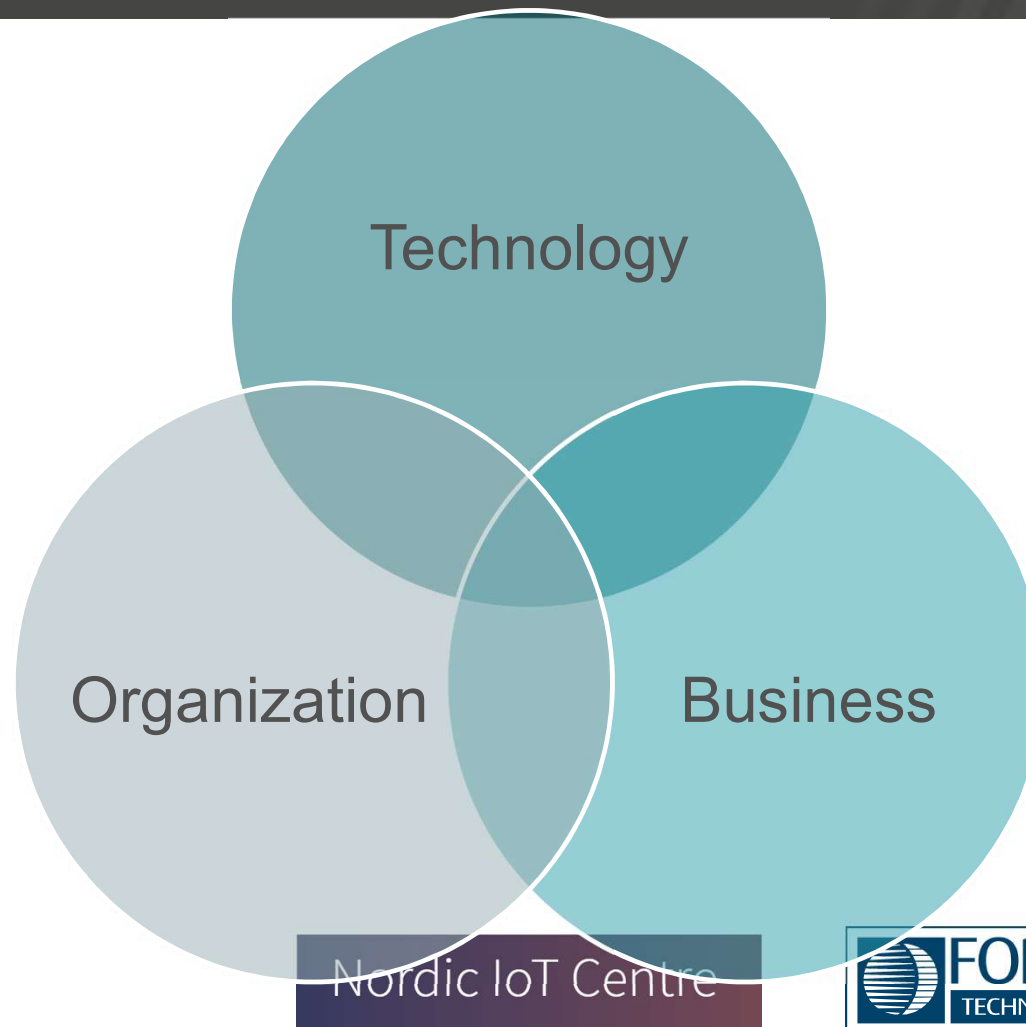
1. Desk study
2. Preliminary model of change + hypotheses about success factors
3. Interviews: companies and experts
4. Iteratively discussing findings using the Delphi method
5. Empirical analysis
6. Typological maturity model for IoT security
7. Interdisciplinary recommendations for each typology

Nordic IoT Centre



ALEXANDRA  
INSTITUTTET

# HOLISTIC APPROACH

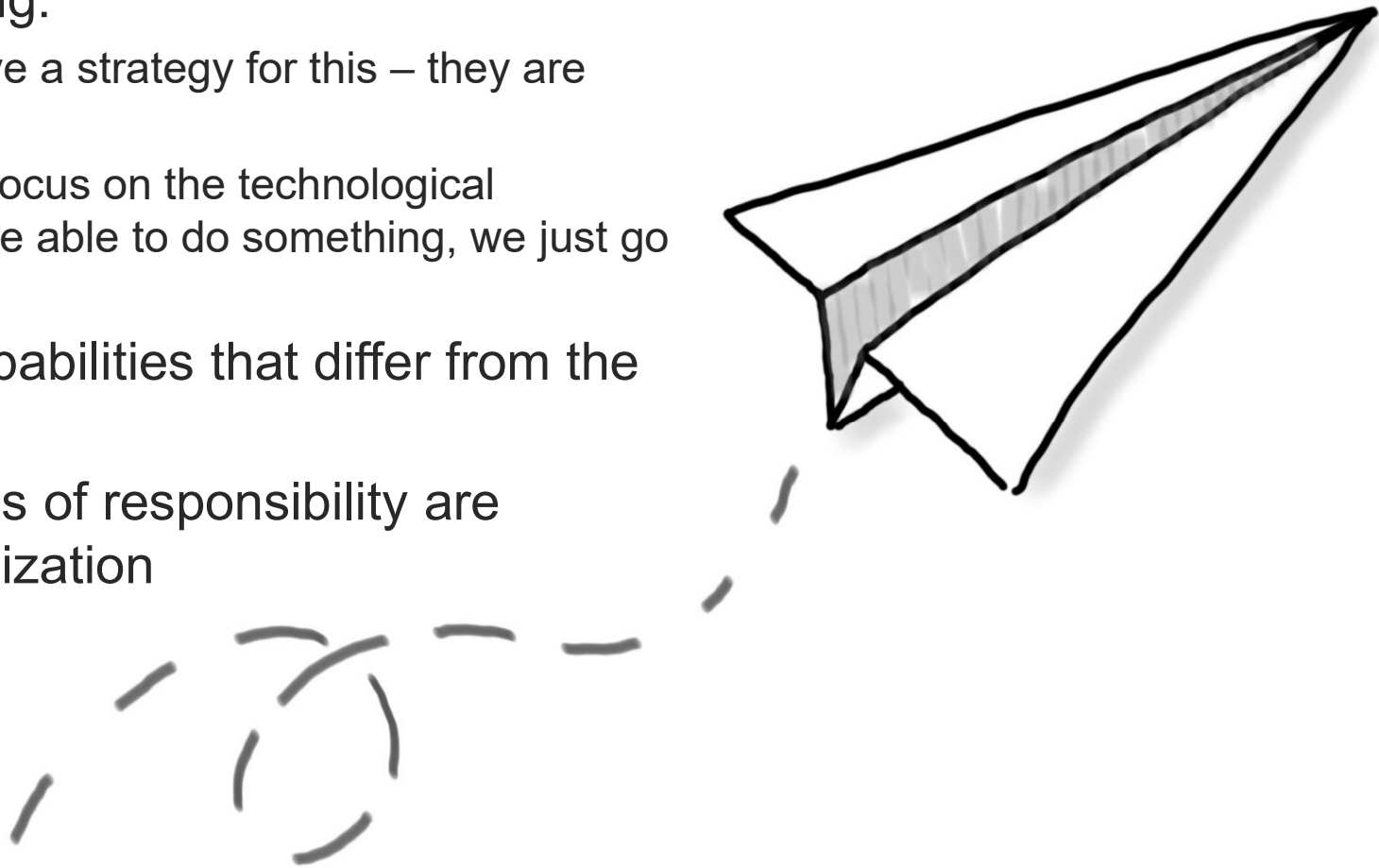


# INITIAL FINDINGS



# UNCHARTED TERRITORY

- Technology in the making:
  - “Our customers don’t have a strategy for this – they are lagging behind”
  - “We have a tendency to focus on the technological possibilities – once we are able to do something, we just go ahead and implement it”
- IoT security requires capabilities that differ from the companies’ DNA
- Competencies and areas of responsibility are fragmented in the organization





# WHAT IS THE RIGHT LEVEL OF SECURITY?

- Lack of standards and/or check lists
  - Neither deficiency and overinvestment
  - Communicating with customers
- Different security requirements from different customers
  - and sometimes they are not the right ones
- Setting up their own metrics
  - “If it’s good enough for them, it’s good enough for us”
  - “We have created a cross-functional security board”



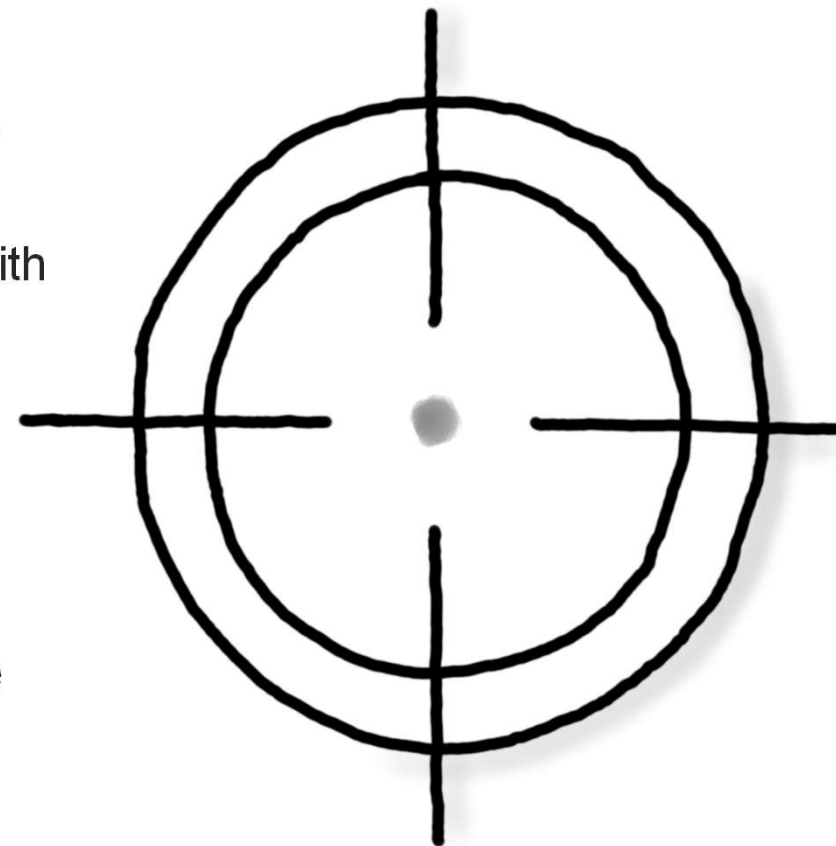
Nordic



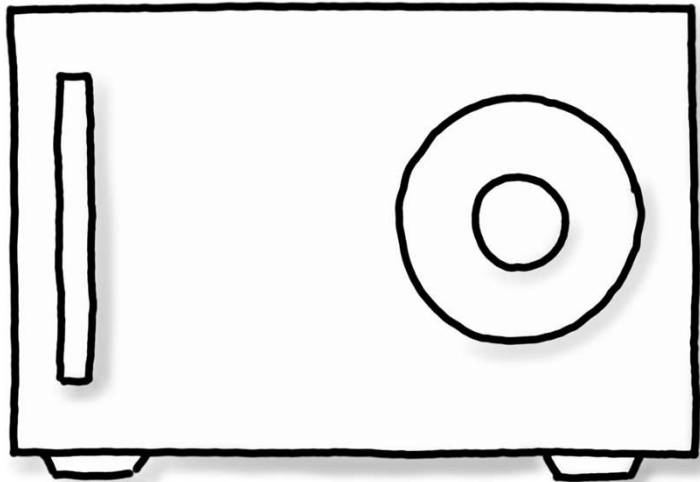


# USING YOUR IMAGINATION

- Data in themselves are not seen as sensitive
  - *“I really can’t imagine how anyone would get anything out of our data”*
  - *“Every time we have a new idea, this guy comes up with all the ways it could go wrong”*
- Physical security
  - *“Well, if someone is willing to go through all that, we say: “Let them””*
- Mental models: What counts as a breach?
  - *“We haven’t had any breaches. However, we did have this little incident...”*



# SECURITY IS BUSINESS CRITICAL



- Customers are worried about security in IoT products
- Crucial for scalability
- Security enabling new business models, products and developments

# STANDARDS CAN HELP PART OF THE WAY

	General	Consumer	Industrial	Medical	Maritime
General	<ul style="list-style-type: none"> <li>• ISO 27000</li> <li>• NIST SP 800 (53, 171)</li> <li>• NIST Cybersecurity framework</li> </ul>	<ul style="list-style-type: none"> <li>• ISO 27000</li> </ul>	<ul style="list-style-type: none"> <li>• ISA 62443-1-X</li> </ul>	<ul style="list-style-type: none"> <li>• HIPAA</li> </ul>	
Policies and Procedures	<ul style="list-style-type: none"> <li>• ISO 27000 (1-32)</li> <li>• ETSI TS 103 305, 309,</li> <li>• ETSI TR 103 331</li> <li>• IASME</li> <li>• ISO/IEC 22301</li> </ul>		<ul style="list-style-type: none"> <li>• ISA 62443-2-X</li> </ul>	<ul style="list-style-type: none"> <li>• ISO/IEC 80001</li> <li>• AAMI TIR57</li> </ul>	<ul style="list-style-type: none"> <li>• BIMCO CS guidelines v3</li> <li>• IMO MSC-FAL.1/Circ.3</li> </ul>
System	<ul style="list-style-type: none"> <li>• ISO 27000 (33, 34, 39 – 41)</li> <li>• ETSI TR 103 421</li> </ul>		<ul style="list-style-type: none"> <li>• ISA 62443-3-X</li> </ul>	<ul style="list-style-type: none"> <li>• TIR 80001-2-2:2012</li> </ul>	<ul style="list-style-type: none"> <li>• BIMCO CS guidelines v3</li> </ul>
Component	<ul style="list-style-type: none"> <li>• UL2900-1</li> <li>• ISO 15408</li> </ul>	<ul style="list-style-type: none"> <li>• ETSI TS 103 645</li> </ul>	<ul style="list-style-type: none"> <li>• ISA 62443-4-X</li> <li>• UL2900-2-2</li> </ul>	<ul style="list-style-type: none"> <li>• UL2900-2-1</li> <li>• CLSI AUTO11-A2</li> </ul>	<ul style="list-style-type: none"> <li>• BIMCO CS guidelines v3</li> </ul>

Nordic IoT Centre



# TS 103 645 – CS FOR CONSUMER IOT

4	Cyber security provisions for consumer IoT .....	8
4.1	No universal default passwords .....	8
4.2	Implement a means to manage reports of vulnerabilities .....	9
4.3	Keep software updated .....	9
4.4	Securely store credentials and security-sensitive data .....	11
4.5	Communicate securely .....	11
4.6	Minimize exposed attack surfaces .....	11
4.7	Ensure software integrity .....	11
4.8	Ensure that personal data is protected .....	12
4.9	Make systems resilient to outages .....	12
4.10	Examine system telemetry data .....	12
4.11	Make it easy for consumers to delete personal data .....	13
4.12	Make installation and maintenance of devices easy .....	13
4.13	Validate input data .....	13