FIND OUR WEBISTE
DIGITAL BUSINESS DEVELOPMENT
ON **DBD.AU.DK**

SITUATIONAL ANALYSES

Scan the QR code to find a step-by-step guide for this tool, digital business development cases and further inspiration at dbd.au.dk

Building block: Alignment between business and security

Main question 1:

What does the company do to align business and cybersecurity?

Answer:

Supporting questions

Is the business purpose of using IoT solutions clear?

Does the company have plans for further development of the IoT solutions?

Clarify how critical cybersecurity is for business. What should be prevented because it could damage your business? For example, if:

- data is disclosed
- data in systems/machines is rendered inaccessible to the company

Main question 2:

Why has the company chosen this approach to ensure alignment between business and cybersecurity?

Answer:

Supporting questions

Is there a risk of cyber-attacks?

Would a potential IoT security breach have consequences for your business? Would it cause e.g. bad publicity or delays?

Does the company perceive cybersecurity as a value-add for your business?

Is there an external demand for more cybersecurity? From e.g. customers, suppliers, or regulation.

Main question 3:

How does the company want to proceed to ensure alignment between business and cybersecurity?

Answer:

Supporting questions

Can the company create new business with a cybersecure IoT solution? Would it attract different customers?

Is it likely to be an increasing problem in the future if data is disclosed, if you cannot access data and systems, or if unauthorised persons modify data?

Is cybersecurity perceived as a business opportunity or as an insurance?

"CyPro", supported by Industriens Fond.

INDUSTRIENS FOND

UGLA INSIGHTS

FORCE TECHNOLOGY

DAMRC

ALEXANDRA INSTITUTTET

DEPARTMENT OF BUSINESS DEVELOPMENT AND TECHNOLOGY
AARHUS UNIVERSITY
AARHUS BSS

FIND OUR WEBISTE
DIGITAL BUSINESS DEVELOPMENT
ON **DBD.AU.DK**

SITUATIONAL ANALYSES

Scan the QR code to find a step-by-step guide for this tool, digital business development cases and further inspiration at dbd.au.dk

Building block: Approach to security and risk

Main question 1:

How does the company work with its risk mindset and approach to cybersecurity?

Answer:

Supporting questions

Does the company have specific cybersecurity goals or initiatives related to its IoT-solutions?

Does the company perform methodical risk assessments in relation to IoT cybersecurity?

Does the company perform structured threat modelling of IoT systems and solutions?

Main question 2:

Why has the company chosen this way of developing its risk mindset and approach to cybersecurity?

Answer:

Supporting questions

Is the company at risk of cyberattacks on IoT systems and solutions?

Has the company actively considered how to deal with potential threats and risks of attacks on IoT systems and data?

Is the company's development of IoT cybersecurity based on specific risks and treats?

Main question 3:

How does the company intend to move forward in developing its risk mindset and approach to cybersecurity?

Answer:

Supporting questions

Could it be an advantage for the company if both management and employees share a common risk-based mindset concerning potential attacks on IoT systems and data?

Would it be a concern if the company lacks a shared understanding and approach to risk and IoT cybersecurity?

Is there a need for standardised procedures regarding risk assessment and threat modelling of solutions and systems?

"CyPro", supported by Industriens Fond.

INDUSTRIENS FOND

UGLAINSIGHTS

FORCE TECHNOLOGY

DAMRC

ALEXANDRA INSTITUTTET

DEPARTMENT OF BUSINESS DEVELOPMENT AND TECHNOLOGY
AARHUS UNIVERSITY
AARHUS BSS

FIND OUR WEBISTE
DIGITAL BUSINESS DEVELOPMENT
ON DBD.AU.DK

SITUATIONAL ANALYSES

Scan the QR code to find a step-by-step guide for this tool, digital business development cases and further inspiration at dbd.au.dk

Building block: Regulation and standards

Main question 1:

How does the company work with regulations and standards for IoT cybersecurity?

Answer:

Supporting questions

Does the company use standards for IoT cybersecurity (or guidelines)?

Is there any specific IoT cybersecurity regulation that the company should look more into?

Is the company aware of forthcoming regulation that could impact its own IoT solutions?

Is IoT cybersecurity part of the company's ongoing quality management?

Main question 2:

Why has the company chosen this approach to regulation and standards for IoT cybersecurity?

Answer:

Supporting questions

Has the company actively considered existing and forthcoming regulation relevant for its IoT solutions?

Has the company actively considered how to work with standards for IoT cybersecurity?

Has the company allocated resources for using guidelines and standards for IoT cybersecurity in the development of its solutions, products, and services?

Does the company assign any business significance to IoT cybersecurity standards?

Main question 3:

How does the company intend to move forward in implementing regulation and standards for IoT cybersecurity?

Answer:

Supporting questions

How could standards for and IoT cybersecurity regulation be implemented in a meaningful way in the company?

Would it be a concern if the company does not apply standards for IoT cybersecurity? For example for customers and suppliers?

Would it be a concern if the company fails to comply with regulation and standards related to IoT security?

Is the company adequately sized to work with standards and/or guidelines for IoT cybersecurity?

"CyPro", supported by Industriens Fond.

INDUSTRIENS FOND

UGLA INSIGHTS

FORCE TECHNOLOGY

DAMRC

ALEXANDRA INSTITUTTET

DEPARTMENT OF BUSINESS DEVELOPMENT AND TECHNOLOGY
AARHUS UNIVERSITY
AARHUS BSS

FIND OUR WEBISTE
DIGITAL BUSINESS DEVELOPMENT
ON DBD.AU.DK

SITUATIONAL ANALYSES

Scan the QR code to find a step-by-step guide for this tool, digital business development cases and further inspiration at dbd.au.dk

Building block: Processes and organisational integration

Main question 1:

What approach has the company chosen to organise its IoT cybersecurity tasks?

Answer:

Supporting questions

Is the responsibility for IoT cybersecurity assigned to one or more individuals in the company?

Is the responsibility for IoT cybersecurity assigned to an external partner?

Does the company monitor how the external partner handles the company's IoT cybersecurity?

Has the company made a structured plan incl. goals and tasks for the development of IoT cybersecurity in the company?

Is IT security (e.g. office IT) addressed in conjunction with IoT cybersecurity, or does the company consider them as two separate issues?

Main question 2:

Why has the company chosen this approach to organising its IoT cybersecurity tasks?

Answer:

Supporting questions

Has it been clarified in the company if there is a need for assigning IoT cybersecurity responsibility to one or more specific individuals?

Has the company allocated time and resources for building up in-house competence in IoT cybersecurity?

Does the organisation of IoT cybersecurity correspond to the importance of cybersecurity for the business?

How/when do you discuss IoT cybersecurity in the company? Who participates in the discussions?

Main question 3:

How does the company intend to move forward in organising its IoT cybersecurity tasks?

Answer:

Supporting questions

Does the company consistently develop its IoT cybersecurity?

Should IoT cybersecurity be part of other quality assurance initiatives in the company?

Is there a need for involving employees in the company's IoT cybersecurity initiatives?

Is it relevant to have a plan for in-house competence development in IoT cybersecurity?

Is it important to have a dialogue with the external supplier (if any) about the company's IoT cybersecurity requirements?

"CyPro", supported by Industriens Fond.

INDUSTRIENS FOND

UGLA INSIGHTS
FORCE TECHNOLOGY
DAMRC
ALEXANDRA INSTITUTTET
DEPARTMENT OF BUSINESS DEVELOPMENT AND TECHNOLOGY
AARHUS UNIVERSITY
AARHUS BSS