REFERENCE SHEET: BUSINESS

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

Awareness

- Monitoring of operations, possibly using operational data for reporting or optimisation.
- Data and other assets in the IoT solution are not considered crucial for business development.
- The benefits of increased IoT-cybersecurity are always weighed against the disadvantages for the users on the customer side.
- If the use of data-based services is considered in collaboration with other companies or partners, IoT-cybersecurity does not play a significant role in these considerations.
- The criticality of operational data is often referred to in terms of confidentiality and GDPR compliance.

Practice

- Focus on automation, optimisation and operational performance as well as production insights.
- Focus on the business potential of adopting a systematic approach to collecting data with integrity, while also focusing on availability and confidentiality.
- Strong interest in cloud solutions in the business and on identifying the security aspects if a cloud solution or a digital platform is part of the IoT solution.
- Regards IoT-cybersecurity as a benefit that can lead to increased sales, a stronger competitive advantage, and a solid reputation.
- This is combined with a focus on defining a cost-effective level of IoT-cybersecurity.
- Customers make increasing demands and ask more questions regarding IoT-cybersecurity, and the company is increasingly focusing on vendors security.
- Typically, the focus is on the availability and integrity of data to maintain operations. Confidentiality does not seem to be relevant in relation to production data.

Structure

- Focus on automation and on enhancing products and devices with services. Increased focus on providing visualised/modelled data to customers, for example via a digital platform.
- New business models based on services and data as a commodity. Cloud solutions and digital platforms for the customers have been implemented, and data sharing is increasing in usage.
- IoT-cybersecurity is a competitive parameter and a 'selling point' that differentiates the company from its competitors; it is a key brand value that requires both financial and resource investments.
- The collaboration on IoT solutions and their security is often formalised and documented.
- Focus on managing the fact that IoT solutions vary from solution to solution, and on risk appetite in terms of the availability, integrity and confidentiality of data. The new enterprise-wide digital solutions involving customer data may actualise confidentiality.

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

"CyPro", supported by Industriens Fond.

INDUSTRIENS FOND

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

REFERENCE SHEET: QUALITY

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

Awareness

- The companies in this phase are hesitant and have not typically worked with standards.
- Initiatives are in the early stages in relation to security reviews and documentation of practice.
- There are no or few daily routines, processes and procedures across the company.
- There are many ad hoc solutions, which increases system complexity.
- Standards are considered an opportunity to avoid special adaptations; however, the standardisation process is considered overwhelming.

Practical

- The companies may have – or want to obtain – a domain-specific or general ISO certification, or they use partial standards as a systematic approach.
- The standards contribute to establishing a common language around security – both internally in the company and externally in the dialogue with customers.
- Security tasks no longer arise from individual customer requirements but aim to ensure alignment with overall targets and objectives.
- There is an increasing focus on security in the overall system, rather than on individual solutions.
- The motivation for having a structured approach to standards is that the dialogue with customers on security will be strengthened, which will provide a solid basis for making informed IoT-cybersecurity decisions.

Structure

- The companies often adhere to several ISO and domain-specific standards, as well as IT standards and some (sub)standards for cybersecurity.
- Standards and/or frameworks for IoT-cybersecurity provide a structured foundation for establishing requirements and creating a common language across departments. This facilitates the dialogue with management regarding risk assessments and the allocation of resources for security.
- Typically, documentation is an integral part of the companies' development process from the beginning.
- The motivation for using standards is that certification is considered a competitive advantage and provides a systematic approach to communicating about IoT-cybersecurity both internally and externally. Additionally, the use of standards makes it easier to comply with regulation.

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

"CyPro", supported by Industriens Fond.

INDUSTRIENS FOND

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

REFERENCE SHEET: ORGANISATION

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

Awareness

- The responsibility for IoT cybersecurity is not in focus or is unresolved.
- There are no or few in-house competencies in IoT cybersecurity. In-house competencies may be found with a technically savvy enthusiast who often relies on external advisers and vendors for sparring and for delivering IoT cybersecurity.
- Technical enthusiasts may deliver presentations on IoT cybersecurity to managers/executives. It is a huge communication task to make the business understand the consequences of a given risk level/risk appetite.
- Internally, discussions around IoT projects mainly focus on technical and operational perspectives, which sometimes also include IoT cybersecurity.
- There are no IoT contingency plans.
- Generally, the IoT cybersecurity approach is often a response to customer inquiries about IoT cybersecurity.

Practical

- One or more persons have a formalised role that involves responsibility for IoT cybersecurity, either internally or externally (for example the IoT vendor).
- There are some in-house competencies, as well as external sparring with for example consultants, partners and vendors. External risk assessments are carried out on a regular basis for quality purposes.
- Management supports IoT cybersecurity and has a clear stance on it, considering the financial aspects of security investments. Management receives reports on IoT cybersecurity and allocates funds for it.
- Internal communication focuses on a shared understanding of IoT cybersecurity based on frequent dialogue.
- Contingency plans for IT exist, but not for IoT explicitly. Would have to rely on vendors or partners if an incident occurred.
- In the process of developing procedures for IoT cybersecurity (such as contingency, risk assessment, reporting, and IoT cybersecurity throughout the lifecycle of the solution).

Structure

- The responsibility for IoT cybersecurity is anchored in-house, supplemented by external advisers. Clear organisation of roles and how they collaborate, incl. business, operations, and strategy.
- Access to necessary IoT cybersecurity competencies, both in-house and externally.
- Management takes part in assessing risks and consequences on an informed basis, enabling them to allocate resources or accept the risk. The main purpose of IoT cybersecurity is to develop the business.
- Internal communication is inter-disciplinary, with a focus on knowledge sharing, policies, guidelines, etc. Clear communication from management about the importance of IoT cybersecurity.
- Contingency plans exist for critical IoT systems.
- Structured approach to IoT cybersecurity and risk assessment from concept to implementation, incl. financial consequences such as product price. As part of the risk assessment, all products are mapped, perhaps in collaboration with vendors.

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

"CyPro", supported by Industriens Fond.

INDUSTRIENS FOND

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

REFERENCE SHEET: TECHNICAL 1/2

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

Awareness

- The focus is on strengthening and cultivating a shared understanding of IoT cybersecurity. The general attitude regarding the risk landscape is that the functions and data associated with the IoT solution are not critical per se.
- The main focus is on providing security around the critical functions of a particular product, which often means ensuring operational performance.
- The general security measures do not yet encompass IoT cybersecurity, and there is no shared approach to IoT cybersecurity in the company.
- The IoT components that are part of the solutions may have been acquired from a specialist vendor who is expected to have built security into their components.
- The physical dimension of the IoT solution is often not secured, or physical security is not considered relevant.
- Solution updates do occur; however, it is often a manual process. In some cases, updates are not released at all, or the company relies on the vendor to do it.

Practical

- The approach to IoT cybersecurity is seen as a shift from performing ad hoc tasks to establishing a uniform, risk-based IoT cybersecurity level and foster a shared understanding of security practices across the company.
- Security is either built into the IoT solution from the start, or it will be upgraded on a regular basis as more insight is gained.
- The necessary IoT cybersecurity competencies are available in-house but external experts are consulted when necessary.
- The physical dimension of the IoT solution is assessed separately: Is there physical access to data? What are the associated risks? How can such risks be mitigated?
- The aim is to establish both a technical framework and procedures for releasing updates on a regular basis. Work is in progress to create a structured overview of known vulnerabilities, how to patch them, and which devices are to be updated by the company and which by the vendor.
- Systems are in place for monitoring patterns in the system, and an alarm is triggered in case of anomalies.

Structure

- There is a holistic approach to security where all usage scenarios and contexts for the solution are assessed.
- Managers and staff develop IoT cybersecurity based on shared and structured technical processes, and dedicated resources have been allocated.
- When building security, the choice of options is based on a structured and ongoing risk assessment that involves the entire value chain and lifecycle of the product.
- The solution incorporates multiple layers of security, including both external defence and in-depth layers to limit the damage in the event of a security breach.
- There is a shared understanding that failure to control physical access to the solution is equivalent to lack of security.
- Most of the system is designed to accommodate updates, and updates are released regularly. Targets have been set for the time it should take to patch a solution after a vulnerability is discovered.

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

"CyPro", supported by Industriens Fond.

INDUSTRIENS FOND

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

REFERENCE SHEET: TECHNICAL 2/2

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

Awareness

- Some companies do not have any logging in place; some see it as the vendor's responsibility, while others have logs but use them only sporadically.
- The primary focus is on securing user access to the platform rather than to the unit itself.
- Encryption is used on an ad hoc basis, depending on the capabilities of the platforms already chosen, or what the developers are familiar with. Communication is for example encrypted using HTTPS(TLS) without considering additional cipher-modes and key management.

Practical

- The main focus of monitoring is operational performance, for example by logging errors.
- Security measures are in place for user creation, along with traceability of user behaviour and restricted user actions.
- Developers are familiar with best practice and use only 'secure' algorithms. Components/platforms are rejected if they do not support an appropriate level of algorithms

Structure

- The system is constantly and systematically monitored, and fixed response times have been established.
- The solution incorporates built-in access control – also physical. As an example, users must authenticate themselves using two or three factors.
- The choice of cryptographic algorithms has been registered and is reviewed on a regular basis to identify any new vulnerabilities. Components are chosen based on the prerequisite that the cryptographic algorithms can be replaced if necessary.