THE CURRENT STATE OF CYBERSECURITY IN DIFFERENT SECTORS – KEY SURVEY FINDINGS

HUOLTOVARMUUSORGANISAATIO

THE CURRENT STATE OF CYBERSECURITY IN DIFFERENT SECTORS – KEY SURVEY FINDINGS

www.huoltovarmuus.fi

HUOLTOVARMUUSORGANISAATIO
DIGIPOOLI

Security of supply refers to society's ability to maintain the basic economic functions required for ensuring people's livelihood, the overall functioning and safety of society, and the material preconditions for military defence in serious disruptions and emergencies.

The National Emergency Supply Agency (NESA) is an organisation operating under the Ministry of Economic Affairs and Employment. It is tasked with planning and measures related to developing and maintaining security of supply.

Publisher:
The National Emergency Supply Organisation's Digital Pool

Authors of the summary:
The National Emergency Supply Agency in collaboration with the Digital Pool and the Finnish Transport and Communications Agency's National Cyber Security Centre. Based on a survey commissioned by the Digital Pool and carried out by KPMG.

Images: Shutterstock

Layout: Up-to-Point Oy

Year of publication: 2020

ISBN: 978-952-5608-83-0

Table of contents

1 INTRODUCTION

The importance of cybersecurity in terms of security of supply is constantly increasing as companies critical to the functioning of society continue to digitise their key functions. As a result of this development, digital environments and connections no longer merely support companies' business operations, but have in fact become essential for them. With digital security becoming an increasingly vital precondition for companies' business operations, the relative extent at which it is examined from a security of supply standpoint should also be increased accordingly.

Targeting measures for promoting cybersecurity and monitoring their effectiveness has so far been difficult due to a lack of comparable data. To address this, the National Emergency Supply Organisation's Digital Pool decided to carry out a comprehensive survey of the current state of cybersecurity, covering 12 sectors and over 100 companies. The survey consisted of 30 questions designed to shed light on the current perspectives of companies' business management personnel on the management and steering of cybersecurity in Finland. The results of the survey were used to determine areas in need of development in regard to the cybersecurity of companies, sectors and the dependencies between them.

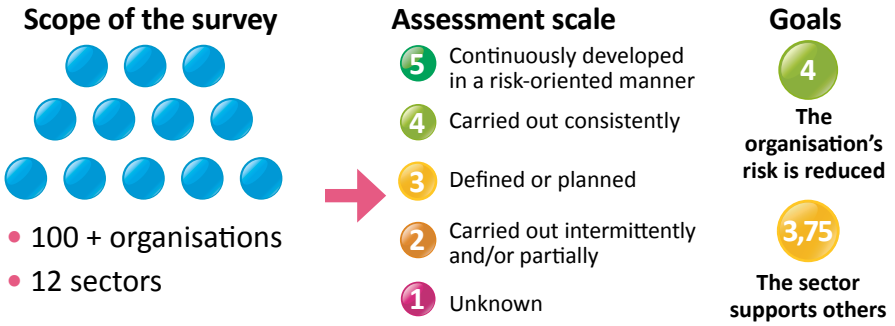
The factor that has the most notable long-term positive impact on the development of an organisation's cybersecurity is the commitment of the organisation's top management to promoting cybersecurity by setting objectives for it and defining associated responsibilities. When this is the case, the development of cybersecurity is most likely to be systematic and risk-based instead of being dependent on the expertise and enthusiasm of individual cybersecurity experts. It is the consistent realisation of these basic aspects that was measured in the survey.

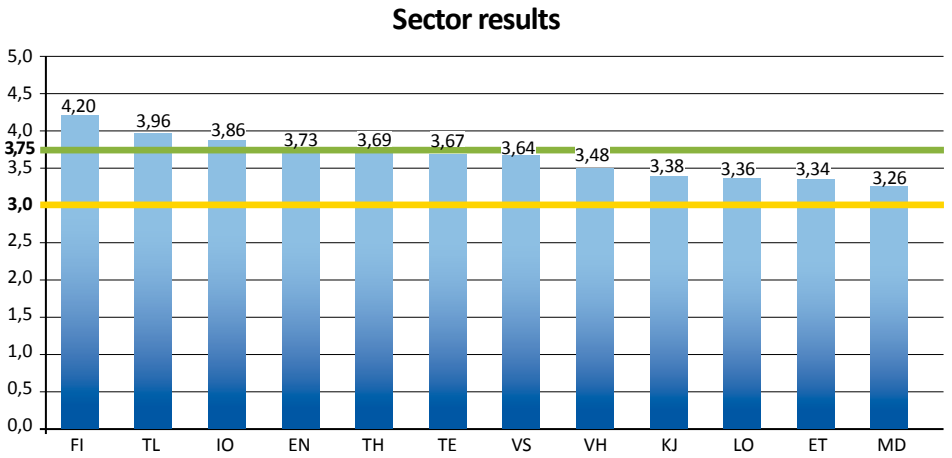
This summary presents the most notable development areas and key findings based on the results of the survey reports. The companies that participated in the survey have also been provided with reports of their own and sector-specific results. In addition to this, reports on sector-specific results will also be distributed to parties responsible for the development of operations, such as the NESO pools.

The core finding of the survey was that the state of cybersecurity is, on average, at least moderate in all sectors, though there is broad variation between companies. From a security of supply standpoint, it is imperative that these differences be evened out so that interdependent networks remain capable of withstanding cyberattacks throughout. The current state of cybersecurity provides a good starting point for ensuring this. The results of the survey will also serve as an important knowledge base for selecting projects for the National Emergency Supply Agency's Digital Security 2030 programme for 2020–2025, which is currently under preparation.

Commissioned by the Digital Pool, the survey was carried out by KPMG's cybersecurity consultants in winter 2019–2020. The results were used to determine the starting level of cybersecurity for each of the included sectors. The survey is planned to be carried out regularly approximately every two or three years for the purpose of monitoring the impacts of development measures initiated and general trends.

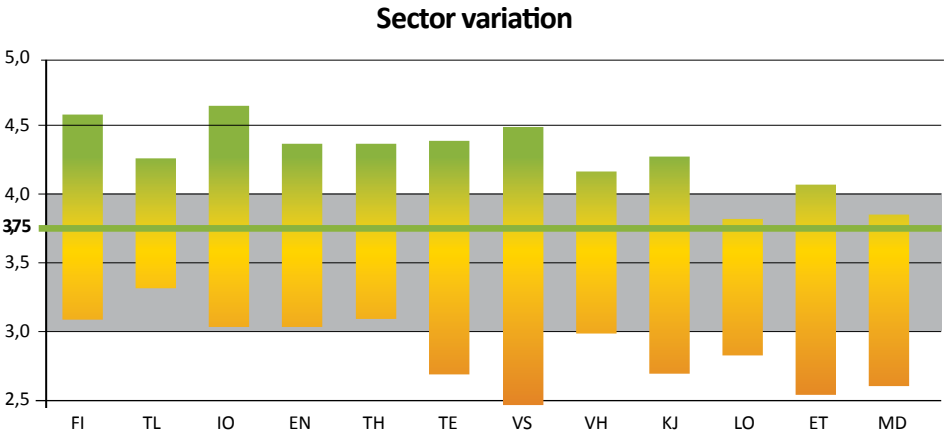
2 SUMMARY OF THE RESULTS





FI= financial, TL= telecommunications, IO= ICT and software, EN= energy, TH= health care, TE= manufacturing, VS= port and maritime, VH= water services, KJ= trade and distribution, LO= logistics, ET= food, MD= media

Figure 1. All sectors exceeded the rating of mediocre.



FI= financial, TL= telecommunications, IO= ICT and software, EN= energy, TH= health care, TE= manufacturing, VS= port and maritime, VH= water services, KJ= trade and distribution, LO= logistics, ET= food, MD= media

Figure 2. Variation between companies was high in many sectors.

DEVELOPMENT AREAS

The most notable common ones from a security of supply standpoint

1. common situational awareness
2. secure software development
3. personnel skills

The most important common ones from the perspective of companies' business operations

1. company cybersecurity strategy
2. cybersecurity architecture
3. technical traceability

In addition to the above, there are also sector-specific development areas that will facilitate security not only in the sector in question, but in terms of the dependencies between sectors.

CONCLUSIONS BASED ON THE RESULTS

Present challenges

1. Understanding dependencies between sectors is important for security of supply.
2. The management of cybersecurity is often isolated to individual departments instead of being all-encompassing.
3. There is still room for improvement in the basics.

Support development

4. Variation facilitates cooperation.
5. Maturity levels highest in reactive operations.
6. Companies recognise cybersecurity in the supply chain in a contract-based manner.
7. Regulation has a positive effect on the promotion of cybersecurity.

To note:

The results illustrate the maturity of cybersecurity processes and methods to companies' business management for the purpose of supporting management and steering. The results do not directly describe the technical level or realisation of cybersecurity in individual companies, which may differ from the results when managed by capable cybersecurity personnel or service providers. However, it can be assumed in general that cybersecurity is best developed when management is committed to it and steer operations – when set objectives are in line with the practical realisation.

3 KEY DEVELOPMENT AREAS

The survey revealed several cross-cutting development areas that were highlighted in the results by all of the three assessment methods used (business risk-oriented, risk-based and sector dependence-oriented). The key development areas were determined with an emphasis on how critical they are from a business risk standpoint, as this aspect was considered to have the most notable impact on security of supply in terms of the functioning of companies and critical sectors. The development areas highlighted based on this broad, consistent assessment are the most significant merit of the survey.

In the figure below, the development areas are divided into two categories based on whether the realisation of the objective is primarily up to individual companies or a joint, security of supply concern.

Key company-level development areas common to several companies:

1. company cybersecurity strategy (3.1)
2. cybersecurity architecture (3.2)
3. technical traceability (3.3).

Key security of supply-level development areas:

1. common situational awareness (3.4)
2. secure software development (3.5)
3. personnel skills (3.6).

The most important development areas may vary greatly between companies, as there was a considerable amount of variation in the results. Companies that attempted to prove the realisation of cybersecurity in practice despite a lack of documentation generally had lower results. Such attempts were seen as indicating that the company's management had not prepared a clear strategic policy and associated objectives. Many of the differences in the results between sectors can be explained by the special characteristics of individual sectors and the extent to which the sectors have been affected by digitalisation. The key points of sector-specific results are presented in section 5 and the appendices. The key development areas common to a large proportion of the sectors are examined in the following sections.

3.1 Planning a company cybersecurity strategy

Explanation: A company cybersecurity strategy serves as the foundation for the development of cybersecurity. At its simplest, a company cybersecurity strategy includes the goals of cybersecurity and a plan for achieving said goals. At higher maturity level, a company cybersecurity strategy also includes priorities, a description of the management model, the structure and responsibilities of the cybersecurity management organisation and the executive management's commitment to and participation in the planning and organisation of cybersecurity management.

According to the survey results, companies in several sectors do not possess a sufficiently comprehensive risk management strategy, cybersecurity strategy or cybersecurity risk management system. When this is the case, cybersecurity is viewed primarily as a technical support function instead of being seen as an area subject to long-term development and risk management that supports the company's business operations. A company wishing to adopt an operating model that makes effective use of information technology must define a goal state for cybersecurity and a strategy for achieving it.

The preparation of a cybersecurity strategy can be carried out as part of business risk management or security planning, for example. Without a cybersecurity strategy, increasing IT dependencies will significantly increase the business risks associated with functions dependent on information technology. The preparation of a cybersecurity strategy paves the way for adopting a model that supports and facilitates operations instead of merely reacting to threats.

It should be noted that a cybersecurity strategy need not necessarily be a long document, as long as it effectively steers the security development, choices and investments of personnel responsible for cybersecurity over the long term. When it does, policymakers are provided with development proposals that correspond to their vision for cybersecurity.

Every company is individually responsible for preparing their own cybersecurity strategy and managing cybersecurity risks based on it. That being said, the preparation of company cybersecurity strategies can be promoted through the issuing of guidelines and the establishment of practices for facilitating it.

3.2 Cybersecurity architecture

Explanation: Cybersecurity architecture is an essential part of a company's overall information system architecture. It is used to describe the structure of the organisation's security processes, cybersecurity systems and personnel and their relationship to the organisation's goals and strategic plans. The successful differentiation of IT and OT environments is an important part of cybersecurity strategy.

Based on the survey, only few companies currently manage their cybersecurity architecture as part of their overall IT system architecture. Furthermore, the level of architecture is quite varied. The security management of IT (information technology) and OT (operational technology) environments should be an everyday part of operations and a way of implementing the company's cybersecurity strategy instead of consisting of protection and observation measures built after the fact around digital implementations. While in some organisations this was already case, which was a positive finding, at most companies the management or cybersecurity architecture was still under preparation at the idea level or would require external support to set up. The majority of organisations reported that their management strongly supports the maintaining and development of cybersecurity architecture, but that it is not yet a part of their operations.

Each company's cybersecurity architecture is individual, requiring a company-specific implementation. To develop security of supply, the best way to support companies is to establish practices and develop methods for assessing solutions implemented.

3.3 Technical traceability

Explanation: The state of the assets being protected (identified through monitoring) affects the situational awareness. At the highest maturity level, log data from critical systems is systematically collected by a centralised log management system for continuous monitoring, and the organisation's threat profiles and risks are taken into account in log management.

Technical traceability, i.e. log management, is in and of itself an important measure that promotes cybersecurity, but it also serves as a foundation for many other measures. Logs facilitate situational awareness and are an vital part of the successful remediation of and quick recovery from security incidents. Thus technical traceability also supports development work by facilitating the remediation of observed problems. A logging policy based on best practices, i.e. sufficiently comprehensive logging and asset management that supports logging, is one of the cornerstones of forming a good and up-to-date situational awareness (3.4). However, the results of the survey indicate that there is still room for improvement in the logging practices of many operators.

Implementing a logging system is a company-specific procedure for which there are many solutions and guidelines for ideal implementation available on the market, as a result of which implementation is relatively easy. Improving security of supply in this regard requires finding ways of allowing companies to implement comprehensive logging in their networks and systems. This will facilitate the practical implementation of logging systems in companies, thus supporting the maintenance of cybersecurity.

3.4 Situational awareness development

Explanation: One of the core aspects of maintaining a common situational awareness is communicating the situational awareness to key policymakers and the interest group network. Many common situational awareness implementations also include visual elements (such as control panels, maps or other graphical interfaces), but they are not mandatory for achieving objectives. Organisations can also employ other means of communicating their situational awareness.

The primary goal of a situational awareness is to provide information of the current or future situation that supports cybersecurity. The need for a common situational awareness was highlighted in the both the company-specific and sector-specific results of the survey. The concept of a situational awareness is broad, encompassing many different areas, the current maturity level of which varies greatly. The figure below provides a rough division of these levels.

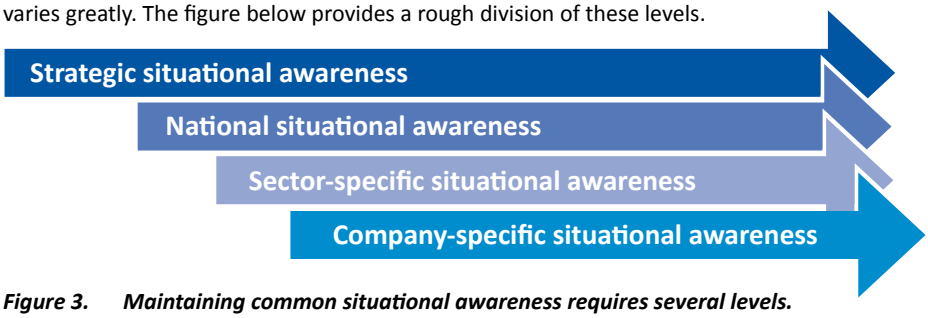


Figure 3. Maintaining common situational awareness requires several levels.

For company management, a strategic situational awareness provides information on future development trends. It provides the necessary support for defining strategies and corresponding investments to support business operations. Thus, it is important from a security of supply perspective to develop a strategic situational awareness of cybersecurity that can be commonly utilized.

Over the years, a number of development measures have been carried out in Finland to establish a national situational awareness. Examples include the establishment of the National Cyber Security Centre, which has in turn established various situational awareness products and ISAC information sharing networks. Cooperation between companies and the authorities has also been increased, and the results of the survey indicate that this cooperation should be continued and further developed.

Companies also have a need for a sector-specific situational awareness. The realisation of a sector-specific situational awareness is facilitated by joint development, in which companies are strongly committed to. This development should be invested in through the utilisation of existing network structures, especially ISAC networks.

There is also a need for company-specific situational awareness, the establishment of which is primarily a part of companies' internal development efforts. A company-specific situational awareness facilitates the maintenance of the cybersecurity of the organisation's systems in terms of company-specific hardware and software choices and in relation to organisations in the dependence chain of operations. It can be supported through the preparation of best practices, which comprehensively help companies critical to security of supply to define examples of situational awareness content that support their operations. The aforementioned sector-specific and national situational awareness support the establishment of company-specific situational awareness in terms of content.

3.5 Secure software development

Explanation: It is important to adhere to and require compliance with secure software development guidelines when developing software that contains protected assets. Doing so significantly decreases the probable occurrence of vulnerabilities.

Secure software development is mentioned in the development area lists of all sectors and was highlighted as the most important development area in the results of several sectors. It is highlighted as particularly important in sectors where the lifecycles of the systems used are typically long, such as in energy production and water services.

Cyber risks are realised in practice through software. Secure software development reduces the realisation of threats, steers personnel to use software and applications in a secure manner and reduces the impact of errors. Software security should be taken into account in all the stages of a system's lifecycle, from procurement all the way to decommissioning. Systems with long lifecycles pose particularly high risks in terms of their software vulnerabilities because of how expensive such software is to update and maintain. Furthermore, the continuity of the software developer's operations also becomes a risk over time. Software security should be taken into account not only in the procurement of off-the-shelf software, but also in the use of customized software, self-made software and pieces of code in both the organisation's own environments and on cloud services as well.

Taking the security of software into account is first and foremost a shared development area. This shared need stems from the broadly adopted approach of taking cybersecurity and continuity management into account in software development from the very beginning. This approach is systematically realised when the employees of software developers are adequately trained to carry out and offer secure software development. On the other hand, as purchasers, companies must also be able to demand software security as part of software procurement and contracts. At national level, it would be useful to adopt shared recommendations concerning minimum requirements for software security, for example, as has been done on the consumer side with the National Cyber Security Centre's Cybersecurity label.

3.6 Development of personnel skills

Explanation: To uphold a culture of cybersecurity, companies should preferably plan and implement measures, processes and technologies and train personnel to cultivate a positive attitude towards cybersecurity and increase associated skills – taking into account risks related to the organisation's goals and critical infrastructure.

The cybersecurity skills of personnel are highlighted in the results of the survey from several different perspectives. One perspective is the basic cybersecurity skills of a company's entire personnel, another is the upholding of the skills of cybersecurity experts in the sector and a third is the lifecycle management of employees' employment relationships. These perspectives are all important.

The cybersecurity skills of personnel should be improved particularly in sectors where they are not part of core competencies or where personnel turnover is high, such as in the trade and distribution sector. Additionally, attention should also be paid to the cybersecurity skills of personnel in sectors requiring special know-how, such as manufacturing, water services or energy production.

The development of cybersecurity personnel also includes addressing recognised skill needs through recruitment and training. For example, companies should have recruitment measures in place for ensuring that the individuals carrying out recruitment and the interviewees are aware of cybersecurity personnel needs. This also includes understanding of security clearances. Furthermore, new employees (and software and service providers) should complete a cybersecurity training course to reduce their susceptibility to social hacking and other threats.

The cybersecurity skills of employees vary between companies, though many of the basic skills that personnel are required to possess are the same across different companies and sectors. Because of this, there are numerous common development areas to be found in this field, which, when addressed, would benefit all companies and comprehensively improve the cybersecurity of companies critical to security of supply.

4 CONCLUSIONS ABOUT THE ADVANCEMENT OF CYBERSECURITY

The results of the survey convey an impression that the organisations selected to take part in the survey have a very good understanding of their important position as providers of products and services that are vital to Finnish society. This understanding facilitates the preparation of common development measures.

The results of this survey provide some insight as to which previously implemented measures have improved cybersecurity in specific sectors or areas. On the other hand, the results also highlight areas where a more comprehensive overall understanding is needed before cybersecurity can be advanced in an all-encompassing manner.

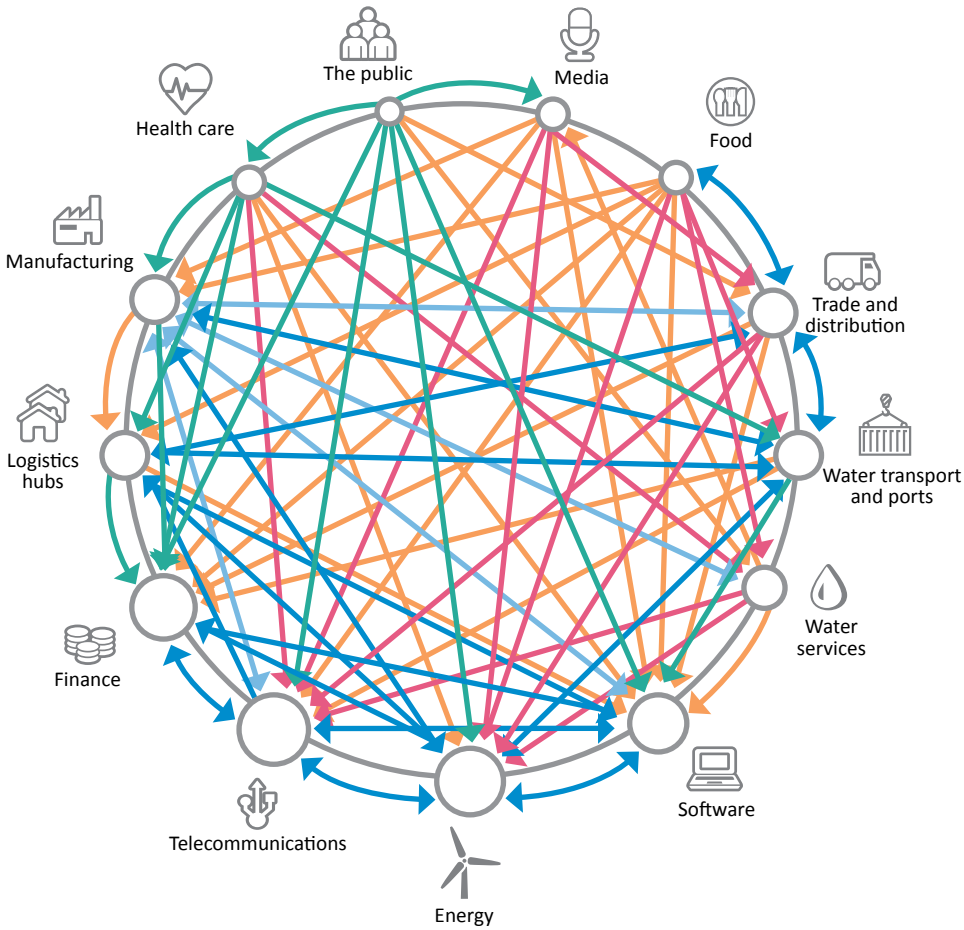
One general observation is that in many organisations, cybersecurity matters are not handled at the executive management level. A good starting point for supporting company management personnel in the handling of cybersecurity matters and facilitating the resulting cultural change would be to introduce them to the Cyber security and the responsibilities of boards guide prepared by National Cyber Security Centre of Traficom. This cultural change is also a prerequisite for the deployment of many effective development measures and thus the key to the national development of cybersecurity, which also promotes the realisation of digital security of supply.

4.1 Understanding dependencies between sectors

Safeguarding the functions critical to society and security of supply is based on chains of dependencies. From a security of supply standpoint, these chains should be identified so that the impacts of any disruptions within them can be minimised. All of the sectors included in the survey recognised that their current digitalised operating models make them dependent on the basic infrastructure sectors, namely the financial, telecommunications, software, energy and manufacturing sectors. These sectors form the core of basic infrastructure, the disruption of which is quickly and broadly reflected in the rest of society.

The dependencies between sectors can be examined at a general level via the figure below. Actual threats are ultimately realised via individual operators and the individual systems that they use instead of directly as depicted by the figure. Nevertheless, the figure helps illustrate how diverse and interdependent a network the sectors form. As digitalisation continues to progress, the network will also continue to grow more complex. Disruptions have different impacts on the network depending on their duration: short disruptions lasting only minutes or hours are different in terms of the applicable measures and impacts than ones lasting days or weeks. These different temporal dimensions must be taken into account when planning continuity management measures.

Sector dependencies



= the sector that the arrow is drawn from is fully dependent on the sector that the arrow points to

= the sector that the arrow is drawn from is dependent to a significant degree on the sector that the arrow points to

= the sector that the arrow is drawn from is partly dependent on the sector that the arrow points to

= the sectors that the arrow points to are dependent on each other

= the intensity of the blue colour indicates the degree of dependence

= the size of the circle denotes how important the node is in the dependency network

Figure 4. Sector dependencies according to the Cybersecurity in Different Sectors survey in 2020.

Disruptions in the network can be prepared for in the following two typical ways, for example:

1. ***By improving the cybersecurity of the sector to make it more resistant to disruption,*** thus lessening the impact on operations. In cyber environments, resistance to disruptions means alternative connections and backup systems, for example.
2. ***By adopting alternative operating methods*** for the duration of the effects of disruptions. A typical example of an alternative operating method would be the use of backup power in the event of a power outage or reverting to manual operation for the duration of a software problem.

It should be noted that even if operational capability is maintained, the measures implemented to maintain it can also affect other sectors. The most recent example of this would be the safeguarding of the operational capability of the health care sector during the COVID-19 pandemic, which has had secondary effects on many other sectors. Even short disruptions can affect the operations of several sectors. One example of this is water services: a water supply interruption lasting only a few minutes can cause food sector operators, hospitals and manufacturing plants to suspend their operations unless they have a backup water supply for temporary interruptions.

The most important customers of an individual organisation or sector in the network usually consist of other organisations, through which the effects of disruptions are also reflected on the authorities and citizens. The fact is that nobody is capable of fully controlling the entire network. Instead, each organisation is a kind of node that serves as both the source and target of changing connections. Improving the maturity of your own node improves the operating reliability of the entire network. For example, problems affecting telecommunications connections are quickly reflected in the everyday operation of other sectors as well if they cause networks to become inaccessible and prevent the sending of e-mails. Similarly, a software problem affecting a logistics company can cause transport disruptions, which will in turn affect the availability of products and spare parts in other sectors.

For the aforementioned reasons, organisations hoping to develop their cybersecurity should not limit their focus to their own operations, instead they should also consider how their operations are dependent on other sectors or how their operations affect other sectors – and engage in cooperation and the exchange of information with other operators in their supply chains for their own benefit in the area of cybersecurity. It might be worth considering whether the exchange of information and common preparation should also be noted in contracts.

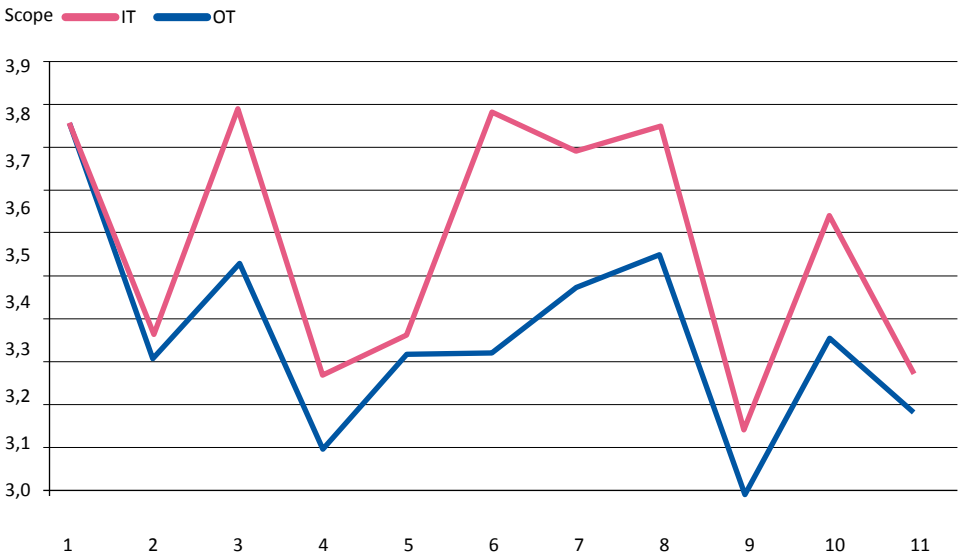
4.2 Managing cybersecurity and the division between information technology (IT) and operational technology (OT)

The concept of cybersecurity is often divided into two or more environments. These environments typically consist of:

- the IT environment, meaning the traditional office network
- the OT environment, meaning the operational production environment

Based on the survey, these two environments are often managed and controlled completely separately. In several sectors, this has resulted in differences in the cybersecurity maturity of the two environments within companies. Because of this, the results of the maturity assessment of IT and OT environments were recorded separately for each environment. The average results are present-

ed as a graph on page 18. As a result of networking, operations in the two environments are rarely completely separate, and ideally the advancement of cybersecurity should be managed consistently across both environments. This kind of consistency can be ensured via the preparation of an all-encompassing cybersecurity strategy (3.1), in which the separate needs and security environments are taken into account via segmentation in the implementation of cybersecurity architecture (3.2).



1. protection of critical services
2. risk management
3. management of protected assets, changes and configurations
4. cybersecurity management system
5. supply chain and external dependency management
6. identity, access and authorisation management
7. event and incident management, continuity of operations
8. information sharing and communications
9. situational awareness
10. threat and vulnerability management
11. personnel management

Figure 5. Maturity assessment of IT and OT environments.

4.3 Still room for improvement in the basics

The results of the survey indicate that there are still many basic areas of cybersecurity that are not being systematically managed. For example, many companies list technical traceability (logging) and access control (identity management) among their development areas, even though there have been plenty of guides and technical solutions available for implementing them for years.

Unfortunately, raising the level of cybersecurity is only possible once the fundamentals have been sufficiently well realised, which requires constant work on improving the basics. This, in turn, requires increasing the cybersecurity awareness of management, personnel and cybersecurity experts alike. In practice, cybersecurity awareness can be increased though personnel development (3.6) and exercises.

4.4 Variation facilitates cooperation

The survey results revealed similar development areas across a number of sectors. With many sectors facing the same challenges, focusing on common development areas can effectively improve best practices. This approach also supports security of supply by decreasing differences between companies in regard to cybersecurity within and across sectors. This will also reduce the impact of cybersecurity disruptions on the chains of dependence between sectors.

Cooperation between organisations should be supported via the development of existing cooperation structures, such as exercises, examples of which include the Digital Pool's TIETO exercises and the National Cyber Security Centre's ISAC sector networks, which are tailored for exchanging cybersecurity information. To supplement these, it would also be beneficial to come up with new cooperation methods that would facilitate the exchange of situational awareness information across sectors (3.4), for example.

4.5 Maturity levels highest in reactive operations

Of all the cybersecurity measures covered in the survey, the most effectively managed overall were reactive and observational operations. This is reflected in the results in both the documenting of event and incident management and the continuity planning of basic operations: based on the results, the safeguarding of critical services and the management of protected assets, changes and configurations are moderately well acknowledged in many companies.

Many reported cybersecurity incidents have ultimately been the result of problems in identity, authorisation and access management. These problems have apparently also gained much-needed attention as a result of security breaches, as this area was not among the key development areas highlighted in the survey results. While continued development is essential in this area as well, the results indicate that organisations have successfully implemented related solutions. There are also existing models and solutions available to companies that still need to develop in this area.

Over the years, guides on how to manage incidents have been prepared by several different parties. The development of reactive operations has also most likely been facilitated by the HAVARO system implemented in previous development programmes, the exchange of information and exercises carried out as part of ISAC operations and exercises themselves. However, there is variation in the results and the cybersecurity environment is constantly changing, which means that development efforts should be continued and kept up to date.

4.6 Companies recognise cybersecurity in the supply chain in a contract-based manner

The survey revealed that companies are well-versed at taking continuity management into account in contracts when procuring know-how, products or services from companies operating in other sectors in the chain of dependence. Contracts include clauses on how the continuity of the service should be realised and what the consequences are if interruptions or disruptions affect the client's operations. These results provide a good foundation for further reducing impacts in the chains of dependence in the future.

4.7 Regulation has a positive effect on the promotion of cybersecurity

Sectors can be steered to improve their security though legal statutes and regulations. They also promote the security of the dependency network by providing companies with access to impartial information on what is expected of the companies in their dependency chain operating in different sectors and issues that do not need to be separately agreed upon to ensure one's own security.

The results show that sectors that have long been regulated and steered and monitored by the authorities come out on top in the comparison. While the extent to which regulation plays a role in this was not separately assessed in the survey, the positive effect is apparent both statistically and when comparing sectors based on workshop discussions.

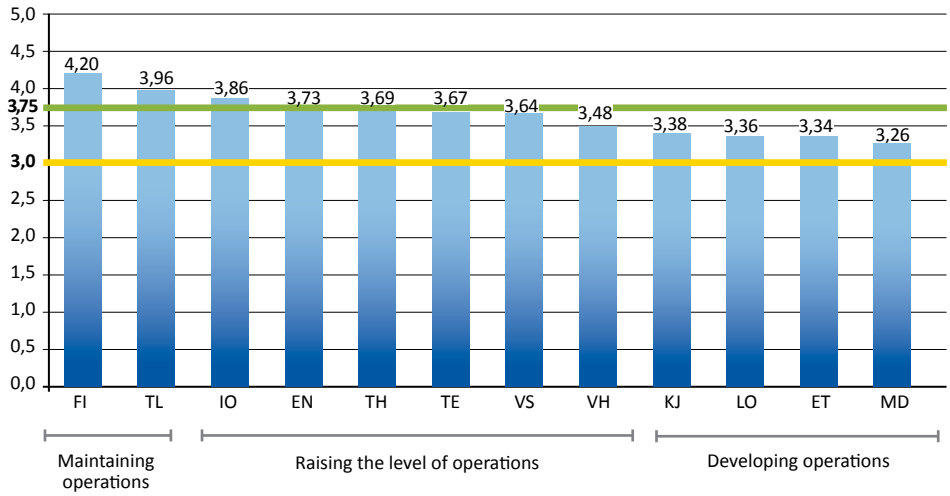
It should be noted that regulation is a slow way of improving the rapidly changing field of cybersecurity. The precise targeting of measures is challenging due to rapid transformation of threats. Experience also indicates that preparing regulations that treat organisations of different sizes equally is no simple task, with the results often impeding the operations of small and medium-sized organisations in particular, which are common in Finland. Regulation is most effective when it is used to set a minimum level for requirements. Some measures can be steered with the help of initially less demanding recommendations. One of the most notable regulations steering the operations of the most critical sectors is the EU Directive on security of network and information systems (the NIS Directive), which entered into effect in 2018 and continues to be developed.

Finally, it should be noted that an individual company's state of cybersecurity is primarily dependent on the commitment and steering of the company's management – how effectively required measures have been implemented and whether their implementation is promoted for the purpose of supporting the company's own operations, or for the sake of fulfilling requirements. At best, these aims can mesh in a way that allows regulation to support the realisation of cybersecurity.

5 KEY OBSERVATIONS BASED ON SECTOR-SPECIFIC RESULTS

In all sectors critical to the functioning of Finnish society, the level of cybersecurity is at least moderate, meaning that associated measures have been defined or planned. This is a good starting point for further improving and standardising cybersecurity. However, it should be noted that there are significant differences between and within sectors. The reasons behind these difference include:

- size differences between operators
- available resources
- the effects of domestic and international regulation on the sector
- contractual demands from clients
- different sectors are at different positions in regard to the advancement of digitalisation.



FI= financial, TL= telecommunications, IO= ICT and software, EN= energy, TH= health care, TE= manufacturing, VS= port and maritime, VH= water services, KJ= trade and distribution, LO= logistics, ET= food, MD= media

Figure 6. The maturity level of sectors can be divided into three categories: maintaining operations, raising the level of operations and developing operations.

The financial sector and the telecommunications sector have reached the target maturity level of four, meaning that cybersecurity is consistently realised in these sectors. It is important to continue to implement development measures in these sectors to maintain the achieved level as the cybersecurity environment continues to change.

In the sectors occupying the subsequent positions in the results (i.e. ICT and software, energy, health care, water transport and ports, water services), cybersecurity measures have been widely realised as planned, though there is still room for improvement in some specific areas and several individual

companies. These sectors are in a good position to develop their operations to a more mature, i.e. consistently realised, level. The main development goal of these sectors is harmonisation, which will facilitate the improvement of their maturity level.

The media, logistics, food and trade and distribution sectors, which have all entered a period of extensive digital transformation, achieved a moderate level of maturity in the results. In these sectors, raising the level of cybersecurity requires companies to set common goals and engage in harmonised development so that cybersecurity is also taken into account in the advancement of digitalisation.

From the perspective of the interdependencies of cybersecurity, it is worth noting that the sectors occupying the four top positions in the results (finance, software and ICT, telecommunications and energy) are the same four sectors that form the core of basic infrastructure (4.1). Considering security of supply as a whole, it is appropriate for the level of maturity of cybersecurity to be highest in the sectors that are the most important in terms of interdependencies.

All operators in a digitalised society face similar cybersecurity threats, as a result which the identification and management of threats should be carried out collaboratively between public and private sector operators. Cybersecurity should be developed at all levels: by organisations that provide services critical to society, by the National Emergency Supply Organisation's sector-specific pools and by the entire National Emergency Supply Organisation. Summaries of sector-specific results are presented in appendices 1–12.

6 EXECUTION OF THE SURVEY

The survey was carried out by first choosing the maturity assessment model and the sectors and companies critical to security of supply to participate in the survey. The scores and clarifying explanations were reviewed in interviews in winter 2019–2020. From companies, representatives from business, data management and security were interviewed. Before the interviews, the interviewees were provided with the opportunity to independently review the maturity assessment questions to gain an understanding of the areas covered. The maturity values were proportioned in accordance with an objective set of criteria with the help of clarifying justifications. After this, the company-specific results were aggregated to determine the sector-specific results. As such, the comparability and quality of the results can be considered good, as the results of different companies were objectively scaled to the same scale.

Selection of participants

With the assistance of the NESO's sector-specific pools, companies of different sizes operating in 12 sectors around Finland were selected to participate in the survey, to ensure that the results would provide a comprehensive understanding of the current state of cybersecurity. Selection was based on the NIS Directive, the pool organisation and security of supply decisions. Some compromises had to be made in the naming of the sectors so that the survey work would remain manageable while still providing a sufficiently broad sample of different organisations. In addition to providing a national overview, it was considered important to provide sector-specific results.

The participating organisations included the following producers or service providers:

1. **food sector:** primary production and food industry
2. **energy sector:** electricity production and distribution and oil refinement
3. **financial sector:** banking, insurance
4. **ICT and software sector:** data security, software production
5. **trade and distribution sector:** retail trade, wholesale trade, distribution
6. **logistics sector:** logistics and transportation hubs
7. **media sector:** graphic media, mass communication
8. **telecommunications sector:** operators, network contracting
9. **manufacturing sector:** chemistry and construction
10. **health care sector:** pharmaceutical production, logistics and treatment
11. **water services sector:** water supply, distribution and sanitation
12. **water transport and ports:** port authority and operator

In total, over 100 companies participated in the survey. At least six companies participated from each sector to ensure that the survey included different types of operators and so that the operations of an individual company would not affect the entire sector's results to an excessive degree. The participating companies were selected from among the organisations of each sector based on their turnover, geographical location, their significance to security of supply and willingness to participate in the survey.

The cybersecurity maturity assessment model used

The cybersecurity maturity assessment model used in the survey is based on the United States Energy Information Administration's C2M2 (Cybersecurity Capability Maturity Model) assessment model, which the National Cyber Security Centre has translated into Finnish and expanded to serve as a basis for its cyber meter tool. The expansion was carried out taking into account the NIST's Cybersecurity Framework model's critical infrastructure assessment sections in Germany and Australia. The full assessment includes approximately 300 questions, ranging all the way to very detailed implementations. Since the aim was to focus particularly on the business risk perspective, the survey was assembled out of the two highest levels of the C2M2 model (11 areas and 30 goals). Additionally, the assessment model was modified by adopting the maturity levels of the Capability Maturity Model Integration (CMMI) standard instead of the C2M2 model's minimum capability requirements for performance and target levels. The resulting assessment scale is presented below.

Level	Explanation
5	Continuously developed in a risk-oriented manner
4	Carried out consistently
3	Defined or planned
2	Carried out intermittently and/or partially
1	Not carried out

The model's business risk-oriented questions cover the following areas:

1. protection of critical services
2. risk management
3. management of protected assets, changes and configurations
4. cybersecurity management system
5. supply chain and external dependency management
6. identity, access and authorisation management
7. event and incident management, continuity of operations
8. information sharing and communications
9. situational awareness
10. threat and vulnerability management
11. personnel management

Presentation of results

The results have been compiled into detailed reports, which were handed out to each participating company at the conclusion of their interview. After this, the sector-specific results were aggregated into main observations regarding the sector for each question, which then underwent a business risk-oriented assessment, a dependence-oriented assessment and a risk-based assessment. These different assessment methods provided slightly different results, which can be utilised for different development needs. The sector-specific results were also compiled into a summary, which was delivered to the participating companies and to the parties contributing to development work. Based on these, the cross-cutting development areas and the development areas highlighted by the different assessment methods were compiled into this summary.

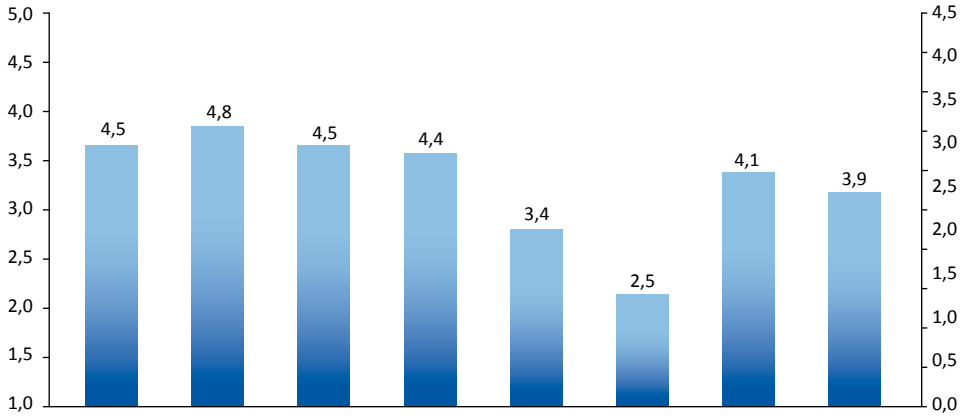


Figure 7. An example of one sector's results for a certain question. Each column represents the results of a different company.

7 APPENDICES

Appendix 1

FOOD SECTOR

MATURITY LEVEL
3,34

CONSISTENCY
36,3%

SPECIAL CHARACTERISTIC

The sector is characterised by strong quality control.

SUCCESSES

- Strict quality criteria
- Investment in product safety
- Disruption management
- Analysis of supply chain dependencies

DEVELOPMENT AREAS

- Secure software development
- Cybersecurity architecture
- The sharing of cybersecurity-related information

Appendix 2

ENERGY SECTOR

MATURITY LEVEL
3,73

CONSISTENCY
49,7%

SPECIAL CHARACTERISTICS

All sectors are strongly dependent on energy. The phase-out of fossil fuels will also transform security of supply.

SUCCESSES

- Critical services have been identified and protected
- Operative activities in regard to incident and continuity management are at a good level

DEVELOPMENT AREAS

- Secure software development
- Common situational awareness
- Cybersecurity architecture

Appendix 3

FINANCIAL SECTOR

MATURITY LEVEL
4,20

CONSISTENCY
80,8%

SPECIAL CHARACTERISTICS

A strongly regulated sector, in which the supervision of operative activities has been taken into account.
The digital, rapidly developing operating environment imposes requirements on infrastructure and the security thereof.

SUCCESSES

- Well-ensured and resourced basic data security
- Management support for the maintenance and development of data security

DEVELOPMENT AREAS

- Continuity planning
- Management of cybersecurity risks
- Vulnerability management

Appendix 4

ICT AND SOFTWARE SECTOR

MATURITY LEVEL
3,86

CONSISTENCY
59%

SPECIAL CHARACTERISTICS

Plays a key role in cybersecurity, as the services and solutions designed, realised and maintained by the sector are also used in all other sectors.

SUCCESSES

- Escalation of cybersecurity events and announcement of disruptions
- Processing of cybersecurity events and disruptions

DEVELOPMENT AREAS

- Common situational awareness
- Cybersecurity architecture
- Management of dependency risks

Appendix 5

TRADE AND DISTRIBUTION SECTOR

MATURITY LEVEL
3,38

CONSISTENCY
34,2%

SPECIAL CHARACTERISTIC

Material flows are controlled, monitored and reported on completely automatically.

SUCCESSES

- High familiarity with supply chains
- The acknowledgement of cybersecurity in the management of external dependencies

DEVELOPMENT AREAS

- The sharing of cybersecurity-related information
- Follow-up
- Vulnerability management

Appendix 6

LOGISTICS SECTOR

MATURITY LEVEL
3,36

CONSISTENCY
39,1%

SPECIAL CHARACTERISTIC

Logistics hubs are highly automated and there are no alternative manual operating methods in the event of a cyber disruption of warehouse robotics.

SUCCESSES

- Management system
- Cybersecurity strategy
- Risk management strategy
- Cybersecurity architecture
- Management support

DEVELOPMENT AREAS

- The sharing of cybersecurity-related information
- Identification of critical services and their dependencies
- Development of cybersecurity personnel

Appendix 7

MEDIA SECTOR

MATURITY LEVEL
3,26

CONSISTENCY
19,5%

SPECIAL CHARACTERISTICS

Notable load spikes on service platforms.
High degree of digitalisation and very active use of cloud services.
Special data security challenges regarding the protection of sources.

SUCCESSES

- To its merit, the media sector has recognised that the digital stream can spread harmful news

DEVELOPMENT AREAS

- Follow-up
- Identification and management of threats
- Common situational awareness

Appendix 8

PORTS AND MARITIME SECTOR

MATURITY LEVEL
3,64

CONSISTENCY
51,3%

SPECIAL CHARACTERISTIC

Operations divided between numerous small operators.

SUCCESSES

Cybersecurity definitions
- primarily carried out
- deployed almost throughout the entire sector

DEVELOPMENT AREAS

- Increasing cybersecurity awareness
- Cybersecurity responsibilities
- Management of dependency risks

Appendix 9

TELECOMMUNICATIONS SECTOR

MATURITY LEVEL
3,96

CONSISTENCY
65%

SPECIAL CHARACTERISTIC

All sectors are dependent on telecommunications and the functionality thereof.

SUCCESSES

- Automation of incident identification
- Disruption management

DEVELOPMENT AREAS

- Cybersecurity architecture
- Common situational awareness
- Secure software development

Appendix 10

MANUFACTURING SECTOR

MATURITY LEVEL
3,67

CONSISTENCY
52,7%

SPECIAL CHARACTERISTIC

The sector has a very low level of regulation and supervision due to the fragmentation of its operators.

SUCCESSES

- Identification of dependencies
- Management of access rights
- Employment relationship lifecycle management
- The sector is consistently good in regard to different goals

DEVELOPMENT AREAS

- Common situational awareness
- Management of critical services
- The sharing of cybersecurity-related information

Appendix 11

HEALTH CARE SECTOR

MATURITY LEVEL
3,69

CONSISTENCY
48,5%

SPECIAL CHARACTERISTICS
Various, very different operating environments to manage
- office network
- medical devices
- patient records

Management of data protection in addition to data security.

SUCCESSES
- Identification of dependencies in supply and partnership chains

DEVELOPMENT AREAS
- Development of cybersecurity personnel
- Common situational awareness
- Follow-up

Appendix 12

WATER SERVICES

MATURITY LEVEL
3,48

CONSISTENCY
41,7%

SPECIAL CHARACTERISTIC
Telecommunications and IT infrastructure often administered by a city or municipality.

SUCCESSES
- Preparedness well-planned and operations can generally be carried out manually ('blind')

DEVELOPMENT AREAS
- Follow-up
- Monitoring of cybersecurity risks
- Implementation of logging

HUOLTOVARMUUSKESKUS
FÖRSÖRJNINGSBEREDSKAPSCENTRALEN
NATIONAL EMERGENCY SUPPLY AGENCY