Cyber Survey of Finnish Sectors 2025

National summary report

Huoltovarmuuskeskus

Huoltovarmuuskeskus

www.huoltovarmuuskeskus.fi

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 the event of serious disruptions and emergencies.

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

The National Emergency Supply Organisation (NESO) is a network that works together for the good of Finland’s operating capability and the security of supply necessitated by it. It includes the National Emergency Supply Agency and its Board of Directors, the National Emergency Supply Council and the sectors and pools of different industries. The NESO also engages in cooperation with regional actors, such as Regional State Administrative Agencies, municipalities, cities and regional committees.

Published by: The National Emergency Supply Agency
Commissioned by: The Digital Pool
Implemented by: Accenture Oy
Cover photo: pexels
Year of publication: 2026
ISBN: 978-952-7470-45-9

Contents

Foreword

Digitalisation and the changing security environment challenge security of supply

Security of supply and digital security are inextricably intertwined. The critical functions of society, such as energy supply, logistics, finance and food supply, increasingly rely on digital systems and networked supply chains. Without reliable digital solutions, society cannot function during disruptions or emergencies conditions.

In the last two years, the security environment has also changed at an exceptional pace. Geopolitical polarisation, military pressure and economic disruptions have further underlined the importance of digital resilience. Digitalisation continues to advance rapidly, but cyber security has not kept pace with this change. The rapid adoption of cloud computing, automation, artificial intelligence and networked devices has expanded the attack surface faster than security and management practices have evolved.

The recent increase in military pressure has added a new operational dimension to the cyber environment. In Europe, cyber operations targeting critical infrastructure have increased and become more determined. Finland is also part of this wider trend as part of European energy, telecommunications and logistics systems. At the same time, broad-spectrum influencing has intensified. Cyber attacks, disinformation and political pressure form a mutually reinforcing whole, in which the digital envi- ronment has become a key platform for social influence. People's trust in institutions and decision-making is increasingly being undermined. The importance of geo-economics has also grown. Supply chain vulnerabilities, technological interdependence and cyber threats becoming part of economic competition underline the interdependence of security of supply and cyber security.

Despite the rapidly changing security situation, the cyber maturity of Finnish sectors has increased only moderately since 2022. The top spots continue to be occupied by heavily regulated industries, such as finance, telecommunications and ICT, where cybersecurity is an essential prerequisite or a major competitive advantage. The least mature sectors are food; ports, shipyards and operators; and transport and logistics – sectors that are especially critical for security of supply. The last two years have been a period of great change for cyber security. However, its development has not kept apace with the changes in the security environment: technological transformation and new types of cyber threats are advancing faster than the preparedness of organisations and sectors. For Finland, this results in a need for coherent and long-term cyber security development and investments, in the context of which cyber security should be viewed as a foundational structure of security of supply and economic resilience instead of a separate technical issue. Without a clear increase in the level of development measures, there is a risk that ostensible progress will mask an actual decline in relation to the changing threat environment.

The world is changing rapidly. If our cyber security does not develop by leaps and bounds, we are actually moving backwards.

Juha Ilkka, National Emergency Supply Agency
Programme Director, Digital Security 2030

Management summary

The survey shows that national cyber maturity has improved only moderately since 2022. Meanwhile, technological transformation is progressing and the threat landscape is changing much faster than the ability of organisations to evolve and invest in cyber security.

The fact that the areas for improvement are still the same as they were the previous survey carried out three years ago is indicative of slow progress. At the same time, one fifth of the surveyed companies were assessed to be of low maturity.

Small and medium-sized companies are notably concentrated at lower levels of maturity, and this phenomenon cannot be explained solely by resource constraints. The clearest missing element is the support of senior management. In higher maturity companies, management teams have made a conscious decision to raise the priority of cyber security.

In a networked society, a company's own high level of maturity is not enough to protect it against threats. Shortcomings in supply chain risk management expose even high cyber maturity sectors and companies to cyber threats through their networks. The risk will be even greater if Finnish companies become too differentiated in terms of their level of preparedness.

Awareness of cyber threats is growing, but concrete measures are lagging behind

Organisations and their management teams have become more aware of cyber threats. However, especially in low maturity companies, progress is hindered by resource and structural constraints and the separation of cyber security from business operations.

Cyber risk management is developing unevenly and the data that it generates is not being used to inform decision-making

The maturity of cyber risk management varies significantly between sectors and companies. At higher levels, it is business-driven and active, whereas especially among SMEs, risk management is more often sporadic or reactive.

Incident preparedness has taken a leap forward

The vast majority of companies have prepared contingency plans at least for critical services, and in many companies the preparation of these plans has also led to concrete measures. However, their development is often reactive instead of proactive, and only a few companies engage in exercises.

Recommendations

These recommendations are based on cross-sectoral areas for improvement and are presented in order of criticality in relation to the cyber threats identified in the survey. Recommendations for companies are compiled in the sector-specific reports.

Recommendations to promote national cyber preparedness:

More attention should be paid to the cyber security of supply chains
The slow development of national cyber maturity and the differentiation in the level of preparedness of companies can threaten all companies in the whole supply chain, regardless of their own cyber maturity. Managing supply chain risks and cyber security is a key capability to develop, regardless of the cyber maturity of the company.

Joint exercises at the national and sector level are important
For many SMEs, joint exercises are the only way to practise continuity management. They are therefore important not only for these companies, but also for more mature organisations that may be exposed to cyber security incidents in the supply chain.

Implementation of the Cybersecurity Act
The monitoring of the national implementation of the NIS2 Directive should focus on practical implementation. Companies must be required to provide concrete evidence of implementing cyber security measures so that the law raises actual rather than apparent maturity.

Cyber security training for management
Translating management's awareness of cyber threats into practical cyber maturity requires training that speaks to the target audience and links cyber security directly to business continuity and financial success.

Recommendations to promote business continuity:

Management involvement is key to raising cyber maturity
Management support can be fostered through active collaboration and trackable metrics and by developing the cyber security competence of management through targeted training.

Development of cyber security competence
Depending on the size of the organisation and the sector, companies should ensure an adequate level of cyber security competence by hiring experts, utilising partners and supporting the retraining of employees.

Comprehensive security management
In many organisations, cyber security, operational technology (OT) security and physical security are managed as separate entities, even though shared situational awareness would improve the prioritisation of cyber risks and resources and help identify broader influence attempts.

Integrating operational cyber risk management into overall business risk management
Especially in small and medium-sized companies, cyber risk management is limited, reactive and disconnected from other business risk management.

Results

National cyber maturity is developing slowly and companies' ability to evolve and invest in cyber security is not keeping pace with the threat landscape and technological transformation. The average maturity of most Finnish sectors is over 3.00, which is considered a good basic level, but some critical sectors fall below this level, meaning that their cyber maturity is only moderate.

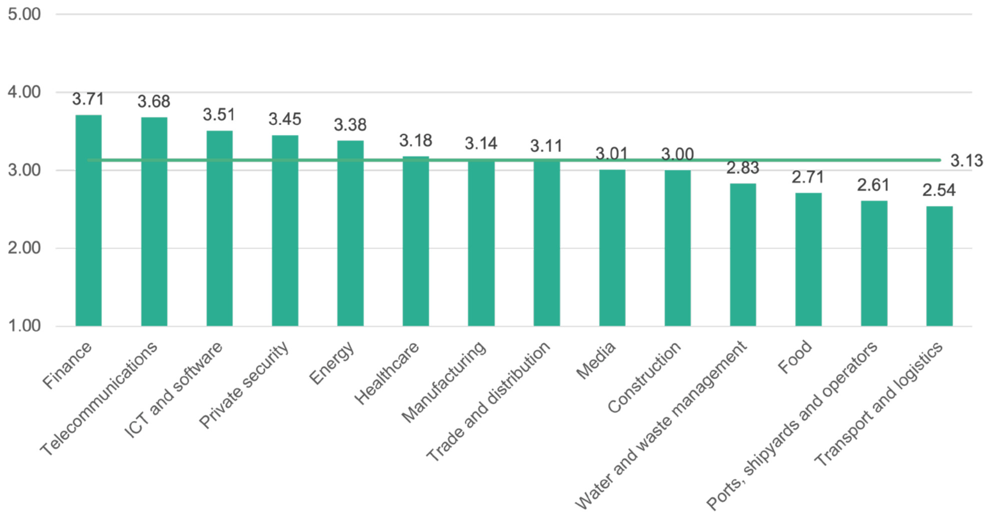

Figure 1: Sector comparison by average[*1]

Sectors subject to strict cyber security regulations, such as the finance, telecommunications and ICT sectors, rank at the top in this comparison of sectors. In these sectors, cyber security has long been developed in a business-driven and goal-oriented manner. Companies in these sectors have had the opportunity to define cyber security management models and to measure and evaluate their effectiveness in the long term. At the bottom of the comparison are sectors where digitalisation has traditionally progressed slower and cyber security has remained more of a support function separated from business operations.

Based on the interviews conducted as part of the survey, the most important factor currently influencing the cyber security landscape is the NIS2 Directive and its national implementation as the Cybersecurity Act. The Cybersecurity Act entered into force while the survey was underway. The majority of the surveyed companies had launched development measures to prepare for the changes brought about by the Act. These measures included the systematisation of cyber security management, the definition of a risk management approach or the mapping of supply chains. Attitudes towards the new regulation varied among the companies. In the best cases, it was not seen as a one-off project, with those responsible for cyber security matters instead using the obligations as leverage to implement longer-term development plans.

There are significant differences between companies in cyber maturity, with a fifth assessed as being of low maturity. The best performers include various types of companies ranging from medium-sized to large. Some of them operate in highly regulated sectors, while others are newer and growing technology companies. Looking at the best performing companies, it can be seen that the smaller size of the organisation is not a barrier to high cyber maturity, but there are more small and medium sized companies at lower levels of maturity.

[1*] The average maturity of all sectors, 3.09, was calculated on the basis of the company-specific results. Averaging the averages of the sectors gives a different result. The sample sizes vary between sectors, which means that the weight of an individual company's results also vary from sector to sector.

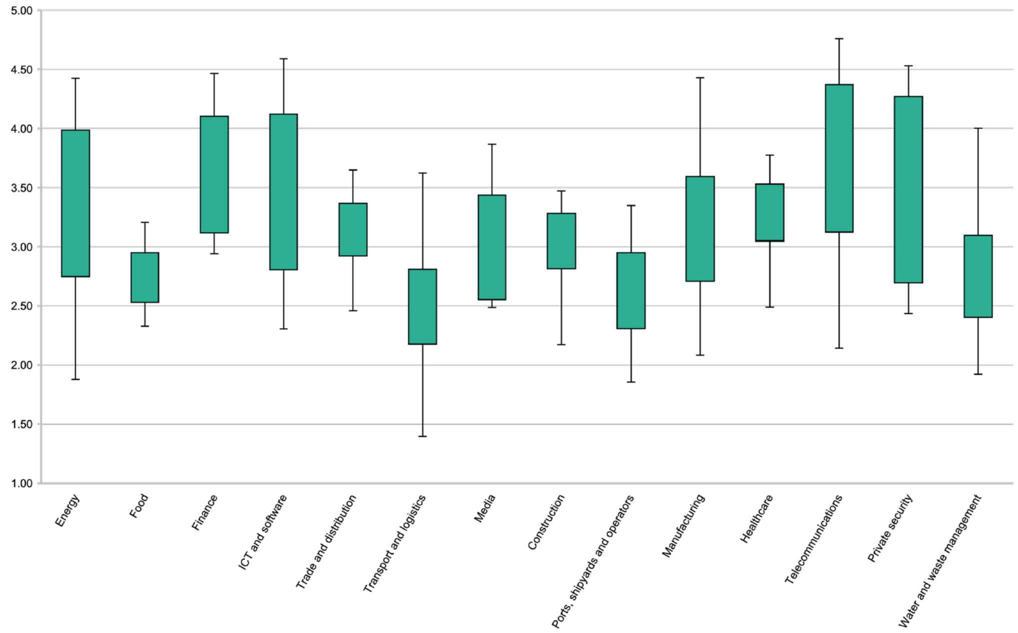

Figure 2: There is variation in the results of all sectors[2]

Change compared to 2022

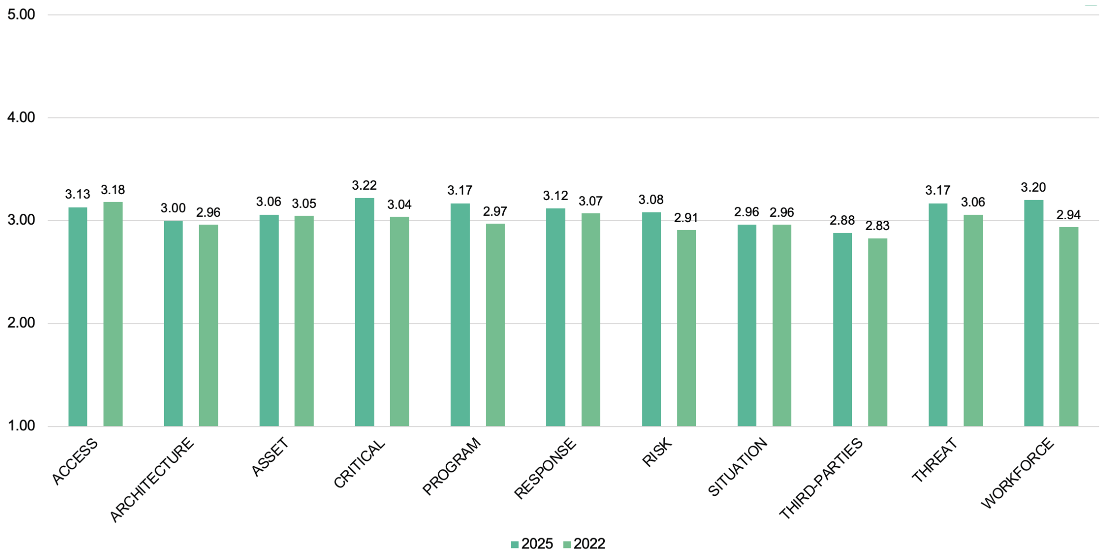

Figure 3: Cyber Meter results by domain in 2022 and 2025*[3]

The previous cyber maturity survey of Finnish sectors was carried out in 2022 and included a total of 121 companies. The 2025 survey included a total of 146 companies and two completely new sectors, namely construction and private security, in addition to which there were some changes in the samples of other sectors, which are described in more detail in the methodology description*[4].

Examined by domain, the cyber maturity of Finnish companies has not changed to any significant degree, with small numerical changes explainable by changes in the samples (Figure 3). Based on the interviews, cyber situational awareness has also not changed significantly between the surveys. Companies are still struggling with the same challenges, such as lack of resources and cyber security competence. As in 2022, the strengths and areas for improvement remain primarily company-specific, as there can be completely different levels of implementation within the same sector. As in 2022, the most common weaknesses are a lack of incident response exercises,

[2] The figure shows the variation of company-specific results by sector. The range of variation within the sector is marked with black lines, while the green bar shows the interquartile range, meaning the range that the middle 50% of results fell in. When looking at the variation, it should be noted that the sample sizes of the sectors range from 7 to 15 companies. The numbers of companies in each sector's sample are detailed in the appendices to the report (Table 1).

[3] The domains are based on the Finnish Transport and Communications Agency Traficom's Kybermittari and their content is explained in more detail in the methodology description at the end of the report.

[4] The sector samples in the 2025 survey and changes compared to 2022 survey are described in the methodology section at the end of the report (Table 1).

risk management and especially third-party risk management. Furthermore, the differentiation of operational technology (OT) management continues to negatively affect the cyber maturity of sectors where it is relevant.

Although the average cyber maturity of all sectors has increased by only one tenth (0.09) since 2022, cyber security management is becoming more systematic and the interest of companies' management in it has increased. In the interviews, several companies highlighted in particular the NIS2 Directive and communication about the heightened cyber threat situation as having increased management interest in cybersecurity issues. On the other hand, the increased cyber threat awareness of management was already noted in the 2022 survey, but at least for now, this increase is not yet reflected in cyber maturity.

The 2022 survey report drew particular attention to the development of cybersecurity awareness and competence and stressed that maintaining these skills and awareness requires continuous effort on the part of companies. It would seem that companies have taken measures to develop their cyber security competence, as the domain in which maturity had increased the most was workforce management and development (WORKFORCE). The NIS2 Directive and increased threat awareness have also contributed to this trend. In general, companies consider the development of cyber security competence and awareness important and support it through various types of regular training. Overall, the cyber maturity of Finnish sectors has remained largely unchanged, despite some positive trends. No significant progress can be observed despite the escalating threat landscape. Numerically, there is very little increase in the results, with wide variation in responses in almost every sector. Comparing the results with the 2022 report, it is also noteworthy that the areas for improvement have remained nearly identical. In other words, the challenges are known, but no sustainable solutions have been found to address them.

Factors explaining differences in maturity between companies

Figure 4 shows the distribution of the surveyed companies in 2022 and 2025. On a positive note, the number of companies in the lowest category indicating low cyber maturity was smaller in the 2025 survey, but this category still accounted for nearly a fifth of the surveyed companies.

The survey included companies ranging in size from small and medium-sized to large. Geographically, medium-sized to large. Geographically, the surveyed companies operate throughout Finland, in addition to which most of them engage in some international business activities. All of the surveyed companies are critical to either the security of supply or crisis resilience of Finnish society.

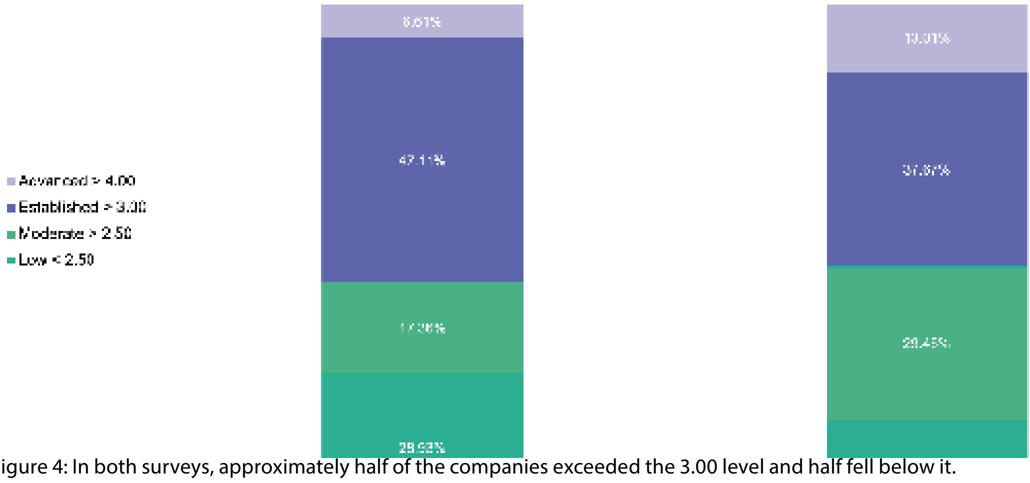

Figure 4: In both surveys, approximately half of the companies exceeded the 3.00 level and half fell below it.

Companies that performed well in the cyber maturity survey are implementing cybersecurity in a layered and multi-dimensional manner. What they have in common is a mindset of continuous and active development and sensitivity to cyber threat trends and changes in the operating environment.

Management support

The clearest single factor that high-maturity companies have in common is the support of the organisation's executive management. In the most mature organisations, the management team discusses the strategic-level cybersecurity landscape, the most significant cyber risks, and the measures to manage them. The interviews show that in these companies, the management team has made a conscious decision to raise the priority of cybersecurity, carry out strategic-level cybersecurity management, and allocate the necessary resources for this. In some of the top-ranked companies, management's ability to make

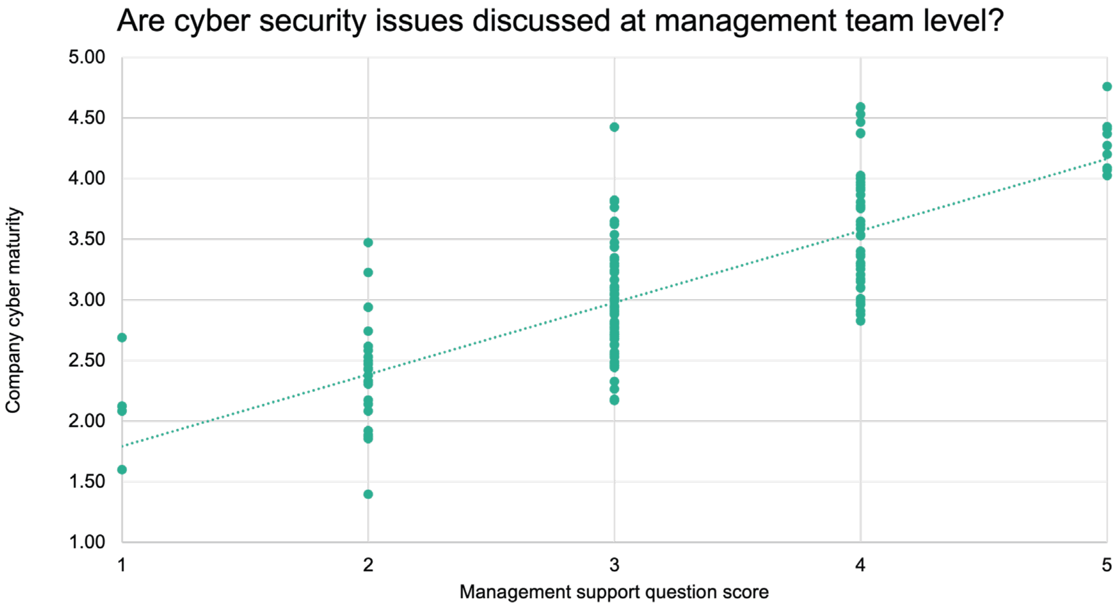

Figure 5: Regular discussion of cyber security by management has a strong correlation with the cyber maturity of the company

decisions related to cybersecurity has been strengthened through cybersecurity training for managers. Companies that performed well in the cyber maturity survey are implementing cybersecurity in a layered and multi-dimensional manner. What they have in common is a mindset of continuous and active development and sensitivity to cyber threat trends and changes in the operating environment.

Exercises and detection capability

The most mature companies not only carry out effective planning and continuous development, but also maintain a constant ability to detect and respond to incidents. Their ability to identify incidents is based on a multi-layered, round-the-clock detection capability. Regardless of whether they carry out cyber security monitoring in-house or have outsourced it, the most mature companies operate a security operations centre (SOC) as a seamless part of their preparedness organisation and monitoring capability. They also constantly develop their incident response procedures in a highly collaborative manner.

High cyber maturity companies actively test their cyber resilience in incident response exercises that range in scope from systems recovery to larger, organisation-wide continuity exercises. In addition to this, high maturity companies engage in joint exercises with their key partners and participate in sector-wide and national continuity exercises.

Factors associated with lower cyber maturity

Lower cyber maturity companies more often employ approaches established through practice that are less comprehensively documented. Undocumented processes not only reduce the regularity, standardisation and measurabilit y of ac tivities, but also create key personnel risks, especially as these companies often have fewer cyber security staff.

The survey data shows that low and moderate cyber maturity companies are more likely to have shortcomings in the human resources allocated to cyber security. The persons responsible for their cyber security are solely responsible for all aspects of cyber security or have been assigned cyber security tasks in addition to other, already full-time duties. In smaller organisations, hiring a larger cyber security team may not be feasible, but even smaller companies cannot ignore the need to ensure an adequate level of cyber security competence by outsourcing some tasks or supporting staff training for new responsibilities, for example.

Lower maturity companies often have shortcomings in regard to ensuring that procedures work in practice. These companies may carry out annual cyber security tasks in accordance with a yearly schedule and draw up various plans, but their level of technical implementation of cyber security remains unclear due to lack of testing and exercises. Their lack of practical-level verification is also reflected in a lack of cyber security metrics, and they often do not monitor their outsourced services or the fulfilment of partners' obligations, for example.

Cyber threats

According to several authorities[5] the cyber security threat level has remained consistently high in recent years, which was also reflected in the interviews conducted for the survey. State-sponsored cyber threats are common and serious incidents have increased. Vulnerabilities are being exploited more quickly, and phishing and scams are on the rise. Nation state threat actors are key threat actors that can potentially be behind all of the cyber threats listed below; 43% of the surveyed companies considered them to be significant in terms of their business operations. Nation-state threat actors have extensive resources, expertise and longer-term strategic objectives, driven by military, political or economic goals. Their campaigns can be part of hybrid influence efforts or industrial espionage, which 11.6% of the surveyed companies highlighted as a key cyber threat.

Supply chain attacks

- An attacker can gain access to the target organisation's systems, data or software through trusted partners or suppliers. Being part of a critical supply chain can expose an organisation to attacks, even if they are not the primary target of the attack. Dependence on partners providing critical services such as cloud computing, telecommunications and energy was highlighted in the interviews, with 80% of respondents feeling that cyber threats related to supply chains are significant.

Software vulnerabilities

- Cyber attacks that target or exploit vulnerabilities in information and production systems and IoT devices to breach systems, disrupt or interrupt operations or damage systems, for example.

Ransomware

- Ransomware is a type of malware that prevents normal use of the infected device, usually by encrypting files, which the attacker then demands a ransom to open. Ransomware is usually spread through targeted data breaches, spam and phishing messages.

Phishing

- In a phishing attack, the attacker tries to trick the recipient into disclosing confidential information, such as usernames, passwords or payment details, by posing as a trusted party in an email, text message or phone call. Phishing attacks may also be carried out with the goal of installing malware or breaching systems. Approximately a third of the survey respondents identified phishing as a critical cyber threat.

Insider threats

- A person who has or has had authorised access to an organisation's critical resources can exploit that access, either intentionally or unintentionally, in a way that adversely affects the organisation.

AI-based attacks

- The rapid development of artificial intelligence (AI) increases the threat of more persuasive social manipulation, various scams and the automation of attacks or parts thereof. There is also the threat of data leaks through the uncontrolled use of AI tools.

[5] Including Traficom and Supo: https://www.kyberturvallisuuskeskus.fi/en/news/traficom-and-supo-cyber-security-threat-level-remains-high-serious-cases-rise

Conclusions

Cyber threat awareness continues to develop, but concrete action is lagging behind

As already noted in the previous survey carried out in 2022, events that have a significant impact on the security environment raise the cyber security awareness of organisations, at least temporarily. Such events include geopolitical changes or cyber attacks highlighted by the media, especially ones affecting peer organisations. Based on the interviews, the threat awareness of cyber security experts, on the other hand, is contributed to especially by cyber security networks and sector-specific information exchange forums. However, increased awareness of the heightened cyber threat landscape is still not automatically reflected in the day-to-day practices of companies. One of the challenges that many organisations face in regards to this is the concentration of cyber security awareness to specific people. This can lead to management not seeing threat developments in a business context, at which point they have no incentive to allocate sufficient resources for the development of cyber security.

In lower maturity sectors, the expansion of the threat landscape is generally recognised, but many organisations have quite a narrow view of how attractive a target they are for attacks. In particular, some smaller companies do not understand their place in the whole supply chain, which is reflected in their lower level of cyber preparedness. The interviews showed that especially in sectors with low levels of digitalisation, some companies have made conscious decisions to limit their cyber security investments. These decision are based on the notion that even a cyber attack that paralysed all digital systems would not pose a critical threat to their business continuity. The low cyber maturity of SMEs also poses a risk to higher maturity organisations, both in terms of technical and operational interfaces in supply chains and the confidentiality of information. In the threat discussions carried out as part of the interviews, many interviewees highlighted nation-state threat actors and espionage. Despite this, when discussing cyber preparedness, the interviewees did not extensively cover measures aimed at ensuring that their organisation does not lose their own or their customers' confidential data unnoticed.

One factor slowing down progress is that, as in 2022, cyber security is still often viewed as a support function separate from business operations, resulting in resourcing challenges and development inertia. Risk-based decisions cannot be made if cyber risks are not reflected in business decisions. Furthermore, awareness cannot be translated into performance without metrics, and many lower maturity companies have not set targets against which they could measure their progress. In many cases, the reason for slow progress at the concrete level is not indifference, but rather a lack of structures and resources. When there is no regular and effective dialogue between management and cyber security functions, information does not flow from cyber security personnel to business operations and risks are not translated into priorities or actions.

Cyber risk management is developing unevenly and the data that it generates is not being used to inform decision-making

The way in which organisations manage cyber risk varies significantly. The interviews found that the risk management obligations imposed by the NIS2 Directive have resulted in many organisations having cyber risk management models that had just been completed at the time of the interviews, but not yet been put into practice. However, it can still be said that especially among SMEs, there is less cyber risk management, especially as part of day-to-day activities.

Cyber risk management is typically well established in higher cyber maturity sectors, such as finance; telecommunications; ICT and software; and energy. In these sectors, large companies in particular engage in systematic and comprehensive cyber risk management at both operational and strategic levels. In such companies, strategic-level cyber risks are monitored at the top level of the organisation, and as a result, cyber risk monitoring has also become a natural part of the business risk management carried out by management.

In the 2022 cyber maturity survey, cyber risk management was still typically a separate function, and in light of the results of the 2025 survey, the situation seems to have deteriorated slightly between the surveys (Figure 6).

Based on the survey data, low maturity organisations are either not managing cyber risk at all or are doing so on an ad hoc basis, in response to threats that have already materialised. This kind of reactive approach leaves an organisation vulnerable because cyber security decisions and developments cannot be prioritised based on risk-based information. Even in 2022, it was found that in some organisations risk management is carried out only in a limited part of the organisation or cyber risks are only discussed between cyber security experts. The interviews found that the terms 'cyber risk,' 'cyber threat' and 'vulnerability' are often confused in lower cyber maturity companies. The same observation was made in the previous survey; at the time, cyber security experts often perceived risk management as the technical management of threats and vulnerabilities. Although in 2025 more organisations understand the differences between the terms, this kind of confusion can lead to misprioritisation and make genuinely risk-based decision-making impossible. Especially in small and medium-sized companies, there are challenges in assessing the impact and criticality of the materialisation of identified cyber threats, i.e. the evaluation lacks a key perspective to enable risk-based action. In addition to this, it is often challenging for these companies to identify which cyber risks affect their core business, as the interviewees frequently highlightephenomena that have been more widely reported by the press, for example.

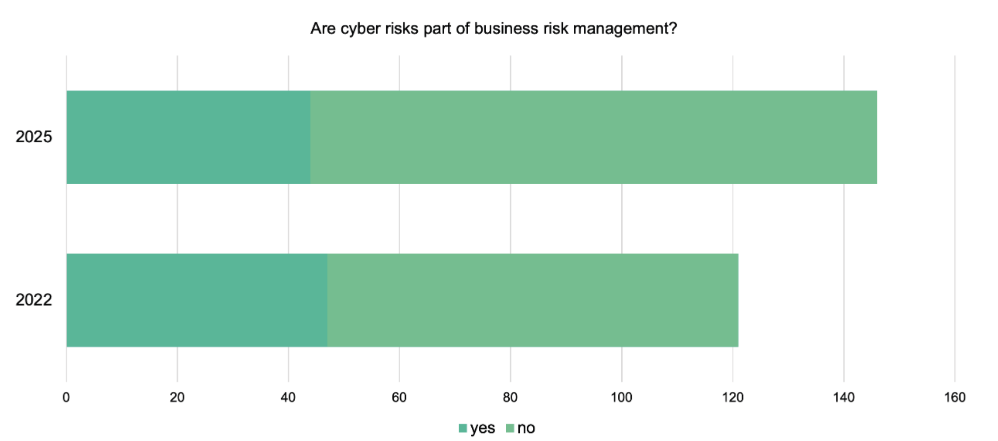

Figure 6: The figure shows the numbers responses received from companies in 2022 and 2025

Based on the survey data, low maturity organisations are either not managing cyber risk at all or are doing so on an ad hoc basis, in response to threats that have already materialised. This kind of reactive approach leaves an organisation vulnerable because cyber security decisions and developments cannot be prioritised based on risk-based information. Even in 2022, it was found that in some organisations risk management is carried out only in a limited part of the organisation or cyber risks are only discussed between cyber security experts. The interviews found that the terms 'cyber risk,' 'cyber threat' and 'vulnerability' are often confused in lower cyber maturity companies. The same observation was made in the previous survey; at the time, cyber security experts often perceived risk management as the technical management of threats and vulnerabilities. Although in 2025 more organisations understand the differences between the terms, this can lead to misprioritisation and make genuinely risk-based decision-making impossible. Especially in small and medium-sized companies, there are challenges in assessing the impact and criticality of the mate-rialisation of identified cyber threats, i.e. the evaluation lacks a key perspective to enable risk-based action. In addition to this, it is often challenging for these companies to identify which cyber risks affect their core business, as the interviewees frequently highlighted phenomena that have been more widely reported by the press, for example. In companies where cyber risk management is based on compliance, its practical implementation is often incomplete or has not yet started. Such companies face challenges in identifying risks on a regular basis and rarely account for new or updated risks in their risk management process. In addition to this, their cyber risk management is isolated, and risks related to factors such as production environments are not accounted for in their risk management processes, even if they are highly relevant to their business. In some of the responses, risk management was confused not only with cyber threats and vulnerabilities, but also with different levels of contingency and continuity plans, which indicates that risk management measures are not being implemented as planned.

Partner risk management:

Of all the domains assessed in the survey, third-party risk management was the least mature, even though 80% of the surveyed companies have identified supply chains as a key cyber threat. Comprehensive supply chain management was also rated at a low level of maturity and identified as a clear area for improvement in the 2022 survey. However, the identification of dependencies has generally improved, with more companies having mapped their supply chains beyond the first link than in the previous survey.

Many companies have partners that are responsible for several of their business-critical functions, but despite this, partner risk management practices are not yet well established in all companies.

The challenges that companies face in partner risk management relate in particular to the identification and management of dependencies, the division of responsibilities and the setting and compliance monitoring of cyber security requirements. The survey included a number of companies that had no clear understanding of what services their partners were providing them and how or how their service providers take care of their own cyber security. Partners are often trusted by default without any evaluation or knowledge of their security practices, especially when the partnership is based on a longer contractual relationship. In the water and waste management; transport and logistics; and trade and distribution sectors, this has been identified as a sector-wide challenge. The same challenges were also identified in the 2022 survey, but this time there were also more companies included in the survey that had comprehesive partner risk management programmes that include regular audits or inspections. Since threats realised through supply chains are usually evaluated as being critical, some companies have made efforts to extensively map their supply chains and monitor them down to the level of software libraries.

Incident preparedness has taken a leap forward

While overall cyber maturity has not significantly increased, the survey data indicates that companies' incident preparedness has improved. The vast majority of companies have prepared contingency plans at least for services that they have identified as being critical, and in many companies the preparation of these plans has also led to concrete preparedness measures. According to the interviews, this overall improvement has been contributed to at least by the preparedness requirements of the NIS2 Directive and the general development of the threat landscape.

Although overall preparedness has improved, there are large differences between companies. Some of these differences can be explained by the fact that not all companies have taken cyber incidents specifically into account sufficiently in their contingency plans. Based on the interviews, one reason for this is because the impact of cyber incidents is not the same everywhere due to variations in the resilience of companies and the extent to which their business operations are dependent on technology. On the other hand, in some low cyber maturity companies, decisions related to preparedness are not necessarily based on judgements made on the basis of threat modelling, risk analysis or situational awareness. In many cases, preparedness measures are only taken in response to threats that have already materialised. For example, some companies have duplicated their telecommunications connections only after losing confidence in telecommunications operators due to cable damage instead of evaluating and preparing for critical dependencies in advance.

In most cases, however, lower levels of cyber preparedness are attributable to a lack of resources or competence. In particular, the number of companies that engage in exercises is still relatively low, with those that do not remaining unable to verify the effectiveness of their contingency plans, which, in turn, results in them neglecting the regular development and updating of the plans. Continuity exercises, whether sector-specific or broader in scope, have a positive impact on cyber preparedness. This holds especially true for small and medium-sized companies, for which joint exercises are one of the few ways to practise incident management. Joint exercises can form a fundamental part of the preparedness of an entire sector.

In certain sectors, preparedness is an established part of the operating culture, and cyber incidents are comprehensively accounted for in plans, which are constantly updated and based on practical lessons learned from exercises. Higher maturity companies engage in exercises at multiple levels, ranging in scope from the recovery of individual systems to large-scale crisis exercises with senior management and stakeholders. High maturity companies also have a wide range of concrete preparedness measures in place, such as back-up systems, differentiated environments and redundancy.

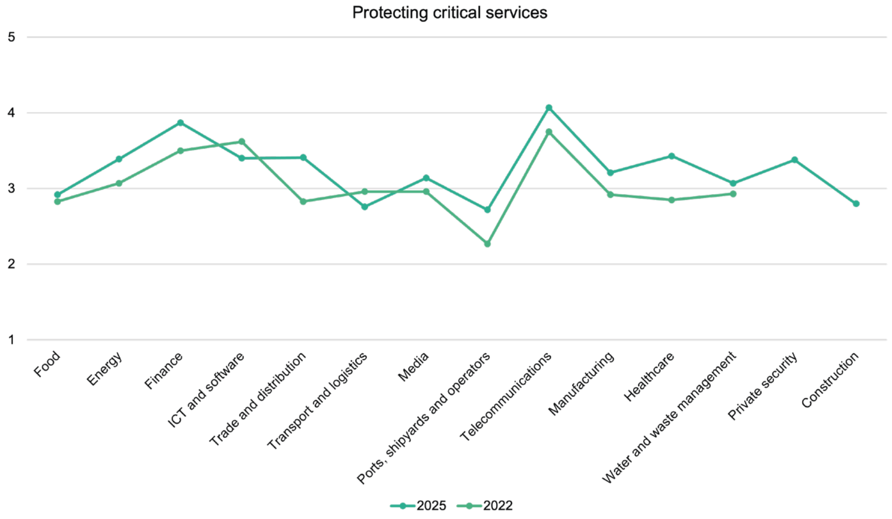

Figure 7: The average maturity of all but two sectors has risen in the domain measuring the identification, protection and incident preparedness of critical services

Appendices

Methodology

Cyber maturity survey of Finnish sectors

Cyber Maturity of Finnish Sectors 2025 is a survey funded by the National Emergency Supply Agency, commissioned by the National Emergency Supply Organisation's Digital Pool and carried out by Accenture. The survey is part of the National Emergency Supply Agency's Digital Security 2030 programme (DT2030) and a follow-up to the cyber maturity surveys carried out in 2019–2020 and 2022. The 2025 survey involved assessing the cyber security of 146 Finnish companies in fourteen sectors critical to security of supply. The actors included in the survey were selected with the aim of producing a broad sample of different sectors and different organisations within sectors. The survey covered 14 sectors. The participants were selected and invited to participate in the survey with the help of the National Emergency Supply Organisation's (NESO) sector-specific pools and comprised a comprehensive sample of security of supply chain actors with different profiles, organisational sizes, operating areas and business models. The number of companies per sector varied from 7 to 15. In the sector-specific reports, the emphasis was on qualitative analysis rather than direct numerical comparisons, as the sectors are not directly comparable with each other. It should also be noted that the participating companies are not exactly the same as in the 2022 survey, which must be taken into account when comparing the two surveys.

Sector and company selection

The sectors included in the survey were decided by the project steering group based on the critical sectors defined in the NIS2 Directive. Table 1 below describes the sector samples and changes from the 2022 survey.

Sector	2022	2025
Energy	Local and national energy companies that engage in theproduction and distribution of electricity and heat and fuel trading; companies that maintain grid services and transmission infrastructure; and other energy technology and service companies	No changes
Finance	Banks and insurance companies	Added financial administration
Telecommunications	Telecommunications operators	No changes
ICT and software	ICT and software companies	No changes
Healthcare	Private and public healthcare providers	Excluded public health care actors
Manufacturing	Forestry, chemical, engineering, construction and defence industries	Construction separated into adedicated sector
Trade and distribution	Retailers, wholesalers, grocers, distributors and food service actors	No changes
Media	Media companies	No changes
Water supply	Water supply companies	Added waste management
Food	Primary production and food industry	No changes
Ports, operators and shipyards	Ports, operators, shipyards and maritime transport	Maritime logistics moved to transport and logistics
Transport and logistics	Air, road and rail transport	Added maritime transport

Construction		Infrastructure and building construction companie
Private security		Companies that provide solutions for the design, installation and maintenance of access management, surveillance and alarm systems, locking solutions, camera surveillance, security technology, guarding and security services

Table 1: The sectors included in the survey

Assessment tool

The maturity level of cyber security was assessed using a domain-based approach adapted from the Finnish Transport and Communications Agency Traficom's Kybermittari (Cybermeter) tool. The version used in the survey featured the same domains as the original Kybermittari, but some of the domain-specific questions were condensed or removed due to the amount of time available in the workshops. Kybermittari was updated in 2025, and this updated version was condensed for the survey while making sure that it did not differ signifiantly from the version used in the 2022 survey.

Traficom has prepared a presentation in which Kybermittari is compared to the condensed assessment tool used in this survey (in Finnish): https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kybermittari_vs_HVK_Digipoolin_toimialaselvitys-2025_vertailu.pdf

Domain	Name	Description
PROGRAM	Cyber security programme management	Assessment of the organisation’s ability to manage and maintain an organisation-wide cyber security programme.
ARCHITECTURE	Cyber security architecture	Assessment of the organisation’s ability to manage and maintain cyber security architecture.
RISK	Risk management	Assessment of the organisation’s capacity to identify and manage risk related to information and cyber security (cyber risks).
CRITICAL	Protection of critical services	Assessment of the organisation’s ability to recognise its role in the provision of services critical to society and, as a result, their protection.
THREAT	Threat and vulnerability management	Assessment of the organisation’s ability to define and maintain plans, processes and technologies to detect, identify, analyse, manage and address cyber threats and vulnerabilities.
ASSET	Asset, change and configuration management	Assessment of the organisation’s ability to manage its hardware, software and information assets commensurate with the risk to the organisation and organisational objectives.
WORKFORCE	Workforce management and development	Assessment of the cyber security awareness, skills and readiness to respond to various cyber incidents of the organisation’s workforce.
THIRD-PARTIES	Partner network risk management	Assessment of the organisation’s ability to identify and manage risks related to supply chains and third parties.
SITUATION	Situational awareness	Assessment of the organisation’s capacity to maintain cyber security situational awareness.
RESPONSE	Event and incident management	Assessment of the organisation’s ability to manage, respond to and recover from cyber security incidents.
ACCESS	Identity and access management	Assessment of the organisation’s ability to manage and restrict logical and physical access rights to the company’s protected assets.

Table 2: Descriptions of the domains

Assessment scale and criteria

The assessment scale of the maturity assessments was based on a general five-level maturity model similar to the Capability Maturity Model (CMM), for example. The general requirements of the different maturity levels are described in Table 3 below.

Maturity level	Description
1	No defined practices. The organisation is not implementing the practices related to the domain. Any implementation is reactive and unplanned.
2	The organisation implements practices on a case-by-case basis and irregularly. For example, some processes are in place, but are not documented. Development and administration do not need to be systematic.
3	Systematic action, e.g. regulation-driven. Procedures and processes are documented, but only apply to some operations, require updating or have not been implemented across the board. No continuous evaluation/auditing.
4	The organisation has documented cyber security management models, responsibilities and authorisations for implementing practices that are regularly repeated and maintained. Clear processes and procedures that are followed and monitored. Prioritisation based on criticality and risk assessment.
5	The organisation implements practices in a risk-based manner, maintains organisation-wide perating models continuously and has defined objectives for cyber security, based on which performance is regularly measured. The activities are strategically managed, and the organisation's management is committed to them. Modern technological capabilities are in place to support operations.

Table 3: Cyber maturity assessment scale

Threat mapping

The sectoral threat mapping was carried out as part of the workshops with all participants. The sector threat lists were based on sector threats gleaned from Accenture's global cyber threat intelligence reports and insights from Traficom and the Digital Pool. In addition to these initial threats, the mapping took into account and listed the views of companies on recurring threats to their sectors, as revealed in the workshops. The threat mapping discussion was stimulated with the help of the threats compiled in advance and their definitions, with the interviewees verbally assessing their likelihood and impact. The threats were scored on a heat map based on frequency and significance and also compared to the maturity level of the different domains, with a lower maturity in a domain increasing the significance of the threat, for example. The scored threats were taken into account in the company-specific recommendations. Only the most frequently occurring themes across all sectors were compiled in this national-level report.

Workshops

The workshops were conducted as interviews that were structured based on the aforementioned tool and threat mapping. Participants from the included companies varied from company to company; some companies' participants consisted of one or two cyber security specialists (often CISOs), but many sent a larger group of participants that included representatives from risk management, production technology and general IT, among others. The maturity assessments were carried out by going over all the questions in each domain with the participants, who were also asked to provide clarifications where necessary and examples to illustrate things, particularly in relation to various documents or process descriptions.

Sector-specific summaries

Finance: Established level: 3.71

- The sample included banks and insurance companies. Unlike in the 2022 survey, the sample also included financial administration companies, whose participation is not estimated to have had a significant impact on the average maturity of the sector.

Strengths

- Companies in this sector have been developing their cyber security for a long time, which means that they have had the opportunity to define cybersecurity management models and to measure and evaluate their effectiveness in the long term.
- Finance sector companies invest heavily in the cyber security competence of their employees. Best practices include weekly training time for employees who focus on cyber security and role-specific cyber security training focusing on critical roles. Most of the companies regularly measure and assess their level of cyber security competence in relation to the threat situation.
- High maturity in risk management. This is partly due to legislation and standards, but most companies in the sector go beyond the minimum requirements. Best practices include automated due diligence scanning.

Areas for improvement:

- The most critical challenge is dependence on legacy infrastructure. As a result, otherwise mature processes and technical capabilities cannot be extended to the entire IT infrastructure, due to which overall cyber security cannot be considered sufficient.
- There is also room for improvement in information security monitoring, the level of which varies between companies. Not all companies have a seamless SOC collaboration that would allow them to utilise the service beyond generating alerts. Companies that cannot utilise monitoring services comprehensively as an extension of their own preparedness organisation are less cost-effective and less capable of responding to complex cyber threats.
- The management of information assets is often less mature than other asset management. Companies report challenges in maintaining a register of information assets and the ability to control the acceptable use, sharing and storage of data.

Comparison between the 2022 survey and the 2025 survey

- The average cyber maturity of the finance sector has increased from 3.34 in the 2022 survey to 3.71 in the 2025 survey, indicating steady and positive progress. The biggest improvements were seen in the domains of cyber security programme management, threat and vulnerability management and third-party risk management. Progress has been driven by geopolitical tensions, the increase in cyber threats and updated regulation, which, despite the associated administrative burden, has led to organisations strengthening their resilience and strategic management. Significant progress has been made in developing workforce competence, but challenges remain in regard to asset management, legacy systems and distributed environments. Monitoring practices and SOC cooperation need to be further improved, although progress has been made. Overall, the trend is positive, but maintaining a high level of maturity requires continued investment and commitment in a rapidly changing threat environment.

Telecommunications: Established level: 3.68

- The sample consists of large and medium-sized telecommunications actors.

Strengths

- In telecommunications companies, cyber security is an integral part of organisational management and overall risk management instead of being a separate support function. Information security management models and processes are an established part of daily operations, and the effectiveness of practices is continuously monitored and developed.
- In the most mature organisations, the protection of critical services, preparedness and continuity exercises are at a high level. Maturity is supported by the impacts of legislation on preparedness and the active role of management teams in monitoring the availability of critical functions and services, which is also reflected in sufficient resources for information security activities.
- Organisations carry out continuous, automated vulnerability scans, which are supported by up-to-date asset registers. Technical preparedness is complemented by regular penetration and red teaming exercises. Threat intelligence is an integral part of operations and companies utilise multi-source threat intelligence data at technical, tactical and strategic levels. In the most mature organisations, intelligence is automated and integrated into information security monitoring.

Areas for improvement:

- More balanced development of the sector would reduce cyber threats and risks realised through subcontracting chains and networked operating models.
- As regards identity and access management, some organisations exhibit privilege creep and use manual practices, which increase dependency on individuals and reduce visibility of the overall threat landscape. Manual practices are also common in some organisations in asset management, limiting visibility and slowing down incident response.
- As regards partner management, practices and the scope of requirements vary considerably. The audit practices and contractual obligations that partners are subject to are not fully harmonised, making it difficult to assess supply chain risks and build comprehensive situational awareness in monitoring.

Comparison between the 2022 survey and the 2025 survey

- The average cyber maturity of the telecommunications sector based on the 2025 survey is 3.68, almost the same as in 2022, when it was 3.71. The sector has high average maturity, but there is wide variation. Cyber security culture has strengthened, but lower maturity companies still face challenges in defining responsibilities. Strategic development continues to be risk-based, with the majority of organisations exceeding minimum regulatory requirements. Vulnerability management has developed through automation and asset registers, and threat intelligence is comprehensive. The weakest domain is partner network risk management, where more resources and systematic methods are needed. The maturity of identity and access management and asset management has declined, partly due to development projects still in progress. A strong culture of preparedness and protection measures for critical services remain the key strengths of the telecommunications sector.

ICT: Established level: 3.51

- The sector sample consisted of medium-sized and large ICT organisations.

Strengths

- The ICT Sector's best practices in cyber security are based on long-term development, clear management structures and a business focus. Meeting customer demands often requires proof of capabilities, which is why management systems and certifications such as ISO 27001 are common.

- High maturity companies build risk-based approaches around compliance, with technical, operational and strategic capabilities supporting one another. This is reflected in elements such as partner risk management, with the most advanced companies monitoring risks and dependencies down to the software component level.

- The surveyed organisations are characterised by clearly differentiated resources, such as a dedicated security operations centre, the operation of which is not dependent on the availability of customer resources. Companies in the sector invest systematically in employee competence development, and training is often linked to compensation and career development. The development of a strong cyber security culture is supported by diverse and role-specific training content.

Areas for improvement:

- There are development needs in the building of situational awareness, especially as regards the coverage of monitoring, the collection of up-to- date information and the use of this information to support decision-making.

- Some actors still use threat intelligence only sporadically or only from individual sources. More attention should be paid to software security, as it is a part of the core business of the sector, and only some companies have a comprehensive approach to secure software development.

- From a risk perspective, the surveyed organisations also have room for improvement in the management of their partner networks, for example in terms of increasing contractual requirements and updating them regularly. The manageability and transparency of supply chains could also be supported by monitoring the implementation of information security and expanding auditing practices. Development needs were also identified in cyber incident and continuity management and testing. Related processes and recovery plans are often in place, but some companies need to test them more systematically.

Comparison between the 2022 survey and the 2025 survey

- The average cyber maturity of the ICT sector based on the 2025 survey is 3.51, down slightly from 3.67 in 2022. The sector's key practices are well-established, but variation has increased, and the smaller sample size may affect comparability. Risk management has improved, with cyber risks being increasingly integrated into other business risk management, although some actors continue to emphasise customer and regulatory requirements.

- Third-party risk management has improved as a result of NIS2 requirements, but monitoring measures and lifecycle management continue to present challenges. Workforce development is the only domain where the sector's average maturity has increased. The weakest domain is situational awareness, in which monitoring and the utilisation of data to inform management decision-making are still inadequate. Overall, development is driven by customer and regulatory requirements, but the development of smaller actors' capabilities is sometimes hindered by resource constraints.

Private security: Established level: 3.45

- The sector sample consists of companies that provide solutions for the design, installation and maintenance of access management, surveillance and alarm systems, locking solutions, camera surveillance, security technology, guarding and security services to meet the needs of industries, properties and communities. This is the first time that the sector was included in the survey.

Strengths

- Organisations in the sector actively develop their cyber security practices due to the sector's security-critical customer base and regulatory requirements. To increase their competitive advantage and reliability, companies rely on international security standards, with many aiming for an ISO27001-certified security management model, for example.

- For the same reason, companies in the sector have also developed comprehensive contingency and continuity plans, including for cyber incidents. These plans are regularly reviewed, and companies actively organise their own exercises or participate in the cyber exercises of their customers and partners.

- Physical access management is one of the sector's core competences, with technologies and practices implemented and monitored to a high standard. Properly managed physical security complements technical security measures and, together with them, forms a comprehensive security solution.

Areas for improvement:

- The sector's main areas for improvement relate especially to the availability of human resources. Limited resources make it difficult to develop and maintain harmonised processes and documentation, which can undermine overall cyber security management.

- There are challenges in regard to the availability of sector-specific cyber expertise, partly due to the small size of the sector, and some actors have outsourced functions to partners without full visibility or certainty on the practices to be implemented.

- The development of third-party risk management starts with the identification and registration of critical services and partners and their interdependencies. Setting clear and measurable information security requirements for partners and establishing common continuous monitoring practices will support risk management and reduce the likelihood of supply chain threats.

Analysis of the current state of cyber security

- The development of cyber security is driven by customer requirements, the NIS2 Directive and a growing need for structured reporting. Many companies are seeking ISO 27001 certification as a competitive advantage and as a response to requirements. Although the sector is not directly bound by cyber legislation, companies' motivation for development is increased by customer relationships and threat scenarios.

- In many companies, cyber security management is still developing, with responsibilities often falling to the head of security or IT without a separate team. The deployment of information security management systems is still in progress in many companies, and the challenge is to ensure that development is not limited to policy level, but that the technical implementation matches the threats. Limited resources often lead to companies using outsourced services, which can pose risks if priorities and objectives are not clearly defined for partners.

Energy: Established level: 3.38

- Local and national energy companies that engage in the production and distribution of electricity and heat and fuel trading; companies that maintain grid services and transmission infrastructure; and other energy technology and service companies.

Strengths

- All companies in the sector provide cyber security training, which ensures that their workforce is able to identify and respond to cyber threats in different roles and supports the strengthening of a culture of security and compliance with regulatory requirements.
- The domain of threat and vulnerability management is well-developed. Vulnerability data is collected from a wide range of sources, and organisations actively engage with their stakeholders. In addition to systematic vulnerability scanning, the most mature actors carry out information security testing and scenario-based exercises as part of a broader threat and vulnerability management approach.
- There are several companies in the sector that are able to maintain comprehensive cyber security situational awareness, detect incidents and respond to them according to predefined processes in an efficient and timely manner.

Areas for improvement:

- Companies whose IT and OT are organisationally separate face challenges in maintaining comprehensive cyber security situational awareness. Separate areas of responsibility without cooperation models make risk-based decision-making and prioritisation of resources more difficult.
- In smaller organisations, the dependency of cyber security tasks on individual people is highlighted as a key risk. Small IT or cyber security teams can increase operational agility, but workforce and resource constraints often end up overburdening employees or forcing them to prioritise even between critical development needs.
- In response to the sector's preparedness obligations, almost every organisation has created baseline contingency plans for critical services, but in some companies, preparedness may have been implemented mainly from a compliance perspective.

Comparison between the 2022 survey and the 2025 survey

- In 2025, the average cyber maturity of the energy sector increased to 3.38 (2022: 3.12), with 12 companies now included in the survey instead of the previous 9. There are major differences between companies: some are very mature, while smaller local actors are lagging behind due to a lack of resources. Management commitment and long-term plans have also increased in lower maturity companies, but in some of them preparedness does not go beyond legal obligations. Workforce cyber competence and threat management have improved, but there are still shortcoming in the management of OT environments. The energy sector remains a high cyber maturity sector, but the high level of variation and the number of low maturity actors pose a potential threat to the cyber resilience of the entire energy system. The NIS2 Directive may stimulate development, but there is a risk that compliance will remain a one-off project and not lead to continuous development.

Healthcare: Established level: 3.18

- In addition to health service providers, the 2025 survey includes companies from the healthcare production and distribution segments.

Strengths

- In terms of information security awareness and training, practices are generally strong and fairly consistent. All of the organisations in the sample have identified training as important and provide a wide range of training and regular information sessions for their workforce. Some organisations have also introduced role-based training programmes to support risk-based competence development and ensure cyber security competencies appropriate for different work tasks.
- Best practices in the protection of critical services, the sector's strongest domain, include regular resilience testing, which the most mature organisations carry out as part of their continuity management. Regular resilience testing helps identify areas for improvement and reduce potential downtime.
- Most actors in the sector regularly organise cyber exercises at different levels of the organisation to help maintain preparedness and improve response capabilities in the event of a real incident.

Areas for improvement:

- The sector's areas for improvement are to a large extent related to differences in management models, technological solutions and resources between organisations. In many cases, the challenges arise from an inability to effectively translate planned operating models into practice. The adequacy of cyber competence and the availability of resources pose a challenge, especially in terms of continuity of development.
- Third-party risk management is the sector's weakest domain. The risk management of the sector's organisations is primarily based on contracts, and audit practices are often insufficient or sporadic. Challenges in procurement processes arise when information security requirements are not systematically defined or understood, making it difficult for partners to manage and monitor them consistently.
- Automation and efficiency of identity and access management processes are key areas for improvement, as manual approaches slow down responsiveness and increase the risk of human error.

Comparison between the 2022 survey and the 2025 survey

- The 2025 survey included only seven companies from this sector, so no broad conclusions can be drawn for the whole sector. The average maturity of the sector has increased slightly, but the changes in individual domains vary, and variation between companies has decreased compared to the previous survey. The most improved domain is the protection of critical services, which is now the sector's strongest domain alongside event and incident management. Progress has been driven by tightening regulation and the growing threat landscape, but more attention needs to be paid to keeping business continuity plans up to date and testing them. Cyber security management has improved, and all of the surveyed actors have an information security management model in place or under development. The domain of workforce development shows positive development, although its average maturity remains unchanged. The weakest domains are identity and access management, in which manual processes pose risks, and third-party risk management, in which monitoring measures and resources are inadequate. Supply chains are identified as the most critical cyber threat, highlighting the need to systematise monitoring and prioritise development activities based on risks.

Manufacturing: Established level: 3.14

- The sector sample includes companies from the forestry, chemical, engineering and defence industries.

Strengths

- In high maturity organisations, cyber security is a management priority, and situational awareness is reported on regularly. This is supported by a risk-based cyber security strategy, which is tied to a business strategy, and clear management systems, which are often ISO 27001 certified.
- Threat and vulnerability management is the strongest domain: the most mature organisations utilise SOC teams, threat hunting, penetration testing and cyber exercises and actively share threat intelligence across networks.
- Identity and access management is at a consistent level, and many actors have centralised IAM solutions that support automated processes and are based on the principle of least privilege and a role-based model.

Areas for improvement:

- Cyber situational awareness monitoring is lacking in many companies and does not cover all critical production systems. Shortcomings in OT asset management increase exposure to cyber threats and hinder incident response, which can slow down or prevent timely measures.
- In some organisations, lack of management interest in cyber security is reflected in insufficient resources and budgets and fragmented risk management practices.
- Production systems are critical in the manufacturing sector, but their protection practices are often inadequate. There are challenges in protection controls, system segmentation and the mapping of critical resources and assets. The appropriate protection and management of these systems is essential for ensuring the smooth operation of p roduction processes and managing cyber risks
- Automation and efficiency of identity and access management processes are key areas for improvement, as manual approaches slow down responsiveness and increase the risk of human error.

Comparison between the 2022 survey and the 2025 survey

- The cyber maturity of the manufacturing sector has increased, but there are still major differences between companies, with the difference between the lowest and highest maturity level exceeding two points. Companies in the sector fall roughly into three categories: strategically managed and holistic cyber security actors, mid-tier companies in which basic processes are in place but management commitment is lacking and actors that view cyber security as a separate technical domain. The strongest domains are threat and vulnerability management, identity and access management and protection of critical services. The most improved domain is workforce development, which has been boosted by the NIS2 Directive, although not all companies yet meet its requirements.
- The weakest domains are situational awareness, risk management, cyber architecture and asset management; in these domains, the prioritisation of risks is hindered by lack of visibility and decentralised management of OT assets. Third-party risk management is still weak; although its maturity has improved, many companies still lack continuous monitoring and contractual requirements. The role of management is crucial: in strategically committed organisations, risk management is integrated into business operations, while in others it remains fragmented and under-resourced. Overall, the sector is making progress, but strengthening its resilience requires more consistent development of basic structures.

Trade and distribution: Established level: 3.11

- The sample consists of retailers, wholesalers, grocers, distributors and food service actors.

Strengths

- Best practices include management systems based on well-known frameworks, such as ISO/IEC 27001, which support systematic and risk-based development. In addition to this, cyber security is increasingly subject to a strategy or plan that guides development and is linked to business objectives.

- Critical services have been comprehensively identified and taken into account in the sector. Their continuity and operational reliability is examined from a number of different perspectives, which is reflected in contingency planning and efforts to ensure the resilience of services. In the most mature organisations, management is actively involved in incident management, reflecting strong commitment.

- Companies make extensive use of automated and regular vulnerability scans in threat and vulnerability management, and the most mature actors use bug bounty programmes to support continuous vulnerability monitoring.

Areas for improvement:

- The surveyed companies rely on partners for many critical functions, but often lack consistent partner network risk management practices. Partnerships are typically based on long-term relationships of trust, with no systematic monitoring of supplier risk or compliance.

- While the role of critical services has been recognised, in lower maturity companies the related continuity plans are incomplete or not in place, service prioritisation has not been completed and cyber incident preparedness is not supported through exercises.

- Further development is needed in the domain of cyber architecture, although the technical foundations are in place. The preparation of an overview would provide a systematic and strategic perspective to technical development. In particular, data classification and data management are inadequate, even though companies in the sector process large amounts of sensitive data. Some companies also employ manual, error-prone processes in identity management.

Comparison between the 2022 survey and the 2025 survey

- The variation between companies in the trade and distribution sector has levelled off slightly, with the majority of companies reaching a good basic level of maturity. This progress has been driven in particular by the NIS2 Directive and national legislation, which have increased management interest in cyber security and supported the adoption of management models such as ISO 27001. While strategic commitment has strengthened, sufficient resourcing remains a challenge. Companies have improved the protection of critical services and continuity planning, which now take into account the impact of cyber incidents and make use of monitoring. Digitalisation and the increasing adoption of cloud services have increased the pressure to develop cyber resilience. However, cyber risk management remains fragmented, which undermines proactive preparedness. Workforce competence has developed: mandatory training, phishing simulations and awareness-raising activities have become more common, and employees are seen as a key part of comprehensive cyber security.

Media: Established level: 3.01

- The sample consists of large and medium-sized Finnish media companies that engage in a wide range of media activities.

Strengths

- The most cyber mature organisations in the media sector have adopted a strategically managed and documented cyber security management model that supports business objectives. This management model is often based on the ISO/IEC 27001 framework and is certified or there are plans to have it certified.
- An increase in threat awareness is reflected in particular in the strengthening of technical protection measures: SOC services, technical scans and threat detection capabilities have become more common. As regards logical access management, best practices include role-based and automated management and multi-factor authentication (MFA).
- All the surveyed actors have identified their critical services, and more mature organisations have developed continuity plans for them. These plans are also regularly tested, demonstrating a mature approach to resilience development.

Areas for improvement:

- While progress has been made, many organisations still face challenges in terms of resource sufficiency. This is reflected especially in a lack of documentation and fragmented cyber security practices.
- Many companies' risk management processes are still underdeveloped or inconsistent and usually not integrated into overall business risk management.
- Partner risk management is another key area for improvement. The definition of security requirements for partners and related compliance monitoring are often lacking.
- Although critical services have been identified, many organisations still have incomplete or undocumented business continuity plans, which undermines their incident response and recovery capabilities.

Comparison between the 2022 survey and the 2025 survey

- In 2022, the sector's most notable areas for improvement had to do with security culture and strengthening the information security awareness of the workforce, and progress has been made in these areas. Companies have invested in training and awareness-raising, which has improved their ability to identify and manage threats. This progress had been accelerated by geopolitical uncertainty, increasingly complex supply chains and regulatory reforms, such as the NIS2 Directive, which have increased pressure to strengthen cyber security management. Half of the surveyed companies now have an information security management system in place and all are developing their management models.
- Risk management has improved, but remains one of the weakest domains, with many companies lacking harmonised and business-integrated practices. Partner risk management remains a vulnerable domain, although related awareness has increased. The sector has made exceptional progress in threat management: organisations are moving away from reactive approaches towards regular and partly automated vulnerability assessment. Although the sector's average maturity has not changed, there are positive underlying trends, the continuation of which requires management to assume an active role in development and cyber risks to be integrated into business decision-making.

Construction: Established level: 3.0

- The sector sample consisted of large and medium-sized Finnish companies and companies that are part of international groups. In the previous survey carried out in 2022, construction companies were included in the manufacturing sector sample. For this reason, a direct comparison with the previous survey is not possible, which is why the analysis focuses on the current results of the construction sector.

Strengths

- The construction sector's best practices in cyber security are based on clear objectives and continuous improvement. More mature organisations see cyber security as a business enabler, but its development is also steered by external requirements such as customer expectations and regulations, including the NIS2 Directive and its national implementation.
- Management systems, especially those based on well-known frameworks such as ISO/IEC 27001, are seen as a competitive advantage, with most organisations already having a management model in place or aiming to implement and certify one.
- Vulnerability management stands out as a strength, with the most mature companies having largely automated it and engaging in comprehensive testing. Vulnerability remediation measures are prioritised according to criticality, and some organisations have incentive models in place for proactive vulnerability identification.
- Financial and payment systems have been recognised as being critical, with companies in the sector investing in protecting them in particular.

Areas for improvement:

- The survey identified common challenges that are slowing down the development of cybersecurity. Many actors have limited cyber security resources, which is influenced by both the general state of the sector and varying levels of management commitment. Management support is often reactive, and development is sometimes invested in only after an incident has already occurred.
- In many cases, cyber security is developed primarily in response to external requirements, such as customer expectations. When this is the case, the real benefits of the likes of management systems may remain unrealised if their practical application is not embedded in the organisation.
- A challenge common to almost all organisations in the sector is third-party risk management, which contrasts with the fact that many companies in the sector report that a significant proportion of cyber security incidents originate in their supply chains. Poor visibility is contributed to in particular by resource constraints, a lack of clear processes and the challenges of managing a multi-vendor environment.

Analysis of the current state of cyber security

- The construction sector exhibits consistent maturity across the cyber security domains, but there is significant variation between companies. The strongest domain is threat and vulnerability management, in which the most mature actors use automated processes and SOC collaboration, while lower maturity ones employ reactive operating models and have limited resources. The main development needs are related to cyber risk management, which is often separate from business risk management. The sector's weakest domain is third-party risk management. Development is driven by customer requirements and certifications such as ISO 27001, which are seen as a competitive advantage, but many companies are still in the process of developing a risk-based operating model. To ensure that limited resources are properly targeted and that cyber security activities deliver real added value, a more risk-based approach is essential.

Water and waste management: Moderate level: 2.83

- The sample consists of a total of nine water or waste management companies and covers the largest actors in the sector; small local actors are not included.

Strengths

- Management systems based on well-known frameworks such as ISO/IEC 27001 are becoming more common in the sector. They provide organisations with a clear structure for managing cyber security, which strengthens the security culture and ensures continuity. At their simplest, companies use a yearly information security schedule, which improves planning and manageability.
- Critical services have been identified in the sector and measures to protect them and ensure their continuity are regularly monitored and developed. Organisations are actively involved in the work of the sector's ISAC information sharing group, which shares threat information and develops common situational awareness. Cooperation with stakeholders is an important part of operational reliability.
- The incident preparedness of many organisations is advanced. Plans, guidelines and responsibilities are clearly defined and operating models have been practised in exercises. This preparedness is particularly evident in companies where management is actively involved in incident management and preparedness.

Areas for improvement:

- Cyber security work in the sector is constrained by limited resources. Budgets, availability of talent and management commitment are not always at a level that would allow for long-term and planned development. This is particularly evident in the fragmentation of cyber security architecture management, process implementation and practical arrangements. Although documentation and guidelines are often in place, their administration and use in practice are often lacking.
- Access management is largely manual in many companies and presents many practical challenges. Privilege creep occurs and practices related to checking that access rights are up to date vary. Multi-factor authentication is not yet in place at all levels, which can leave critical systems vulnerable.
- Many organisations are strongly reliant on partners and suppliers, but the risks associated with cooperation are not always systematically identified or managed. The information security requirements imposed on suppliers are sometimes too general and are not actively monitored.

Comparison between the 2022 survey and the 2025 survey

- The previous survey only included water supply companies, while this survey's sample included nine water and waste management actors, with a focus on the largest companies in the sector. While there are large differences between the companies, there is little variation within individual domains, and development is consistent, with the exception of cyber architecture and risk management, the maturity of which has not changed. Progress continues to be hindered by human resource and budget constraints, whereas the NIS2 Directive and joint development projects are key drivers. The weakest domain is cyber security management, even though its average maturity increased by 0.41 points and all actors score higher than 2.00; companies lack broad management models and management commitment. The strongest domain is protection of critical services (average 3.07), but preparedness does not always cover ICT and automation systems, highlighting the importance of developing cyber security to ensure the continuity of the sector.

Food: Moderate level: 2.71

- The sector sample consists of organisations from the primary food production and food processing industries.

Strengths

- Best practices in the most mature organisations are to a large extent built around management support, strategic management and long-term development.
- The most mature organisations have long been taking measures to promote cyber maturity and investing in a risk-based manner in areas such as network segmentation and the segregation of IT and OT environments. These organisations actively develop the protection of OT environments and related monitoring and documentation, as this has traditionally been the weakest point of manufacturing companies.
- At its best, cyber security development is risk-based and decision-making is guided by a comprehensive understanding of the cyber threat landscape and risk levels. In the most mature organisations, situational awareness is supported by the likes of SOC services, which cover not only the IT environment but also the OT side.
- In higher maturity companies, cyber security objectives are defined in documents such as a cyber strategy, and the compensation of cyber security experts is linked to the achievement of strategic objectives.

Areas for improvement:

- While even the lowest maturity organisations in the sector engage in cyber security work, it is often still reactive and in many cases stems from the need to meet the requirements of the NIS2 Directive. Management commitment varies, and cyber security is often seen as a technical support function rather than a strategic entity.
- In addition to strategic-level areas for improvement, some organisations have room for improvement in the basics. Some companies lack role-based access models and centralised identity and access management solutions and engage in manual access rights management that is dependent on individual people, which increases the risk of privilege creep and complicates lifecycle management. MFA is not comprehensively used and there is a lack of protection practices especially in OT environments.
- Supply chain risk management is structurally weak. Partners' information security requirements are not systematically defined or included in contracts. Lower maturity organisations lack visibility into subcontracting chains and do not understand that technical dependencies are largely universal, as a result of which they also do not carry out active monitoring.

Comparison between the 2022 survey and the 2025 survey

- In the 2022 survey, the sector's areas for improvement included outlining strategic objectives and drawing up a plan to drive management commitment and risk-based decision-making. Over the past three years, cyber security management has been strengthened, ISMS models have been deployed and risk management has developed through more comprehensive identification and assessment. Management commitment, regular assessment and understanding of the business impact of cyber risks have become trends, partly due to geopolitical uncertainty and regulatory pressure. The sector's weakest domain is situational awareness, especially its communication to management, and the challenge is underlined by decentralised environments and low utilisation of SOC information. The maturity of event and incident management has declined, but the increasing utilisation of exercises and the development of documentation are indications of progress, although continuity plans are lacking. Progress is being accelerated by NIS2, but many organisations are still at the planning stage, and the growing threat landscape is increasing the need for preparedness.

Ports, shipyards and operators: Moderate level: 2.61

- In this survey, the sector analysis included actual port operators, i.e. not only ports but also shipyards and operators.

Strengths

- As regards cyber security management practices, higher maturity organisations have a documented information security strategy that is aligned with their business strategy. They develop information security with the help of, for example, a management system based on the ISO27001 framework, and management support is reflected in the results of six of the surveyed organisations.
- The most advanced protection measures are multi-layered, including SOC services, IDS/ IPS systems and network segmentation. Cyber risk management is integrated with the help of business risk management practices. In partner network management, best practices take risks into account as part of overall risk management, and contracts are regularly updated.
- High maturity companies have business continuity and recovery plans as well as workforce substitution plans in place. Employee information security training is varied and its effectiveness is monitored. Identity and access management is the sector's strongest domain, and high maturity organisations have centralised IAM systems in place.

Areas for improvement:

- In lower maturity organisations, cyber security management is reactive and not based on a strategy or documented practices. Architecture design and documentation are lacking, undermining the overall management of protection measures.
- Risk management practices vary, and continuity and recovery plans are often incomplete, outdated and untested. Many actors have shortcomings in threat and vulnerability management processes and documentation. Many also have shortcomings in the protection of OT environments, including limited segmentation, updating and monitoring. Information asset management is fragmented, and lifecycle management tools are to varying degrees manual or semi-automated.
- In partner management, information security is not always systematically considered in terms of contractual requirements, for example. There are significant differences in monitoring capabilities between actors, with some lacking any real-time operational situational awareness.

Comparison between the 2022 survey and the 2025 survey

- In the 2025 survey, this sector's sample only included ports, shipyards and operators, as maritime transport organisations were moved to the transport and logistics sector. The sector's average maturity increased to 2.61 from 2.16 in 2022, reflecting both changes in the sample and genuine progress towards more consistent practices. The most significant improvements were made in workforce management and cyber security management, of which the latter was previously the sector's weakest domain. Challenges such as resource constraints and unclear division of responsibilities have not been eliminated, but there has been a shift from reactive measures towards a more systematic approach, partly driven by the NIS2 Directive and geopolitical uncertainty. The directive has increased management commitment, clarified responsibilities and strengthened risk management, even though its requirements are sometimes perceived as burdensome. Furthermore, the outsourcing of IT services to market- driven partners has improved visibility and management.

Transport and logistics: Moderate level: 2.54

- The 2025 sample consisted of companies in the land, maritime and air transport industries. The size of the actors ranged from small companies to international groups, but the majority were companies employing approximately 100–500 people.

Strengths

- The most mature actors in the sector are multinational groups with centralised cyber security management but separate teams responsible for different domains of cyber security. These actors engage in risk-based cyber security planning and management and have defined a strategic direction for it. The most mature actors describe their dialogue with management as an active and important part of development.
- The most mature actors focus on ensuring that their understanding of the cyber security landscape (including vulnerabilities, monitoring and asset management) is constantly evolving and that development measures can be targeted in a risk-based manner. These objectives are supported by processes and documentation, but they are not based on compliance.
- The companies in the middle of the sector sample in terms of maturity are linked by relatively recent cyber security development projects, the most effective of which are based on an assessment of the current state of cyber security and risk assessment.

Areas for improvement:

- Some companies face significant challenges in organising cyber security domains. These are often small or medium-sized companies that do not necessarily have any employees dedicated to cyber security. With limited in-house human resources, these companies have outsourced a significant proportion of their IT and cyber security services.
- Outsourcing can be cost-effective and appropriate, but the survey found that lower maturity companies were not clear on what their partners' responsibilities were in terms of cyber security or how certain aspects of it, such as asset or vulnerability management, are implemented. This lack of understanding of the current state of cyber security is reflected in the fact that some companies have entire domains rated at level 1, which indicates an unplanned or fully reactive level.
- The biggest difference between the most mature and least mature company is in risk management. At the lower maturity level, cyber risks are assessed sporadically or not at all.

Comparison between the 2022 survey and the 2025 survey

- The average cyber maturity of the transport and logistics sector based on the 2025 survey is 2.54, compared to 2.95 in 2022, but changes in the sample make direct comparison difficult. There is wide variation in maturity between companies, with as many as half falling below 2.5. The differences are actor-specific, not domain-specific. The variation is explained by a lack of guiding requirements and the uneven progress of digitalisation. Cyber security management and identity and access management remain the sector's strongest domains, while the weakest is situational awareness. As regards identity management, the sector's strength is physical access control and process development, while the challenges in situational awareness are related to outsourced monitoring and the invisibility of OT systems. There are no common areas for improvement, but some companies have made significant progress by creating an annual cyber security schedule or carrying out exercises focusing on automation system failures, for example.

Huoltovarmuuskeskus