Report

Impacts of coronavirus pandemic on digital security

VAHTI / Rousku Kimmo (DVV)

Document management

Owner	Finnish Public Sector Digital Security Management Board (VAHTI)
Author	Kimmo Rousku – kimmo.rousku@dvv.fi
Checked by	Erja Kinnunen
Approved by	Finnish Public Sector Digital Security Management Board (VAHTI) digiturva@vahti.fi

Version management

Version no	Action	Date/author
0.90	Draft version	KR 9 June 2020
0.95	Updated draft version	EK 10 June 2020
0.99	Presentation version of the Finnish Public Sector Digital Security Management Board (VAHTI)	KR 10 June 2020
1.00	Version discussed by the Finnish Public Sector Digital Security Management Board (VAHTI)	11 June 2020 KR

Contents

VAHTI / Rousku Kimmo (DVV)

Report

General points

This report has been produced by the Finnish Public Sector Digital Security Management Board (VAHTI), which operates at the Digital and Population Data Services Agency. In order to produce the content of the report, the VAHTI Secretariat organised a survey on the coronavirus pandemic to which it received 136 responses. The results are divided into four categories according to the sector of the respondents.

This is version 1.0 of the report. We will supplement the report's sector-specific results during the summer and publish version 2.0 in August.

The purpose of the report includes

- determining how public administration organisations have succeeded in the changes to their digital operations caused by the spring 2020 coronavirus pandemic, for example how have they succeeded in the organisation of telework and the provision of digital services

- describing the types of threats related to their activities and services organisations have identified and how the threats and the risks arising from them have been managed

- identifying the type of assistance and support that public administration organisations wish to receive from VAHTI

Public sector organisations and all VAHTI Board and the VAHTI Expert Group members will be sent the report as notification. We will present the report to key stakeholders and report on the results and the necessary digital security development measures at our autumn 2020 events.

The report’s target groups include the organisation's management and the persons responsible for digital security and digital security experts (risk management, operational continuity and preparedness, information security, cyber security and data protection).

The Digital and Population Data Services Agency is responsible for compiling an overall picture of the various aspects of digital security in public administration. The on-going public administration digital security development project (JUDO) will implement a digital service that will enable us to carry out similar surveys in coming years. The purpose of the service is to collect centralised, up-to-date information on digital security and to produce reports for public administration organisations on their state of digital security and comparative information on other similar organisations.

VAHTI / Rousku Kimmo (DVV)

Executive Summary

Accelerated digital leap

In March 2020, the global pandemic caused by the coronavirus and the resulting adoption of emergency legislation resulted in a new situation for public administration organisations. The majority of the personnel were directed to telework mainly from home, but at the same time it had to be possible to ensure the performance of statutory or otherwise critical official tasks and services in a rapidly changing situation. The organisations had to provide e-services intended for citizens in both a physical and digital environment and ensure that the performance of the required services was scaled.

When assessed in advance, the success of such a change would have been considered particularly challenging. However, based on the retrospective assessment of this and other surveys, the change has been implemented well, partly even very well. A similar "digital leap" has also been carried out in other countries, but, for example, according to a Eurofound[1] study nearly 60% of the personnel in Finland transitioned to remote work, which is more than in any of the 26 other countries in the comparison. One of the organisations that responded stated that 92% of their staff transitioned to telework at rapidly and successfully.

Good results from long-term digitalisation

The success described above is not just a coincidence or good luck, but the result of the long-term, systematic development of a digital society. This is evidenced, among other things, by Finland maintaining its number 1 ranking in the 2020 DESI index[2]. For a long time, Finland has invested significantly in the digitalisation of operations, in electronic services, and in services for staff and citizens. Finland has long been the nation that uses the world's largest number of mobile data connections[3], and the processes and technical equipment required for remote work have been easily available. One observation made with the survey was that some areas have experienced temporary difficulties with the availability of certain ICT devices (for example, laptops, monitors and headsets), but due to well-functioning logistics chains, these have not created a larger problem.

The corona era has increased threats, but organisations have managed to respond to them

The coronavirus pandemic has required the development of all five areas of digital security. The survey presented 12 general threats. Although all of these had occurred in at least one respondent organisation, it has been possible to successfully manage these threats and the risks arising from them.

[1] https://www.eurofound.europa.eu/sites/default/files/ef_publication/field_ef_document/ef20058en.pdf
[2] https://ec.europa.eu/digital-single-market/en/desi
[3] https://www.traficom.fi/sites/default/files/media/file/Telecommunications-Markets-in-the-Nordic-and-Baltic-Countries-2018.pdf

The responses highlighted three threats that had occurred in at least half of the respondent organisations:

Disruptions related to remote work connections 81%
Communications capacity disruptions 62%
New types of email scams or attacks 59%

Although the volume of digital communication has increased significantly both nationally and internationally, operators have been able to guarantee the required performance and transfers capacity in Finland. Some services have experienced a slowdown and functional interruptions due to a significant increase in the number of users. This is reflected as the above-mentioned disruptions in teleworking connections (81%) and telecommunications capacity (62%). The same phenomenon has also been observed when using services located outside Finland. Most of us have noticed that cybercriminals have been more than capable of changing their fraud methods to exploit the Covid-19 and coronavirus pandemic topics, which is reflected in new types of scam or attack messages (59%).

The operational change has required numerous changes both in the provision of ICT services and in personnel's working methods. As the changes were implemented in an exceptionally short period of time, for example related impact, threat and risk assessments have not been possible. In many organisations, some of the staff may have now had to work remotely for the first time ever, which has meant that the application and development of existing instructions and processes as well as the provision of quick instructions and training for staff have played a key role.

Areas requiring special attention

For the time being, there have been no wide-ranging or otherwise significant data breaches, data leaks or cyberattacks in Finland that could be linked to the pandemic. This does not mean that organisations should not continue to develop digital security. Of the twelve threats to digital security, the three that have materialised the least indicate that the active development of the availability and integrity of services, confidentiality of information and data protection must continue.

Denial of service attacks 10%
Leakage of confidential information 8%
Data and software losses 1%

Of these, denial of service attacks and the leakage of confidential information in particular are threats that, if implemented, may cause significant problems in the organisation's operations. In critical services, they can even hamper society as a whole, which can lead to a loss of public confidence.

What help did the respondents wish to receive?

In the survey, we asked respondents to present their wishes on the type of assistance they would want to be given in the future or how the exceptional circumstances

in spring 2020 should otherwise be taken into account in the development of operations. The most common wish among respondents was that the security of joint communication services be ensured and that uniform instructions on teleworking be provided. A second point that was raised was the need to coordinate and harmonise surveys carried out by the authorities, both in terms of content and the services used. Third, respondents requested that support to make it possible for us to work together in developing things, drawing on the best experiences from different parties and also in learning from mistakes.

Five key observations

Below are the five key observations found in the survey's results. Two positive observations are related to the success of the operational change and three to the development of digital security. Each section also contains extracts of the open feedback respondents submitted.

1. **The transition to remote work and the related technical solutions have been implemented at least well, and partly very well, and no significant exceptions have been observed so far.**

   The persons responsible for digital security and digital security experts see the operation change that took place this spring as a positive, highly successful entity.

   > "Our operational and service capacity has been almost normal for the period following the beginning of March."
   >
   > "Remote work was already used in several functions, although not to the same extent as during the special measures for corona. Even so, our most critical functions have still been implemented on site at our offices."
   >
   > "The greatest challenges have been related to the introduction of new services and processes without being able to ensure their security in the same way as in normal conditions."
   >
   > "The transition was more challenging for some due to the nature of their duties and to disruptions in remote connections."

   In April and May 2020, the Digital and Population Data Services Agency also organised five webcasts intended for different digital security experts. The participants were asked "How well have you managed to carry out your work in emergency conditions?" The views of the responses submitted by 462 respondents support the result of this survey:

   Poorly 0%
   Satisfactorily 5%
   Well 62%
   Very well 33%

   The transition to remote work has been seen as a success, which will certainly change our way of working in the future, so special attention should be paid to the

change. Organisations must ensure their personnel's mental well-being[4] and resilience (crisis resilience), including when returning to the workplace.

According to studies, 95% of information and cyber security incidents and personal data breaches result from human activities[5]; human activities completed negligently due to being rushed or for some other reason or errors. In addition to unintentional activities, attention should be paid to activities that are contrary to instructions and technical solutions should be developed to manage the risks caused by intentional activities. The development of personnel competence and motivation are the most cost-effective ways of improving the digital security of the organisation.

2. **The availability and security of statutory services used or produced by organisations has remained at a high level.**

   Although numerous responses show that the number of e-services has grown even significantly, no major problems have been detected in services intended for citizens or clients. Possible problems apply more often to the organisation's internal technical solutions, such as those related to telework.

   > "The pandemic has had no impact on the functionality of the information systems in use. The number of infections in Finland is so small that the maintenance of information systems has not been disrupted. "
   >
   > "Information systems and other technical environments have been stable throughout the state of emergency and have maintained their performance."
   >
   > "In these areas, the transition to emergency conditions and remote work required significant additional work for a period of a few weeks, but, as a result, the systems are now able to support operations very well."

3. **There is a lack of uniform guidelines and policies for the inspection and safe use of newly commissioned communication systems and possible cloud services.**

   The responses show that some organisations have had to introduce new services at a very fast pace. It appears that interpretations on the use of services have varied a great deal between different public administration organisations. Some organizations may have completely denied access to a service, some have allowed access with additional controls, and the rest allowed access to the service as is.

   > "Analysis of risk scenarios, development of preparedness and instructions in a coordinated manner e.g. in remote work (information security, data

[4] https://www.ttl.fi/ohje-etatyosta-ja-henkisesta-hyvinvoinnista-tyopaikoille-koronavirusepidemian-ehkaisyyn/
[5] https://www.researchgate.net/publication/329806166_Botching_Human_Factors_in_Cybersecurity_in_Business_Organizations

protection aspects). The implementation of national, independent information security audits or similar of various communication and remote meeting tools (Meet, Skype, Teams, Zoom).“

"We need uniform and clear operating instructions, for example, for the implementation of broad-scoped telework in municipal functions and for the implementation of the electronic functions required by law (e.g. electronic signature) with a remote connection. Instructions on the confidentiality of electronic customer service (e.g. education services, early childhood education and care), implementation of electronic customer service in practice).“

Webcasts organised by the Digital and Population Data Services Agency asked participants “In what direction do you feel digital security has developed over the past few months?” The 454 submitted replies were divided as follows:

Improved somewhat 10%
Remained the same 47%
Worrying 42%
Very worrying 2%

44% of survey respondents stated that security is developing in a worrying direction, while 10% felt that digital security has improved. This is likely due to the fact that these organisations have had to pay more attention and perhaps had to improve their information security or preparedness for disruptions. Although experts have been concerned about the current security situation, our survey shows that so far these concerns have not materialised to a large extent.

4. No harmonised guidelines for remote work

One clear area of development is related to remote work by personnel and, in particular, to ensuring the confidentiality of confidential or personal data that must be processed. Some experts are concerned about how confidential or personal data are securely processed in remote work. Another concern is that when the majority of work takes place remotely, guaranteeing and supervising security becomes significantly more difficult than when these duties are carried out in shared offices.

"National steering in, for example, the selection of teleworking tools. Risk management processes - assistance in the selection of common approaches. “

"Remote work increases data protection risks. I can even be impossible to monitor compliance with guidelines. The supervision of remote work is an unfamiliar task for some supervisors.“

"In my opinion, information security and data protection have declined by a unit due to the fact that more employees have been left to take care of matters alone at home.”

5. Development of a coherent situational picture and processes for collecting information

Another area which was highlighted as a development area was the compilation of a “situational picture” both within an organisation and between authorities. The respondents had received numerous, partly overlapping surveys from different authorities. The level of information security of implemented surveys and the reporting services used seems to vary. The survey conducted to produce this report was produced as an Excel file, which the respondents classified according to their own instructions. The majority submitted their responses by secure mail.

> "We did not have the data required to build the situational picture, systems have been developed at a fast pace”
>
> "An electronic analysis and situational awareness system is missing. Too Word, PowerPoint, email focused.“
>
> "We do not always know what information we can include in our response to a survey sent to us because the tool used does not tell us about its security”

The VAHTI Board has discussed this report at its meeting on 11 June 2020, where its key observations were examined. The planning of the necessary development measures will be assigned to the five VAHTI working groups to be appointed summer 2020. The groups will regularly report on their activities to the Board and present the results of their activities at VAHTI events.

1 Report respondents and sectors

On 11 May, the survey concerning the coronavirus pandemic was sent to the registries of approximately 490 public administration organisations, and the response period ended on 29 May. We know that organisations have been asked to submit numerous other reports participate in numerous other surveys over the spring. The submitted 136 responses and a response rate of 26% can be considered good compared to the available response time and timing of the survey. It is our experience, that this number of responses and response rate form a sufficiently reliable base for an overall picture.

The responses were divided by sector as follows:

1. Municipalities and joint municipal authorities 60 responses 44%
2. Hospital district or other social and health sector actor 12 responses 9%
3. Central government and indirect central government 55 responses 40%
4. University or other educational institution 9 responses 7%

2 Implementation method and results of survey

The survey comprised five multiple choice questions and two open questions. The questions concerned what kind of assistance the organisations would like to receive and feedback on the survey. An effort was made to keep the survey concise and quick to answer as the organisations had numerous other surveys to respond to at the same time. The respondents were also exceptionally busy with other work due to the current situation.

2.1 Topics surveyed in questions

2.1.1 Progress of statutory duties

The survey's first question was "How would you rate on average the performance of your organisation's statutory duties since the beginning of March 2020?" The purpose of the question was to find out how successful the performance of the organisations' statutory duties has been since March 2020. The question aimed to focus on activities that are critical to the organisation's operations, because it is clear that some organisations had to prioritise other activities, processes and services.

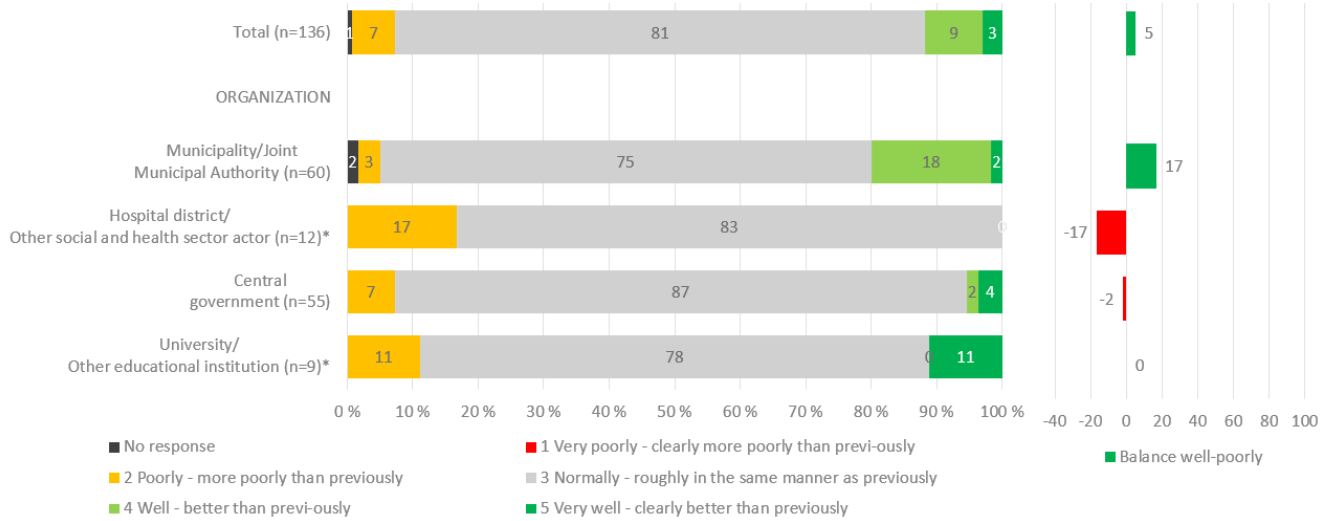

Figure 1. Chart Performance of statutory duties in spring 2020.

As a whole, the organisations' operations have mainly been carried out normally, in much the same way as before. The greatest differences can be seen between two sectors: Municipalities and joint municipal authorities have been able to operate significantly better than before, while hospital districts and other social and health sector actors have fared more poorly than previously. On average, the situation is slightly better than before, but the difference is not a significant one. The operations of hospital districts and social and health sector actors are likely affected by the influx in their workload caused by the pandemic as well as administrative and technical changes and other threats to the organisation's activities.

	Total	**Municipality/Joint Municipal Authority**	**Hospital district/ Other social and health sector actor**	**Central government**	**University/ Other educational institution**
No response	1 %	2 %	0 %	0 %	0 %
1 Very poorly - clearly more poorly than previously	0 %	0 %	0 %	0 %	0 %
2 Poorly - more poorly than previously	7 %	3 %	17 %	7 %	11 %
3 Normally - roughly in the same manner as previously	81 %	75 %	83 %	87 %	78 %
4 Well - better than previously	9 %	18 %	0 %	2 %	0 %
5 Very well - clearly better than previously	3 %	2 %	0 %	4 %	11 %
Total	100 %	100 %	100 %	100 %	100 %

Table 1. Performance of statutory duties in spring 2020.

2.1.2 Transition to remote work

Perhaps the most significant change during the coronavirus pandemic was the need to transition quickly and to a large extent to remote work. The question "How well has the transition to remote work succeeded in your organisation?" helped in determining whether the overall positive image of the effectiveness and success of remote work was correct.

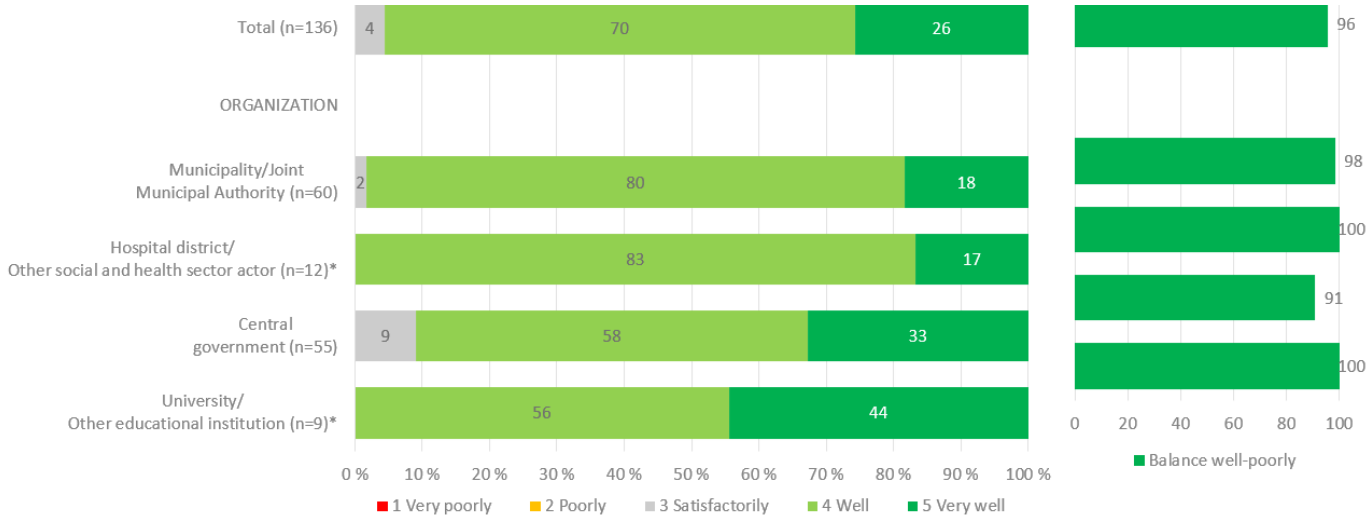

Figure 2. Chart Transition to remote work in spring 2020.

The answers show that telework has gone well and very for some of the respondents. None of the respondents reported that operations had suffered due to telework. Every sector was satisfied to a significant extent with the operational change related to remote work. 9% of respondents in central government alone found that the transition had been satisfactory.

	Total	**Municipality/Joint Municipal Authority**	**Hospital district/ Other social and health sector actor**	**Central government**	**University/ Other educational institution**
1 Very poorly	0 %	0 %	0 %	0 %	0 %
2 Poorly	0 %	0 %	0 %	0 %	0 %
3 Satisfactorily	4 %	2 %	0 %	9 %	0 %
4 Well	70 %	80 %	83 %	58 %	56 %
5 Very well	26 %	18 %	17 %	33 %	44 %
Total	100 %	100 %	100 %	100 %	100 %

Table 2. Transition to remote work in spring 2020.

2.1.3 Support for information systems and services in emergency conditions

The third question was "How well have information systems and e-services supported operations under the Emergency Powers Act?" The aim of this question was to find out how successfully the transition to operations under the Emergency Powers Act, which was implemented for the first time in Finnish history, has progressed with regard to information systems and electronic services.

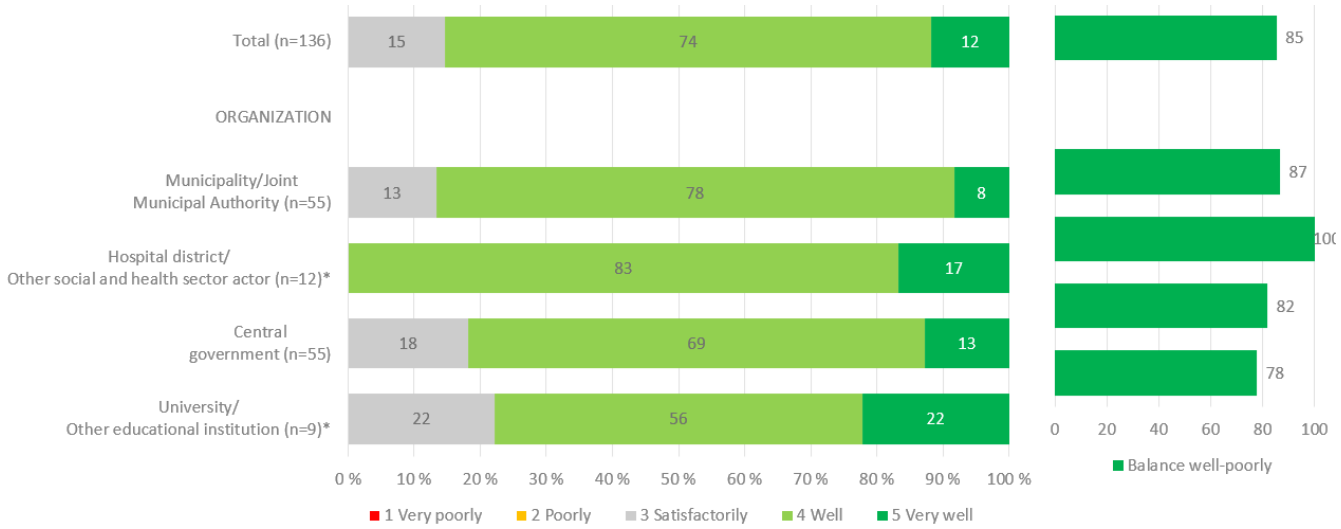

Figure 3 Chart Support for information systems and services for activities under the Emergency Powers Act.

One of the more unforeseen positive surprises of the survey was that based on the responses, the introduction of the Emergency Powers Act, which had previously only been tested in various exercises in Finland, and operating under it, have on average gone well, in some cases even exceptionally well.

In particular, the situation of hospital districts and other social and health sector actors is somewhat better than that of other sectors where only small differences can be observed.

	Total	Municipality/Joint Municipal Authority	Hospital district/ Other social and health sector actor	Central government	University/ Other educational institution
1 Very poorly	0 %	0 %	0 %	0 %	0 %
2 Poorly	0 %	0 %	0 %	0 %	0 %
3 Satisfactorily	15 %	13 %	0 %	18 %	22 %
4 Well	74 %	78 %	83 %	69 %	56 %
5 Very well	12 %	8 %	17 %	13 %	22 %
Total	100 %	100 %	100 %	100 %	100 %

Table 3. Support for information systems and services for activities under the Emergency Powers Act.

2.1.4 Implementation of digital security

The fourth question was "How well have you managed to deal with the various areas of digital security since the beginning of March 2020?" The aim was to determine how organisations assessed the development of activities in the five different areas of the digital security framework during the coronavirus pandemic. The Digital Security Framework comprises:

- Risk management
- Continuity of operations and preparedness
- Information security
- Cyber security
- Data protection

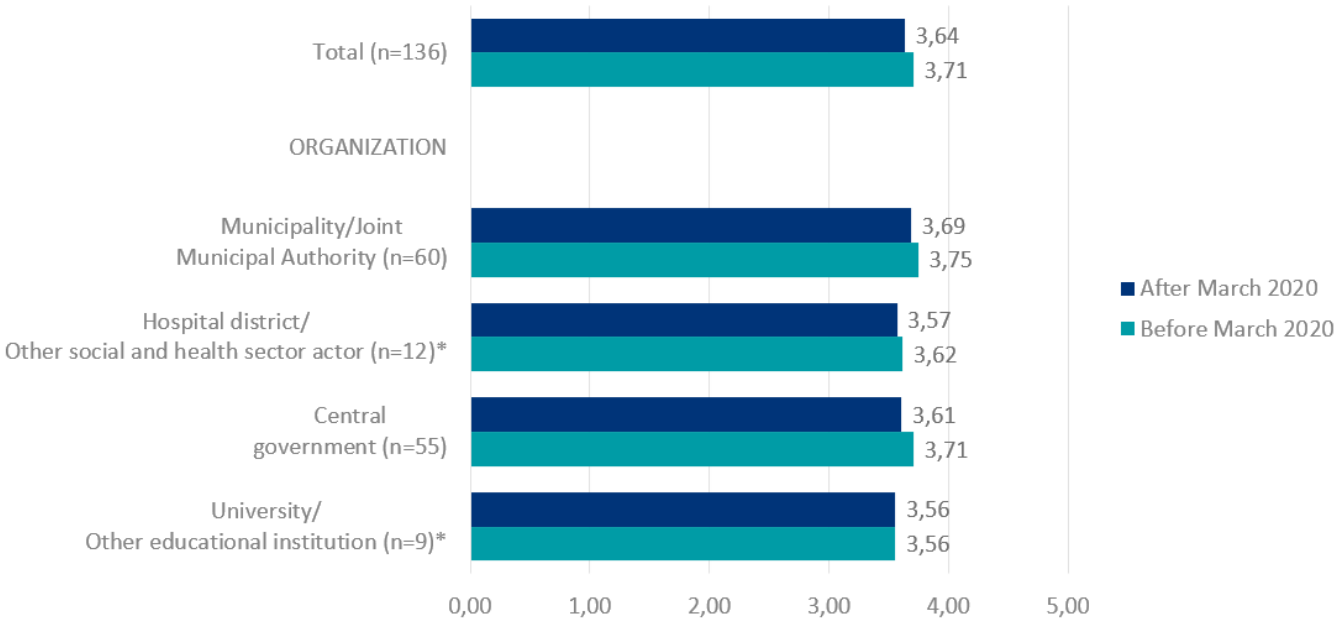

Figure 4. Chart Development of digital security during spring 2020.

The assumption associated with the question was that the organisations would report that the individual areas of digital security, such as information security or data protection, had clearly weakened as a result of the spring's operational change. Based on the responses, organisations have assessed that they were able to take care of digital security almost as well as before the corona era.

The average achieved before March was 3.71 (which was good on the survey's scale). The 0.07 unit decline caused by the coronavirus pandemic can be considered small. 37% of respondents feel that their digital security has deteriorated, while 16% feel that the situation has improved. As a whole, the assessment and maintenance of the existing level can be considered a very good result.

	Total	Municipality/Joint Municipal Authority	Hospital district/ Other social and health sector actor	Central government	University/ Other educational institution	Average
How well have you managed to deal with the various areas of digital security since the beginning of March 2020?	3.64	3.69	3.57	3.61	3.56	3.61
Prior to March 2020	3.71	3.75	3.62	3.71	3.56	3.67
Difference	-0.07	-0.06	-0.05	-0.10	0.00	-0.06

Table 4 . Development of digital security during spring 2020.

A different view can be produced of the previous chart, which better describes the development of digital security by sector. The situation has weakened most percentage-wise in municipalities and joint municipal authorities, while it has otherwise improved in these. 43% of the respondents in this group estimated that digital security had suffered and 18% that it had improved.

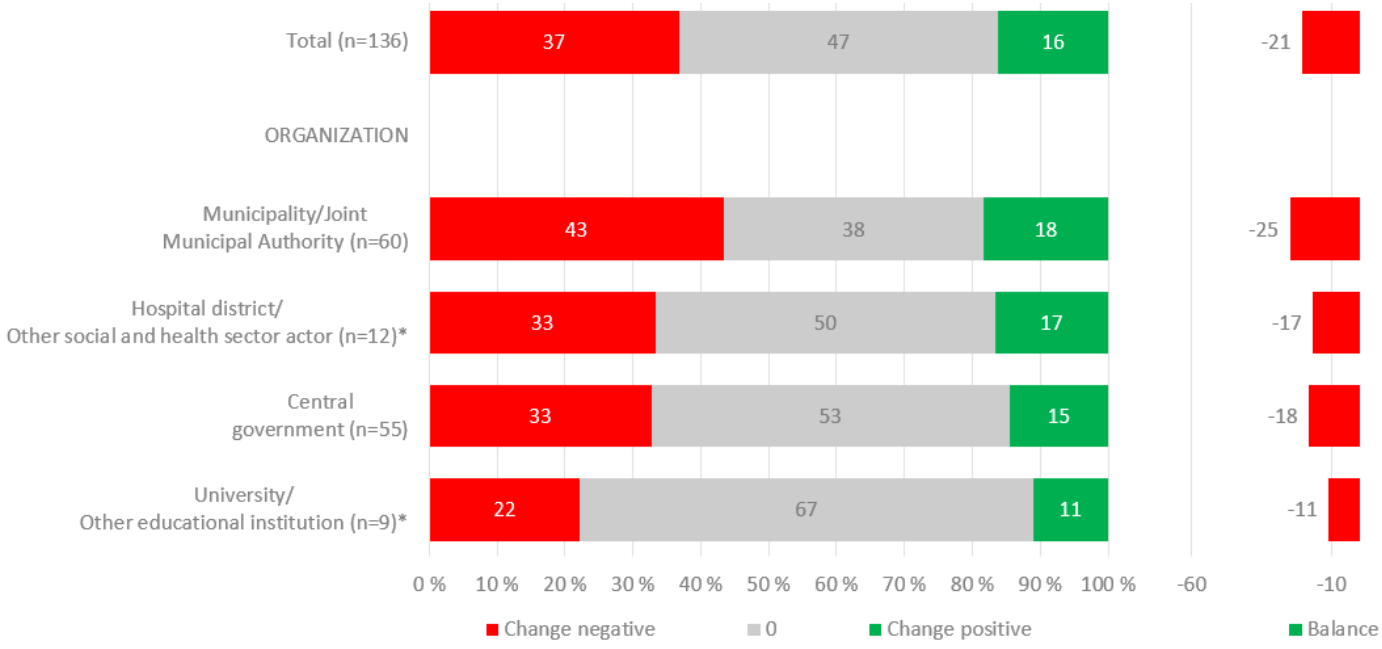

Figure 5. Chart Development of digital security by sector during spring 2020.

	Total	Municipality/Joint Municipal Authority	Hospital district/ Other social and health sector actor	Central government	University/ Other educational institution
Has declined	37 %	43 %	33 %	33 %	22 %
Remained at the same level	47 %	38 %	50 %	53 %	67 %
Improved	16 %	18 %	17 %	15 %	11 %
Total	100 %	100 %	100 %	100 %	100 %

Table 5. Development of digital security by sector during spring 2020.

2.1.5 Response averages

In this paragraph, we have calculated the average of the four previous questions, which allows us to assess the differences between sectors - or rather the lack of these.

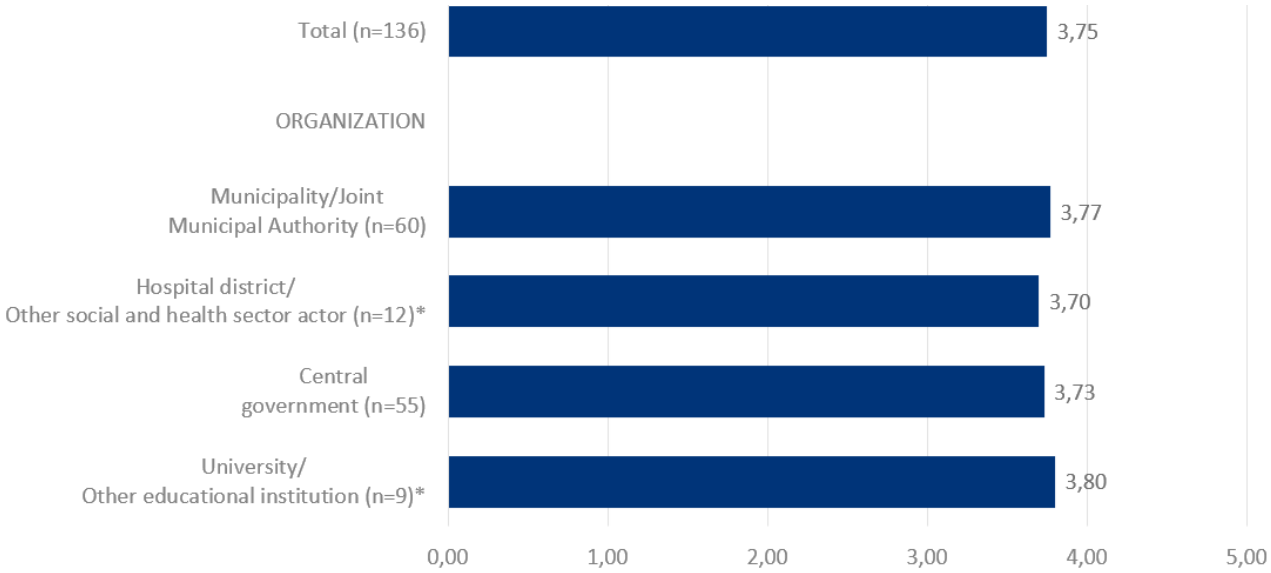

Figure 6. Chart Average of questions 1 to 4.

The average for all the responses is 3.75, which rates slightly below good. Differences between sectors are extremely rare in this case, at just 0.05 below and above the average. This demonstrates that the coronavirus pandemic has had very similar impacts on all the sectors that participated in the survey. Difference were slightly greater in some questions, but as a whole they were quite minor.

	Total	Municipality/Joint Municipal Authority	Hospital district/ Other social and health sector actor	Central government	University/ Other educational institution
Average for sections 1-4.	3.75	3.77	3.70	3.73	3.80

Table 6. Average of questions 1 to 4.

2.2 Threats experienced by organisations

The second section of the survey consisted of questions related to the identification of threats and the development of operations. The purpose of these questions was to determine what kind of threats related to the activities have been materialised during the spring and how successfully they have been managed. At the same time, the aim was to find out how organisations have developed their activities and how they have been able to take digital security into account in this development.

2.2.1 Realisation of different threats

Organisations were asked in what manner 12 pre-selected threats have been realised in their activities. The response options for each threat were either yes or no. It was also necessary to assess how many threats have materialised and how they have been taken into account in risk management.

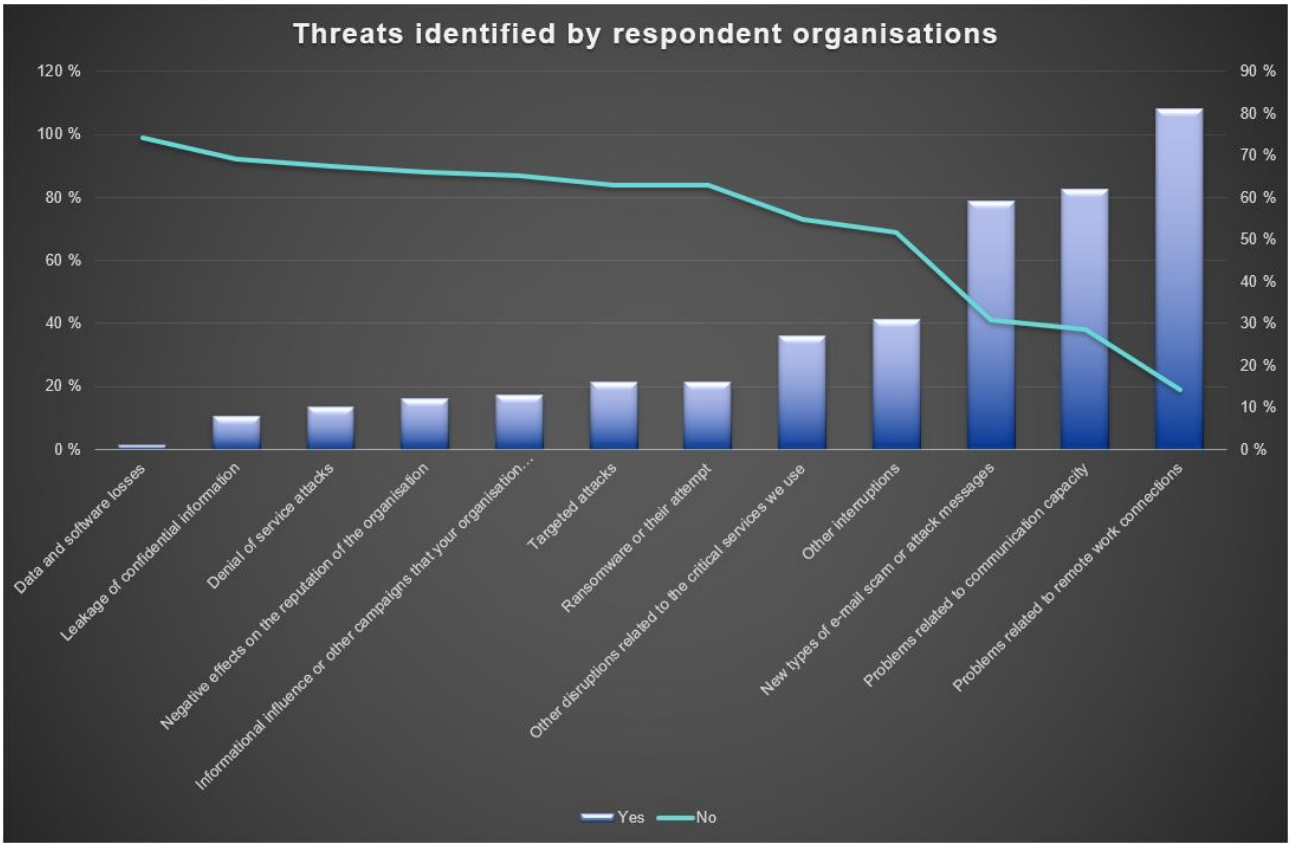

Figure 7. Chart Threats identified by the respondent organisations, the blue bar represents the percentage, how many respondent organisations has the threat materialised in - the orange line represents the number of organisations in which the threat did not materialise.

By far, the largest number of problems have been caused by disruptions related to remote connections (81%), although after the very first stages, the problems related to these have been better managed.

The second largest number of problems were caused by disruptions related to telecommunications capacity (62%). As a result, there has been a need to restrict or provide guidelines for personnel activities, for example in the use of the VPN service. For some of the respondents, this threat has materialised in the form of a slowdown and overload in international cloud services. On the other hand, operators that provide telecommunications connections in Finland have been able to successfully provide telecommunications capacity despite a significant increase in load.

The third most common threat has been "New types of email scams or attacks" (59%). In practice, numerous criminal organisations and cybercriminals quickly altered to topics of their existing scam methods to Covid-19 or the coronavirus pandemic. The malware solutions used by organizations are normally able to filter these, and, in practice, they are a bigger problem for people who use e-mail in their free time.

The materialisation rate for the remaining nine threats remained below 50%. With regard to these it is worthwhile noting that there is a relatively high number in the section Ransomware or their attempt (16%). This figure may in part be due to the fact that many people receive individual scam emails that aim at extorting the email user. These messages often threaten to the publish a lewd video of the person if they do not pay the blackmailer. Naturally, organisations must warn and instruct personnel to act correctly in these situations.

It was positive to note that the threats that materialised the least were the particularly critical ones, including denial of service attacks (10%), leakage of confidential information (8%) and loss of data and software (1%). On the other hand, it was concerning to note that 8% of organisations have identified the leakage of confidential information as a threat. The survey did not provide information on the classification or quantity of this data, so no further analysis of this could be carried out.

Threat	Yes	No
Problems related to remote work connections	81 %	19 %
Problems related to communication capacity	62 %	38 %
New types of e-mail scam or attack messages	59 %	41 %
Other interruptions	31 %	69 %
Other disruptions related to the critical services we use	27 %	73 %
Targeted attacks	16 %	84 %
Ransomware or their attempt	16 %	84 %
Informational influence or other campaigns that your organisation has been a target of	13 %	87 %
Negative effects on the reputation of the organisation	12 %	88 %
Denial of service attacks	10 %	90 %
Leakage of confidential information	8 %	92 %
Data and software losses	1 %	99 %

Table 7. Threats identified by respondent organisations, the threats with the highest rate of materialisation shown at the top and those with the lowest rate at the bottom.

2.2.2 Implementation of risk management related to threats

Organisations were asked how well they have identified and managed the risks mentioned above. The table below shows that risk management has for the most part corresponded with the identification of materialised risks; the more the threat has hampered the organisation's operations, the more attention has been paid to the management of the risk in question.

Risk management was assessed on the following scale:
4 The threat has been identified and the resulting risk has been well-managed
3 The threat has been identified and the residual risks associated with it are for the most part under control
2 The threat has been identified but involves clear, partly unknown and uncontrolled risks
1 The threat has been identified and involves clear, significant, uncontrolled risks that threaten our activities.
0 We have not identified and addressed this threat at all

Threat	Risk management
Problems related to remote work connections	2.88
New types of e-mail scam or attack messages	2.59
Problems related to communication capacity	2.45
Other interruptions	1.87
Other disruptions related to the critical services we use	1.95
Targeted attacks	1.70
Ransomware or their attempt	1.84
Informational influence or other negative campaigns that your organisation has been a target of	1.76
Negative effects on the reputation of the organisation	1.73
Denial of service attacks	1.78
Leakage of confidential information	1.76
Data and software losses	1.76

Table 8. The respondents have identified and managed various threats

The table shows that for example the section “Other interruption of operations”, Targeted attacks”, “Negative effects on the reputation of the organisation”, and Denial of service attacks” are not in exactly the same order as in which they have materialised

in organisations, but the difference is not significant. What is most important is that the three risks that have overwhelmingly harmed activities the most have been identified and attention has been paid to their management.

Note

> *Some organisations have responded to individual threats by selecting option* ***1 The threat has been identified and involves clear, significant, uncontrolled risks that threaten our activities.***
>
> *Each respondent organisation should review its response and reassess what kind of management measures should be taken for such a risk. Organisations should use the table above to assist in this task. The higher the incidence of such a threat has been in other organisations, the more important it is to manage this uncontrolled risk that threatens an organisation's activities.*

In August 2020, we will publish an updated version of this report in which we will discuss the different aspects in more detail. The table above can also be interpreted in such a way that although the organisation has not identified the risks associated with the threats on the list, they may need to manage them better in the future.

The average risk management value for all identified risks (i.e. risks included in responses) was 3.23, which can be considered surprisingly high. However, it should be noted that some respondents had only identified one or two threats that they were targeted by. If these were well-managed, the response was 4, i.e. the organisation was able to successfully manage the threat and the resulting risk.

The respondent organisations can check their own their own response tables in the Summary of answers tab in the section "How many different threats have you experienced - the minimum is 0 and the maximum is 12 (the larger the number the more concerning the situation)". The table below shows the average number of threats various organisations have identified being targets of.

	All	Municipality/Joint Municipal Authorities	Hospital district / other social and health sector actor	Central government	University/ other educational institution
Number of actual threats: How many different threats have you experienced - the minimum is 0 and the maximum is 12	3.39	3.13	3.00	3.67	3.89

Table 9. On average, how many individual threats have organisations identified by sector.

Universities and other educational institutions identified the largest number of materialised threats (3.89 threats / organisation), while hospital districts and other social and health sector actors identified the least (3 threats / organisation) with the overall average being 3.39.

2.2.3 Extent of materialised threats/threat

The respondent organisations can check their own response tables in the Summary of answers tab under "Extent of materialised threats: How many different threats have been targeted at you". The table below shows how many threats have materialised in different sectors.

The organisations specified the number of threats for each materialised threat and they were awarded points as follows:
None 0 points
Individual/few 1 point
Some 2 points
A significant number 3 points
A large amount 4 points

A comparative figure has been calculated from these. The larger the number is, the threats have materialised in the organisation.

	All	Municipality/Joint Municipal Authorities	Hospital district / other social and health sector actor	Central government	University/other educational institution
Extent of actual threats: How many different threats have been targeted at you - the minimum is 0 and the maximum is 48	5.02	4.40	4.50	5.78	5.22

Table 10. How many different threats materialised in the organisations.

The average of the comparative figure is 5.02. Central government identified the largest number of materialised threats, while the municipalities and joint municipal authorities identified the least.

In this context, it is worth mentioning separately that the majority of responses related to the number of materialised threats comprised either Individual/Few or Some responses. Only a few organisations had noticed a significant incidence of individual threats, and the option Many had only been selected in one response.

This is also illustrated by the fact that when the average of 5.02 is divided by the average of materialised threats 3.39, the value is 1.48. This value ranges between Individual/Few and Some.

The threats that materialised the most often also had the largest incidence of problems:

- Problems related to remote work connections
- New types of e-mail scam or attack messages
- Problems related to communication capacity

2.2.4 Bringing threats into the scope of risk management

The respondent organizations can review their own response tables in the Summary of answers tab under "How has your risk management managed these threats?" This section describes how successfully organisations have on average managed threats.

The organisations' assessments of the level of risk management for each of the 12 threats have been scored as follows:
4 The threat has been identified and the resulting risk has been well-managed 0 points
3 The threat has been identified and the associated residual risks have for the most part been managed 1 point
2 The threat has been identified, but it involves clear risks that are partly unknown and unmanaged 2 points
1 The threat has been identified and involves significant unmanaged risks that threaten our activities 3 points
0 We have not identified and addressed this threat at all

The minimum comparative figure is 0 points and the maximum 36 points, the lower the score, the better the threat management.

	All	Municipality/Joint Municipal Authorities	Hospital district / other social and health sector actor	Central government	University/other educational institution
Identification and management of risks: How has your risk management managed these threats?	6.67	6.50	7.17	5.80	12.44

Table 11. How has risk management managed threats?

The average response was 6.67. Central government was awarded the lowest score (5.80), with only universities and other educational institutions deviating significantly from the average. When evaluating responses, it should be noted that the value is also influenced by the fact that not all respondents have identified and processed all threats, and, in this respect, there are significant differences between the different respondents.

2.3 Development of operations in a changed operating environment

The last two questions in the survey concerned how the organisation may have changed its digital security operating principles in the changed operating environment.

2.3.1 Change of processes and security-related policies

The organizations that responded can check their own response tables on the Summary Answers tab under "How much have you had to change your existing processes and security-related policies?"

This section included the following questions:

Developing activities and facilitating development in a changed operating environment

A) We have introduced new processes or services without adequate risk management OR
B) Risk management has not been compromised even though we have introduced new processes or services OR
C) both

A) We have introduced new tools or services without adequate safety testing OR
B) we have introduced new tools or services after sufficient safety testing OR
C) both

A) We have compromised our security-related processes to enable the availability of services OR
B) We have not compromised our safety processes to enable availability of services OR
C) both

A) While working remotely, our personnel may have processed materials that they were previously not permitted to process
B) While working remotely, our personnel have not been able to process materials that they were not previously permitted to process or
C) both

A) The instructions and training provided to our personnel in the unusual circumstances have been inadequate OR

B) The instructions and training provided to our personnel in the unusual circumstances have been sufficient OR
C) both

A) We have had to undermine processes related to the processing of personal data OR b) We have not had to undermine processes related to the processing of personal data OR
C) both

4 points were awarded for the first answer option, 0 points for the second answer option, and 2 points for the third answer option. The minimum total score was 0 (no compromise on security) and the maximum was 24 (significant process changes have been required).

While the highest score for an individual organisation was 16 points, about 20 respondents received 10 or more points. The lowest score was 2, received by two respondents.

	All	Municipality/Joint Municipal Authorities	Hospital district / other social and health sector actor	Central government	University/other educational institution
How much have you had to change your existing processes and security-related policies?	5.07	4.88	4.33	5.33	5.78

Table 12. How much have you had to change your existing processes and security-related policies?

The average for all respondents was 5.07. Hospital districts and other social and health sector actors had the lowest average (4.33), while universities and other educational institutions had the highest (5.78). The more compromises or downgrades an organisation has had to make to its existing digital security operating models or processes, the more carefully it must ensure the security of its operations and information and the realisation of data protection when returning to normal operations.

2.3.2 Scope of changes

The organizations that responded can check their own response tables on the Summary Answers tab under "How much have you had to change your existing processes and security-related policies?" This section compares the extent to which the organisation has had to implement these changes in its operations.

The answers have been given using the following scale:

- Not at all
- Single/a few
- Some
- A significant number
- A large amount

The table shows a calculate comparative number, which is based on the option selected in the previous section and the extensiveness of the change. For example, if the organisation has implemented "New processes or services without adequate risk management" and these have been "Many", 16 points will be awarded. Correspondingly, if the organization has chosen "We have not undermined security processes to enable access to services", 0 points will be awarded.

The minimum for this comparative figure is 0 (security has not been compromised at all or it has been compromised very little) and the maximum is 96 (a large number of security downgrades have had to be implemented).

	All	Municipality/Joint Municipal Authorities	Hospital district / other social and health sector actor	Central government	University/other educational institution
How extensively have you had to implement these changes?	4.44	3.93	4.50	4.75	5.89

Table 13. How extensively has your organisation had to implement these changes?

Although the scale was broader in this question than in others, the average remained at a moderate level (4.44). In this section, municipalities and joint municipal authorities received the lowest comparative figure while universities and other educational institutions received the highest (5.89). Differences between sectors can be considered small.

In total, about 15 organisations received a higher value than 10 and two organisations higher than 30.

This question has also been used to encourage organisations to assess what digital security changes they have made and what impacts these changes may have on the organisation's security. The changes should be recorded, and the associated risks assessed to ensure that the security and reliability of operations can be restored to a level at least equivalent to that which it was at prior to the coronavirus pandemic when returning to normal conditions.

2.4 Open questions

2.4.1 Assistance that respondents would like to see from VAHTI and other authorities

At the end of the survey there were two open questions, the first of which was "What kind of help would you like from VAHTI activities or other authorities in this situation or to enable recovery and to ensure security and trust?”

A total of 49 responses were given to this, some of the key wishes of which are summarised in the word cloud below.

Organisations do not expect any actual help in dealing with the coronavirus pandemic, as the situation is considered to be under control, but the following summarised proposals were highlighted:

- assessment of remote work tools and mobile solutions, cloud information security (the independent assessment of the security of services commonly used)
- further instructions and training in the different areas of digital security
- snapshot reporting
- confirmation of the adequacy of telecommunications capacity
- network-based work to ensure cooperation and share the best experiences
- training and exercises to prepare for similar situations
- instructions and guidelines on the use of cloud services
- joint risk reporting and scenarios
- the situation should be calmed down during crisis work – which means that everything unnecessary must be eliminated
- development of the competence and awareness of organisation management
- support in identifying critical services and processes
- VAHTI could compile all the lessons learnt from the coronavirus

The following are three wishes picked out of the responses:

- "VAHTI work should be focused on ensuring that 20% of the organisation’s resources cover and manage 80% of risks. The rest remain a residual risk, and it is not worth sacrificing resources for them. “
- "A summary of what types of cyber security incidents that have been detected in Finland during the pandemic and how these have been prevented/investigated.”

- "General and easy to understand remote work instructions (staff + shop stewards)."

Both in this answer and in some of the previous questions highlighted the support and materials provided by the Cyber Security Centre located at the Finnish Transport and Communications Agency and other communication not only in the management of the coronavirus pandemic but more generally in the development of information and cyber security.

2.4.2 Comments, ideas and feedback

Ultimately, we received 36 other comments. The feedback included comments thanking us for the survey and expressing how necessary it was. The largest number of development proposals were given for the last questions as they did not include all the response options that the respondent organisation wanted. Feedback was also given on how the scales in all the questions should be uniform. In addition, respondents requested that in future the survey could be answered online.

All this feedback will be taken into account in the Digital and Population Data Services Agency's JUDO project, which is developing the overall digital security image service that can be used to implement such surveys in the future.

Below are three feedbacks picked out of the responses:

"Thank you for the survey, it is good that information on these matters is collected. Completing this with an expert group was rewarding.“

"As a municipal actor, it is difficult to fill in this table because our activities are so extensive.”

"Responding as such benefited the organisation, and we will use this form for our own follow-up. The compilation and internal processing of the responses helped to inform our top management of matters related to digital security in an appropriately concise form, although the management has been occupied with other urgent tasks and concerns over the spring, and digital security itself has not been a concern for top management during the corona situation.“