



SECUREHOSPITALS.EU

RAISING AWARENESS ON CYBERSECURITY IN HOSPITALS ACROSS EUROPE AND BOOSTING
TRAINING INITIATIVES DRIVEN BY AN ONLINE INFORMATION HUB

D2.2 Current perceptions and trends on cybersecurity in hospitals



This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No 826497.

PROJECT DESCRIPTION

Acronym: **SecureHospitals.eu**

Title: **Raising Awareness on Cybersecurity in Hospitals across Europe and Boosting Training Initiatives Driven by an Online Information Hub**

Coordinator: INTERSPREAD GmbH

Reference: 826497

Type: CSA

Program: HORIZON 2020

Theme: eHealth, Cybersecurity

Start: 01. December, 2018

Duration: 26 months

Website: <https://project.securehospitals.eu/>

E-Mail: office@securehospitals.eu

Consortium: **INTERSPREAD GmbH**, Austria (INSP), Coordinator
Erasmus Universiteit Rotterdam, Netherlands (EUR)
TIMELEX, Belgium (TLX)
Fundacion Privada Hospital Asil de Granollers, Spain (FPHAG)
Cooperativa Sociale COOSS Marche Onlus, Italy (COOSS)
Arbeiter-Samariter-Bund, Austria (SAM)
Johanniter International, Belgium (JOIN)
European Ageing Network, Luxembourg (EAN)

DELIVERABLE DESCRIPTION

Number:	D2.2
Title:	Current perceptions and trends on cybersecurity in hospitals
Lead beneficiary:	EAN
Work package:	WP2
Dissemination level:	PU
Type	R
Due date:	30.04.2019
Submission date:	10.15.2019
Authors:	Karel Vostry, EAN
Contributors:	Tessa Oomen, EUR Jason Pridmore, EUR Stela Shiroka, INSP Yung Shin Van Der Sype, TLX Georg Aumayr, JOIN Marc Jofre, FPHAG Sigrid Panovsky, SAM Marco Antomarini, COOSS Francesca Cesaroni, COOSS
Reviewers:	Stela Shiroka, INSP

Acknowledgement: This project has received funding from the European Union's Horizon 2020 Research and Innovation Action under Grant Agreement No 826497.

Disclaimer: The content of this publication is the sole responsibility of the authors, and does not in any way represent the view of the European Commission or its services.

TABLE OF CONTENT

1. Introduction.....	9
2. Methodology and Demographics of the respondents	10
3. Findings.....	14
3.1 Staff Training and Awareness.....	14
Q1: Do you have a Data Protection Officer or someone in charge of Data Security at your organization?	14
Q2: What is the number of staff members working at your organisation who use IT devices? ...	15
Q3: How is the relation of the cybersecurity responsible in your organisation?.....	17
Q4: What is the ratio of staff responsible for cybersecurity to those who use IT devices at your organisation?	18
Q5: Are all employees trained and assessed in privacy and data security related matters (such as phishing, identity theft, social media and mobile devices) on at least an annual basis?	19
Q6: What is the percentage of your staff trained in GDPR rules?	21
Q7: In which topics is the staff of your organisation regularly trained?	22
Q8: Does your organisation have an education/training department?	23
Q9: How many hours of education/training in cybersecurity are mandatory at your organisation?	25
3.2 Risk Assessment	26
Q10: How often do you use a computer?	26
Q11: How often do you manage personal data (i.e. of patient, clients)?	27
Q12: Are you concerned about cybersecurity?.....	28
Q13: Do you know the potential impacts of a cybersecurity attack? If yes, which impacts do you think a cyberattack can have to your organisation?	30
Q14: How important do you think is cybersecurity for your organisation?.....	32
Q15: Do you interact with your organisation's IT department?	33
Q16: When you have cybersecurity concerns, who do you contact what to do?	35
Q17: How frequently are cybersecurity risk assessments conducted at your organisation?	37
Q18: Are all users required to change passwords on at least a quarterly basis and instructed to use at least six characters with a combination of lowercase, uppercase, digits and symbols?....	39
Q19: Has your network been EXTERNALLY assessed/penetration tested in the past year?	40
Q20: Has your network been INTERNALLY assessed/penetration tested in the last year?	41
Q21: Do you have a data retention & destruction policy?.....	42
Q22: Are firewalls in place at all external connection points?.....	43

Q23: Do you allow remote access to your corporate network?	44
Q24: Are all connecting devices required to have anti-virus and firewall installed in accordance with your organisation's policy for updates and patching?	46
Q25: Are employees allowed to bring their own IT devices and use these on the organisation's network?.....	47
Q26: Are employees allowed to use personal USB storage devices to store workplace-related data?	48
Q27: Is sensitive data encrypted when sent outside your network?	50
Q28: Does your organisation have physical back-ups stored off-site?	51
Q29: Please estimate the number of individual records currently stored within your owned network?.....	52
Q30: Within the last 5 years, have you sustained any of the following options?	53
Q31: What is the percentage of your organisation's budget allocated to IT?	55
Q32: What is the percentage of your organisation's IT budget allocated to cybersecurity?	55
4. Conclusion	56
4.1 Survey Summary	56
4.2 Findings and recommendations based on the sample.....	58
Annex 1.....	59
Annex 2.....	60

EXECUTIVE SUMMARY

The objective of this deliverable is to map current perceptions and trends on cybersecurity in hospitals and social care providers in Europe, as means of engaging stakeholders throughout Europe to share their knowledge, practices and perspectives on cybersecurity. This investigation was carried out through an online survey conducted in March – April 2019, reaching out 1010 respondents from different European countries. The outcomes of the survey are described in detailed charts and general findings and recommendations are drawn at the concluding part of this document. These outcomes will moreover be helpful for the upcoming training and awareness raising activities planned in the project.

TABLE OF CHARTS

Chart 1: Survey respondents by country (%)	11
Chart 2: Survey respondents by the type of the organization	12
Chart 3: Survey respondents by the legal status of the organization.....	12
Chart 4: Survey respondents by their role in the organization	13
Chart 5: DPO or person in charge of Data Security per organisation	14
Chart 6: Number of staff members working with IT devices	15
Chart 7: No. of staff working with IT devices, by organization type	16
Chart 8: Relationship of the cybersecurity responsible and the organization	17
Chart 9: Outsourced cybersecurity, by number of staff members with access to IT devices	17
Chart 10: Ratio of staff responsible for cybersecurity to those who use IT devices	18
Chart 11: Ratio of staff responsible for cybersecurity in organizations with 500+ access to IT devices.....	18
Chart 12: Employee training and assessment in privacy and data security	19
Chart 13: Organizations where employees are NOT trained and assessed, by type of organization.....	19
Chart 14: Organizations where employees are NOT trained and assessed, by no. of staff with access to IT devices (% of NO).....	20
Chart 15: Organizations where employees are NOT trained and assessed in privacy and data security related matters, by country (% of NO).....	20
Chart 16: Percentage of staff trained in GDPR rules (%)	21
Chart 17: Topics of regular staff training	22
Chart 18: Education / training department in the organization	23
Chart 19: Organizations with and without an education / training department (absolute numbers)	24
Chart 20: No. of hours of mandatory cybersecurity education / training	25
Chart 21: Surveyed organizations without a mandatory cybersecurity training (% of none)	25
Chart 22: Frequency of computer use (%)	26
Chart 23: Client / patient data management frequency (% of role).....	27
Chart 24: Concerns about cybersecurity (%)	28
Chart 25: Concerns about cybersecurity (% of organization type)	29
Chart 26: Awareness of the potential cybersecurity attack impacts (%).....	30
Chart 27: Awareness of the potential cybersecurity attack impacts (% of organization type)	31
Chart 28: Importance of cybersecurity for the organization	32
Chart 29: Importance of cybersecurity for the organization	32
Chart 30: Interactions with the IT department.....	33
Chart 31: Interactions with the IT department by organisation type.....	34
Chart 32: Interactions with the IT department by the role in the organization	34
Chart 33: Means of addressing cybersecurity concerns	35
Chart 34: Means of addressing cybersecurity concerns (% of I SOLVE IT ON MY OWN)	35
Chart 35: Means of addressing cybersecurity concerns (% of I CHECK ON THE INTERNET)	36
Chart 36: Frequency of cybersecurity risk assessment	37
Chart 37: Frequency of cybersecurity risk assessment (% of DO NOT KNOW)	37
Chart 38: Frequency of cybersecurity risk assessment by organisation	38
Chart 39: Users requested to change their password quarterly and use strong combinations	39
Chart 40: Users requested to change their password quarterly and use strong combinations, by organisation type	39
Chart 41: Organization externally assessed / penetration tested in the past year	40
Chart 42: Organization externally assessed / penetration tested in the past year (% of YES)	40
Chart 43: Organization internally assessed / penetration tested in the past year (%).....	41
Chart 44: Organization internally assessed / penetration tested in the past year (% of YES).....	41

<i>Chart 45: Data retention & destruction policy in place in the organization</i>	42
<i>Chart 46: Data retention & destruction policy in place in the organization (% DO NOT KNOW)</i>	42
<i>Chart 47: Firewalls in place at all external connection points</i>	43
<i>Chart 48: Firewalls in place at all external connection points (% of DO NOT KNOW)</i>	43
<i>Chart 49: Remote access to corporate network (%)</i>	44
<i>Chart 50: Remote access to corporate network by organization type</i>	45
<i>Chart 51: Devices required to have anti-virus and firewall installed in accordance with your organisation's policy for updates and patching</i>	46
<i>Chart 52: Devices required to have anti-virus and firewall installed in accordance with your organisation's policy for updates and patching (% of do not know)</i>	46
<i>Chart 53: Employees allowed to bring their own IT devices and use these on the organisation's network (%)</i> ...	47
<i>Chart 54: Employees allowed to use personal USB storage devices to store workplace-related data</i>	48
<i>Chart 55: Employees allowed to use personal USB storage devices to store workplace-related data by organization type</i>	49
<i>Chart 56: Sensitive data encrypted when sent outside your network</i>	50
<i>Chart 57: Physical back-ups stored off-site</i>	51
<i>Chart 58: Individual records currently stored within your owned network</i>	52
<i>Chart 59: Individual records currently stored within your owned network (% of 100 001 – 1 000 000)</i>	52
<i>Chart 60: Cybersecurity incidents in the last 5 years</i>	53
<i>Chart 61: Virus or malicious code attack by organization type</i>	53
<i>Chart 62: Virus or malicious code attack by organization type</i>	54
<i>Chart 63: Number of incident types vs number of organizations</i>	54
<i>Chart 64: Percentage of budget allocated to IT</i>	55
<i>Chart 65: Percentage of IT budget allocated to cybersecurity</i>	55

1. Introduction

The objective of this deliverable is to map current perceptions and trends on cybersecurity in hospitals and social care providers in Europe via the on-line survey. This survey provides insight into what healthcare and social care providers and organizations are doing to protect their information and assets.

Based on the feedback from 101 healthcare and social care providers and organizations, an analysis of the findings yielded a few notable themes, which could be explored further in the following activities of the project.

The participating organizations nominated qualified respondents – mostly managers, data protection officers or IT staff, all in direct contact with cybersecurity issues of the organization. We believe that the data collected is valid and highly representative of the organization types – health care and social care providers.

The findings are summarized at the end of this analysis, and in brief indicate that cybersecurity is reflected in everyday activities not only through large data sets, the presence of IT devices and IT staff, but also through direct experience of most participants with cybersecurity incidents.

The sample also shows that the health care providers – mostly large hospitals – are a step ahead compared to the social services providers in terms of cybersecurity awareness and understanding of damaging impact of security breaches, be it internal or external.

The survey also indicates that cybersecurity is underbudgeted across the organizations and there is still a lot of potential in the external and internal trainings for IT and non-IT staff.

Lastly, cybersecurity is an ongoing and fluid effort, as new risks and threads emerge relative to the exponential growth and reach of the technology, processing and innovative approaches, such as artificial intelligence.

Thus, it needs to become an integral part of the organizational culture, strategic and policy documents, and the staff needs to be reminded constantly that modern health care and social care requires aggregation of large amounts of very sensitive data to provide the best possible treatments, and this data needs to be well managed and strictly protected.

The full survey is annexed to this deliverable.

2. Methodology and Demographics of the respondents

The survey questions were prepared in cooperation with all project partners, and the survey was active online for a period of one month with the aim of reaching at least 100 responses.

Start of the survey	: March 20, 2019
Closing of the survey	: April 20, 2019
Evaluation and report	: April 21 – April 30, 2019
Comments and review	: Mai 1 – May 9, 2019

The information page at the opening of the survey presented that it was being held under the framework of the SecureHospitals.eu project, referencing to EU funding and the survey aims:

*'This questionnaire is being conducted under the framework of the **SecureHospitals.eu** project, a **Coordination and Support Action** funded by the European Commission's H2020 programme under grant agreement no. 826497 and implemented by 12 partners constituting the research team.*

*The aim of the questionnaire is to acquire a general understanding on the perceptions of healthcare professionals and IT staff on cybersecurity issues with a focus on awareness, training and protection measures. Following this assessment and other research activities, the project will develop tailor-made training packages and offer training sessions for multiple types of stakeholders in different European countries.'*¹

Findings from the SecureHospitals.eu online survey are based on the feedback from 101 respondents from a variety of European healthcare organisations and social care providers and organizations.

Survey participants included SecureHospitals.eu project partners organisations and their members and other stakeholders. The survey was distributed uniformly through the partner networks, its completion and submission were voluntary and at the discretion of the respondent organizations.

Respondents generally identified themselves by a country as either representatives of health care organisation (hospitals, umbrella organizations) or social care providers (nursing homes, home care) or others (insurance companies).

As displayed in Chart 1, most respondents are based in 3 countries – Belgium (25 respondents), Spain (20 respondents) and the Czech Republic (20 respondents), followed by Italy, Austria and the Netherlands (all over 5 respondents). Three respondents did not indicate their country of origin. Given that these countries represent those of the consortium partners,

¹ The full content of the information sheet can be found in Annex 1.

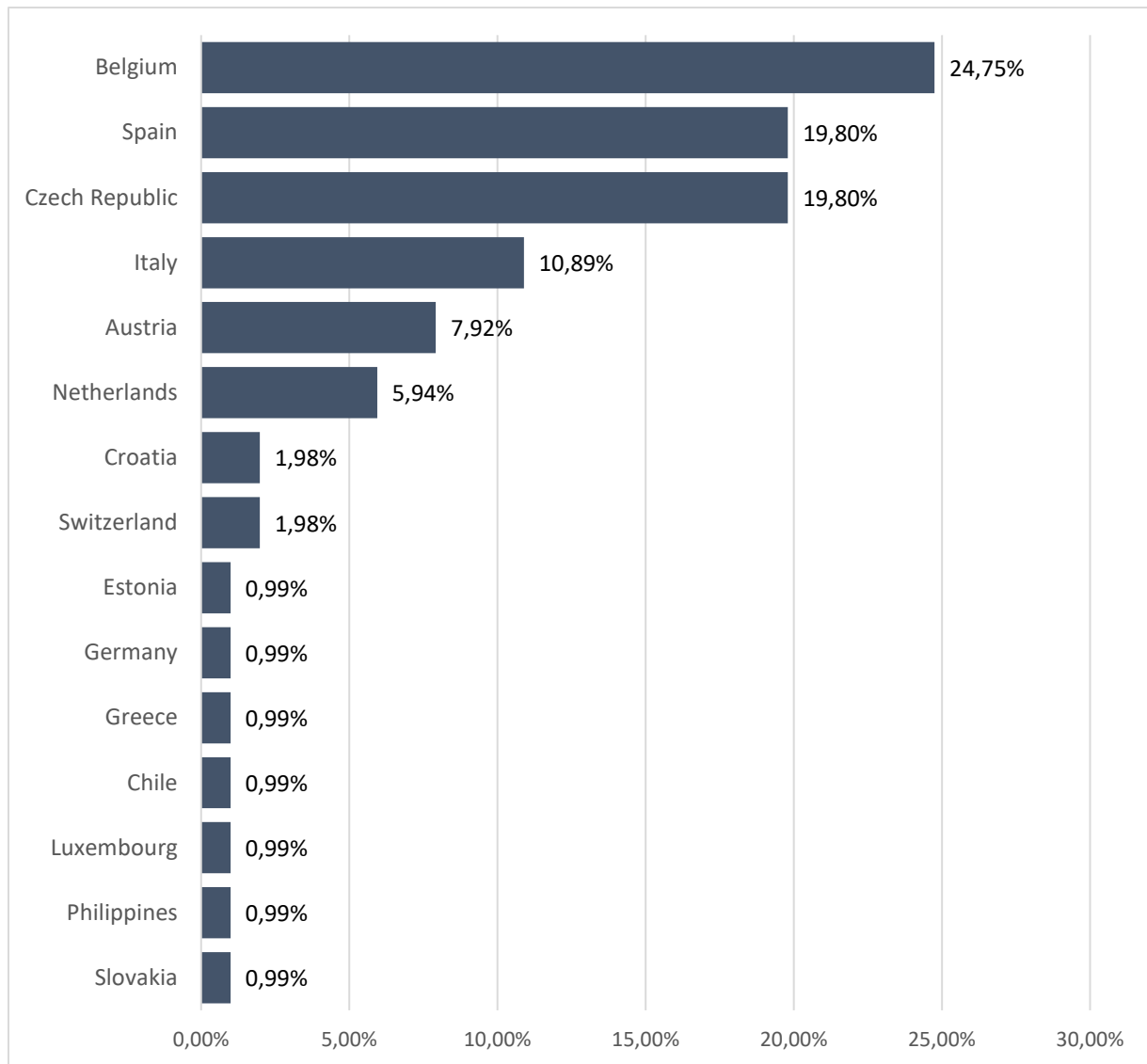


Chart 1: Survey respondents by country (%)

The survey includes respondents from health care and social care providers, as well as service organizations in the sector. The project was initially limited to the health care providers. The European Ageing Network as one of the project partners enabled the extension to the social care sector. The social care providers have been further surveyed in finer detail.

As expected, almost two thirds of respondents are hospitals (Chart 2) – 63 organizations. Almost 16 % (16 organizations) of the survey participants are nursing homes providing care to the elderly. These respondents.

A closer look at the “Other” group reveals 9 mostly service oriented organizations, such as research centres, IT service providers, consulting services, and in one case a nursing home combining elderly and other care.

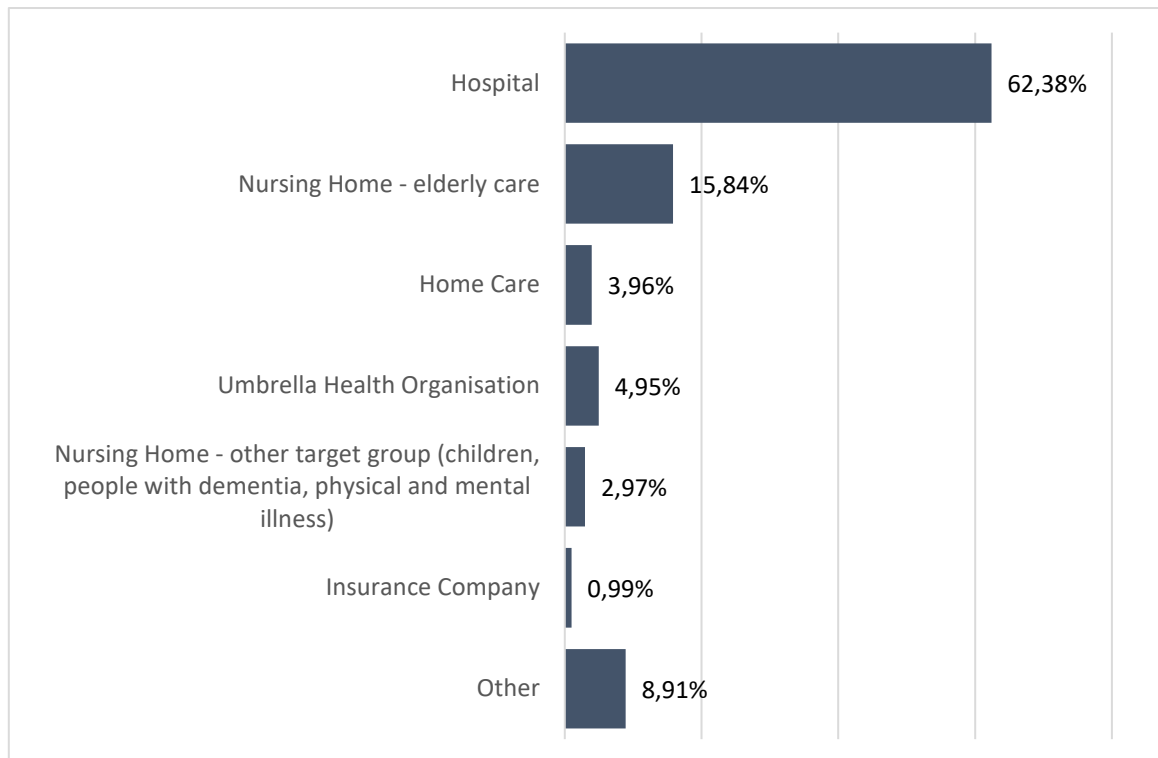


Chart 2: Survey respondents by the type of the organization

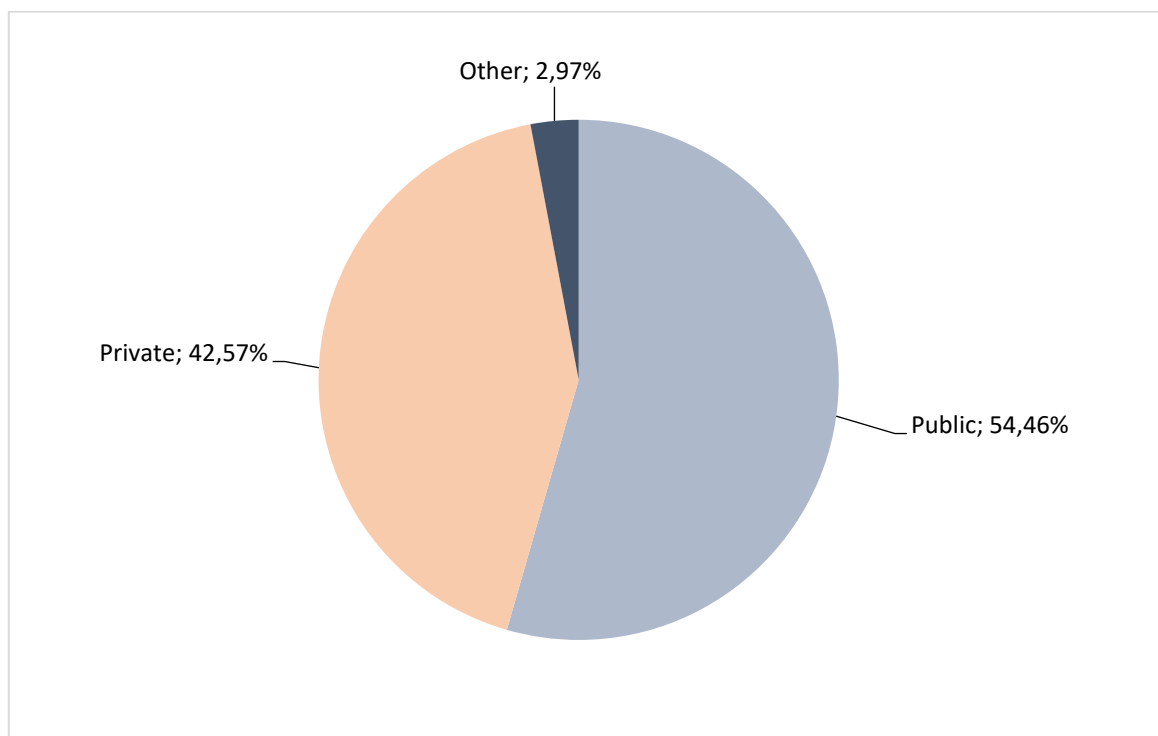


Chart 3: Survey respondents by the legal status of the organization

Over 54 % of the respondents are public organizations, 42,6 % are private entities (Chart 3). As the General Data Protection Regulation is equally applicable to all public and private entities active within the European Union, the query regarding the legal status was included in the survey mostly to provide a further insight into the structure and the representativeness of the participating sample.

Respondents also identified themselves by their role in the organization (**Chart 4**). 75 % of the respondents (management, DPOs, IT specialists) are expected to deal with cybersecurity of the organization daily and are therefore well informed to provide valid answers.

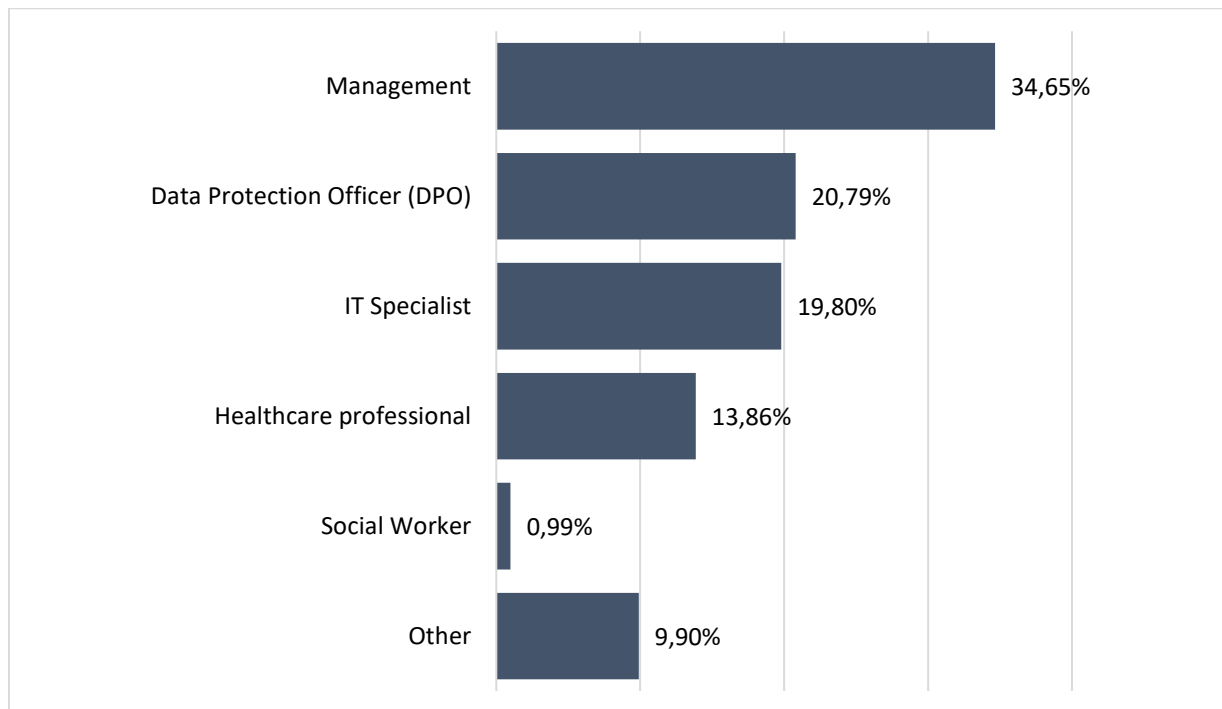


Chart 4: Survey respondents by their role in the organization

The demographics of the survey participants in terms of the type of the organization give a solid base for the collection of relevant information regarding cybersecurity. The nature of the partner networks defines the somewhat limited geographic distribution; however, we still consider the collected sample as valid and representative.

3. Findings

This section presents the finding of the survey, divided into two main query sections: 1) Staff Training and Awareness and 2) Risk Assessment. Each of the sections presents the response graphs and discusses the findings.

3.1 Staff Training and Awareness

This section was composed of X questions. Each of the questions and respective findings are presented below:

Q1: Do you have a Data Protection Officer or someone in charge of Data Security at your organization?

All organizations that systematically process large amounts of data are obliged to have the Data Protection Officer (DPO). 88 % confirm (Chart 5) the existence of the DPO in the organization.

5 respondents answered DO NOT KNOW, these are almost entirely health care professionals.

7 respondents answered NO – 6 of them managers and IT specialists in nursing homes. We can only assume that they interpreted the question as having an internal DPO, while they are using external services.

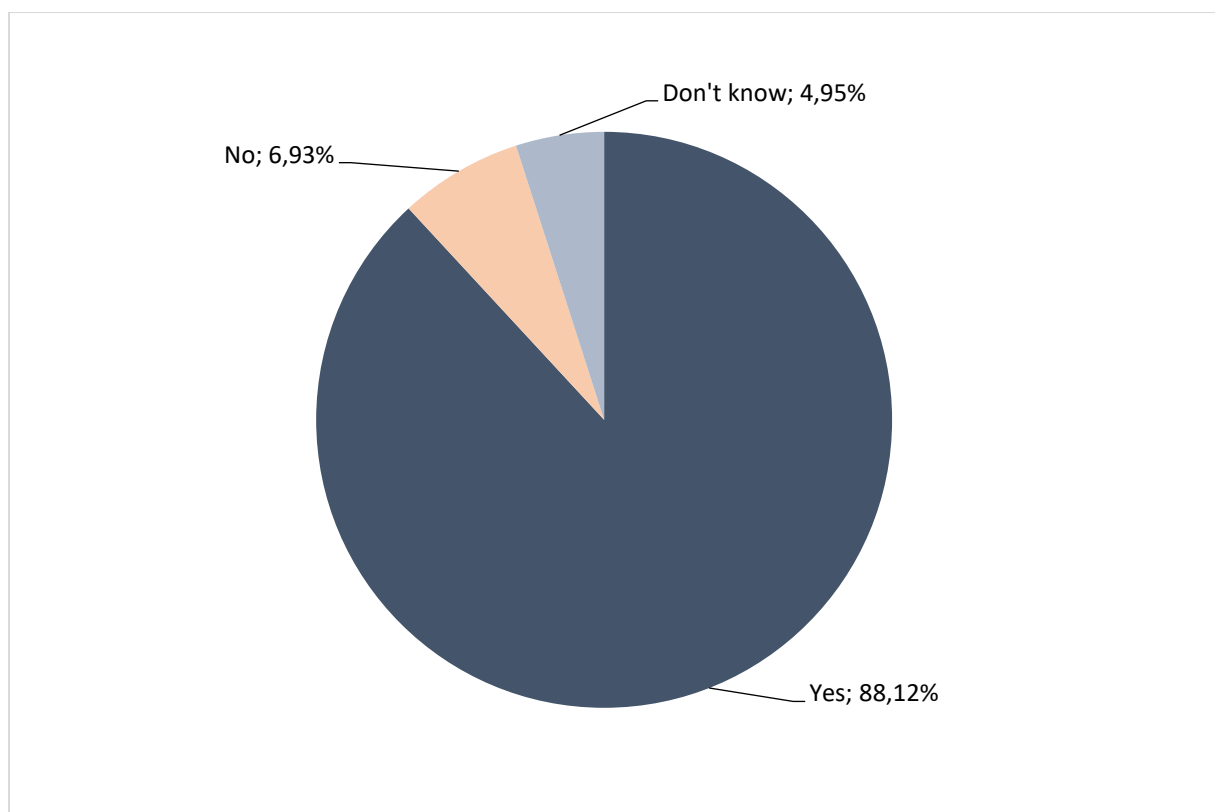


Chart 5: DPO or person in charge of Data Security per organisation

Q2: What is the number of staff members working at your organisation who use IT devices?

This query offered the respondent to choose from 3 defined ranges (1-100, 100-500 and 500+). Almost a half of the respondents (**Chart 6**) are large organizations with a substantial number of persons with a regular access to IT devices.

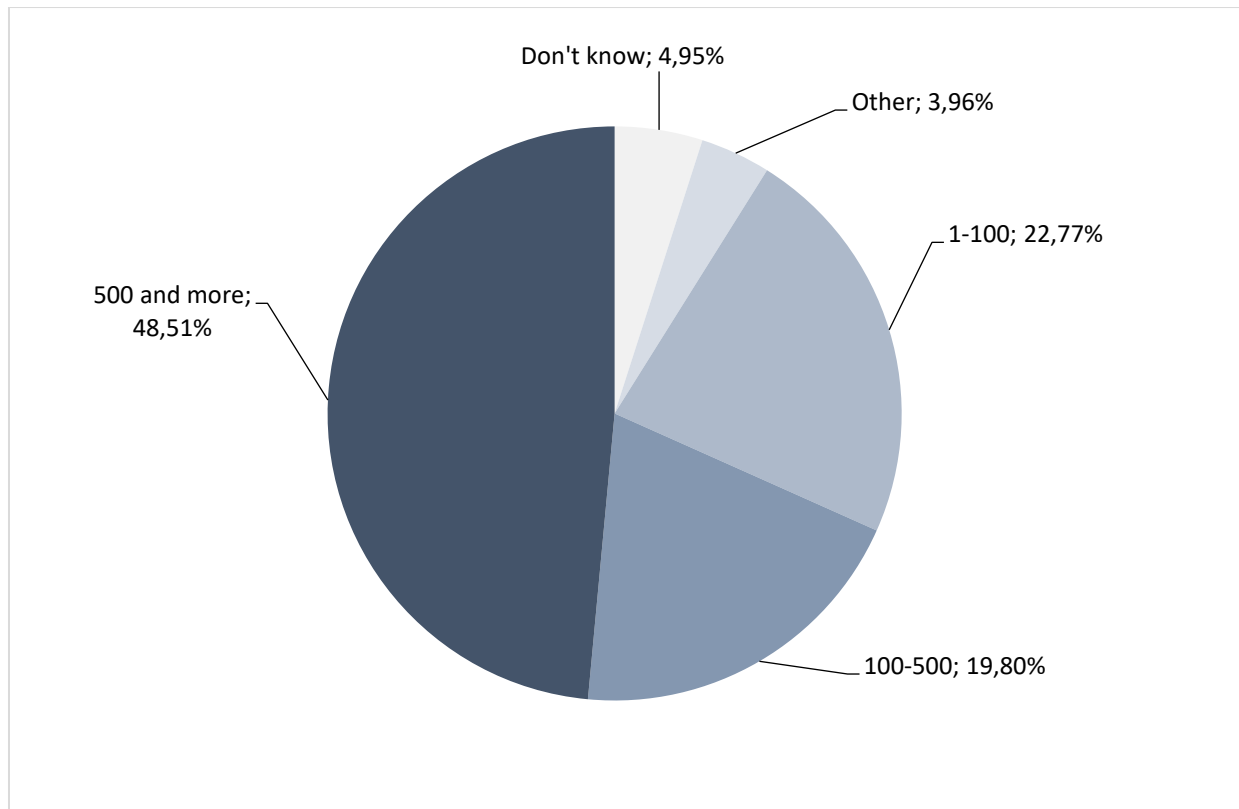


Chart 6: Number of staff members working with IT devices

A closer look at the structure of the individual ranges (**Chart 7**) shows, as expected, that these large organizations with a substantial number of staff members accessing IT devices, are mostly hospitals. Social care providers are mostly represented in the ranges 1-100 and 100-500 ranges.

The answer OTHER reveals 4 hospitals with over 2 000 persons (2 000, 3 000, 3 000, 7 500) accessing IT devices.

43 out of 101 respondents are therefore large hospitals with more than 500 employees with regular access to IT devices.

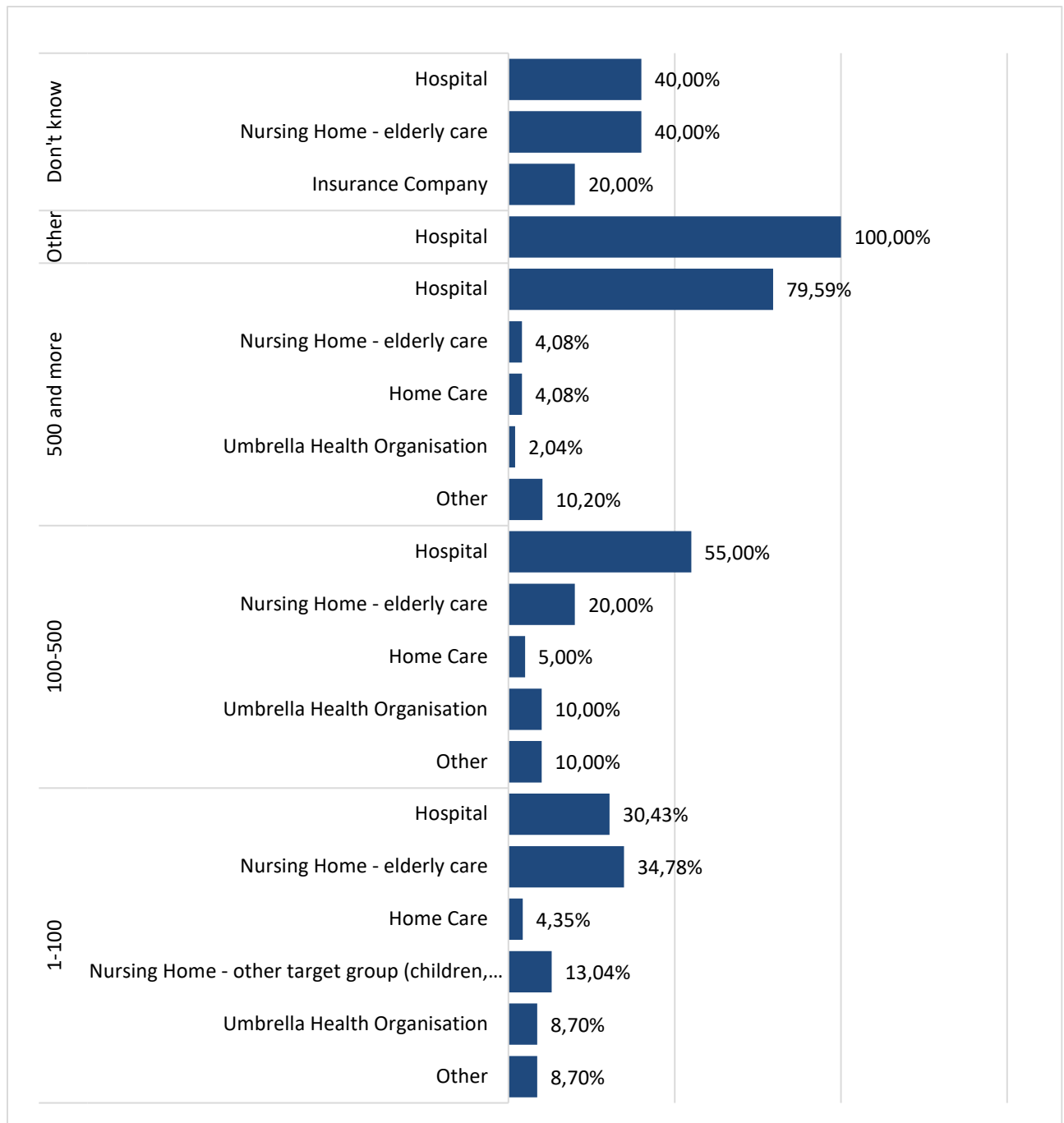


Chart 7: No. of staff working with IT devices, by organization type

Q3: How is the relation of the cybersecurity responsible in your organisation?

The query is examining the relationship of the subject responsible for the cybersecurity and the organization. Almost 70 % of the organizations (**Chart 8**) choose to delegate the responsibility to their employees. 17.8 % of organizations outsource cybersecurity, almost two thirds are smaller organizations with 1-100 persons with access to IT devices (**Chart 9**).

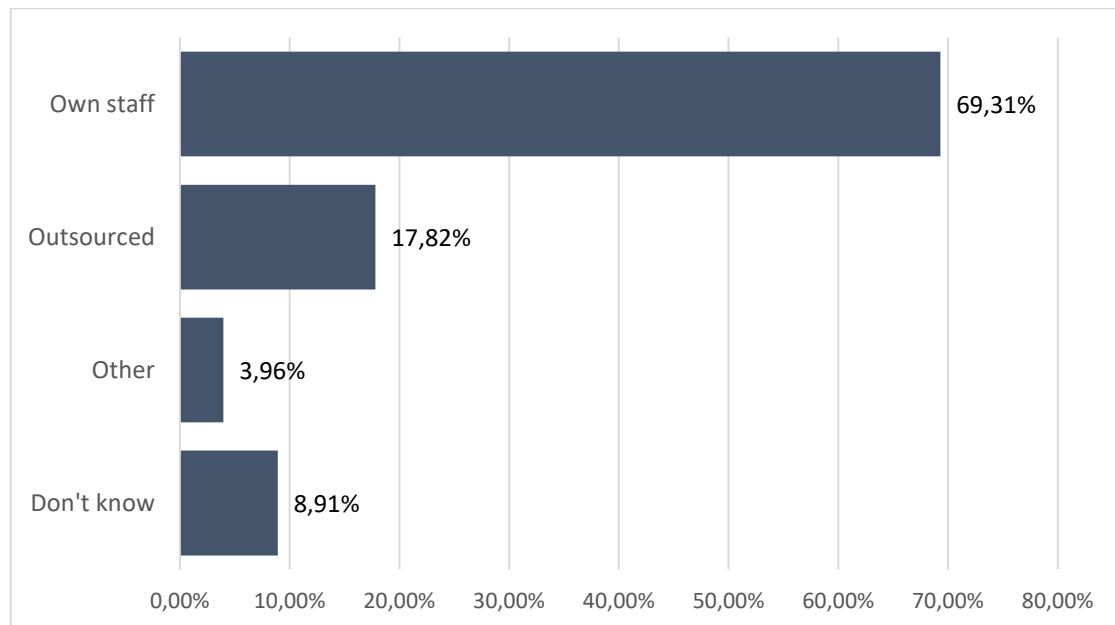


Chart 8: Relationship of the cybersecurity responsible and the organization

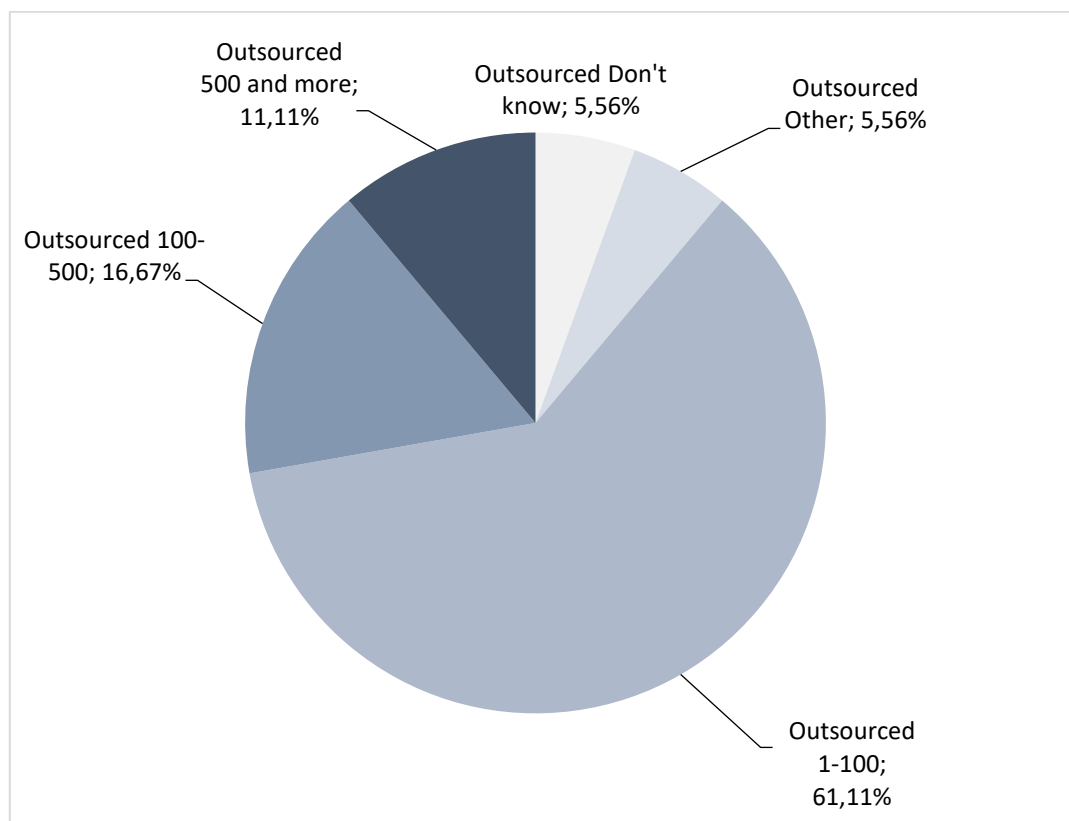


Chart 9: Outsourced cybersecurity, by number of staff members with access to IT devices

Q4: What is the ratio of staff responsible for cybersecurity to those who use IT devices at your organisation?

This query examines the relationship of the number of people with access to IT devices to the number of persons responsible for the cybersecurity in the organization. Chart 10 needs to be look at in context with Chart 6. It is obvious that the average number of people responsible for cybersecurity in an individual organization in the sample is 1-2, even though almost half of the organizations allow IT access to 500+ persons. This is further confirmed in **Chart 11** – almost 74 % of organizations with 500+ persons with IT access basically employ only 1 person in the domain of cybersecurity.

A half of the DO NOT KNOW answers were given by the health professionals, probably without the perspective needed to provide the answer. The remaining answers were given by the managers, DPOs or IT staff – it may be that in that 10 % of organizations the cybersecurity procedures, processes and responsibilities are not set or distributed properly.

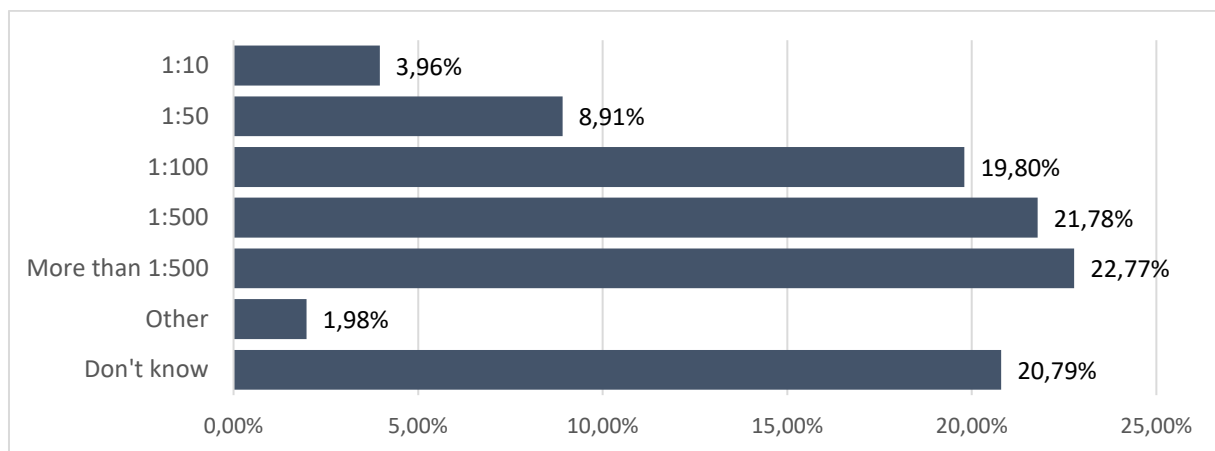


Chart 10: Ratio of staff responsible for cybersecurity to those who use IT devices

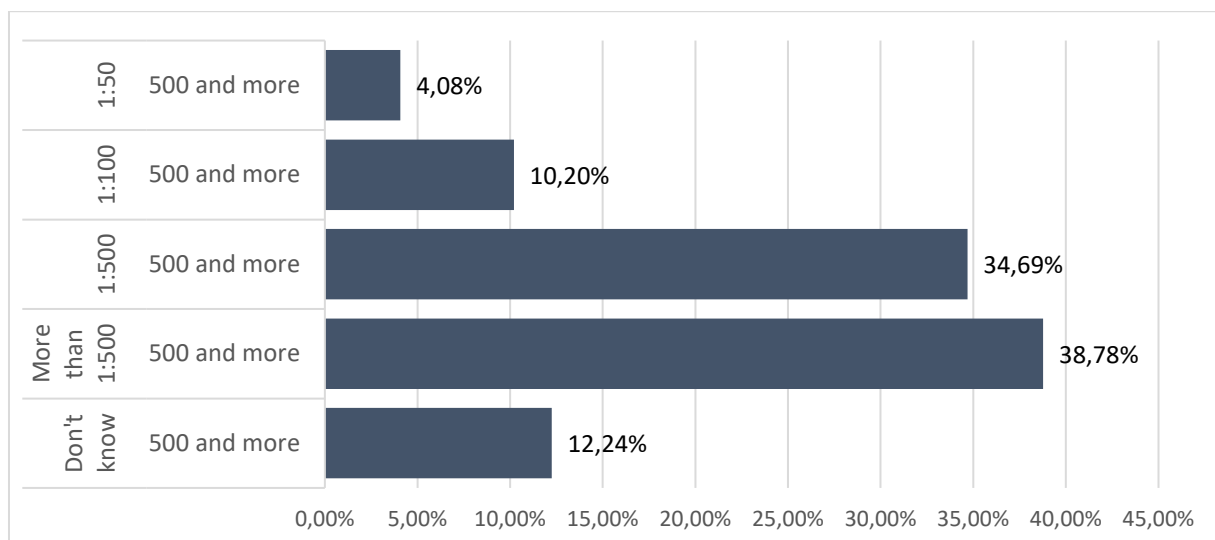


Chart 11: Ratio of staff responsible for cybersecurity in organizations with 500+ access to IT devices

Q5: Are all employees trained and assessed in privacy and data security related matters (such as phishing, identity theft, social media and mobile devices) on at least an annual basis?

This query gives a rather surprising result (**Chart 12**) – 57.4 % of respondents state that staff in their organization is not trained in basic cybersecurity measures. As further elaborated in charts 13, 14 and 15, these are mostly hospitals (62 %), logically therefore organizations with 500+ persons accessing IT devices (46.6 %), and interestingly, located in Belgium (31 %), Spain (20.7 %).

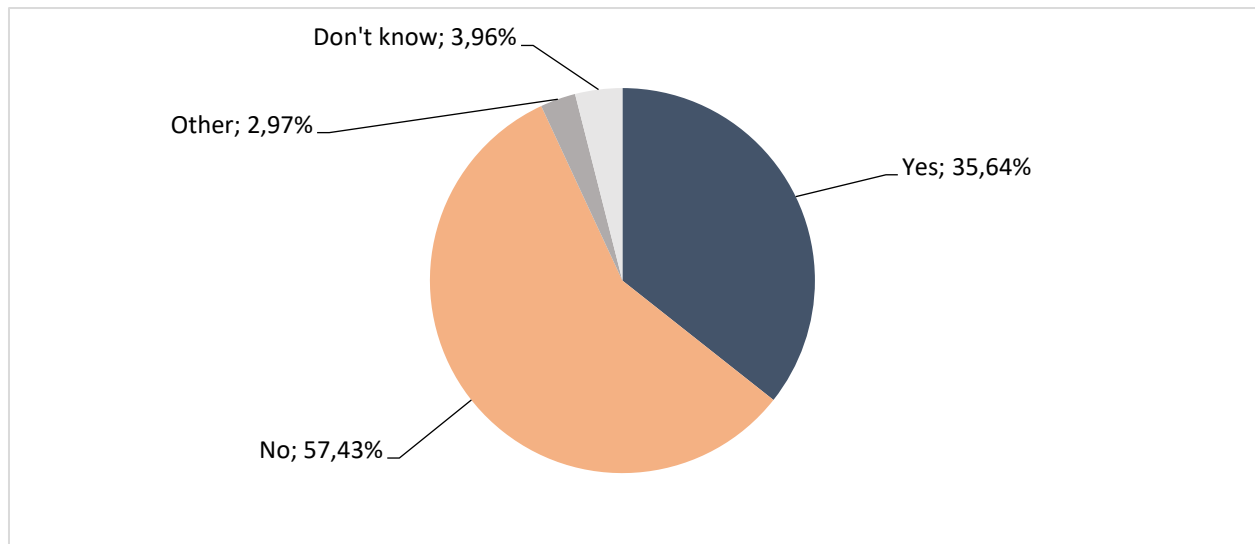


Chart 12: Employee training and assessment in privacy and data security

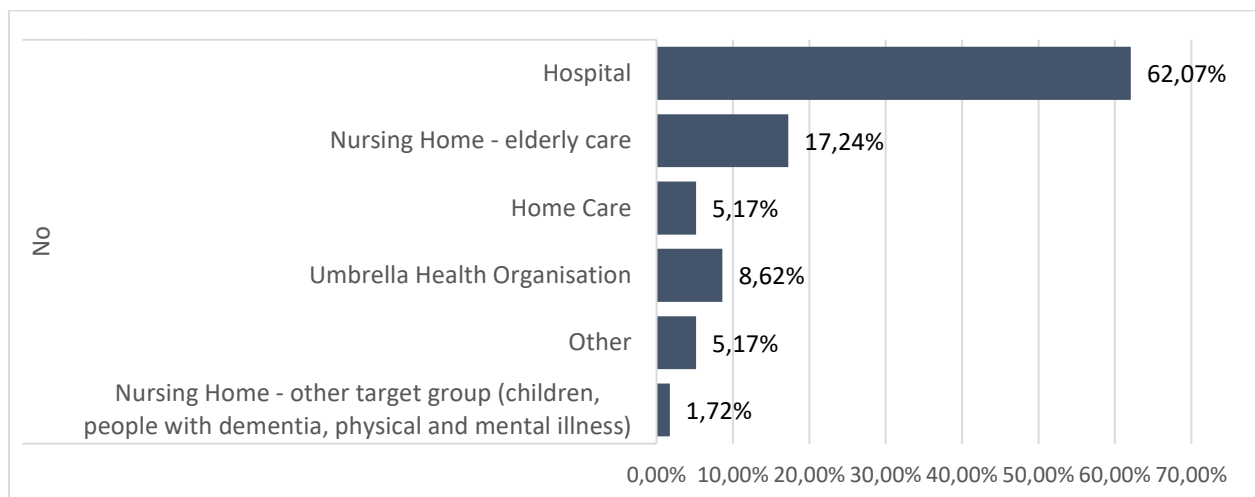


Chart 13: Organizations where employees are NOT trained and assessed, by type of organization

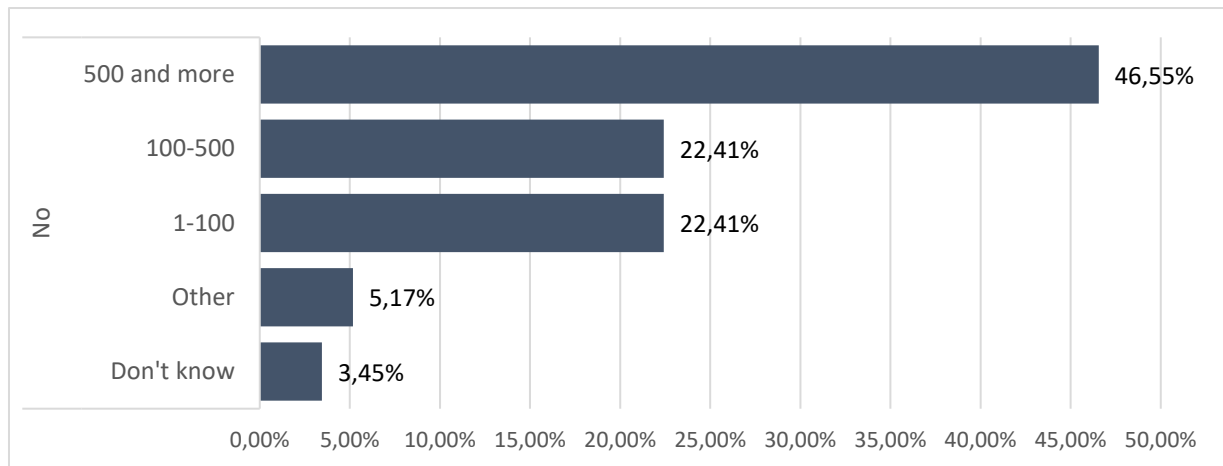


Chart 14: Organizations where employees are NOT trained and assessed, by no. of staff with access to IT devices (% of NO)

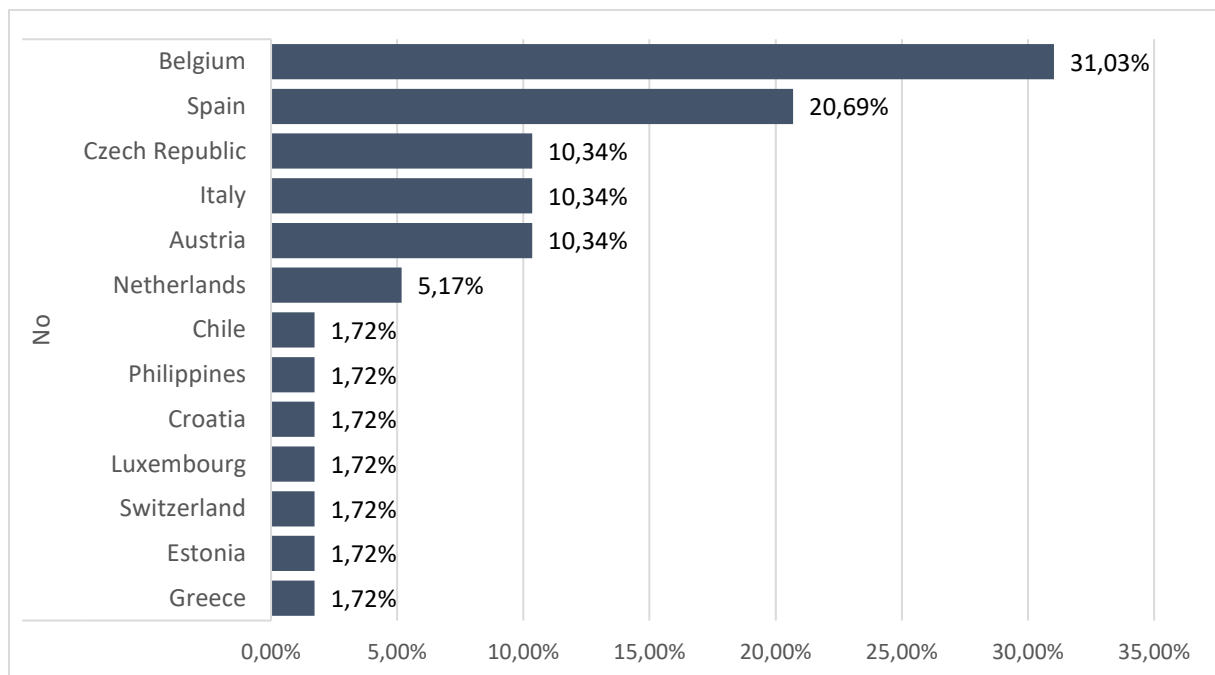


Chart 15: Organizations where employees are NOT trained and assessed in privacy and data security related matters, by country (% of NO)

The results indicate that a regular cybersecurity minimum training, especially in large health care organizations is an important security measure.

Q6: What is the percentage of your staff trained in GDPR rules?

While the survey did not further specify the extent of the training, it is rather surprising that 48.5 % of the participating organizations have less than half of the staff trained, with a significant number of organizations (21.8 %) with less than 5 % of staff trained (**Chart 16**). The answer DO NOT KNOW was given by the health professionals in the most part (59 % of the answers).

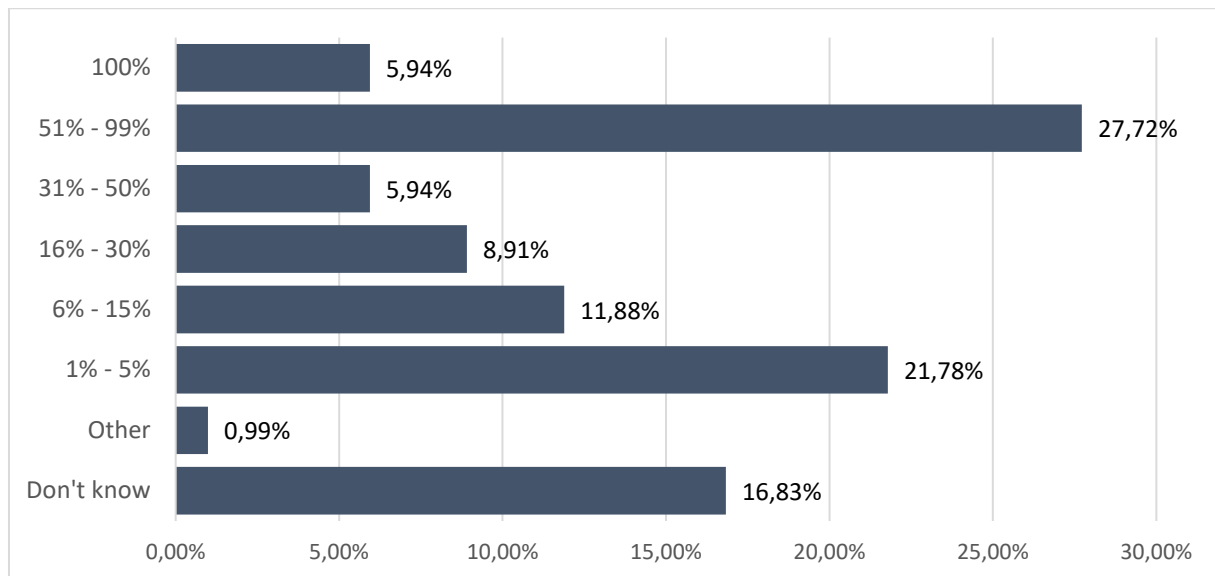


Chart 16: Percentage of staff trained in GDPR rules (%)

This clearly shows that while the GDPR is being enforced, the real acceptance process is slow and not perceived as critical. The changes will accelerate once they start being accepted not as rules and restrictions but as necessary and practical measures.

The lead should be taken by the role models – persons that have the capacity to initiate the changes and influence others.

Q7: In which topics is the staff of your organisation regularly trained?

This was a multiple-choice query – more answers could be selected. As demonstrated in the **Chart 17**, organizations mostly train staff in the more traditional policies – Clean desk policy, Data management, Removable media, Physical Security and Environmental Controls and Email Scams.

The newer risks and policies are promoted less.

It is obvious that there is still lack of sufficient training that would reflect the variety of potential everyday cyber-risks.

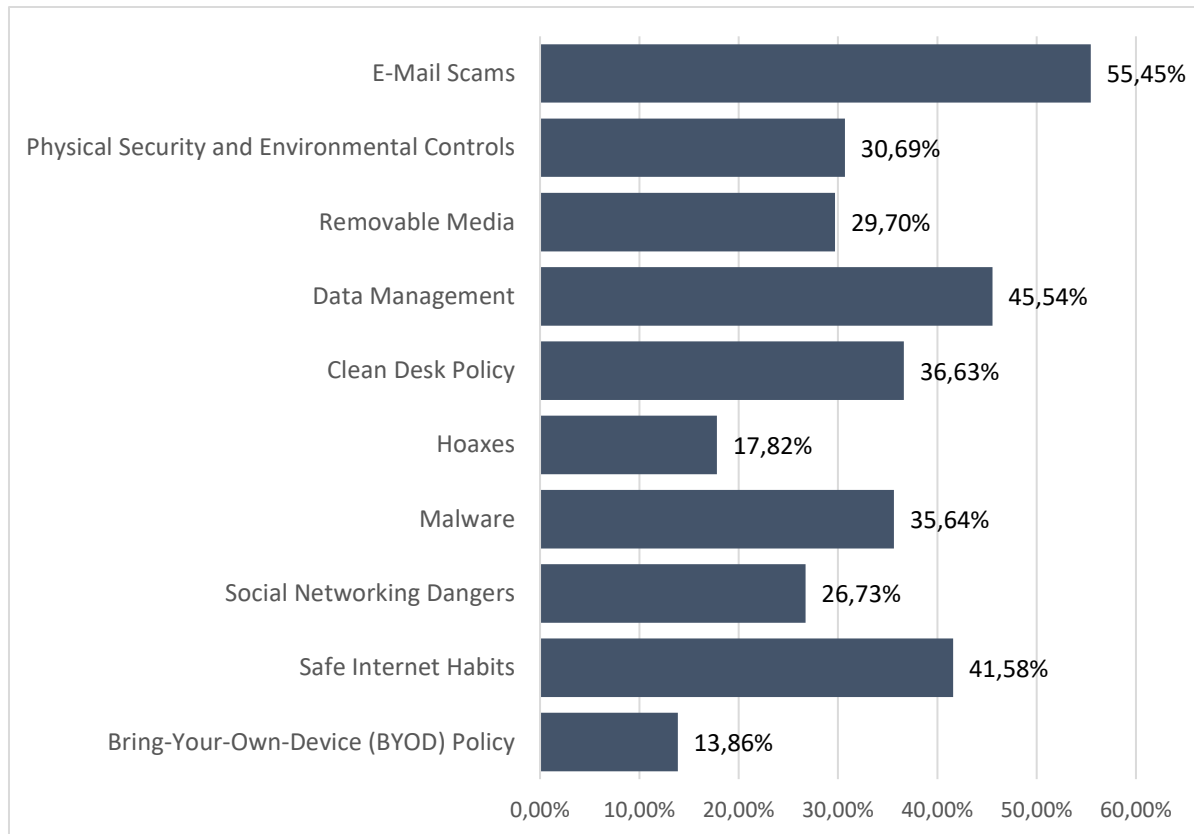


Chart 17: Topics of regular staff training

Q8: Does your organisation have an education/training department?

As show in **Chart 18**, there are training departments in almost two thirds of the surveyed organizations. The cybersecurity appears not to be a priority of those training departments in light of the results of the previous 3 queries.

The clear advantage is that the basic infrastructure for an improved cybersecurity is in place in the majority of the participating organizations.

In terms of the structure of organizations without training departments in the surveyed sample (**Chart 19**) – these are mostly hospitals (20 organizations).

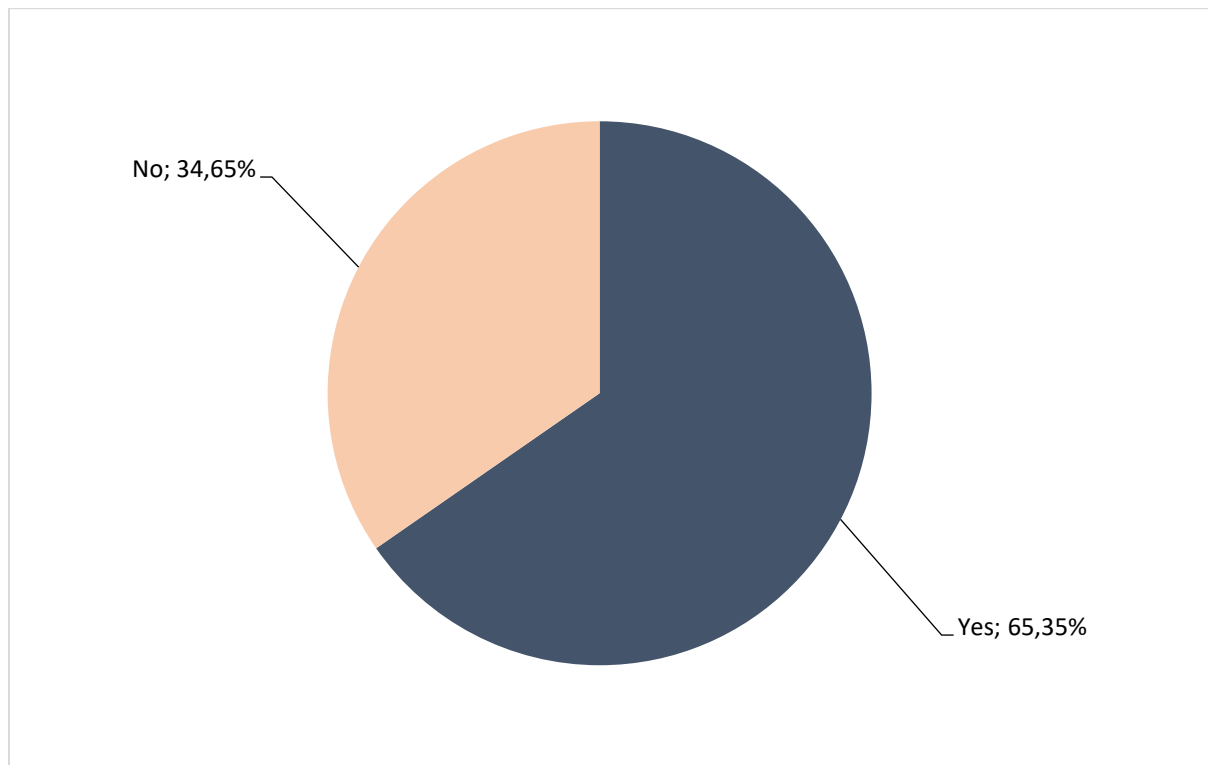


Chart 18: Education / training department in the organization

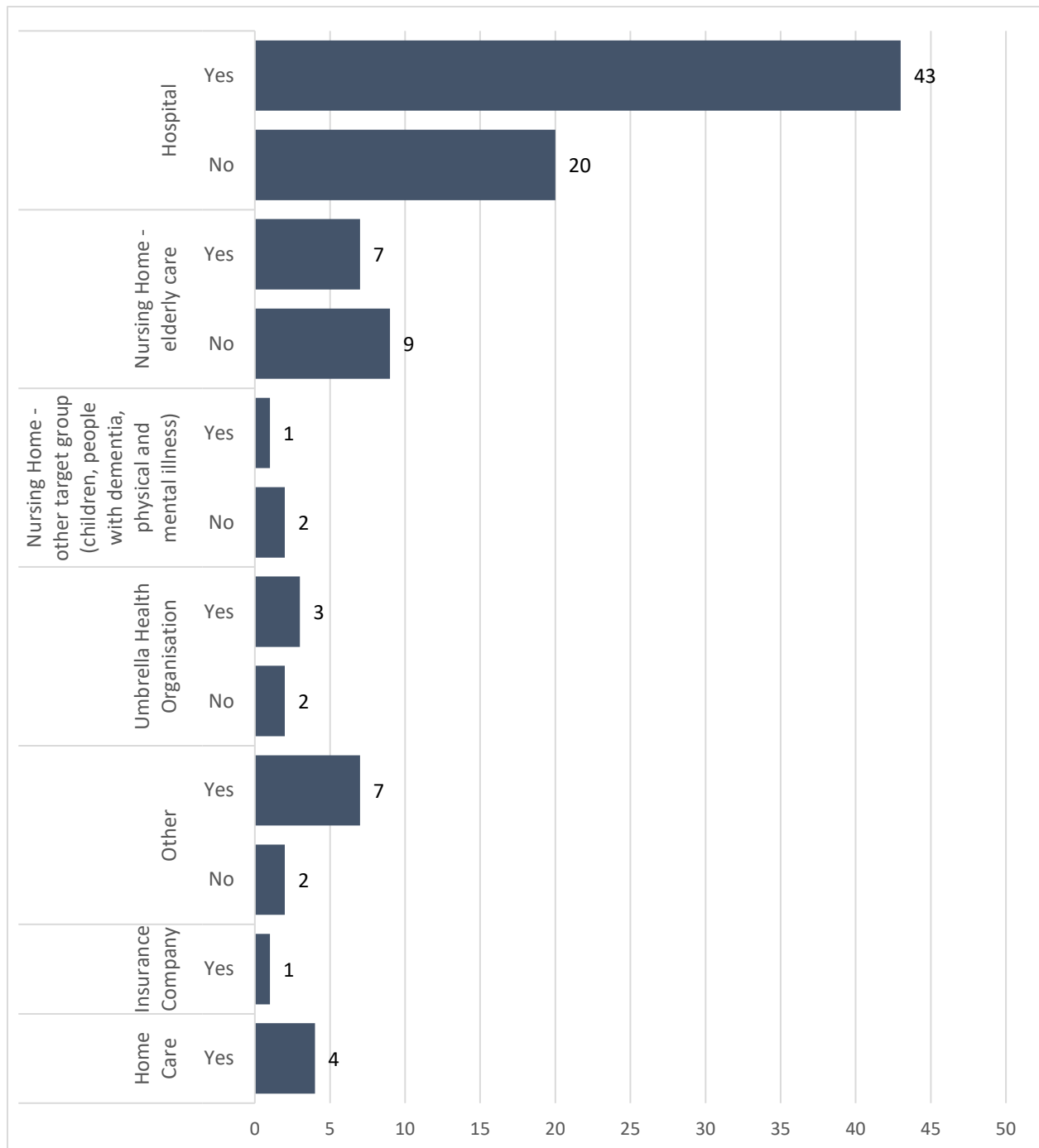


Chart 19: Organizations with and without an education / training department (absolute numbers)

Q9: How many hours of education/training in cybersecurity are mandatory at your organisation?

Chart 20 demonstrates again that the cybersecurity training is not a high priority for the organizations. Over half of the survey participants do not require that their staff complete a mandatory cybersecurity training. Looking further into the survey data, over 60 % of the organizations that have NO mandatory cybersecurity training are hospitals.

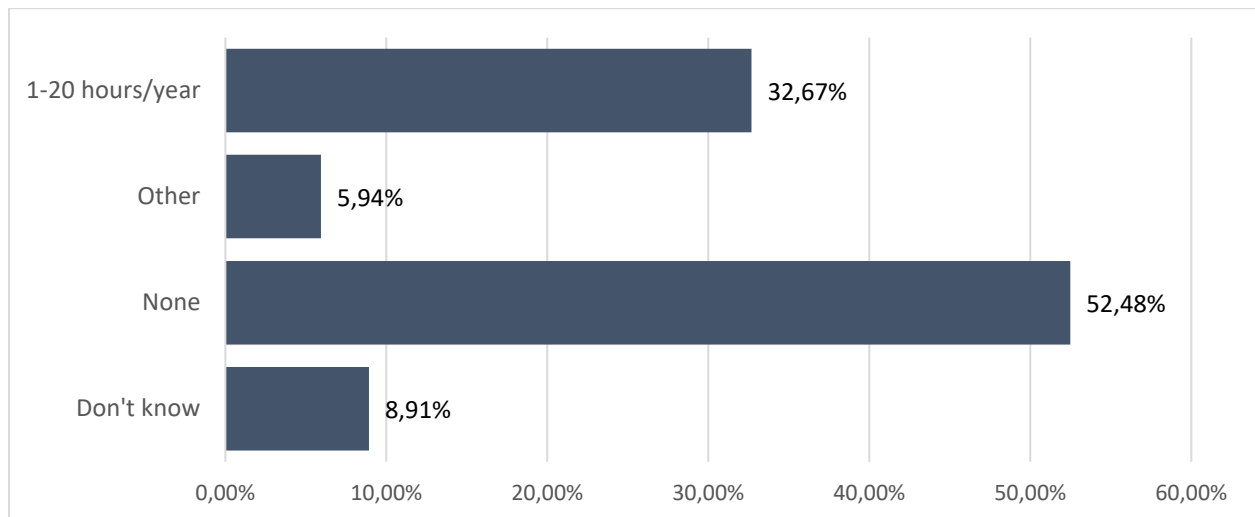


Chart 20: No. of hours of mandatory cybersecurity education / training

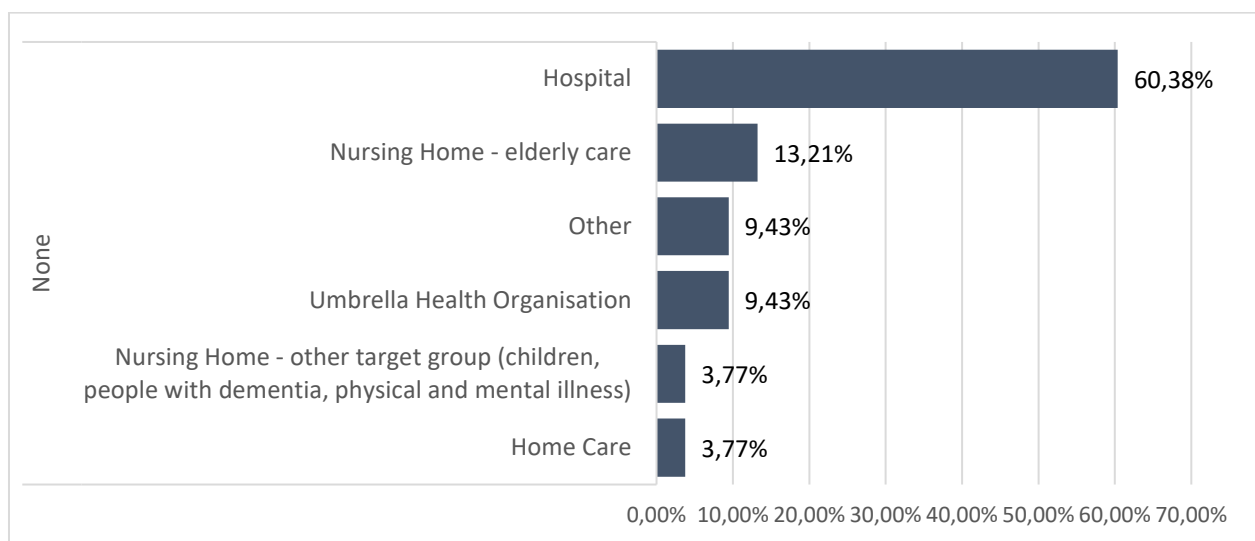


Chart 21: Surveyed organizations without a mandatory cybersecurity training (% of none)

3.2 Risk Assessment

Q10: How often do you use a computer?

This question is targeting directly the person responding to the survey, and given the structure shown in the Chart 4, it is expected that the respondents access their computer daily, or multiple times per day **Chart 22** shows the structure of answers for each type of an organization.

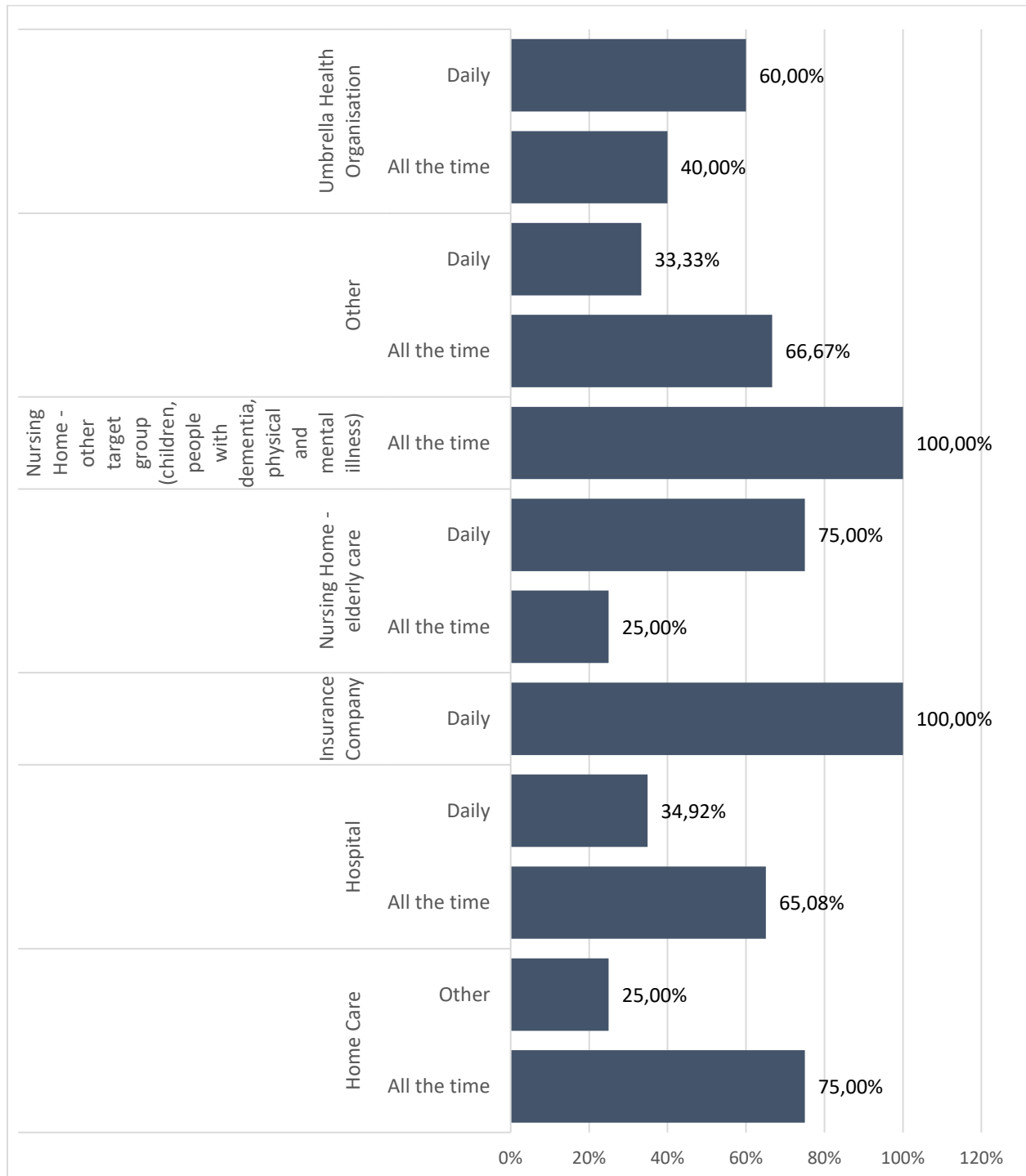


Chart 22: Frequency of computer use (%)

Q11: How often do you manage personal data (i.e. of patient, clients)?

Chart 23 gives an overview of the frequency of access to patient / client data by the respondents. This chart only reflects the answers of the individual participants. It however provides a good insight into the fact that the data is accessed by a wide range of users – from managers, through IT specialists, DPOs to health and social work professionals, in general on a daily or weekly basis.

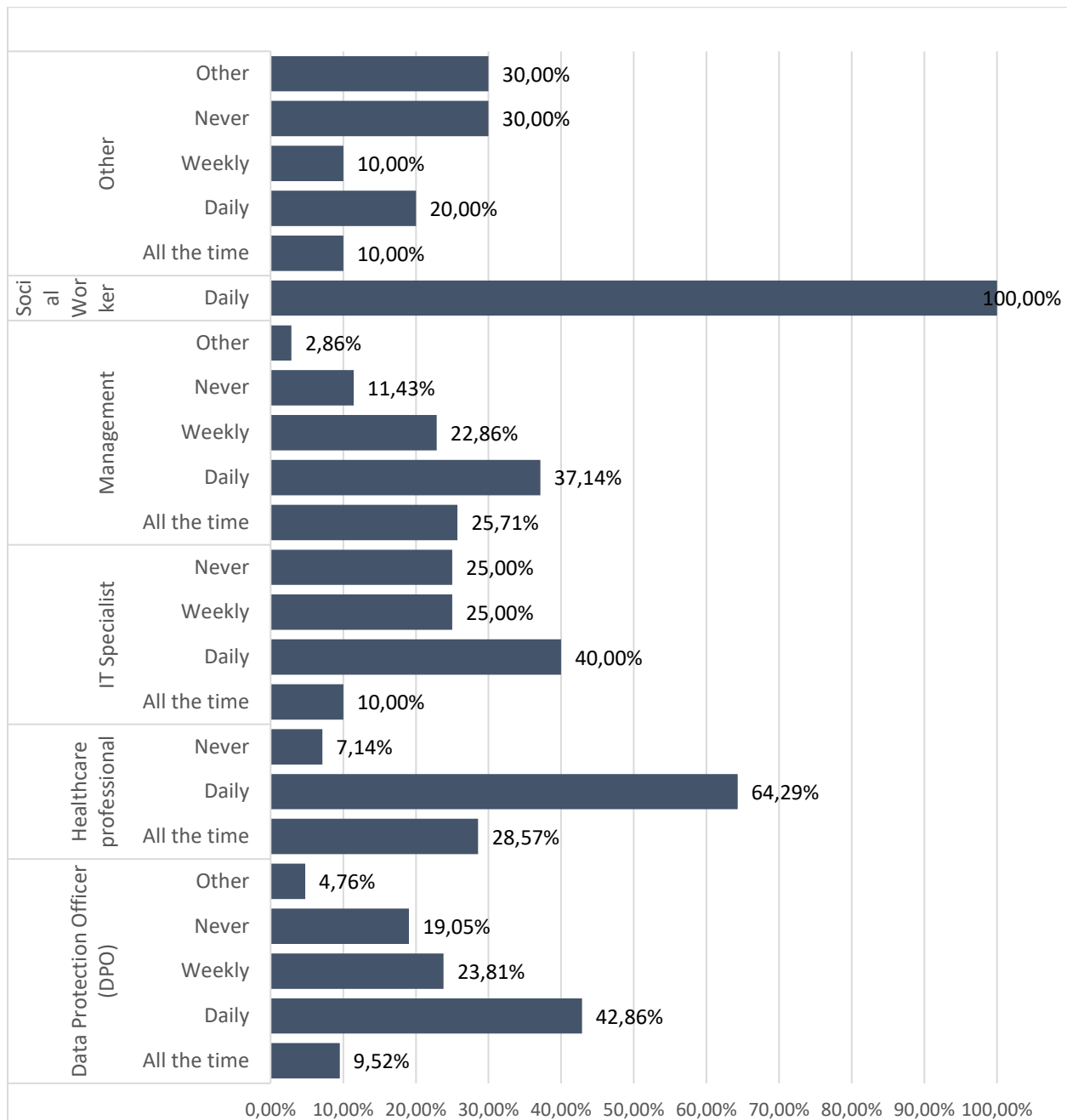


Chart 23: Client / patient data management frequency (% of role)

Q12: Are you concerned about cybersecurity?

Most of the respondents are concerned about cybersecurity – 83 % (**Chart 24**).

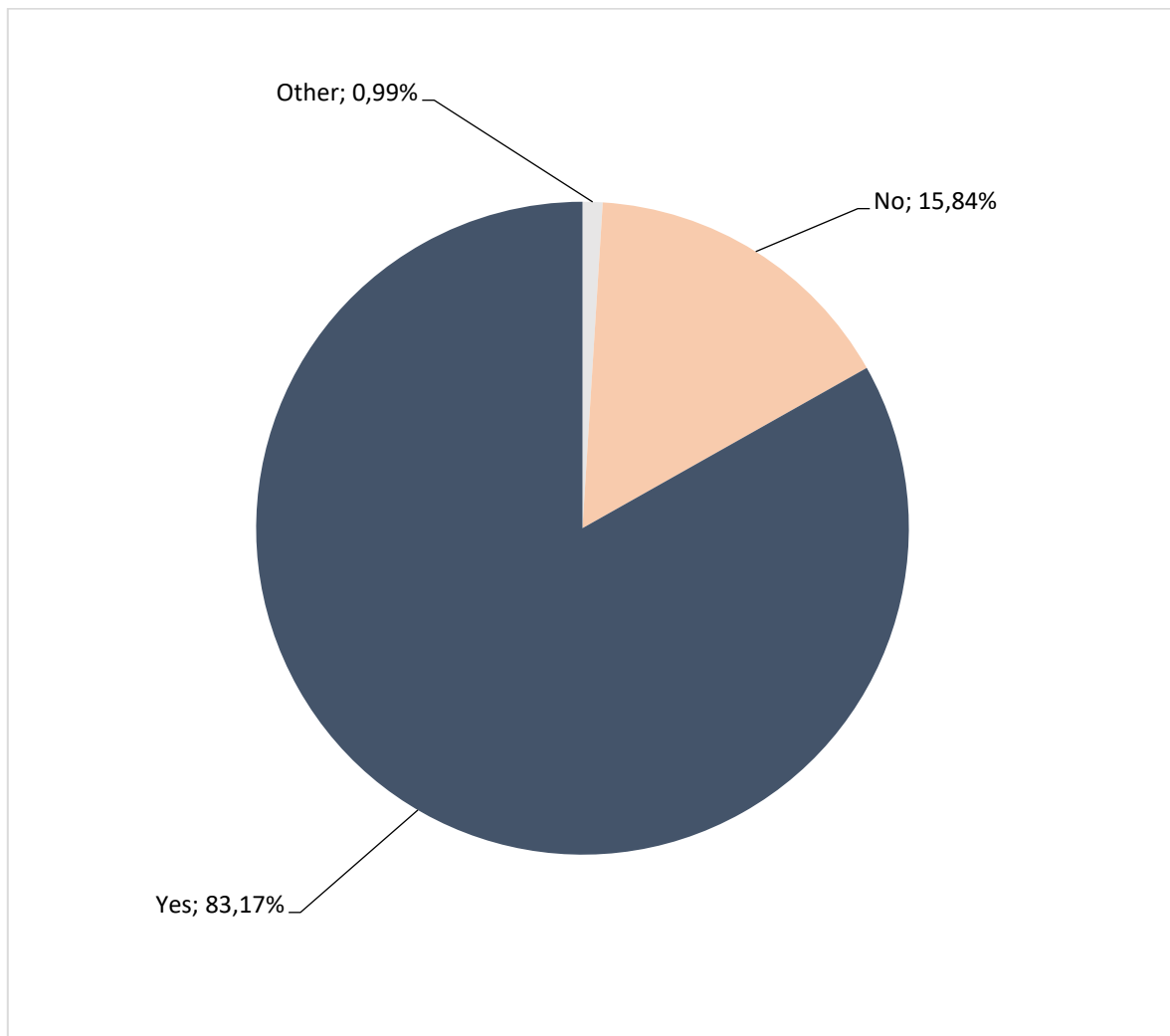


Chart 24: Concerns about cybersecurity (%)

The cybersecurity concerns are higher with the respondents working in hospitals than with the respondents from the social care organizations (**Chart 25**).

There is also an indication of higher variability of the sense of cybersecurity among the social care organizations.

While both types of organizations store sensitive data, we may assume that the staff of the health care organizations is more aware of their sensitivity and the risks of the data loss or theft.

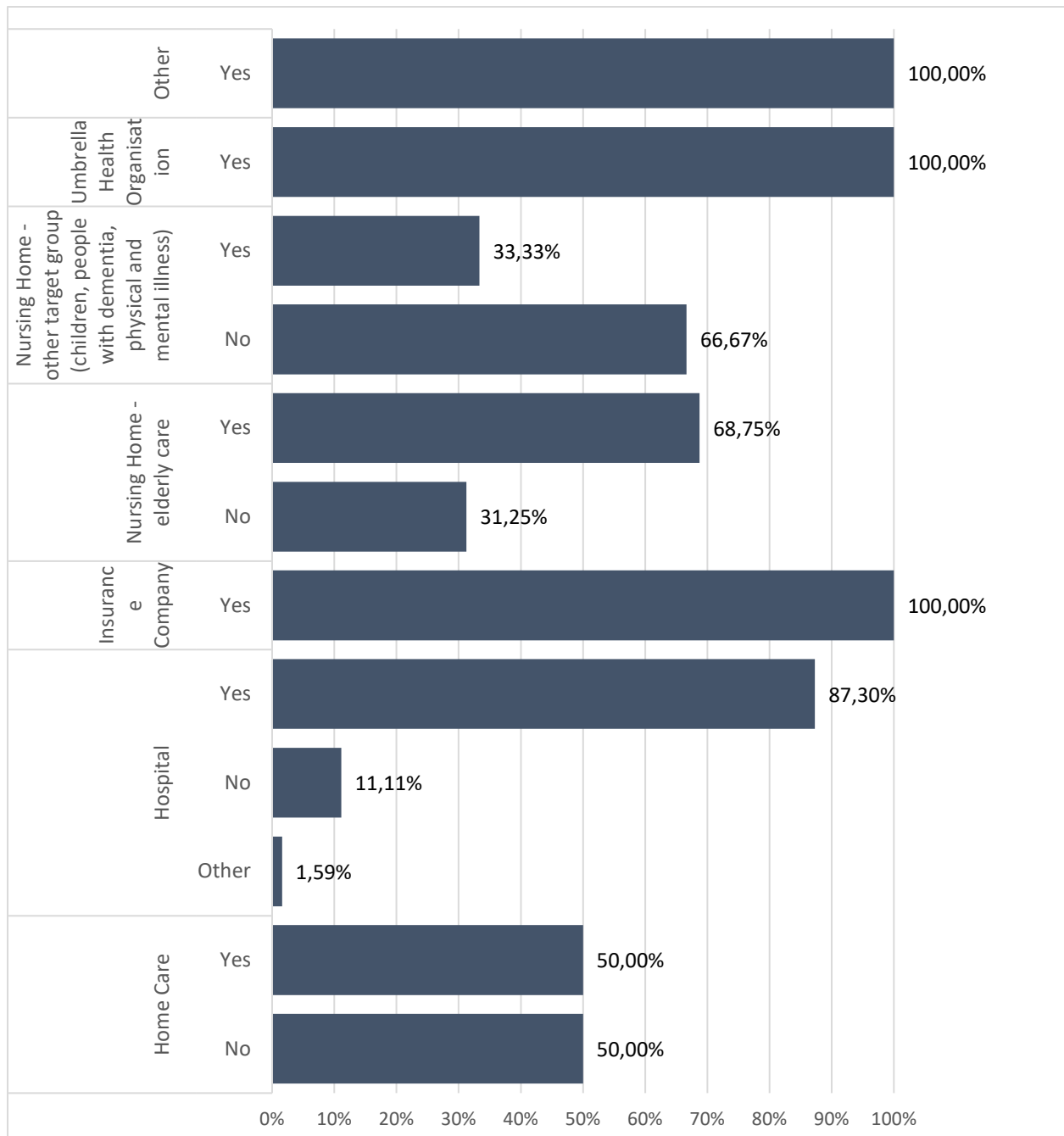


Chart 25: Concerns about cybersecurity (% of organization type)

Q13: Do you know the potential impacts of a cybersecurity attack? If yes, which impacts do you think a cyberattack can have to your organisation?

Three quarters of the respondents are aware of the potential impacts of a cybersecurity attack (**Chart 26**). When examining the data closely, this awareness is again stronger among the respondents representing the hospitals (**Chart 27**, 81 % vs less than 60 % on average among the respondents from the social services).

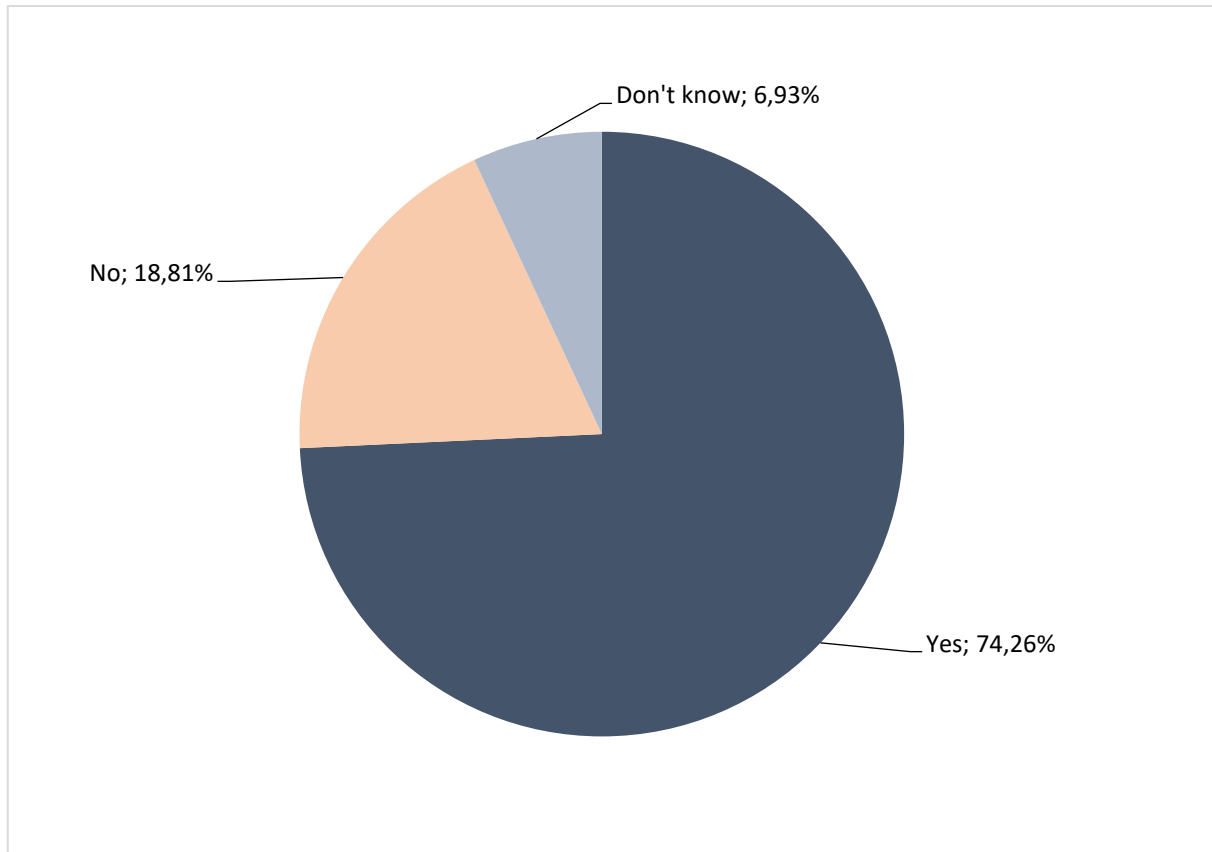


Chart 26: Awareness of the potential cybersecurity attack impacts (%)

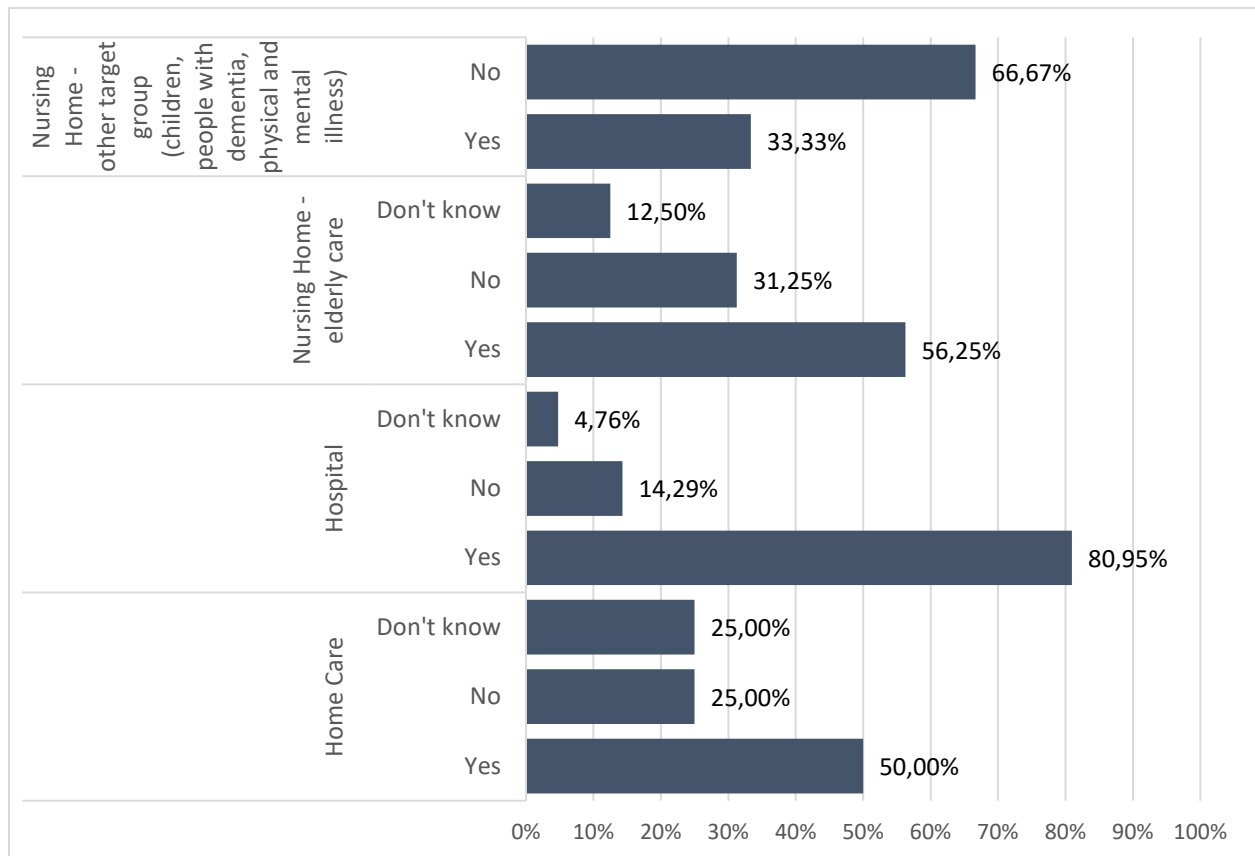


Chart 27: Awareness of the potential cybersecurity attack impacts (% of organization type)

The respondents also gave specific impacts that could be summarized into the 3 following categories:

- Data loss / data breach / data theft / data shared with unauthorized persons, made public
- Outages / restricted hospital functions / decrease of productivity
- Loss of credibility / reputation

Q14: How important do you think is cybersecurity for your organisation?

Two thirds of the surveyed organizations consider the cybersecurity as very important (Chart 28). On average, hospitals give the cybersecurity more importance than the social care organizations (Chart 29).

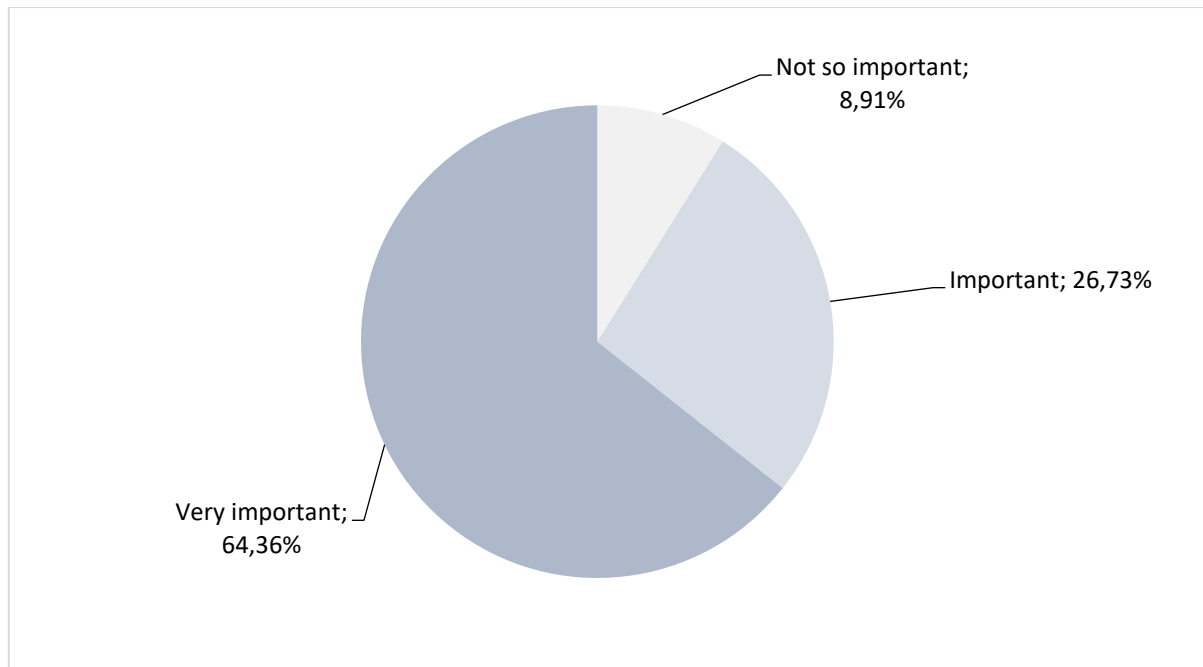


Chart 28: Importance of cybersecurity for the organization

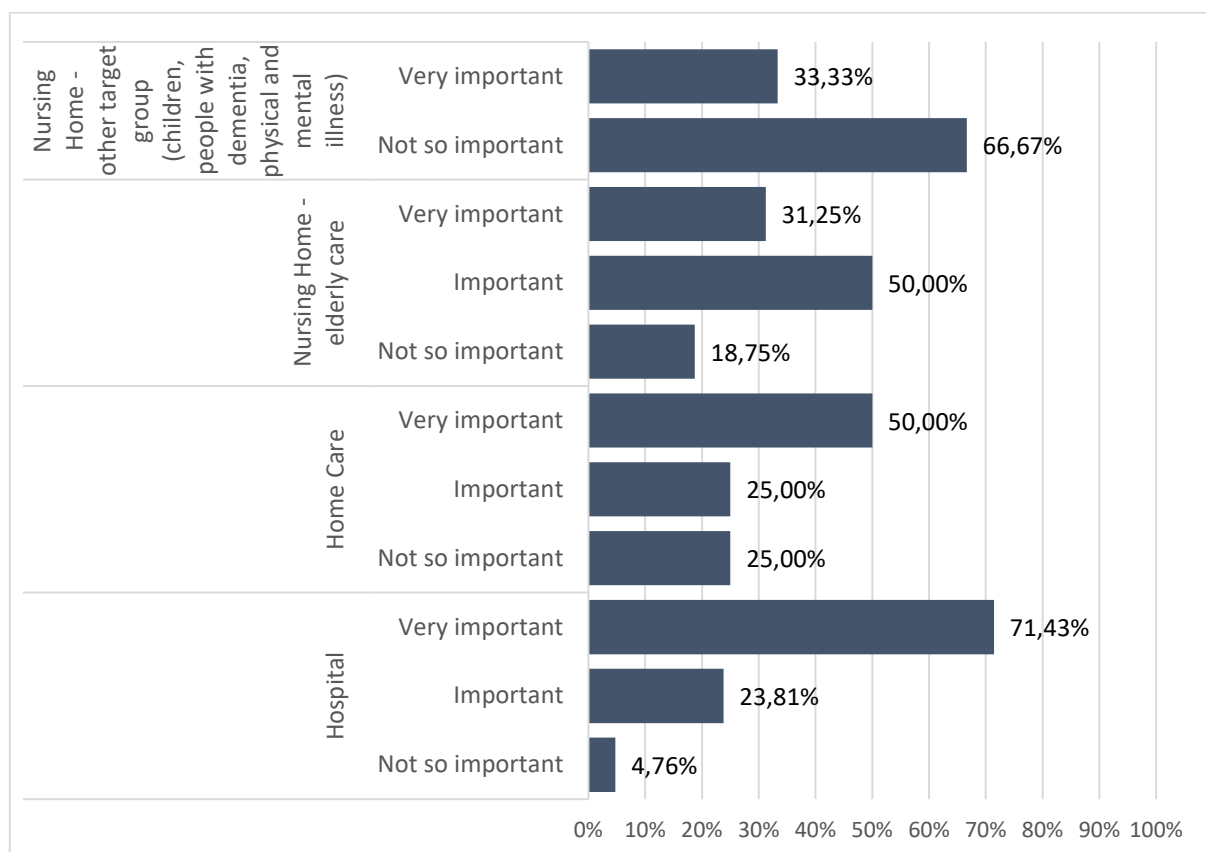


Chart 29: Importance of cybersecurity for the organization

Q15: Do you interact with your organisation's IT department?

This question closely examines interactions of the respondents with their IT department. In total, over 72 % of the respondents interact closely and regularly (**Chart 30**). We have also examined the structure by the type of the organization and the role in the organization. The “RARELY” replies are less common from the respondents representing hospitals (16 % vs 38 % in elderly care organizations as the most frequent type, **Chart 31**). Out of 35 respondents representing managerial roles, 10 persons are rarely or never in contact with their IT department (**Chart 32**).

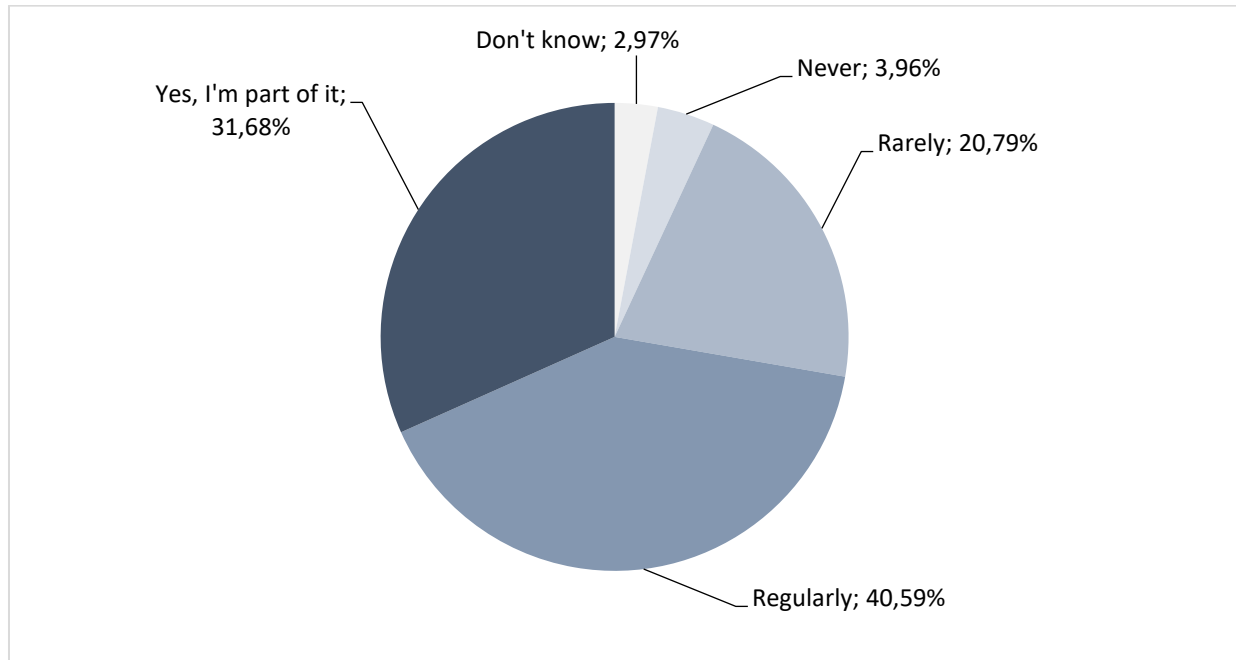


Chart 30: Interactions with the IT department

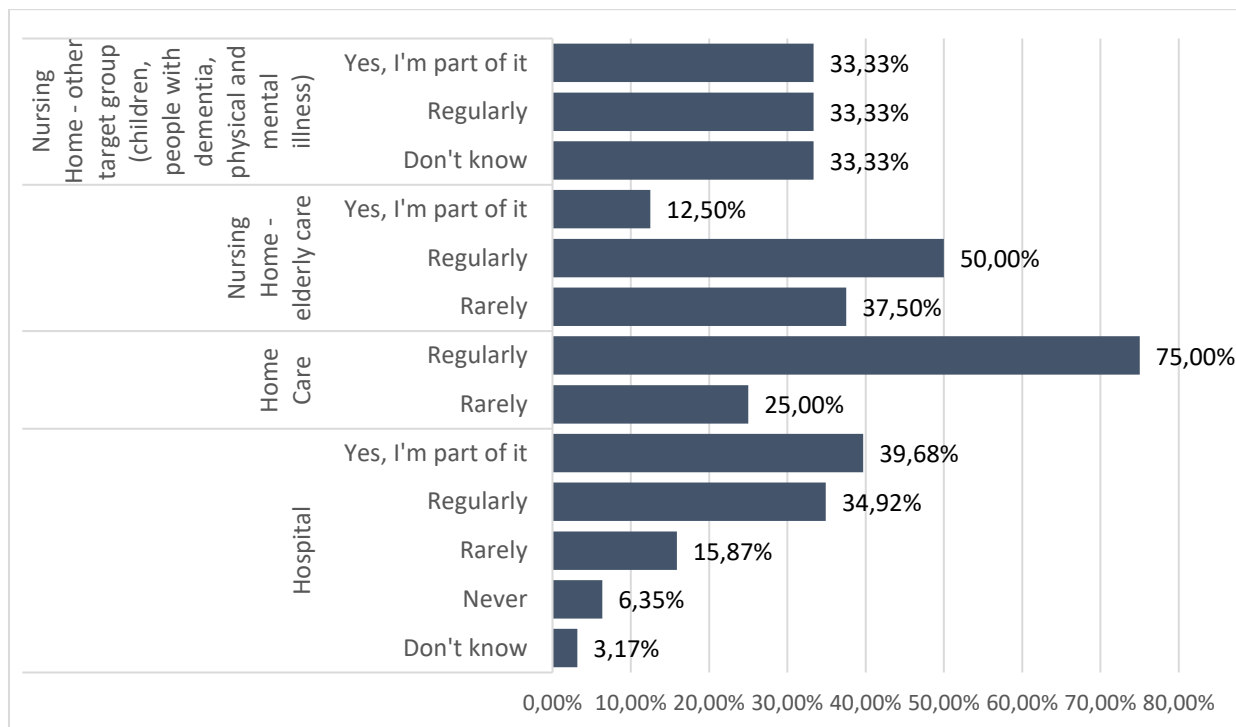


Chart 31: Interactions with the IT department by organisation type

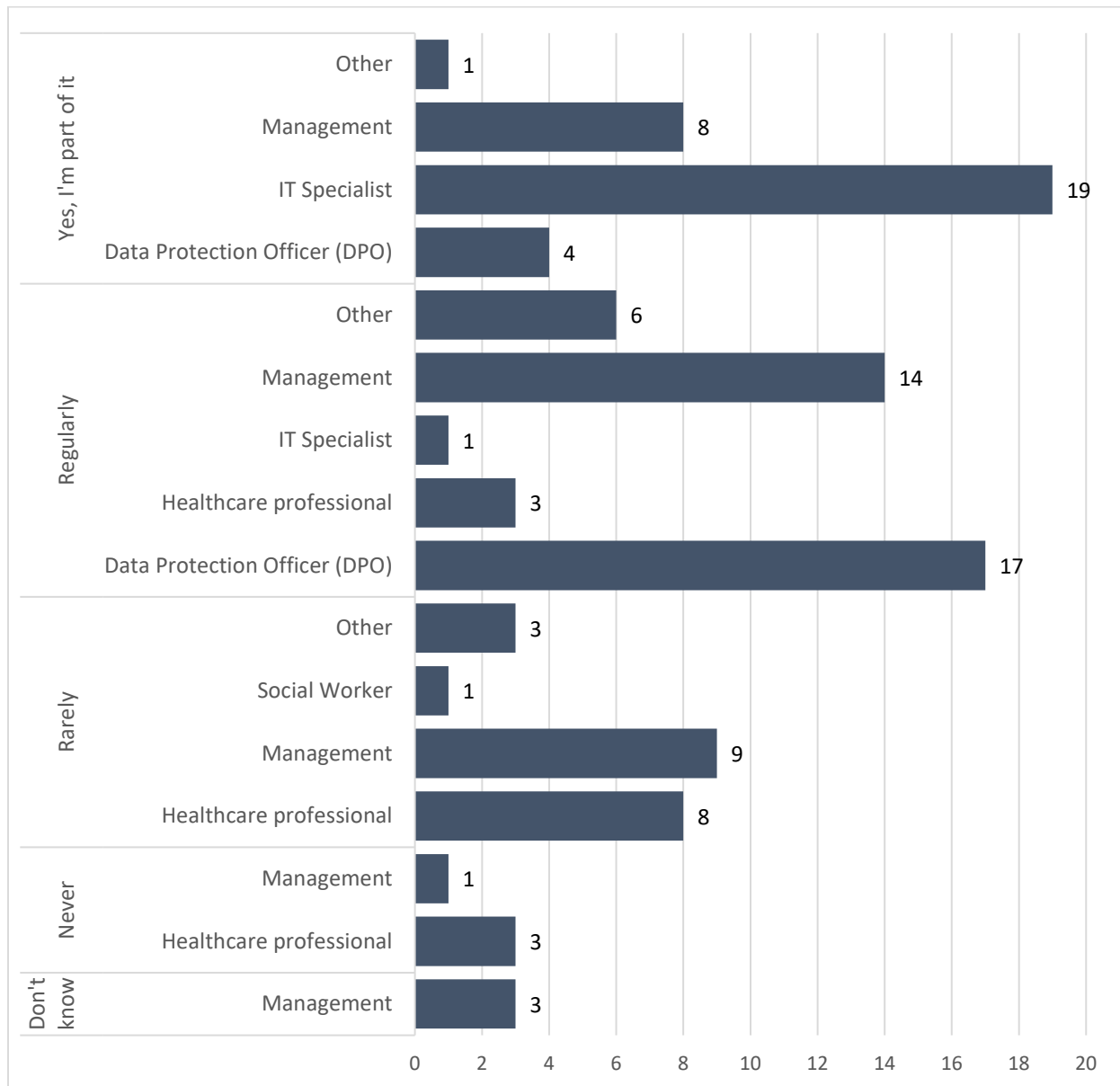


Chart 32: Interactions with the IT department by the role in the organization

Q16: When you have cybersecurity concerns, who do you contact what to do?

Multiple answers were possible for this query. The answer „I contact the IT department“ was selected most frequently, by over 70 % of respondents (**Chart 33**). Those applying their own solutions are logically mostly IT specialists, almost 58 %, followed by 27 % of managers ().

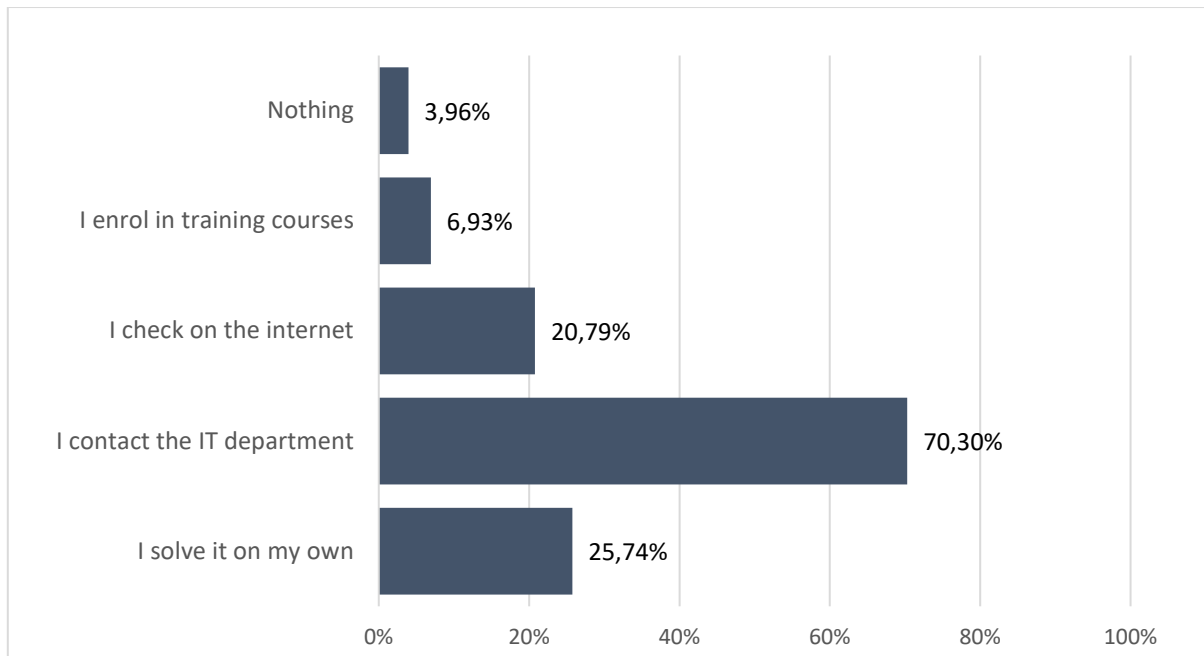


Chart 33: Means of addressing cybersecurity concerns

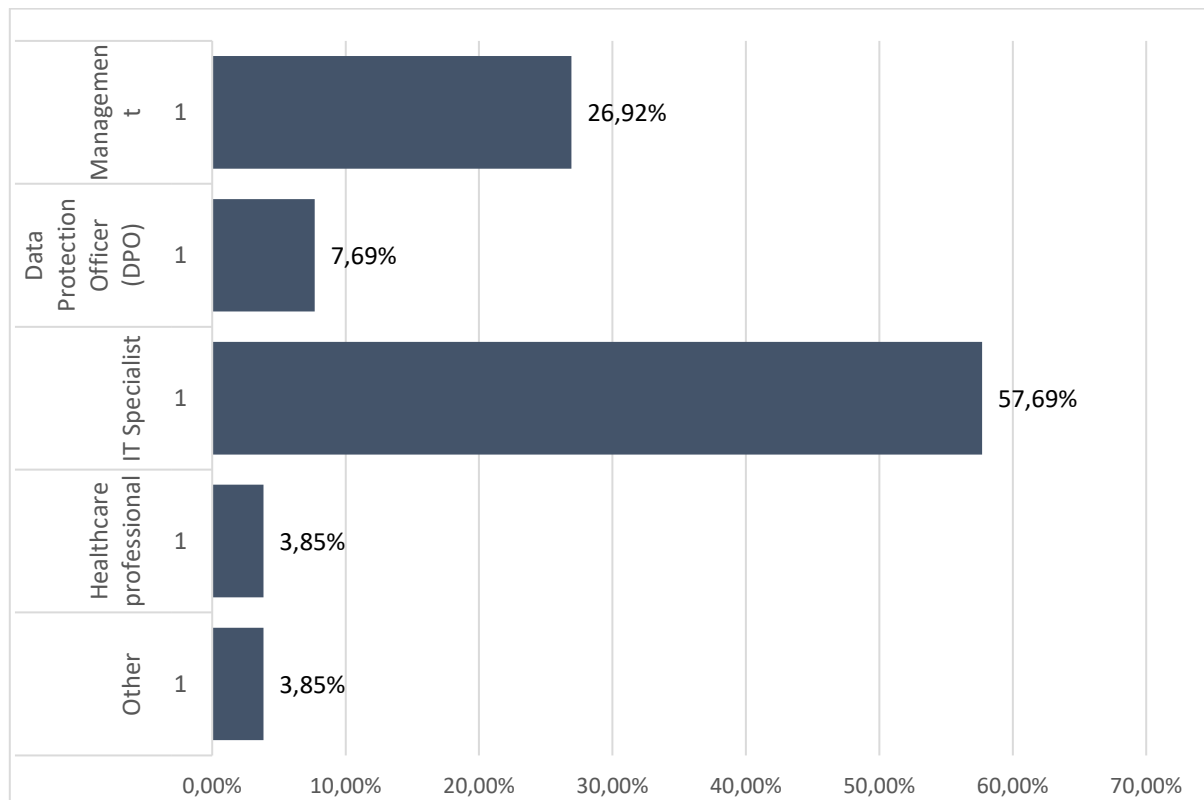


Chart 34: Means of addressing cybersecurity concerns (% of I SOLVE IT ON MY OWN)

Interestingly, most persons checking for solutions on the internet are DPOs, almost 50 % of respondents in this category (**Chart 35**).

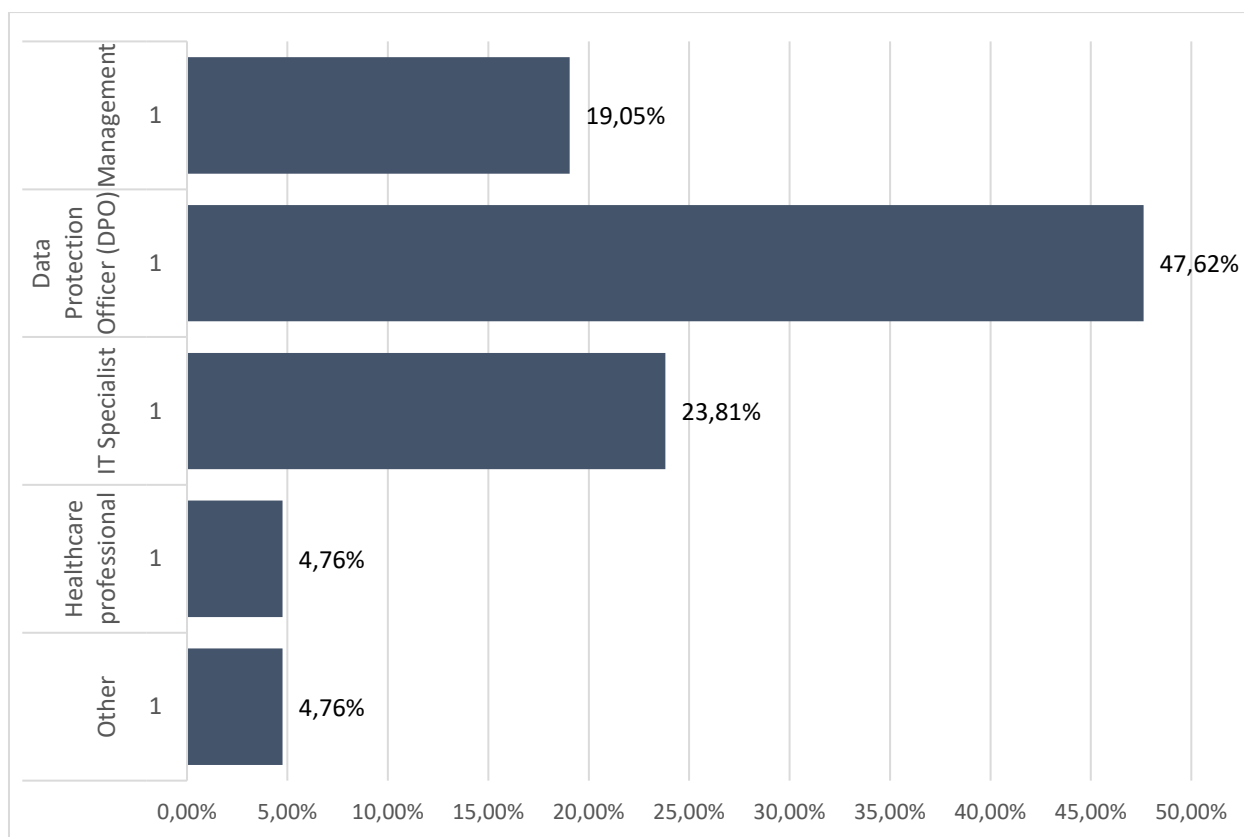


Chart 35: Means of addressing cybersecurity concerns (% of I CHECK ON THE INTERNET)

The respondents could also provide their own answer. The 9 received answers could be summarized into – I contact the management / I contact my boss / I contact the external service provider.

Q17: How frequently are cybersecurity risk assessments conducted at your organisation?

As per the answers, most participating organizations conduct cybersecurity risk assessments annually, bi-annually or semi-annually (**Chart 36**).

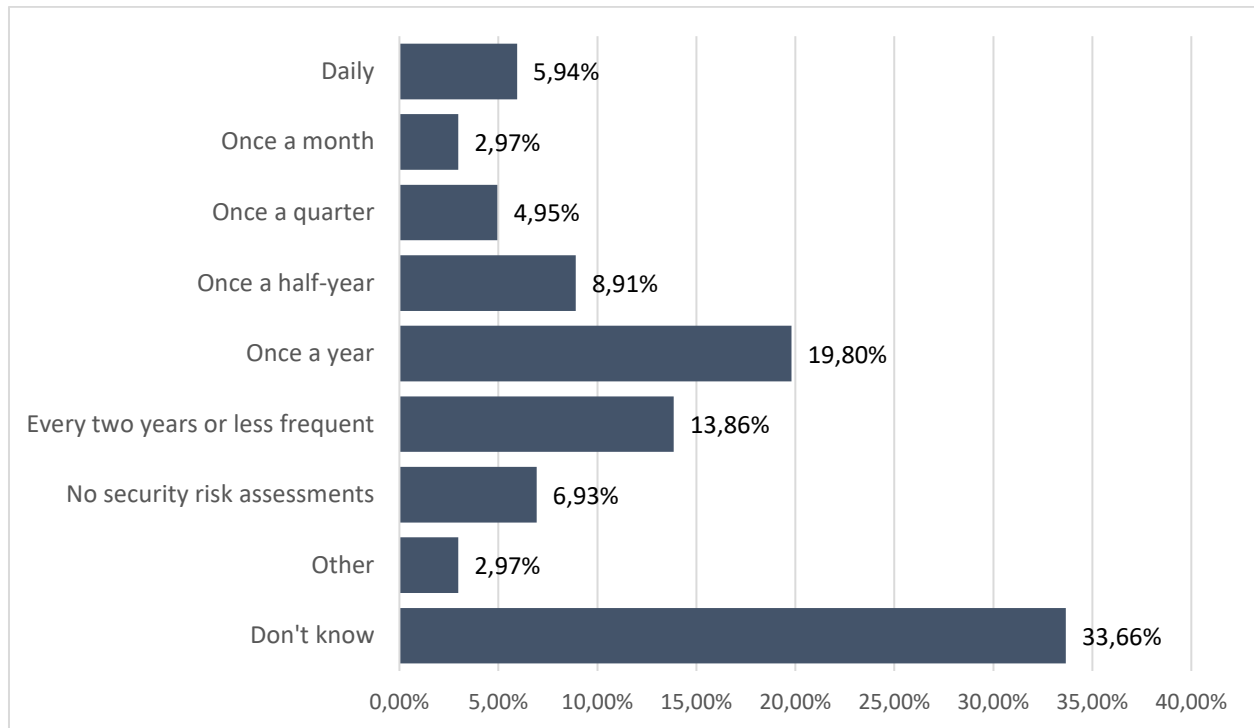


Chart 36: Frequency of cybersecurity risk assessment

Given the significant amount of responses under DO NOT KNOW we have closely looked at the structure of answers in this category (**Chart 37**). Interestingly, there is a significant share of responses from managers (32,4 %, or 11 respondents), almost as many as the healthcare professionals.

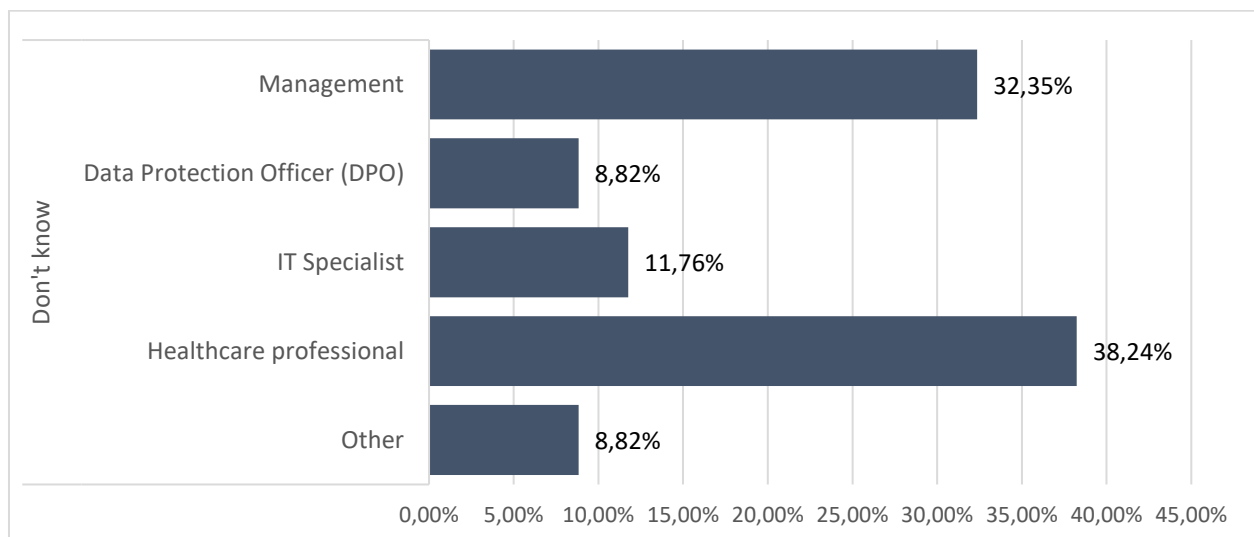


Chart 37: Frequency of cybersecurity risk assessment (% of DO NOT KNOW)

We had a closer look at two types of organizations – hospitals and nursing homes for elderly (**Chart 38**) and have not found significant differences. Approximately a quarter of each type of organizations conducts assessment annually.

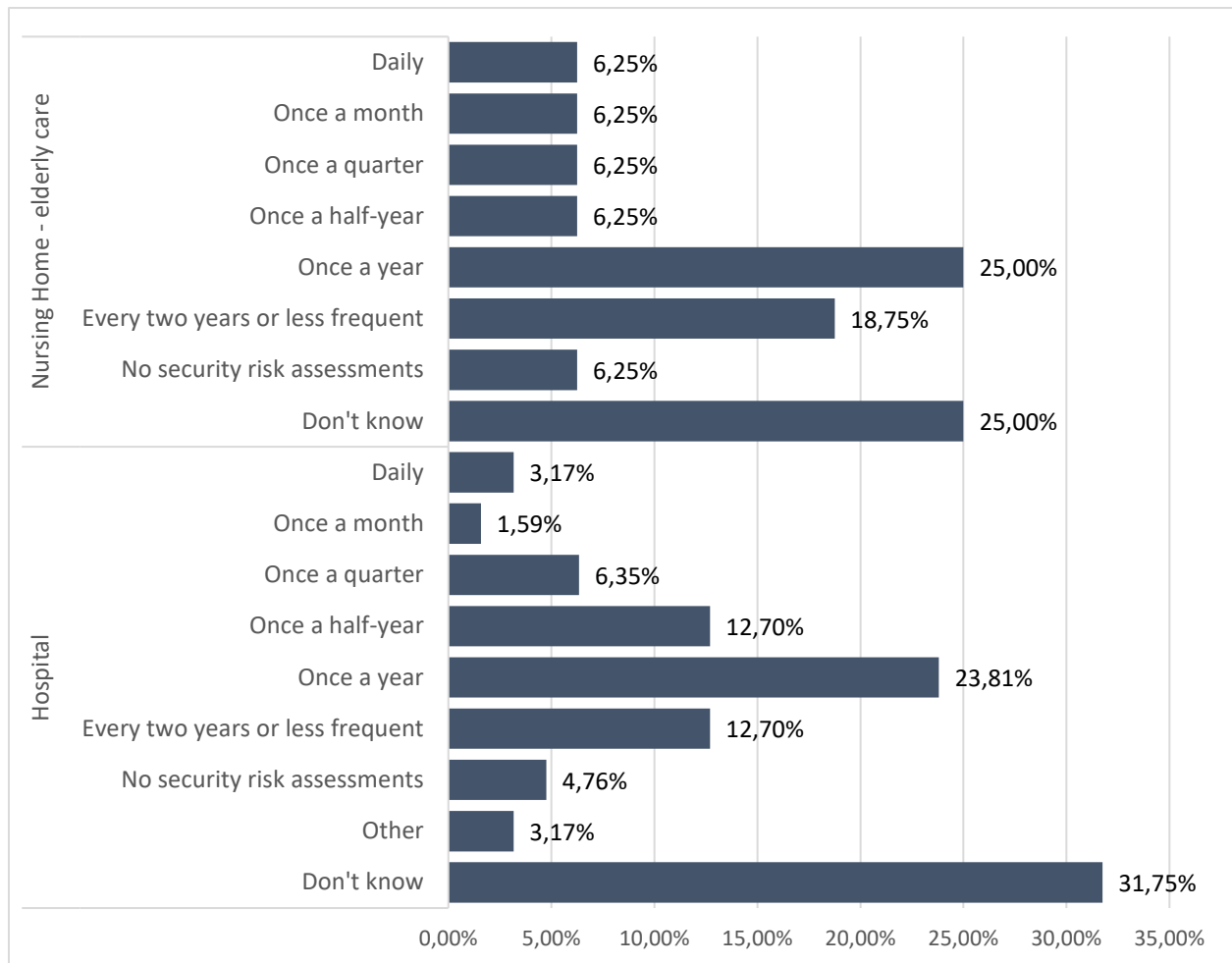


Chart 38: Frequency of cybersecurity risk assessment by organisation

While we have not acquired detailed information regarding the procedures and processes of the cybersecurity risk assessments, we assume from the sample that assessments more frequent than annually are not very common in the surveyed organizations.

Also, it is worth noting that the answer DO NOT KNOW contains about 60 % respondents that, in our view, should be aware of such procedures.

Q18: Are all users required to change passwords on at least a quarterly basis and instructed to use at least six characters with a combination of lowercase, uppercase, digits and symbols?

This query explores the most common practice in terms of requirements regarding user passwords. While at first glance the results in **Chart 39** might give good sense of access security, it may also indicate potential risks of users not storing their passwords securely (written on “post-its”, kept at the computer).

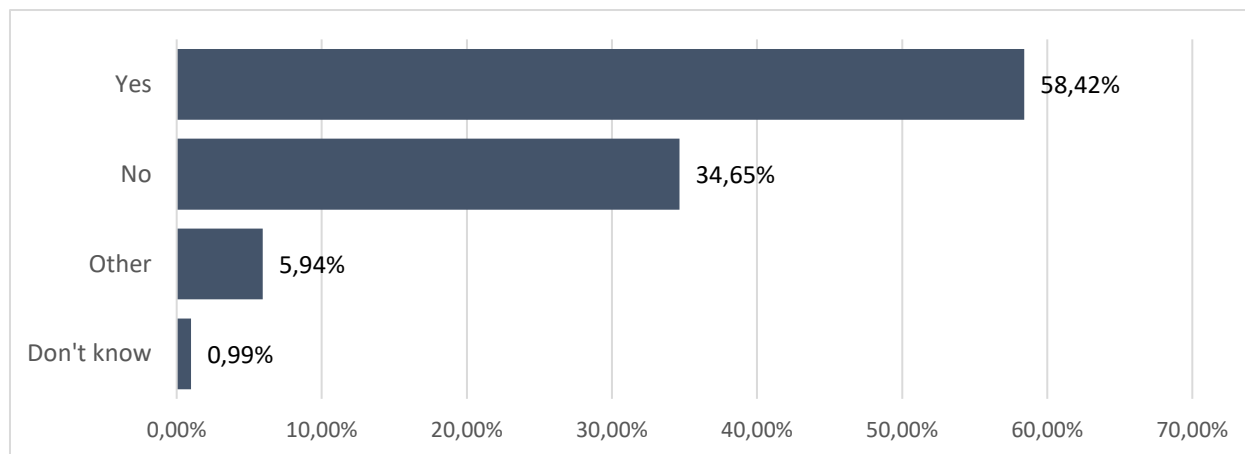


Chart 39: Users requested to change their password quarterly and use strong combinations

A closer look at the two major respondent groups shows that the policy of more frequent password changes and stronger passwords is more common in the hospitals (**Chart 40**).

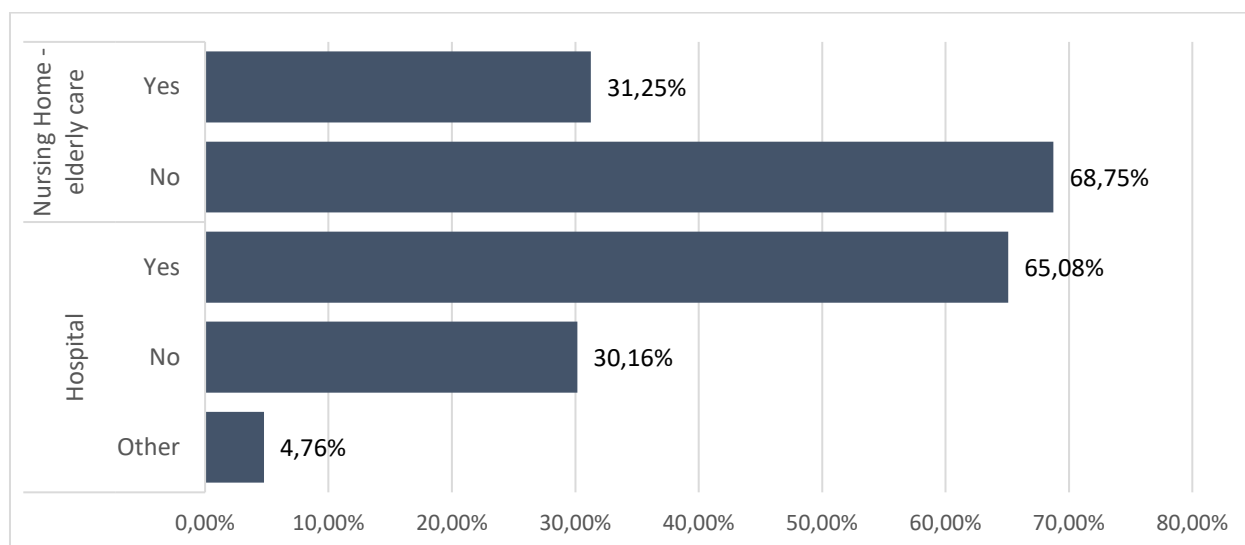


Chart 40: Users requested to change their password quarterly and use strong combinations, by organisation type

This query should ideally be followed upon in individual interviews regarding the common practice in the organizations that would reveal whether the apparent security reflects the reality of the workspace.

In general, the policy of frequent password changes and very strong passwords has been eased, as its stringent application resulted in unsafe user behaviour.

Q19: Has your network been EXTERNALLY assessed/penetration tested in the past year?

Only one quarter of the organizations have been externally penetrated in the past year (**Chart 41**). Even though the organizations were not further queried, the reasons for the low number are obvious – the external penetration testing / ethical hacking is expensive, demanding, and unfavourable results can bring bad publicity.

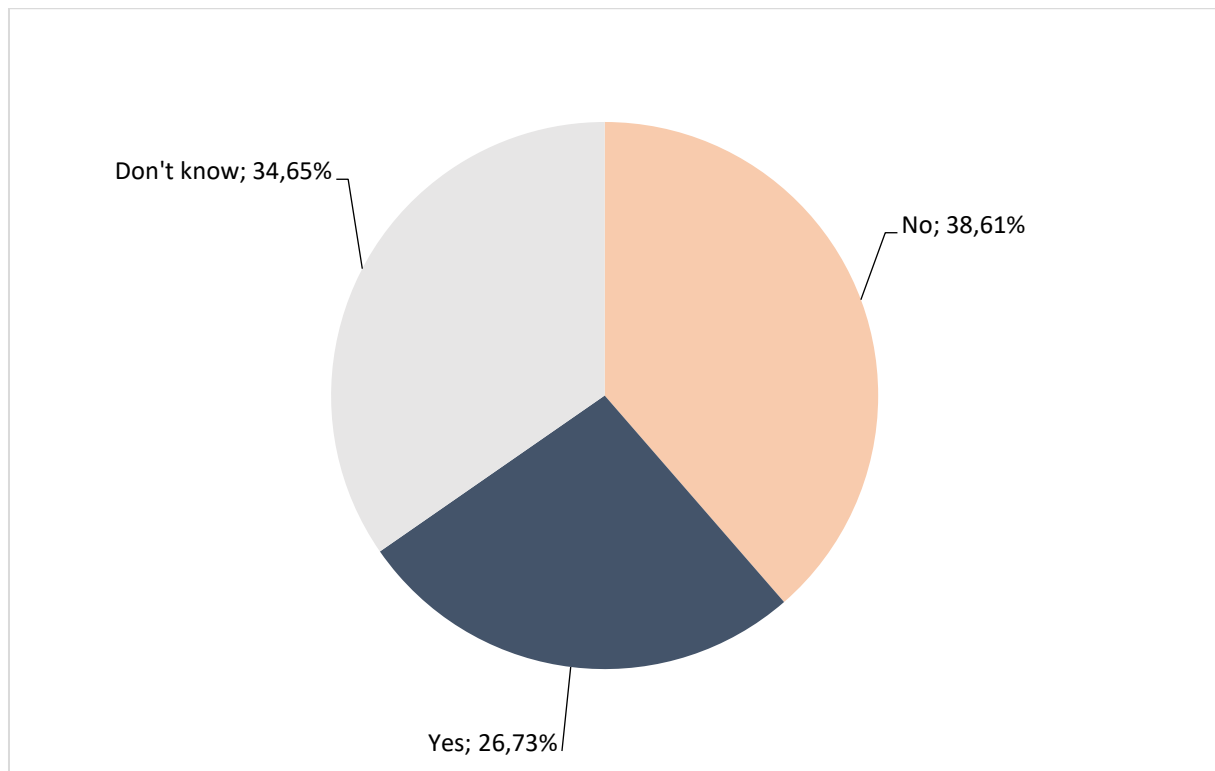


Chart 41: Organization externally assessed / penetration tested in the past year

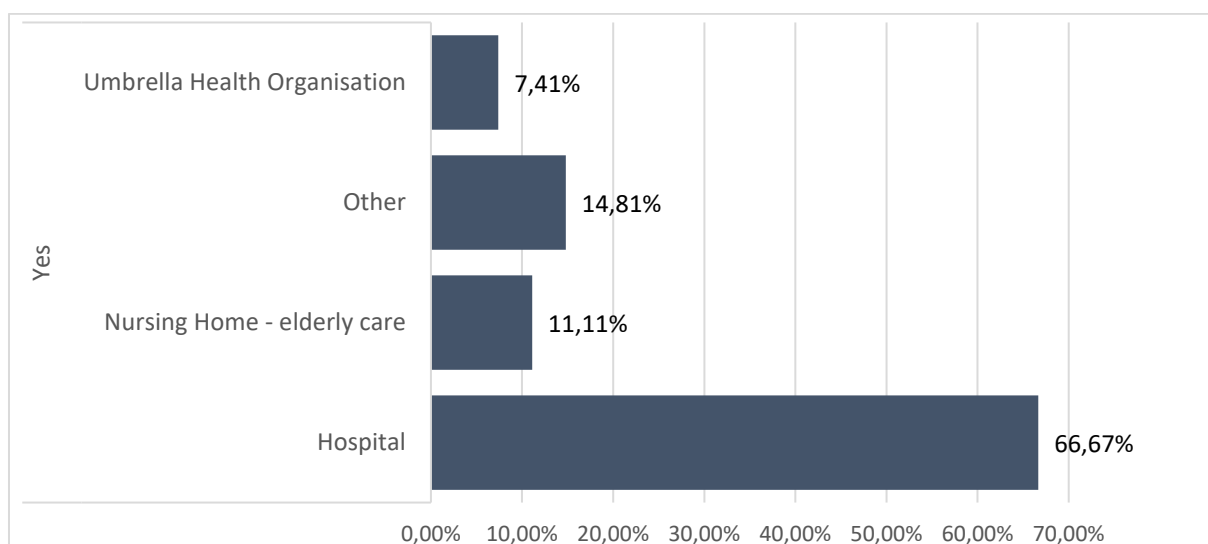


Chart 42: Organization externally assessed / penetration tested in the past year (% of YES)

A closer look at the positive answers reveals that two thirds of penetration tested organizations were hospitals.

Q20: Has your network been INTERNALLY assessed/penetration tested in the last year?

Internal penetration tests are usually conducted by the senior IT staff with sufficient expertise. The results of this query are similar to the previous one (**Chart 43**) – about 30 % of the organizations conducted such tests.

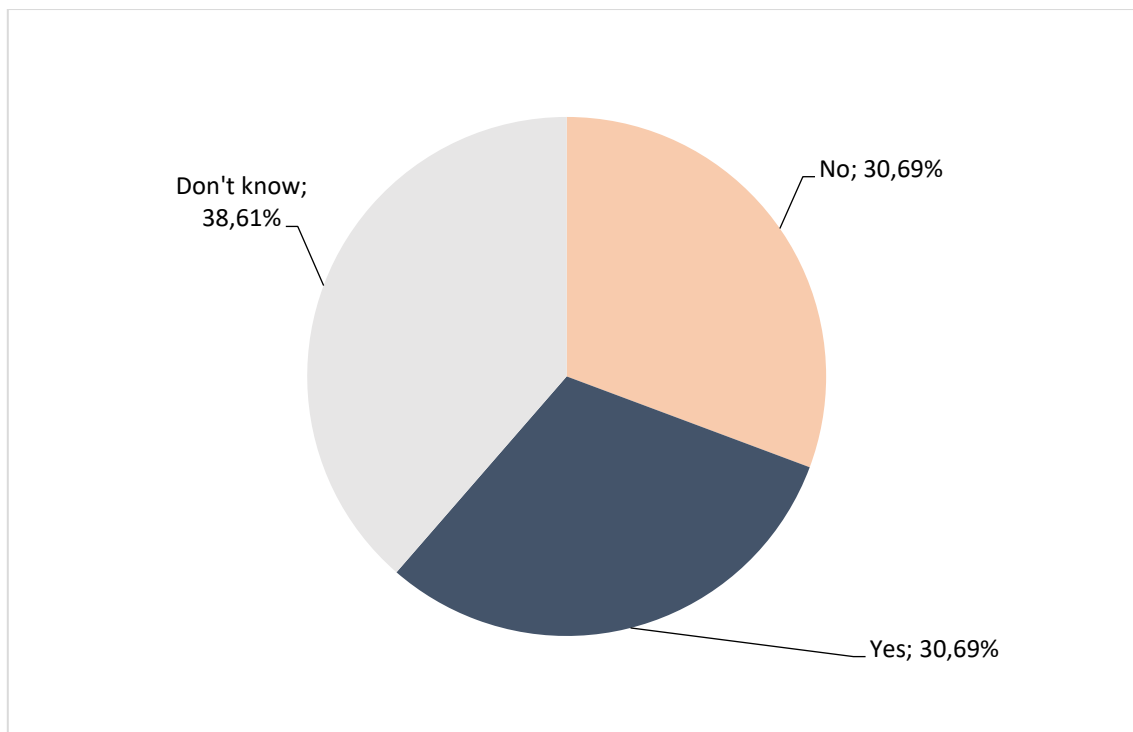


Chart 43: Organization internally assessed / penetration tested in the past year (%)

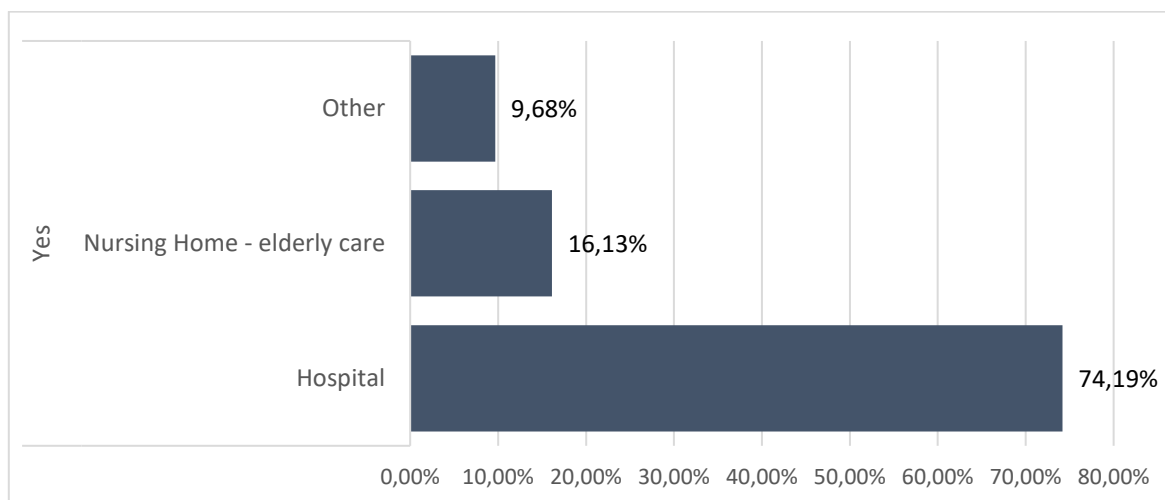


Chart 44: Organization internally assessed / penetration tested in the past year (% of YES)

As expected, internal penetration tests are mainly conducted in hospitals. We have not closely examined the structure and extent of internal penetration tests. These, to be done properly and sufficiently, require significant expertise and experience. The experience shows that only a limited number of IT staff with such qualifications holds internal positions in the domain of health care or social services.

Q21: Do you have a data retention & destruction policy?

Two thirds of the organizations have a data retention and destruction policy in place (**Chart 45**). We also closely examined the DO NOT KNOW answers, as they were given by over 20 % of the respondents (**Chart 46**). 10 respondents working as managers, DPOs or IT specialists responded that they do not know whether such policy is in place.

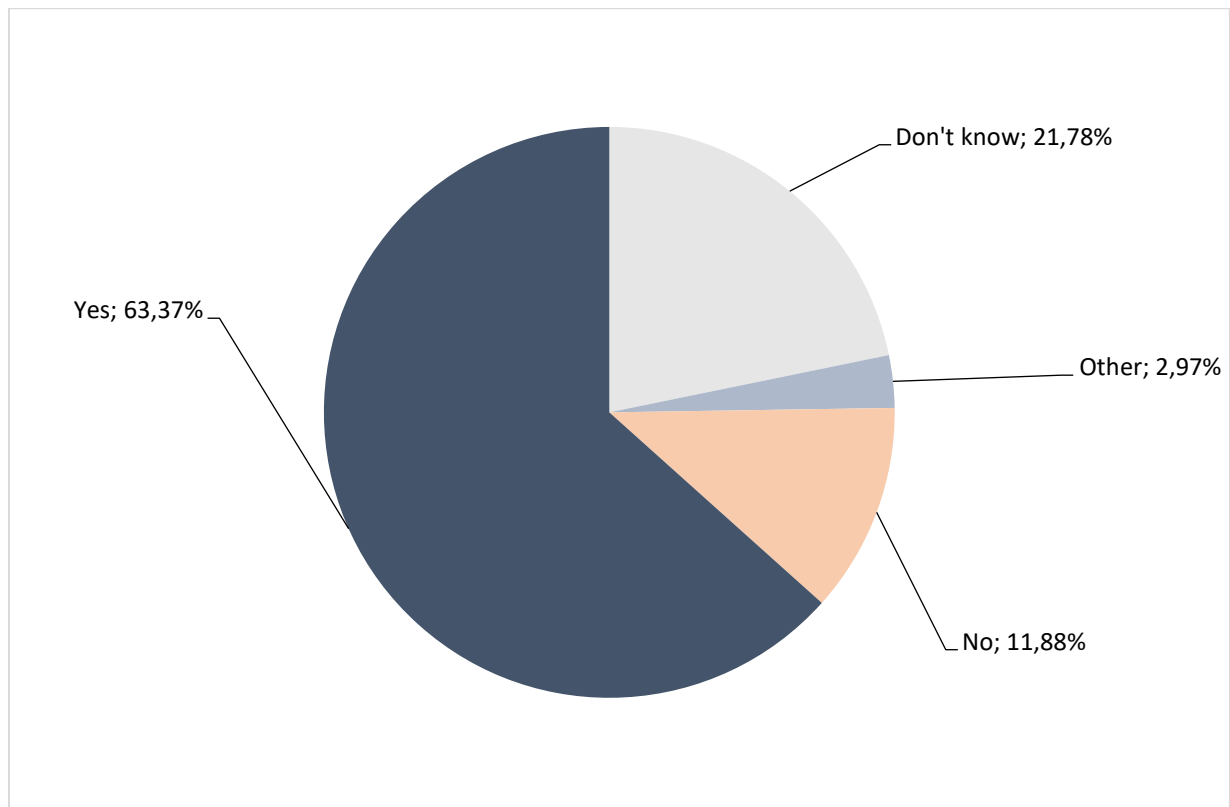


Chart 45: Data retention & destruction policy in place in the organization

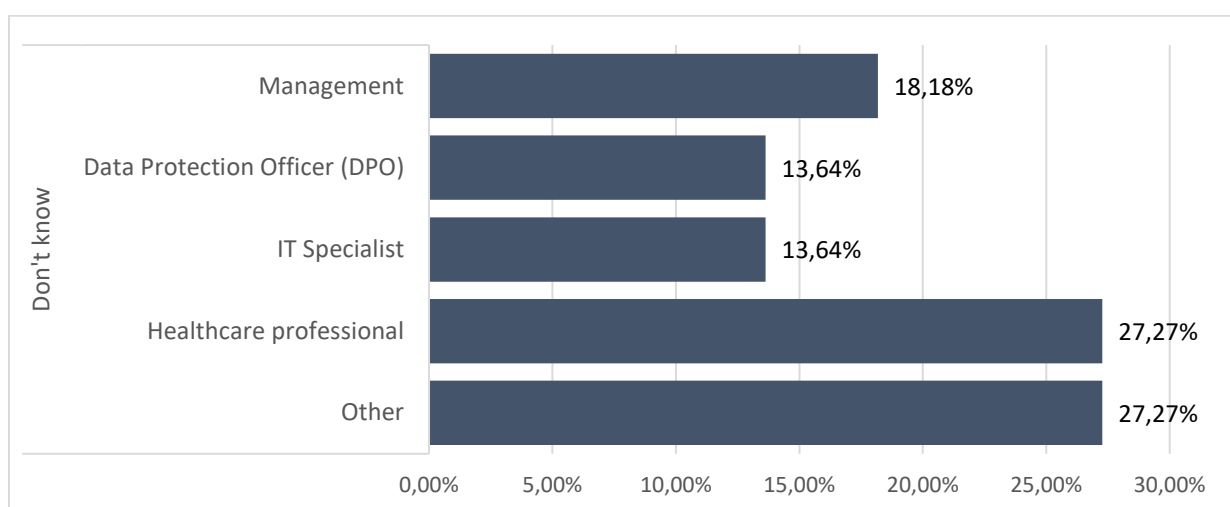


Chart 46: Data retention & destruction policy in place in the organization (% DO NOT KNOW)

Q22: Are firewalls in place at all external connection points?

The results of this query confirm that the basic security infrastructure is in place in most organizations (**Chart 47**). The number of DO NOT KNOW responses was also further examined – all the answers were given by non-IT staff, therefore the total number of organizations with firewalls in place will certainly be higher than 74 %.

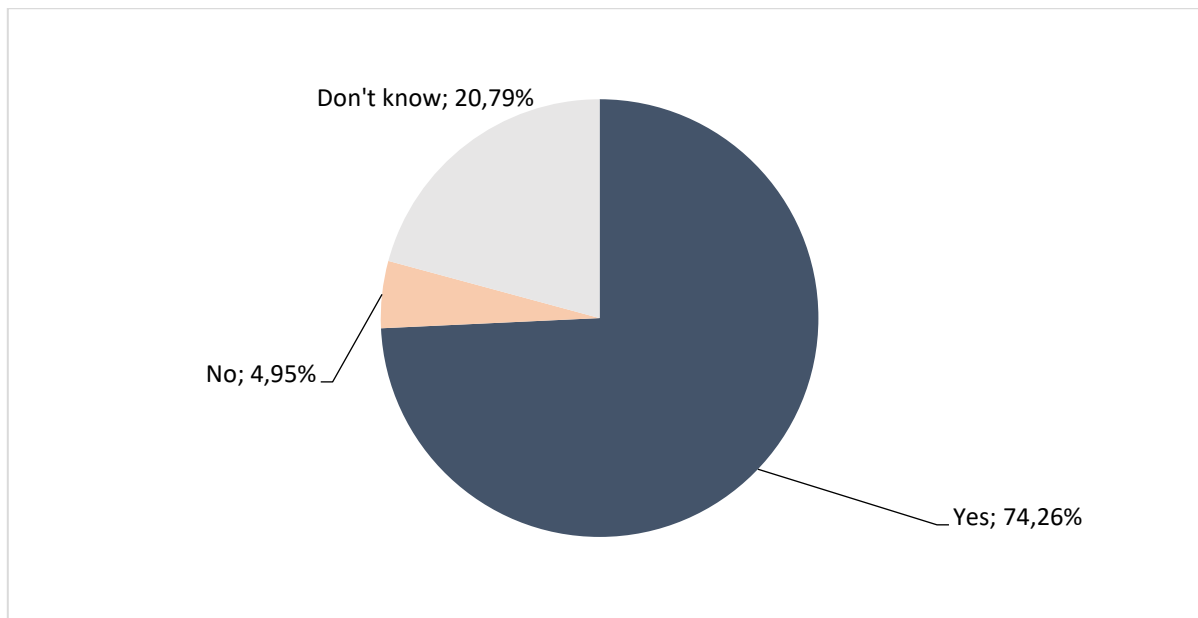


Chart 47: Firewalls in place at all external connection points

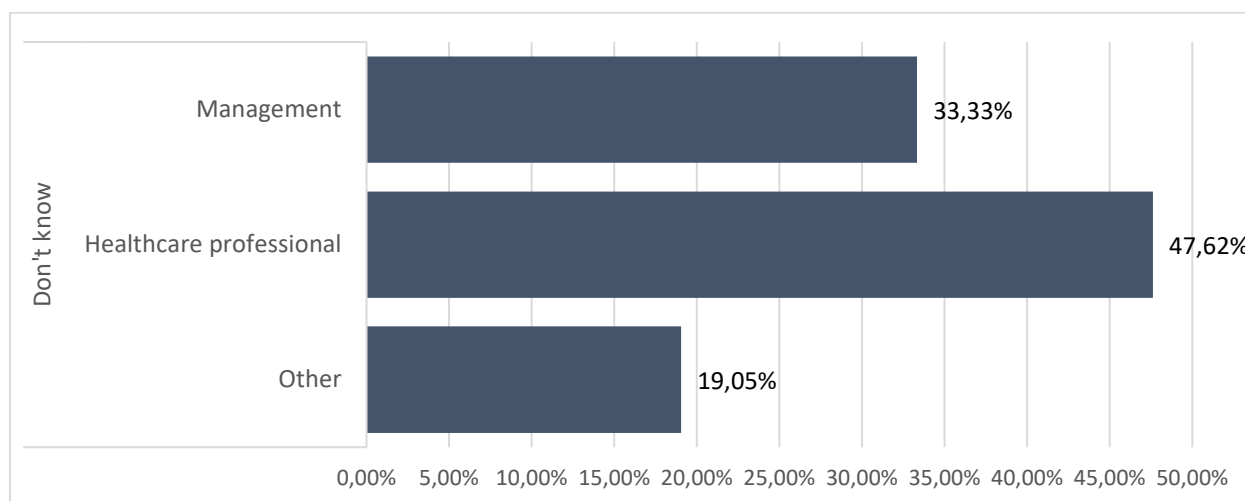


Chart 48: Firewalls in place at all external connection points (% of DO NOT KNOW)

We have not further examined how the firewalls are set up and administered. We can only assume from the previous queries that only about one third of these devices were penetration tested.

Q23: Do you allow remote access to your corporate network?

Two thirds of the organizations allow remote access to the corporate network (**Chart 49**).

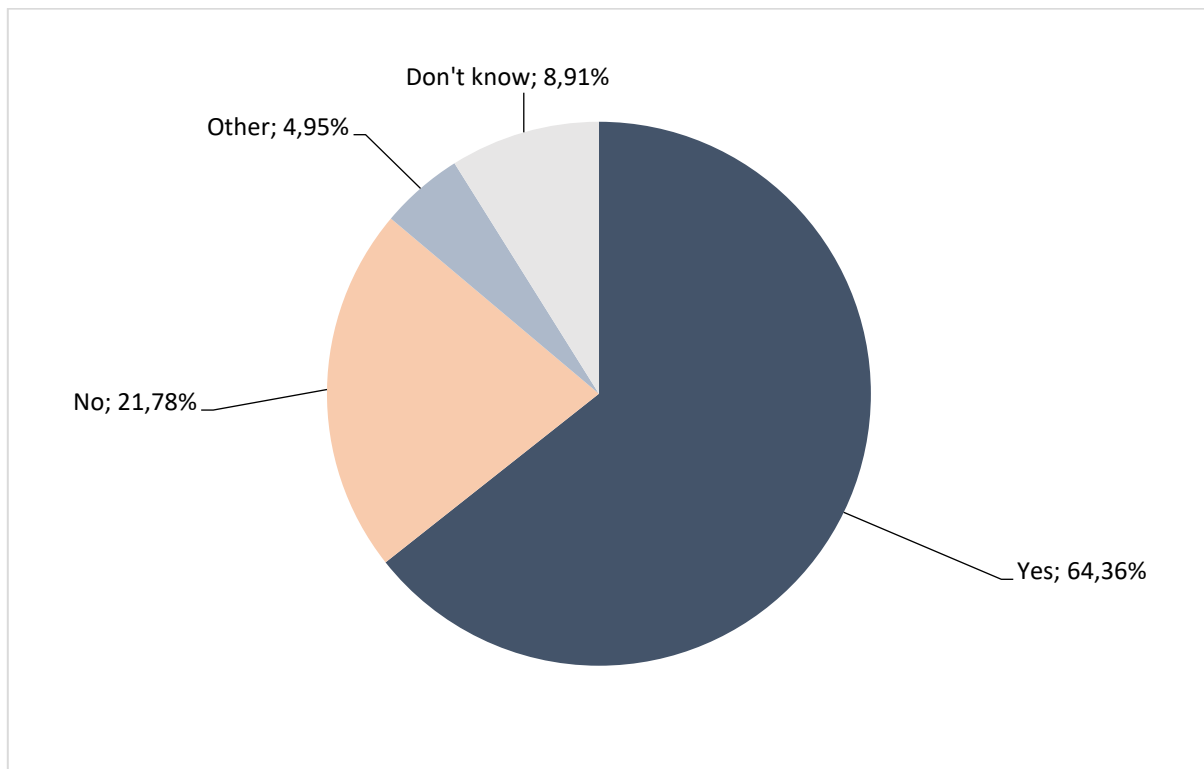


Chart 49: Remote access to corporate network (%)

We have not further examined the extent of the access to the network and applications, access rights to view, read and write, as well as specific forms of access (VPN, remote desktop...).

The remote access option is also more common among the surveyed hospitals (75 % of the hospitals, only 31 % of the elderly care organizations, **Chart 50**).

Typically, organizations provide remote access to reflect the needs of the flexible workspace. Health and social care organizations are not typical examples of employers with high workspace flexibility.

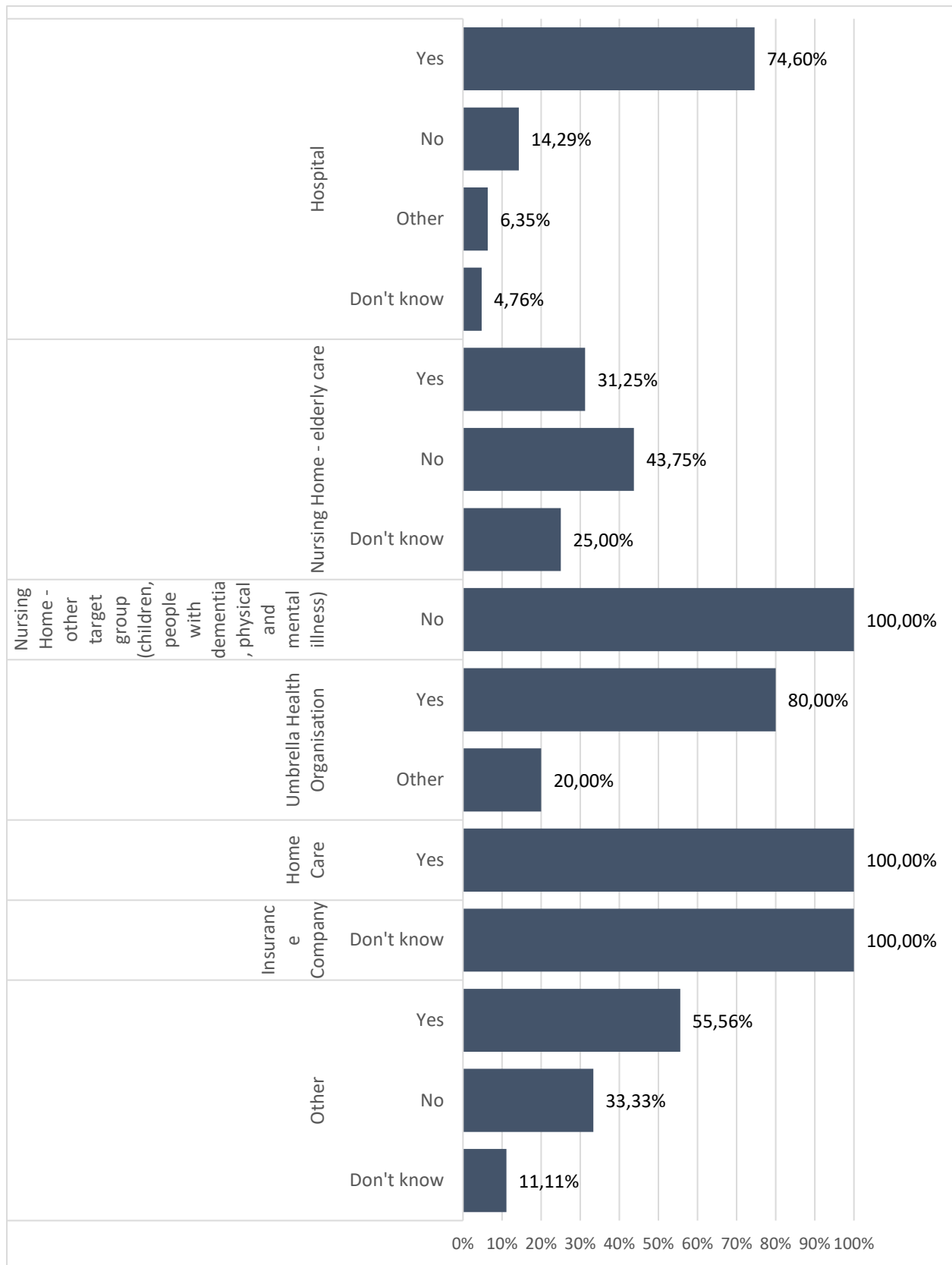


Chart 50: Remote access to corporate network by organization type

Q24: Are all connecting devices required to have anti-virus and firewall installed in accordance with your organisation's policy for updates and patching?

The results of this query are similar to those with firewalls – 73 % of the organizations have anti-virus and firewalls installed, up to date and patched (**Chart 51**). This number will most probably be higher given the structure of the DO NOT KNOW answers (**Chart 52**).

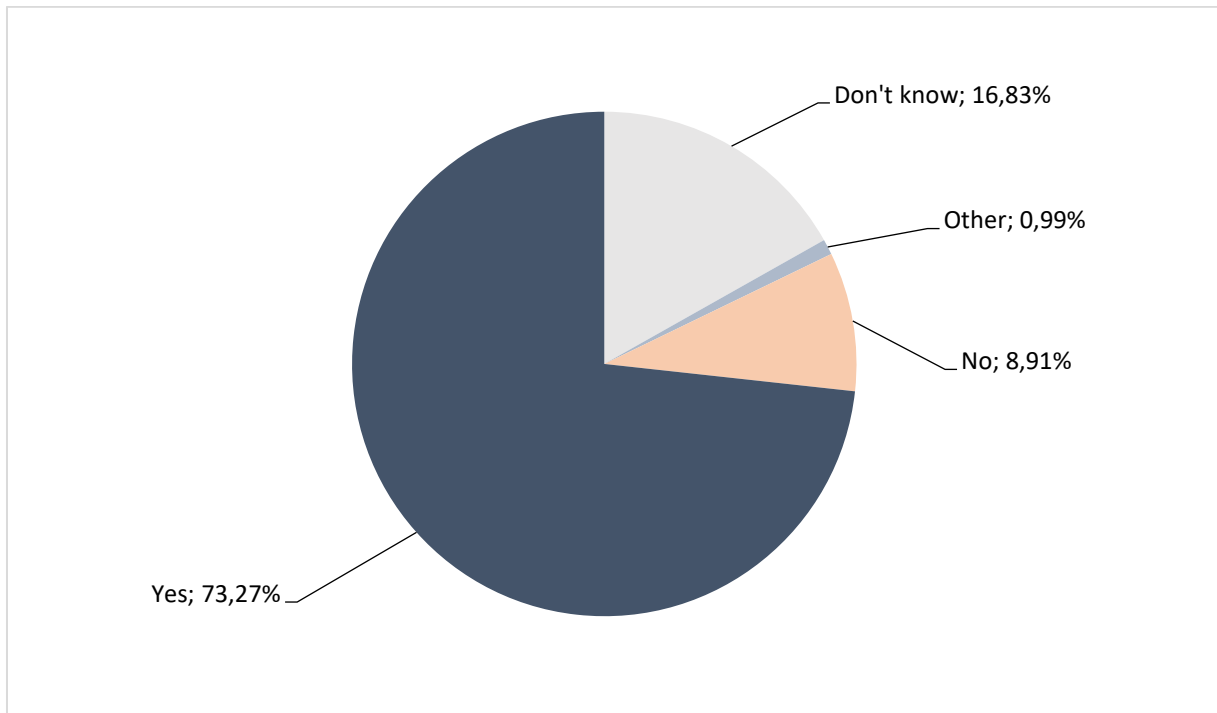


Chart 51: Devices required to have anti-virus and firewall installed in accordance with your organisation's policy for updates and patching

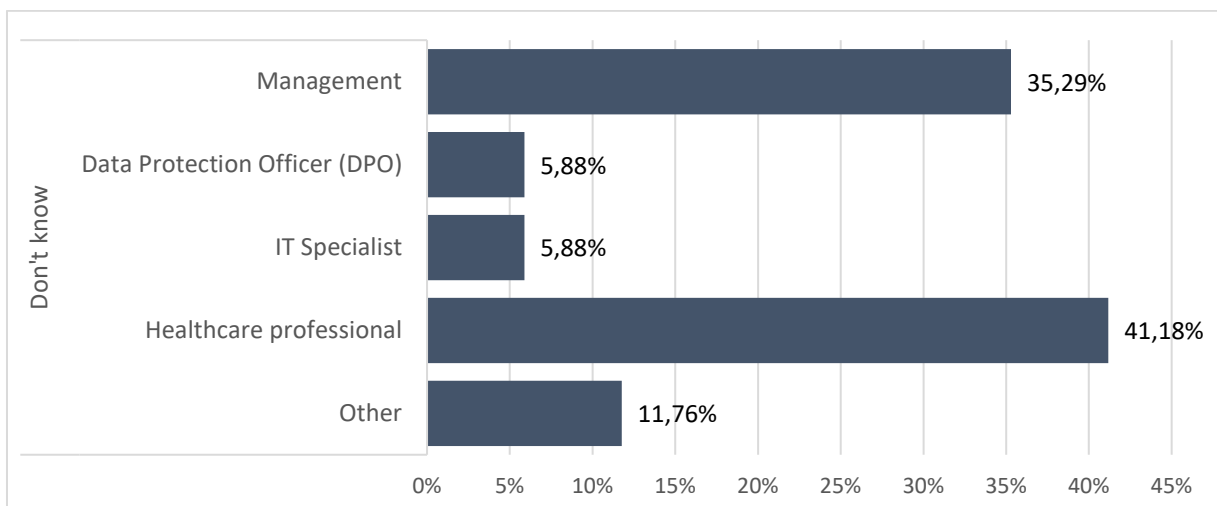


Chart 52: Devices required to have anti-virus and firewall installed in accordance with your organisation's policy for updates and patching (% of do not know)

Q25: Are employees allowed to bring their own IT devices and use these on the organisation's network?

Only one third of the organizations support BYOD (Bring Your Own Device). The respondents that gave the YES answers also indicated that the security measures for the BYOD policy are rather strict.

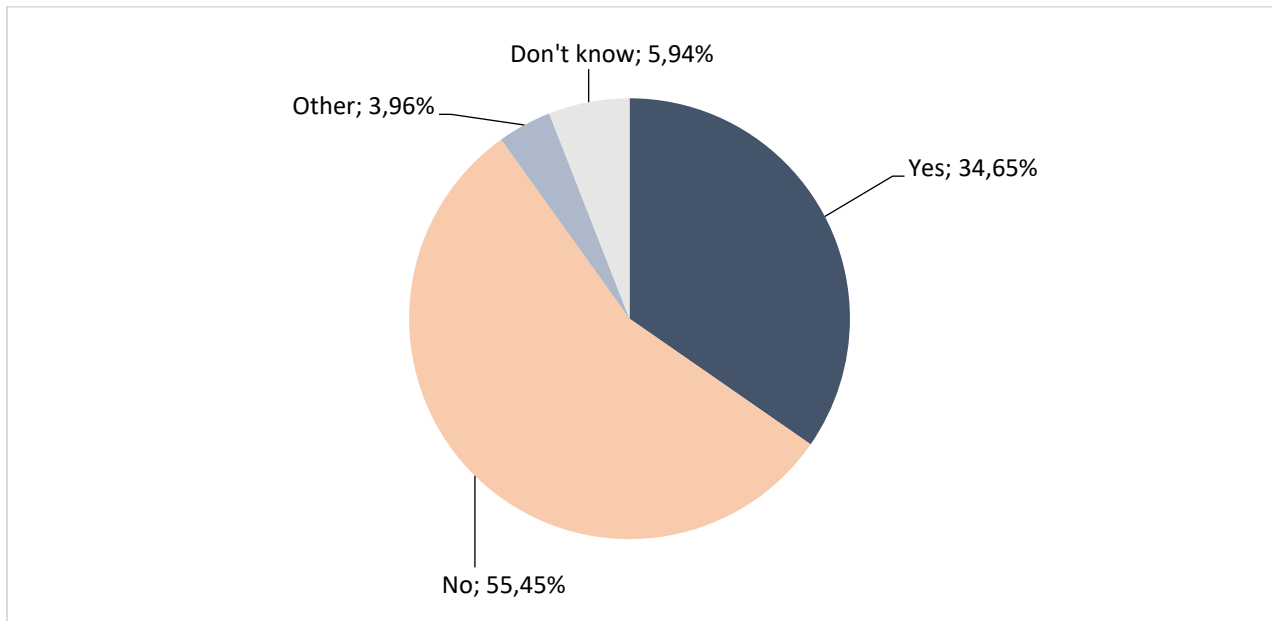


Chart 53: Employees allowed to bring their own IT devices and use these on the organisation's network (%)

Q26: Are employees allowed to use personal USB storage devices to store workplace-related data?

Over 40 % of the organizations does not allow the use of USB storage devices (**Chart 54**). In practice this might mean that the USB ports are not accessible.

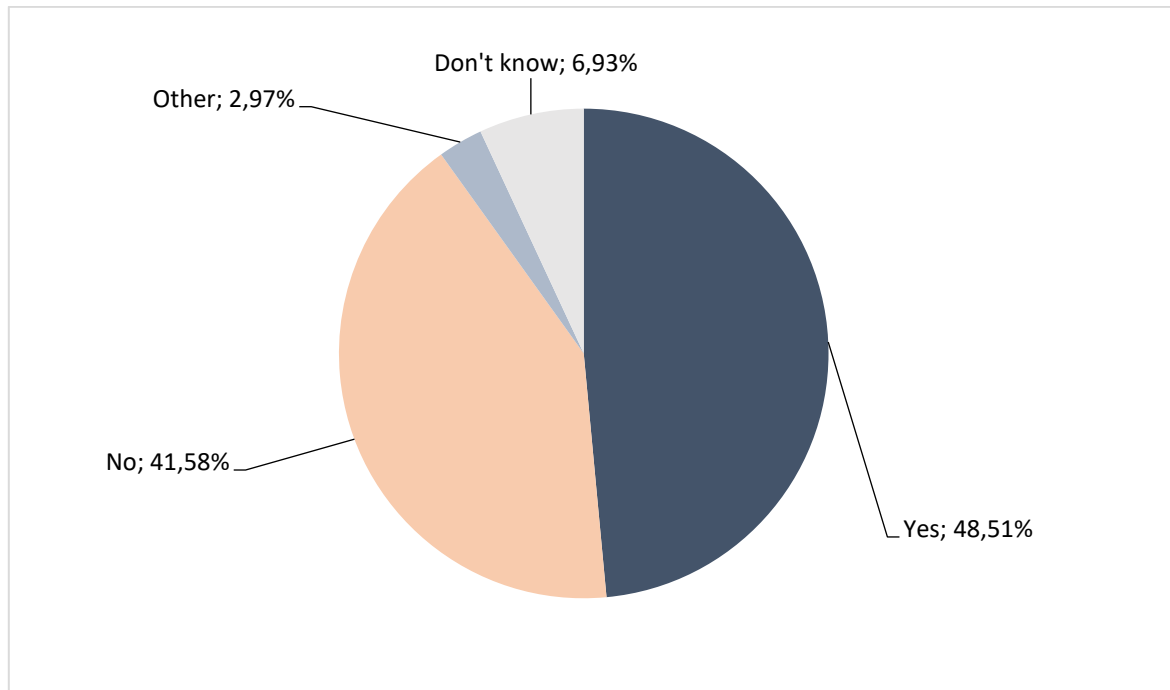


Chart 54: Employees allowed to use personal USB storage devices to store workplace-related data

In hospitals, the number of organizations that allow and do not allow the use of USB storage devices is in balance (**Chart 55**), elderly care organizations in two thirds of the cases allow the use.

Not allowing the unauthorized use of the USB devices is a simple and efficient way of limiting the risks of virus or malware being introduced into the system, as well as potential data leaks. It also provides more transparency in terms of safe and GDPR compliant data handling and tracking.

Technically, this can be done in several ways, ranging from physically disabling access to the USB ports to editing Windows registry.

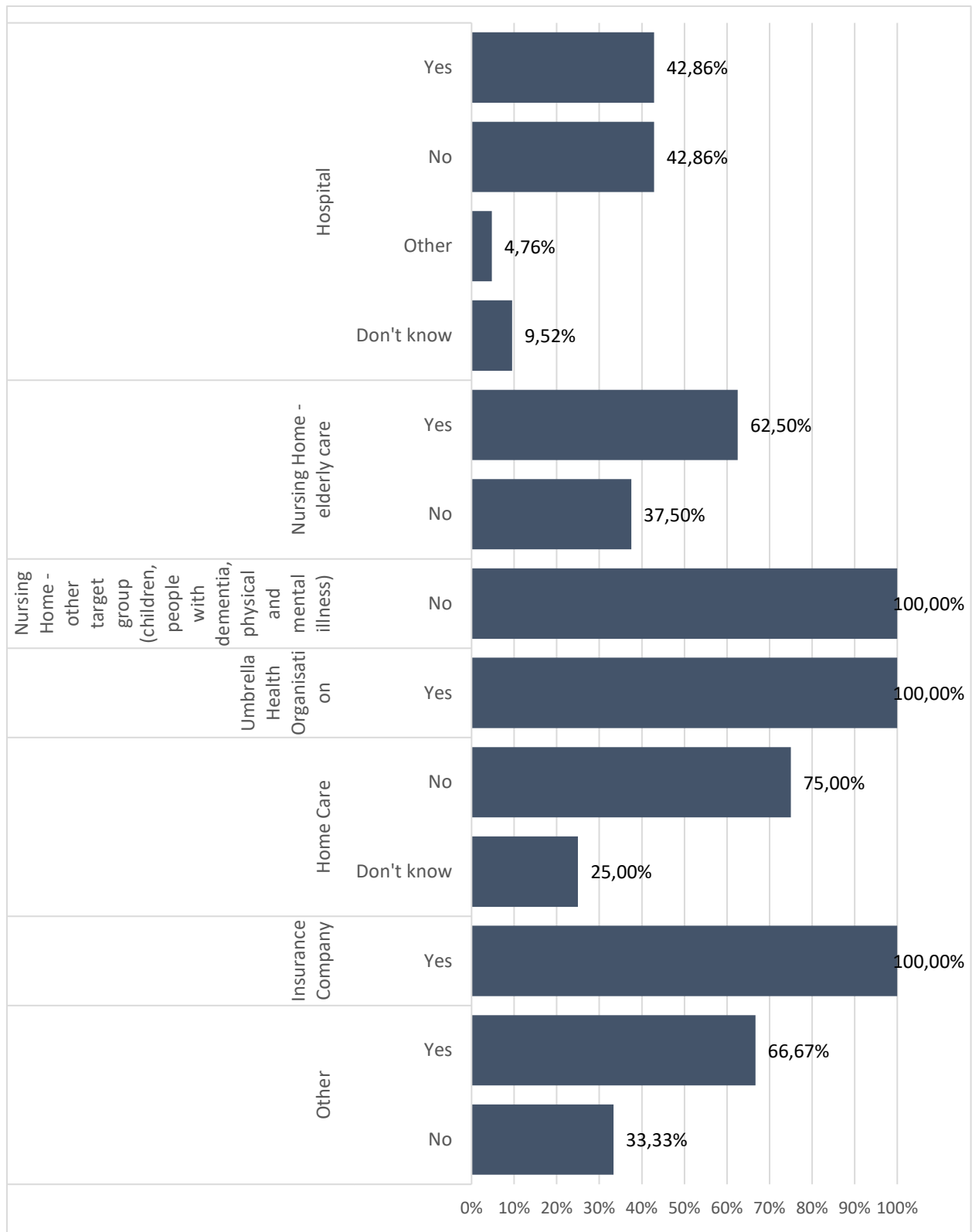


Chart 55: Employees allowed to use personal USB storage devices to store workplace-related data by organization type

Q27: Is sensitive data encrypted when sent outside your network?

Only about a half of the surveyed organizations encrypts sensitive data when they are sent outside the organization (**Chart 56**).

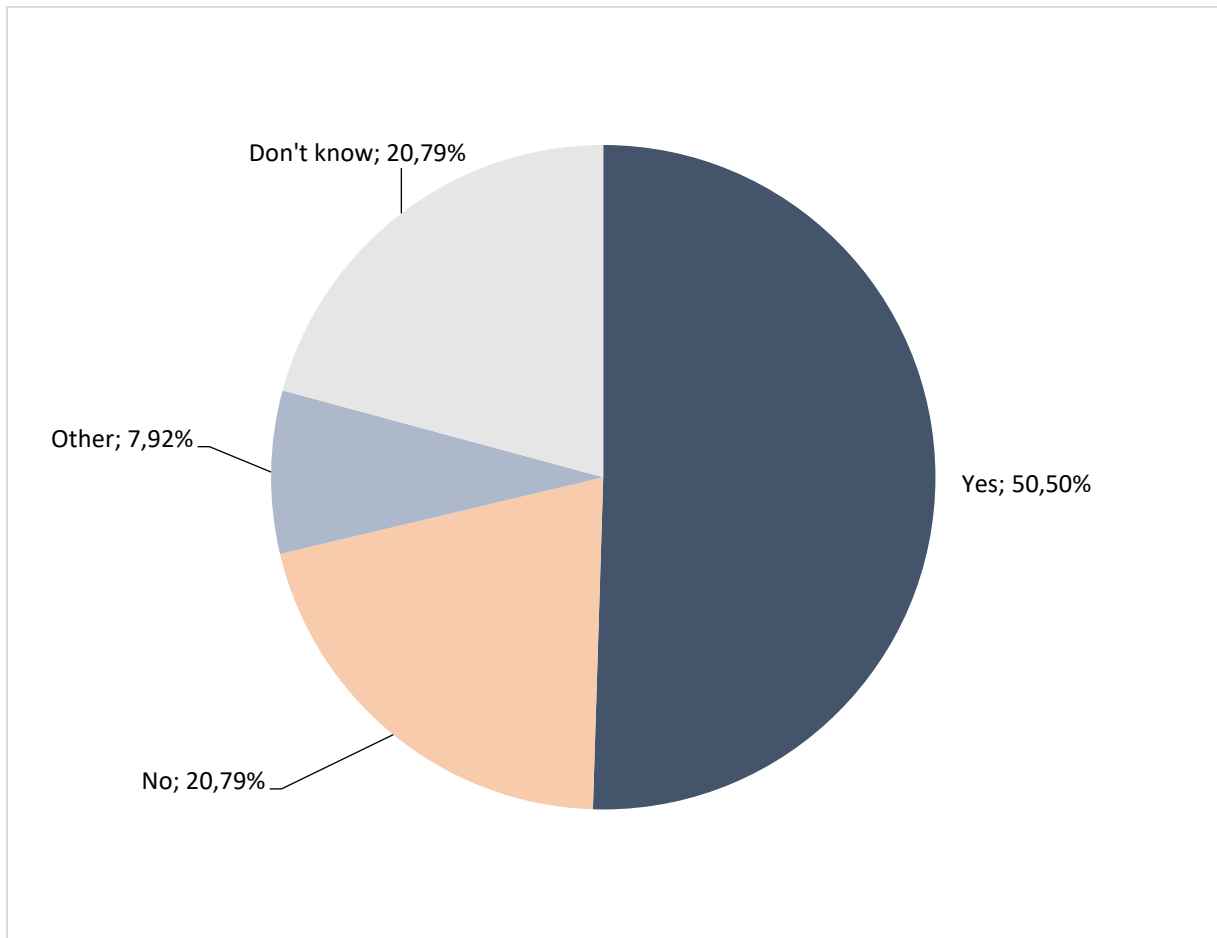


Chart 56: Sensitive data encrypted when sent outside your network

While for everyday general communication and non-sensitive data transfers encryption can add a layer of complexity that hinders productivity of the untrained staff, sensitive data should always be encrypted, when sent outside the internal network.

This query indicates a significant cybersecurity risk in a substantial number of surveyed organizations and represents an area for further detailed investigation.

Q28: Does your organisation have physical back-ups stored off-site?

Two thirds of the surveyed organizations state (**Chart 57**) that they use physical back-ups stored off-site. Such back-up is usually defined as not physically placed inside the organization's core infrastructure and networks. Cloud storage and similar services are considered off-site storage.

Off-site storage usually represents a second layer of safety, in case the reliability, stability and safety are ensured. Back-up frequencies, back-up data management policies, encryptions are just a few examples that go with these back-ups as well. Also, any off-site back up will incur additional, often significant cost.

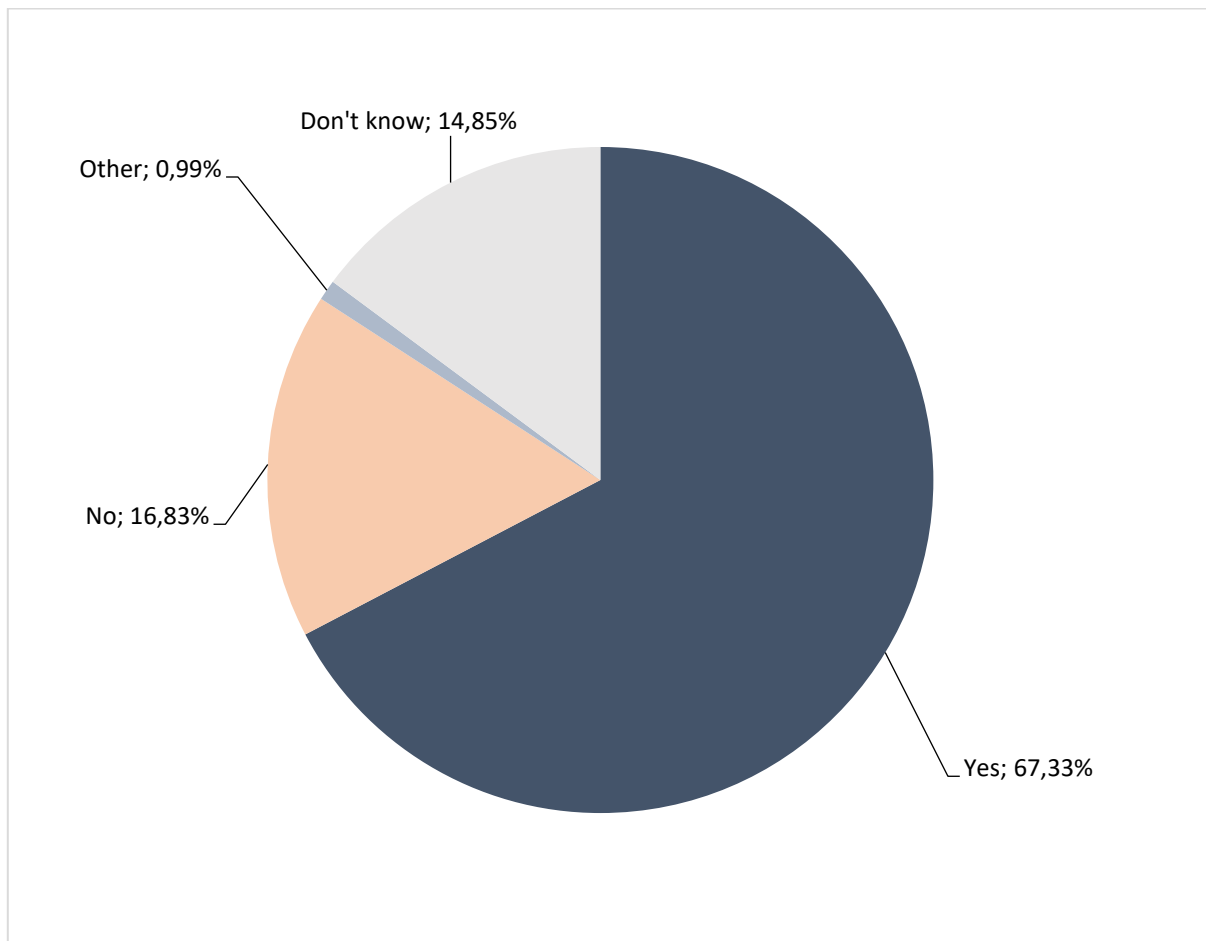


Chart 57: Physical back-ups stored off-site

Almost 17 % of the organizations does not use off-site back-ups, almost 15 % of the respondents do not know. These numbers would need further queries regarding back-ups strategies and policies to draw further conclusions.

This query also indicates a potential for security measure improvements, with regard to ransomware attacks and similar.

Q29: Please estimate the number of individual records currently stored within your owned network?

This query sought to estimate the data records quantity stored on the network. 39 % of the organizations state that they manage over 100 000 individual records, almost all of them are hospitals (*Chart 59*).

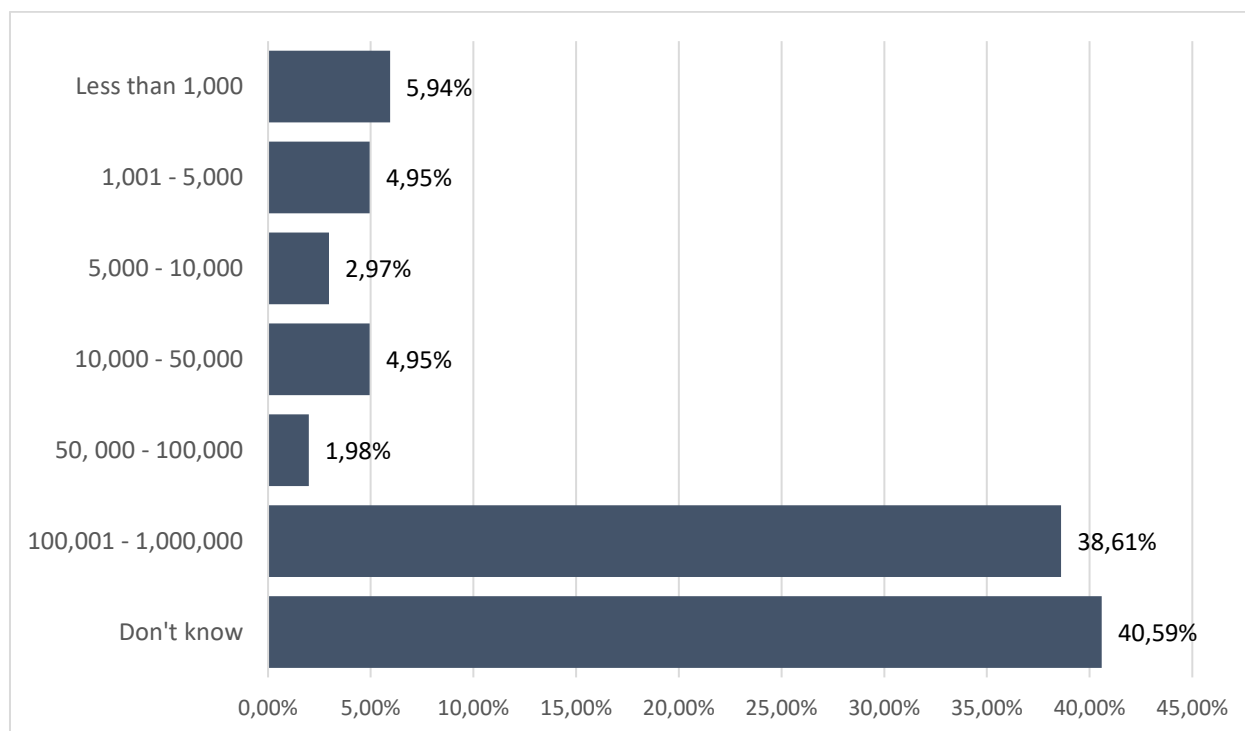


Chart 58: Individual records currently stored within your owned network

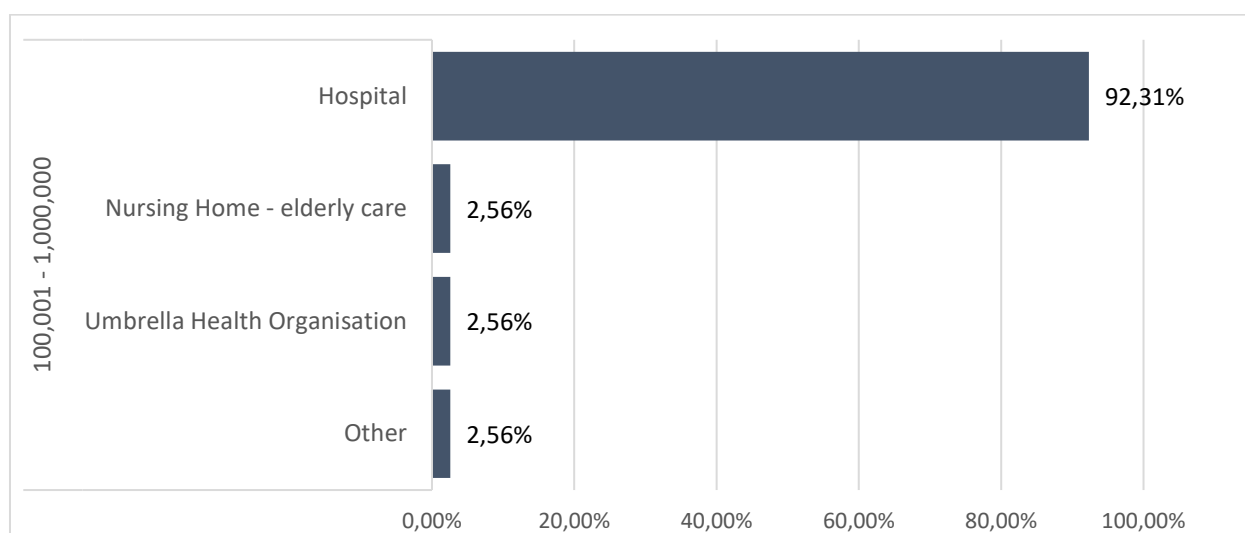


Chart 59: Individual records currently stored within your owned network (% of 100 001 – 1 000 000)

A significant number of the respondents was not sure about the number (41 %). In any case, the sample shows a substantial data management flow.

Q30: Within the last 5 years, have you sustained any of the following options?

Multiple answers were possible for this query. Two thirds of the organizations experienced virus or malicious code attack in the past 5 years, 26 % of organizations experienced data loss of any extent. 15 % reported a hacking incident.

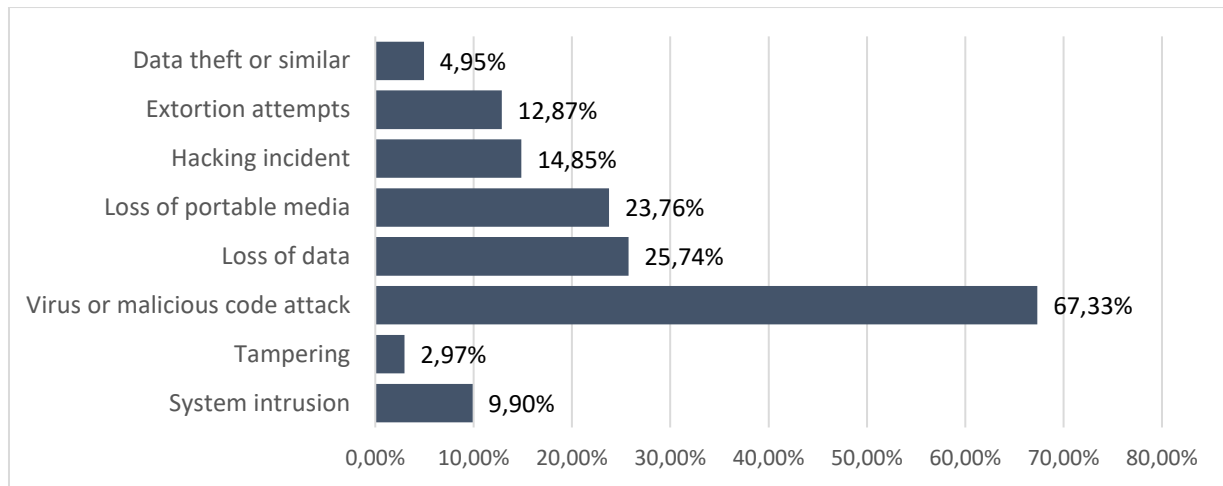


Chart 60: Cybersecurity incidents in the last 5 years

41 hospitals (65 % of hospital respondents) and 12 elderly care nursing homes experienced a virus or malicious code attack in the past 5 years (**Chart 61, Chart 62**).

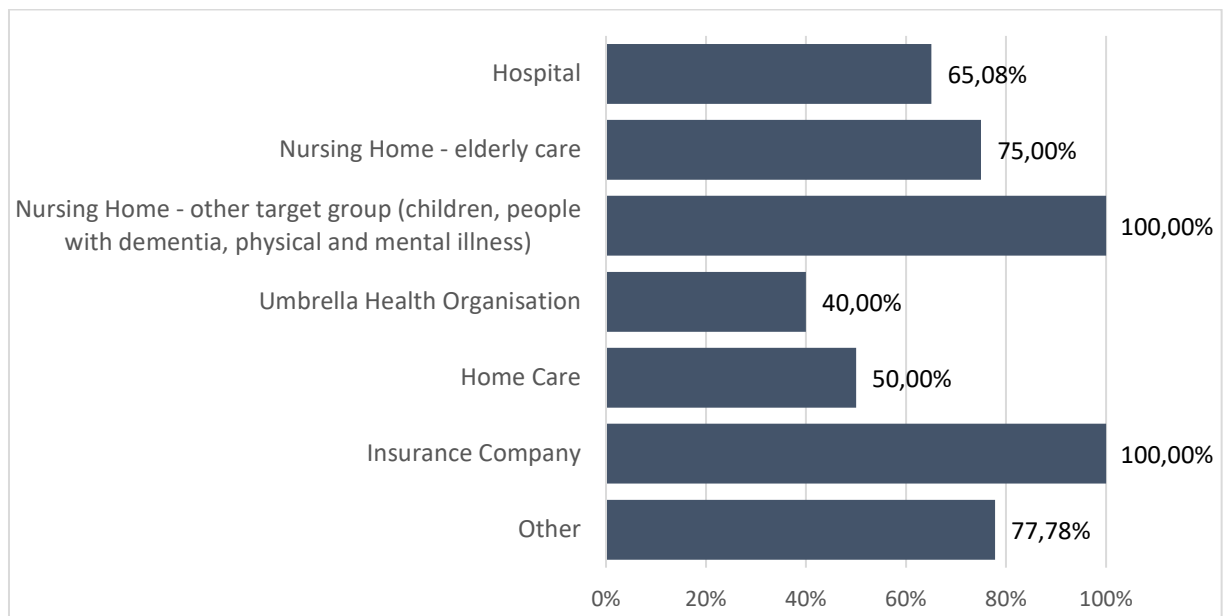


Chart 61: Virus or malicious code attack by organization type

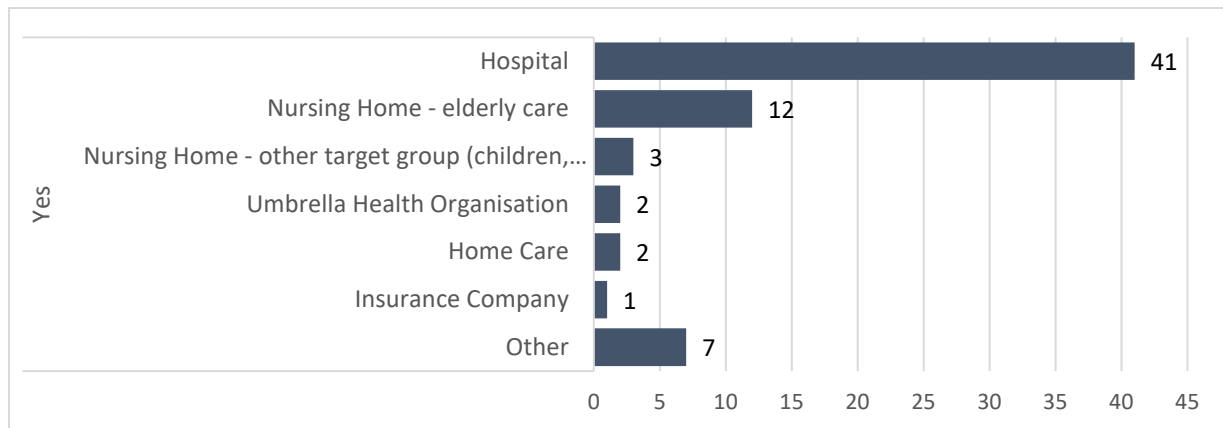


Chart 62: Virus or malicious code attack by organization type

The following chart summarizes the number of incident types occurring in one organization in the last 5 years. 55 respondents reported only 1 type of an incident, a significant number of respondents reported multiple incidents and only 5 respondents out of 101 reported 0 incidents. Thus, almost all organizations in the sample experienced some sort of an incident in the past 5 years.

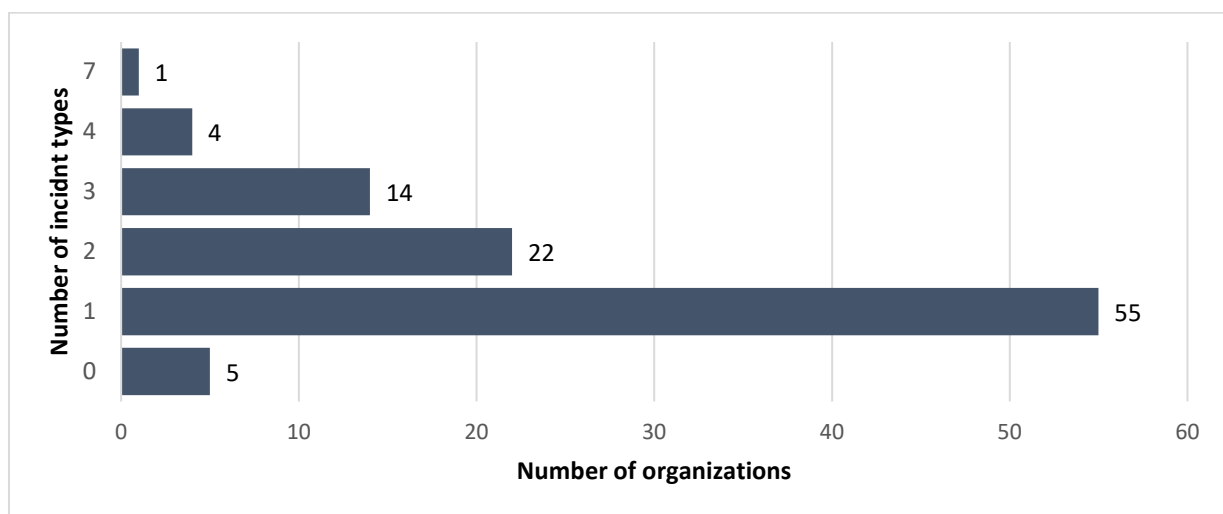
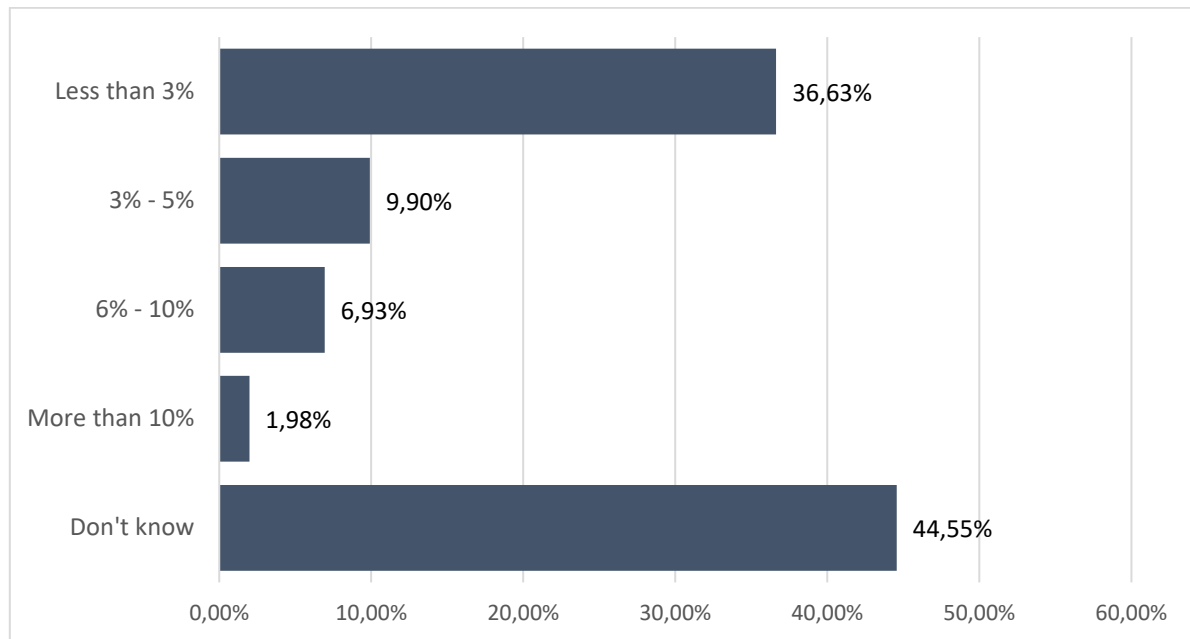
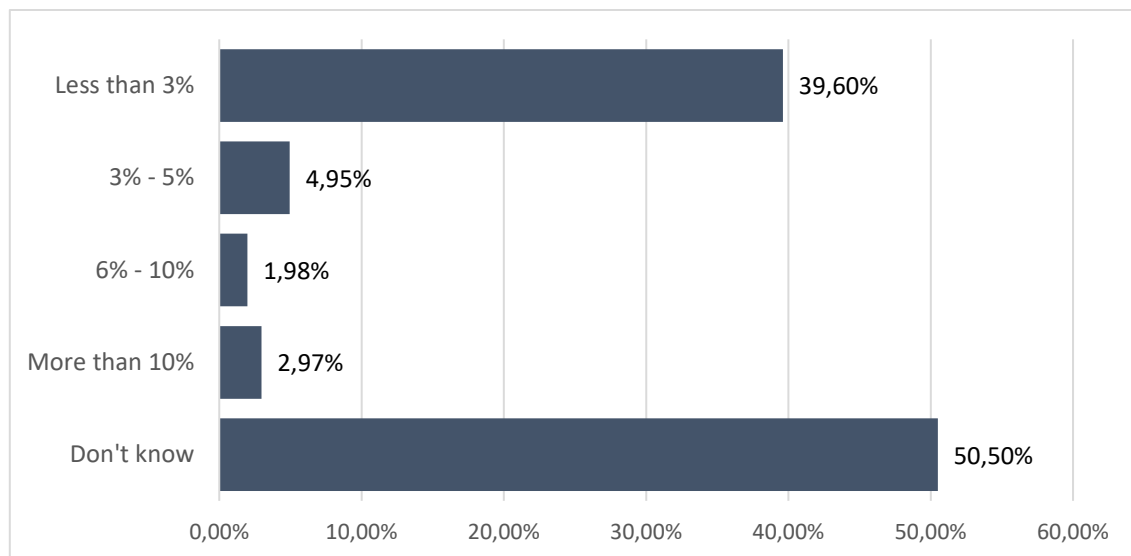


Chart 63: Number of incident types vs number of organizations

Q31: What is the percentage of your organisation's budget allocated to IT?*Chart 64: Percentage of budget allocated to IT***Q32: What is the percentage of your organisation's IT budget allocated to cybersecurity?***Chart 65: Percentage of IT budget allocated to cybersecurity*

The previous two charts demonstrate that in most organizations less than 0,1 % of the total organization budget is spent directly on cybersecurity. While there is no referential framework of the “right” amount to be spent on cybersecurity, given the variety of internal and external risks, this percentage seem very low even for health and social care organizations.

It also needs to be said that the budget allocation is only a quantitative measure that does not provide insights into qualitative indicators – efficiency, impact on productivity, reasonable resources allocation (40-60 % of cybersecurity risks are internal).

4. Conclusion

The survey collected responses from 101 organizations in the domain of health care and social care regarding a range of cybersecurity aspects. The demographics of the survey, as well as cross-referencing the responses leads us to believe that we have collected a valid and representative data sample and the results and conclusions are valid, reflect the cybersecurity landscape of the target group and provide a solid basis for recommendations and further activities.

The Conclusions section is divided into two parts.

Given the substantive extent of the survey questionnaire and a detailed analysis of the results of each query we have prepared a table summary of the main findings of the survey in a simplified format. This table can also become a starting point before looking deeper into the individual queries.

The next part offers several base recommendations. We are aware of the fact that the “care” organizations operate with very limited resources. However, it has to be again re-affirmed that these organizations manage personal, highly sensitive data of the patients, clients as well as staff members and external parties, and every security breach shall be considered as potentially impacting the provision of care. Therefore, we strived to balance those perspectives in the recommendations.

4.1 Survey Summary

SAMPLE CHARACTERISTICS
<ul style="list-style-type: none"> 101 respondents participated in the summary, mostly from Belgium, Spain, Czech Republic, Italy, Austria and the Netherlands. 62.4 % of the respondents represent hospitals, 15.8 % represent elderly care nursing homes, 4 % home care, 3 % nursing homes for other target groups. The rest are mostly service organizations. 54.5 % of the organizations are public, 42.6 % private. 34.7 % respondents were managers, 20.8 % DPOs, 19.8 % IT specialists, 13.9 % health care professionals 38.6 % of surveyed organizations reported that they manage over 100 000 individual records.
CYBERSECURITY & DATA PROTECTION MEASURES AND POLICIES
<ul style="list-style-type: none"> The surveyed organizations spend 3 % of total budget on IT, and 3 % of the IT budget on cybersecurity (i.e. 0.1 % of the total organization budget on cybersecurity) 88.1 % of the surveyed organizations have a Data Protection Officer 83.2 % of the respondents are concerned about cybersecurity Cybersecurity is considered as very important in 64.3 % organizations (very important for 71.4 % of hospitals and only for 31.3 % elderly care nursing homes). 74.2 % of the respondents are aware of the impacts of the cyber-attacks (81 % of hospitals, 56.3 % elderly care nursing homes) 69.3 % of the surveyed organizations have internal cybersecurity staff, only 17.8 % organizations outsource it. Outsourcing is most typical in 1-100 staff organizations. 20.8 % of the respondents interact rarely with the IT department. A half of those are

managers. The rest of the respondents are either a part of the IT department or interact regularly.

- Cybersecurity risk assessments are conducted annually in 19.8 % surveyed organizations, bi-annually in 13.9 % organizations. 22.8 % of organizations conduct the assessment more frequently than annually.
- Only 26.7 % of surveyed organizations were EXTERNALLY penetration tested, these were mostly hospitals. INTERNAL penetration tests were conducted in 30.7 % organizations, again mostly hospitals.
- 63.4 % respondents state that the organization has a data retention and destruction policy, only 11.9 % responded negatively

CYBERSECURITY – TECHNICAL MEASURES

- 74.3 % of the respondents confirm firewall at all external connection points
- 64.4 % of organizations allow remote access to the corporate network, 21.8 % do not allow
- 73.3 % of the organizations have antivirus and firewall and all connecting devices, 8.9 % do not have
- Only 34.7 % of the organizations allows own IT devices on the network
- 48.5 % of the organizations allows USB storage devices, 41.6 % does not allow
- 50.5 % of the organizations state that they encrypt sensitive data when sent outside the internal network, 20 % does not encrypt
- 67 % of the organizations uses off-site physical backup

CYBERSECURITY INCIDENTS

- 55 surveyed organizations experienced 1 type of cybersecurity incident in the past 5 years, 22 organizations experienced 2 types of incident. No incidents were reported by only 5 organizations.
- The most frequent incident type is a virus or a malicious code attack (experienced by 67.3 % of organizations, followed by loss of data (25.7 %). Hacking was experienced by 14.9 % of the surveyed organizations.

CYBERSECURITY TRAINING

- 65.4 % of the surveyed organizations have training departments
- Staff is not trained in privacy and data security in 57.4 % of the surveyed organizations, the training is conducted in 35.6 % organizations.
- There is no mandatory cybersecurity training in 52.5 % of the surveyed organizations, and 1-20 hours per year in 32.7 % of organizations.
- The staff is mostly trained regarding e-mail scams, data management and safe internet habits.
- More than half of the staff is trained in GDPR rules in only 27.7 organizations. Less than 5 % of staff is trained in GDPR rules in 21.8 % of organizations

4.2 Findings and recommendations based on the sample

1. **Cybersecurity needs continuous attention** – most organizations experienced security incidents and cybersecurity is a concern for them – cybersecurity as high priority in the strategic and policy documents of the organizations, under continuous scrutiny.
2. **Increase cybersecurity awareness, especially among social care providers** – the results of the survey indicate that while the cybersecurity is a concern, it needs relevant deeper understanding. The sample data shows that hospitals take the issue more seriously, the social care providers might be underestimating potential impacts – trainings, workshops, the influence of internal role models.
3. **Continue strengthening the role of the Data Protection Officers** – provide further training as needed, empower, promote formal and informal influence within the organization, promote common sense good practice.
4. **Explain the practical importance of GDPR** – mandatory data protection is not an EU enforced rule but a very practical and useful approach – internal and external trainings, examples of practical application.
5. **Increase budget allocation for cybersecurity** - the budget allocation for the cybersecurity is on average very low – only 0.1 % of the total budget. While there is no “magic number”, the needs differentiate, the requirement to protect the sensitive data is not very well reflected in the budget allocation, as well as staff allocation.
6. **Set a cycle (annually, bi-annually) for external penetration testing / cybersecurity audits** – implement into strategic documents and reflect in budgets. Possibly make it a firm budget item.
7. **Train internal IT staff in regular penetration testing and other cybersecurity skills** – provide proper training to the IT staff, have the staff test the infrastructure regularly, but not routinely.
8. **Create a simple procedure for IT and non-IT staff in case a cyberattack is identified** – a simple list of steps that is promoted regularly, explaining clearly the point of contact and the most immediate steps (i.e. shut-down, disconnect from network, contact IT at...)
9. **Review data management and back-up policy vs everyday practice**
10. **Collect feedback from the users regarding the ratio between productivity and cybersecurity**
11. **Increase the coverage of cybersecurity training for non-IT users**

To summarize, cybersecurity needs to become an integral part of the organization’s strategic and policy documents, not as a formality but as good practice. The surveyed sample shows that hospitals might be a small step ahead of the social care organizations in understanding the potential impacts.


Cybersecurity is an ongoing and fluid effort, as new risks and threats emerge relative to the exponential growth and reach of the technology, processing power (Moore’s laws suggest that the processing power doubles every 18 months, however the cycle is much faster and accelerating now), and innovative approaches, such as artificial intelligence.

As data stored in the infrastructure of these institutions is key for the provision of individualized, high quality care, this needs to be regularly reminded to the staff at all levels. External and internal trainings and workshops provide the staff with structured and targeted information and make sure a certain standard of cybersecurity is communicated throughout the organization.

Annex 1

Survey information sheet and consent form

CURRENT PERCEPTIONS AND TRENDS ON
CYBERSECURITY IN HOSPITALS
Load unfinished survey Exit and clear survey



Current perceptions and trends on cybersecurity in hospitals

This questionnaire is being conducted under the framework of the **SecureHospitals.eu** project, a **Coordination and Support Action** funded by the European Commission's H2020 programme under grant agreement no. 826497 and implemented by 12 partners constituting the [research team](#).

The aim of the questionnaire is to acquire a general understanding on the perceptions of healthcare professionals and IT staff on cybersecurity issues with a focus on awareness, training and protection measures. Following this assessment and other research activities, the project will develop tailor-made training packages and offer training sessions for multiple types of stakeholders in different European countries. More information on the project objectives and future activities can be found on the project website www.project.securehospitals.eu.

This questionnaire should take approximately 10-15 minutes to complete. Your participation is entirely **voluntarily**. You are free to leave at any time, without giving reason and without any consequences on you or your future participation in the project. You may withdraw your consent for participation at any time without giving a reason. To do so, simply contact us (see below) and we will delete any responses you have provided.


We do not ask you for your name or any other information that could directly identify you. Nonetheless, we will assign a participant number to your responses in order to analyse and compare them with the responses from other participants. We only collect and process data that is strictly necessary for running the research survey and for our internal project administration. These data will not be shared with or disclosed to anyone outside the research team. **We will analyse your answers and will use aggregated research data for scientific publications and presentations at conferences, workshops and other dissemination purposes.**

If you want to know more about how the SecureHospitals.eu project processes your personal data, please consult our [Data Protection Notice](#).

If you have any questions about this research or your prospective involvement in it, please contact:

Researcher Karel Vostry European Ageing Network info@ean.care	Project Coordinator Stela Shiroka INTERSPREAD GmbH stela.shiroka@interspread.com
--	---

CURRENT PERCEPTIONS AND TRENDS ON
CYBERSECURITY IN HOSPITALS
Resume later Exit and clear survey



0%

Electronic Consent

*
Please select your choice below. You may print a copy of this consent form for your records.

Clicking on the "Agree" button indicates that you, after reading and understanding the information provided in above and in our [Data Protection Notice](#), voluntarily participate in the SecureHospitals.eu survey under the terms as described above and on our website.

Choose one of the following answers

☐ Agree
☐ Disagree

Annex 2

Survey questions

General Questions

[] In which country are you a resident?

Only answer this question if the following conditions are met:

Answer was 'Agree' at question '1 [A000]' (Please select your choice below. You may print a copy of this consent form for your records. Clicking on the "Agree" button indicates that you, after reading and understanding the information provided in above and in our Data Protection Notice, voluntarily participate in the SecureHospitals.eu survey under the terms as described above and on our website.)

Please choose **only one** of the following:

- ☐ Albania
- ☐ Andorra
- ☐ Austria
- ☐ Azerbaijan
- ☐ Belarus
- ☐ Belgium
- ☐ Bosnia and Herzegovina
- ☐ Bulgaria
- ☐ Croatia
- ☐ Cyprus
- ☐ Czech Republic
- ☐ Denmark
- ☐ Finland
- ☐ France
- ☐ Georgia
- ☐ Germany
- ☐ Gibraltar
- ☐ Greece
- ☐ Iceland
- ☐ Ireland
- ☐ Israel
- ☐ Italy
- ☐ Latvia
- ☐ Liechtenstein
- ☐ Lithuania
- ☐ Luxembourg
- ☐ Macedonia (the former Yugoslav Republic of)
- ☐ Malta
- ☐ Moldova (Republic of)
- ☐ Monaco
- ☐ Montenegro
- ☐ Netherlands
- ☐ Norway

- ☐ Poland
- ☐ Portugal
- ☐ Romania
- ☐ Serbia
- ☐ Spain
- ☐ Sweden
- ☐ Switzerland
- ☐ Turkey
- ☐ United Kingdom
- ☐ Other

[] In which type of organisation do you work? *

Only answer this question if the following conditions are met:

Answer was 'Agree' at question '1 [A000]' (Please select your choice below. You may print a copy of this consent form for your records. Clicking on the "Agree" button indicates that you, after reading and understanding the information provided in above and in our Data Protection Notice, voluntarily participate in the SecureHospitals.eu survey under the terms as described above and on our website.)

Please choose **only one** of the following:

- ☐ Hospital
- ☐ Nursing Home - elderly care
- ☐ Nursing Home - other target group (children, people with dementia, physical and mental illness)
- ☐ Home Care
- ☐ Insurance Company
- ☐ Umbrella Health Organisation
- ☐ Other

[] What type is your organisation? *

Only answer this question if the following conditions are met:

Answer was 'Agree' at question '1 [A000]' (Please select your choice below. You may print a copy of this consent form for your records. Clicking on the "Agree" button indicates that you, after reading and understanding the information provided in above and in our Data Protection Notice, voluntarily participate in the SecureHospitals.eu survey under the terms as described above and on our website.)

Please choose **only one** of the following:

- ☐ Public
- ☐ Private
- ☐ Other

[] What is your role in the organisation? *

Only answer this question if the following conditions are met:

Answer was 'Agree' at question '1 [A000]' (Please select your choice below. You may print a copy of this consent form for your records. Clicking on the "Agree" button indicates that you, after reading and understanding the information provided in above and in our Data Protection Notice, voluntarily participate in the SecureHospitals.eu survey under the terms as described above and on our website.)

Please choose **only one** of the following:

- ☐ Management
- ☐ IT Specialist
- ☐ Trainer in data security
- ☐ Healthcare professional
- ☐ Social Worker
- ☐ Data Protection Officer (DPO)
- ☐ Other

Staff Training and Awareness

[] Do you have a Data Protection Officer or someone in charge of Data Security at your organisation? *

Only answer this question if the following conditions are met:

Answer was 'Agree' at question '1 [A000]' (Please select your choice below. You may print a copy of this consent form for your records. Clicking on the "Agree" button indicates that you, after reading and understanding the information provided in above and in our Data Protection Notice, voluntarily participate in the SecureHospitals.eu survey under the terms as described above and on our website.)

Please choose **only one** of the following:

- ☐ Yes
- ☐ No
- ☐ Don't know

[] What is the number of staff working at your organisation who use IT devices regularly or rarely? *

Only answer this question if the following conditions are met:

Answer was 'Agree' at question '1 [A000]' (Please select your choice below. You may print a copy of this consent form for your records. Clicking on the "Agree" button indicates that you, after reading and understanding the information provided in above and in our Data Protection Notice, voluntarily participate in the SecureHospitals.eu survey under the terms as described above and on our website.)

Please choose **only one** of the following:

- ☐ 1-100
- ☐ 100-500
- ☐ 500 and more
- ☐ Don't know
- ☐ Other

[] How is the relation of the cybersecurity responsible in your organisation? *

Only answer this question if the following conditions are met:

Answer was 'Agree' at question '1 [A000]' (Please select your choice below. You may print a copy of this consent form for your records. Clicking on the "Agree" button indicates that you, after reading and understanding the information provided in above and in our Data Protection Notice, voluntarily participate in the SecureHospitals.eu survey under the terms as described above and on our website.)

Please choose **only one** of the following:

- ☐ Own staff
- ☐ Outsourced
- ☐ Don't know
- ☐ Other

[] What is the ratio of staff responsible for cybersecurity to those who use IT devices at your organisation? *

Only answer this question if the following conditions are met:

Answer was 'Agree' at question '1 [A000]' (Please select your choice below. You may print a copy of this consent form for your records. Clicking on the "Agree" button indicates that you, after reading and understanding the information provided in above and in our Data Protection Notice, voluntarily participate in the SecureHospitals.eu survey under the terms as described above and on our website.)

Please choose **only one** of the following:

- ☐ 1:10
☐ 1:50
☐ 1:100
☐ 1:500
☐ More than 1:500
☐ Don't know
☐ Other

[]Are all employees trained and assessed in privacy and data security related matters (such as phishing, identity theft, social media and mobile devices) on at least an annual basis? *

Only answer this question if the following conditions are met:

Answer was 'Agree' at question '1 [A000]' (Please select your choice below. You may print a copy of this consent form for your records. Clicking on the "Agree" button indicates that you, after reading and understanding the information provided in above and in our Data Protection Notice, voluntarily participate in the SecureHospitals.eu survey under the terms as described above and on our website.)

Please choose **only one** of the following:

- ☐ Yes
☐ No
☐ Don't know
☐ Other

[]What is the percentage of your staff trained in GDPR rules? *

Only answer this question if the following conditions are met:

Answer was 'Agree' at question '1 [A000]' (Please select your choice below. You may print a copy of this consent form for your records. Clicking on the "Agree" button indicates that you, after reading and understanding the information provided in above and in our Data Protection Notice, voluntarily participate in the SecureHospitals.eu survey under the terms as described above and on our website.)

Please choose **only one** of the following:

- ☐ 1% - 5%
☐ 6% - 15%
☐ 16% - 30%
☐ 31% - 50%
☐ 51% - 99%
☐ 100%
☐ Don't know
☐ Other

[]In which topics is the staff of your organisation regularly trained? *

Only answer this question if the following conditions are met:

Answer was 'Agree' at question '1 [A000]' (Please select your choice below. You may print a copy of this consent form for your records. Clicking on the "Agree" button indicates that you, after reading and understanding the information provided in above and in our Data Protection Notice, voluntarily participate in the SecureHospitals.eu survey under the terms as described above and on our website.)

Please choose **all** that apply:

- ☐ Clean Desk Policy
☐ Bring-Your-Own-Device (BYOD) Policy

- ☐ Data Management
- ☐ Removable Media
- ☐ Safe Internet Habits
- ☐ Physical Security and Environmental Controls
- ☐ Social Networking Dangers
- ☐ E-Mail Scams
- ☐ Malware
- ☐ Hoaxes
- ☐ Other:

[] Does your organisation have an education/training department? *

Only answer this question if the following conditions are met:

Answer was 'Agree' at question '1 [A000]' (Please select your choice below. You may print a copy of this consent form for your records. Clicking on the "Agree" button indicates that you, after reading and understanding the information provided in above and in our Data Protection Notice, voluntarily participate in the SecureHospitals.eu survey under the terms as described above and on our website.)

Please choose **only one** of the following:

- ☐ Yes
- ☐ No
- ☐ Don't know

[] How many hours of education/training in cybersecurity are mandatory at your organisation? *

Only answer this question if the following conditions are met:

Answer was 'Agree' at question '1 [A000]' (Please select your choice below. You may print a copy of this consent form for your records. Clicking on the "Agree" button indicates that you, after reading and understanding the information provided in above and in our Data Protection Notice, voluntarily participate in the SecureHospitals.eu survey under the terms as described above and on our website.)

Please choose **only one** of the following:

- ☐ None
- ☐ 1-20 hours/year
- ☐ More than 20 hours/year
- ☐ Don't know
- ☐ Other

Risk Assessment

[]How often do you use a computer? *

Only answer this question if the following conditions are met:

Answer was 'Agree' at question '1 [A000]' (Please select your choice below. You may print a copy of this consent form for your records. Clicking on the "Agree" button indicates that you, after reading and understanding the information provided in above and in our Data Protection Notice, voluntarily participate in the SecureHospitals.eu survey under the terms as described above and on our website.)

Please choose **only one** of the following:

☐ All the time

☐ Daily

☐ Weekly

☐ Never

☐ Other

[]How often do you manage personal data (i.e. of patient, clients)? *

Only answer this question if the following conditions are met:

Answer was 'Agree' at question '1 [A000]' (Please select your choice below. You may print a copy of this consent form for your records. Clicking on the "Agree" button indicates that you, after reading and understanding the information provided in above and in our Data Protection Notice, voluntarily participate in the SecureHospitals.eu survey under the terms as described above and on our website.)

Please choose **only one** of the following:

☐ All the time

☐ Daily

☐ Weekly

☐ Never

☐ Other

[]Are you concerned about cybersecurity? *

Only answer this question if the following conditions are met:

Answer was 'Agree' at question '1 [A000]' (Please select your choice below. You may print a copy of this consent form for your records. Clicking on the "Agree" button indicates that you, after reading and understanding the information provided in above and in our Data Protection Notice, voluntarily participate in the SecureHospitals.eu survey under the terms as described above and on our website.)

Please choose **only one** of the following:

☐ Yes

☐ No

☐ Don't know

☐ Other

[]Do you know the potential impacts of a cybersecurity attack? If yes, which impacts do you think a cyberattack can have to your organisation? *

Only answer this question if the following conditions are met:

Answer was 'Agree' at question '1 [A000]' (Please select your choice below. You may print a copy of this consent form for your records. Clicking on the "Agree" button indicates that you, after reading and understanding the information provided in above and in our Data Protection Notice, voluntarily participate in the SecureHospitals.eu survey under the terms as described above and on our website.)

Please choose **only one** of the following:

- ☐ Yes
- ☐ No
- ☐ Don't know

Make a comment on your choice here:

[]How important do you think is cybersecurity for your organisation? *

Only answer this question if the following conditions are met:

Answer was 'Agree' at question '1 [A000]' (Please select your choice below. You may print a copy of this consent form for your records. Clicking on the "Agree" button indicates that you, after reading and understanding the information provided in above and in our Data Protection Notice, voluntarily participate in the SecureHospitals.eu survey under the terms as described above and on our website.)

Please choose **only one** of the following:

- ☐ Not so important
- ☐ Important
- ☐ Very important
- ☐ Don't know

[]Do you interact with your organisation's IT department? *

Only answer this question if the following conditions are met:

Answer was 'Agree' at question '1 [A000]' (Please select your choice below. You may print a copy of this consent form for your records. Clicking on the "Agree" button indicates that you, after reading and understanding the information provided in above and in our Data Protection Notice, voluntarily participate in the SecureHospitals.eu survey under the terms as described above and on our website.)

Please choose **only one** of the following:

- ☐ Yes, I'm part of it
- ☐ Regularly
- ☐ Rarely
- ☐ Never
- ☐ Don't know
- ☐ Other

[]When you have cybersecurity concerns, who do you contact what do you do? *

Only answer this question if the following conditions are met:

Answer was 'Agree' at question '1 [A000]' (Please select your choice below. You may print a copy of this consent form for your records. Clicking on the "Agree" button indicates that you, after reading and understanding the information provided in above and in our Data Protection Notice, voluntarily participate in the SecureHospitals.eu survey under the terms as described above and on our website.)

Please choose **all** that apply:

- ☐ I solve it on my own
- ☐ I contact the IT department
- ☐ I check on the internet
- ☐ I enrol in training courses
- ☐ Nothing
- ☐ Other:

[]How frequently are cybersecurity risk assessments conducted at your organisation? *

Only answer this question if the following conditions are met:

Answer was 'Agree' at question '1 [A000]' (Please select your choice below. You may print a copy of this consent form for your records. Clicking on the "Agree" button indicates that you, after reading and understanding the information provided in above and in our Data Protection Notice, voluntarily participate in the SecureHospitals.eu survey under the terms as described above and on our website.)

Please choose **only one** of the following:

- ☐ Daily
- ☐ Once a month
- ☐ Once a quarter
- ☐ Once a half-year
- ☐ Once a year
- ☐ Every two years or less frequent
- ☐ No security risk assessments
- ☐ Don't know
- ☐ Other

[]Are all users required to change passwords on at least a quarterly basis and instructed to use at least six characters with a combination of lowercase, uppercase, digits and symbols? *

Only answer this question if the following conditions are met:

Answer was 'Agree' at question '1 [A000]' (Please select your choice below. You may print a copy of this consent form for your records. Clicking on the "Agree" button indicates that you, after reading and understanding the information provided in above and in our Data Protection Notice, voluntarily participate in the SecureHospitals.eu survey under the terms as described above and on our website.)

Please choose **only one** of the following:

- ☐ Yes
- ☐ No
- ☐ Don't know
- ☐ Other

[]Has your network been EXTERNALLY assessed/penetration tested in the past year? *

Only answer this question if the following conditions are met:

Answer was 'Agree' at question '1 [A000]' (Please select your choice below. You may print a copy of this consent form for your records. Clicking on the "Agree" button indicates that you, after reading and understanding the information provided in above and in our Data Protection Notice, voluntarily participate in the SecureHospitals.eu survey under the terms as described above and on our website.)

Please choose **only one** of the following:

- ☐ Yes

- ☐ No
- ☐ Don't know
- ☐ Other

[]Has your network been INTERNALLY assessed/penetration tested in the last year? *

Only answer this question if the following conditions are met:

Answer was 'Agree' at question '1 [A000]' (Please select your choice below. You may print a copy of this consent form for your records. Clicking on the "Agree" button indicates that you, after reading and understanding the information provided in above and in our Data Protection Notice, voluntarily participate in the SecureHospitals.eu survey under the terms as described above and on our website.)

Please choose **only one** of the following:

- ☐ Yes
- ☐ No
- ☐ Don't know
- ☐ Other

[]Do you have a data retention & destruction policy? *

Only answer this question if the following conditions are met:

Answer was 'Agree' at question '1 [A000]' (Please select your choice below. You may print a copy of this consent form for your records. Clicking on the "Agree" button indicates that you, after reading and understanding the information provided in above and in our Data Protection Notice, voluntarily participate in the SecureHospitals.eu survey under the terms as described above and on our website.)

Please choose **only one** of the following:

- ☐ Yes
- ☐ No
- ☐ Don't know
- ☐ Other

[]Are firewalls in place at all external connection points? *

Only answer this question if the following conditions are met:

Answer was 'Agree' at question '1 [A000]' (Please select your choice below. You may print a copy of this consent form for your records. Clicking on the "Agree" button indicates that you, after reading and understanding the information provided in above and in our Data Protection Notice, voluntarily participate in the SecureHospitals.eu survey under the terms as described above and on our website.)

Please choose **only one** of the following:

- ☐ Yes
- ☐ No
- ☐ Don't know
- ☐ Other

[]Do you allow remote access to your corporate network? *

Only answer this question if the following conditions are met:

Answer was 'Agree' at question '1 [A000]' (Please select your choice below. You may print a copy of this consent form for your records. Clicking on the "Agree" button indicates that you, after reading and understanding the information provided in above and in our Data Protection Notice, voluntarily participate in the SecureHospitals.eu survey under the terms as described above and on our website.)

Please choose **only one** of the following:

- ☐ Yes

- ☐ No
- ☐ Don't know
- ☐ Other

[]Are all connecting devices required to have anti-virus and firewall installed in accordance with your organisation's policy for updates and patching? *

Only answer this question if the following conditions are met:

Answer was 'Agree' at question '1 [A000]' (Please select your choice below. You may print a copy of this consent form for your records. Clicking on the "Agree" button indicates that you, after reading and understanding the information provided in above and in our Data Protection Notice, voluntarily participate in the SecureHospitals.eu survey under the terms as described above and on our website.)

Please choose **only one** of the following:

- ☐ Yes
- ☐ No
- ☐ Don't know
- ☐ Other

[]Are employees allowed to bring their own IT devices and use these on the organisation's network? *

Only answer this question if the following conditions are met:

Answer was 'Agree' at question '1 [A000]' (Please select your choice below. You may print a copy of this consent form for your records. Clicking on the "Agree" button indicates that you, after reading and understanding the information provided in above and in our Data Protection Notice, voluntarily participate in the SecureHospitals.eu survey under the terms as described above and on our website.)

Please choose **only one** of the following:

- ☐ Yes
- ☐ No
- ☐ Don't know
- ☐ Other

[]Are employees allowed to use personal USB storage devices to store workplace-related data? *

Only answer this question if the following conditions are met:

Answer was 'Agree' at question '1 [A000]' (Please select your choice below. You may print a copy of this consent form for your records. Clicking on the "Agree" button indicates that you, after reading and understanding the information provided in above and in our Data Protection Notice, voluntarily participate in the SecureHospitals.eu survey under the terms as described above and on our website.)

Please choose **only one** of the following:

- ☐ Yes
- ☐ No
- ☐ Don't know
- ☐ Other

[]Is sensitive data encrypted when sent outside your network? *

Only answer this question if the following conditions are met:

Answer was 'Agree' at question '1 [A000]' (Please select your choice below. You may print a copy of this consent form for your records. Clicking on the "Agree" button indicates that you, after reading and understanding the information provided in above and in our Data Protection Notice, voluntarily participate in the SecureHospitals.eu survey under the terms as described above and on our website.)

Please choose **only one** of the following:

- ☐ Yes
- ☐ No
- ☐ Don't know
- ☐ Other

[] Does your organisation have physical back-ups stored off-site? *

Only answer this question if the following conditions are met:

Answer was 'Agree' at question '1 [A000]' (Please select your choice below. You may print a copy of this consent form for your records. Clicking on the "Agree" button indicates that you, after reading and understanding the information provided in above and in our Data Protection Notice, voluntarily participate in the SecureHospitals.eu survey under the terms as described above and on our website.)

Please choose **only one** of the following:

- ☐ Yes
- ☐ No
- ☐ Don't know
- ☐ Other

[] Please estimate the number of individual records currently stored within your owned network? *

Only answer this question if the following conditions are met:

Answer was 'Agree' at question '1 [A000]' (Please select your choice below. You may print a copy of this consent form for your records. Clicking on the "Agree" button indicates that you, after reading and understanding the information provided in above and in our Data Protection Notice, voluntarily participate in the SecureHospitals.eu survey under the terms as described above and on our website.)

Please choose **only one** of the following:

- ☐ Less than 1,000
- ☐ 1,001 - 5,000
- ☐ 5,000 - 10,000
- ☐ 10,000 - 50,000
- ☐ 50,000 - 100,000
- ☐ 100,001 - 1,000,000
- ☐ Don't know

[] Within the last 5 years, have you sustained any of the following options? If yes please provide details and remediation work which has been undertaken. *

Only answer this question if the following conditions are met:

Answer was 'Agree' at question '1 [A000]' (Please select your choice below. You may print a copy of this consent form for your records. Clicking on the "Agree" button indicates that you, after reading and understanding the information provided in above and in our Data Protection Notice, voluntarily participate in the SecureHospitals.eu survey under the terms as described above and on our website.)

Please choose **all** that apply:

- ☐ System's intrusion
- ☐ Tampering
- ☐ Virus or malicious code attack
- ☐ Loss of data
- ☐ Loss of portable media

- ☐ Hacking incident
- ☐ Extortion attempts
- ☐ Data theft or similar

[]What is the percentage of your organisation's budget allocated to IT? *

Only answer this question if the following conditions are met:

Answer was 'Agree' at question '1 [A000]' (Please select your choice below. You may print a copy of this consent form for your records. Clicking on the "Agree" button indicates that you, after reading and understanding the information provided in above and in our Data Protection Notice, voluntarily participate in the SecureHospitals.eu survey under the terms as described above and on our website.)

Please choose **only one** of the following:

- ☐ Less than 3%
- ☐ 3% - 5%
- ☐ 6% - 10%
- ☐ More than 10%
- ☐ Don't know
- ☐ Other

[]What is the percentage of your organisation's IT budget allocated to cybersecurity? *

Only answer this question if the following conditions are met:

Answer was 'Agree' at question '1 [A000]' (Please select your choice below. You may print a copy of this consent form for your records. Clicking on the "Agree" button indicates that you, after reading and understanding the information provided in above and in our Data Protection Notice, voluntarily participate in the SecureHospitals.eu survey under the terms as described above and on our website.)

Please choose **only one** of the following:

- ☐ Less than 3%
- ☐ 3% - 5%
- ☐ 6% - 10%
- ☐ More than 10%
- ☐ Don't know
- ☐ Other

Thank you for your participation or interest!

The survey results will be published soon through all our communication channels.

If you want to receive information on the survey results, future research, training and awareness raising activities, please subscribe to our newsletter [here](#).

By subscribing to our newsletter, you give us the right to inform you about our project updates and to contact you with training opportunities, such as workshops, webinars and summer schools. You may withdraw your subscription to our newsletter at any time by clicking 'unsubscribe' on the e-Mail you receive or by sending us an e-Mail directly.

Our additional communication channels to remain informed on future publications and training and awareness raising activities in different European countries, are:

- www.project.securehospitals.eu
- www.twitter.com/SecureHospitals
- www.facebook.com/SecureHospitals.eu

If you have questions or comments regarding this survey, future research or the project in general, do not hesitate to contact us: stela.shiroka@interspread.com

Submit your survey.
Thank you for completing this survey.