BYOD SECURITY AND CORPORATE ENVIRONMENT: A SURVEY AMONG PROFESSIONALS

by
DIMITRIOS KYRITSIS

Thesis Submitted in Partial Fulfillment of the
Requirements for the Degree of
Master of Science

in
Digital Systems Security

Under the supervision of Professor CHRISTOS XENAKIS

MAY 30, 2023

UNIVERSITY OF PIRAEUS, DEPARTMENT OF DIGITAL SYSTEMS
POSTGRATUATE PROGRAMME “DIGITAL SYSTEMS SECURITY”

ACKNOWLEDGEMENTS

I would first like to thank my thesis advisor, PhD candidate Aristeidis Farao of the School of Information and Communication Technologies, at the Department of Digital Systems of the University of Piraeus. He was always available to answer my questions, and he consistently steered me in the right direction from the beginning until the completion of this thesis.

I would also like to express my gratitude to my Professor Christos Xenakis who gave me the opportunity to write this thesis on the topic of BYOD and supported me during the difficult period of its accomplishment. I benefited enormously from his excellence as a professor and as a researcher.

Finally, I want to express my gratitude to my family and to my partner Livia for providing me with unfailing support and continuous encouragement during these two years of study and through the process of researching and writing this thesis. This accomplishment would not have been possible without you. Thank you!

Author
Dimitrios Kyritsis

Table of Contents

Table of Figures

Tables

1 Introduction

1.1 Problem and Motivation

In recent years, in various organizations and companies around the world, more and more employees are allowed to use personally owned devices rather than corporate ones to perform their tasks. By personally owned devices we mean smartphones, tablets and laptops with which they can check their emails, attend calls and virtual meetings and perform their everyday tasks. This specific way of working is called Bring Your Own Device (BYOD) and has become a trend in recent years. Many organizations use it in the workplace, where it refers to a policy of permitting employees to bring their devices and use them to access privileged company information and applications [1]. The growing trend of BYOD has many benefits, including:

- **Satisfaction** – Employees tend to be satisfied when using their own devices and the reason is that they had chosen to own these devices, and they feel comfortable when using them [1].

- **Increased employee productivity** - Employees feel comfortable when using their own devices so they can work more efficiently and get tasks done faster. This increased efficiency can lead to getting more work done in less time, which is obviously a huge advantage for employers [2].

- **Flexibility** – Employees who work with BYOD can perform their tasks anywhere without the need to use company-owned tools to access corporate documents and files. This level of convenience also removes the need to email copies of documents back and forth to be stored in corporate devices after working on them from home [2].

- **Reduced costs** – When the employees use their devices, they also pay for most, or all of the costs for the hardware, voice or data services, and other associated expenses. This results in companies saving a lot of money [1].

However, apart from the above advantages, the use of BYOD has as result some serious risks for the respective organizations. These risks mainly concern the security of sensitive corporate data and the monitoring of personal user devices and include:

- **Stolen or hacked devices -** The personal device of an employee can be stolen or hacked by malicious users who might want to harm an organization. Subsequently, these malicious users can retrieve unsecured data from this device including sensitive corporate data [21].

- **Poor security –** The personal device of the employee may not follow the organization's security policy. Additionally, it may not be equipped with the appropriate security software [2].

- **End node problem -** BYOD security relates strongly to the end node problem, whereby a device is used to access both sensitive and risky networks and services; risk-averse organizations issue devices specifically for Internet use (termed Inverse-BYOD) [22].

- **Complex control and management of employees' personal devices** - Organizations need an efficient inventory management system that keeps track of the devices employees are using, where the device is located, whether it is being used, and what software it is equipped with [23].

- **Complex monitoring of employees' personal devices** - IT security departments wishing to monitor usage of personal devices must ensure that they monitor only activities that are work-related or access company data or information [23].

The preceding risks make cybersecurity awareness necessary for both employees and organizations when the use of BYOD is allowed.

1.2 Contribution

In this research our goal is to examine BYOD users' cybersecurity awareness and behavior. Consequently, we conducted a survey asking relevant questions in a sample of 80 employees who were allowed to use BYOD in their organizations. The questions of the survey were based on BYOD guidelines retrieved from the work of Souppaya et al. [3]. The results helped us draw useful conclusions regarding the cybersecurity awareness of both the employees and their organizations. More specifically our survey tries to answer the following three research questions:

R1 Are BYOD users careful when using their personal laptop devices in their organizations?

R2 Are BYOD users aware of the security measures implied on them by their organizations?

R3 Do organizations implement the appropriate levels of security when they allow BYOD?

The scope includes only users who use their personal laptops at work. The participants who use corporate devices are excluded from this survey. The structure of this document is as follows: in Section 2 we summarize the related work and previous similar studies, while in Section 3 we outline the survey methodology. Next, in Section 4 we present the descriptive statistics results, while the inferential statistics results are presented in Section 5. In section 6 we discuss the limitations of the study. Finally, in the last two Sections we provide a discussion and analysis of the results as well as the conclusion of this research. The whole questionnaire is also included at the end of this document.

2 Related Work

The main areas of this research include BYOD and the various security measures that can be taken in order to provide a safe environment for both the organizations and their employees. The related work includes various research studies relevant to these fields.

In general, there is plenty of research regarding BYOD after the term entered common use back in 2009. Most of this work investigates the various threats and risks of BYOD. For example, Miller et al. [4] focus on threats introduced by BYOD. More specifically in their paper they distinguish two main threats to corporate information security, malware intrusion (worms, viruses, trojans) and the increased possibility of data loss. Respectively, Yeboah-Boateng et al. [5] in their study evaluate the characteristics of BYOD and assess associated risks, threats and vulnerabilities, while Hayes et al. [6] examine the emerging BYOD trend in corporate IT, describing the various security challenges, risks, and liabilities.

Apart from the previous works there are plenty of other studies which focus on BYOD security, proposing guidelines or frameworks to use in order to secure it. The highlight is the work of Souppaya et al. [3], which is the base of this research, providing the guidelines which help organizations protect their IT systems and information from the security risks that accompany the use of telework and remote access technologies. In addition, Wang et al. [7] compare existing BYOD solutions and present a BYOD security framework that provides guidance for enterprises when adopting BYOD. In [8] the authors discuss the security issues related to BYOD programs and explore the benefits, risks, available controls and solutions to mitigate the inherent security concerns with mobile devices, in general, and BYOD programs specifically. Last but not least in [9] the authors present an approach for creating metrics which can be used to align security policies with BYOD policy in creating metrics based on ISO 27000 standard family.

Apart from the previous work which mostly investigates the general aspect of BYOD and the various threats and security measures, there are other studies which focus on more specific domains. For example, Koohang et al. [10] try to build a research model to examine the impact of security policy awareness and data protection awareness of mobile devices on employees' trust belief, while Li et al. [11] propose a periodic smartphone sampling mechanism that significantly improves BYOD security mechanism's effectiveness without incurring further costs. Furthermore, regarding BYOD in education, AlHarthy et al. [12] explain the implementation of BYOD security solution in higher education institution in Oman. The goal of this research is to protect the network data from unauthorized access, as well as, controlling unmanaged devices such as smartphones and mobile devices. Additionally, regarding BYOD in healthcare, Wani et al. [13] identify key security challenges associated with hospital BYOD usage as well as relevant solutions that can cater to the identified issues by reviewing gray literature.

Another field of study is BYOD and access control methods. Work on this field include M. Muhammad et al. [14] research, which aims to fill up the access control gap in the BYOD environment by developing an Intelligent Filtering Technique (IFT) using Artificial Intelligence (AI) Technique. Respectively, Concepcion et al. [15], aim to establish and enforce security policies in BYOD using the in-band approach by integrating the combination of NAC and MDM.

Last but not least there are surveys which investigate BYOD and provide useful results. For example, in [16] the authors questioned over 1000 employees who use BYOD about their preferences for what type of device they use and how the devices they use impact their productivity and work-life balance. Additionally, it questioned about security, aiming to identify whether the employees had the appropriate knowledge. Respectively, Mahinderjit et al. [17] in their survey investigated the current awareness of security and privacy importance in BYOD for higher education in Malaysia. The survey results have proven that the current fundamental security and privacy awareness and knowledge on mobile devices or applications is important in order to protect their mobile devices or data.

Our work, while it deals with the subject of the above research works, which is BYOD risks and measures in organizations, it differs for two main reasons. Initially, it is not focused on a specific field. More specifically, our research includes results from the job sectors of Information Technology, Telecommunications, Business and Finance, Education, Accommodation and Food/Beverage Services, Culture and Arts, Law, Energy, Engineering, Health Care, Marketing, Physics and Public Administration/ Government. Additionally, it includes results from different job departments e.g., R&D, IT, Legal department, Information Security, Sales, Human Resources etc., providing a wide range of results. The main difference though is that it doesn't try to provide general conclusions on the broad topic of BYOD. On the contrary, taking as input already tested and certified guidelines from NIST [3], it tries to provide useful insight of whether these guidelines are used in practice by both companies and employees. These differences make our work unique, offering additional knowledge to the already existing literature.

3 Methodology

3.1 Ethics of the questionnaire

As already mentioned, for the purposes of this document a questionnaire has been created. The fact that this questionnaire is addressed to people, can imply ethical issues. According to [18] the following ten points represent the most important principles related to ethical considerations in dissertations and thesis projects:

1. Research participants should not be subjected to harm in any ways whatsoever.
2. Respect for the dignity of research participants should be prioritized.
3. Full consent should be obtained from the participants prior to the study.
4. The protection of the privacy of research participants has to be ensured.
5. Adequate level of confidentiality of the research data should be ensured.
6. Anonymity of individuals and organizations participating in the research has to be ensured.
7. Any deception or exaggeration about the aims and objectives of the research must be avoided.
8. Affiliations in any forms, sources of funding, as well as any possible conflicts of interests have to be declared.
9. Any type of communication in relation to the research should be done with honesty and transparency.
10. Any type of misleading information, as well as representation of primary data findings in a biased way must be avoided.

Our questionnaire respects the previous points, and the result is totally safe in terms of ethics.

3.2 Questionnaire description

The questionnaire is separated in four parts referred as sections. Their names and description are shown below:

- **Section 1, Introduction and Ethics** – This section includes a description of the questionnaire along with information regarding ethics. Additionally, there is a user consent part which is obligatory for every user and defines whether the questionnaire will pass to the next section or be terminated based on users' choice.
- **Section 2, User Demographics –** This section includes questions regarding demographic data of the users who take part in the survey. These questions provide the requested background of the users, while at the same time giving the appropriate attention to any possible ethics issues that might appear.
- **Section 3, BYOD related questions –** This is the main part of the questionnaire which includes the BYOD related questions. This section provides the majority of the collected data on which our research is based upon.

- **Section 4, Security Awareness related questions** – This is the last section of the questionnaire which provides information regarding possible Security Awareness trainings the recipients of the questionnaire have taken part in.

3.3 Questionnaire's dissemination

The questionnaire was shared in various groups and teams in Facebook, LinkedIn, different working groups and forums.

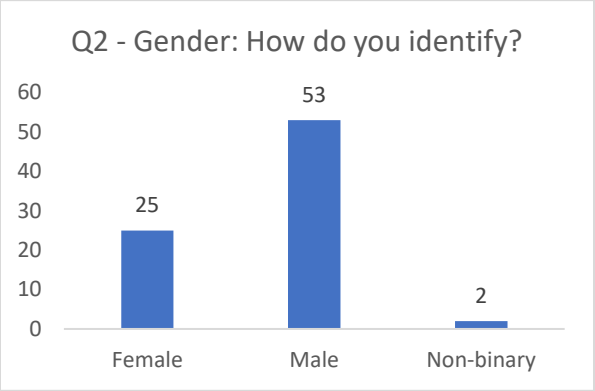
3.4 Results' Analysis methodology

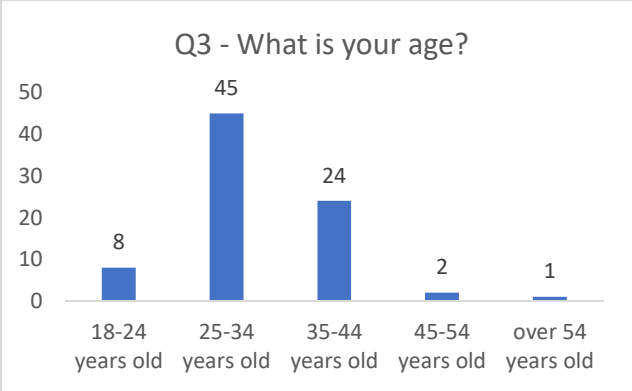
The survey answers are processed with both descriptive and inferential statistics. Initially, we perform the descriptive statistics in order to show and describe the results of each question. Subsequently, we perform the comparative statistical analysis in order to determine the association between two or more categories, employing χ^2 tests (statistical hypothesis test) to explore significant differences between the expected and the observed frequencies, where applicable. More specifically, a chi-square (χ^2) statistic test is a measure of the difference between the observed and expected frequencies of the outcomes of a set of events or variables. It is useful for analyzing such differences in categorical variables, especially those which are of nominal nature. It depends on the size of the difference between actual and observed values, the degrees of freedom, and the sample size and can be used to test whether two variables are related or independent from one another. Last but not least, χ^2 can also be used to test the goodness-of-fit between an observed distribution and a theoretical distribution of frequencies [19].

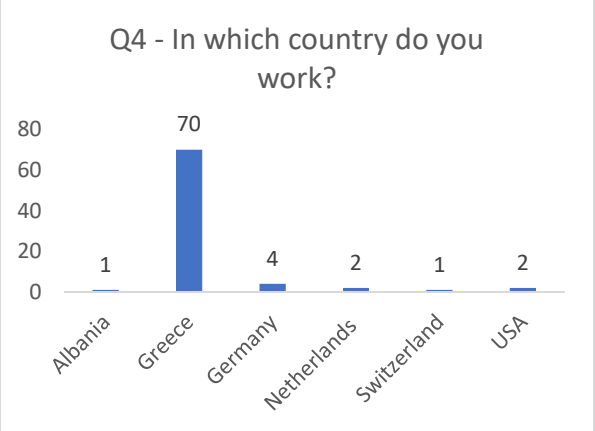
4 Descriptive statistics results

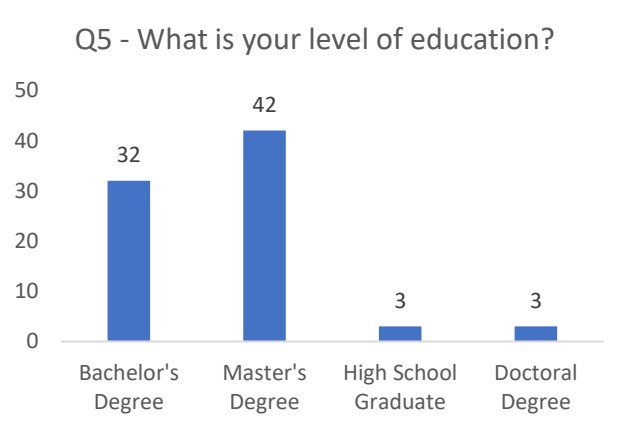
4.1 Demographics section results

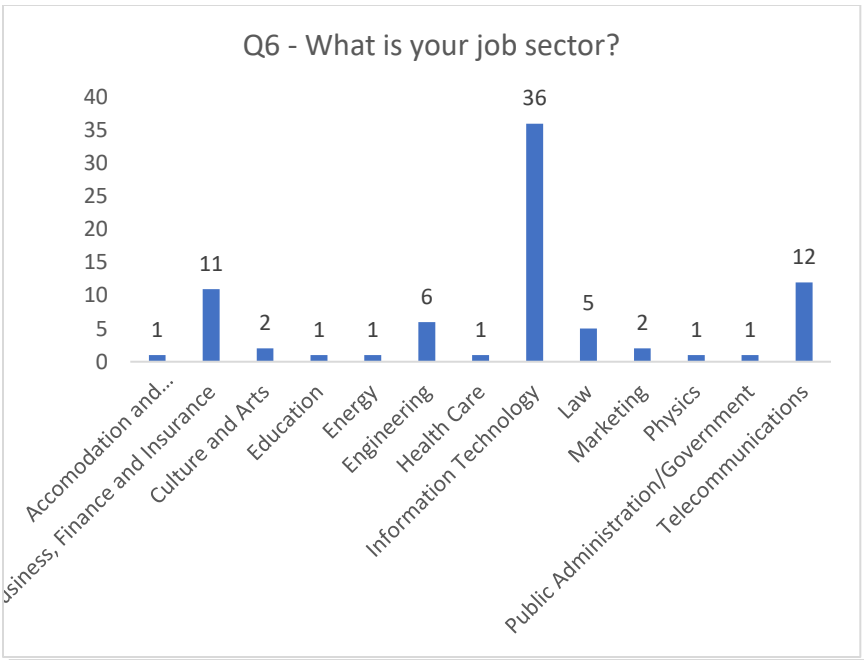
The demographics section of the questionnaire (questions 2-9) includes general questions about the participants, like their gender, age, job sector, country of work etc. It provides us with useful information regarding the participants and reveals important information about their background. More specifically, we can see that the majority of our participants are males (53 out of 80 participants) who work in Greece and that the most common age range is 25-34 years old (45 out of 80 participants), followed by 35-44 years old (24 out of 80). A notable detail is that more than half of the participants have a master's degree (42 out of 80 participants). Respectively, most of the participants are employees in the Information Technology field (36 participants), followed by those working in the Telecommunications (12 participants) and the Business-Finance-Insurance sector (11 participants). Regarding the department of the participants, most of them work in the R&D and software development departments of their organization (27 participants), followed by those working in IT (5 participants), Information Security (5 participants) and Legal departments (5 participants). Finally, the vast majority of the participants (75 out of 80) are employees, while 5 of them are high officials. The demographics results are shown in Figure 1.










Q6 - What is your job sector?
40
35
30
25
20
15
10
5
0
1
11
2
1
1
6
1
36
5
2
1
1
12
Accomodation and...
usiness, Finance and Insurance
Culture and Arts
Education
Energy
Engineering
Health Care
Information Technology
Law
Marketing
Physics
Public Administration/Government
Telecommunications

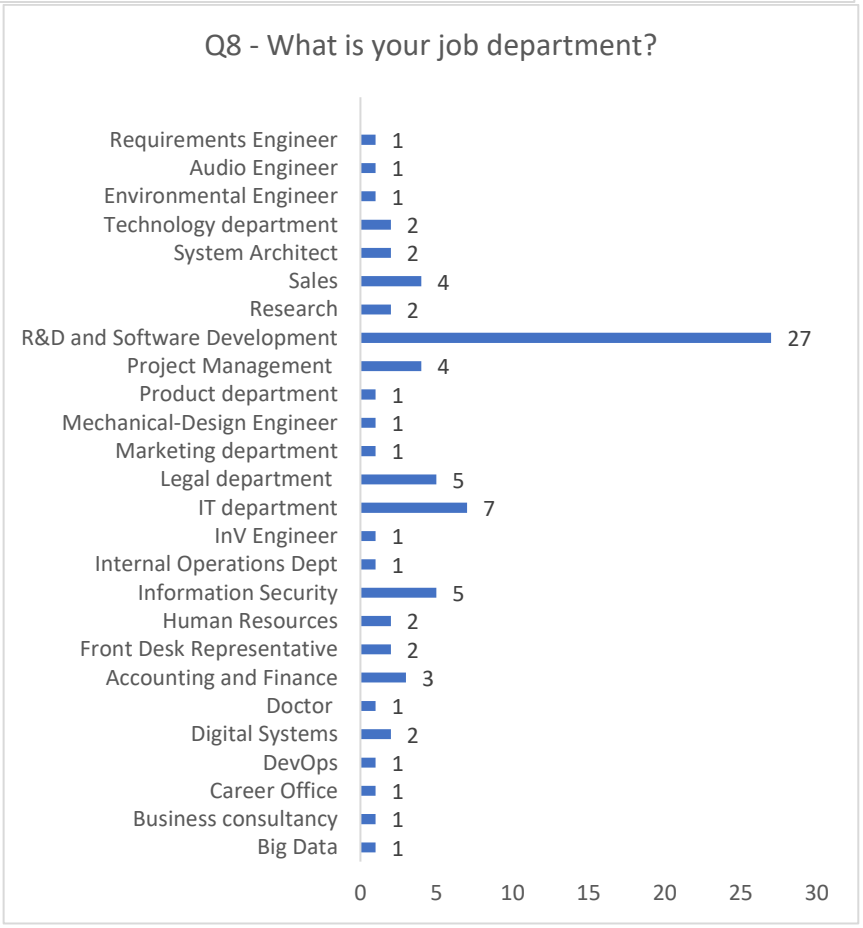

Q8 - What is your job department?
Requirements Engineer 1
Audio Engineer 1
Environmental Engineer 1
Technology department 2
System Architect 2
Sales 4
Research 2
R&D and Software Development 27
Project Management 4
Product department 1
Mechanical-Design Engineer 1
Marketing department 1
Legal department 5
IT department 7
InV Engineer 1
Internal Operations Dept 1
Information Security 5
Human Resources 2
Front Desk Representative 2
Accounting and Finance 3
Doctor 1
Digital Systems 2
DevOps 1
Career Office 1
Business consultancy 1
Big Data 1
0 5 10 15 20 25 30

Figure 1 - Demographics section results

4.2 Cyber Security section results

The Cyber Security section results (questions 11-35) are the most important part of the survey. Depending on their replies, the participants show whether they are aware and follow the security guidelines proposed in [3].

Initially, we see that the majority of the participants (56 out of 80) are allowed to store sensitive corporate data in their personal laptops (Q11 – "Are you allowed to store sensitive data of your organization in your laptop?"). Most of the times this is necessary, however it requires that both the company and the employees have taken various measures to protect these data. One of these measures is the encryption of such data by the organization which shares them. According to our survey (Q12 – "Does your organization encrypt its sensitive data?") this indeed happens in most cases (47 participants), however there is also a big number of participants who replied that there is no encryption in their companies (13 participants) while others don't know whether this happens or not (20 participants). Another measure to protect corporate data from theft is to have the employees' laptop storage encrypted. According to our survey (Q13 – "Does your organization encrypt your laptop's storage?") this is not the case in most organizations, as the majority replied in the negative (45 out of 80 participants). The results of the previous questions are shown in Figure 2.

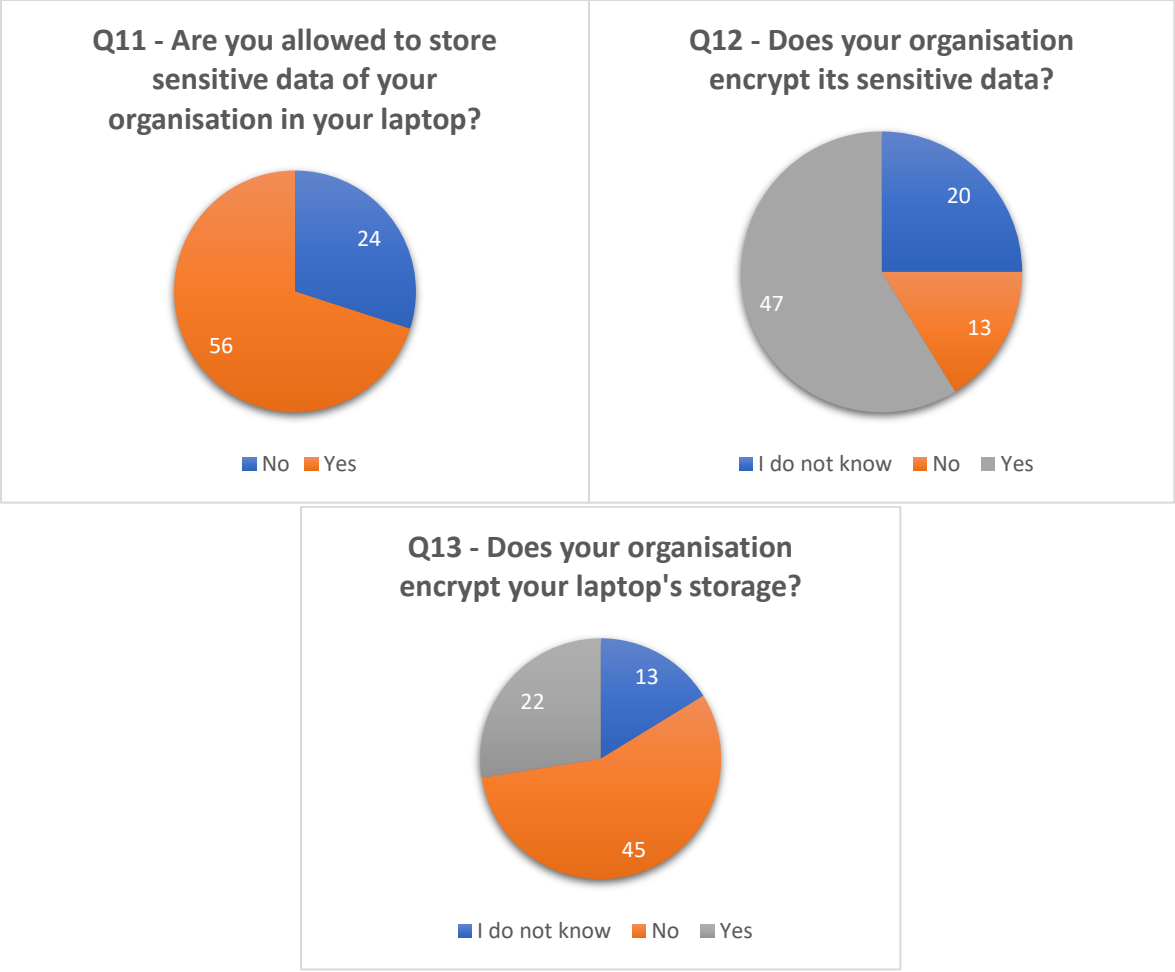


Figure 2 - Questions 11-13

The next four questions are about connectivity and authentication methods as well as system threat models. More specifically, the majority of the participants (62 out of 80) use a second security factor in addition to their password in order to connect to their company's network or VPN (Q14 – "Do you use multi-factor authentication or other types of authentication when connecting from your laptop to your company's network?"). They also stated (66 out of 80) that their organization uses Network Access Control (NAC) solutions to secure access to its network nodes (Q15 – "Does your organization use Network Access Control (NAC) solutions to secure access to its network nodes?"). However, the majority of the participants (42 out of 80) replied that they don't know whether their organization has developed system threat models for the remote access servers (Q16 – "Has your organization developed system threat models for the remote access servers and the resources that are accessed through remote access?"). This is quite usual since this information is not shared very often to regular employees, however at the same time it shows that either the organizations don't find it important to pass this information to their employees or the employees haven't paid the necessary attention to the respective announcement. Either way, this shows a downgrading of the importance of security for both the management and the regular employees of an organization. Finally, most of the participants declared tunneling (VPN) as the method used to connect to their organization's network (Q17 – "Which remote access method do you use to

connect to your organization's network?"). The other choices were "Application Portals", "Remote Desktop", "Direct Application Access" and finally the choice "None". The results of the previous questions are shown in Figure 3.

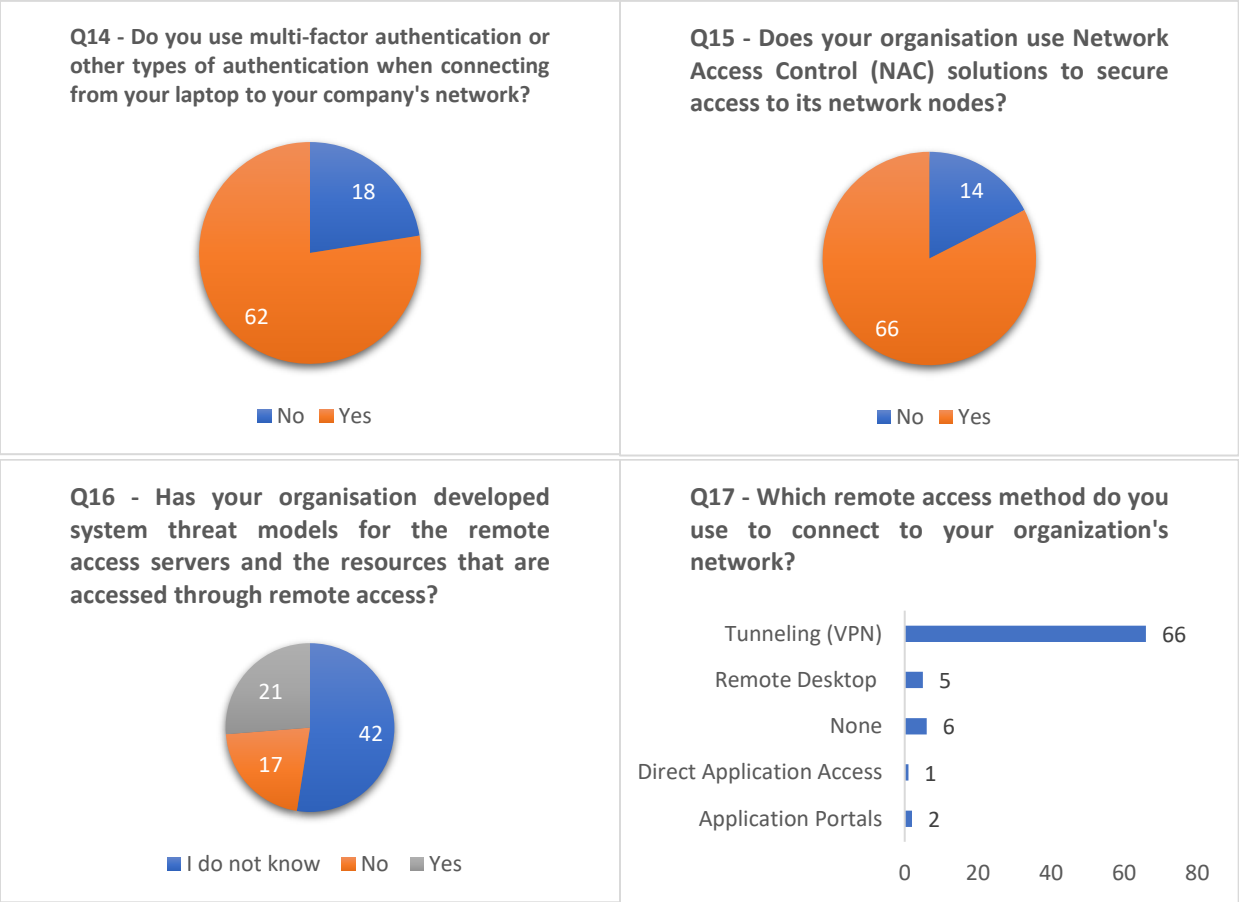


Figure 3 - Questions 14-17

The next three questions are about whether organizations have established separate external networks for BYOD devices and the measures which have been put in place regarding these possible networks. As can be seen from the replies (41 out of 80 participants), most organizations use separate networks for their BYOD employees (Q18 – "Has your organization established separate, external networks for remote and BYOD devices within enterprise facilities?"), however the negative answers are almost equal, which means that more attention is needed by the organizations in these cases. The questionnaire recipients who answered "Yes" in the previous question were subsequently asked about the security and the monitoring of these separate networks (Q19 – "If yes, are these networks secured and monitored in a manner consistent with how remote access segments are secured and monitored?"). More than half of them (24 participants) agreed that these networks were secured and monitored in a manner consistent with how remote access segments are secured and monitored, while 16 participants replied, "I do not know". Finally, the results were divided between "Yes" (28 participants) and "I do not know" (13 participants) regarding the question "Does these networks' traffic pass through a firewall?" (Q20). The fact that there are many "I do not know" answers in both questions shows once more that many employees

are unaware of the security measures taken in their companies and organizations, which is a bad sign and can be translated as weak communication between the high management and the regular employees or lack of attention of employees to respective management announcements. The results of the previous questions are shown in Figure 4.

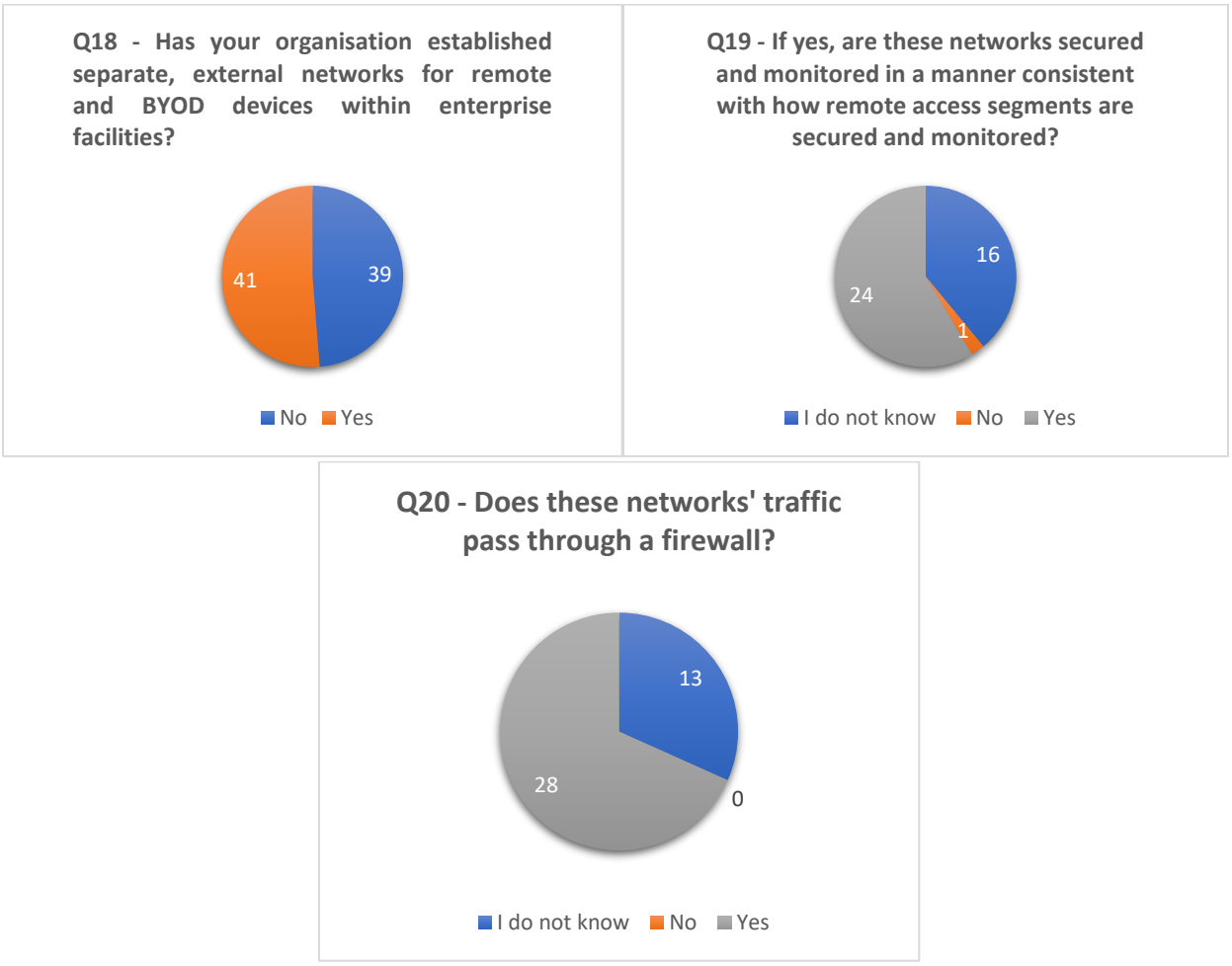


Figure 4 - Questions 18-20

Subsequently, there are three questions regarding tools that can help increase the security of users' devices. In the first one (Q21 – "Do you use antimalware software in your laptop?"), 62 participants replied "Yes". This is an encouraging fact, and it shows that the participants acknowledge the various risks which can be caused from viruses. However, 18 participants replied "No". This shows that there is an important number of participants who are exposed to viruses, even if some of them might use a safer operating system e.g., Unix-like operating systems. Respectively, we get similar results for the next question (Q22 – "Do you use a firewall?"). Again, 65 participants replied "Yes" while 15 replied "No". The participants that answered "No" and subsequently their organizations, similarly to the previous question, are exposed to risks. These risks include unsolicited and unwanted incoming network traffic, originated from malicious sources like malware or hackers. In general, a firewall provides a first line of defense for your computer and helps protect your personal information from cyberthreats, which are widespread

and evolving [24]. In Q23 – "Is your firewall properly configured for the enterprise environment?", the results are divided equally. This shows that either the organization has not imposed a security policy to its BYOD employees, or these employees don't follow the existing security policy [30]. Whatever the case, the result is possible risk for BYOD devices and additionally for the organizations that allow them. For example, if a BYOD user doesn't follow the security policy of his company, which demands to block AnyDesk, there is the possibility that an attacker who knows his AnyDesk ID and password, to potentially have full access to his device depending on the available permissions. After getting access to the BYOD device the attacker can steal sensitive corporate data and passwords or perform lateral movement within the corporate network to gain access to additional resources and potentially sensitive data [25]. The results of the previous questions are shown in Figure 5.

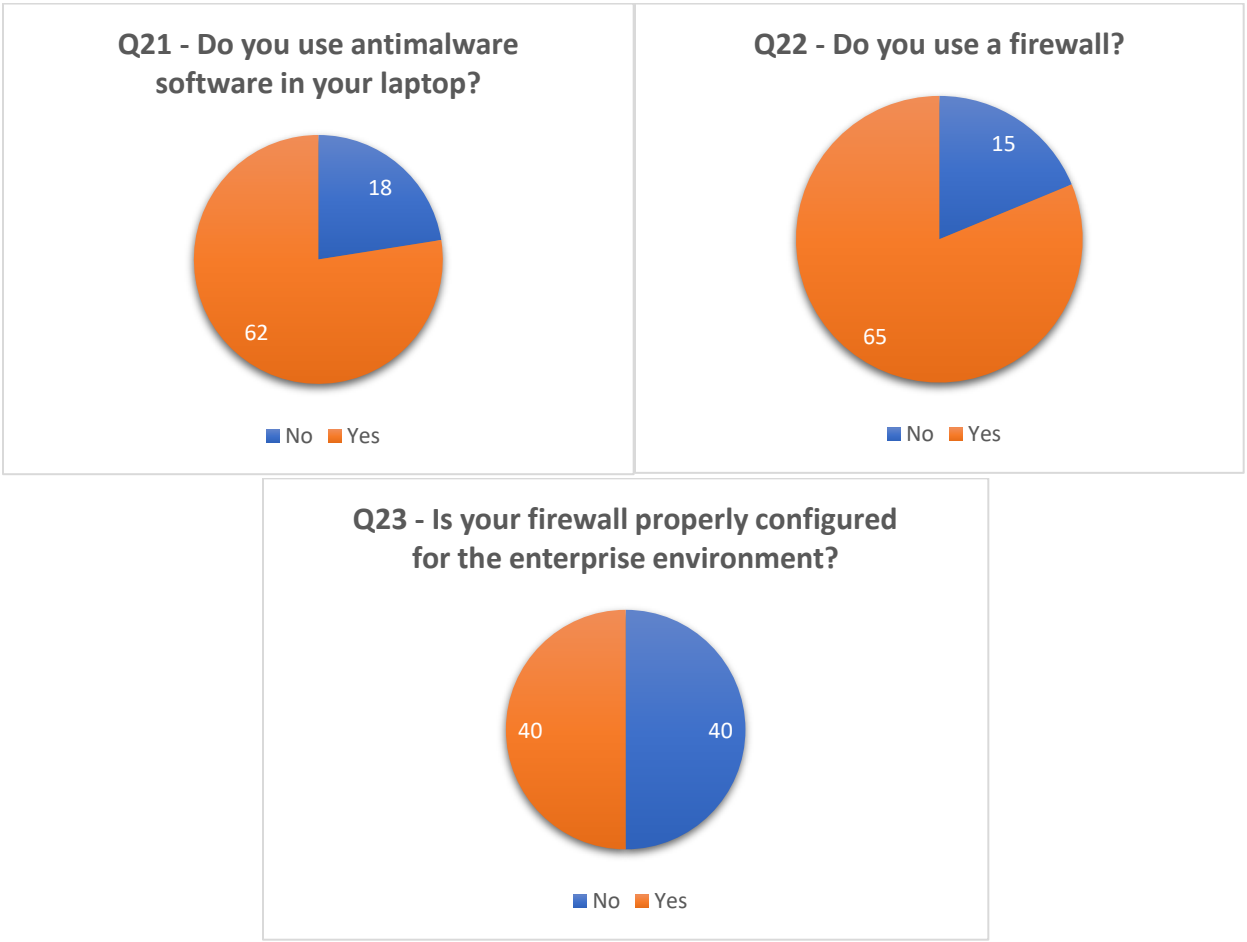


Figure 5 - Questions 21 -23

The next two questions focus on the security of BYOD users against malicious users who intend to steal the physical devices and subsequently the corporate data from them and who might be in the same workspace as them. This workspace also includes cafes or other places where the victims might work remotely. In Q24 – "Do you use any physical security means to protect your device from theft?" only 20 participants answered "Yes". This means that the remaining 60 participants are at risk of losing their devices from thieves that are eager to steal them when opportunity arises.

Of course, the theft of a personal laptop which is used for BYOD can furtherly harm the organization of the victim. Contrary to the previous question, in Q25 – "Do you lock your device when you leave your desk?" the majority of the participants answered "Yes" (58 participants). This is a very important action which discourages any would-be malicious users who may think of taking advantage of a user's absence from his/her device and steal sensitive corporate data. The results of the previous questions are shown in Figure 6.

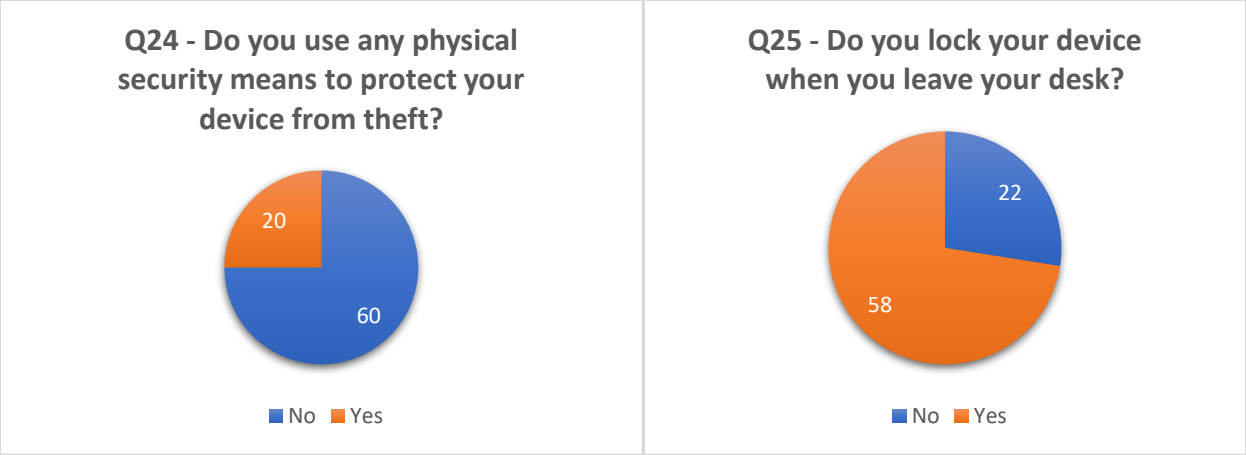


Figure 6 - Questions 24-25

In the next question (Q26 – "Has your organization provided you with flash drives that are specifically configured for telework use in order to prevent you from using your own?"), the vast majority of the participants (70 of them) answered "No". This means that the majority of the participants use their own flash drives which might have been infected from viruses or other types of malware [31]. The possibility of infection can be even stronger when the participants don't use antivirus or firewall tools. Respectively, in the next question (Q27 – "Has your organization provided you with a bootable OS and read-only removable media with pre-configured remote access client software?"), 72 participants answered "No". This means that the participants use their own system (operating system and software). This is enough when the user has good knowledge of computer security, however most of the times it is safer to use a preconfigured environment created by security professionals. The results of the previous questions are shown in Figure 7.

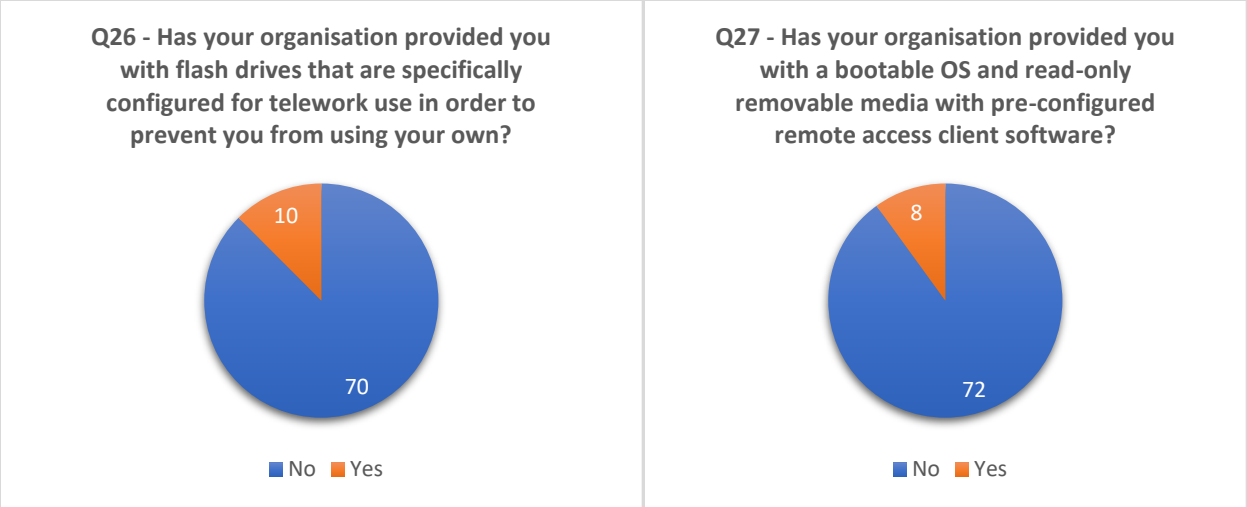
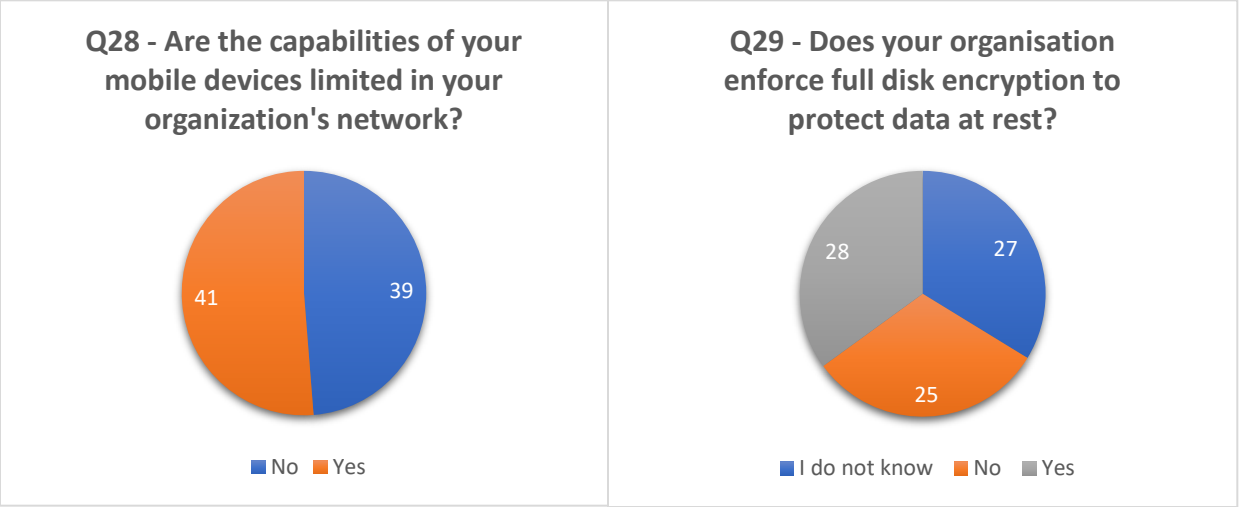


Figure 7 - Questions 26-27

In Q28 – "Are the capabilities of your mobile devices limited in your organization's network?" more than half of the participants (41 out of 80) replied "Yes". This means that most users are not allowed to browse to various websites like Facebook, Instagram, Spotify etc. or use Bluetooth when connected to their organization's network. Additionally, in Q29 – "Does your organization enforce full disk encryption to protect data at rest?", 52 participants replied "No" and "I don't know", which means that there is risk, since this data is usually subject to threats from hackers and other malicious users who seek to gain access to the data digitally or by physical theft of the data storage media. The remaining 28 participants had their disk encrypted by using specific tools like BitLocker, IBM Guardium etc. Finally, in Q30 – "Does your organization prompts you to use virtual machines (VMs) in order to carry out your job?", 51 out of 80 participants replied "No". The results of the previous questions are shown in Figure 8.



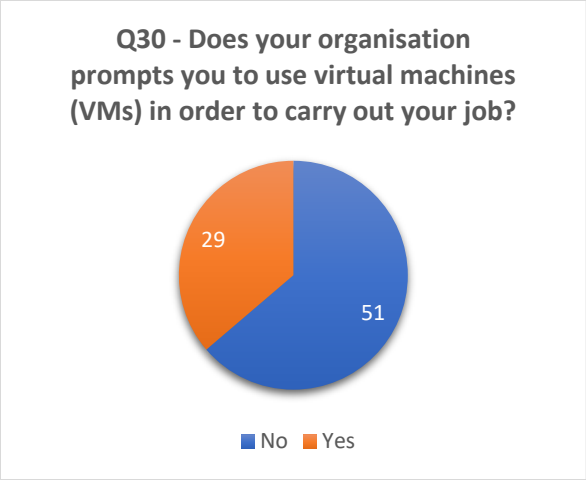


Figure 8 - Questions 28-30

Continuing with the Cyber Security section results we find backup related questions. In Q31 – "Are you backing up data in your telework device?", the results are equal (40 "Yes" versus 40 "No"). Unfortunately, 50% of people who don't take backup of their work is a very big percentage and shows that many users don't take security risks seriously. For those that they replied "Yes", 11 participants take backups monthly, 6 of them weekly, 8 of them daily while 14 answered "Other" (Q32 – "If yes, how regularly do you take backups?"). The results of the previous questions are shown in Figure 9.

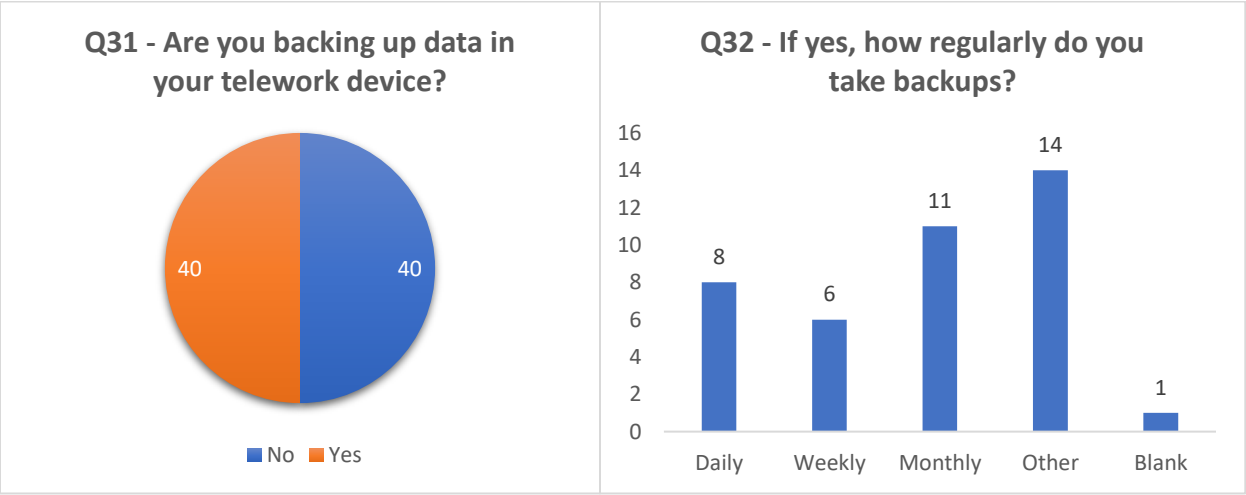


Figure 9 - Questions 31-32

The last three questions of the Cyber Security section are about possible security policies in organizations. More specifically, in Q33 – "Has your organization developed a security policy that defines telework, remote access, and BYOD requirements?", 24 of the participants replied "No". This is a big number which shows that some organizations don't pay due attention to cybersecurity. Another possibility though, could be that these participants are not aware of their organization's security policy. Those who answered "Yes" in the previous question, gave an almost equal result when asked whether they had read the security policy of their organization or not (Q34 – "If yes, did you read the security policy?"). More specifically, 26 of them answered "No", while 30

answered “Yes”. Finally, regarding Q35 – “Do you put the security policy in practice?”, 37 of the participants answered “Yes”, while 18 answered “No” (there was also a blank answer). The results of the previous questions are shown in Figure 10.

Figure 10 - Questions 33-35

4.3 Cyber Awareness section results

The final section of the questionnaire includes three questions which are about the familiarity of the participants with cyber security and the possible cybersecurity awareness trainings which might have attended. More specifically, in Q36 – “How familiar are you with Cybersecurity?”, the participants answered as follows:

Novice – 24 participants
Advanced Beginner – 25 participants
Competent – 17 participants
Proficient – 9 participants

Expert – 5 participants

The results show that there are many users who are not experienced in cyber-security and that's the reason why there are some weak results in previous questions. Subsequently the participants were asked about possible security awareness trainings that might have attended. More specifically, in Q37 – "Have you attended any security awareness trainings?", 50 of the participants answered "Yes" while the other 30 answered "No". This means that almost 40% of the participants haven't attended any security awareness trainings. This increases the dangers of using BYOD even more, putting in danger the security of the organizations and companies of the participants. In the last question of the questionnaire (Q38 – "If yes, were these security trainings organized by your company?"), the participants who answered "Yes" in the previous question were called to answer whether their companies have organized cyber-security awareness trainings. The result was that 39 out of 50 participants answered "Yes", while 11 answered "No", which means that the majority of companies are aware of the various dangers that lurk when using BYOD and try to "enlighten" their employees too. This doesn't mean that these companies are completely safe from the various BYOD risks, however, they are safer than those who don't organize such trainings at all. The results of the previous questions are shown in Figure 11.

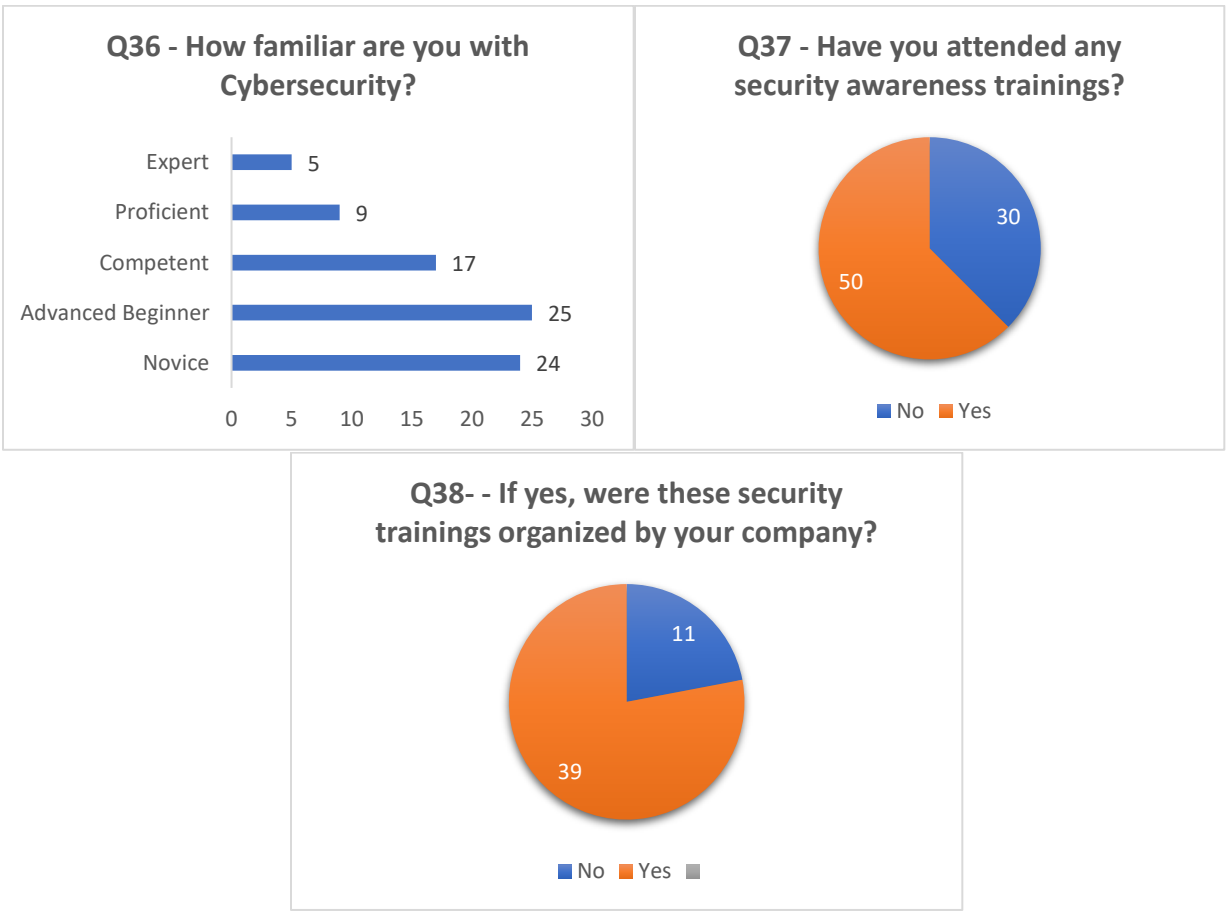


Figure 11 - Questions 36-38

5 Inferential Statistics results

In this section we will analyze the most interesting results of our questionnaire with the help of inferential statistics. More specifically, since most of the questions' answers are of nominal type (nominal data are categorical data without any order of value) we will use χ^2-tests for independence to check for independence of the response categories. The null hypothesis to every χ^2 test that is performed in the following pages is that there is no relationship or correlation between the category counts and variable values. On the contrary, the research hypothesis states that there is an underlying association between them [20].

5.1 Security measures implied by the participants are correlated with their Cybersecurity familiarity

In the first test we will investigate whether the results of our questionnaire agree with the hypothesis that greater familiarity with Cybersecurity has as result a more secure personal device. More specifically we will state that greater familiarity with Cybersecurity has as result the use of antimalware software (research hypothesis). In Table 1 we can see the associations between Cybersecurity familiarity and the use of antimalware.

Cybersecurity familiarity	Using antimalware	Not using antimalware	Row total
Novice	17	7	24
Advanced Beginner	21	4	25
Competent	13	4	17
Proficient	7	2	9
Expert	4	1	5
Column Total	62	18	80

Table 1 - Cybersecurity familiarity and use of antimalware

To calculate the obtained statistic, we must first calculate the expected value for each one of the observed values. The Expected Frequencies can be found with the help of the following type: **fe = Row Total * Column Total / Total Sample**. For example, to calculate the Expected frequency of Novice participants who use antimalware we have: **fe = Row Total * Column Total / Total Sample = 24 * 62 / 80 = 18.6**. The same procedure is followed for the remaining expected frequencies. Subsequently, the x^2 value can be found using the following type: $\mathbf{x^2 = \Sigma\ (fo - fe)^2 / fe}$ where fo is the observed frequency (columns 2 and 3 of Table 1). The final result of this calculation is: $\mathbf{x^2 = 1.246093658}$.

Before we can come to a conclusion, we need to find our critical statistic, which entails finding our degrees of freedom. In this case, the number of degrees of freedom is equal to the number of columns in the table minus one multiplied by the number of rows in the table minus one (The row Column Total and the column Row Total are out). In our case, we have (5-1) * (2-1), or 4 degrees

of freedom. Finally, we compare our obtained statistic to our critical statistic found on the chi-square table which can be found in Table 2.

	α									
df	0.995	0.990	0.975	0.950	0.900	0.100	0.050	0.025	0.010	0.005
1	0.000	0.000	0.001	0.004	0.016	2.706	3.841	5.024	6.635	7.879
2	0.010	0.020	0.051	0.103	0.211	4.605	5.991	7.378	9.210	10.597
3	0.072	0.115	0.216	0.352	0.584	6.251	7.815	9.348	11.345	12.838
4	0.207	0.297	0.484	0.711	1.064	7.779	9.488	11.143	13.277	14.860
5	0.412	0.554	0.831	1.145	1.610	9.236	11.070	12.833	15.086	16.750
6	0.676	0.872	1.237	1.635	2.204	10.645	12.592	14.449	16.812	18.548
7	0.989	1.239	1.690	2.167	2.833	12.017	14.067	16.013	18.475	20.278
8	1.344	1.646	2.180	2.733	3.490	13.362	15.507	17.535	20.090	21.955
9	1.735	2.088	2.700	3.325	4.168	14.684	16.919	19.023	21.666	23.589
10	2.156	2.558	3.247	3.940	4.865	15.987	18.307	20.483	23.209	25.188

Table 2 - Chi-Square table [26]

We also need to reference our alpha, which we set at 0.050 (significance level of 5%). As you can see, the critical statistic for an alpha level of 0.05 and 4 degrees of freedom is 9.488, which is greater than our obtained statistic of 1.246093658. Since the critical statistic is greater than our obtained statistic, we can't reject our null hypothesis. This means that regarding the results of our questionnaire, the familiarity with Cybersecurity of the participants doesn't have any association with the use of antimalware.

The same test will be applied to investigate whether the level of familiarity with Cybersecurity has any association with the backups that the participants of the questionnaire might take to protect their data. As in the previous example the null hypothesis is that Cybersecurity familiarity and taking backups are independent while our research hypothesis will be that greater Cybersecurity familiarity is associated with taking backups. In Table 3 we can see the associations between taking backups and Cybersecurity familiarity.

Cybersecurity familiarity	**Taking backups**	**Not taking backups**	**Row total**
Novice	11	13	24
Advanced Beginner	9	16	25
Competent	12	5	17
Proficient	6	3	9
Expert	2	3	5
Column Total	40	40	80

Table 3 - Cybersecurity familiarity and backups

We perform the calculations as in the previous example and we find that **x2 = 6.209019608**. This means that as before, 6.209019608 < 9.488 and so the null hypothesis is again valid. More specifically, the level of familiarity with Cybersecurity of the participants of the questionnaire and the backups which they take are independent (there is no association between them) so the test is not significant.

Subsequently, we perform similar chi-square tests of independence to investigate whether there is any correlation between security familiarity and other security measures taken via the participants of the questionnaire (Table 4).

Variables	x^2 value	df
Security familiarity and properly configured firewall for enterprise environment	6.582352941	4
Security familiarity and locking device when leaving desk	2.702727068	4
Security familiarity and physical security to protect BYOD device from theft	1.979084967	4

Table 4 - Associations between security familiarity and security measures of the participants of the questionnaire

We see that all the above associations are insignificant since their x^2 values are less than the critical chi-square value (9.488) for df = 4 and a = 0.50. This means that the above variables of our tests are independent and there is no significant relationship between them. In general, based on the above x^2 tests it seems that the participants of the questionnaire do not confirm the hypothesis that a greater familiarity with cybersecurity has as result a more secure BYOD device. This implies risk for their organizations which must take actions to prevent possible security flows, perhaps with the development of a strict BYOD security policy.

5.2 Organizations' measures are correlated with job sector

The next test that we will perform is based on the hypothesis that the job sector of the participants plays important role to whether companies have implemented a security policy. More specifically, we assume that since most of our participants work in fields which depend on technology, their companies need to implement a security policy in order to protect their assets, both digital and physical. The null hypothesis will be the opposite fact. In Table 5 we can see the discussed associations (we included only 4 job fields since the others didn't have the required number of participants that would mark the test as valid).

Job sector	Security policy implemented	Security policy not implemented	Row total
Business, Finance and Insurance	9	2	11
Engineering	5	1	6
Information Technology	19	17	36
Telecommunications	12	0	12
Column Total	45	20	65

Table 5 - Job sector and security policy implementation

Respectively, the results of the x^2 test are shown in Table 6.

Variables	x^2 value	df
Job sector and security policy	11.28654602	3

Table 6 - Chi-square value of the association of the job sector and the security policy

The above value $x^2 = 11.28654602$ is greater than the critical statistic (see Table 2 for df = 3 and a = 0.050). More specifically 11.28654602 > 7.815 which means that regarding our test, there is significant relationship between the job sector of the participants and the security policy of their organizations.

In Table 7 are shown the associations between the job sector of the participants and the various security measures taken by their organizations.

Variables	x^2 value	df
Job sector (Q6) and sensitive data storage in BYOD devices (Q10)	0.838231683	3
Job sector (Q6) and multi-factor authentication (Q13)	3.752799219	3
Job sector (Q6) and NAC solutions (Q14)	0.805232459	3
Job sector (Q6) and separate, external networks for BYOD users (Q17)	12.55838143	3
Job sector (Q6) and limited capabilities for BYOD devices in organization's network (Q27)	0.520092019	3
Job sector (Q6) and use of virtual machines (Q29)	1.567182547	3

Table 7 - Associations between job sector and organizations' applied security measures

We can see that contrary to the previous test of independence between job sector and security policy implemented, which showed a significant relationship between the two variables, the tests of Table 7 are mostly insignificant, which means that their variables are independent. More specifically, we can see that the job field of the participants is independent from whether their organizations let them save sensitive data in their BYOD devices or not. The same applies to the following two tests (job sector and multi-factor authentication and job sector and NAC solutions).

However, the next test which investigates the independence between the job sector of the participants and the existence of separate external networks for the BYOD users in their organizations is significant. More specifically, we can see that the chi-square value $x^2 = 12.55838143 > 7.815$. This happens mostly due to the answers of the users of the Telecommunications field (11 out of 12 participants answered that their organizations have established separate, external networks for BYOD). So, we could say that for our sample, the job

sector can affect the establishment of external networks for BYOD users and these two variables are dependent.

Finally, we can see that there is no significant relationship between the variables of the last two chi-square tests (a. job sector and limited capabilities for BYOD devices in organization's network and b. job sector and use of virtual machines) which means that the previous variables are independent for each test.

6 Limitations

This research as any other research which is based on questionnaires has some limitations. The first one concerns the method of collection of survey responses. More specifically, as already discussed in Section 2 – Methodology, the survey was advertised on internet channels and through contact networks (various groups and teams in Facebook, LinkedIn, different working groups and forums). This means that the sample which is collected is not independent. Furthermore, the randomness of the survey is somewhat limited by the fact that similar internet surveys are answered by a self-selected pool of respondents.

Another fact is that the majority of the recipients of the questionnaire are between 25 and 34 years old, most of them are well educated and they originate mostly from Greece. A wider variety of participants from different countries, different age groups and education could improve the quality and the validity of the results. The same applies with the job sector of the questionnaire's recipients. More specifically, as we have already emphasized, the majority of the participants work in the Information Technology field. This implies that they most possibly have a wider knowledge regarding computer security than those working in different fields, which automatically increases the chances of good results regarding computer security awareness.

Finally, a bigger sample of participants could also improve certain parts of the statistical analysis, that is the χ^2 tests for independence. More specifically the χ^2 tests would gain more power with a larger sample size. The reason is that with a bigger sample the correlation of the different tables could provide safer results, making the χ^2 tests more reliable.

7 Discussion and Analysis

The findings of our survey show some interesting behavior which will be discussed throughout this section in response to the three research questions leading this survey. To reach a conclusion, the results of the survey are compared to the NIST guidelines for BYOD [3] which were used to create the survey's questions.

Regarding **R1 – "Are BYOD users careful when using their personal laptop devices in their organizations?"**, we see the following interesting facts. Initially, we see that 77.5% of the participants use antimalware software in their devices while 81.25% of them use a firewall. Both these percentages are high, and they show that the survey participants generally follow NIST guidelines which request the use of antimalware software and firewall in BYOD devices. However, the remaining participants are in serious risk. According to SonicWall Cyber Threat Report [27] there were 5.4 billion malware attacks, 623.3 million ransomware attacks and 5.3 trillion intrusion attempts in 2022. These statistics clearly show the importance of antimalware software and firewalls for every device, both personal and corporate. Concerning the firewall quality of use, in our survey we see that only 50% of the participants stated that it is properly configured for the enterprise environment. As we discussed in Section 4 this result causes concern. More specifically it means that 50% of the survey participants don't follow the NIST guideline which requests to have a properly configured personal firewall installed and enabled.

Another concerning result is the percentage of the participants who use physical security means to protect their devices from theft. More specifically only 25% of them use cable locks or other deterrents to protect their devices, which means they are at risk of having them being stolen from thieves both in the office but also in other places like restaurants, airports, cafes etc. The research company Gartner suggests that a laptop is stolen every 53 seconds [28]. Additionally, research done by the University of Pittsburgh says that a laptop has a 10% chance of being stolen and only a 2% chance of recovery [28]. Thus, it's obvious that BYOD users should give more attention to the physical security of their devices by using preventive measures against thieves. Fortunately, the percentage changes a lot when referring to screen locking of BYOD devices. More specifically, 72.5% of the survey participants lock their device when they leave their desk. Nevertheless, almost 30% of them don't follow the NIST guideline and put in risk important corporate and personal information.

Another interesting result is that 50% of the survey participants don't back up their data. This is a very high percentage compared to the risks that might face. These risks include accidental deletion of data, security incidents, hard drive crashes and shared or synced drive deletion. Last but not least, 53.6% of the participants read the security policy of their organization, while around 66% put the security policy in practice. Both these percentages are low (very close to 50%) and show that the BYOD users who took part in the survey do not take the security policy of their organization very seriously. Of course, it is also the job of each organization to imply rules to their employees.

Overall, we conclude that BYOD users need to be more careful regarding the security of their devices. Especially, some of the previous percentages should cause major concern. One solution could be the scheduling of security awareness trainings from the management in order to raise the security awareness of the employees, even if the results of the inferential statistics (Section 5.1 - Security measures implied by the participants are correlated with their Cybersecurity familiarity) showed that for our survey the cybersecurity familiarity doesn't have as result a more secure BYOD device, as even advanced users follow weak practices.

Regarding **R2 – "Are BYOD users aware of the security measures implied on them by their organizations?"**, we take as data the more complex questions of our survey where there was also the choice "I do not know". Initially, we see that 25% of the BYOD users don't know whether their organization encrypts its sensitive data, while 16.25% are not aware whether their organization encrypts their device storage. In both these two cases the percentages are quite alarming and especially the second percentage (16.25%), which although lower, it shows that there are employees who they don't have a clue about software running on their devices. Furthermore, 52.5% of the participants don't know whether their organizations have developed system threat models for the remote access servers and the resources that are accessed through remote access. As we already discussed before, although this is not a very common and known measure, the percentage of unaware employees is too high. This is a bad sign, and it shows lack of communication between the management and the employees of an organization.

Subsequently, 39% of the BYOD users don't know whether their organizations' external networks for remote and BYOD devices are secured and monitored in a manner consistent with how remote access segments are secured and monitored and respectively, 31.7% of them don't know whether these networks' traffic pass through a firewall. Finally, 33.75% of the BYOD users don't know whether their organization enforces full disk encryption to protect data at rest. All these percentages are quite high showing that BYOD users lack proper knowledge of the security measures implied on them.

Regarding **R3 – "Do organizations implement the appropriate levels of security when they allow BYOD?"**, our sample showed the following interesting facts. First of all, 78.3% of the participants answered that their organization uses an encryption method for its sensitive data (we skipped the "I do not know" answers for this percentage), while 32.8% answered that their organization encrypts the employees' devices storage (again only the "Yes" and "No" answers have been included). Subsequently, 77.5% of the participants answered that they use a second type of authentication apart from their normal username/password authentication (e.g., multifactor authentication) when connecting from their laptop to their company network. This is an important percentage and shows that companies take the authentication process of their employees seriously. However, despite the more secure environment provided by multifactor authentications the organizations should still be careful not to complex a lot the lives of their employees. A survey performed by 1Password on 2000 adults in Canada and U.S. provided some very interesting findings [29]. Nearly half of employees (44%) say that the process of logging in and out at work

harms their mood or reduces productivity, while 26% of workers have given up on doing something at work to avoid the hassle of logging in. Additionally, 41% of employees say having to remember multiple logins heightens their stress levels and strains their mental health. These facts can prove fatal for an organization, as stressed-out employees can behave against the organization's security rules and that is the reason why it is needed a simple and sophisticated authentication solution.

Similar with the high percentage of organizations that they use multifactor authentication on their employees, 82.5% of the BYOD users answered that their organization uses Network Access Control solutions to secure access to its network nodes. On the contrary, only 51.25% of the participants answered that their organization has established separate, external networks for remote and BYOD devices within enterprise facilities, while 55.3% (again "I do not know" choices are not counted) answered that their organization has developed system threat models for the remote access servers and the resources that are accessed through remote access. The previous statistics show that most organizations that support BYOD are confident that their networks are secured enough with a combination of multifactor authentication and NAC solutions, and they are not willing to spend more money and time for additional measures. However, regarding the organizations that they have established external networks for their BYOD users, the 96% of the participants answered that these networks are secured and monitored in a manner consistent with how remote access segments are secured and monitored, while the 100% answered that their network traffic passes through a firewall. The latter statistics are very encouraging and pleasing.

Another interesting fact of the survey is that 82.5% of the participants use Virtual Private Network (VPN) to connect to their organization's network. That's a wise decision since VPN uses authentication and encryption to establish a secure connection to the private network of the organization over the internet. In fact, VPN is the most common form of remote access. The most encouraging fact though, is that the percentage of the participants who don't use any remote access method is only 7.5%. On the contrary, a worrying fact is that almost half of the participants (48.75%) answered that their organizations don't put a limit to their personal devices' capabilities when connecting to their networks. As discussed in Section 4.2 this means that employees can browse freely to any website and use different web applications when connected to their organization's network. This increases the risk of spreading malware in the corporate network and additionally it can decrease the availability of bandwidth.

Subsequently, we see that most organizations prefer to let their employees use their own devices as they are, without offering pre-configured environments and operation systems where they can work more securely. More specifically, 90% of the participants don't use any bootable OS and read-only removable media with pre-configured remote access client software to perform their tasks and additionally, 63.75% are not prompted to use Virtual Machines (VMs) to carry out their jobs. This is fine if the employees keep a high level of security in their devices and avoid risky actions like browsing in suspicious websites, downloading suspicious files, using infected USBs etc. Of course, the level of security of the employees' devices of an organization can be defined by a security policy and more specifically by the security policy regarding BYOD use. Speaking

of which, 70% participants answered that their organization has developed a security policy that defines telework, remote access, and BYOD requirements. In general, this is a good result, however, based on the criticality of the BYOD use, in conjunction with the possible poor level of security awareness of the employees, the result should have been higher.

Overall, we conclude that most of the organizations have implemented a good level of security when allowing BYOD. Of course, there is still room of improvement, especially regarding security policies (they are absent for the 30% of the participants), however the results that we collected seem encouraging. An interesting fact from inferential statistics (Section 5.2) is that the job field plays some role regarding the existence of a security policy and of separate, external networks for BYOD users. More specifically, we see that two job sectors (Information Technology and Telecommunications) affect the result. This might be a limitation for this survey, since most of the participants work in these two fields.

8 Concluding Remarks and Future Work

Overall, it seems that BYOD users tend to underestimate the various security risks that appear when using their personal laptops at work.. While they mostly use traditional security measures like antimalware software and firewalls, they tend to avoid others which are equally important, like taking backups or securing their devices from theft, even if they know that these actions might put their organizations at risk. As has already been pointed out, a solution would be the existence of cybersecurity and safety education at school and universities [32]. At the same time, companies should constantly schedule security awareness trainings in order to raise the security awareness of their employees.

However, while education is important, our results show that even advanced users (higher security familiarity) follow weak practices. This means that education alone will not fix the issue as employees tend to underestimate security risks. Inevitably, the responsibility for the resolution of their employees' behavior lies with the respective organization. More specifically, we saw that in general, organizations have implemented a high level of security when allowing BYOD. However, the most important step should be to imply security policies which they clearly define rules for BYOD use. At the same time, they should communicate these policies to their employees in order to show them the importance of following these rules and the gains that can be achieved.

The survey results indicate several areas of interesting future exploration. For example, a point that has already been discussed in previous sections of this document and could be the subject of further research in the future is the BYOD users' habit to avoid taking security measures, no matter their security familiarity. More specifically, it's interesting to understand why advanced BYOD users (those with higher cybersecurity familiarity) tend to avoid taking certain security measures, while they are aware of the various security risks that might face without them.

Furthermore, another interesting question is about the measures that organizations that allow BYOD take after being hit by a cyberattack. For example, do they imply more strict rules to their BYOD employees? Do they improve their systems in respect to existing BYOD guidelines? What is their behavior regarding their BYOD employees? Do they organize cybersecurity awareness trainings? It would be very interesting to examine their response and whether this response has positive effects on these organizations.

ANNEX

The complete questionnaire is shown below:

Question 1:

Do you consent?
If you consent, you confirm that: 1) You are an adult 2) you grant permission for the data generated from this survey to be used in the thesis researcher's publications and internal reports on this topic 3) you have read the disclaimer 4) your responses will be kept confidential.

- Yes
- No

Question 2:

Gender: How do you identify?

- Male
- Female
- Non-binary
- Other (specify)

Question 3:

What is your age?

- 18-24 years old
- 25-34 years old
- 35-44 years old
- 45-54 years old
- Over 54 years old

Question 4:

In which country do you work?

- Specify

Question 5:

What is your level of education?

- High School Graduate
- Bachelor's Degree
- Master's Degree
- Doctoral Degree
- Other (specify)

Question 6:

What is your job sector?

- Drop down list provided

Question 7:

If you chose "Other" in the previous question, please specify:

- Specify

Question 8:

What is your job department?

- Specify

Question 9:

What is your job position?

- Employee
- High Official

Question 10:

Do you use your laptop to connect to your company's internal network?

- Yes
- No

Question 11:

Are you allowed to store sensitive data of your organization in your laptop?
E.g., are you allowed to store invoice documents?

- Yes
- No

Question 12:

Does your organization encrypt its sensitive data?

- Yes
- No
- I do not know

Question 13:

Does your organization encrypt your laptop's storage?

- Yes
- No
- I do not know

Question 14:

Do you use multi-factor authentication or other types of authentication when connecting from your laptop to your company's network?

E.g., do you use a second security factor in addition to your password when trying to connect to your company's network or your company's VPN?

- Yes
- No

Question 15:

Does your organization use Network Access Control (NAC) solutions to secure access to its network nodes?

E.g., do you need to be authenticated in order to be granted access to your company’s network?

- Yes
- No

Question 16:

Has your organization developed system threat models for the remote access servers and the resources that are accessed through remote access? (Threat modeling is the process of analyzing various business and technical requirements of a system, identifying the potential threats, and documenting how vulnerable these threats make the system)

- Yes
- No
- I do not know

Question 17:

Which remote access method do you use to connect to your organization's network?

- Tunneling (VPN)
- Remote desktop
- Application Portals
- Direct Application Access
- None

Question 18:

Has your organization established separate, external networks for remote and BYOD devices within enterprise facilities?

- Yes
- No

Question 19:

If yes, are these networks secured and monitored in a manner consistent with how remote access segments are secured and monitored?

- Yes
- No
- I do not know

Question 20:

Does these networks' traffic pass through a firewall?

- Yes
- No
- I do not know

Question 21:

Do you use antimalware software in your laptop?

- Yes
- No

Question 22:

Do you use a firewall?

- Yes
- No

Question 23:

Is your firewall properly configured for the enterprise environment?

E.g., have you configured your laptop to block applications like Anydesk when you connect to your company's network?

- Yes
- No

Question 24:

Do you use any physical security means to protect your device from theft?

E.g., do you use cable locks or other deterrents?

- Yes
- No

Question 25:

Do you lock your device when you leave your desk?

- Yes
- No

Question 26:

Has your organization provided you with flash drives that are specifically configured for telework use in order to prevent you from using your own (which might have been infected with malware)?

- Yes

- No

Question 27:

Has your organization provided you with a bootable OS and read-only removable media with pre-configured remote access client software?

E.g., has your organization provided you with flash drives which will boot an operating system every time you turn on your laptop?

- Yes
- No

Question 28:

Are the capabilities of your mobile devices limited in your organization's network?

E.g., can you use Bluetooth or browse to Facebook, Spotify and similar websites when connected to your organization's network?

- Yes
- No

Question 29:

Does your organization enforce full disk encryption to protect data at rest?

E.g., does your organization use tools like BitLocker, IBM Guardium, McAfee Complete Data Protection - Advanced, to encrypt its corporate files stored in the internal network?

- Yes
- No
- I do not know

Question 30:

Does your organization prompt you to use virtual machines (VMs) in order to carry out your job?

- Yes
- No

Question 31:

Are you backing up data in your telework device?

- Yes

- No

Question 32:

If yes, how regularly do you take backups?

- Daily
- Weekly
- Monthly
- Other

Question 33:

Has your organization developed a security policy that defines telework, remote access, and BYOD requirements?

- Yes
- No

Question 34:

If yes, did you read it?

- Yes
- No

Question 35:

Do you put the security policy in practice?

- Yes
- No

Question 36:

How familiar are you with Cybersecurity?

- Novice
- Advanced Beginner
- Competent
- Proficient
- Expert

Question 37:

Have you attended any security awareness trainings?

- Yes
- No

Question 38:

If yes, were these security trainings organized by your company?

- Yes
- No

References

1. Tony Bradley, PCWorld, "Pros and Cons of Bringing Your Own Device to Work" Available from: https://www.pcworld.com/article/473036/pros_and_cons_of_byod_bring_your_own_device_.html

2. Shumate, T.G. & Ketel, M. (2014), "Bring Your Own Device: Benefits, risks and control techniques" IEEE SOUTHEASTCON 2014

3. Souppaya, M., & Scarfone, K. (2016), "Guide to enterprise telework, remote access, and bring your own device (BYOD) security" NIST Special Publication, 800, 46.

4. K. W. Miller, J. Voas and G. F. Hurlburt, "BYOD: Security and Privacy Considerations. in IT Professional" vol. 14, no. 5, pp. 53-55, Sept.-Oct. 2012, doi: 10.1109/MITP.2012.93.

5. Yeboah-Boateng, E. & Boaten F. (2016, August)," Bring-Your-Own-Device (BYOD): An evaluation of associated risks to corporate information security" International Journal in IT and Engineering, 4(8), 12-30. Retrieved October 23, 2016, from https://arxiv.org/abs/1609.01821

6. Hayes, B. & Kotwica, Kathleen. (2013), " Bring Your Own Device (BYOD) to Work" 10.1016/C2012-0-07723-X.

7. Y. Wang, J. Wei and K. Vangury, "Bring your own device security issues and challenges" 2014 IEEE 11th Consumer Communications and Networking Conference (CCNC), 2014, pp. 80-85, doi: 10.1109/CCNC.2014.6866552.

8. Shumate, T.G., & Ketel, M. (2014), "Bring Your Own Device: Benefits, risks and control techniques", IEEE SOUTHEASTCON 2014, 1-6.

9. K. Hajdarevic, P. Allen and M. Spremic, "Proactive security metrics for Bring Your Own Device (BYOD) in ISO 27001 supported environments" 2016 24th Telecommunications Forum (TELFOR), 2016. pp. 1-4, doi: 10.1109/TELFOR.2016.7818717.

10. Koohang, K. Floyd, N. Rigole, and J. Paliszkiewicz, "Security policy and data protection awareness of mobile devices in relation to employees' trusting beliefs" Online J. Appl. Knowl. Manag., vol. 6, no. 2, pp. 7–22, 2018, doi: 10.36965/ojakm.2018.6(2)7-22.

11. F. Li, C. -T. Huang, J. Huang and W. Peng, "Feedback-based smartphone strategic sampling for BYOD security," 2014 23rd International Conference on Computer Communication and Networks (ICCCN), 2014, pp. 1-8, doi: 10.1109/ICCCN.2014.6911814.

12. K. AlHarthy and W. Shawkat, "Implement network security control solutions in BYOD environment," 2013 IEEE International Conference on Control System, Computing and Engineering, Penang, Malaysia, 2013, pp. 7-11, doi: 10.1109/ICCSCE.2013.6719923.

13. Wani T, Mendoza A, Gray K, "Hospital Bring-Your-Own-Device Security Challenges and Solutions: Systematic Review of Gray Literature", JMIR Mhealth Uhealth 2020;8(6):e18175, doi: 10.2196/18175.

14. M. A. Muhammad, A. Ayesh, and P. B. Zadeh, "Developing an Intelligent Filtering Technique for Bring Your Own Device Network Access Control," in Proceedings of the International Conference on Future Networks and Distributed Systems, 2017, p. 35.

15. J. Concepcion, J. Chua, and G. Siy, "Securing Android BYOD (Bring your Own Device) with Network Access Control (NAC) and MDM (Mobile Device Management)," 2015.

16. Beyond Identity, "BYOD: Exploring the Evolution of Work Device Practices in a New Remote-Forward Era [Survey]," Beyond Identity Blog, pp. 1–14, 2021, [Online]. Available: https://www.beyondidentity.com/blog/byod-exploring-evolution-work-device-practices-survey.

17. M. Mahinderjit, C. Wai, and Z. Zulkefli, "Security and Privacy Risks Awareness for Bring Your Own Device (BYOD) Paradigm," Int. J. Adv. Comput. Sci. Appl., vol. 8, no. 2, pp. 53–62, 2017, doi: 10.14569/IJACSA.2017.080208.

18. Bryman, A. & Bell, E. (2007) "Business Research Methods", 2nd edition, Oxford University Press

19. Hayes, A. (2022) "Chi-Square (x2) Statistic: What It Is, Examples, How and When to Use the Test", Available from: https://www.investopedia.com/terms/c/chi-square-statistic.asp

20. "Chi-Square - Sociology 3112 - Department of Sociology - The University of Utah". soc.utah.edu. Retrieved 2022-11-12.

21. Wiech, Dean. "The Benefits And Risks Of BYOD". Manufacturing Business Technology. Archived from the original on October 24, 2013. Retrieved January 28, 2013.

22. Tim Fisher. "What Is a Node in a Computer Network: Your computer and printer are both network nodes". Retrieved 24 December 2018.

23. Kenneth C. Laudon, Jane P. Laudon, "Management of Information Systems".

24. Alison Grace Johansen. (2021), "What is a firewall? Firewalls explained and why you need one" Available from: https://us.norton.com/blog/emerging-threats/what-is-firewall

25. Q. Liu et al., "Latte: Large-Scale Lateral Movement Detection," MILCOM 2018 - 2018 IEEE Military Communications Conference (MILCOM), Los Angeles, CA, USA, 2018, pp. 1-6, doi: 10.1109/MILCOM.2018.8599748.

26. Shaun Turney. (2022) "Chi-Square (X^2) Table | Examples & Downloadable Table" Available from: https://www.scribbr.com/statistics/chi-square-distribution-table/

27. "2022 SonicWall Cyber Threat Report" available from https://www.infopoint-security.de/media/2022-sonicwall-cyber-threat-report.pdf

28. 2019 "A Lost Laptop Is a Cybersecurity Threat" available from https://www.gcu.edu/blog/engineering-technology/lost-laptop-cybersecurity-threat

29. Stacey Harris. (2022) "New 1Password research reveals the risks of login fatigue" available from https://blog.1password.com/report-login-fatigue-research/

30. Valenza, Fulvio, and Manuel Cheminod, "An Optimized Firewall Anomaly Resolution." J. Internet Serv. Inf. Secur. 10.1 (2020): 22-37.

31. Mueller, P., & Yadegari, B. (2012) "The stuxnet worm" Département des sciences de linformatique, Université de lArizona. Recuperado de: https://www2.cs.arizona.edu/~collberg/Teaching/466-566/2013/Resources/presentations/2012/topic9-final/report.pdf

32. Androulidakis, Iosif. (2011) "Mobile Phone Security Awareness and Practices of Students in Budapest". 18-24.