A Bring Your Own Device security awareness survey among professionals

George Petihakis[*]
georgios.petihakis@ssl-unipi.gr
Department of Digital Systems,
University of Piraeus
Piraeus, Greece

Dimitrios Kiritsis[*]
d.kiritsis@ssl-unipi.gr
Department of Digital Systems,
University of Piraeus
Piraeus, Greece

Aristeidis Farao[*]
arisfarao@unipi.gr
Department of Digital Systems,
University of Piraeus
Attica, Piraeus, Greece
European Doctoral School, European
Security and Defence College
Brussels, Belgium

Panagiotis Bountakas[*]
bountakas@unipi.gr
Department of Digital Systems,
University of Piraeus
Attica, Piraeus, Greece

Aggeliki Panou[*]
apanou@unipi.gr
Department of Digital Systems,
University of Piraeus
Attica, Piraeus, Greece

Christos Xenakis[*]
xenakis@unipi.gr
Department of Digital Systems,
University of Piraeus
Attica, Piraeus, Greece

ABSTRACT

The increasing prevalence of Bring Your Own Device (BYOD) practices in the workplace has posed significant challenges to organizations in terms of security and management. This paper presents a survey-based study aimed at exploring the adoption, implications, and security considerations associated with BYOD policies. The study utilized a questionnaire developed based on guidelines provided by the National Institute of Standards and Technology (NIST). The primary objectives of this research are to investigate the cautiousness and awareness of BYOD users, as well as the effectiveness of security measures implemented by organizations, in order to gain insights into the key aspects of BYOD practices in the workplace. The findings of this paper highlight the need for increased caution among BYOD users regarding device security, a lack of knowledge among users about organizational security measures, and the potential for enhancing security policies and implementing additional measures despite organizations having achieved a satisfactory level of security for BYOD.

[*]These authors contributed equally to this research.

KEYWORDS

Cybersecurity education, Questionnaire survey, Bring Your Own Device practices

1 INTRODUCTION

In recent years, organizations and companies worldwide have embraced the Bring Your Own Device (BYOD) trend (the BYOD market has increased 1000% from 2014 to 2022 [43]), allowing employees to use their personally owned devices like smartphones, tablets, and laptops for work-related tasks. This shift offers numerous advantages. Firstly, it boosts employee satisfaction as they can use devices they are familiar with and have chosen for themselves, creating a sense of comfort and convenience [7]. Secondly, productivity tends to increase when employees work on their own devices, enabling them to work efficiently and complete tasks more quickly. This improved efficiency can lead to greater output, benefiting employers [34]. Moreover, BYOD provides flexibility, empowering employees to work from anywhere without relying on company tools or constantly transferring documents back and forth. This freedom eliminates the need for cumbersome processes and streamlines workflow [34]. Lastly, BYOD often results in cost savings for companies, as employees bear the expenses associated with their own devices, hardware, voice or data services, and related costs. This alleviates financial burdens on organizations [7].

However, alongside these benefits, the use of BYOD introduces significant challenges that organizations must address. Stolen or compromised personal devices pose a considerable threat, potentially exposing sensitive corporate data to malicious actors seeking to harm the organization. Unauthorized access to unsecured data on these devices can have severe consequences [42] . Furthermore,

personal devices may not adhere to the organization's security policies or lack the necessary security software, making them vulnerable to various cybersecurity threats [34]. The end node problem further complicates matters, as BYOD intersects with managing devices accessing both sensitive and vulnerable networks and services. Some risk-averse organizations adopt an Inverse-BYOD approach, issuing devices exclusively for internet use. Effectively controlling and managing employees' personal devices presents its own challenges, requiring efficient inventory management systems to track device usage, location, and software configurations [22]. Additionally, monitoring employees' personal devices is a complex task for IT security departments, as they must strike a balance between monitoring work-related activities and respecting personal privacy while accessing company data or information [22]. These risks underscore the critical need for cybersecurity awareness among both employees and organizations when implementing BYOD policies.

In this study, our objective is to investigate the cybersecurity awareness and behavior of users who bring their own devices into organizational settings by addressing the following three research questions:

R1: Are BYOD users cautious when utilizing their personal laptop devices within their organizations?

R2 : Are BYOD users knowledgeable about the security measures imposed on them by their organizations?

R3 : Do organizations implement adequate levels of security when allowing BYOD?

To achieve this, we conducted a survey among a sample of 80 employees who had permission to use BYOD in their organizations. The survey questions were based on BYOD guidelines referenced from "Guide rise Telework, Remote Access, and BYOD Security" [36]. The findings of our survey provided valuable insights into the cybersecurity awareness of both employees and their organizations. Specifically, the contributions of this paper lie in the following aspects:

- We conduct a security awareness survey, among security professionals, regarding the BYOD paradigm.
- We have identified several pitfalls regarding the adoption of BYOD.
- Based on the conducted research, we have identified and proposed directions for future research.

The rest of the paper is organized as follows. Section 2 presents the existing related works that explore various challenges of the BYOD approach and security measures to mitigate them. Section 3 presents the methodology used in this research, while Section 4 presents descriptive and inferential statistics of the results, and Section 5 describes the limitations of the research. Finally, Section 6 discusses the results of this work, and Section 7 concludes the paper.

2 RELATED WORK

This research primarily focuses on the topic of BYOD and explores the different security measures that can be implemented to ensure a secure environment for organizations and their employees. The related work covers a range of research studies related to this domain.

A significant amount of research has been conducted on the subject of BYOD since the term gained popularity in 2009. The majority of existing works explore the diverse range of threats and risks associated with BYOD. In particular, Miller et al. [26] concentrate on the threats posed by BYOD. In their paper, they identify two main risks and threats to corporate information security, malware intrusion (worms, viruses, trojans) and the increased possibility of data loss. Respectively, in their study, [32] assesses the characteristics of BYOD and evaluates the related risks, threats, and vulnerabilities. On the other hand, [16] explores the trend of BYOD in corporate IT, providing an overview of security challenges, risks, and liabilities involved.

In addition to the aforementioned research, numerous other studies have been conducted with a focus on BYOD security. These studies offer guidelines or frameworks that can be employed to enhance the security of BYOD implementations. More specifically, the work of Souppaya et al. [36] which is the base of this research, provides guidelines that assist organizations in safeguarding their IT systems and information against the security risks associated with the utilization of telework and remote access technologies. Moreover, [40] compares currently available BYOD solutions and introduces a comprehensive BYOD security framework that offers valuable guidance for enterprises during the adoption of BYOD. Shumate et al. [34] examines the security challenges associated with BYOD programs, examining the advantages, risks, existing controls, and potential solutions to address the inherent security concerns associated with mobile devices in general, and specifically focus on BYOD programs. Lastly, but equally important Hajdaveric et al. [15] introduces a methodology for developing metrics that align security policies with BYOD policies. They propose the utilization of metrics based on the ISO 27000 standard family to facilitate this alignment.

Furthermore, to the prior research that primarily examines the overall aspects of BYOD, including threats and security measures, there exist other studies that concentrate on more specific domains. As an example, Koohang et al. [20] endeavor to construct a research model to assess how security policy awareness and data protection awareness on mobile devices impact employees' trust beliefs. Similarly, Li et al. [23] propose a periodic smartphone sampling mechanism that significantly enhances the effectiveness of BYOD security mechanisms without incurring additional costs. Additionally, in the context of BYOD in education, AlHarthy et al. [1] aims to safeguard network data from unauthorized access and manage uncontrolled devices, including smartphones and mobile devices. Moreover, concerning BYOD in healthcare, Wani et al. [41] identify critical security challenges associated with the use of BYOD in hospitals and present pertinent solutions derived from a comprehensive review of gray literature.

Another area of research focuses on BYOD and access control methods. Within this domain, notable work includes the research conducted by M. Muhammad et al. [28]. Their study aims to address the access control challenges in the BYOD environment by developing an Intelligent Filtering Technique (IFT) that leverages Artificial Intelligence (AI) techniques. Similarly, Concepcion et al. [8] aim to establish and enforce security policies in BYOD through the integration of Network Access Control (NAC) and Mobile Device Management (MDM) using the in-band approach.

Last, but certainly not least, there are surveys conducted to explore the realm of BYOD and yield valuable insights. For instance,

in reference [4], the authors conducted a survey that involved over 1000 employees who utilize BYOD. The survey aimed to gather information regarding their device preferences, the impact of their devices on productivity and work-life balance, and their awareness of security measures. Similarly, Singh et al. [35], conducted a survey to investigate the current level of security and privacy awareness in BYOD within the higher education sector in Malaysia. The survey findings demonstrated the significance of fundamental security and privacy awareness and knowledge pertaining to mobile devices and applications for safeguarding personal devices and data.

Our research addresses the topic of BYOD risks and countermeasures in organizations, aligning with the subject matter explored in the above research works. However, our work distinguishes itself in two significant ways. Firstly, it does not confine itself to a specific field. More specifically, our research includes results from the various job sectors encompassing a broader perspective. The primary differentiation, however, lies in the fact that our research does not seek to present general conclusions on the broad topic of BYOD. Instead, it takes pre-established and validated guidelines from NIST [36] as input and aims to provide valuable insights into their practical implementation by both companies and employees. These distinctions make our work distinctive, contributing additional knowledge to the existing literature.

3 METHODOLOGY

Between March 2022 and March 2023, an online survey was undertaken to evaluate the security preferences, awareness behavior, and education of BYOD users. The survey's ethical considerations, its process, and information on the statistical significance of the results are briefly explained below.

The fact that this survey focuses on people may raise issues regarding ethics. Below are enumerated the 10 most significant ethical issues in surveys, according to [3].

(1) Research participants should not be subjected to harm in any way 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.

Private connections and a number of professional networking sites, including LinkedIn, Research Gate, and Reddit, were used to distribute the questionnaire. This was considered crucial in order to make sure that the questionnaire was disseminated to a variety of nations. Anyone above the age of 18 who is employed and uses a personal computer for business is considered to be a member of the targeted audience. Other restrictions, such as those based on age, gender, nationality, years of experience, position seniority, or the kind of workplace, were not used because the goal was to collect a diverse sample of responses. Additionally, a disclaimer page was provided at the start of the questionnaire as soon as the participant visited the form, outlining the research and soliciting their agreement. The survey itself consisted of 38 questions (35 multiple choice, and 3 free response). Overall, the questionnaire respects the previous points, and the result is safe in terms of ethics. Regarding the questionnaire's structure, it is broken up into four distinct sections that can be referred to individually by their respective names. The completed questionnaire may be found in [12]. Below there are their names and brief descriptions:

Introduction and Ethics: The questionnaire's description and information on ethics are included in this section. Additionally, there is a mandatory user consent area that determines whether the questionnaire will pass to the next section or be terminated based on the users' choice.

User Demographics In this section, survey participants' demographic information is questioned. These questions include the: age, gender, country of employment, level of education, industry, subject's job department, subject's job position, and if the subject uses her personal device for employment purposes.

Questions about BYOD This is the questionnaire's main section and icludes the *BYOD-related* questions. The majority of the information gathered that forms the basis of the survey is presented in this part.

Cybersecurity awareness In the final part, the questionnaire asks cybersecurity awareness-related questions about the subject's training and familiarity with cybersecurity.

Regarding the analysis of the survey outcomes, both descriptive and inferential statistics have been used. In order to display and characterize the outcomes of each inquiry, we first do descriptive statistics. Then, we do a comparative statistical analysis to see if there is a link between two or more groups. If necessary, we use χ^2 tests (statistical hypothesis tests) to look for significant differences between the expected and observed rates. A χ^2 statistic test compares the observed and anticipated frequencies of a set of events or variables. It helps analyze category variables, especially nominal ones. It tests whether two variables are connected or independent based on the difference between actual and observed values, degrees of freedom, and sample size. Finally, χ^2 may examine the goodness-of-fit between an actual distribution and a theoretical frequency distribution [21].

4 RESULTS

4.1 Descriptive statistics

4.1.1 Demographics. The questionnaire's demographics section (questions 2-9) gathers general information about the participants, including their gender, age, job sector, and country of work, among

others. This section provides valuable insights into the participants' background and demographic characteristics. The analysis of this data reveals interesting findings. Among the 80 participants, it is observed that a majority of them are males, accounting for 53 participants. Additionally, the majority of participants work in Greece. In terms of age distribution, the most common age range is 25-34 years old, with 45 participants falling within this range, followed by the 35-44 years old category, consisting of 24 participants. Notably, more than half of the participants hold a master's degree, with 42 individuals having this qualification. The participants primarily belong to the Information Technology field, with 36 individuals employed in this sector. Telecommunications and the Business-Finance-Insurance sector follow, with 12 and 11 participants, respectively. Regarding the department within their organization, the majority of participants work in R&D and software development (27 participants), followed by IT (5 participants), Information Security (5 participants), and Legal departments (5 participants). Furthermore, the majority of participants (75 out of 80) hold employee positions, while 5 participants occupy high official positions. The demographic results are visually presented in Table 1.

Gender	
Female	31.25%
Male	66.25%
Non-binary	2.5%
Age	
18-24	10%
25-34	56.25%
35-44	30%
45-54	2.5%
>54	1.25%
Country	
Albania	1.25%
Greece	87.5%
Germany	5%
Netherlands	2.5%
Switzerland	1.25%
USA	2.5%
Education	
Bachelor's Degree	40%
Master's Degree	52.5%
High School Graduate	3.75%
Doctoral Degree	3.75%
Job Sector	
Accommodation	1.25%
Finance	13.75%
Culture & Arts	2.5%
Education	1.25%
Energy	1.25%
Engineering	7.5%
Health Care	1.25%
Information Technology	45%
Law	6.25%
Marketing	2.5%
Physics	1.25%
Public Sector	1.25%
Telecommunications	15%

Table 1: Demographics.

4.1.2 Cyber Security section results. The pivotal section of the survey lies in the results of the Cyber Security section, encompassing questions 11-35 (Table 2). Through their responses, participants demonstrate their level of awareness and adherence to the security guidelines proposed in [36].

Initial, it is notable that a significant portion of participants (70%) have permission to store sensitive corporate data on their personal laptops (Q11 - "Are you allowed to store sensitive data of your organization in your laptop?"). While this is often necessary, it necessitates the implementation of various measures by both the company and its employees to protect such data. One such measure is the encryption of sensitive data by the organization itself. Our survey reveals that in most cases (58.75% participants), organizations indeed encrypt their sensitive data (Q12 - "Does your organization encrypt its sensitive data?"). However, a considerable number of participants stated that their companies do not employ encryption (16.25% participants), while others were uncertain about the existence of encryption measures (25% participants). Another protective measure against data theft is the encryption of employees' laptop storage. According to our survey (Q13 - "Does your organization encrypt your laptop's storage?"), the majority of organizations do not encrypt laptop storage, as indicated by the negative responses from the majority of participants (56.25).

The following set of four questions focuses on connectivity, authentication methods, and system threat models. Notably, a majority of participants (77.5%) employ a second security factor alongside their password 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?"). Additionally, participants indicated that their organizations utilize Network Access Control (NAC) solutions to safeguard access to network nodes, as confirmed by 82.5% of the respondents (Q15 - "Does your organization use Network Access Control (NAC) solutions to secure access to its network nodes?"). However, when asked about whether their organizations have developed system threat models for remote access servers and accessed resources, a majority of participants (52.5%) expressed uncertainty (Q16 - "Has your organization developed system threat models for the remote access servers and the resources that are accessed through remote access?"). Although it is common for this information to be sparingly shared with regular employees, this also suggests a potential lack of emphasis placed by organizations on communicating such important details or a lack of attention from employees towards relevant announcements. This underscores a diminishing emphasis on security for both organizational management and regular employees. Lastly, most participants indicated the use of tunneling (VPN) as their chosen method to connect to their organization's network (Q17 - "Which remote access method do you use to connect to your organization's network?"). The alternative choices included "Application Portals," "Remote Desktop," "Direct Application Access," and "None.".

The next set of three questions pertains to whether organizations have established separate external networks for BYOD (Bring

Your Own Device) devices and the corresponding measures implemented for these networks. Based on the responses (51.25% of the participants), it is evident that most organizations utilize distinct networks for their BYOD employees (Q18 - "Has your organization established separate, external networks for remote and BYOD devices within enterprise facilities?"). However, the nearly equal number of negative responses suggests the need for increased attention by organizations in these cases. Participants who answered "Yes" in the previous question were further asked about the security and 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?"). Of those, more than half (30% of the participants) confirmed that these networks were secured and monitored in line with remote access segments, while 20% of the participants responded with "I do not know". Lastly, responses to the question "Does this networks' traffic pass through a firewall?" (Q20) were divided between "Yes" (35% of the participants) and "I do not know" (16.252% participants). The prevalence of "I do not know" answers in both questions indicates that many employees lack awareness of the security measures implemented by their companies and organizations. This highlights potential weaknesses in communication between higher management and regular employees, or a lack of employee attention to management announcements.

Following that, three questions are presented concerning tools that can enhance the security of users' devices. In the first question (Q21 - "Do you use antimalware software in your laptop?"), 77.5% of the participants responded with "Yes." This is an encouraging finding as it demonstrates the participants' recognition of the various risks associated with viruses. However, 22.5% of the participants responded with "No," indicating that a significant number of participants are exposed to potential virus threats, even if some of them may use more secure operating systems such as Unix-like systems. Similarly, the subsequent question (Q22 - "Do you use a firewall?") yielded comparable results. Once again, 81.25% of the participants confirmed using a firewall, while 18.75% of the participants responded negatively. Those who answered "No," along with their respective organizations, are exposed to risks. These risks encompass unsolicited and unwelcome inbound network traffic originating from malicious sources such as malware or hackers. Generally, a firewall serves as the first line of defense for a computer, safeguarding personal information against the prevalent and ever-evolving cyber threats . In Q23 - "Is your firewall properly configured for the enterprise environment?," the results are evenly divided. This suggests that either the organization has not enforced a security policy for its BYOD employees, or these employees are not adhering to the existing security policy [39]. In either case, the outcome presents potential risks for both the BYOD devices and the organizations permitting their usage. For instance, if a BYOD user fails to comply with the company's security policy that prohibits AnyDesk, there is a possibility that an attacker with knowledge of the user's AnyDesk ID and password could gain full access to the device based on the available permissions. Subsequently, the attacker can pilfer sensitive corporate data and passwords or traverse within the corporate network to gain access to additional resources and potentially sensitive information [24].

Question	Yes (%)	No(%)	I don't Know(%)
Q11	30%	70%	N/A
Q12	58.75%	16.25%	25%
Q13	27.5%	56.25%	16.25
Q14	77.5%	22.5%	N/A
Q15	82.5%	17.5 %	N/A
Q16	26.25%	21.25%	52.5%
Question:		Q17	
Tunneling (VPN)		82.5%	
Remote Desktop		6.25%	
None		7.5%	
Direct Application Access		1.25%	
Applications Portals		2.5%	
Question	Yes (%)	No(%)	I don't Know(%)
Q18	51.25%	48.75%	N/A
Q19	58.5%	2.5%	39%
Q20	68.3%	0%	31.7%
Q21	77.5%	22.5%	N/A
Q22	81.25%	18.75%	N/A
Q23	50%	50%	N/A
Q24	25%	75%	N/A
Q25	72.5%	27.5%	N/A
Q26	12.5%	87.5%	N/A
Q27	10%	90%	N/A
Q28	51.25%	48.75%	N/A
Q29	35%	31.25%	33.75%
Q30	36.25%	63.75%	N/A
Q31	50%	50%	N/A
Question:		Q32	
Daily		20%	
Weekly		15%	
Monthly		27.5%	
Other		35%	
Blank		2.5%	
Question	Yes (%)	No(%)	I don't Know(%)
Q33	70%	30%	N/A
Q34	53.5%	46.5%	N/A
Question	Yes (%)	No(%)	blank(%)
Q35	66.1%	32.1%	1.8%

Table 2: Questions results 11-35

The subsequent two questions center around the security of BYOD users against malicious individuals aiming to steal their physical devices, along with the corporate data stored on them, particularly in shared workspaces like cafes or remote working locations. In Q24 - "Do you use any physical security means to protect your device from theft?" only 25% of the participants responded with "Yes." Consequently, the remaining 75% of the participants are vulnerable to potential device theft by opportunistic thieves. It is important to note that the theft of a personal laptop used for BYOD can have further detrimental effects on the victim's organization. In contrast, in Q25 - "Do you lock your device when you leave your desk?" the majority of participants (72.5% of the participants) answered affirmatively. This crucial practice serves as a deterrent for any potential malicious users who might contemplate taking

advantage of an individual's absence from their device and pilfering sensitive corporate data.

In the subsequent 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 overwhelming majority of participants (87.5%) responded with "No." Consequently, most participants utilize their personal flash drives, which could potentially be infected with viruses or other forms of malware [27]. The risk of infection becomes even greater when participants do not employ antivirus or firewall tools. Similarly, in the following question (Q27 - "Has your organization provided you with a bootable OS and read-only removable media with preconfigured remote access client software?"), 90% of the participants answered with "No." This indicates that participants rely on their own system, including the operating system and software. While it can be sufficient if the user possesses strong knowledge of computer security, in many cases, it is safer to utilize a preconfigured environment developed by security professionals.

In Q28 - "Are the capabilities of your mobile devices limited in your organization's network?" more than half of the participants (51.25%) responded with "Yes." This indicates that the majority of users are restricted from accessing various websites [25, 37] such as Facebook, Instagram, Spotify, and are also prohibited from using Bluetooth while connected to their organization's network. Furthermore, in Q29 - "Does your organization enforce full disk encryption to protect data at rest?", 65% of the participants answered with "No" or "I don't know." This implies a potential risk as data at rest is typically vulnerable to threats from hackers and malicious users who aim to gain access either digitally or through physical theft of the data storage media. Conversely, the remaining 35% of the participants reported having their disks encrypted using specific tools like BitLocker, IBM Guardium, and so on. Lastly, in Q30 - "Does your organization prompt you to use virtual machines (VMs) in order to carry out your job?", 63.75% of the participants answered negatively.

Continuing with the findings from the Cyber Security section, we come across questions related to data backups. In Q31 - "Are you backing up data on your telework device?", the responses are evenly split. Unfortunately, a 50% non-compliance rate in data backups is significant and highlights that many users do not take security risks seriously. Among those who responded "Yes", 11 participants perform backups on a monthly basis, 7.5% of the participants do so weekly, 10% participants do so daily, and 17.5% of the participants selected the option "Other" (Q32 - "If yes, how regularly do you take backups?").

The final three questions in the Cyber Security section pertain to potential security policies within organizations. In Q33 - "Has your organization developed a security policy that defines telework, remote access, and BYOD requirements?", 30% of the participants responded with "No". This substantial number signifies that some organizations may not prioritize cybersecurity adequately. However, it is also plausible that these participants are unaware of their organization's security policy. Among those who answered "Yes" in the previous question, there was nearly an even split when asked whether they had read the security policy of their organization (Q34 - "If yes, did you read the security policy?"). Specifically, 46.5% of the participants replied "No", while 53.5% of the participants replied "Yes". Finally, in regards to Q35 - "Do you put the security policy into practice?", 66.1% of the participants responded "Yes", while 32.1% of the participants responded "No" (with one blank response).

4.1.3 Cyber Awareness section results. The concluding section of the questionnaire encompasses three inquiries relating to participants' familiarity with cybersecurity and any cybersecurity awareness training they may have received. In Q36 - "How familiar are you with Cybersecurity?", participants responded as follows:

- Novice – 30%
- Advanced Beginner – 31.25%
- Competent – 21.25%
- Proficient – 11.25%
- Expert – 6.25%

Question	Yes (%)	No(%)	I don't Know(%)
Q37	62.5%	37.5%	N/A
Q38	78%	22%	N/A

Table 3: Questions results 37-38

These results indicate that a significant number of participants lack experience in cybersecurity, which may explain the weaker outcomes observed in previous questions. Subsequently, participants were asked about their attendance of security awareness trainings in Q37 - "Have you attended any security awareness trainings?". Of the respondents, 62.5% of the participants answered "Yes", while the remaining 37.5% answered "No". This implies that almost 40% of the participants have not attended any security awareness trainings. This further amplifies the risks associated with using BYOD, thereby jeopardizing the security of participants' organizations and companies.

In the final question of the questionnaire (Q38 - "If yes, were these security trainings organized by your company?"), participants who responded "Yes" to the previous question were queried about whether their companies had organized cybersecurity awareness trainings. The outcome revealed that 78% of the participants answered "Yes", while 22% of the participants answered "No". This suggests that the majority of companies are aware of the various hazards associated with using BYOD and are taking steps to educate their employees. However, it should be noted that organizing such trainings does not guarantee complete safety from the various risks posed by BYOD. Nevertheless, these companies are in a relatively safer position compared to those that do not provide such trainings at all. The results of the preceding questions are depicted in Table 3.

4.2 Inferential statistics

In this section, we aim to examine the most captivating outcomes from our survey by utilizing inferential statistics. Specifically, due to the majority of responses being in the form of nominal data (categorical data lacking a value order), we will employ chi-square-tests for independence to assess the independence of response categories. The null hypothesis for each chi-square-test conducted in subsequent pages asserts the absence of any relationship or correlation between the counts of categories and variable values. Conversely,

the research hypothesis posits the existence of an underlying association between them [38]

4.2.1 Correlation between Participants' Cybersecurity Familiarity and Implied Security Measures. We proceed to conduct chi-square tests of independence to explore the potential correlation between security familiarity and other security measures Table 4 taken by the participants of the questionnaire

Variables	chi-square value	df
Security familiarity and using malware	1.246093658.	4
Security familiarity and taking backups	6.209019608	4
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: Job Sector and Organizational Measures implementations

The insignificance of all the aforementioned associations becomes evident as their x^2 values fall below the critical chi-square value (9.488) for df = 4 and a = 0.05. Consequently, it can be concluded that the variables tested are independent of each other, lacking any significant relationship. In a broader context, the results of the x^2 tests indicate that the participants surveyed do not support the hypothesis that a higher level of familiarity with cybersecurity leads to a more secure BYOD device. This realization highlights the potential risks faced by their organizations, which necessitate proactive measures to prevent potential security vulnerabilities, possibly through the implementation of a stringent BYOD security policy.

4.2.2 Correlation between Job Sector and Organizational Measures. In the upcoming test, we will examine the hypothesis that the job sector of participants significantly influences whether companies have implemented a security policy. We posit that due to the reliance on technology in the majority of participants' fields, their respective companies are compelled to establish a security policy to safeguard their digital and physical assets. The null hypothesis contradicts this assertion. Table 4 presents the associations under discussion, with only four job fields included as the remaining fields lacked the necessary number of participants to validate the test.

Table 5 displays the connections between the participants' job sectors and the diverse security measures implemented by their organizations

The analysis of the results presented in Table 5 reveals that the job field of the participants is independent of several factors pertaining to their organizations, including:

- The permission to save sensitive data on their BYOD devices
- The utilization of multi-factor authentication
- The implementation of NAC solutions
- The imposition of limitations on BYOD device capabilities within the organization's network

Variables	chi-square value	df
Job sector and security policy	11.28654602	3
Job sector and sensitive data storage in BYOD devices	0.838231683	3
Job sector and multi-factor authentication	3.752799219	3
Job sector and NAC solutions	0.805232459	3
Job sector and separate, external networks for BYOD users	12.55838143	3
Job sector and limited capabilities for BYOD devices in organization's network	0.520092019	3
Job sector and use of virtual machines	1.567182547	3

Table 5: chi-square test values associated with 'Job Sector and Organizational Measures'

- The employment of virtual machines

However, Regarding the hypothesis concerning the significance of the participants' job sectors in determining whether companies have implemented a security policy (Table 5), the chi-square value of 11.28654602 surpasses the critical statistic, specifically 11.28654602 > 7.815. This outcome indicates a significant relationship between the job sector of the participants and the security policy of their organizations. Furthermore, the test examining the independence between the job sectors of the participants and the presence of distinct external networks for BYOD users within their organizations yields significant results. Specifically, the chi-square value (x^2 = 12.55838143) exceeds the critical threshold of 7.815. Notably, this outcome primarily stems from the responses of participants in the Telecommunications field, as 11 out of 12 individuals reported that their organizations have implemented separate, external networks for BYOD usage. Thus, based on our sample, it can be inferred that the job sector can influence the establishment of external networks for BYOD users, indicating a dependent relationship between these two variables.

5 LIMITATIONS

Like any research based on questionnaires, this study has its limitations. The first limitation pertains to the method of collecting survey responses, as discussed in Section 3 - Methodology. The survey was promoted through internet channels and various contact networks, including Facebook groups, LinkedIn, working groups, and forums. Consequently, the collected sample is not entirely independent, and the randomness of the survey is constrained due to the self-selection bias commonly observed in internet surveys.

Another limitation is the composition of the questionnaire recipients, with the majority falling within the 25-34 age range, predominantly well-educated, and mainly originating from Greece. To enhance the quality and validity of the results, a more diverse range of participants from different countries, age groups, and educational backgrounds would be beneficial. Similarly, the distribution of job sectors among the questionnaire recipients is skewed, with a predominant presence of participants from the Information Technology field. This bias implies that the participants in this study likely possess greater knowledge in computer security compared

to individuals from other fields, which may influence the outcomes and potentially lead to inflated results regarding computer security awareness.

Lastly, a larger sample size would improve certain aspects of the statistical analysis, particularly the chi-square tests for independence. With a larger sample, the tests would yield more robust outcomes by enhancing the statistical power. This increase in sample size would provide more reliable results as the correlations between different tables would become more representative and ensure greater confidence in the chi-square tests.

6 DISCUSSION

The results of our survey reveal intriguing patterns and behaviors, which will be thoroughly discussed in this section, addressing the three research questions that guided our investigation. In order to draw meaningful conclusions, we compare the survey findings with the guidelines for BYOD provided by NIST [36], which served as the foundation for designing the survey questions.

Regarding R1 – "Are BYOD users careful when using their personal laptop devices in their organizations?", The following interesting facts emerge from our findings. Firstly, 77.5% of the participants use antimalware software on their devices, while 81.25% of the participants utilize a firewall. These percentages indicate a high adherence to NIST guidelines, which recommend the use of antimalware software and firewalls in BYOD devices. However, the remaining participants are at significant risk. According to the SonicWall Cyber Threat Report [9], there were billions of malware attacks, ransomware attacks, and intrusion attempts in 2022, emphasizing the importance of these security measures for both personal and corporate devices [5, 6, 31]. Regarding firewalls, only 50% of the participants stated that their firewall is properly configured for the enterprise environment, which raises concerns as it deviates from NIST guidelines.

Another concerning finding pertains to the use of physical security measures to protect devices from theft. Only 25% of the participants employ cable locks or other deterrents, leaving their devices vulnerable to theft in various locations. Research by Gartner reveals that a laptop is stolen every 53 seconds, while the University of Pittsburgh highlights a mere 2% chance of recovery for stolen laptops [14]. Therefore, BYOD users should prioritize the physical security of their devices by implementing preventive measures against theft. Fortunately, when it comes to screen locking, 72.5% of the participants lock their devices when leaving their desks. However, nearly 30% of the participants do not follow the NIST guideline, jeopardizing important corporate and personal information. Additionally, 50% of the survey participants do not back up their data, which is a high percentage considering the potential risks such as data deletion, security incidents, and hardware failures. Lastly, 53.6% of the participants read their organization's security policy, while approximately 66% of the participants actually implement it. These percentages are relatively low, indicating that the surveyed BYOD users do not prioritize their organization's security policy. However, it is also the responsibility of each organization to enforce rules for their employees [17].

In conclusion, it is crucial for BYOD users to exercise greater caution regarding the security of their devices [29, 30]. Several of the aforementioned percentages raise significant concerns. One potential solution could involve scheduling security awareness trainings conducted by management to enhance employee awareness. It is noteworthy that the inferential statistics results (Security measures implied by the participants are correlated with their Cybersecurity familiarity) indicate that familiarity with cybersecurity does not necessarily lead to a more secure BYOD device, as even advanced users may follow weak practices.

Regarding R2 "Are BYOD users aware of the security measures implied on them by their organizations?", We analyzed the more complex survey questions that included the option "I do not know" and obtained the following data. Initially, 25% of the BYOD users were uncertain about whether their organization encrypts sensitive data, while 16.25% of the participants were unaware of whether their organization encrypts their device storage. These percentages are concerning, particularly the latter (16.25%), which indicates a lack of awareness among employees regarding the software running on their devices. Furthermore, 52.5% of the participants were unsure if their organizations had developed system threat models for remote access servers and accessed resources. As previously discussed, while this may not be a widely known countermeasure, the high percentage of unaware employees is problematic, highlighting a communication gap between management and employees.

Subsequently, 39% of the BYOD users did not know if their organizations' external networks for remote and BYOD devices were secured and monitored in a manner consistent with remote access segments, and similarly, 31.7% of the participants were uncertain if the network traffic passed through a firewall. Finally, 33.75% of the BYOD users were unsure if their organization enforced full disk encryption to protect data at rest. These percentages are significantly high, indicating a lack of knowledge among BYOD users regarding the security measures implemented by their organizations.

Regarding R3 – "Do organizations implement the appropriate levels of security when they allow BYOD?", Firstly, 78.3% of the participants reported their organizations using encryption methods for sensitive data. Additionally, 32.8% of the participants stated that their organization encrypts employees' device storage. In terms of authentication, 77.5% of the participants use a second type of authentication when connecting to their company network. However, organizations should be cautious not to overly complicate the authentication process for employees. Regarding security measures, 82.5% of BYOD users mentioned their organizations using Network Access Control (NAC) solutions. However, only 51.25% of the participants reported separate networks for remote and BYOD devices, and 55.3% of the participants stated the existence of system threat models for remote access servers and resources. Most organizations seem confident in their existing security measures and are not inclined to invest further. Nevertheless, organizations with separate networks for BYOD users expressed high levels of security and monitoring. Regarding remote access, 82.5% of the participants utilize Virtual Private Networks (VPNs) to connect to their organization's network. Only 7.5% of the participants do not use any remote access method. However, 48.75% of the participants mentioned their organizations not imposing limitations on personal devices' capabilities, which poses risks such as malware spread and reduced bandwidth availability. Most organizations allow employees to use their own devices without pre-configured environments.

Specifically, 90% of the participants do not use bootable OS or read-only removable media with pre-configured remote access client software, and 63.75% of the participants are not prompted to use Virtual Machines (VMs). Establishing a security policy is crucial for maintaining device security [11, 18]. Approximately 70% of participants reported their organizations having a security policy defining telework, remote access, and BYOD requirements. However, there is room for improvement in this area.

While many companies are aware of the potential risks associated with BYOD and are taking steps to educate their employees, there are various ways organizations can further enhance security awareness and education among their workforce. Exploring practical strategies and interventions can be instrumental in achieving this goal. For instance, incorporating gamification elements into security training programs can transform the learning process into an engaging and interactive experience. By utilizing interactive learning techniques, offering rewards and incentives, and implementing leaderboards, organizations can effectively motivate employees and encourage active participation.Another valuable approach is the use of scenario-based simulations, which provide a safe environment for employees to gain firsthand experience with real-world security scenarios. By immersing employees in simulated situations, organizations can help them develop crucial skills and decision-making abilities. Recognizing and showcasing employees' security knowledge and expertise through badging and certification systems can further encourage their commitment to maintaining a secure work environment.Moreover, fostering collaboration and promoting shared responsibility among teams is vital for maintaining security. Team-based activities can facilitate knowledge sharing, problem-solving, and collective vigilance, enabling employees to collectively contribute to the overall security posture of the organization. [13, 19, 33]. However, it is important to acknowledge that implementing these measures and exploring additional strategies does not guarantee absolute protection against all risks. Nevertheless, companies that invest in security training and awareness programs are generally in a more secure position compared to those that neglect such initiatives altogether.

In conclusion, while most organizations have implemented a satisfactory level of security for BYOD, enhancements can be made in security policies and additional security measures. The influence of job sectors, such as Information Technology and Telecommunications, on security policies and separate networks should be taken into account.

7 CONCLUSION

In general, there is a pressing need for BYOD users to prioritize the security of their devices. Although they predominantly rely on conventional security measures such as antimalware software and firewalls, they often neglect other equally critical practices like backing up data or securing their devices against theft, despite being aware of the potential risks posed to their organizations. As previously mentioned, addressing this issue would involve the inclusion of cybersecurity and safety education within school and university curricula [2]. Simultaneously, companies should consistently schedule security awareness training sessions to enhance employees' awareness of security practices.

However, our findings highlight that even advanced users with higher levels of security familiarity exhibit weak security practices. This implies that education alone will not fully resolve the issue, as employees tend to underestimate security risks. Consequently, the responsibility for addressing employees' behavior lies with the respective organization. Specifically, while organizations, in general, have implemented a commendable level of security when allowing BYOD, the most crucial step is to enforce security policies that clearly define rules for BYOD usage. Additionally, organizations should effectively communicate these policies to their employees, emphasizing the importance of adherence and the potential benefits that can be achieved.

The survey results indicate several areas that warrant further exploration in future research. For instance, a significant aspect that has already been discussed in previous sections of this document and merits further investigation is the tendency of BYOD users to neglect security measures, regardless of their level of security familiarity. Specifically, it would be intriguing to comprehend why advanced BYOD users (those with higher cybersecurity familiarity) tend to overlook certain security measures despite being aware of the various risks involved.

Furthermore, another intriguing question pertains to the actions taken by organizations that permit BYOD after experiencing a cyberattack [10]. For instance, do they enforce stricter rules for their BYOD employees? Do they enhance their systems in alignment with existing BYOD guidelines? How do they handle their BYOD employees in response to such incidents? Do they organize cybersecurity awareness trainings? Exploring their responses and evaluating the potential positive effects on these organizations would be particularly captivating.

ACKNOWLEDGMENTS

This research has received funding from European Commission's Horizon Europe and Horizon 2020 research and innovation programs under grant agreements No. 823997 (SECONDO), No. 824014 (INCOGNITO), No. 101092702 (OASEES), and No. 101070214 (TRUSTEE).

REFERENCES

[1] Khoula AlHarthy and Wael Shawkat. 2013. Implement network security control solutions in BYOD environment. In *2013 IEEE International Conference on Control System, Computing and Engineering*. 7–11. https://doi.org/10.1109/ICCSCE.2013.6719923

[2] Iosif Androulidakis and Gorazd Kandus. 2011. Mobile phone security awareness and practices of students in budapest. In *Proceedings of the 6th International Conference on Digital Telecommunications*. 17–22.

[3] Emma Bell, Alan Bryman, and Bill Harley. 2022. *Business research methods*. Oxford university press.

[4] Beyond Identity Blog. 2021. BYOD: Exploring the evolution of work device practices in a new remote-forward era [survey]. https://www.beyondidentity.com/blog/byod-exploring-evolution-work-device-practices-survey

[5] Panagiotis Bountakas, Christoforos Ntantogian, and Christos Xenakis. 2022. EKnad: Exploit Kits' network activity detection. *Future Generation Computer Systems* 134 (2022), 219–235.

[6] Panagiotis Bountakas and Christos Xenakis. 2023. Helphed: Hybrid Ensemble Learning Phishing Email Detection. *Journal of Network and Computer Applications* 210 (2023), 103545.

[7] Chris Caldwell, Steven Zeltmann, and Ken Griffin. 2012. BYOD (bring your own device). In *Competition forum*, Vol. 10. American Society for Competitiveness, 117–121.

[8] Jericho Concepcion, Jed Chua, Gregory Siy, and A Ballon. 2015. Securing android byod (bring your own device) with network access control (nac) and mdm (mobile device management). In *Teoksessa Proceedings of the DLSU Research Congress*, Vol. 3. 2–4.

[9] IN DEN, SECHS MONATEN, PROFITIEREN VON, DER PANDEMIE, PRÄZISER ALS, JE ZUVOR, IST IHR STAAT DURCH EINEN, and CYBERANGRIFF GEFÄHRDET. 2021. Sonicwall cyber threat report. (2021).

[10] Aristeidis Farao, Sakshyam Panda, Sofia Anna Menesidou, Entso Veliou, Nikolaos Episkopos, George Kalatzantonakis, Farnaz Mohammadi, Nikolaos Georgopoulos, Michael Sirivianos, Nikos Salamanos, et al. 2020. SECONDO: A platform for cybersecurity investments and cyber insurance decisions. In *Trust, Privacy and Security in Digital Business: 17th International Conference, TrustBus 2020, Bratislava, Slovakia, September 14–17, 2020, Proceedings 17*. Springer, 65–74.

[11] Aristeidis Farao, Eleni Veroni, Christoforos Ntantogian, and Christos Xenakis. 2021. P4G2Go: A Privacy-Preserving Scheme for Roaming Energy Consumers of the Smart Grid-to-Go. *Sensors* 21, 8 (2021), 2686.

[12] George Petihakis, Dimitrios Kiritsis, Panagiotis Bountakas, Aristeidis Farao, Aggeliki Panou, and Christos Xenakis. 2023. The complete questionnaire of the survey. https://drive.google.com/open?id=1csWu_GXKfAn4_4U61GMg-KHKi3XqrYvX&usp=drive_fs. Online; Last Accessed: 05/2023.

[13] Eyvind Garder B Gjertsen, Erlend Andreas Gjære, Maria Bartnes, and Waldo Rocha Flores. 2017. Gamification of Information Security Awareness and Training.. In *ICISSP*. 59–70.

[14] Grand Canyon University. 2019. A Lost Laptop Is a Cybersecurity Threat. https://www.gcu.edu/blog/engineering-technology/lost-laptop-cybersecurity-threat. Online; Last Accessed: 05/2023.

[15] Kemal Hajdarevic, Pat Allen, and Mario Spremic. 2016. Proactive security metrics for Bring Your Own Device (BYOD) in ISO 27001 supported environments. In *2016 24th Telecommunications Forum (TELFOR)*. IEEE, 1–4.

[16] Bob Hayes and Kathleen Kotwica. 2013. *Bring your own device (BYOD) to work: Trend report*. Newnes.

[17] Ioannis Kalderemidis, Aristeidis Farao, Panagiotis Bountakas, Sakshyam Panda, and Christos Xenakis. 2022. GTM: Game Theoretic Methodology for optimal cybersecurity defending strategies and investments. In *Proceedings of the 17th International Conference on Availability, Reliability and Security*. 1–9.

[18] Marios Karatisoglou, Aristeidis Farao, Vaios Bolgouras, and Christos Xenakis. 2022. BRIDGE: BRIDGing the gap bEtween CTI production and consumption. In *2022 14th International Conference on Communications (COMM)*. IEEE, 1–6.

[19] Khando Khando, Shang Gao, Sirajul M Islam, and Ali Salman. 2021. Enhancing employees information security awareness in private and public organisations: A systematic literature review. *Computers & security* 106 (2021), 102267.

[20] Alex Koohang, Kevin Floyd, Neil Rigole, and Joanna Paliszkiewicz. 2018. Security policy and data protection awareness of mobile devices in relation to employees' trusting beliefs. *Online Journal of Applied Knowledge Management* 6 (04 2018), 7–22. https://doi.org/10.36965/OJAKM.2018.6(2)7-22

[21] Henry Oliver Lancaster and Eugene Seneta. 2005. Chi-square distribution. *Encyclopedia of biostatistics* 2 (2005).

[22] Kenneth C Laudon and Jane P Laudon. 2015. *Management information system*. Pearson Education India.

[23] Feng Li, Chin-Tser Huang, Jie Huang, and Wei Peng. 2014. Feedback-based smartphone strategic sampling for BYOD security. In *2014 23rd International Conference on Computer Communication and Networks (ICCCN)*. 1–8. https://doi.org/10.1109/ICCCN.2014.6911814

[24] Qingyun Liu, Jack W Stokes, Rob Mead, Tim Burrell, Ian Hellen, John Lambert, Andrey Marochko, and Weidong Cui. 2018. Latte: Large-scale lateral movement detection. In *MILCOM 2018-2018 IEEE Military Communications Conference (MILCOM)*. IEEE, 1–6.

[25] Gloria Mark, Mary Czerwinski, and Shamsi T Iqbal. 2018. Effects of individual differences in blocking workplace distractions. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. 1–12.

[26] Keith Miller, Jeffrey Voas, and G.F. Hurlburt. 2012. BYOD: Security and Privacy Considerations. *IT Professional* 14 (09 2012), 53–55. https://doi.org/10.1109/MITP.2012.93

[27] Paul Mueller and Babak Yadegari. 2012. The stuxnet worm. *Département des sciences de linformatique, Université de lArizona. Recuperado de: https://www2.cs. arizona. edu/˜ collberg/Teaching/466-566/2012/Resources/presentations/topic9-final/report. pdf* (2012).

[28] Musa Abubakar Muhammad, Aladdin Ayesh, and Pooneh Bagheri Zadeh. 2017. 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*. 1–8.

[29] Antonio Muñoz, Aristeidis Farao, Jordy Ryan Casas Correia, and Christos Xenakis. 2020. ICITPM: integrity validation of software in iterative continuous integration through the use of Trusted Platform Module (TPM). In *Computer Security: ESORICS 2020 International Workshops, DETIPS, DeSECSys, MPS, and SPOSE, Guildford, UK, September 17–18, 2020, Revised Selected Papers 25*. Springer, 147–165.

[30] Antonio Muñoz, Aristeidis Farao, Jordy Ryan Casas Correia, and Christos Xenakis. 2021. P2ISE: Preserving Project Integrity in CI/CD Based on Secure Elements. *Information* 12, 9 (2021), 357.

[31] Christoforos Ntantogian, Panagiotis Bountakas, Dimitris Antonaropoulos, Constantinos Patsakis, and Christos Xenakis. 2021. NodeXP: NOde. js server-side JavaScript injection vulnerability DEtection and eXPloitation. *Journal of Information Security and Applications* 58 (2021), 102752.

[32] Ezer Osei Yeboah-Boateng and Francis Edmund Boaten. 2016. Bring-Your-Own-Device (BYOD): An Evaluation of Associated Risks to Corporate Information Security. *arXiv e-prints*, Article arXiv:1609.01821 (Sept. 2016), arXiv:1609.01821 pages. https://doi.org/10.48550/arXiv.1609.01821 arXiv:1609.01821 [cs.CR]

[33] Karzan H Sharif and Siddeeq Y Ameen. 2020. A review of security awareness approaches with special emphasis on gamification. In *2020 International Conference on Advanced Science and Engineering (ICOASE)*. IEEE, 151–156.

[34] Thomas Shumate and Mohammed Ketel. 2014. Bring your own device: Benefits, risks and control techniques. In *Ieee Southeastcon 2014*. IEEE, 1–6.

[35] Manmeet Mahinderjit Singh, Chen Wai Chan, and Zakiah Zulkefli. 2017. Security and privacy risks awareness for bring your own device (BYOD) paradigm. *International Journal of Advanced Computer Science and Applications* 8, 2 (2017).

[36] Murugiah Souppaya and Karen Scarfone. 2016. Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security. https://doi.org/10.6028/NIST.SP.800-46r2

[37] Vincent W-S Tseng, Matthew L Lee, Laurent Denoue, and Daniel Avrahami. 2019. Overcoming distractions during transitions from break to work using a conversational website-blocking system. In *Proceedings of the 2019 CHI conference on human factors in computing systems*. 1–13.

[38] Antony Ugoni and Bruce F Walker. 1995. The Chi square test: an introduction. *COMSIG review* 4, 3 (1995), 61.

[39] Fulvio Valenza and Manuel Cheminod. 2020. An Optimized Firewall Anomaly Resolution. *J. Internet Serv. Inf. Secur.* 10, 1 (2020), 22–37.

[40] Yong Wang, Jinpeng Wei, and Karthik Vangury. 2014. Bring your own device security issues and challenges. In *2014 IEEE 11th Consumer Communications and Networking Conference (CCNC)*. 80–85. https://doi.org/10.1109/CCNC.2014.6866552

[41] Tafheem Ahmad Wani, Antonette Mendoza, and Kathleen Gray. 2020. Hospital Bring-Your-Own-Device Security Challenges and Solutions: Systematic Review of Gray Literature. *JMIR Mhealth Uhealth* 8, 6 (18 Jun 2020), e18175. https://doi.org/10.2196/18175

[42] Dean Wiech. 2013. The benefits and risks of BYOD. *Manufacturing Business Technology* 28 (2013).

[43] ZIPPIA THE CAREER EXPERT. 2022. 26 SURPRISING BYOD STATISTICS [2023]: BYOD TRENDS IN THE WORKPLACE. https://www.zippia.com/advice/byod-statistics/. Online; Last Accessed: 05/2023.