University of Piraeus

Postgraduate Program
M.Sc. *Digital Systems Security*

Master's Thesis

Security Unawareness

Zamanis Georgios
MTE 1909

Supervisor
Prof. Christos Xenakis

May, 2022

This document reflects the results of a study that has been prepared on behalf of the Postgraduate Program "Digital Systems Security" at University of Piraeus. The information and conclusions contained in this thesis express the author's personal, opinion and arguments, and therefore should not be interpreted that they represent the official concepts of University of Piraeus.

Abstract

In an era where mobile smartphones are used in every aspect of our work life, every organization's data can exist in multiple smartphones, regardless of their significance. Furthermore, the same smartphones ease our lives being used as a tool for entertainment, navigation and access to valuable personal information. Regardless of these many benefits, the same smartphones may be used as a way to exploit valuable information and data for both users and every organization’s data, which can be crucial to the business need. This thesis, aims to find out the degree of maturity regarding the awareness and proper ways of using smartphones, from the aspect of cyber security for both technological measures and knowledge of both users, by using their personal smartphones for work related issues (BYOD) and organizations, issuing smartphones for work-related matters. The conducted survey produced interesting results regarding organizations following the guidelines of ENISA and NIST for proper smartphone practices in the working environment. Examining the findings, overall actions show positive remarks in comparison to the previous years, organizations still should begin enforcing security for smartphones according to appropriate official guidelines.

Keywords: Smartphone, ENISA, NIST, EMM, awareness, BYOD, organization-issued

Table of Contents

1. Introduction

Smartphones have become a must have tool for every person, due to the accessibility and versatility that they offer. It can be almost collated to a fully functional personal computer just in the palm of every user's hand. As a result, personal data and accounts are being used more and more with the purpose of easing of our daily lives. A significant aspect of daily for the majority of people is their job, so with the use of the same smartphones a new range of tools is presented for many organizations, offering better productivity and accessibility to data, and sometimes helping employees do their job on the go.

As times go by, many organizations such as the private sector, public administration and even the military, have started to accept those devices and even seen their use as an opportunity in order to improve their productivity and budget, by issuing those smartphones to their employees. With this way they can have all the necessary tools and gain access to various resources inside and outside of their working environment with the proper access and control measures. On the other hand, some organizations, employing a different way of thinking, allow employees to do the same but with their own personal devices (BYOD) without consideration of access and control measures.

It is only natural that those devices will be targeted by adversaries with the purpose of breaching their defenses, considering that the same users that use those tools are always considered the most vulnerable to attacks (social engineering attacks) or aiming the vulnerabilities of the smartphones. Additionally most of the smartphones contain not only the data of the organization but every user's personal, and sometimes, sensitive data and accounts. Finally, by installing various applications) considering the access they have (e g. Wi-Fi, GPS, SMS and tethering) the smartphones can be abused even in scenarios of creating bot networks.

In current times, with the coronavirus pandemic having led to unprecedented conditions, the usage of smartphones has become crucial. Modes of daily work life has been transformed due to government restrictions and are taken place outside the workplace (remote work, home office work). Smartphones changed various organizations' resources, for example, replacing the typical VoIP connectivity, meetings in person and gaining access to sensitive resources and servers. Research shows that during the pandemic most of the organizations have been targeted with various cyberattacks to a significant increased number (Interpol, 2020). As expected, cybersecurity is becoming an important issue to be considered as employees have been forced into using their own devices.

This new phenomenon of widespread use of smartphones in the workplace raises many questions:
R1.Are organizations mature enough to understand that smartphones have become more evolved to the point that their security needs to be on a level equal to that of a regular laptop?
R2. Do users understand the need to follow proper guidelines in order to keep their personal information and organization's resources safe?

R3. Have organizations invested more resources in the security of smartphones in the midst of pandemic?

R4. Do organizations follow proper official guidelines in order to allow smartphones to enter their infrastructure therefore gain access to organization's data?

This thesis includes the following sections: Prior Work - examining the work of previous researches about smartphone security. Guidelines Summary - Explaining briefly the guidelines of ENISA and NIST and their focus. Methodology - Analyzing the survey methodology, through the questions created by the guidelines and how presented to the subjects. Analysis - analyzing the survey answers with the use of statistical tools and raising our concerns. Discussion - Examining our results in combination with the four research questions primarily used to launch the survey and perform check for association between pairs of questions for statistical interests. Finally, the last section Conclusion and future work - making conclusion remarks and examining future possibilities.

2. Prior Work: What do we know so far?

Smartphones have capture the research interest for researchers for the last 15 years. Traditionally companies could be considered as "immature" as they forbade users to bring their own smartphones as all mobile devices were considered personal entertainment and disregarded as a tool for work. The first field of study for researchers was the malwares. Early studies (McAfee Labs, 2009) observed that malwares started targeting more high level devices, leaving the traditional attacks and becoming more and more sophisticated in order to gain more profit. This occurred due to the fact that mobile phones have become more "smart" and have been widespread to everyone. In addition, Android and iOS (PandaLabs, 2011) have become more popular to the point that customized malwares become more dangerous (Cisco, 2011). At this point users do not possess the train of thought of securing their smartphones, or to think about the impact on their data. As is the more natural thing to do, the main focus of all studies was on authentication methods and mechanisms used by users to unlock their smartphones. In contrast with the previous researchers, the main focus was the lack of technology in security measures. In years this changed as smartphones entered the market of industries and into the daily life of every user. Studies began to arise regarding the users' awareness of security measures through surveys and for organizations regarding the use of smartphones (BYOD) and associated policies.

Concerning the user's awareness, Androulidakis and Kandus (2011) created a survey through a questionnaire based mainly on the knowledge of the users and their behavior and not business like. Their survey showed that users do not care about their privacy, even if new security capabilities are offered to them. Harris et al. (2013) published the results of their survey conducted among college students entering the workforce, demonstrating a lack of security awareness due to the high increase of smartphone usage and the rise of BYOD method. The results showed that 75% of the users believed that it is responsibility of organizations to train and raise the users' awareness in order to increase their security on corporate data. The paper also reviews some major security concerns regarding the mobile devices and makes some general security recommendations for devices in organizations. A year later, Markelj and Bernik (2014) published a study survey that tried to assess the level of knowledge an average user have regarding security threats and what is their response to those threats. The survey concluded that users are in need to raise security awareness and should be educated about cyberspace work safety. A few months later, Cherapau et al. (2015)

published a survey in order to discover if Apple users are taking advantage of Touch ID technology , released the same year, in order to enforce the security of their passwords in contrast to weaker technologies (e.g. 4-digit PINs). The conclusion was that users do not took advantage of the Touch ID, 30% of users were not aware of the existence of additional security measures (e.g. password instead of PINs) and users feedback for Touch ID technology was regarding the conveniences it offered rather than the security. Bitton et al. (2016), published a paper named in order to create a factor of mobile security awareness (MSA) for users in order to understand how susceptible the human factor is in an event of an attack. The factor focused in 4 main areas: “applications”, “browsing & communication”, “communication channels” and “device” expanded to security focus matters. The purpose of the study was to find how organizations should invest in user awareness for their own security matters. Their study outcome suggests that organizations and users have begun to realize the importance of securing their mobile phones. Alani (2016) published a survey focused on android users based on privacy and leaks through malware/adware and permissions options due to the fact that android had the 80% percent of the market. The results showed that awareness of privacy in android users had weaknesses regarding their data due to flaws like rooted devices, lack of extra security applications and users' neglecting of proper ways of installing and examining the applications. Breitinger et al. (2020) created a survey focused on younger generations (born between the years 1984 - 2012), regarding users' awareness, choices and education in respect of cybersecurity towards their smartphones. The results showed that sample's physical access to smartphone was appropriate, the sample had total disregard for addition cybersecurity practices (e.g. Use of VPN in public Wi-Fi).

Regarding organizations’ practices, Leavitt (2013) raised questions about how companies adopt the BYOD model and become essential and something permanent. Suggesting organizations to enforce their security more and previous mobile-security approaches alone won’t protect BYOD environments. As a solution Mobile-application management is encouraged. Additionally, Kravets et al. (2014) encourage the use of technologies like Mobile device management (MDM), similar to the previous study and close to the NIST guide suggestions. The study shows how MDM technology will allow both organization-issued and BYOD smartphones to enter the network. In spite of previous studies it focuses more on technical and networking aspects offering architectural solutions. Finally, Chigona et al. (2011) attempted to study the privacy and security measures for BYOD smartphones between personal data and separating organizations data, due to their rise. The study suggests that organizations should reconsider their policies addressing personal smartphones due to data security and privacy conflict between personal and corporate data.

In sum, it can be observed a gradual transformation of the focus of the studies overtime which has involved from studying the vulnerabilities of a smartphone device reaching to a point that shows that organizations are not taking into consideration the rise of smartphone usage in their procedures and are not still ready to implement them into their systems. The above results informed efforts to define and publish a set of guidelines which would help organizations and publish a set of guidelines which will help organizations to oversee the use to oversee the use of smartphones in the workplace and guarantee relevant procedures and infrastructure.

3. Guidelines summary

In order to raise awareness among organizations about the security requirements involved in the safeguarding of their infrastructure/systems ENISA and NIST (cybersecurity institutes of Europe and North America respectively) have created their own guideline each assisting organizations to implement proper measures for the use of smartphones in their systems.

ENISA's guidelines are summarized in the report "Smartphones Information security risks, opportunities and recommendations for users" (Hogben and Dekker, 2010) and demonstrates a more user oriented approach ranking important security risks and opportunities for users and provides recommendations on how to handle them. The devised user ranks are: Consumer, Employee and High official. Consumer, for ENISA, uses his smartphone for his personal activities in his daily life. This includes from phone calls to internet browsing, also personal data as well as sensitive information that can be used by various applications. According to ENISA employees refers to the category where the smartphone is used for business or government purposes such as phone calls, video conferencing and tasks. The usage of this smartphone is considered to have policies installed from the IT department, set by IT officers thus limiting the usage for personal purposes. ENISA considers High officials employees such as top-level management, where the smartphone's usage has access to sensitive information and tasks. The usage is highly restricted by security policies and very limited customized functionality such as cryptographic modules. Additionally, ENISA considers that these smartphones sometimes can be used by some close aides such as secretaries etc.
Some ENISA recommendations according user rank/category include:

- *Consumer:*

Automatic locking: configure the smartphone in such a way that it locks automatically after some minutes.
Check reputation: before installing or using new smartphone apps or services, check their reputation. Never install any software onto the device unless it is from a trusted source and you were expecting to receive it.
Scrutinize permission requests: scrutinize permission requests when using or installing smartphone apps or services.
Reset and wipe: before disposing of or recycling their phone, wipe all the data and settings from the smartphone.

- *Employees:*

Confidentiality: use memory encryption for the smartphone memory and removable media.
Decommissioning: before being decommissioned or recycled, apply a thorough decommissioning procedure, including memory wipe processes.
App installation: if any sensitive corporate data is handled or if the corporate network is accessible to the smartphone then define and enforce an app whitelist.

- *High Officials:*

No local data: do not store sensitive data locally and only allow online access to sensitive data from a smartphone using a non-caching app.
Encryption software: for highly confidential usage, use additional call and SMS encryption software for end-to-end confidentiality.

Periodic reload: smartphones may be periodically wiped (using secure deletion) and reloaded with a specially prepared and tested disk image.
Confidentiality: use memory encryption for the smartphone memory and removable media.
Decommissioning: before being decommissioned or recycled, apply a thorough decommissioning procedure, including memory wipe processes.
App installation: if any sensitive corporate data is handled or if the corporate network is accessible to the smartphone then define and enforce an app whitelist.

We will mainly focus on the latter two. Although ENISA supports that recommendations for consumers should be applied to employees and those for employees to high officials. Furthermore, ENISA created an informed assessment of the information security and privacy risks of using smartphones, with more practical recommendations on how to address these risks. It considers the optimal objective as to allow users, businesses and governments to take every advantage of the opportunities and capabilities offered by smartphones while minimizing the information security risks to which they can be exposed.

ENISA's report analyses 10 information security risks for smartphone users and 7 information security opportunities. It makes 20 recommendations to address the risks.

***Risks*:**

- R1. Data leakage: a stolen or lost phone with unprotected memory allows an attacker to access the data on it.
- R2. Improper decommissioning: the phone is disposed of or transferred to another user without removing sensitive data, allowing an attacker to access the data on it.
- R3. Unintentional data disclosure: most apps have privacy settings but many users are unaware (or do not recall) that the data is being transmitted, let alone know of the existence of the settings to prevent this.
- R4. Phishing: an attacker collects user credentials (e.g. Passwords, credit card numbers) using fake apps or (SMS, email) messages that seem genuine.
- R5. Spyware: the smartphone has spyware installed allowing an attacker to access or infer personal data. NB spyware includes any software requesting and abusing excessive privilege requests. It does not include targeted surveillance software (R7).
- R6. Network spoofing attacks: an attacker deploys a rogue network access point and users connect to it. The attacker subsequently intercepts the user communication to carry out further attacks such as phishing.
- R7. Surveillance: spying on an individual with a targeted user's smartphone.
- R8. Diallerware: an attacker steals money from the user by means of malware that makes hidden use of premium SMS services or numbers.
- R9. Financial malware: malware specifically designed for stealing credit card numbers, online banking credentials or subverting online banking or ecommerce transactions.
- R10. Network congestion: network resource overload due to smartphone usage leading to network unavailability for the end-user.

Opportunities:

- O1. Sandboxing and capabilities: most smartphones use sandboxes for apps and capability-based access control models.
- O2.Controlled software distribution: gives providers the opportunity to have more control over app security by vetting apps submitted for security flaws and removing insecure apps.
- O3. Remote application removal: functionality allowing removal of malware from devices after installation.
- O4. Backup and recovery: most smartphones ship with convenient backup and recovery functions to address risks to data availability
- O5. Extra authentication options: smartphones can function as a smartcard reader, giving additional options for authentication and non-repudiation.
- O6. Extra encryption options: several third-party applications are now offering encryption for smartphone voice calls, on top of the standard encryption provided by mobile network operators.
- O7. Diversity: smartphones are diverse in terms of hardware and software, which makes it more difficult to attack a large group of users with one virus.

Recommendations:

- Addressing the risk of device theft or loss
- Addressing the risk of unintentional disclosure of data
- Addressing the risk of attacks on decommissioned phones
- Addressing the risk of phishing attacks
- Addressing the risks of malware attacks
- Addressing the risks of network spoofing
- Addressing the risk of surveillance attacks

NIST's guidelines are summarized in the report "Guidelines for Managing the Security of Mobile Devices in the organization" (Franklin et al., 2020) addresses the subject more technically and addresses to IT staff. The purpose of their publication is to assist organizations with securing and managing every smartphone device. It begins by recommending that organizations should conduct a threat analysis for mobile devices and for every information system accessed from smartphones. Then, those organizations should employ organization Mobility Management, Mobile Threat Defense, and other applicable organization mobile security technologies helping to manage smartphones both company-issued and BYOD. Also, suggests to regularly maintain mobile device security through log monitoring and vulnerability assessments. Additionally, if a company provides a smartphone should be more careful with the smartphone's lifecycle and any new device should be implemented and test a pilot solution before putting the solution into production, fully secure each organization-issued mobile device before allowing a user to access the organization's systems or information and should keep smartphone's operating systems and apps updated. Finally, NIST's publication analyzes every threat to smartphones and to device management systems and offers mobile security technologies (both smartphones and management systems). Also, recommend mitigations and countermeasures, and thorough explanation of the mobile device deployment lifecycle through risk assessments, auditing and choosing strategies.

Worth mentioning is that NIST (in contrast to ENISA ranking) has categorized the smartphones rather than the users. The three types are strict organization Usage, Corporate Owned Personally Enabled (COPE) and BYOD and Choose Your Own Device (CYOD). The strictly organization usage smartphones are organization-issued devices with very limited personal use. NIST considers those devices to have many common basic applications removed (e.g. Texting), limited access to various functionalities (e.g. Wi-Fi) and to be fully managed by a MDM device ownership status. COPE devices are issued by the organization to employees. While the organization owns (or leases) the device, like the previous rank, and enforces usage restrictions, these restrictions are less strict, allowing employees some personal use of the device (e.g. download certain apps or receive personal text messages).Although such a smartphone is personally enabled, the device and information on the device belongs to the organization. Employees should be informed about organizational restrictions and have appropriate expectations of software and device configurations that affect functionality and privacy. BYOD devices are the typical rank where an employee uses his own smartphone for work. Also, a Choose Your Own Device (CYOD) device is purchased by an employee for personal use. Because in this rank sensitive information may be in the device and the organization has little knowledge about the origin of such a device (e.g. rooted-devices) in order to protect the confidentiality and integrity of organization data and systems as well as the privacy of the device user/owner, IT staff may use a tool such as an EMM to enforce data loss protection by applying restrictions (e.g. disabling the copy/paste feature when in organizations applications).

4. Methodology

In this chapter it will be demonstrated the train of thought that helped create the questionnaire. First we ensure that our work differs from any prior work on the previous chapter. While other works revised in previous sections focus on users awareness and the technology used in order to protect personal and organizational data, this research seeks to produce evidence how close organizations are in the guidelines offered by ENISA and NIST considering the time passed from their publish. Then, after carefully reading both reports from ENISA and NIST questions were elaborated that many times coincided with both guidelines. As mentioned above, each guideline approaches the matter differently. In this study the questions were based upon users' feedback of how they use the smartphone, based on restrictions of their organization (if the smartphone is provided). The survey was distributed through private contacts and various professional networking platforms (e.g. LinkedIn, Research Gate, Reddit). This was deemed necessary in order to ensure that the questionnaire was distributed to a range of countries and not only in the immediate social circle or the research team’s social media accounts. The target audience was defined as any adult person who uses their smartphone for work, thus people over 18 years old. There were no other limitations applied such as age, gender, nationality, years of experience, position seniority or type of work environments as the aim was to capture a varied sample of respondents. Additionally, in the beginning of the questionnaire a disclaimer page was introduced as soon as the participant entered the page, presenting the research and asking their consent. Furthermore, as it is the legal thing to do subjects were offered the option to retrieve their data back in case they do not wish to participate anymore.

The questionnaire is divided in 4 sections:

The 1st section has demographic questions, which are accounted for in 6 questions. These questions include the: age, gender, country of origin, level of education and the industry in which the subject works.

Subsequently the participant is asked (question 6 in section 1) if she/he uses his smartphone for work-related actions. When the user answers (2 answers) these questions, then he/she is referred accordingly to either section 2, which is the Bring Your Own Device section (BYOD), or section 3, which is the organization-issued smartphone.

Sections 2 and 3 consist of 31 smartphone questions each. The questions of these sections are about the use and technical aspects of the subject's smartphones in relation to the guidelines. This includes questions about the type and operating system of the smartphone, authentication and locking mechanisms, accessibility to various resources, services and applications that are used and how used, backup mechanisms, encryption mechanisms, cooperation with the IT department and about the lifecycle of the smartphone (e.g. decommission, remote access).

In the final section we raise some awareness questions regarding the subject's training and familiarity with cybersecurity as both guides support that awareness is the better way to secure the data of every user and organization. The section consists of 3 questions.

Questions were elaborated in a clear and concise way avoiding technical language in order to be understood by everyone, not only from professionals, as the survey is focused on simple users in every organization. When the questions were unavoidably too technical, simple examples were given in order to help the responder understand what is asked. Furthermore, they were created in such a way to address every type of smartphone type. For example, question 16 asks "Do you have access to the organization's resources with your smartphone?" Then an example is provided which in these cases is the servers, something that is the most common resource that an employee needs to have access. The survey went through several drafts and was piloted to ensure the questions were preside, clear and understood from everyone. Some of the questions have optional follow-up questions if the prior question was positively answered, while there was not a requirement to answer in the cases where the prior question received a negative response. Every question with multiple answers has a subheading indicating that more than one answer can be given. Whether it is an open type question the answer is kept short in order to avoid problems with unnecessary given information and try to minimize the number of those questions. The survey answers will be processed with comparative statistical analysis in order to determine the difference between two or more groups employing χ^2 tests (statistical hypothesis test) to explore significant differences between the expected and the observed frequencies, where applicable.

5. Analysis

After a time frame of approximately 8 months we received 232 answers. As mentioned some of the questions are optional, due to being a follow up question. That means that statistics for those questions will not be equal to those of other questions. Those are questions n.16, 25, 32 from the BYOD section and questions n.12, 17, 25, 28 from the Organization-issued section. Additionally, question n1 from General Questions section, question n.9 from the BYOD section and question n.10 from the Organization-issued section are open text, due to the large number of various smartphone models and number of countries.

Lastly, questions n10, 13 from the BYOD section and questions n.12, 13, 15, 23 from the Organization-issued section may provide more statistical information due to the fact that multiple answers can be provided.
We will refer our correspondents as users due to the fact that our survey is on users of various smartphone devices. The charts, made from the answers, will be placed in the order of the questions. First the analysis will begin with the demographic information of the sample, then the analysis will be divided in BYOD section and Organization-issued section with questions corresponding to each targeted group and finally the Awareness questions.

5.1. Demographic Information

Table.1.1

Q1. Country of residence	Sum	Percentage
Responses		
Austria	3	1.29%
Belgium	1	0.43%
Canada	1	0.43%
Cyprus	3	1.29%
Denmark	2	0.86%
England	1	0.43%
Germany	5	2.16%
Greece	153	65.95%
India	1	0.43%
Iraq	2	0.86%
Italy	10	4.31%
Kenya	1	0.43%
Malaysia	2	0.86%
Netherlands	1	0.43%
Nigeria	1	0.43%
Philippines	1	0.43%
Qatar	1	0.43%
Romania	3	1.29%
South Africa	2	0.86%
Spain	1	0.43%
Sri Lanka	2	0.86%
Sweden	1	0.43%
Ukraine	1	0.43%
United Kingdom	16	6.90%
United States	17	7.33%
Grand Total	**232**	**100.00%**

Question 1 is about the country of residence of all our users. The majority of our respondents consist of Greek ethnicity with 153 users (65.95%), followed by United States with 17 users (7.33%), United Kingdom with 16 users (6.9%), Italy with 10 users (4.31%), Germany with 5 users (2.16%), Austria - Cyprus and Romania with 3 persons each (1.29% each), then Iraq - Malaysia - Denmark- Sri Lanka and South Africa with 2 persons (0.86% each) and the rest of the countries in the table with 1 user each (0.43%) for the total of 25 countries and 232 users. The majority of our sample is of Greek residence and the rest 34,05% being users from all over the world.

Question 2 concerning with the age of the users. Results reveal that the majority of the users belong to ages 24-30 a total of 96 users (41,38%), then in the range of 31-40 years old we have 69 user (29,74%), 18-23years old we find 33 user (14,22%) , 41-50 years old are 22 users (9,48%) , 51-60 years old 10 users (4,31%) and last 2 users (0,86%) over 60 years old.

Question 3 focusing on the gender of our sample users. The sample consists of 140 males (60, 34%) 86 females (37,1%),5 people who preferred not to answer (2.16%) and 1 person identified as other(0,43%). Finally, in Question 4 asking the level of education of the sample users. Users' answers results are Bachelor's Degree, 87 users (37.5%), followed by Master's degree, 85 users (36.64%), Doctoral Degree with 30 users (12.93%) and also followed closely by the High School graduates level, 29 users (12.5%). Finally, 1 user replied as an Undergraduate Student that corresponds to the 0.43% of our sample.

Table 1.2

Q2. Age	Sum	Percentage
Responses		
18-23	33	14.22%
24--30	96	41.38%
31-40	69	29.74%
41-50	22	9.48%
51-60	10	4.31%
Over 60	2	0.86%
Q3. Gender	Sum	Percentage
Responses		
Female	86	37.07%
Male	140	60.34%
Other	1	0.43%
Prefer not to say	5	2.16%
Q4. Level of education	Sum	Percentage
Responses		
Bachelor's Degree	87	37.50%
Doctoral Degree	30	12.93%
High School Graduate	29	12.50%
Master's Degree	85	36.64%
Undergraduate student	1	0.43%
Grand Total	**232**	**100.00%**

Table 1.3

Q5. Industry	Sum	Percentage
Responses		
Agriculture, Forestry, Fishing, Mining, Quarrying	1	0.43%
Building and Other Support Services	1	0.43%
Real Estate and Leasing Services	1	0.43%
Culture, Recreation and Entertainment/Media	4	1.72%
Energy/Utilities	4	1.72%
Accommodation/Hospitality and Food/Beverage Services	5	2.16%
Logistics, Maritime and Warehousing	6	2.59%
Manufacturing and Engineering	9	3.88%
Public Administration/Government	9	3.88%
Retail/Trade	9	3.88%
Telecommunications	10	4.31%
Educational Services	16	6.90%
Business, Finance, Legal, Insurance and Consulting Services	25	10.78%
Healthcare and Social Assistance	25	10.78%
Other	36	15.52%
Information Technologies Services	71	30.60%
Grand Total	**232**	**100.00%**

Question 5 is concerning in what industry the corresponded users work. The question is concerned in what industry their organization is and not what is their job position in the organization. The purpose of the question is the need to know whether the organization is focusing on cybersecurity measures for every employee rather specifically due to user's positions in it. For example, an IT department employee may be found in every kind of industry. Additionally it is really important to know which industries are giving importance to cybersecurity, as some of them should be extra vigilant. For example, Healthcare and Social Assistance responses due to the sensitive nature of the data that has been processed. According to the table the highest industries acquired from the responses are the Information Technologies Services with 71 users (30.6%), then the Other category with 36 users (15,52%),Healthcare and Social Assistance and Business, Finance, Legal, Insurance and Consulting Services with 25 users each (10,78% each), Educational Services with 16 users (6,90%), Telecommunications with 10 users (4.31%),Manufacturing and Engineering –Retail /Trade and Public Administration /Government with 9 users each (3.88% people each) ,Logistics, Maritime and Warehousing with 6 users (2.59%), Accommodation/Hospitality and Food/Beverage Services with 5 users (2.16%), Energy /Utilities and Culture , Recreation and Entertainment /Media with 4 users each (1.72% each) and finally Agriculture, Forestry, Fishing, Mining, Quarrying, Building and Other Support Services, Real Estate and Leasing Services with 1 user each (0.43% each).

Question 6 is the last question of the demographic section. The question explores if the users are using their smartphones for business related matters. The question's response leads to the corresponding chapter of the questionnaire with different questions, based on BYOD smartphones or organization-issued smartphones answer.

The majority of the users, 196 users (84,5%) have given the answer that use their own smartphone for their work related matters (BYOD) and the rest 36 users (15,5%) have answered the organization-issued smartphones option. BYOD is the most preferable method showing that is creating a challenge for organizations as many "uncontrolled" smartphones will gain access to their resources.

Table 1.4

Q6. Smartphone Use for work-related actions?	Sum	Percentage
Responses		
No, I use a company Provided smartphone	36	15.52%
Yes	196	84.48%
Grand Total	**232**	**100.00%**

5.2. Smartphone Questions

5.2.1. BYOD section

Question 1 of the section is asking the job position. According to ENISA's guideline the users should be divided into 3 usage scenarios. That is consumers, employees and high officials. The search focuses on scenario 2 and 3 while scenario 1 is out of scope for this survey. Regarding the position ENISA sets a likelihood, an impact and a risk for each categorization of its attacks and how to address them.
NIST is not concerned with the job position.

Table 2.1

Q1. Job Position	Sum	Percentage
Responses		
Employee	170	86.7%
High Official	26	13.3%
Grand Total	**196**	**100.00%**

The results show that from the BYOD sample the 26 users (13,3%) are categorized as High officials and the rest 170 users (78,7%) as employees. The sample shows that most organizations may address the attacks with lower risk as most of the staff is employees.

Question 2 and 3 observes the choice of users made as to what model and operating system they choose for their smartphones. ENISA's guidelines support that by having a diversity in OS and models helps organizations in case of being targeted by a form of malware as different software and hardware exist the cost of creating a malware is lowered. NIST guideline is similar to ENISA's, as NIST supports that with a larger variety of smartphones the chance of creating damage to an organization lowers as it is more difficult to find the corresponding vulnerabilities in each firmware or hardware. NISTs mitigations propose OS & Application Isolation, users should adopt fast any software updates and installation of Mobile Threat Defense for handling updates and incidents.

The most observed operating systems are the iOS users 59 smartphones (30,10%) and the 134 Android users (68,37%), while 2 users (1,02%) use Windows phones and 1 user (05,1%) Linux-based operating system. Organizations should focus on the top 2 operating systems in order to patch the firmware regularly and advise their users to do so, considering it is up to the users. Proper designed policies may help raise users acknowledge the need to update frequently in order to secure their smartphones.

Table 2.2

Q2. Smartphone Operating System (OS)	Sum	Percentage
Responses		
Android	134	68.37%
iOS	59	30.10%
Linux	1	0.51%
Windows	2	1.02%
Grand Total	**196**	**100.00%**

The top brand chosen from the sample users, is the Apple iPhone with a count of 59 smartphones (30,09% of total smartphones) and 19 different models. Followed next by Xiaomi, with 47 smartphone devices (23,97% of total smartphones) with 23 different models.

Table 2.3

Q3. Apple	Sum	Percentage
Responses		
iPhone 11	10	5.10%
iPhone 11 Pro	2	1.02%
iPhone 11 Pro Max	3	1.53%
iPhone 12	2	1.02%
iPhone 12 Mini	1	0.51%
iPhone 12 Pro	1	0.51%
iPhone 12 Pro Max	2	1.02%
iPhone 4S	1	0.51%
iPhone 6S	2	1.02%
iPhone 7	5	2.55%
iPhone 7 Plus	3	1.53%
iPhone 8	7	3.57%
iPhone 8 Plus	2	1.02%
iPhone SE	3	1.53%
iPhone X	4	2.04%
iPhone X Plus	1	0.51%
iPhone XR	6	3.06%
iPhone XS	3	1.53%
iPhone XS Max	1	0.51%
Grand Total	**59**	**30.09%**

Table 2.4

Q3. Xiaomi	Sum	Percentage
Responses		
Xiaomi Mi 10	1	0.51%
Xiaomi Mi 11	6	3.06%
Xiaomi Mi 8	1	0.51%
Xiaomi Mi 9	1	0.51%
Xiaomi Mi 9 Lite	1	0.51%
Xiaomi Mi 9T	2	1.02%
Xiaomi Mi A3	1	0.51%
Xiaomi Pocophone F1	6	3.06%
Xiaomi Pocophone x3	1	0.51%
Xiaomi Redmi 10	1	0.51%
Xiaomi Redmi 7	2	1.02%
Xiaomi Redmi 9	1	0.51%
Xiaomi Redmi A7	1	0.51%
Xiaomi Redmi Note 10	1	0.51%
Xiaomi Redmi Note 10 Lite	1	0.51%
Xiaomi Redmi Note 10+ 5g	1	0.51%
Xiaomi Redmi Note 4X	1	0.51%
Xiaomi Redmi Note 7	5	2.55%
Xiaomi Redmi Note 7 Pro	1	0.51%
Xiaomi Redmi Note 8	3	1.53%
Xiaomi Redmi Note 8 Pro	4	2.04%
Xiaomi Redmi Note 9	2	1.02%
Xiaomi Redmi Note 9 Pro	3	1.53%
Grand Total	**47**	**23.97%**

Third brand option is Samsung with 43 (21,93% of total smartphones) smartphones and 24 different models and fourth option is Huawei with 22 smartphones (11,22% of total smartphones) and 14 different models.

Table 2.5

Q3. Samsung	Sum	Percentage
Responses		
Samsung Galaxy A20	1	0.51%
Samsung Galaxy A21s	1	0.51%
Samsung Galaxy A51	9	4.59%
Samsung Galaxy A6+	1	0.51%
Samsung Galaxy A7	1	0.51%
Samsung Galaxy A70	2	1.02%
Samsung Galaxy A71	3	1.53%
Samsung Galaxy A8	1	0.51%
Samsung Galaxy A9	1	0.51%
Samsung Galaxy J1	1	0.51%
Samsung Galaxy J5	1	0.51%
Samsung Galaxy Note 10	1	0.51%
Samsung Galaxy Note 8	2	1.02%
Samsung Galaxy Note 9	1	0.51%
Samsung Galaxy S10	2	1.02%
Samsung Galaxy S10+	3	1.53%
Samsung Galaxy S20	1	0.51%
Samsung Galaxy S20 Ultra	1	0.51%
Samsung Galaxy S20+	2	1.02%
Samsung Galaxy S21	2	1.02%
Samsung Galaxy S21 Ultra	1	0.51%
Samsung Galaxy S8	2	1.02%
Samsung Galaxy S8+	2	1.02%
Samsung Galaxy S9	1	0.51%
Grand Total	**43**	**21.93%**

Table 2.6

Q3. Huawei	Sum	Percentage
Responses		
Huawei Mate 10 Lite	2	1.02%
Huawei Mate 20 Pro	1	0.51%
Huawei Nova 5t	1	0.51%
Huawei P Smart	2	1.02%
Huawei P10 Lite	1	0.51%
Huawei P20	1	0.51%
Huawei P20 Lite	2	1.02%
Huawei P20 Pro	1	0.51%
Huawei P30 Lite	1	0.51%
Huawei P30 Pro	2	1.02%
Huawei P40	2	1.02%
Huawei P50	4	2.04%
Huawei Y5	1	0.51%
Huawei Y7 Pro	1	0.51%
Grand Total	**22**	**11.22%**

Table 2.7

Q3. Rest of Smartphones	Sum	Percentage
Responses		
Asus Zenfone 5	1	0.51%
Google Pixel 3a	2	1.02%
Google Pixel 4a	1	0.51%
Honor 9	2	1.02%
HTC Desire 20 Pro	1	0.51%
Lenovo K6	1	0.51%
LG G7	1	0.51%
LG V	1	0.51%
LTE 4G android	1	0.51%
Meizu Pro 6 Plus	1	0.51%
Motorola G5	1	0.51%
Motorola Moto E5	1	0.51%
Motorola One	1	0.51%
Nokia 4.2	1	0.51%
Nokia XR20	1	0.51%
One Plus 5T	1	0.51%
One Plus 6	1	0.51%
One Plus 6T	2	1.02%
One Plus 8	1	0.51%
Realme 6	1	0.51%
Realme 7 Pro	1	0.51%
Sony Xperia XA	1	0.51%
Grand Total	**25**	**12.75%**

Finally, the remaining of the sample smartphone options are 25 (12,75% of total smartphones) smartphones with 13 different brands and 22 different models. Among the brands found are LG, Nokia and Lenovo and some new brands like OnePlus and RealMe, all raising concerts for rising cyberattacks in their threat intelligence reports.Due to personal preferences, the observation of a wide variety of models is considered natural. Organizations should be prepared, considering that BYOD is encouraged for daily work related matters, while there is a variety of different models, the choice of top brands is limited to 4 options. Thus in case of an exploit in an operating system or a specific brand (for example iPhone) will affect a big percentage of those smartphones devices.

Question 4 is exploring users' choice of authentication methods. Authentication is one of the most important measures for any smartphone as it acts as a gateway between a user and the smartphone's content. Thus an attacker may be prevented from accessing any data (personal and organization) given any situation (e.g. loss, unattended device etc.). Depending on the situation, BYOD or organization-issued, is up to the user in or the organization to enable the desired method. ENISA scope is not about the authentication weakness, as it is covered in another guide and considered as basic necessity. The guide's concerns are about authentications needed to address the risk of device theft or loss. Additionally the guide regards access control to be high in risk and urges users and IT officers to take necessary precautions, limited by what is offered off-the-shelf by smartphone vendors and developers. Finally ENISA urges to configuring smartphones to require an authentication method before any new applications are installed, otherwise the risk of physically installing malware, spyware or social engineering attacks. NIST acknowledges that smartphones offer many options for authentication and proposes the use of biometric authentication as a combination with or in substitution of passwords or PINs due to the fact that biometric tokens are not stored in smartphones and help mitigate attacks. EMM technology can support basic operations such as requiring

a proper authenticator to unlock the device. This includes basic parameters for password strength and a limit on the number of retries permitted without negative consequences (e.g., locking out the account). Finally the guide marks that user awareness is important because smartphone security is important for organization's data. Users should properly manage authentication credentials, else endanger their personal and organizations information. Education is essential for enabling users to do their part securing their smartphones and organizations should contribute to it.

The question offers multiple choices. The choices were between Password-based, Pattern Lock, PIN Number, Fingerprint Scanner, Facial Recognition/Iris Scanning/Intelligent Scan, Smart Lock – Other Security Measures where the example of Smart Watch was given and a free text answer.

Table 2.8

Q4. Authentication Methods	Sum	Percentage
Responses		
Password-based	73	18.86%
Pattern Lock	48	12.40%
PIN Number	87	22.48%
Fingerprint Scanner	119	30.75%
Facial Recognition/Iris Scanning/Intelligent Scan	49	12.66%
Smart Lock – Other Security Measures (example: Smart Watch)	9	2.33%
None	2	0.52%
Grand Total	**387**	**100.00%**

Table 2.9

Single Authentication	Count	Percentage
Responses		
None	2	1.02%
PIN Number	15	7.65%
Pattern Lock	11	5.61%
Password-based	5	2.55%
Fingerprint Scanner	26	13.27%
Total	**59**	**30.10%**

The sum count of each choice singly is 387 counts for 196 users. The most preferred authentication method is fingerprint scanner (119 users - 30.75%) followed by the PIN number (87 users - 22.48%) and Password-based (73 users - 18,86%) choice. Although many users of the sample prefer a biometric option (token based authentication without local keys) the next options, based on legacy authentication, combined a bigger percentage. Finally 2 users (0,52%) responded that use no authentication, a response mostly negative as the smartphone exposure can initiate every kind of attack.

Furthermore, a questioning fact is that many users choose a single authentication instead of multiple ways. The percentage of those are 59 counts out of 196 different counts summing to 30,10% of our sample. The rest 69,90% consists of multiple authentication ways. In case an attacker wants to access the smartphone it gives the advantage of multiple tries instead of forcefully prompting another way to authenticate, preferable token based.

Question 5 is a follow-up to the previous question and asks if the users use two-factor authentication with their smartphone. A given example like PIN and Biometrics is offered. Two-factor authentication is important as is proven that single-factor is insecure (e.g. dictionary attacks, brute-force attacks, etc.) and offers a second layer of security usually relied in something that you own (e.g. password, SMS) and

something that you are (e.g. biometrics). ENISA states that smartphones are a great tool for online authentication and provide mechanisms like the SIM (SMS and as a card read) and online applications (e.g. Google Authenticator) to do so. Additionally for high employees, two-factor addressing the risk of device theft or loss as a mitigation towards the user-to-device authentication. NIST supports configuring multi-factor authentication policies that may be pre-required from the user to authenticate before accessing for example the organization's resources. Further, policies for system administrators should be created to enforce on the smartphones in order to protect against attackers gaining unauthorized access to enterprise resources with higher privileges.

The results show that 118 users (60,20%) use two-factor while 78 users (39,80%) responded that do not. A few of our example two-factor ways were text message, Google authenticator and Microsoft Authenticator. Although the results are overall positive the percentage of users without two-fact is still high. NIST's EMM may help to enforce policies but user education may help raise awareness to apply better security layers.

Table 2.10

Q5. Two-factor Authentication	Sum	Percentage
Responses		
No	78	39.80%
Yes	118	60.20%
Grand Total	**196**	**100.00%**

Question 6 addresses the time of auto-locking. Auto-lock time in smartphones is considered to be essential as unattended smartphones could fall into unauthorized access. Auto-lock protects and reduces this risk as the time is shortened. ENISA considers auto locking in the scenario where the smartphone is lost or stolen and supports that with auto-lock the content is secured. ENISA enforces the opinion that all smartphones should automatically lock and high official's smartphones should also be enforced with policy. NIST also supports that the smartphone devices should be auto-locked and proposes to be done through the use of EMM technology, enforcing policies and user education.

Table 2.11

Q6. Smartphone's Auto-Lock Time	Sum	Percentage
Responses		
0 - 1 min	108	55.10%
1 - 2 min	33	16.84%
15 + min	3	1.53%
3 - 5 min	20	10.20%
5 - 10 min	3	1.53%
Never	8	4.08%
Not sure	21	10.71%
Grand Total	**196**	**100.00%**

Observing the results the most users have their smartphones locks in "0 - 1 min" (108 users of 55,10%), then 33 users responded "1 - 2 min" (16.84%), 20 users responded "3 - 5 min" (10.20%) and 3 users responded with "5 - 10 min" and "15+ min" (1.53% each). Peculiar, 21 users (10.71%) responded that were not sure what their smartphones auto lock time is. The assumption is that those smartphones may not lock or not know how much time remains unattended making them vulnerable to attacks. Finally 8 users (4,08%) replied "never".

The time responses are positive as more than 80% percent of our sample smartphones are locked in the timeframe of 5 minutes. For the percentage of uncertain users and negative responses, organizations should educate the users in order to protect the content of their smartphones.

Question 7 concerns with what technical features the users disremember to turn off when leaving the work and home network. Options were given between "GPS", "Wi-Fi", "Bluetooth" and that "no feature was left turned on" offering both single and multiple answers. Features were selected considering the risk that those features may pose if an adversary targets them. Scenarios like Wi-Fi connecting to Rogue access points, tracking geological connections from GPS signals and Bluetooth tampered communications are posing a high risk to organizations and can be exploited for threats. ENISA concerns that technologies like Wi-Fi and Bluetooth can be used to intercept and tamper the network communications of the smartphone with the organization (MitM). Additionally concerns that various applications are exposing location data, for example in messages or uploaded photo metadata GPS, often used in social networks. NIST also refers to communications including wireless systems such as Bluetooth and Wi-Fi networks that have no control over the security of the external communications networks. Concerns of eavesdropping and man-in-the-middle (MitM) attacks that can intercept and modify communications. Sometimes Bluetooth often transmits notifications and health information from wearable devices and are susceptible to attacks. Furthermore, NIST concerns about privacy violation from user location tracking. Location services are commonly used by applications such as social media, navigation and weather apps and organization's security. An adversary can pinpoint where the user is located and correlate information from the user's other activities and raise the risk of privacy violation. EMM technology offers support to misconfigured smartphones and turns off features depending on the EMM's capabilities.

Table 2.12

Q7. Enabled Features leaving Home/Work Networks	Sum	Percentage
Responses		
Bluetooth	6	3.06%
GPS	15	7.65%
GPS, Bluetooth	3	1.53%
GPS, Wi-Fi	19	9.69%
GPS, Wi-Fi, Bluetooth	47	23.98%
No Feature	42	21.43%
Wi-Fi	43	21.94%
Wi-Fi, Bluetooth	21	10.71%
Grand Total	**196**	**100.00%**

Table 2.13

Left Turned-On Features	Count	Percentage
Responses		
GPS	84	28.87%
Wi-Fi	130	44.67%
Bluetooth	77	26.46%
Grand Total	**291**	**100.00%**

Observing the responses, the highest combination is 47 users (23,98%) who leave enabled all the features open. On the other hand the users that do not leave anything turned-on is 42 users (21,43%). The count percentage of combinations left turned-on is high, raising the risks that the guides highlight. Furthermore the risk is raised even more as we observe that there are multiple combinations of features turned-on in contrast to a single feature. Finally the most counted left turned on feature users responded is the Wi-Fi

with almost 45% percent count next to GPS with almost 29% percent count and finally Bluetooth with 26,46% percent count.

Question 8 is asking if the users use tethering, also known as roaming/mobile data for their work issues. According to ENISA's guidelines, smartphones consume much of the signal network and create congestion exceeding data capacity creating a low chance of unavailability suggesting that smartphones smartphone should switch between idle and active mode. Additionally ENISA believes that smartphones can be used as tools, due to the multiple interfaces (like roaming data and cellular) to perform DDoS attacks. NIST notes that if an organization permits tethering, it should ensure the network connections involving tethering are strongly protected (e.g., communications encryption). Otherwise it is concerned that cellular traffic can be monitored (MitM attack) due to the fact that various types of traffic are transmitted. NIST proposes the use of VPNs to mitigate this. Also organizations should have policies regarding the use of tethering.

Observing the sample the 128 users (59.26%) are using tethering and 68 users (31.48%) are not. As over the half percentage of organizations employees are using tethering enforces the guideline's concerns. Organizations should implement mitigation as the number of tethering usage will keep increasing.

Table 2.14

Q8. Use of Tethering	Sum	Percentage
Responses		
No	68	34.69%
Yes	128	65.31%
Grand Total	**196**	**100.00%**

Question 9 is asking users if they use sensitive applications with their smartphones. Sensitive applications are considered those that require an extra layer of protection since from their nature process sensitive data and the risk of losing or manipulating those data is harmful. An example is given to the users and that is the electronic wallets. ENISA considers that those applications make the smartphone an interesting choice as a target for spyware through various channels. Additionally the smartphone becomes a target from a financial malware in order either to hijack communications with a financial vendor or impersonating a legitimate application. NIST supports that smartphones that use this kind of applications should have better hardware processing in order to use better security mechanisms such as faster encryption, secure data processing and usage of trust execution environments. Furthermore, NIST raises a concern with the BYOD and sensitive organization applications as a user's smartphone may be infected and the user is not aware of or a leakage from a non-trusted application installed by the user. It suggests the use of EMM in order for restrictions to be applied (for example disabling copy paste).

Table 2.15

Q9. Use of Sensitive Applications	Sum	Percentage
Responses		
No	57	29.08%
Yes	139	70.92%
Grand Total	**196**	**100.00%**

From our sample 139 users (64.35%) use sensitive applications and the rest 57 users (26.39%) do not. As it seems a large number of users are using sensitive applications either personal or organization related. Organizations may need to implement policies or inspect the BYOD in order to protect the sensitive data or the privacy of the users.

Question 10 is following-up the previous question asking if these applications are locked with a separately method than these of unlocking their smartphone. The question aims to understand if the user takes an extra layer of protection to applications he considers sensitive as according to ENISA the impact of a breach in such an application is high and the measures must be chosen carefully. NIST on the other hand does not address the subject directly but rather concerns the fact that improper methods like weak passwords or insecure lock screen may provide sensitive information to unauthorized users.

From the 139 users that responded positively to Question 15 collected that 100 of them (71.94%) use extra authentication for their sensitive applications when the rest (39 with 28.06%) do not. The results are rather hopeful as we see that many users, considering the fact that they own the device, value sensitive applications and enforce, as guides propose, their security.

Table 2.16

Q10. Separate Lock Authentication	Sum	Percentage
Responses		
No	39	28.06%
Yes	100	71.94%
Grand Total	**139**	**100.00%**

Question 11 asks if the user inspects the permissions that an application needs from another application, giving the example of Contacts. Many applications require or give permission to many third party applications in order to function properly or give some flexibility.
ENISA's concern is that some applications may pose as spyware in order to retrieve sensitive information. Also supports that even if there is a legitimate need for an app to send data over various channels, the permission model of smartphones is not always granular enough to protect users against abuse. ENISA advice to download applications only from trusted sites and monitor the smartphone's resources for NIST once again addresses the problem from the use of MAM (Mobile Application Management) ,through EMM technology, by giving an organization application catalog with a mobile device vendor's catalog (e.g., Apple Store, Google Play) to allow mobile users to easily install an application. MAM may also be able to restrict app functionalities without affecting the entire device, an approach that is preferred by BYOD users.

Table 2.17

Q11. Inspecting Permissions for Third-Applications	Sum	Percentage
Responses		
No	38	19.39%
Yes	158	80.61%
Grand Total	**196**	**100.00%**

From the results, we observed that 158 users (80,61%) do inspect the permissions an application needs from another application while the rest 38 users (19,39%) do not. The results are very positive as most of our sample has grown a general awareness of inspecting what their applications need.

Question 12 is a follow-up question to question 17, asking if the users inspect what kind of permissions an application needs in order to operate. The concerns of both guidelines, regarding sensitive information loss and untrusted applications, are identical to those of question 17.

The results show that 170 users (86,73%) responded positively to the question and 26 (13,27%) negatively. Once again the results are positive towards the users' awareness of the matter and more users are inspecting what application permissions need than inspecting the permissions an application needs from another application.

Table 2.18

Q12. Inspecting Permissions for Applications	Sum	Percentage
Responses		
No	26	13.27%
Yes	170	86.73%
Grand Total	**196**	**100.00%**

Question 13 asking if users have access to the classified/sensitive information with their smartphones. The question is considering what access a user has with their BYOD device to an organization's sensitive data. The problem is that not only the user has their own sensitive information and data but also interact with organizations sensitive information (e.g. corporate email). The risk of losing such data is very high. ENISA's consideration is that this category of data is creating a very high risk if the device is lost or even if an unwanted application leaks them. ENISA proposes that proper protective methods should be implemented, such as authentication mechanisms, encryption of data, auto-lock time, and the choice should be cautious and proper because as for example a legacy phone can be easily decrypted.
NIST's consideration is similar to ENISA, considering better hardware and storage for better encryptions, applications making security decisions (e.g., granting access to a privileged API to the right parties), trusted execution environments and security chips (e.g. Secure Element).

Table 2.19

Q13. Classified/Sensitive Work Data Access	Sum	Percentage
Responses		
No	108	55.10%
Yes	88	44.90%
Grand Total	**196**	**100.00%**

Results show that 108(55.1%) users have access to sensitive information opposed to 88 users (44.9%) that do not. Half of the organizations are trusting users to have access to their information with their BYOD, thus organizations should encourage users to use extra authentication methods or even supervise the use of such data.

Question 14 is inspecting the existence of extra security applications in the user's smartphone. Examples of such security include end to end confidentiality (e.g. VPN technologies) and antivirus-antimalware applications. An example of each application was given in the question. Such features can be a tool in order to prevent many common attacks like infections or man in the middle attacks. ENISAS's addresses the matter that the aforementioned applications are recommended as a measure concerning the risks of network spoofing and surveillance attacks. More specifically all employees are recommended to have them installed and more strongly recommended to the higher officials. NIST believes that VPN applications are a way to enhance organizational security and proper selection of VPN algorithms should be done. Interesting fact is that NIST is addressing the matter of antivirus and instead results that malware should be identified and handled by EMM technologies.

The results are that 86 users (43,88%) use additional applications to 110 users (56,12%) that do not. The results indicate that more than half of the organizations are prompted to have a security breach in their data as more than half of the sample responded negatively. That means that data are insecure either in places such as public Wi-Fi due to the lack of end to end Connectivity, or leak in the form of a virus-malware.

Table 2.20

Q14. Additional Security Applications	Sum	Percentage
Responses		
No	110	56.12%
Yes	86	43.88%
Grand Total	**196**	**100.00%**

Question 15 refers to the elevated administration privileges a user has in their own smartphone unlocked either through jail-breaking (iOS devices) or rooting (Android devices). In both cases the user has the highest privileges in the smartphone freeing the user from the limitations of the designed operating systems. In addition to the yes no answer due to the technical nature of the question a not sure option is given as not many users are familiar with the concept of elevated administrative privileges or not aware of the status of their smartphone. Rooting may escalate to a point where unwanted software can operate with malicious intents towards the organization. Furthermore many applications will not operate if the system is rooted. ENISA addresses the matter from the distribution channel side. According to the guide a privileged device can gain access and install applications not from the traditional channels (e.g. Play-Stores) giving an adversary the ability to infect a smartphone. Instead ENISA suggests the use of controlled software distribution where applications can be reviewed and tested in order of security aspects and removed from those channels. NIST believes that jail-break and rooted devices should be automatically assumed as untrustworthy and high risk devices as those smartphones may gain access to sensitive data, especially BYOD devices as organizations are unaware of their security status, and must be inspected from the organization before accessing any data. Additionally, EMM should limit or prevent access to organization services.

Table 2.21

Q15. Unlocked Administration Privileges	Sum	Percentage
Responses		
No	127	64.80%
Not sure	51	26.02%
Yes	18	9.18%
Grand Total	**196**	**100.00%**

The observed results are 127 users (64.8%) have no elevated privileges while 51 users (26.02%) are not sure if their smartphones have elevated privileges and 18 users (9.18%) have access to those privileges. Our statistics match ENISA's statistics (10% of iPhone users unlock their device to allow installation of software from other sources) supporting the guide's thesis. Furthermore, a larger percentage of our users responded negatively, a positive result as these smartphones are not infected by PUA. Last, the 25% of users responded not sure, unaware with the concept or the status of their smartphone, thus inspections from the organization should be made before accessing any data.

Question 16 addresses the organization's capability to implement the policies to each user's smartphone when their devices are needed to connect to the organization's network. Policies are an important aspect representing a working set of rules that permits or restricts the users depending on their design. As the question can become hard to comprehend (users in a non IT related field) is kept simple without any technical aspects as many of the users may not be aware of what those policies restrict or allow thus a simple policy awareness question is asked (the option not sure is also implied).
ENISA insists that security policies must be set from each organization's IT officer. Policy should be implemented in order to restrict or customize the functionality of the smartphones. Furthermore, should prevent policy breaches by technical means (default configurations, security Software, and mobile device management software). NIST, very similar to ENISA, believes that general policies should be implemented. NIST once again supports EMM technology that should be implemented, for monitoring, detection and reporting when policy violations occur and automatically take actions, by System administrators.

Results show that 43 users (21,94%) responded "Yes", 87 users(44,39%) responded "No" and the rest of the 66 users (33,67%) "Not Sure". The results are mostly negative as nearly 78% of the sample have responded either negatively or doubted. That may translate that many organizations leave the smartphones unattended without creating a general guideline for the corporate usage of resources or organizations have created the policies but do not inspect the users implementing them thus they are unaware of those policies. Overall many organizations may not consider them as important as implementing security policies for computer devices as smartphones.

Table 2.22

Q16. Smartphone Installed Security Policies	Sum	Percentage
Responses		
No	87	44.39%
Not sure	66	33.67%
Yes	43	21.94%
Grand Total	**196**	**100.00%**

Question 17 is asking the users if their smartphone device has ever been inspected from their organization's IT department. The results are important as being in the category of BYOD, is unknown to what content any user's smartphone may exist (e.g. PUA). ENISA instructions do not hold a concern of inspecting the smartphone but rather ensuring that each organization's policies are followed, different for each classification (employees and high officials). NIST's concern is that with BYOD smartphones the proper configurations, set by policies, are not implemented in contrast to organization-issued smartphones which are preconfigured. It supports that the organizations should request the smartphone owner to bring their device into the organization to be properly configured before any organization access. Additionally, those smartphones should become part of Mobile Threat Defense (MTD) system, if implemented in an organization. The role of such a system is to inspect and continuously monitoring the smartphone's various functions and files for any vulnerabilities, misconfigurations, malwares and network-based patterns.

Table 2.23

Q17. IT Smartphone Inspection	Sum	Percentage
Responses		
No	174	88.78%
Yes	22	11.22%
Grand Total	**196**	**100.00%**

From the 196 users the 174 responded negatively (88,78%) opposed to the 22 (11,22%) that responded positively. The difference is very significant, giving us the assumption that almost 90% of the organizations in our sample are not aware of what their employees' smartphone configurations are or what kind of devices are allowed in their organization network.

At this point, an interesting statistic is that the percentage of answering positively in inspecting smartphones is close to the positive answer in implementation in organizations policies, giving the assumption that the same organizations care if their policies are implemented and inspecting if they have been followed.

Question 18 asks how often the users back-up their smartphones. Back-ups are crucial to be repeated often as any smartphone is susceptible to various hazards and dangers, physical and technical. In this case this process is up to users' awareness and judgment to perform them regularly as the user's smartphones (BYOD) are not checked, prior to the previous two questions. ENISA believes that every employee should make frequent backups, even in an automatic procedure and high officials should avoid sensitive data and backup non sensitive ones. Additionally it mentions that smartphones are very convenient with backups as they have new ways and recovery functions (e.g. remote commands) to address the risk of data availability addressing either the risk of failure, loss or theft. NIST on the other hand, raises questions about the smartphone's location of backup as back-up locations may be infected transmitting malwares. Also encryption storage keys must be encrypted and the organization should address the existence and location of them.

Table 2.24

Q18. Smartphone Backup	Sum	Percentage
Responses		
Once every 3 Months	3	1.53%
Never	49	25.00%
Once a Day	22	11.22%
Once a Month	31	15.82%
Once a Week	16	8.16%
Once a Year	3	1.53%
Once every 6 Months	2	1.02%
Once or Twice a Year	3	1.53%
Real Time	5	2.55%
When I switch to Another Device	1	0.51%
When Prompted by my Device	61	31.12%
Total	**196**	**100.00%**

The most answered option by 61 users is “When prompted by my device” (31,12%). The second most answered is 49 users (25%) that responded with “Never”. 31 user (15,82%) responded “Once a month”,22 users (11,22%) responded “Once a day” 16 users (8,16%) responded” Once a week”, 5 users (2.55%) responded “Real Time”, then “Once Every 3 months”, “Once a Year“ and “Once or twice a year ” of 3 users each (1,53%) , 2 users (1,02%) responded “Once every 6 months“ and finally 1 user (0,51%) responded “When I switch to another device”. Our sample has a variety of answers. That is due to the fact that the BYOD section implies that it is up to any user to choose the frequency of those backups. The negative answers stand out as the 55% responded negatively or

"when prompted by my device" which means that is up to the OS making the assumption that this is either neglected by the user or not frequent prompts by the device. Also interesting was the user who answered "when I switch to another device" as it shows that sometimes backup may be considered a way of transferring data and not as a problem of availability. Over 55% of the sample organizations may be susceptible to data loss from smartphone unavailability. The positive responses are the 36% who answered either "once a day", "once a week" or "once a month".
Finally the best practice is the answer of "Real Time" where 5 users have their smartphone's data synchronized in a storage unit making it impossible to lose data. The rest of the 9% of our sample are creating a big risk for the organizations as the risk of the loss is increased due to the big gap of time between backups. The risk can be decreased by implementing backup procedures in the policies and regularly checked from various means (e.g. IT Department inspections).

Question 19 is a follow-up to the previous question. The question asks if a user reported positively in the previous question if this back-up is performed on a cloud service. Cloud services are important for back-ups as those services ensure that the data are always available and accessible everywhere with proper authentication methods and proper security measures. The scope of this question does not include if the service is in house or leased. ENISA acknowledges the benefits of cloud services and supports them as long as any organization accepts the risks of the security measures that are implemented by the provider of such services. Additionally the use of cloud services are the best tools for ENISA's recommendation of almost automatic back-ups and high officers with the "no local data storage" policy. NIST also acknowledges those services and as the previous question is concerned again with the location of the data as with cloud services the locations are more and even in another device. Also warns the organizations about the risks and whether to accept them or not.

Table 2.25

Q19. Cloud Based Backup	Sum	Percentage
Responses		
No	40	27.21%
Not sure	10	6.80%
Yes	97	65.99%
Total	**147**	**100.00%**

The 97 users (66%) reported that they use such a cloud service in contrast to 40 users (27,2%) that responded that they do not. Finally 10 users (6,8%) that are not sure where their data are stored and if those services are being implemented. The results show that approximately 66% of our sample data are safe in a cloud service and their and organizations data may not be lost in case of a smartphone malfunction or general loss. As always there is always the risk mentioned by the guidelines that organizations must consider.

Question 20 is about the application's sources a user selects. The question is examining if the user prefers to install applications from other sources rather than the official distributing channels as the App-Store. Applications outside those channels may be considered untrustworthy as the proper channels check the legitimacy of those applications. ENISA holds that organizations should use the proper stores for applications as it believes that those distribution channels offer better control over applications security by carefully examining submitted applications for security flaws and removing any insecure application found. On the other hand ENISA trusts that organizations should acknowledge that there is always the risk of an adversary placing a fake application in those stores and pass undetected. As a risk minimizing solution

proposes that spyware software should be installed in the smartphones. NIST differentiate from ENISA's thought, especially for BYOD. For start , as mentioned in a previous chapter all new devices must be considered untrusted, as there is no knowledge of what third-party applications are installed. Additionally, the term Shadow IT is quoted from NIST. The term translates to applications and actions that users do when they are not permitted, under the awareness of organization. As a solution NIST results in MDM technologies where the existence of any application installed is informed and policies can be applied to every EMM profile. Furthermore the technology provides lists of applications allowed (whitelists) and restricts those that are unwanted (blacklist) and if needed limits access to the official stores. Digital certificates are to be applied through EMM profile policies, used for authenticating applications and making decisions about applications by showing warnings to users. Finally, Application Vetting technologies are encouraged in order to carefully examine any application.

The sample shows that 154 users (78.57%) responded negatively opposed to 37 users (18,88%) that answered positively. The 5 remaining users (2,55%) of the sample responded "Not Sure". The overall results are very positive as it shows that most users do not trust third-party channels to install applications.

Table 2.26

Q20. Other Application Sources	Sum	Percentage
Responses		
No	154	78.57%
Not sure	5	2.55%
Yes	37	18.88%
Grand Total	**196**	**100.00%**

Question 21 is exploring the automatic update of smartphones. The user is asked if updates the installed applications or OS of his smartphone automatically. Updating applications is considered important as outdated versions are vulnerable to exploits or lacking security measures. The same is implied for the OS as patches and updates also help fix bugs and errors. ENISA supports that idea as updates often help as patching helps against malware installation. Additionally in order for a patch to be placed to the proper channel, vetting is in order. Finally ENISA concerns about the time and the delay created in order for smartphones to update regarding the variety of OS and the complexity each applications possess, as some patches may create problems if not tested beforehand. NIST, as in the previous question, results in management systems. Firstly, MAM uses safeguard mechanisms to update any applications. Additionally, EMMs can notify the user when OS and applications updates are available. If the user neglects any appropriate updates, the administrator can enforce compliance actions. These actions vary to blocking or restricting access to organization information or even complete removal of organization information on the mobile device. If application management is enabled and the smartphone found to be compatible, EMMs can manually update apps and apply them to smartphones.

Table 2.27

Q21. Automatic Updates	Sum	Percentage
Responses		
No	58	29.59%
Not sure	7	3.57%
Yes	131	66.84%
Grand Total	**196**	**100.00%**

The responses show that 131 user's (66,84%) are automatically updating their smartphones, 58 users (29,59%) are not and 7 users (3,57%) are not sure if the updates are automatic. The results are positive as the highest percentage of our sample users are found to update their smartphones automatically, thus patching errors and security flaws as soon as possible.

Question 22 asks if the user's smartphone interacts with other devices, giving as an example "Personal Computer". Interactions with other devices may lead to a smartphone infection and also to data sharing without the user's knowledge. Although ENISA does not object to smartphone's interactions directly, the relevancy can be found in that of the applications concerns: "Most applications have privacy settings for controlling how and when location data is transmitted, but many users are unaware (or do not recall) that the data is being transmitted" (ENISA: page17). As an example applications that automatically connect to a personal computer data begin synchronizing (example: iTunes). On the other hand NIST recognizes that smartphones may interact and synchronize with other systems both wirelessly and physically. With these in mind the guide raises the risk of data leaking to undisclosed sources or the smartphone's infection with malwares. Furthermore NIST refers to the shadow IT term to enforce the aforementioned concerns as users in an organization's environment will find ways to overpass policies and restrictions, especially with BYOD environments. The guide trusts EMM technologies to reduce such risks (not a complete solution).

Examining the responses, 146 users (74,49%) responded "Yes" and 50 users (25,51%) responded "No". Answers ought to trouble organizations, raise their awareness and create policies as most of the results of the sample smartphones are interacting with other devices. The risk created is high concerning the aforementioned possibilities.

Table 2.28

Q22. Interaction with other devices	Sum	Percentage
Responses		
No	50	25.51%
Yes	146	74.49%
Grand Total	**196**	**100.00%**

Question 23 explores where the data are saved. The user is asked if the smartphone stores data to removable media, and given the example of the memory cards. Removable media is an option of storing data usually found in older smartphones and a way to expand internal memory. Due to the nature of those media it is easy to lose or get stolen thus raising the risk of data disclosure. ENISA acknowledges those facts and requires that data on the removable media is not sufficiently protected by encryption. Otherwise an attacker can access that data, both personal and organizations. Additionally, regular back-ups should be made in tandem with the smartphone's internal storage. Finally when decommissioning a smartphone any removed media should be wiped as well. NIST also supports that the proper use of removable media is that the stored data are strongly encrypted. Additionally NIST follow-ups with the removable media to be bound to the smartphones so encrypted data only can be decrypted when the removable media is attached to that specific smartphone, thereby mitigating the risk of attacks on the data for example being stolen.

Table 2.29

Q23. Removable Media	Sum	Percentage
Responses		
No	130	66.33%
Not sure	9	4.59%
Yes	57	29.08%
Grand Total	**196**	**100.00%**

Inspecting the responses, we observe 130 negative answers (66,33%), 57 positive answers (29,08%) and 9 uncertain answers (4,59%). The overall users of smartphones with removable media is not high but organizations should ensure that those users are following the proper guidelines, especially regarding their position. Additionally, inspecting users' smartphones can help with the uncertain users in order for the data to be properly secure.

Question 24 is addressing the users' choice of extra encryption for their files. The question is asked in order to identify if users are extra careful with their data and even the extent of their communications as such applications are up to users' judgment to be installed as an extra layer of security.
ENISA encourages the use of third-party encryption applications only with the proper conditions. Those are proper key management, regulatory provisions governing the use of encryption technologies and accepting the risk that most smartphones do not have the same integrity controls as a standard smartcard reader; thus a malicious app could limit the effectiveness of the end-to-end encryption.
NIST believes that EMM technologies (Enterprise mobility management) for encrypting storage should also be implemented in a smartphone, supporting the use of additional applications. Additionally, encouraging the use of data isolation mechanisms for authorized access for data communications and on-device data storage. The drawback is that data may be encrypted with a key that is not managed by the user, developer or organization but from the OS.

Our sample responses are 151 users (77,04%) as "No", 30 users (15,31%) as "Yes" and 15 users (7,65%) "Not sure". Results are rather negative as most of our sample users depend solely on OS authentication mechanisms for the protection of their data and mostly their communications.

Table 2.30

Q24. Extra Encryption	Sum	Percentage
Responses		
No	151	77.04%
Not sure	15	7.65%
Yes	30	15.31%
Grand Total	**196**	**100.00%**

Question 25 is about the smartphone's access to organizations resources. An example of such a resource is a server containing organizations data. Access to those resources should be limited and controlled. That is why those data and systems found in those resources are important for the availability of services in organizations. It is important that proper access should be implemented. ENISA addresses the issue with public key certificates of corporate servers (email, intranet) found pre-installed in smartphones and configure clients to deny other certificates. NIST addresses the issue with EEM technology by enforcing organization security policies on a smartphone and configuring the use of mobile functionality and security capabilities.

Table 2.31

Q25. Access to the Organization's Resources	Sum	Percentage
Responses		
No	141	71.94%
Yes	55	28.06%
Grand Total	**196**	**100.00%**

From the sample is observed that only 55 users (28,06%) have access to their organizations resources, opposed to 141 users (71,94%) that do not. Our results show that organizations may not be ready for smartphones to gain this kind of access as regular network devices (e.g. laptop) do.

Question 26 is a follow up question of question 25, asking if users do have access to resources if the access is limited. Authorization measures should be implemented as important as authentication, for the resources. Ideally, access may be identical to the access a personal computer has, considering the smartphone's

flexibility in working everywhere. ENISA does not address the matter directly and is up to the certificates, aforementioned in the previous question, to also authorize access. NIST's concern is that connecting an improperly configured device to an organization resource (e.g. networked drive) may lead to data exposure. These exposure may be to entities monitoring the network, applications with no rights to do so or those improperly accessing the device directly. Finally, EMM technologies may limit or prevent access to organization services based on the mobile device's OS version (including whether the device has been rooted/jailbroken found in questions before), vendor/brand, model, or mobile device management software client version (if applicable).

From the 55 users that have access to their organization resources, 35 users (63,64%) responded that the access is limited, 13 users (23,64%) responded that the access is unlimited and 7 users (12,73%) are not sure if they are limited or not. The outcome is encouraging as the biggest percentage indicates that organizations do limit their users in order to protect their resources.

Table 2.32

Q26. Limited Resource Access	Sum	Percentage
Responses		
No	13	23.64%
Not sure	7	12.73%
Yes	35	63.64%
Grand Total	**55**	**100.00%**

Question 27 asks if a user loses his smartphone can a remote wipe performed. The cause of loss may include theft. Considering that smartphone flexibility being mobile is easy to be lost or stolen, especially in BYOD where the user's smartphone is part of his daily life. When a user can wipe the data in case of such a scenario, it helps protect data fallen into untrusted hands and gain ground in security where other misconfigured security measures may fail (e.g. 4 pin password). ENISA acknowledges that various smartphones can be wiped remotely and combined with proper backup methods should be used to mitigate the risks associated with theft or loss. In addition, in cases where data crucial data exist, for example a high official's smartphone, in order to prevent an attacker from preventing remote-wipe by blocking network-connectivity, the smartphone may be configured to automatically wipe in case of blocked network connectivity for a given period and unsuccessful authentication tries. NIST believes that administrators should install an EMM agent in users' smartphones (BYOD). Remotely performing wipe methods according to the device needs (data and/or applications). Additionally, EMM can confirm the actions taken responding to the server. Finally NIST urges not to rely completely on remote wiping but rather be a part of a multi-layered approach to protection.

Table 2.33

Q27. Remote Wipe Data	Sum	Percentage
Responses		
No	101	51.53%
Yes	95	48.47%
Grand Total	**196**	**100.00%**

The sample answered are divided as 101 users (51,53%) responded negatively and 95 users (48,47%) responded positively. The results are slightly positive as more than 50% percent care about their data in case of smartphones loss and if organizations enforce it as a policy should raise their awareness.

Question 28 is examining the user actions in case their smartphone is lost, especially if their IT department is informed. With the term loss the scenario of malfunction and steal is included. In case of a smartphone loss where the employee uses the BYOD policy the organization data are at great risk. Thus the IT department should be informed in order to protect the organization's data. Activities such as credential rotation, isolating applications access or moving the data to new resources can be implemented from the proper departments as early as possible. ENISA believes the risk of losing a smartphone is high due to their value and size. The data in risk are both organizational and personal, especially with BYOD policies where the data may be also sensitive. As measures of lowering those risks ENISA proposes the use of better authentication methods, remote wiping the data after proper backup have pre occurred, encryption of data and removable media and minimizing the storage of sensitive data even to the point of no local data storage for proper cases (high officials). NIST's concern is the mobility of the smartphones and even if a prohibition on the device leaves the organization premises the risk of loss is still high, thus compromising the organization. NIST's suggested solution to the problem involves Mobile Threat defense technologies, proper use of Mobile device security policies, remote wiping the smartphone's data and finally proper user education.

The results show a significant difference as 183 users (93,37%) responded that they do not inform the IT department if their smartphone is lost, to 13 users (6,63%) that do. Risk of data loss is high for each organization. The problem may be related to the fact that there is no proper awareness from the users, as a device that is BYOD may not be considered an organization's issue.

Table 2.34

Q28. Smartphone Loss Update	Sum	Percentage
Responses		
No	183	93.37%
Yes	13	6.63%
Grand Total	**196**	**100.00%**

Question 29 is examining if the users' smartphone wipes out any data if the unsuccessful tries pass a certain limit. Mitigations like this help in securing that data could not be obtained by an adversary in case of a smartphone loss or social engineering attempt. ENISA believes that any employee or high official user-to-device authentication is considered weak, an auto-wipe after "x" failed access attempts mechanisms should be done. Frequent backups should be a prerequisite for unwanted data losses. NIST falls to EMM technology where auto-wipe should be performed after a certain x number of incorrect authentication attempts or after a preset time interval without the smartphone checking into the EMM. Unfortunately, this mitigation can be found difficult to implement as in BYOD category the smartphones may not have the pre required agents in order to take actions.

Table 2.35

Q29. Automatic Smartphone Data Wipe	Sum	Percentage
Responses		
No	88	44.90%
Not sure	77	39.29%
Yes	31	15.82%
Grand Total	**196**	**100.00%**

The results are 88 users (44,90%) responded "No", 77 users (29,29%) responded "Not sure" and 31 users (15,82%) responded "Yes". Most of the results have negative feedback as the majority of users do not have auto-wiping data leaving the smartphone prone to attacks especially if the authentication methods are weak (e.g. 4 PIN code).

Most peculiar is that users are not aware whether the smartphone auto-wipes the data with a percentage close to the negative answers as these users own the smartphone and auto-wipe should be considered disabled.

Question 30 is asking if the users wipe the data in their decommissioned smartphones. Most users tend to replace smartphones with new models removing the SIM and any external media while neglecting to wipe the internal storage. The data may contain personal information and to an extent, if the user uses the smartphone to work (BYOD) organization data. In the case the smartphone is sold or found misplaced the data can be accessed without the users or organization knowledge. Such data may be sensitive to the user or the organization. For those reasons decommissioned smartphones should be wiped. ENISA supports that the risk of an attack on a decommissioned smartphone and the likelihood of recovering sensitive data including call history, address book entries, diary, emails, etc. is high. For the aforementioned reason, the likelihood of the term 'smartphone dumpster divers' may occur. ENISA proposes that IT officers should have policy rules on decommissioning where every smartphone should have any internal data thoroughly removed including any removable media. NIST also supports wiping the data according to his guidelines. Additionally, ENISA proposes to follow NIST standards. NIST proposes the use of EMM technologies before retiring the device or reused by another employee.

The sample data shows that 127 users (64,8%) do wipe their old smartphone data and 69 users (25,2%) do not. A rather positive result as most users are aware of their data security and wipe them before decommissioning their smartphone. As a good percentage of users responded negatively, organizations should encourage users to wipe their decommissioned smartphones considering that BYOD control of smartphone contents is up to the user.

Table 2.36

Q30. Wipe Old Smartphone Data	Sum	Percentage
Responses		
No	69	35.20%
Yes	127	64.80%
Grand Total	**196**	**100.00%**

Question 31 asks if the users travel with their smartphones. As mentioned above smartphone size makes it easy in terms of mobility to work everywhere. Thus an employee can travel with that smartphone for any related business actions. Additionally, in the case of BYOD it is natural that the same device being used for work reasons to be used also as an everyday tool for traveling. The risk of loss is increasing significantly. Additionally the risk of compromise is rising as the same smartphone is needed to access the organization network from an unsafe location. ENISA is considering the use of smartphones for these activities as travel assistance and believes that it should be subject to IT (security) policies, set by the employer's IT officer. The policies may concern risks like unintentional disclosure of data, authentications methods etc. NIST confines in EMM technologies for remote management of the smartphone devices. Also NIST is concerned that updating software may be almost infeasible due to continuous traveling and falling behind. Finally, employees may send work-related emails or documents to their personal email accounts to enable better access during travel.

Table 2.37

Q31. Travel with Smartphone	Sum	Percentage
Responses		
No	11	5.61%
Yes	185	94.39%
Grand Total	**196**	**100.00%**

The sample results show that 185 users (94,39%) travel with their smartphone and 11 users (5,51%) do not. Considering the category is BYOD, it is only natural for those users to use it as a travel assistance even for their personal travels. These users should be aware of the risks of traveling with that smartphone as both their personal data and organization's data are in danger. Finally, organizations should encourage users to keep up with policies (e.g. better authentication methods, encrypt data, etc.)

5.2.2. Organization-issued Smartphone section

Question 1 concerns with the job position of the user. Similarly to the BYOD section is focusing on ENISA's scenario 2 and 3 for the risks raised concerning the position of the employee.

From the grand total of 36 answers, 33 users (91, 67%) responded that categorize themselves as employees and 3 users (8,33%) categorized as High officials. The results show that issued smartphones may not be carefully prepared as the not significant percentage of high officials may lower the risks of attacks.

Table 3.1

Q1. Job Position	Sum	Percentage
Responses		
Employee	33	91.67%
High Official	3	8.33%
Grand Total	**36**	**100.00%**

Question 2 asking if the smartphone is used for personal activities. Organization-issued smartphones are usually provided in order to be used solely as a tool for business purposes and not for personal use. Using it as a personal tool may create a risk of smartphone compromise. ENISA supports this idea and believes that smartphone use should be limited or restricted according to the occasion depending on the sensitivity of information and tasks. NIST on the other hand approaches the matter via security and privacy policies with monitoring the smartphones being a key method of the process. Depending on many factors like the organization's missions or the characteristics of the data, monitoring policies from the help of EMM and MAM could help with a possible compromise.

Table 3.2

Q2. Personal Smartphone Usage	Sum	Percentage
Responses		
No	17	47.22%
Yes	15	41.67%
Yes, in a limited way.	4	11.11%
Grand Total	**36**	**100.00%**

Sample responses show that 17 users responded negatively, 15 users responded positively and 4 users responded "Yes, in a limited way" (Personal data are saved separately by Corporate data). The difference in our results show that organizations are showing flexibility in their

issued smartphones as the mission and security needs are different to every one of them.

Question 3 and 4 explore the operating systems and models provided in those users. As in Question 2 and 3 of BYOD section, the concerns and proposals are the same (e.g. diversity in models and OS).
Similar to BYOD answers, the higher preferences in OS are Android with 20 users (55,56%) and iOS (26,11%), with only 1 Blackberry (2,78%), 1 Windows (2,78%) and 1 Satphone (2,78%). The variety in OS is very limited thus raising the risk of targeted attacks.The top brands chosen from the sample users in order are, the Apple iPhone with a count of 14 (38.89% of total smartphones) and 9 different models, followed by Xiaomi with a count of 7 (19.44%) and 5 different models, Samsung with a count of 7 (19.44%) and 6 different models, Huawei with a count of 4 (11.11%) and 4 different models and finally the rest of the smartphone models with 4 different brand, 1 count each (2,78%).

Table 3.3

Q3. Smartphone Operating System (OS)	Sum	Percentage
Responses		
Android	20	55.56%
Blackberry	1	2.78%
iOS	13	36.11%
Satphone	1	2.78%
Windows	1	2.78%
Grand Total	**36**	**100.00%**

Table 3.4

Q4. Model of Provided Smartphone	Sum	Percentage
Responses		
Huawei Mate 10 Lite	1	2.78%
Huawei P Smart	1	2.78%
Huawei P40	1	2.78%
Huawei P50	1	2.78%
Tesco IMO Q4	1	2.78%
iPhone 10	1	2.78%
iPhone 11	1	2.78%
iPhone 12	1	2.78%
iPhone 6	1	2.78%
iPhone 7	4	11.11%
iPhone SE	1	2.78%
iPhone X	2	5.56%
iPhone XR	2	5.56%
iPhone XS Max	1	2.78%
Iridium,Thuraya	1	2.78%
BlackBerry KEY2 LE	1	2.78%
One Plus 5	1	2.78%
Samsung Galaxy A20e	1	2.78%
Samsung Galaxy A32	1	2.78%
Samsung Galaxy A5	2	5.56%
Samsung Galaxy A52	1	2.78%
Samsung Galaxy S20	1	2.78%
Samsung Galaxy S20 FE	1	2.78%
Xiaomi Mi 11	3	8.33%
Xiaomi Redmi Note Pro 6	1	2.78%
Xiaomi Redmi Note 5	1	2.78%
Xiaomi Redmi Note 7	1	2.78%
Xiaomi Redmi Note 9S	1	2.78%
Grand Total	**36**	**100.00%**

Interesting submission was a user with the Satphone OS who submitted 2 devices, Iridium and Thurasya and submitted that the organization swapped in turns in the timeframe of 6 months. Overall the results are very similar to BYOD category, where although the count of different models is high the brands remain the same thus the same risk is applied.

Question 5 concerning if the user had the opportunity to choose between different options of smartphones. The question's purpose is to find out if the organizations provided a pre chosen smartphone or it gave the choice to the users to do so. When the choice is made by the organization the smartphone should possess the proper security qualifications. ENISA is not so addressing organizations about the choice of device, although as long as there is OS diversity and the smartphone can support the proper security methods (e.g. cryptographic modules) the choice is adequate. NIST believes that the choice should be according to the organization's mission needs (what data, why and where). Cost factor may affect on how to select a smartphone but factoring the security needs, it is important to select smartphones that are still supported by the manufacturer and can accommodate OS and application updates and patches.

The results are divided to 18 users (50%) chose the smartphone that was provided while the other half did not have the choice. The sample results show us that half of organizations issued smartphones may not fulfil the device security qualifications as it is dependent on a user's awareness of security matters.

Table 3.5

Q5. Choice of Smartphone	Sum	Percentage
Responses		
No	18	50.00%
Yes	18	50.00%
Grand Total	**36**	**100.00%**

Table 3.6

Q6. Smartphone Choice Criteria	Sum	Percentage
Responses		
Branding	5	27.78%
Branding, Hardware Capabilities	2	11.11%
Branding, Hardware Capabilities, Security Features	2	11.11%
Branding, Security Features, Easy to Use for Work	1	5.56%
Easy to Use for Work	4	22.22%
Hardware Capabilities	2	11.11%
Hardware Capabilities, Security Features	1	5.56%
Hardware Capabilities, Security Features, Easy to Use for Work	1	5.56%
Grand Total	**18**	**100.00%**

Question 6, a follow up question to question 5, is addressing the users' criteria of the choice they made. The multiple choices given were "Branding"," Hardware capabilities", "Security features", "Easy to use for work" and "Other" - an open text answer for any remaining reason.

From the 18 users that had the free choice of selecting the smartphone only 5 (27,78%) users had the security features selected combined with another choice. The top results were Branding counted 10 times and Hardware capabilities counted 8 times.
It is advised that a list of appropriate devices should be given to users from the organization, before choosing a device in order to follow the organization's mission.

Question 7 is exploring the authentication methods that the user uses in the provided smartphone. As in question 4 of the BYOD section, guides are concerned about the authentication methods (e.g. token based), their combinations, the risks involved with weak authentication choices and the mitigations and awareness of the users for the data. Finally the question has multiple answers, as previously seen.

Examining the results 17 different combinations are identified ,where Fingerprint Scanner is found 16 times in combinations ,then PIN Number is found 14 times, next is Pattern Lock found 7 times, Facial Recognition/Iris Scanning/Intelligent Scan found 6 times and finally Smart Lock - Other Security Measures 1 time. Furthermore 1 user responded with "None", meaning that no authentication is used. The results show that secret authentication is surpassing token-based authentication, thus increasing the risk of compromise due to weak authentication. Additionally, 17 counts were identified, with a single way to authenticate the users preferred instead of multiple, the 47,23% percent of total counts. Repeating from the BYOD section, troubling results as a single authentication can give advantage to an attacker of multiple tries instead the device forcefully prompts over to another way, preferably token-based.

Table 3.7

Single Authentication	Count	Percentage
Responses		
None	1	2.78%
PIN Number	3	8.33%
Pattern Lock	1	2.78%
Password-based	6	16.67%
Fingerprint Scanner	5	13.89%
Smart Lock – Other Security Measures	1	2.78%
Total	**17**	**47.23%**

Table 3.8

Q7. Authentication Method(s) of provided smartphone	Sum	Percentage
Responses		
Facial Recognition/Iris Scanning/Intelligent Scan	1	2.78%
Fingerprint Scanner	5	13.89%
Fingerprint Scanner, Facial Recognition/Iris Scanning/Intelligent Scan, Smart Lock – Other Security Measures	1	2.78%
None	1	2.78%
Password-based	6	16.67%
Password-based, Fingerprint Scanner	3	8.33%
Password-based, Pattern Lock	1	2.78%
Password-based, Pattern Lock, PIN Number	1	2.78%
Password-based, PIN Number, Facial Recognition/Iris Scanning/Intelligent Scan	2	5.56%
Pattern Lock	1	2.78%
Pattern Lock, Fingerprint Scanner	1	2.78%
Pattern Lock, PIN Number	1	2.78%
Pattern Lock, PIN Number, Fingerprint Scanner	2	5.56%
PIN Number	3	8.33%
PIN Number, Facial Recognition/Iris Scanning/Intelligent Scan	2	5.56%
PIN Number, Fingerprint Scanner	4	11.11%
Smart Lock – Other Security Measures	1	2.78%
Grand Total	**36**	**100.00%**

Question 8 asking the users if the authentication methods were chosen by them or were pre-set by the organization. The importance of this question is in the fact that users may not set the proper authentication methods (token based authentication) and ignore two-factor authentication. ENISA believes that the risks associated with weak authentication methods are high, especially for employees and high officials. Recommendations for end-users and IT officers for necessary precautions have been offered. NIST relies on EMM technology where it requires a password and other authentication mechanism (e.g., token-based), before accessing the organization's resources, basic parameters for password strengthening. Additionally, creation of policies acceptable for these devices, addressing the standard security protections to be applied to all enterprise smartphones, as well as configuring different policies according to users' roles. Then smartphones can be properly configured and enrolled into the EMM by installing an EMM certificate and finally provisioning the device to the users.

Table 3.9

Q8. Chosen Authentication Method	Sum	Percentage
Responses		
By me	25	69.44%
Pre-set	11	30.56%
Grand Total	**36**	**100.00%**

Exploring the results, 25 users (69,44%) chose their own authentication methods and the 11 users (30,56%) had pre-set by their organization. Although 1/3 percent of our sample is following the guidelines, the remaining 2/3 percentage organizations may have a higher risk of having an authentication attack. Organizations should pre-set the authentication mechanisms prior to giving the smartphone or provide proper guidelines for the users.

Question 9 addresses the issue of access to various features of a smartphone a user has access to. Given options regarding those features were, Wi-Fi, Camera, Microphone, Bluetooth, Tethering, QR code Scanning. Additionally the option of no access to the various features was given. The question relates to question 4 of the BYOD regarding the guide's thesis of leaving some of those features open when leaving home/work networks. Additionally, corporate policies are prohibiting the use of cameras, microphones or scanning QR codes in order to prevent data leakage. NIST's guide mentions that each new feature has the potential to introduce new threats to security and privacy. A list including all the aforementioned features is offered by the guide with baseline characteristics in order to consider various threats and opportunities.

Table 3.10

Q9. Access to Settings	Sum	Percentage
Responses		
Microphone	1	2.78%
Wi-Fi, Camera, Bluetooth	1	2.78%
Wi-Fi, Camera, Bluetooth, QR code Scanning	1	2.78%
Wi-Fi, Camera, Microphone	1	2.78%
Wi-Fi, Camera, Microphone, Bluetooth	3	8.33%
Wi-Fi, Camera, Microphone, Bluetooth, QR code Scanning	5	13.89%
Wi-Fi, Camera, Microphone, Bluetooth, Tethering	5	13.89%
Wi-Fi, Camera, Microphone, Bluetooth, Tethering , QR code Scanning	18	50.00%
Wi-Fi, Camera, QR code Scanning	1	2.78%
Grand Total	**36**	**100.00%**

The 50% percent of issued smartphone device users reported that they have access to every option that was given, where the rest of 48% are allowed to use more than 2 features. A single user (2,78%) responded that has access only to the microphone. It is unknown if organizations are considering those features a possible threat to their or user's data in analogy to the responses. Proper policies should be designed after carefully considering the threats that may be created by allowing free use of such features.

Question 10 is concerned with whether the provided smartphone has access to organization's resources, giving the example of a server. The question is the same with question 25, thus the same guide concerns apply. Those are ENISA's preoccupation with access and NIST's configuration of policies and settings through EMM.

Table 3.11

Q10. Access to the organization's resources	Sum	Percentage
Responses		
No	16	44.44%
Yes	20	55.56%
Grand Total	**36**	**100.00%**

The survey shows that 20 users (55,56%) responded positively while the rest 16 (44%) responded negatively. Considering the fact that the allowed percentage is high, organizations should follow the guide's proposals in order to protect the resources.

Question 11 is a follow up question to question 10 asking if the access in those resources is limited.
Both guides' concerns are the same with the one found in question 26 of BYOD section, which is ENISA allowing access to devices with certificates and NIST's concerns of misconfigurations and EMM solution.

Examining the results, 11 users (55%) responded as “Yes”. 6 users (30%) responded as “No” and 3 users (15%) responded “Not Sure”. Although the results are very positive as more than 50% percent of sample smartphones are restricted, giving control access to valuable resources, organizations may consider their policies to cover the control access and become clearer to those that are uncertain.

Table 3.12

Q11. Limited Resource Access	Sum	Percentage
Responses		
No	6	30.00%
Not sure	3	15.00%
Yes	11	55.00%
Grand Total	**20**	**100.00%**

Question 12 concentrating on smartphone access to classified/sensitive work-related data. The risks considered by the guides, gaining access to such data, involve categories like data leakage with guides proposing better authentication mechanisms or better hardware mechanisms for encryption as mitigations. The risks and mitigations are identical to those in question 13 of the BYOD section following an in-depth analysis.

Table 3.13

Q12. Classified/Sensitive Work Data Access	Sum	Percentage
Responses		
No	19	52.78%
Yes	17	47.22%
Grand Total	**36**	**100.00%**

Observing the results, organizations should ensure that the guides' mitigations are keeping up as 17 users (47,22%) responded positively. The rest of 19 users (52,78%) may show that organizations are not yet prepared for smartphone devices to be given this kind of access.

Question 13 asking if the IT department enforces security policies or lock permissions in the provided smartphones. Policies should be designed and enforced to every device entering an organization network including smartphones. As mentioned above, policies should be designed according to the organization's missions and users’ roles. It is as important for the same policies to be properly enforced by the additional responsible organization authority. ENISA supports that policies should have policies on various security measures, covering all the risk and employees and High officials should have protective measures, such as memory encryption and auto-locking the device, enforced more often by an IT officer. NIST, relying on EMM technology, believes that automatically enforcing and enabling those policies can help with smartphone devices through detecting changes of the approved security configuration baseline set by IT administrators.

From the total of 36 users, 12 (33,33%) responded negatively, 18 users (50%) responded positively while the remaining 6 users (16,67%) responded as "not sure". As an overall result, this is positive but improvements may be needed as the negative responses are noticeable. Regarding the "not sure" response organizations should make more clear positions about policies as to cover any user's doubt.

Table 3.14

Q13. Enforcing security policies	Sum	Percentage
Responses		
No	12	33.33%
Not sure	6	16.67%
Yes	18	50.00%
Grand Total	**36**	**100.00%**

Question 14 concerning the possibilities available for the users to change the permissions of the applications. The question is both for permissions of an application is requiring from various features (e.g. microphone) and from other applications (example: contacts needed from phone application).Due to risks implied (e.g. Data leakage from applications), organizations should allow specific applications for users and not allow the change of those permissions when applicable. ENISA and NIST concerns are about legitimacy of those applications, proper distribution channels and mitigations. More found in question 11 and 12 of the BYOD section for inspecting permissions.

Table 3.15

Q14. Applications Changing Permissions	Sum	Percentage
Responses		
No	13	36.11%
Not sure	13	36.11%
Yes	10	27.78%
Grand Total	**36**	**100.00%**

The sample results show that 13 users (36,11%) cannot change the permissions while 10 users (27,78%) can change and 13 users (36,11%) are not sure. Organizations should consider locking those permissions as the percentage of people that are allowed to change them is close to those who cannot. Additionally better education and a more clear purpose can help clear any uncertainties a user may have and help understand the purposes of not changing any permissions.

Question 15 explores the matter of auto-locking. Considering that the smartphone is issued by the organization and pre-configured it is important to be auto-locked in order to protect the smartphone's content. Both ENISA concerns of loss or theft and NIST concerns and mitigation with EMM can also be found in question 6 of BYOD section.

Examining our results we find 31 users (86,11%) where their provided smartphones are auto-locked enabled while 5 users (13,87) are not enabled. Considering the fact that auto-locking is considered a basic requirement for security needs and that the smartphone is organization-issued, is very troublesome. NIST's EMM technology may help organizations to fix those errors with the options offered like remote locking.

Table 3.16

Q15. Smartphone Auto-Lock	Sum	Percentage
Responses		
No	5	13.89%
Yes	31	86.11%
Grand Total	**36**	**100.00%**

Question 16, a follow-up question to question 15, considers with the smartphone auto-lock time. Time is a factor reducing the risk of an adversary gaining access to an unattended smartphone. As abovementioned risks and mitigations of both guides, also support that auto-lock time should be minimized as soon as possible.

Table 3.17

Q16. Smartphone's Auto-Lock Time	Sum	Percentage
Responses		
0 - 1 min	18	58.06%
1 - 2 min	8	25.81%
3 - 5 min	3	9.68%
Not sure	2	6.45%
Grand Total	**31**	**100.00%**

The overall results are very positive as 18 users (58,06%) responded "0 - 1 min" , 8 users (25,81%) responded "1 - 2 min" and 3 users (9,68%) "3 -5 min". The timeframes are short, with most users having the lowest minute option while the "3 - 5 min" being only 10%. Finally 2 users (6,45%) responded "Not sure", an answer connected with users' education and awareness of security measures that organizations should raise.

Question 17 is addressing if the provided smartphones turn off automatically features if the device is idle for a long time. The question offers multiple choices between "Bluetooth", "GPS", "Wi-Fi", "Tethering" and a negative answer. Those features may unwillingly be exploited as a threat to the organizations as are most commonly used daily and various exploits have been seen before.
ENISA and NIST raise those concerns and explain the risks by giving examples. Additionally NIST is offering mitigations for those threats. As a previous analysis made in question 7 of the BYOD section, addressing the same problem, more details can be found.

After inspecting the results, we find that 30 users (83,33%) responded that their provided smartphones do not turn off any features when the device is idle. A result with negative impact on many organizations as multiple risks are created. EMM mitigation can help monitor those features and automatically turn them off.
Additionally 5 users (16,67%) reported some features to turn-off automatically with the highest being Bluetooth with a count of 4 and Wi-Fi, GPS and Tethering with a count of 3. Finally only 1 user (2,78%) reported that all features are turned-off automatically.

Table 3.18

Q17. Idle Features	Sum	Percentage
Responses		
Bluetooth	2	5.56%
GPS, Wi-Fi, Bluetooth	1	2.78%
GPS, Wi-Fi, Bluetooth, Tethering	1	2.78%
GPS, Wi-Fi, Tethering	1	2.78%
No Features	30	83.33%
Tethering	1	2.78%
Grand Total	**36**	**100.00%**

Question 18 is concerned with the smartphone's backup time. Back up is an important action, often needed for auditing purposes, in order to secure data and support business continuity. Given the fact that the smartphones are organization-issued, preconfiguring is in order in the best possible timeframe. As explained in question 18 of BYOD section, ENISA supports and offers guidelines for backup employees. While NIST supports backup, it raises various concerns about backup locations and managing the key of those locations.

Table 3.19

Q18. Smartphone Backup	Sum	Percentage
Responses		
Never	9	25.00%
Not sure	15	41.67%
Once a day	2	5.56%
Once a month	1	2.78%
Once a week	2	5.56%
Once per year	1	2.78%
When Prompted by my device	6	16.67%
Grand Total	**36**	**100.00%**

Inspecting the sample, 15 users (41,67%) responded “Not sure”, 9 users (25%) responded “Never , 6 users (16,67%) responded “When prompted by my device”, 2 users responded “Once a day” and
“Once a week” (5,56% each) and 1 user responded “Once a month” and “Once per year” (2,78% each). Considering the smartphones are organization-issued, the results are mostly negative. The timeframe of positive answers is not positive as “when prompted by my device” is up to the smartphone's OS and applications limit. Interesting is the percentage of users responding “Not sure”, being the highest percentage, where users are not aware of backup operations. Organizations should make clear of any backup operations needed in order for users to grow more aware.

Question 19 is a follow up question, considering if the backup is made in a cloud system. Given the opportunities cloud systems offer, organizations should consider the use as in a regular laptop device. Both guides offer recommendations combining cloud storage with backup systems and considerations regarding various risks (more found in question 19 of BYOD section).

Although the percentage of positive responses is low, the results show that the highest percentage of cloud based backup is 10 users (83,33%) opposed to 1 user responding negatively and "not sure" (8,33% each). Organizations are safer as cloud services are the best choice for backing up big amounts of data, protecting the users' data too.

Table 3.20

Q19. Cloud Based Backup	Sum	Percentage
Responses		
No	1	8.33%
Not sure	1	8.33%
Yes	10	83.33%
Grand Total	**12**	**100.00%**

Question 20 is concerned with the users availability to install applications on their own, by lists provided by the organizations, or if they are limited. As many breaches in organizations are originating from potentially unwanted applications, lists should be provided with either allowing apps (whitelisting) or the apps that are not allowed (blacklisting). ENISA recommends enforcing whitelists considering the smartphone has access to sensitive data or access to an organization network and its resources. Furthermore an extra caution to the permission of those applications should be taken as easy read access of data by those apps raise the risk. NIST acknowledges the risks of applications posing to an organization, mentioning that any application can act as a portal for the developer to compromise the device and access sensitive enterprise information. As a mitigation, NIST rely on EMM technology with MAM functionality where smartphones can be restricted on which official app stores may be used and limit their content and restrict which apps can be installed through whitelisting apps (preferable) or blacklisting apps.

Table 3.21

Q20. Installing Applications Restrictions	Sum	Percentage
Responses		
No	12	33.33%
Not sure	7	19.44%
Yes	17	47.22%
Grand Total	**36**	**100.00%**

The results show that 17 users (47,22%) responded that can install applications without restrictions, 12 users (33,33%) responded that cannot install applications freely and 7 users (19,44%) responded that are not aware of any limits. Although a significant percent cannot install apps freely the bigger percentage can, leaving the organizations exposed to malware threats. By using EMM technologies organizations can restrict the applications allowed and ensure that users, who are unaware, may follow proper guidelines.

Question 21 is asking if an unwanted application is installed in the smartphone does the IT department remove it. The PUA is usually a policy violation, where the user succeeds in installing an app bypassing the IT systems under the awareness of the IT department (shadow IT). Additionally a PUA can be installed without the user's awareness as for example in a part of a bundle. As the smartphone is pre managed by the

organization proper methods of identifying such activities may be implemented in order to proceed with the application removal. ENISA acknowledges the fact of risk and additionally explains ways that fake applications can be posed as legitimate in order to infect a smartphone. In order to mitigate infection risks, in case it can be applied depending on the smartphones, PUA must be remotely removed if installed. NIST mitigation through EMM with MAM functionality. When applied to smartphones, remote removal and management of applications should take place and enterprise system administrators can monitor applications behavior, configuration compliance or presence of unauthorized apps on a user device.

Examining the results, 13 users (36,11%) responded positively, 11 users (30,56%) responded negatively and 12 users (33,33%) responded as "Not sure". It is significant that the biggest percentage of answers replied as "Yes", still worries are raised as the percentage of negative answers is big added with the uncertain answers. Organizations should enforce policies regarding the applications installations according to their mission and issue and educate users regarding proper guidelines to install and use applications.

Table 3.22

Q21. PUA Removal	Sum	Percentage
Responses		
No	11	30.56%
Not sure	12	33.33%
Yes	13	36.11%
Grand Total	**36**	**100.00%**

Question 22 is a follow up question to question 21, regarding the users' notification about the existence of a potentially unwanted application and the removal of it. It is important to inform the smartphone user as soon as possible in order to proceed with the appropriate actions and recommendations. ENISA is not addressing the matter of notification although in the previous question acknowledges PUA and their immediate removal. NIST believes that organizations should have security policies and rules that produce remediation actions when such activities occur. Through EMM agents can easily notify users via a push notification or potentially an SMS. Additionally remote removal of applications or temporary revocation of access to enterprise resources is often seen as the next step if the notification does not remediate the issue.

Table 3.23

Q22. PUA Notification	Sum	Percentage
Responses		
No	1	7.69%
Not sure	4	30.77%
Yes	8	61.54%
Grand Total	**13**	**100.00%**

The sample results show that 8 users (61,54%) are notified, for example through SMS, Push notification, or Email, while 4 users (30,77%) responded "Not sure" and 1 user (7,69%) that is not notified. An overall positive result as 61,54% are notified through a channel about a threat. Additionally as observed a big percentage of users not notified it is suggested for organizations to create policies regarding such activities.

Question 23 explores the smartphone update policy. In order to patch any vulnerabilities, organizations should configure the smartphones to automatically update both OS and the applications installed. Following question 21 of the BYOD section, both guides support that automatic updates should be regular, with

previous vetting of the patches, raising their concerns for misconfigured smartphones and proportion of EMM technologies as a mitigation (NIST).

Examining the results 23 users (63,89%) responded that the smartphones are updated automatically, 11 users (30,56%) responded that do not, while the rest of the 2 users (5,56%) are not sure about automatic updates. The results show a positive outcome but considering the fact that the smartphones can be pre-configured the 30,56% should be minimized, even after the smartphones have been handled. EMM can help configure those smartphones remotely and ensure, in case a user is unaware, that updates properly.

Table 3.24

Q23. Automatic Updated	Sum	Percentage
Responses		
No	11	30.56%
Not sure	2	5.56%
Yes	23	63.89%
Grand Total	**36**	**100.00%**

Question 24 survey if the provided smartphones have pre-installed security features, for example VPN or antivirus scanners, from the IT department. Security features offer an extra layer of security in case of multiple threats. For example an antivirus can mitigate malwares or a VPN can mitigate man in the middle attacks. As in question 14 of the BYOD section both guides support the existence of such features. On the other hand NIST, although it supports anti malware products, stands firm to the usage of EMM technologies for handling infected smartphones.

Table 3.25

Q24. Additional Security Applications	Sum	Percentage
Responses		
No	11	30.56%
Not sure	6	16.67%
Yes	19	52.78%
Grand Total	**36**	**100.00%**

The survey results are 19 users (52,78%) responded “Yes”, 11 users (30,56%) responded “No” and the rest 6 users (16,67%) responded “Not sure”. Results are negative as only half of the percentage is using extra security measures. Organizations should pre install security applications in order to decrease risks of attacks and take proactive actions

Question 25 asking if users' smartphones get infected, is the IT department informing them. The IT department should inform users about any breaches or infections of their smartphones in order for the user to be aware. As smartphones are part of the organization and many antivirus products offer a collective way to inform a centralized software controller, IT departments may find it easier to do so. Due to the nature of ENISA guide, addressing risks and mitigations, users’ notification is out of scope. NIST proposes the use of MTD technologies integrated with an EMM to enable users’ notification or automated response to remediate detected vulnerabilities or quarantine apps. Additionally if measures want to be taken EMM agents can first warn the users then take appropriate actions (wiping data not owned by the organization can cause legal issues).

Results show that 10 users (27,78%) responded that they are getting informed in case of an infection, 11 users (30,56%) responded that they do not and 15 users (41,67%) responded that they are not sure. The users responding are a low percentage. Most worrying is the percentage that responded negatively as the 30% of our sample have been infected and were not informed. The highest percentage is the "Not sure" answer where either the users have not experienced such a scenario or their smartphones were infected without being aware. Organizations should inform users in order to avoid risks escalating from users actions due to their no knowledge of an incident.

Table 3.26

Q25. IT Department Information	Sum	Percentage
Responses		
No	11	30.56%
Not sure	15	41.67%
Yes	10	27.78%
Grand Total	**36**	**100.00%**

Question 26 is concerned with the smartphone interaction with other devices. Those devices can include personal computers where smartphones can be infected or transmit data without the user's knowledge. Guides considerations include smartphone interaction with devices, raising alerts of data leakage through various technologies and offer mitigations through policies and EMM technologies, as seen in question 22 of the BYOD section.

Table 3.27

Q26. Interaction with other devices	Sum	Percentage
Responses		
No	5	13.89%
Not sure	5	13.89%
Yes	26	72.22%
Grand Total	**36**	**100.00%**

Examining the survey, 26 users (72,22%) responded positively and 5 users reported negatively and "not sure" (13,89 each). The majority of our users are able to interact with other systems creating a risk for all those organizations of data disclosure and possible infections. Organizations should issue policies and preconfigure smartphones before issuing them to users in order to interrupt any unwanted connections.

Question 27 exploring the smartphones storing data to removable media. The risk raised of data loss through for example loss is rising as removable media as memory cards are easy to lose. It is up to organizations to permit or forbid the use, depending on the policies and their mission. According to guides, also mentioned in question 23 of BYOD section, those risks are acknowledged and offered as mitigation encryption in order to protect from such risks and in cases bounding the devices with those removable media.

Examining our results 11 users (30,56%) reported that use removable media, 17 users (47,22%) that are not using removable media and 8 users (22,22%) responded “Not sure”. As 30% of the users are using removable media they should be aware if the organization is allowing such actions and if they do must ensure that encryption is used. Users that responded “Not sure” must be made clear from the organization as to know how to operate correctly.

Table 3.28

Q27. Removable Media	Sum	Percentage
Responses		
No	17	47.22%
Not sure	8	22.22%
Yes	11	30.56%
Grand Total	**36**	**100.00%**

Question 28 is surveying the use of extra encryption for smartphone files or communications. As mentioned in the previous question, encryption is considered a mitigating factor for many threats including the risk of loss or theft. Depending on the organization's mission, encryption may vary depending on the sensitivity of the data. As in question 24 of the BYOD section, guides are agreeing with the use of such applications and offer various options to do so although raising alerts for proper key management.

Table 3.29

Q28. Extra Encryption	Sum	Percentage
Responses		
No	20	55.56%
Not sure	6	16.67%
Yes	10	27.78%
Grand Total	**36**	**100.00%**

Survey results show that 20 users (55,56%) responded negatively, 10 users (27,78%) responded positively and 6 users(16,67%) responded “Not sure”. Organizations should create a plan considering the encryption methods that the smartphones that are going to be issued to users and configure them according to their needs. Furthermore users must be informed about proper encrypting the data or communications in need as the overall results show that users do not use encryption.

Question 29 is asking if the users inform the IT department in case of smartphone loss. With the term loss the scenarios of theft and malfunction is included. Smartphones are very susceptible to loss or malfunction (for example destruction) due to their nature. Additionally considering the fact that the smartphones are organization property users must inform the responsible department, most commonly the IT department in order to revoke any access or remote wipe data that the smartphone may have as soon as possible. Both guides find the risk very high and as in question 28 of the BYOD section, propose mitigations. ENISA suggests the use of strong authentication methods while NIST results in EMM technologies.

Inspecting the results, 25 users (69,44%) responded negatively to our question while the rest 11 users (30,56%) responded positively. A negative correlation as almost 70% of our sample have lost/stolen their smartphone and did not inform the IT department, increasing the risk of data disclosure and resources being vulnerable.

Table 3.30

Q29. Smartphone Loss Update	Sum	Percentage
Responses		
No	25	69.44%
Yes	11	30.56%
Grand Total	**36**	**100.00%**

Question 30 examining smartphones automatically wiping data if many authentication tries were unsuccessful. A mitigation like this is implemented in case of loss or social engineering, where an attacker may try to gain access to the device physically. Organizations may pre configure the device with a threshold if the sensitivity of the data is crucial. As mentioned in question 29 of the BYOD section, both guide are in favor of such measures and additionally ENISA suggest frequent backup in addition to deletion while NIST falls to EMM technologies to set the parameters for auto-wiping.

Table 3.31

Q30. Automatic Smartphone Data Wipe	Sum	Percentage
Responses		
No	10	27.78%
Not sure	18	50.00%
Yes	8	22.22%
Grand Total	**36**	**100.00%**

Examining the results, 8 users (22,22%) responded "Yes", 10 users (27,78%) responded "No" while the rest 18 users responded "Not sure". The highest percentage are users that are not sure. Organizations should inform users before handing the smartphone to reduce the chances of mistakenly wiping data and aware the users with the function. Furthermore according to the results the percentage of disabled auto-wipe features is higher than the enabled. The mitigation should be adopted more in case authentication methods fail.

Question 31 is asking if the users are allowed to travel with that smartphone. As mentioned in question 31 of the BYOD section the nature of smartphones make it easier to travel with it including the risks created (loss/theft). Organizations should create policies regarding travel as the smartphone is their own property and should not be part of such activity if no for business needs. ENISA believes that proper policies should be designed including mitigations, to various risks like authentications. NIST on the other hand confines in EMM technologies for remote management and updating as soon as possible and supports the use of personal email accounts for better access to data.

According to our results 25 users (69,44%) are allowed to travel with the provided smartphone while 11 users (30,56%) are not allowed. As most users are allowed to travel with the smartphone devices, organizations should ensure that best authentication practices are in order and follow the proper policies before issuing the smartphones.

Table 3.32

Q31. Travel with Smartphone	Sum	Percentage
Responses		
No	11	30.56%
Yes	25	69.44%
Grand Total	**36**	**100.00%**

5.3. Awareness Questions

Question 1 asks how familiar the user is with cybersecurity. It is important for users to be aware of what cybersecurity is and what the importance is and impact on their smartphones.
ENISA believes that lack of user awareness is factoring the risks of many attack scenarios, for example unintentional disclosure. NIST believes that users that are not educated on how to properly secure their mobile device, this oversight could endanger organizations and user's personal information.

Table 4.1

Q1. Cybersecurity Familiarity	Sum	Percentage
Responses		
I have no knowledge of related topics	39	16.81%
I follow the news of related topics	68	29.31%
I have read/taught myself about related topics	51	21.98%
I have taken one or more courses in a related topic	36	15.52%
I have a degree in this or a related field	38	16.38%
Grand Total	**232**	**100.00%**

The results are, 68 users (29,31%) reported that they follow cybersecurity news of related topics, 51 users (21,98%) that have read/taught themselves about related topics, 39 users (16,81%) that have no knowledge of related topics, 38 users (16,38%) that have a degree on cybersecurity field or related and 36 users (15,52%) that have taken one or more courses in cybersecurity related topics. Overall, the majority of users (83,19% of the sample) are aware of what cybersecurity is, in contrast to 16,81% that have no knowledge. Additionally, a most positive element is just above of 50% of our users are trying to gain cybersecurity knowledge through education means or by themselves.

Question 2 and 3 is about the training in cybersecurity the users had. Question 2 asks the user if they have ever received training for cybersecurity threats, giving the example of phishing mails while question 3 asks if they have ever received training from any organization about security matters for your smartphone. Training is a simple solution of covering many threats for the aforementioned questions of the previous section. According to ENISA, IT officers should raise awareness of the risks and issue organizational advice and guidelines for smartphone users. NIST believes organizations should provide effective ways to teach users how to protect their smartphones and understand the importance of security mechanisms and how to apply them. A few examples of smartphone security trainings should be identification of phishing attacks, proper management of authentication credentials, identifying malicious EMM profiles or other malicious applications, and rapid perform of OS and application updates.

Table 4.2

Q2. Cybersecurity Training for Threats	Sum	Percentage
Responses		
No	106	45.69%
Yes	126	54.31%
Grand Total	**232**	**100.00%**

Table 4.3

Q3. Training for smartphone security matters	Sum	Percentage
Responses		
No	161	69.40%
Yes	71	30.60%
Grand Total	**232**	**100.00%**

According to the data 126 users (54,31%) reported that had cybersecurity training for threats and 71 users (30,60%) had training for their smartphones security. On the other hand 106 users (45,69%) had not received training for cybersecurity threats and 161 users (69,40%) have not received training for their smartphones security.

Although the numbers of cybersecurity threats training are fairly positive the results of training for smartphone security are disappointing. The results show an immaturity of organizations to understand the need of training users even if smartphones are considered a basic asset for the organizations, raising the risk of those organizations to be found vulnerable.

6. Discussion

[R1]*Are organizations mature enough to understand that smartphones have become more evolved to the point that their security needs to be on a level equal to that of a regular laptop?*
In order for smartphones to be considered equal to laptops similar features for both devices operations must be considered. This includes features like auto-locking, backup operations, access control to resources, security enhancement etc., features that a laptop must have in order to follow proper guidelines. Exploring the BYOD answers the number of users smartphone auto lock time between "0-1 min" to "3 - 5 min" is 161 (82,14%). User shortest backup frequency, that is from "Real Time" to "Once a Month", is 74 (37,75%) and overall users cloud based backup is 97 (65,99%). Furthermore, users responding with extra layers of security are 86 (43,88%) and using extra encryption are 30 (15,31%). Finally, in access control we observe that 43 users (21,94%) are having policies installed when enter the organizations network, 146 users (74,49%) can interact with other devices and 55 users (28,06%) have access to organizations resources where the 35 (63.64%) of them are limited. Although some features have positive results, for example cloud backup and auto lock time, the overall results are showing that in BYOD organizations are not treating smartphones to the same level as a laptop device. In the organization-issued category we observe that 31 users (86,11%) have their smartphones auto lock enabled and 29 of them (93,55%) declare between "0 - 1" minutes to "3 - 5" minutes. Regarding brief time backup procedures, 5 users (13,9%) responded from "Real Time" to "Once a Month", and 10 (83,33%) of them use cloud based backup. Additionally, 19 users (52,78%) responded positive in extra layers of security, 10 users (27,78%) use extra encryption and 13 users (36,11%) are having PUA removed by IT department and 8 (30,77%) of them are notified. Finally, 18 users (50%) responded positive that organizations enforce security policies, 26 (72,22%) users smartphones can interact with other devices and 20 users (55,56%) have access to organization's resources

where 11 (55%) of them are limited. Even though the sample is small, organization-issued smartphones shows better results than BYOD but this is still low. Overall, regarding smartphones security compared to laptops in organizations, results show that there is still improvement in order to narrow that gap.

[R2] *Do users understand the need to follow proper guidelines in order to keep their personal information and organization's resources safe?*
Due to the rise of smartphone usage users should separate the usage of personal data with those of corporate. According to our results from the BYOD category, 139 users (70,92%) use sensitive applications and 100 of them (71,94%) are using separate lock authentications. Furthermore 158 users (80,61%) are inspecting the permissions that an application needs from another application, 170 users (86,73%) inspect permissions of application needs in order to operate while 154 users (78,57%) are using only proper sources of installing applications. In terms of mitigations, 86 users (43,88%) use additional applications for security, 131 users (66,84%) are auto-updating their smartphones and 127 users (64,80%) are wiping the data of their decommissioned smartphones. On the other hand, 101 users (51,53%) cannot remote wipe data in case of smartphone loss, 183 (93,37%) do not inform the IT department in case of loss and 88 users (44,90%) reported that the smartphone is not auto wiping the data in case of many failed authentications. Finally, 127 users (64,80%) are following best practices and do not unlock administration privileges through jailbreak.
In terms of organization issued smartphones the results show that 15 users (41,67%) use the smartphone for personal purposes but from the 18 users (50%) who had the option to select the smartphone only 5 (27,78%) of them selected it for the security features.
In sum, users are apt to follow the proper procedures of the guidelines, making better effort to protect the data in question, even if there is a lack in certain fields.

[R3] *Have organizations invested more resources in the security of smartphones in the midst of pandemic?*
Smartphone devices should help the work from home considering the situation. Keeping in mind that questionnaire results were collected during the 6 first months of 2021, organizations were found both to be challenged by the increased demands pose to implementing remote working but also found to be prepared in some aspects given that had already passed a year since the beginning of the pandemic. Remaining in the BYOD section, 88 smartphones (44,90%) have access to classified/sensitive information of their organization, 55 (28,06%) smartphones have access to organizations resources while the 35 (63,64%) of those smartphones have limited access. Such results reflect the increase of home use, but organizational limitations show that may not be ready yet to give full access as it happens with a laptop device. Additionally, the percentage of inspection in BYOD smartphones is low, with 22 users (11,22%) having their smartphone inspected before accessing the organizations systems, even if the access is remotely. In terms of mitigations needed for remote working, only the 43,88% of the sample users install additional security measures and only 30 users (15,31%) use extra encryptions for their files and communications. Finally, regarding the concern of a jailbroken smartphones users responded that do not have elevated administrator privileges thus no suspicious application or activities can take place while can be unattended due to physical access to device by the IT department.
In the issued smartphones section we observe that 15 users (41,67%) use the smartphone for personal purposes and 4 users (11,11%) are limited with separate data save. Furthermore we observe that 17 users (47,22%) have access to classified/sensitive information of their organization and 20 users (55,56%) have access to the organization resource where the 12 (33,33%) of them are limited. Results show that organizations are more keen to allow their issued smartphones to gain access to various data or resources

in contrast to BYOD smartphones but still rather low. In terms of mitigations, organizations restrictions in installing applications are applied to 17 users (47,22%) ,users informed of Possible unwanted application are 13 (36,11%),additional security applications installed in 19 users (52,78%) and only 10 users (27,78%) have extra encryption in their files and communications. Overall organizations were forced to give access to various resources and data through ways not previously used like those of smartphones but the investment in security is still weak.

[R4] *Do organizations follow proper official guidelines in order to allow smartphones to enter their infrastructure therefore gain access to organization's data?*
In order for smartphones to properly gain access to organizations infrastructure conditions should be met regarding the organizations mission. Through the survey questions regarding the access of smartphones according to ENISA and NIST guidelines had been asked in order to offer a better insight. From the BYOD section results showed that only 55 users (28,06%) have access to organizations resources and 35 of them (6,64%)are limited. Additionally, 43 users' smartphones (21,94%) have policies installed while gaining access to the network, 22 users (11,22%) have their smartphones inspected and finally only 50 users (25,51%) cannot interact with other devices.
In the category of smartphones issued by organizations, devices should be preconfigured in a way to be ready for the gain access to data. Results show that 17 users (47,22%) do not use the smartphone for personal purposes, 11 users (30,56%) have pre-set authentication method with most users having access to smartphones features (e.g. Wi-Fi, Camera, Bluetooth) and 18 users (50%) have access to every option given. Furthermore, 20 users (55,56%) have access to the resources and 11 of them (55%) are limited. Finally, 18 users (50%) have enforced security policies or lock permissions in their provided smartphones and only 13 users (36,11%) have possible unwanted applications removed by the IT department. Summing up organizations are surely not ready to allow BYOD device entering the network and their data and should pre configure better the smartphones they issue.

Statistical Interests

In order to produce some meaningful results, we would like to test pairs of questions and see whether there is an association between them or not. For example, let's say that we wanted to see if our respondents installed additional security measures (VPN, Virus Scanner), based on their gender. In other words, we want to see if male and female respondents are distributed randomly in the categories of our additional security measures question. If they are indeed randomly distributed, then we would *expect* male and female respondents to have similar proportions in the categories of our security measures question. If the majority of male respondents installed additional security measures, while the majority of female respondents did not, this provides some evidence that the two variables might not be independent, or, that they might have an association. In order to do that, we first create a sample table as below:

Table 5.1

Installed Additional Security Measures	Female	Male	**Total**
Yes	10	76	110
No	34	74	84
Total	44	150	**194**

This is a two-way contingency table, where we have our female and male respondents allocated according to their answer in the security question. These are our observed counts, meaning the people that we observed in our sample. We notice that out of 194 people, 150, or 77%, are male and only 23% female. We can also see that while our male respondents are almost equally distributed in the two categories (76 and 74 for 'Yes' and 'No' answers respectively), our female respondents favor the second category (a 'No' answer) more.

We can move our analysis a step further so as not to rely only on the proportions above for our result. We can compare these numbers (the observed counts) to what we would expect to see if there was indeed no difference in the security categories for males and females (the expected counts), i.e. how would the table above look if the two variables were not related?

So we would like to use a process that tests the hypothesis:

H_0: "There is no relationship / association between the two variables"

against the hypothesis:

H_1: "There is a relationship / association between the two variables"

The expected counts of our table are calculated as:

$$E = \frac{row\ total * column\ total}{total\ sample\ size}$$

These expected counts should show similarity in the security measures categories between female and male respondents. The important question here becomes: if they are different, how much different need our observed and expected counts be, for us to conclude that there is a relationship between the two variables?

The answer to this question can be achieved with a χ^2 test of independence. For this test we calculate the Chi-square test statistic:

$$\chi^{2*} = \sum_{i=1}^{rc} \frac{(\mathrm{E_i} - \mathrm{O_i})^2}{\mathrm{E_i}}$$

where O denotes the observed counts, E the expected, and r is the number of rows and c the number of columns in our table.

We compare χ^{2*} to that from a Chi-square distribution table with degrees of freedom (r-1)(c-1). The degrees of freedom in our estimate is the number of independent pieces of information that were used to calculate the estimate. For example, let's assume our estimate is the average of 3 numbers and we found it to be 10. These three numbers could be {5, 10, 15} or {6, 8, 16}. Once the first two numbers of the set are picked, the third one cannot vary. If our set was {5, 10} no other number than 15 would produce an average of 10. So the only numbers that have the freedom to vary in our set are the first two, while the third one cannot vary. Therefore, the degrees of freedom of our estimate (the average of the three values)

is two, or 3 – 1, or (the number of elements in our sample – 1). So in our example r - 1 rows are free to vary while the last one has to be fixed in order to get the row total. The same is true for the columns. Our decision for the test will be made based on the p-value approach. A p-value is the probability of finding test results at least as extreme as the ones observed, under the null hypothesis H_0 : "There is no relationship between the two variables". In other words, we want the probability $P(\chi^2 > \chi^{2*})$ with degrees of freedom (r-1)(c-1). A very small p-value indicates that our outcome would be very unlikely under the null hypothesis (H_0). The cutoff p-value will be 0.05, meaning any p-value less than that, gives us enough evidence to reject the null hypothesis, or to reject the hypothesis that the two variables are independent.

Statistically significant p-values are indicated in red in the following tables.

Tables 1, 2, 3 and 4 refer to the respondents who have not been provided with phones from their companies. In total, there were 196 people in that group. Table 5 refers to the respondents who have been provided with phones from their companies. In total, there were 36 people in that group. Due to the low number of respondents in the second group, we were not able to find many statistically significant results.

Associations between countries of origin and cybersecurity familiarity

According to the results in the table below, we can see that there seems to be no difference among countries of origin and the familiarity our respondents had on the subject of cybersecurity. But there seem to be differences between countries and the training employees receive both for threats online and their smartphone's security. We examined four countries in total: Greece, Italy, United Kingdom and the United States (other countries were excluded due to low number of respondents). In Italy, there was a 50-50% distribution on the respondents' answers. In Greece most answers were negative (55%), in contrast to the UK (45%) and the United States (21%). These results show that while in the United States employees seem to be getting some training on matters of cybersecurity, a lot of work still needs to be done in Europe and particularly in Greece.

Table 5.2	Associations between Countries of Origin and Cybersecurity Familiarity		
Question	χ^2	Degrees of Freedom	p-value
Cybersecurity Familiarity	12.15	12	0.4340
Training for Threats	10.82	3	0.0127
Training for Smartphone Security	16.16	3	0.0009

Associations between Respondent Gender and security-related questions

For the Cybersecurity Familiarity question, we have a statistically significant result, which makes us reject the hypothesis of no association between the variables. We have 22% of female respondents answering "I have no knowledge of related topics" and 15% of male. When it comes to respondents with "A degree in this or related field" we have only 1 female respondent which accounts to 2% while we have 37 male respondents which account to 21%. For the Additional Security Measures Installed question, another statistically significant result, 77% of female respondents answered "No" and 51% of male. The majority of females, while the males seem evenly divided between the answers. As for the Data Wipe question, we have a statistically significant result. For female respondents 57% were not sure about the data wipe, while for males it was 34%. Only 14% females and 17% males seemed to wipe their data after many failed authentication attempts. The Data Backup Frequency question is not statistically significant. Here we have 23% of females and 26% of males "Never" backing up their data, while 9% and 12% of females and males respectively backup every day. For those that choose to backup only when prompted by their device, we have 50% of female respondents and 26% of male respondents. And those that chose "Once a week or month" we have 11% of females and 26% of males. We observe that for most categories in this question female and male respondents tend to answer in a similar fashion, hence a non-significant result from the test. In conclusion, we can see that male respondents tend to have some knowledge on the Cybersecurity field and more of them seem to install additional security measures. Female respondents seem to be less willing for additional security measures, while we had only 1 respondent with a degree in the field.

Table 5.3	Associations between Respondent Gender and Security-Related Questions		
Question	χ^2	Degrees of Freedom	p-value
Cybersecurity Familiarity	10.674	2	0.013
Additional Security Measures Installed	9.809	3	0.014
Wipe Data After Failed Authentications	7.68	2	0.021
Data Backup Frequency	6.58	3	0.087

Associations between Industry and Security-Related Questions

The Industries chosen, given the best statistical significance for this analysis, were the following:
1st : Business, Finance, Legal, Insurance and Consulting Services
2nd : Educational Services
3rd : Healthcare and Social Assistance
4th : Information Technologies Services

We can see from the table below that for the Cybersecurity Familiarity question we have a highly statistically significant result. This means that Cybersecurity Familiarity does not seem to have similar proportions across the various Industries that the respondents are working. This makes sense, as people working in IT or related fields tend to have more knowledge on this issue, compared to people from Educational or Health related fields. A similar picture can be seen in the next question, about Cybersecurity Training for threats (such as Phishing). This result makes sense as well, for the reason provided above. People across the various industries seem to behave in a similar manner when it comes to wiping their data after failed authentication attempts. The percentages for a 'Yes' answer are 20% for Business etc., 14% for Education, 14% for Healthcare and 15% for IT. The majority of people here seem to have answered negatively in this question. Another statistically significant result is provided in the last question, where the majority (76%) of IT respondents wipe the data from their old smartphones. The next largest percent of 65% comes from people working Business, while 43% of people in Education and 52% of people working in Healthcare seem to wipe the data from their old smartphones. In conclusion, from the results above we can see that people across different fields of work tend to behave differently when it comes to cybersecurity issues. People working in the IT sector receive more cybersecurity training, but in contrast to that, they tend to behave similarly when it comes to options about wiping their smartphone data.

Table 5.4	Associations between Industry and Security-Related Questions		
Question	χ^2	Degrees of freedom	p-value
Cybersecurity Familiarity	36	9	0.0001
Cybersecurity Training	14.5	3	0.0023
Wipe Data After Failed Authentications	10.78	6	0.095
Wipe Old Smartphone's Data	8.18	3	0.042

Associations between Job Positions and security-related questions

The table below represents associations between job positions and various security related questions. We can see that almost all questions do not offer any kind of association, meaning that regardless of job position the same steps seem to have been taken for extra security, with the majority of respondents answering negatively about Additional Security (56%), IT Inspection of their smartphone (89%), using Extra Encryption (77%). But we can see a difference in job position and their access to company resources, such as servers, with High Officials navigating more freely than other employees. Therefore, we can observe that while High Officials have greater reach in company resources, they are neither implementing additional security steps, nor are aided by the IT department in terms of smartphone safety. The statistical result is opposed to every propose ENISA offered as High Employees are expected to be provided with better security measures, especially when the access to resources is high. This may pose a great threat to most organizations as the impact to High Employees can be severe. Most troubling fact is that the IT inspections is almost 90% negative which can lead to a great number of unattended smartphones, in terms of security, to organizations' infrastructure. Those smartphones can be found with unwanted applications, not updated or even jailbreaked. According to NIST such devices are considered immediately as untrustworthy and high risk devices and should denied access to various resources or sensitive data.

Table 5.5	Association between Job Position and Smartphone Security		
Question	χ^2	Degrees of freedom	p-value
Addition Security (e.g. VPN)	1.210	1	0.271
IT Inspection	0.521	1	0.470
Extra Encryption	1.130	2	0.568
Access to Resources (e.g. Servers)	4.861	1	0.027

Associations between Country of Origin and Security-related questions

The table below represents associations between countries of origin and various security related questions. We can see that only the usage of company-provided smartphones differs from country to country and so produces a statistically significant result. Specifically, we had 71% of respondents in Greece that used their company phones for personal use as well, while in the UK that was 17% and in the US no respondent used their company phone in a personal manner. As far the other 3 questions are concerned, we had similar results among the countries. This statistical result show that users from Greece are more susceptible to cyberattacks or pose as IOC to an infrastructure in contrast to other countries. The reason is due to users from Greece being more likely to use the provided smartphone for personal reason, a phishing attack or lack of users cybersecurity awareness can result to a successful attack. Finally, due to similar statistical results to the other questions, the impact of an attack can be more severe. For example, if the choice of a smartphone is based to a non-security oriented reason or the users' more increased access to resources or information can increase the chance of the risks of an attack to gain access more easily or in more severe resources.

Table 5.6	Association between Country of Origin and Security-related Questions		
Question	χ^2	Degrees of Freedom	p-value
Personal Use of Smartphone	8.191	2	0.017
Choice in Smartphone	2.745	2	0.250
Access to Resources	4.353	2	0.113
Access to Classified Information	1.455	2	0.488

In conclusion, we can observe that there seem to be weaker cybersecurity training practices in Greece, compared to the UK and the US. Also, when a smartphone was provided by the company, we observed that in Greece more users opted in choosing that smartphone in a personal manner, as opposed to respondents from the UK or the US. Moreover, across different job positions, most respondents answered negatively when it comes to extra security steps taken, such as IT smartphone inspection or Extra encryption, while the higher officials, as expected, had more accessibility to a company's resources, such as servers. This raises some concerns on whether the smartphones that have higher accessibility in a company's resources, are indeed used in a safe manner. All the results of this study, but especially the ones concerning the second team of respondents -- those that had been provided with a smartphone from their company – could be better explored in future with a larger sample size, as some important questions worthy of explorations arise which are related to whether/how is Cybersecurity familiarity associated with higher backup rates, faster lock times or more authentication methods.

7. Conclusions and final remarks

The results of this survey suggest that there is still room for improvement regarding cybersecurity smartphone awareness in the workplace. Overall, users and organizations are increasingly adopting a sense of cyber security in comparison to the previous works revised in the previous chapter. This progress is evidenced when the users in this study refer to basic security control methods, for example authentication methods and strong sense of protection for sensitive applications and data.

Nevertheless, the survey results showed that organizations are still not adequately prepared or mature to allow the use of smartphones in the way a regular device is used.

BYOD devices are more likely to be chosen than organization issued as they are less costly and more popular. Organizations should take measures allowing to deal with the vast number of devices that introduced every year and should keep up with their missions.

Additionally, organizations are encouraged to follow NIST's guidelines as the ENISA set of guidelines is not renewed and improved since the date that was published. NIST proposes organization Mobility Management (EMM) systems to be installed in the environment which can help the control of devices that enter the organizations infrastructure in addition to pre configuring organization-issued smartphones.

Considering that EMM policy is a set of rules that defines what a user is allowed (or not allowed) to do on their smartphone and the smartphone's configuration requirements, EMM policies are put in place to assist in securing the enterprise data within the smartphones. In doing so, the organization must understand the type of data the user handles (according to the organization mission) as well as the risks and the proper mitigations from accidental or intentional threats. Upon understanding these key factors, the organization can design proper EMM policies and deploy them.

Finally, the survey revealed many unsure answers within organizations, responses where the user was not sure about the existence of various features such as security measure. In order for users to understand properly how and why cybersecurity matters, organizations should educate them employing for example various mock tests that will allow users to familiarize and know proper procedures. Given that the use of smartphones in the workplace is growing rapidly this survey can lay grounds for future exploration. Automations and cloud-based infrastructure are evolving to a point where all guides mitigations can be deployed remotely and immediately. Vendors offer continuous monitoring of smartphone devices from cloud portals and educate users based on their behavior and alerts, helping IT departments and security officers. Although the question raised is how such automations can help with BYOD devices, where users

mix personal data with corporate, to separate false positives from true positives and how those smartphones can be trusted when found remotely. Finally, concerns may be raised due to IoT devices integration with smartphones regarding organizations' infrastructure security. However on thing is for sure, smartphones are the future of organizations and they can function as a tool to a point where they can even replace.

References

Alani, M. (2017). Android Users Privacy Awareness Survey, in *International Journal of Interactive Mobile Technologies (iJIM)* 11(3), 130-144.

Androulidakis, I., & Kandus, G. (2011). Mobile Phone Security Awareness and Practices of Students in Budapest. Published in ICDT 2011, The Sixth International Conference on Digital Telecommunications. Budapest 17-22 April 2011.

Barrere, M., Hurel, G., Badonnel, R. & Festor, O. (2012). Increasing Android Security using a Lightweight OVAL-based Vulnerability Assessment Framework, in *Automated Security Management*, 41-58.

Bitton, R., Finkelshtein, A., Sidi, L., Puzis, R., Rokach, L., & Shabtai, A. (2018). Taxonomy of Mobile users' security awareness, in *Computers and Security*, 73, 266-293.

Breitinger, F., Tully-Doyle, R., & Hassenfeldt, C. (2020). A survey on smartphone user's security choices, awareness and education, in *Computers & Security, Vol. 88*, January 2020.

Cherapau, I., Muslukhov, I., Asanka, N., & Beznosov, K. (2015). *On the Impact of Touch ID on iPhone Passcodes*. Presented in Eleventh Symposium on Usable Privacy and Security (SOUPS 2015), 257-276.

Chigona W., Robertson B., & Mimbi L. (2012). Synchronised smart phones: The collision of personal privacy and organisational data security, in *South African Journal of Business Management*, volume 43(2), 31-40. June 2012.

Cisco (2011). Cisco 2010 Annual Security Report.
http://www.cisco.com/en/US/prod/collateral/vpndevc/securityannualreport2010.pdf [Retrieved May 2020].

Franklin, J., Howell, G., Sritapan, V., Souppaya, M., & Scarfone, K. for NIST (2020). Guidelines for Managing the Security of Mobile Devices in the organization" Draft NIST Special Publication SP 800-124 Rev 2. March 2020.
https://csrc.nist.gov/publications/detail/sp/800-124/rev-2/draft?fbclid=IwAR0_sPE-9qWZBEQXGysRz0M_vTvRQgzH7SEV83xbRe9hE6XU4LhkqojBJLI [Retrieved May 2020].

Glisson, B., & Storer, T. (2013). Investigating Information Security Risks of Mobile Device Use within Organizations, published in AMCIS 2013.

Harris, M. A., Patten, K., & Regan, E. (2013). *The Need for BYOD Mobile Device Security Awareness and Training*. Presented in Americas Conference on Information Systems. Chicago, IL, United States 15-17 Aug 2013.

Hogben, G., & Dekker, M. (2010). Smartphones Information security risks, opportunities and recommendations for users, Dr. Giles Hogben and Dr. Marnix Dekker for ENISA December 10, 2010

https://www.enisa.europa.eu/publications/smartphones-information-security-risks-opportunities-and-recommendations-for-users [Retrieved May 2020].

INTERPOL, (2020). INTERPOL report shows alarming rate of cyberattacks during COVID-19, https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19, [Retrieved May 2021]

Kravets, A., Duong Bui, N., & Al-Ashval, M. (2014). Mobile Security Solution for Enterprise Network, in *Knowledge-Based Software Engineering*, 371-382.

La Polla, M., Martinelli, F., & Sgandurra, D. (2013). A Survey on Security for Mobile Devices in IEEE Communications Surveys & Tutorials, vol. 15, no. 1, pp. 446-471, First Quarter 2013.

Leavitt, N. (2011). Mobile Security: Finally a Serious Problem? , in *Computer, Vol: 44*, Issue: 6, June 2011, 11 - 14.

Leavitt, N. (2013). Today's Mobile Security Requires a New Approach, in TECHNOLOGY NEWS for in Computer, published by the IEEE Computer Society 2013.
http://www.leavcom.com/pdf/Mobilesecurity2.pdf [Retrieved May 2020]

Li, Q., & Clark, G. (2013). Mobile Security: A Look Ahead, in IEEE Security & Privacy, Volume 11, Issue 1. pp. 78-81, Jan.-Feb. 2013.

Markelj, B., & Bernik, I. (2012). To Use or Not to Use Mobile Devices, in Journal of Internet Technology and Secured Transactions (JITST), Volume 1(2), 34-41. June 2012.

Markelj, B., & Bernik, I. (2014). Safe use of mobile devices arises from knowing the threats, in Journal of Information Security and Applications Volume 20, 84-89.

McAfee Labs (2009). Mobile Security Report 2009.
http://www.mcafee.com/us/resources/reports/rp-mobile- security-2009.pdf [Retrieved May 2020].

MSI (2021). Mobile Security Index.
https://www.verizon.com/business/content/dam/resources/reports/2021/2021-msi-report.pdf [Retrieved May 2020].

PandaLabs (2011). Annual Report 2011.
http://press.pandasecurity.com/wp-content/uploads/2010/05/PandaLabs-Annual-Report-2010.pdf [Retrieved May 2020].

Parker, F., Ophoff, J., Van Belle, J., & Karia, R. (2015). Security awareness and adoption of security controls by smartphone users, 2015 *Second International Conference on Information Security and Cyber Forensics (InfoSec),* 2015, pp. 99-104.

Appendix

*Open text

Complete Questionnaire

A. General Questions

1. What is your country of residence?*

2. What range of Age you fall under?
   (1) 18 - 23
   (2) 24 - 30
   (3) 31 - 40
   (4) 41 - 50
   (5) 51 - 60
   (6) Over 60
   (7) I prefer not to say

3. How do you identify?
   (1) Male
   (2) Female
   (3) Prefer not to say
   (4) Other

4. What is your level of education?
   (1) High School Graduate
   (2) Bachelor's Degree
   (3) Master's Degree
   (4) Doctoral Degree
   (5) Other*

5. What industry are you working in?
   (1) Accommodation/Hospitality and Food/Beverage Services
   (2) Agriculture, Forestry, Fishing, Mining, Quarrying
   (3) Building and Other Support Services
   (4) Business, Finance, Legal, Insurance and Consulting Services
   (5) Culture, Recreation and Entertainment/Media
   (6) Educational Services
   (7) Energy/Utilities
   (8) Healthcare and Social Assistance
   (9) Information Technologies Services
   (10) Logistics, Maritime and Warehousing
   (11) Manufacturing and Engineering
   (12) Public administration/Government
   (13) Real Estate and Leasing Services
   (14) Retail/Trade
   (15) Telecommunications
   (16) Other

6. Do you use your smartphone for work-related actions?
   (1) Yes
   (2) No, I use a company provided smartphone

B. Bring Your Own Device Questions

1. What is your job position?
   (1) Employee
   (2) High Official

2. What kind of operating system (OS) does your smartphone use?
   (1) Android
   (2) iOS
   (3) Blackberry
   (4) Windows
   (5) Other*

3. Which model of smartphone do you have?*

4. What kind of Authentication Method(s) do you use?
   More than one answer available.
   (1) Password-based
   (2) Pattern Lock
   (3) PIN Number
   (4) Fingerprint Scanner
   (5) Facial Recognition/Iris Scanning/Intelligent Scan
   (6) Smart Lock - Other Security measure (example: Smart Watch)
   (7) Other*

5. Do you use Two-factor Authentication? (example: PIN and Biometrics)
   (1) Yes
   (2) No

6. What is your smartphone's auto-lock time?
   (1) Never
   (2) 0 - 1 min
   (3) 1 - 2 min
   (4) 3 - 5 min
   (5) 5 - 10 min
   (6) 15 + min
   (7) Not sure

7. Do you leave one of the following settings enabled when leaving your home/work network?
   More than one answer available.
   (1) GPS
   (2) Wi-Fi
   (3) Bluetooth
   (4) No

8. Do you use tethering for work related issues? (roaming/mobile data)
   (1) Yes
   (2) No

9. Do you have sensitive applications in your smartphone? (example: Wallets)
   (1) Yes
   (2) No

10. If you answered yes to question 9, are these applications locked separately from the method of unlocking your smartphone?
    (1) Yes
    (2) No

11. Do you inspect the permissions that an application

needs from another application?
(example: Contacts)
(1) Yes
(2) No

12. Do you inspect the permissions that an application needs? (example: Microphone)
    (1) Yes
    (2) No

13. Do you have access to classified/sensitive work-related data with your smartphone?
    (1) Yes
    (2) No

14. Do you use additional security applications (example: VPN , Virus Scanner)
    (1) Yes
    (2) No

15. Did you unlock your smartphone administration privileges (jail-breaking/rooting)?
    (1) Yes
    (2) No
    (3) Not sure

16. Does your smartphone install security policies when connected to your organization's network?
    (1) Yes
    (2) No
    (3) Not sure

17. Has your smartphone ever been inspected by the IT department at your work?
    (1) Yes
    (2) No

18. How often do you backup your smartphone?
    (1) Never
    (2) Once a day
    (3) Once a week
    (4) Once a month
    (5) When prompted by my device
    (6) Other*

19. If you answered positive to question 18, when you backup your data, is this usually done with a cloud system?
    (1) Yes
    (2) No
    (3) Not sure

20. Do you install applications from other sources than the App-Stores?
    (1) Yes
    (2) No
    (3) Not sure

21. Do you update your applications automatically?
    (1) Yes
    (2) No
    (3) Not sure

22. Does your smartphone interact with other devices? (example: PC)
    (1) Yes
    (2) No

23. Does your smartphone store data to removable media? (example: Memory Cards)
    (1) Yes

(2) No
(3) Not sure

24. Do you use extra encryption for your files?
(1) Yes
(2) No
(3) Not sure

25. Do you have access to the organization's resources with your smartphone?
(example: Servers)
(1) Yes
(2) No

26. If you answered yes to question 25, is the access to those resources limited?
(1) Yes
(2) No
(3) Not sure

27. If you lose your smartphone, can you remote wipe the data?
(1) Yes
(2) No

28. Have you ever informed the IT department about the loss of your smartphone?
(1) Yes
(2) No

29. Does your smartphone wipe the data if many authentication tries were unsuccessful?
(1) Yes
(2) No
(3) Not sure

30. Do you wipe your old's smartphone data?
(1) Yes
(2) No

31. Do you travel with that smartphone?
(1) Yes
(2) No

C. Organization-Issued Smartphone Questions

1. What is your job position?
(1) Employee
(2) High Official
2. Is the smartphone used for personal use?
(1) Yes
(2) Yes, in a limited way. (Personal data are saved separately by corporate data)
(3) No

3. What kind of operating system does your provided smartphone have?
(1) Android
(2) iOS
(3) Blackberry
(4) Windows
(5) Other*

4. Which model of smartphone have you been provided with?*

5. Did you have the opportunity to choose between different options of smartphones?
(1) Yes

(2) No

6. If you answered yes to question 5, what was the criteria?
   More than one answer available.
   (1) Branding
   (2) Hardware Capabilities
   (3) Security features
   (4) Easy to use for work
   (5) Other*

7. What kind of Authentication Method(s) do you use in the provided smartphone?
   More than one answer available.
   (1) Password-based
   (2) Pattern Lock
   (3) PIN Number
   (4) Fingerprint Scanner
   (5) Facial Recognition/Iris Scanning/Intelligent Scan
   (6) Smart Lock - Other Security measure (example: Smart Watch)
   (7) Other*

8. Was the Authentication Method chosen by you or was it presetted?
   (1) By me
   (2) Pre-sett

9. Do you have access to the following settings of your smartphone?
   (1) Wi-Fi
   (2) Camera
   (3) Microphone
   (4) Bluetooth
   (5) Tethering (roaming/mobile data)
   (6) Scans QR codes
   (7) No

10. Do you have access to the organization's resources with your smartphone? (example: Servers)
    (1) Yes
    (2) No

11. If you answered yes to question 10, is the access in those resources limited?
    (1) Yes
    (2) No
    (3) Not sure

12. Do you have access to classified/sensitive work-related data with your smartphone?
    (1) Yes
    (2) No

13. Does your IT department enforce security policies or lock permissions in your provided smartphone?
    (1) Yes
    (2) No
    (3) Not sure

14. Can you change the permissions of an application?
    (1) Yes
    (2) No
    (3) Not sure

15. Does your smartphone lock automatically?
    (1) Yes
    (2) No

16. What is your smartphone's auto-lock time?
    (1) Never

(2) 0 - 1 min
(3) 1 - 2 min
(4) 3 - 5 min
(5) 5 - 10 min
(6) 15 + min
(7) Not sure

17. Does your provided smartphone turn off automatically one of the following settings if not used for a long time?
(1) GPS
(2) Wi-Fi
(3) Bluetooth
(4) Tethering (roaming/mobile data)
(5) No

18. How often does your smartphone backup?
(1) Never
(2) Once a day
(3) Once a week
(4) Once a month
(5) When prompted by my device
(6) Other*

19. If you answered positive to question 18, when you backup your data, is this usually done with a cloud system?
(1) Yes
(2) No
(3) Not sure

20. Are you allowed to install applications on your own or are you limited? (example: Blacklists, Whitelists)
(1) Yes
(2) No
(3) Not sure

21. If an unwanted application is installed does the IT department remove it? (policy violation)
(1) Yes
(2) No
(3) Not sure

22. If you answered yes to question 21, do you get notified?
(1) Yes (example: SMS, Push notification, Email)
(2) No
(3) Not sure

23. Does your provided smartphone update automatically?
(1) Yes
(2) No
(3) Not sure

24. Does your IT department pre-install additional security applications? (example: VPN, Virus scanner)
(1) Yes
(2) No
(3) Not sure

25. If your smartphone gets infected (example: Malware), are you informed by the IT department?
(1) Yes
(2) No
(3) Not sure

26. Can your smartphone interact with other devices? (example: PC)
(1) Yes

(2) No
(3) Not sure

27. Does your smartphone store data to removable media? (example: Memory Cards)
(1) Yes
(2) No
(3) Not sure

28. Do you use extra encryption for your files?
(1) Yes
(2) No
(3) Not sure

29. Did you ever inform the IT department after losing your smartphone?
(1) Yes
(2) No

30. Does your smartphone wipe the data if many authentication tries were unsuccessful?
(1) Yes
(2) No
(3) Not sure

31. Do you travel with that smartphone?
(1) Yes
(2) No

D. Awareness Questions

1. How familiar are you with cybersecurity?
(1) I have no knowledge of related topics
(2) I follow the news of related topics
(3) I have read/taught myself about related topics
(4) I have taken one or more courses in a related topic
(5) I have a degree in this or a related field

2. Have you ever received training for cybersecurity threats? (example: Phishing Mails)
(1) Yes
(2) No

3. Have you ever received training from any organization about security matters for your smartphone?
(1) Yes
(2) No