Risk Analysis of BYOD in Afghanistan's Organization

Islahuddin Jalal, Hashmatullah Rasekh, Qudrattullah Omerkhel, Qamaruddin Shamsi

Abstract*: *Improving ICT management strategies is an ongoing need for almost all organizations. At the same time, the challenges that BYOD brings to the organization need to be carefully considered. BYOD terminology can refer to related concepts, technologies, and strategies that enable employees to use organizational resources. The use of different databases, applications, and personal devices such as smartphones, laptops, tablets, and any other mobile device such as memory chips and external hard drives can provide examples of these resources. The implementation of BYOD has brought a clear advantage to the organization. However, the use of BYOD in organizations can pose some risks and threats. The main purpose of this study was to analyze BYOD risks in Afghan organizations through cross-sectional quantitative research methods. An online survey of 24 questions was conducted on various aspects of BYOD risk from various organizations in Afghanistan. Through the use of raw data, survey results related to BYOD implementation in Afghanistan have been collected. Thus, the researchers found out that IT staffs have a low level of awareness of the risks and challenges of BYOD security and the latest technologies used by Afghan organizations. Finally, recommendations have been made.

Keywords : Risk Analysis, Bring Your Own Device (BYOD), Cyber Security, Information Security.

I. INTRODUCTION

Today, BYOD (Bring Your Own Device) has become a mandatory factor for every organization to provide better flexibility to employees, due to work and technical requirements while providing employees with different methods and better flexibility through mobile devices. In recent years, the field of IT BYOD has made tremendous progress (French, Guo, & Shim, 2014). Of course, most organizations have implemented and switched to this new technology. BYOD lays the foundation for employees to use and bring their own computing devices (such as laptops, smartphones, tablets, storage devices, etc.) to the organization and connect to the network without using the equipment owned by the organization (Koh, Oh, & Im, 2014).

However, security threats in the BYOD paradigm provide an opportunity for hackers or attackers to find new attacks or vulnerabilities that could exploit employees 'mobile devices and gain important organizational information. It has been proven (Mahinderjit Singh, Wai, & Zulkefli, 2017) that basic security and privacy knowledge and knowledge of mobile devices or applications are crucial to protecting their mobile devices and protecting organizational data.

Afghanistan is a country that uses information and communication technology, which is spreading rapidly, and ICT plays an important role in all aspects of our lives (Republic, 2014). However, Afghan organizations do not have ICT security policies for consumer equipment, and IT staff within these organizations have a low level of understanding of BYOD risk and security, which is a big problem. This will pave the way for cyber security vulnerabilities and gaps across Afghan organizations.

While there are many concerns about BYOD security risks in many organizations in Afghanistan, BYOD has provided significant benefits to workers in recent years, and most employees are satisfied with BYOD. However, identifying BYOD-related security risks and finding the most appropriate solution to reduce these risks poses challenges.

To determine the security risks associated with BYOD in different organizations in Afghanistan, it is necessary to review the ICT department of this organization to understand the existing measures or policies regarding BYOD.

The purpose of this study was to analyze the organizations implementing and disseminating BYOD in Afghanistan to establish strong security mechanisms to reduce BYOD-related risks. This will help Afghan organizations formulate (1) various moving strategies, (2) defense mechanisms, (3) aspects of control, and (4) management and governance to implement BYOD strategies

II. CONCEPT AND DEFINITION OF BYOD

According to (Koh et al., 2014) and (Ogie, 2016), BYOD means a group of integrated technologies and strategies, where employees can connect to organizational networks and access internal resources through internal devices, such as online databases or applications such as Steam memory USB smartphones, laptops and tablets, memory cards and portable hard drives. In addition, according to (Arregui, Maynard, & Ahmad, 2016), there are many definitions to determine the concept and meaning of BYOD.

Revised Manuscript Received on September 25, 2020.

***** Correspondence Author

Islahuddin Jalal*, Lecturer, Department of Information Technology, Shaheed Rabbani Education University, Kabul, Afghanistan. Email: islahuddinjalal@yahoo.com

Hashmatullah Rasekh, Student, Department of Information Technology, Bakhtar University, Kabul, Afghanistan. Email: hashmat.rasekh@gmail.com

Qudratullah Omerkehl, Lecturer, Department of Information System, Shaheed Rabbani Education University, Kabul, Afghanistan.. Email: qudrattulah2014@gmail.com

Qamaruddin Shamsi, Lecturer, Department of Information Technology, Shaheed Rabbani Education University, Kabul, Afghanistan. Email: qamaruddinshamsi@gmail.com

The definition states that BYOD can be Electronic and mobile communication devices or portable storage media (USB memory sticks, memory cards, portable hard drives, floppy disks) and media with the following features:

- Users can use this device for knowledge work.
- It is owned by individuals and not purchased by organizations.
- Equipment should be portable.
- May install third-party software applications on the device.
- The device must be able to connect via one of the wireless network interfaces, mobile phone networks (2G, 3G, 4G and 5G)
- The device has Wi-Fi or Bluetooth.

Many professionals carry or have more than one type of mobile device in their pocket: one for business use, and another for personal use. Some have more than one for another reason. All of these devices have passwords, settings, data sets, configurations, and more. These various devices with different configurations and operating systems will bring complexity and confusion to users and system companies. Nowadays, wireless technology has become part of everyone's daily communication, and most organizations provide convenience to its members by providing a structure that allows them to use their own devices to connect and use the organization's network resources.

III. RELATED WORK ON BYOD

For organizations, there are security concerns that allow the use of customer devices called third-party control technologies beyond the control of the organization. This includes equipment operated by contractors, business partners, and suppliers, as well as individual computers, smartphones, and tablets (BYOD) of individuals, contractors, business partners, and suppliers. While organizations may reach agreements with employees and third parties that require employees and third-party devices to be properly protected, these agreements are often not enforced automatically, so unsafe devices, infected with malware and / or affected, can eventually connect Sources of sensitive organizations (Souppaya & Scarfone, 2016). Today, Bring Your Own Device (BYOD) has become one of the most popular models for every organization to provide mobility and flexibility in the workplace. The advent of new technologies and the capabilities of mobile devices have made them an integral part of all aspects of daily business activities. Moreover, mobile networks are now well integrated with the Internet (such as 3G, 4G, and LTE technologies). Thus, in BYOD, personal devices (i.e., mobile devices) can be used to increase employee satisfaction and reduce the cost of organizational equipment. Compared to computers and computer networks, mobile devices are not well protected, and users pay less attention to updates and security solutions. Thus, when employees use their own mobile devices to access organizational data and systems, mobile security has become a major issue in BYOD (Eslahi, Naseri, Hashim, Tahir, & Saad, 2014). According to Disterer and Kleiner (Disterer & Kleiner, 2013), BYOD is the most significant and serious safety risk. The confidentiality, integrity and authenticity of company data is threatened. When unauthorized parties access sensitive personal information or confidential company information by manipulating the device or intercepting data transmission, confidentiality is compromised. Operations performed using devices with insufficient security threaten the integrity of company data. When a device is used to trigger a business transaction that cannot be clearly detected, its authenticity is threatened. If a mobile device is set up for personal and commercial BYOD access ("double use"), while the company accesses company data, it must also protect the end user's personal data (contacts, addresses, photos, documents) to prevent company access from being guaranteed. Lack of separation between the private sector and the commercial sector poses a significant risk to the company.

According to this work (Arregui et al., 2016), information related to the organization will be compromised by the installation and use of malware. In this case, each organization should use a policy statement to address this risk, and it is only recommended to download the application from a trusted source. During the application installation process, users will grant permissions (such as allowing push notifications or location-based services), as they will benefit, so security considerations are set aside. Also, in the academic environment, most students use social media or social applications such as Facebook, Twitter, and YouTube. However, this can lead to the hosting and spread of malware and viruses such as Wildfire in students' personal devices (Mahinderjit Singh et al., 2017). According to (Fuentes, Álvarez, Ortega, Gonzalez-Abril, & Velasco, 2010) practical examples on mobile devices, how Trojan horses can steal information from mobile devices without the knowledge of the user. Malicious users can access user contact information through a pre-installed Trojan. In addition, common mobile malware attacks such as Dream Droid (Mahinderjit Singh et al., 2017) entice users to click malicious web links on their smartphone web clients and install malware. In addition, BYOD is easily attacked by hackers, thereby sending malicious software via email downloads or applications, thus attacking someone's device. As a result, once a student downloads and implements malicious software, the likelihood of a student's personal information leak increases, and the attacker installs a back door to destroy sensitive information capabilities. Some mobile users intentionally turn off native OS security features through techniques commonly referred to as "jailbreaking" or "rooting". By jailbreaking or rooting on their mobile devices, they can install or upgrade restricted operating systems and mobile applications by default for free. However, jailbreaking or rooting can install unauthorized programs on mobile devices, which may introduce malware to their devices. This can make the user device vulnerable to threats. Mobile devices can be used in safe a d unsafe environments. When users connect their device to an unsecured network (such as public Wi-Fi), the device will be turned on to receive various security and privacy attacks, such as Wi-Fi hijacking, Bluejacking, etc.

For example, when hackers attack, Wi-Fi hijacking can intercept communication between smartphones and insecure Wi-Fi coverage. If a user logs in to a specific mobile application or website, hackers can use the visitor to access the username Password. Implementing BYOD in an organization not only provides employees with a broader endpoint to access organizational resources, but also enables the dissemination of unauthorized sensitive information, thus revealing data (Arregui et al., 2016). If data is copied to a mobile device, control is difficult to perform. Sensitive information such as customer data is usually limited to a small number of users in the organization, however, using personal devices can easily copy that information and make employees inadvertently go beyond organizational security when they need electronic corporate resources to complete tasks. This operation is considered an abuse of harmless organizational resources. In general, employees typically do not intentionally affect the security of an organization’s information, but their actions can reveal confidential organizational information. Organizations must consider BYOD risks and determine which services and applications can be accessed from personal devices such as email, calendars, contacts, and electronic documents. Because BYOD is adopted in a work environment, which allows employees to bring their personal devices to the office, there is a risk of losing employee personal data due to the easy loss or theft of BYOD devices. Later, most people store a lot of sensitive personal and company information on mobile devices. There are some facts about the loss or theft of mobile devices.About 1.3 million mobile phones are stolen annually in the UK (SYBASE, 2013). Thus, lost devices cause a lot of data loss. While large amounts of data are lost through stolen devices, in fact no action is taken to protect company information or customer data on personal devices. Thus, a lost or stolen mobile device is a major attack and affects BYOD security. In BYOD terminology, the privacy aspect always refers to personal data (such as personal emails, photos, videos, bank statements, social security numbers, chat notes, usernames, passwords, and other evidence) that are exposed to the attention of outsiders. In addition, device location tracking issues are also one of the serious privacy issues in the BYOD context (Mahinderjit Singh et al., 2017). While location tracking through mobile device location services or GPS is useful for locating lost devices, illegal tracking can cause serious privacy issues for mobile users. Since the location of the user has been recorded, mobile device tracking or location monitoring can pose a threat to the user, and potential criminals will monitor the target user (Mahinderjit Singh et al., 2017). Nowadays, many legitimate or third-party mobile applications provide not only device tracking functions, but also device tracking functions. This also allows tracking of mobile usage behavior through installed applications. This means that the installed application makes it possible to track selected events that occur on the mobile device and record every action performed by the mobile user. If a user installs various third-party applications, this can pose another privacy threat to the user (Mahinderjit Singh et al., 2017).

Malicious software (Malware) is called a computer program with malicious code, which is programmed to intentionally destroy and / or disrupt the normal functioning of other software, make botnets move, collect information and data from the host, destroy data, etc. In terms of "malware", it can be identified as viruses, worms, spyware, Trojan horses, misleading applications, etc. (By Robert Moir, 2013). There are some software programmers in the world with malicious intent. They deliberately create malicious software to shut down mobile devices, so that malicious users can take control of mobile devices and even steal users' personal information to support storage on personal devices. Some malware includes spyware, Trojan horses and adware (Wu, Narang and Clarke, 2014). A type of malicious software called spyware. Spyware is a spy on computers, phones, and tablet systems. Spyware can collect information from a user's Web browsing history, such as SMS messages, emails, usernames and passwords, bill payments, and credit card information. If the information is not limited, spyware can transfer the information to other users via mobile devices. Now, how does spy software work on mobile devices? Spyware is similar to a virus or infection. When a user opens an SMS message link or email attachment with malicious software, a virus or infection may be installed. When the user installs another program that contains spyware in the installed program, another method that can install spyware into the mobile device. Because of the harmful behavior of spyware, most users do not even know when the spyware is on their mobile device. Trojan horses will steal users' personal information and open pop-up windows in advertisements to obtain personal information and data (Wu, Narang, & Clarke, 2014). Reducing the risk of BYOD is a way to protect an organization’s network from various threats posed by mobile devices and access channels. To reduce the risk of BYOD or mobile devices, use Mobile Security Reference Architecture (MSRA), VPN, Mobile Device Management (MDM) (Donaldson, Siegel, Williams, & Aslam, 2015), Mobile Application Management (MAM) (Eslahi et al., 2014), Identity Access Management (IAM) (Carroll, Rose, & Stritapan, 2013), Mobile App Store (MAS) and Data Loss Prevention (DLP) (Carroll et al., 2013) development encompasses all Management methods and risk control BYOD in a different way.

IV. METHODOLOGY OF THE STUDY

The main purpose and objective of this research is to find appropriate methods for organizations in Afghanistan to reduce and control BYOD-related risks.

To achieve the main purpose and objectives of this research, the researchers used cross-sectional quantitative data collection and analysis methods, including questionnaires with open and closed questions.

A. Data Collection

Primary data gathered through distribution of a simple web based questionnaire with 24 closed ended and open-ended questions to preselected target group of IT professional from different organizations in Afghanistan.

B. Questionnaire Reliability and Validity

The reliability and validity of the questionaries' is achieved through a pilot testing. The researcher targeted a group of five participants and distributed the questionnaire to them; consequently, after analyzing the responses, the main objectives and results of the study were achieved. Furthermore, to conduct a reliable and accurate survey acquire valuable data, several sessions and meetings were held with IT experts of different organizations. These efforts had considerable impacts on the reliability and validity of the study.

C. Research Design

The research objectives, research questions, research methodology and questionnaire were developed which are discussed earlier. The secondary data gathered from different sources (such as official statements, papers submitted, Books, and journals). In addition to above, for collecting primary data, an online survey with 24 questions conducted and the data analyzed by SPSS application. As the result of findings related to implementation of BYOD in Afghanistan, are collected and concrete recommendations and suggestions provided. The research process is shown in the following figure 1.

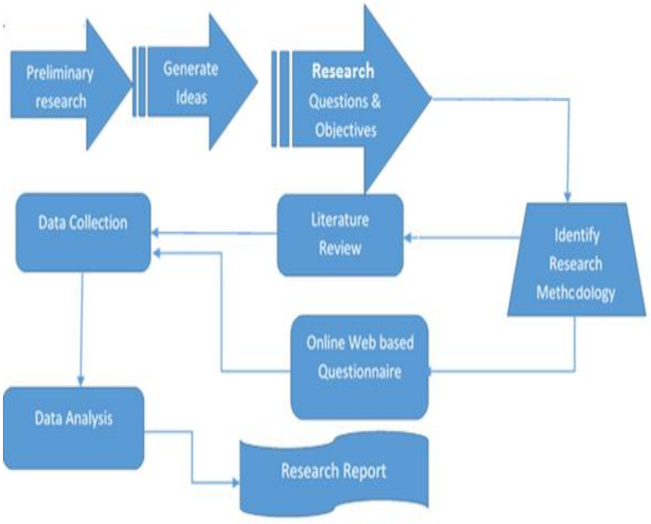


Fig. 1. Research Design

V. ANALYSIS AND RESULT

A. Type of Organization in This Study

The result of the survey provides information about the types of organizations where respondents are working. As per below figure, two-fourth of the respondents are working with governmental organizations, however the remaining respondents are belong to national both non-governmental and private sector and international organizations.

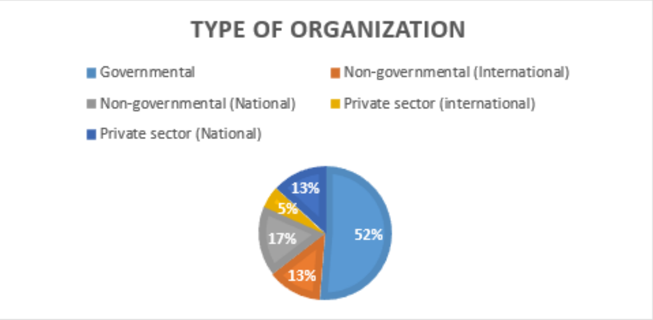


Fig. 2. Type of Organization

B. BYOD Management Personnel

This section provides information on whether different organizations in Afghanistan hire specific staff for BYOD management or not. The purpose of this result is to understand how organizations consider the advantages and disadvantages of having a dedicated staff for BYOD issues.

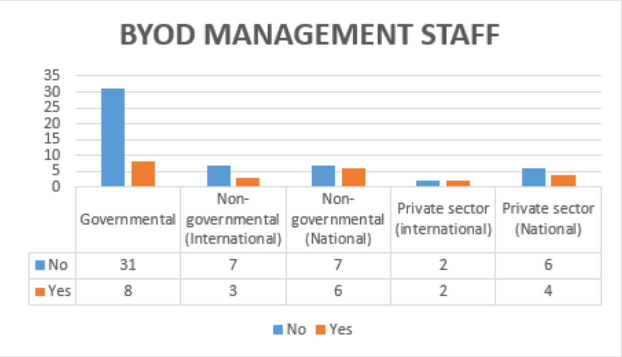


Fig. 3. BYOD Management Staff

Figure 3 shows that most of the organizations, particularly, governmental, non-governmental, and private sectors have not hired a dedicated person to look over BYOD management and security issues. In illustration, two thirds of the respondents have reported that their organizations lack a specific employee for BYOD. That is to say, two thirds of survey participants from governmental and non-governmental (international) organizations reported that there is no specific staff for BYOD issues in their organizations. The result further shows that nearly half of non-governmental (national) and half of private sectors (international) organizations recruited dedicated staff for BYOD. Most seriously, private sectors (national) generally do not hire a dedicated staff for BYOD. Overall, lack of deep understanding on advantages and disadvantages of BYOD, inadequate knowledge about the risks with BYOD, and budget issues in many organizations tend to be the main reasons behind not hiring a dedicated person to deal with BYOD related issues.

C. Awareness and Usage of BYOD

This part of research depicts the level of awareness of IT professionals in different organizations of Afghanistan, and it shows how much BYOD is being used in the workplaces in Afghanistan.

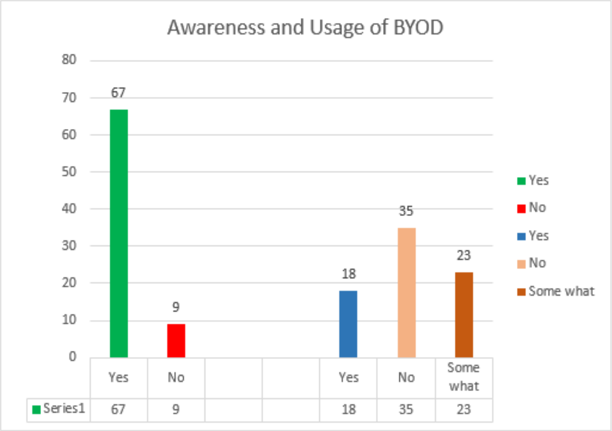


Fig. 4. Awareness and Usage of BYOD

The above graph outlines the result of awareness and use of BYOD in different organizations in Afghanistan. As it can be seen, despite huge use from BYOD, the level of understanding about advantages and risks of BYOD is considerably low. In illustration, more than three-fourths of the respondents answered that they use BYOD devices in their organizations; however the other side of the research shows that slightly over three-fourths of the same respondent replied that they either do not understand the concept and risks of BYOD or they have limited information about it. This finding highlights a concern point related to BYOD use in Afghanistan; to put it differently, majority of the IT professionals use BYOD without understanding the advantages and related risks and threats of BYOD to their organizations.

D. Data Breach Using BYOD in Afghanistan's Organization

This section shows the graph of data breach and leaking using BYOD in different organizations in the country.

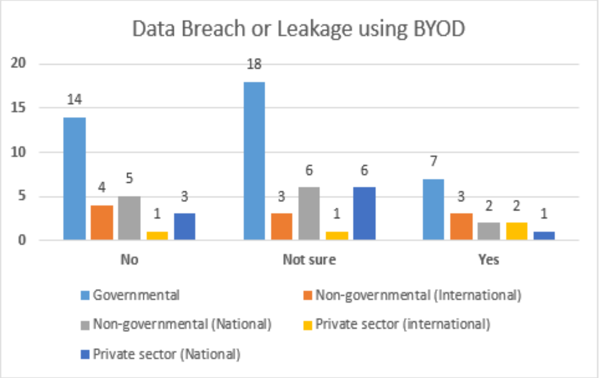


Fig. 5. Data Breach Using BYOD

The graph in the above reveals the extent of data breach in different organizations in Afghanistan while they use BYOD. The figure 5 depicts that most of the IT professionals who responded to the survey either do not know whether their systems are breached while they use BYOD or they have reported that their systems are exploited and data leaking happened. To elaborate, nearly half of the respondents have replied that they do not know whether the act of data breach or system exploitations have occurred or not, and one-fifths of them answered that the act of data leak and breach has happened in their networks while they use BYOD; however slightly above one-thirds of the respondents have responded that they have not faced any data leak and breach while their users use BYOD in the networks. This graph outlines that in many organizations proper infrastructure or controlling appliances are not being used to detect data breach and network exploitation. Also, those who replied that they are not sure whether system leaking happened or could be because of they do not realize and detect data breach incidents.

E. Existing BYOD Policy in Organizations

Obviously, not having corporate policies and standards in the organizations for BYOD is also a big challenge while organizations use BYOD. It is important to standardize and legalize system utilization using BYOD through policies and standards. In this respective, this survey has also paid efforts to examine whether organizations in the country hold policies and standards for BYOD or not.

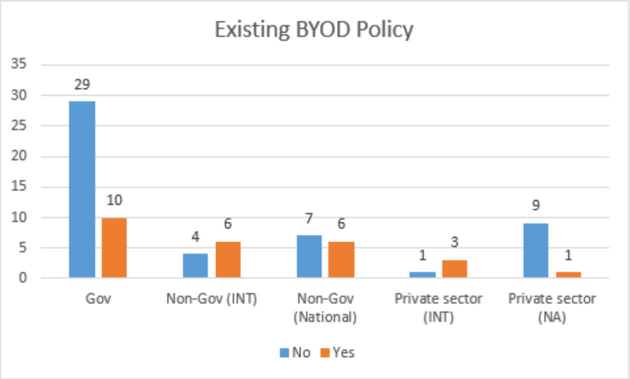


Fig. 6. Awareness and Usage of BYOD

The figure 6 shows which types of organizations consider corporate policy for BYOD, and at the same time it shows how much developing a corporate policy for the organizations are been ignored. As we can see, majority of the organizations prefer to have legal frameworks for BYOD through development of policies in their organizations. To illustrate, government organizations with almost three-fourths of positive responses have confirmed that they use policy for BYOD; nearly half of national and international non-government organization developed policies for BYOD; over two-thirds of national and international private sectors have replied that they have developed policies for their organizations. On the other hand, over one-fourth of government organizations, slightly over half of national and international non-government organization, and almost one-third of national and international private sectors have responded that they do not use any policy for BYOD in their organizations.

F. BYOD Devices Infected by Malware

To identify risks behind BYOD devices in the organizations, this report has also tried to evaluate and understand whether BYOD devices are infected by malicious applications or not. This section will help the readers to understand how much BYOD devices are susceptible to malwares.

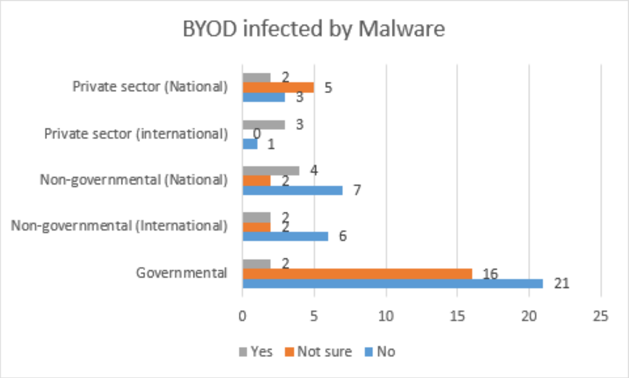


Fig. 7. BYOD Devices Infected by Malware

The figure 7 reveals which organization types have experienced malwares while they use BYOD. It is understandable from the table that many organizations have not faced with malwares in BYOD devices. To explain it further, over half of government organizations and national/international non-government organizations, and one-third of national and international private sectors are reported that they have not seen malware infection in the last 12 months. Nevertheless, below half of government and national/international organizations and two-thirds of national and international private sectors have responded that they have experienced unwanted applications and malwares with their BYOD devices.

G. Usage of Technology in Afghanistan's Organizations

In this section, the intention is to reflect data and information about the technologies and tools being used in different organizations in respects to manage and design defensive measures to the potential threats and attacks against BYOD devices. This will also help the readers to know about the technologies which organizations use, and recommend for improvement in the areas needed.

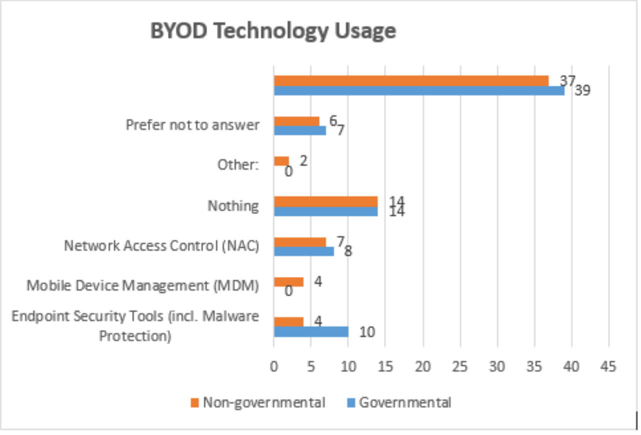
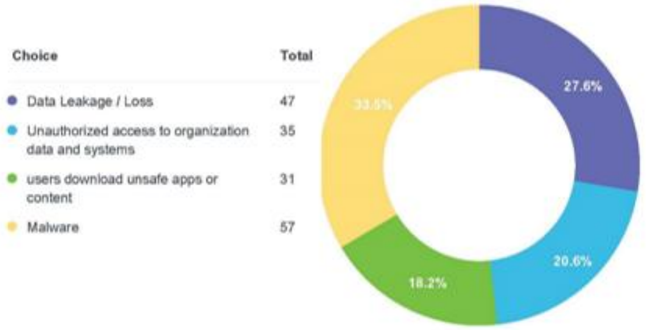


Fig. 8. BYOD Technology Usage

From the figure 14, it is clear that different organizations use different technologies and tools to manage and protect BYOD devices. According to the chart, majority of organizations seem use some tools or technologies for BYOD management and security. In other words, different technologies such as NAC, MDM, and endpoint security tools are being used in governmental and non-governmental organizations to manage and monitor BYODs in their organizations. As we can see, some respondents prefer not to indicate the technologies and tools they use for BYOD management. It is understandable that some organizations and IT professionals refrain to indicate their technologies for security reasons.

H. Technical Staff Concern about BYOD Security

Understanding the concerns and nervousness of IT professionals and organizations are important. Having deep knowledge about the concerns and issues being raised by BYOD users helps experts and technical people to design and improve technology to better respond to the threats and concerns exist against BYOD. Therefore, this section has gathered figures on how much people feel themselves nervous about BYOD and which areas are the biggest concerns.



Choice	Total
● Data Leakage / Loss	47
● Unauthorized access to organization data and systems	35
● users download unsafe apps or content	31
● Malware	57

Fig. 9. Concerns about BYOD Security

The figure 9 depicts the four major concerning areas related to BYOD. In light of the above chart, malware and data leakage or lost of data are the biggest concern of IT professionals in relation to BYOD. In explanation, one-thirds of IT professionals are concern of malware applications, over one-fourths of professionals are worried of data leakage and theft of information, slightly over one-fifths of IT professionals are anxious of unauthorized access to the system, and below one-fifths of them are worried of downloading unsafe and insecure applications by end user while they implement BYOD in their organization.

VI. RECOMMENDATIONS

The recommendations are suggested in the following table 1

Table- I: Recommendations

S/NO	OBJECTIVES	FINDINGS	RECOMMENDATIONS
1	To understand the level of awareness of IT personnel about BYOD in Afghanistan	• The level of awareness of IT personnel in Afghanistan about BYOD technology is very low. • Most of IT personnel working in different organizations do not know whether a data breach using BYOD happened in their organizations or not.	• Ministry of Information and Communication Technology (MoICT) must take initiative to develop a holistic and country wise strategy and policy for increasing and enhancing the awareness of IT personnel in different organizations about BYOD. • MoICT should provide regular trainings on BYOD, possible threats and data breach to all governmental and non-governmental organizations' personnel. • Every organization should nominate one focal point for BYOD trainings and these focal points should act as specific responsible body in their organizations in order to combat against data theft, data breach and disseminate information regarding different security issues. • Implement the required technologies for security of BYOD such as MDM, MAM, IAM, MAS, DLP, and IDS. • Should use the proven reference models for BYOD like MSRA reference model. • Every organization must implement BYOD in order to reduce cost and increase productivity due to off-site working from anywhere at any time.
2	To evaluate the handling of Cyber threats associated with BYOD	• Very few organizations in Afghanistan are using specific technologies for BYOD to handle cyber threats.	
3	To define a secure mechanism for BYOD being used in different organizations to mitigate the risk of BYOD	• Unfortunately, very few IT personnel think positively about BYOD. However, majority of them have largely expressed their concerns about BYOD implementations.	

VII. CONCLUSION

The purpose of this study was to understand the issues related to the implementation of BYOD in the context of the Afghanistan's organizations. In this study, the authors used cross-sectional methods of collecting and analyzing quantitative data, including questionnaires with open and closed-ended questions. The authors find that the implementation of BYOD will bring many benefits to the organization. However, after implementing BYOD in the organizations, there are many risks and challenges. Fortunately, the risks and challenges associated with BYOD discussed in this article can be overcome, and specific mitigation solutions and methods for it have been discussed in the research. In addition, we found that IT staff have a low level of awareness of the risks and challenges of BYOD security and the latest technologies used by Afghan organizations. Finally, this article summarizes the appropriate recommendations discussed in Table 1.

ACKNOWLEDGMENT

The Authors would like to thank *Higher Education Development Program (HEDP) of Afghanistan* for supporting this study financially.

REFERENCES

1. G. O. Young, "Synthetic structure of industrial plastics (Book style with paper title and editor)," in *Plastics*, 2nd ed. vol. 3, J. Peters, Ed. New York: McGraw-Hill, 1964, pp. 15–64.
2. W.-K. Chen, *Linear Networks and Systems* (Book style). Belmont, CA: Wadsworth, 1993, pp. 123–135.
3. H. Poor, *An Introduction to Signal Detection and Estimation*. New York: Springer-Verlag, 1985, ch. 4.
4. B. Smith, "An approach to graphs of linear forms (Unpublished work style)," unpublished.
5. E. H. Miller, "A note on reflector arrays (Periodical style—Accepted for publication)," *IEEE Trans. Antennas Propagat.*, to be published.
6. J. Wang, "Fundamentals of erbium-doped fiber amplifiers arrays (Periodical style—Submitted for publication)," *IEEE J. Quantum Electron.*, submitted for publication.
7. C. J. Kaufman, Rocky Mountain Research Lab., Boulder, CO, private communication, May 1995.
8. Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interfaces(Translation Journals style)," *IEEE Transl. J. Magn.Jpn.*, vol. 2, Aug. 1987, pp. 740–741 [*Dig. 9th Annu. Conf. Magnetics* Japan, 1982, p. 301].
9. M. Young, *The Techincal Writers Handbook.* Mill Valley, CA: University Science, 1989.
10. (Basic Book/Monograph Online Sources) J. K. Author. (year, month, day). *Title* (edition) [Type of medium]. Volume(issue). Available: http://www.(URL)
11. J. Jones. (1991, May 10). Networks (2nd ed.) [Online]. Available: http://www.atm.com
12. (Journal Online Sources style) K. Author. (year, month). Title. *Journal* [Type of medium]. Volume(issue), paging if given. Available: http://www.(URL) research work, membership, achievements, with photo that will be maximum 200-400 words.

AUTHORS PROFILE

Islahuddin Jalal received his BCS (Hons) degree from the University of Peshawar (UoP) Pakistan in 2012. In 2015, he received the Master degree in Cyber Security from FTSM faculty, Universiti Kebangsaan Malaysia (UKM), Malaysia. He is currently a PhD Scholar at the Universiti Kebansaan Malaysia (UKM) Malaysia and Lecturer in the department of information technology (IT), Computer science faculty at the Shaheed Rabbani Education University Kabul, Afghanistan. His research work area includes cyber security, blockchain technology, consensus algorithms, information security and cloud computing.

Hashmatullah Rasekh was born in 1981 in Parwan, Afghanistan. He received a master degree in Computer Science from Bakhtar University in 2018 and BCS degree in Computer Science from Kabul University, Afghanistan, in 2006. Mr Rasekh went through several industrial certifications, and he is a CCNA and MCSA certified. He is an IT expert with 12 years of experience with national and international organizations in Afghanistan.

Qudrattullah Omerkhel is a lecturer at Shaheed prof Rabani Education University Information system and education department faculty of computer science. He is currently a PhD Scholar at the University Technology Malaysia (UTM) Malaysia, he has received both bachelor and master degree BSc(CME), Master degree in Software Engineering from the University of Mysore India in 2012, 2014, respectively. His research interest area is Software Engineering, Software development, Requirement Engineering, Requirement analysis and Agile Methodologies.

Qamaruddin Shamsi is a lecturer and head of information technology (IT) department in Computer Science faculty at Shaheed Rabbani Education University Kabul, Afghanistan. He received his master degree from Sam Higginbottom Institute of Agriculture Technology and Science, Allahabad, UP, India in 2013. His research interest area is Network programming, Robotics and security as well as digital informatics.