ISSN 2350-1022

International Journal of Recent Research in Mathematics Computer Science and Information Technology
Vol. 9, Issue 2, pp: (80-91), Month: October 2022 – March 2023, Available at: www.paperpublications.org

An evaluation of BYOD integration cybersecurity concerns: A case study

David Njuguna[1], Wambui Kanyi[2]

[1,2]Mount Kenya University

[1,2]Kenya Technical Trainers College

DOI: https://doi.org/10.5281/zenodo.7704371

Published Date: 07-March-2023

Abstract: **Personal smartphones, tablets, and laptops have become increasingly popular in the workplace, posing new security challenges in firms where they have been connected with company devices. Bring Your Own Device (BYOD) is a prevalent practice whereby workers are permitted to work on their own devices rather than utilizing company-provided equipment. Because BYOD offers both advantages and disadvantages, its adoption in the workplace is a source of concern. Workers utilizing personal devices to conduct business face significant security hazards, whether they're merely transmitting job-related electronic mails or retrieving protected organization programs from their cellphones or tablets. This study investigated the cybersecurity concerns associated with BYOD integration in work places in Kenya focusing on a Non-governmental organization. The specific objectives of the study were; to investigate the level of awareness of BYOD security challenges, and to investigate the measures put in place to address cyber-security issues associated with BYOD. The results indicate that organizations need to create more awareness in regards to BYOD security since the level of awareness is low. The results also show that security measures related to BYOD has been neglected. It is also imperative that organizations put in place security measures that will ensure data integrity, confidentiality as well as availability.**

Keywords: **BYOD, Benefits, policies, malware, security, mobile devices.**

I. INTRODUCTION

Bring Your Own Device (BYOD) denotes a situation where workers connect to their firm's networks and access work-related systems as well as confidential or private data through personal devices such tablets, Smartphones, Personal Computers, and pen drives, [1]. BYOD also refers to various approaches such as Bring Your Own PC (BYOPC), Bring Your Own Technology (BYOT), Bring Your Own Phone (BYOP), according to [2]. These initiatives have evolved to equip workers and link them with the concept of information technology consumerization, in which personal-use hardware and software are integrated into the workplace. According to reports, firms spend a significant amount of their resources on mobile device provision. This is referred to be a corporate-owned, personally enabled strategy (COPE), [3], Use what you are told (UWYT), Here is your own device (HYOD)[4] or choose your own device (CYOD), [5]. Workers originally exclusively used devices provided by the employer to work. The ubiquity of tablets and smartphones has made workers carry them to work or connect to the firms' network. This indicates that a Worker's potential is greater, [6]. Whether or not personal gadgets are allowed by IT, they are likely to penetrate the workplace. BYOD enhances workers' throughput as well as the psyche. In many circumstances. BYOD poses a significant threat to a firm if they are not properly regulated by the I.T department. "Shadow IT" refers to devices that have not been certified by the company and pose a security risk. The security issue with these devices stems from their inability to be monitored or protected against malicious software and other security threats. As a result, a security policy is required to determine whether personal devices are permitted for usage at work, as well as when Workers should utilize company-provided devices, [7]. As new technologies and functionalities emerge, mobile devices have become essential components of every area of daily business operations.

Additionally, considering that mobile networks have become completely connected to the Internet, BYOD can be used to increase workers' contentment while reducing I.T infrastructure expenses. Mobile devices are not well safeguarded in comparison to computers and computer networks, and individuals give little thought to updates, patches. As a result, mobile safety is now a significant problem in BYOD as personnel utilize individual mobile devices for accessing the firm's information and applications, [8]. Many businesses have allowed staff to work remotely as a result of the COVID-19 outbreak. Workers now have access to organization information systems via their devices, posing a significant security risk to sensitive information in the event the device is stolen or shared with malevolent individuals, [9]. According to research, 95% of firms permit staff to utilize individual devices in the workplace. However, incidents of staff utilizing their devices at work, despite the BYOD policy, cannot be ignored. This shows that some staffs are using personal devices to access the company's I.T infrastructure and applications, regardless of the fact that this is against company policy,[6] (Brook 2020). Worker's frequently carry their devices to work since they own them and utilize them at work for entertainment. Workers preferring to use BYOD for work frequently do so without first obtaining permission from their boss, and in most situations, there's a lack of corporate regulations governing their use, [10]. Many firms, on the other hand, neglect safety concerns about possible breaches of personal information. For example, if a worker's device that bears valuable corporate data like trade secrets and electronic mail is, there is a danger that the information would be illegally leaked to the public. This might have a negative impact on the company's reputation and profits, [11]. According to studies, 74% of companies either now permit or plan to permit workers to take their own devices to work. As of 2016, 87 percent of enterprises relied on staff to access mobile business applications via their smartphones, while 45 percent of U.S. workers were obliged to use their smartphones for business purposes by their employers, [12]. The evolution of mobile devices with the ability to scan the QR code in some network devices to get the network login credentials and also share the network passwords has escalated the threat landscape in organizations. BYOD devices such as laptops that are connected to organization networks are used to share internet connection through mobile hotspots configured by users which compromise data confidentiality besides overloading network resources. The rest of the paper is organized as follows; section 2 deals with related literature, section 3 deals with methodology, and finally conclusion in section 4

II. RELATED LITERATURE

A. Benefits of BYOD

The utilization of personal gadgets at work has advantages for both the company and the Workers. BYOD has had a tremendous impact in enterprises, with data showing that approximately 80% of all organizations now enable BYOD personal devices, and another survey finding that 95% of Workers use at least one BYOD device for work tasks, [13]. BYOD merits include;

Worker Gratification

Workers find it easier to work from home or other locations when they don't have to swap gadgets, according to studies, [13]. Workers can also choose the technologies that best suit their tasks under the BYOD policy. As a result, Workers may be more satisfied working alongside technology rather than against it [14]. Workers have a tendency of taking good care of their devices better when a BYOD policy is established in a firm, since there is typically a larger feeling of individual ownership, leading to less cost of hardware and preservation. Thus workers are more efficient since they feel more comfortable working with equipment they are accustomed to. According to research, 64% of workers in international companies around the Australian and Asian territory revealed that their efficiency had risen as a result of convenience and user-friendliness by incorporating individual devices for official purposes, which led to increased worker's contentment, [15].

Cost saving:

For most businesses, cost-cutting is a top priority. When a BYOD policy is implemented, costs are shifted from employers to workers, resulting in cost savings. According to [5] firms have transitioned to a BYOD culture since the drop in hardware investment results in significant cost savings. The owners, not the corporation, are responsible for the expense of gadget servicing, upgrade, or restoration. BYOD allows an organization to transfer the price of desktop hardware to its workers. Personnel also has a resilient urge to upgrade their devices swiftly, hastening the implementation of cutting-edge technologies, [16].

Increased Productivity and Innovation:

There is indeed a link between workers' satisfaction and subsequent effectiveness. Personnel becomes accustomed to and understand their devices when they have their own. Individual's devices often have the latest innovations, making them valuable to the business. Furthermore, the hardware is very likely to be upgraded on a regular basis, [13].

As per Cisco's recent statistics, an increasing number of companies are implementing a BYOD policy, with 95 percent of the firms letting workers use personal gadgets to work [14]. Staff who work from home are more likely to work outside of business hours, which allows them to handle basic assigned functions, leading to more efficiency. Workers currently are more technologically aware unlike before, therefore BYOD has become a popular option among them. Mobile firms can boost worker productivity by allowing workers to access data in real-time in diverse scenarios and by speedier allocation of necessary communication possibilities, according to [17]. Personnel who are using individual devices for professional and individual purposes added 240 additional operating hours as opposed to those who didn't according to a survey, [18].

Accessibility to data

Workers can now retrieve corporate data without being tied to a specific place thanks to BYOD mobile devices. Effective communication and data accessibility enable businesses to better their goods and services while also increasing customers' worth, [16]. BYOD promotes business growth by allowing workers to use their devices to join the firm's network at any time, [15]. Real-time communication improves operational efficiency by providing an unequalled level of connectedness between Workers and the office.

B. Security Concerns of BYOD

Many firms, according to [19], do not take the essential steps despite the knowledge that there is a high risk of organizational security vulnerabilities being exposed. According to research, more than half of organizations do not have the capability to remotely wipe a device if it is lost or stolen, and 28% were not aware that the organization can remotely clean their device. Most staff had no idea what to do if their gadget was lost or stolen, or who to call in the event that it was. Indeed, 15% indicated they could inform their network operators, while 29% said that they could inform their employer. As Workers use their devices to work, organizations must do more to protect their vital I.T infrastructures. BYOD related to privacy and safety vulnerabilities, according to research, are caused by technical hazards, a dearth of policies, a limitation of protection measures, a dearth of safety knowledge, and inadequate privacy. Technical perils were identified as malicious applications, phishing, hacking, spoofing, network attacks, device loss or theft, and social engineering attacks, [20].

Data loss

BYOD increases the danger of data theft to new levels, and the temptation to provide the much-desired capability of access from anywhere frequently outstrips an organization's ability to successfully safeguard the underlying data, [21]. Data loss as a result of device theft or loss either in or out of the firm is one of the most serious concerns associated with BYOD. The size of smartphones makes them simple to drop or misplace due to their simplicity and comfort, [16]. According to [22], with over 6 billion smartphones in use worldwide in 2022, these devices have become appealing targets for criminals due to their high value and compact size. Furthermore, research indicates that secret and delicate data is passed on to unsanctioned individuals when Workers replace their mobile phones or vend the devices they've been using, [15]. According to experts, the number one risk is lost or stolen BYODs, since data is lost at critical periods, preventing them from gaining an edge over their competitors. Another important aspect of BYOD-related data leakage is the challenge of spotting the leaking in good time. This precludes the potential of initiating countermeasures to lessen the effect, which could be viable early in the diagnosis process. This crisis is exacerbated when workers who do not comprehend technology utilize their devices to manage corporate data, as they are unaware of the weaknesses, [15].

No uniform end-user support:

Challenges will indeed emerge, regardless of the situation or environment. Because the majority of the workers would be working on different types of devices, there isn't really a universal support mechanism in place for any problems that emerge with BYOD. It is critical to comprehend and be cognizant of something like this, [2].

Security

Presently, safety is a concern throughout all technologies, and a BYOD policy is no exception, but overcoming this barrier is not difficult. All that is required is that the IT departments be ready. To keep the job tasks and apps distinct from personal information, a person will require to install strong passwords and antivirus software, [2].

Installation of harmful software

Security profiles for devices that are centrally managed by an enterprise must fulfil tougher standards, therefore they are often kept secure. This implies that these gadgets are in a more controlled setting and are less vulnerable to abuse. Worker personal devices, on the other hand, may or may not conform to regulations and standards, resulting in unmanageable susceptibilities. Compromised devices that are connected to a firm's network, expose new safety weaknesses that can be exploited throughout the entire network, [10].

According to research, more than 20 million malware samples were found in 2017, [23]. Ransomware and malicious files exploiting flaws in job-related programs and procedures persisted in the second half of 2020, according to McAfee research, and continue to cause significant dangers with the ability to seize networks and data and costing millions of dollars in assets and restoration overheads, [23]. In the third quarter of 2020, the proportion of malicious files threats discovered by McAfee ATR averaged 588 per minute, up from 169 per minute the preceding quarter. In the fourth quarter, the number of threats each minute averaged 648, up 60% from the previous quarter, [23]. BYOD could expose the company network to malicious files, raising the threat of exfiltration. The peril of viruses, malware, and network intrusion, according to Cisco, is "by far the biggest drawback of BYOD", [24]. This susceptibility arises since the IT department does not have full control over individuals' devices and may not be knowledgeable of their usage. This may increase the spread of malicious applications affecting computers and the firm's network. Malicious malware, in addition to paralyzing computers, can introduce back doors into servers, enabling hackers to take firm data stored on the systems unknowingly. As a result, BYOD can make it easy for hackers to gain access to a company's system by distributing harmful programs to a worker's device through downloaded applications or electronic mail. Harmful files employ a wider variety of API calls as opposed to benign apps, and mobile malware requests dangerous authorization to retrieve confidential material more consistently than benign apps, according to the research, [25]. Malware attacks on cell phones have increased in recent days as a result of private information leaks, causing the system to crash. Malicious code is embedded in the majority of the applications in order to steal data from others. In this approach, spyware targets every phone, [26].

Lack of control over data and devices

In a BYOD environment, Workers are more likely to misuse and abuse business IT resources. For the ease of utilizing their own devices, Workers purposefully circumvent security restrictions such as password protection, IT procedures, and regulations, jeopardizing the safety of business IT resources. As a result, when individually possessed devices that have circumvented the organizations' regulations are taken, it proves a challenge to erase data remotely, [27]. It is a challenge for a firm to verify and audit whether a legitimate staff is utilizing data or an intruder, [28]. Moreover, tech-savvy personnel can bypass proxies and visit social networking sites through firm resources, which are prohibited on the office network. Users with the goal of working from home can install apps to enable remote access to their work PC. Though these incidents may not be malicious, they may expose the firm's network threats, that can permit intruders to steal critical data, [15], [27].

Retrieving data:

When a worker quits the company, there are security concerns. Preventing Workers from accessing company data could turn into a security nightmare. This is incredibly dangerous for a salesperson, and BYOD policies must handle this. Otherwise, a former Worker could resurface as a rival with convenient access to customer information.

Cost implications:

BYOD has security risks as well as hidden costs. According to a recent study, adopting the BYOD methodology will cost a corporation with 1,000 mobile devices an additional $170,000 per year on average. Furthermore, the intricacy of providing support to different kinds of devices with diverse operating systems has increased. Additionally, the issue of legal accountability, as well as the loss of brand identification because the subscriber's identity belongs to the worker and not the firm, [19].

Time spent configuring and supporting personal devices.

Firms that implement BYOD reduce the expenditure on hardware and software, however, this increases obligations to IT teams in maintaining the individual's devise as well as making sure that this venture doesn't introduce vulnerabilities to the firm's network and data, [6].

Network security issues

Personal devices connected to business networks remotely compromise a firm's data. Criminals may be able to capture a firm's information or even mimic authentic staffs to gain unlawful access to networks and services if they are not properly safeguarded, [10]. BYOD brings network security issues due to the use of modern sophisticated mobile devices. An individual who is legally connected to the firm's network can connect with other people who may or may not be part of the organization. Modern mobile devices with QR code scanners can share login credentials or steal login credentials from wireless routers that are not well secured. Some modern smartphones also have a dynamic MAC address and therefore tracking the devices connected to the network is challenging unless access control rules are imposed.

Legal issues

With the use of BYOD devices, there are legal issues to consider. In the event of a policy violation or a worker's departure from the company, retrieving business data from their device may be difficult. There are legal considerations to address in circumstances where child pornography is discovered on the device, [19].

Safeguarding corporate data on a cloud facility

Data security is a delicate subject since cloud services permit users to retrieve data as they desire and can be used to substitute or eliminate the necessity of maintaining data on mobile devices, [29]. Making cloud-based storage reachable from mobile devices, introduce vulnerabilities such as hacking, software-based assaults and can cause other safety concerns like data contamination, control, containment, and monitoring, [30]. Because a firm's ability to govern data transfer results in safety weaknesses that emerge when workers send the firm's data to public clouds for file sharing and then fail to erase it later, data is never entirely lost since cloud service providers keep backups of data for reliability motives. Enabling the "remember password" feature increases the prospect of dangers against cloud storage and mobile devices, [31].

C. BYOD security solutions

Three main essential elements boost the acceptance rate of BYOD in organizations: Worker's code of behaviour, safety program installation, and well-organized administration guidelines. All of these are aspects that contribute to BYOD's overall success, [32]. Technical and non-technical techniques must be implemented in a business to address the security challenges of BYOD. According to studies, in order to address the escalating list of legal, safety, and privacy concerns related to BYOD implementation, enterprises could also re-evaluate the efficacy of safety and privacy regulation mechanisms, technical controls, policies, procedures, and workers awareness initiatives, [20].

i. Non-technical approaches

Non-technical approaches that can be used include; security culture, security awareness education, security strategies, and policy.

Security Awareness Education

According to recent surveys, there is a lack of privacy and security knowledge when it comes to BYOD, [20]. Worker knowledge of BYOD dangers and tolerable applications are increased through security awareness and education initiatives, which improves policy adherence across a company, [21]. Companies must have policies established to secure their data on individuals' devices, including security and education. Workers make many mistakes that might lead to cyberattacks and security vulnerabilities if they are not educated about the risks of BYOD. According to research, 60% of Workers write passwords down on a piece of paper, and 36% of Workers say they reuse the same password for many accounts, [33]. Security and privacy awareness and education programs, according to [34], are crucial in minimizing BYOD security concerns. Workers should be aware of the implications for violating the BYOD policy, as well as the privacy trade-offs associated with it, such as monitoring personal devices, [35].

Security Culture

Staff's group actions, relationships, and viewpoints toward security and risk minimization make up security culture. Because different value systems can influence how people think about and act about security, research shows that creating a safety Compliant principle is vital for Workers to comprehend the significance of, and their role in, guarding information assets, [36]. Workers may view safety procedures as impediments to getting their work done, thus they choose to disregard policies. As a result of this human error, security breaches may occur. Workers can execute their assigned duties and use BYODs in a way that enhances alleviating perils and preserving information assets by supporting a firm's culture that prioritizes security, [15].

Policies

Authorized utilization, surfing, worker obligation, and incident management will all be covered by BYOD-specific policies, which will establish the context for how the initiative will be handled and maintained, [21]. All of the objectives and limits linked to the use of corporate assets must be clearly stated in an efficient and reliable BYOD policy. It should list all of the operations that are allowed on the devices while they are connected to the firm's network. Infrastructure to be used, services to be offered, risks and obligations to be managed, and minimum device needs or configurations should all be clearly stated in policies. Organizations must use critical technologies to create a boundary between work and personally identifiable data in order to preserve the policy. Device management systems will be used to complete these duties, which will aid in the security of shared resources and collaboration amongst individual devices, [37]. BYOD policies, according to [37], should include guidance on safeguarding mobile devices, encryption, and user passwords, data categorization, antivirus software, and wireless access. Remote working and privacy protection, as well as a security breach and its response. Creating a clear information security policy and privacy policy, as well as merging or aiding the other BYOD control spheres, is a key method for controlling the BYOD environment, [35].

Security Strategy

A very well-crafted BYOD strategy and adoption, according to a study, will ensure that individual's IT devices boost worker motivation and morale while cutting costs. A clear BYOD strategy plan can help generate innovation, worker happiness, cost savings, and asset protection by evaluating opportunities and risks, selecting a suitable platform, implementing policies and controls, business continuity, mitigation, and recovery strategies, [15].

Device registration

If a company enables Workers to bring individual devices, it's critical to identify who the gadgets belong to and who owns them. A device owner must register their personal information as well as their device information such as International Mobile Station Equipment Identity (IMEI). This procedure of registration could be automated. The registration system can link device-identifying data to individual data recorded in the database system of the organization. The most crucial component of BYOD is the registration process. A lack of registration could have the same impact as a lack of log storage, [10].

ii. Technical approaches

To address this issue, some approaches and techniques have been developed to give software tools and security measures that will help to mitigate the obstacles and risks. The techniques and approaches for BYOD security management include; mobile device management (MDM), mobile application management (MAM), mobile information management (MIM), Network Access Control (NAC), and Enterprise Mobility Management (EMM). These programs aid in the management of Worker-owned devices for both personal and professional needs, [8].

MDM is a cross-concept that enables firms to securely administer mobile devices. MDM solutions have an essential element that supports protocols, offers consistent management and oversight, is situated inside a firms' network, and authenticates and connects with MDM agents on mobile devices through certificate sharing,[39] (Rhee, Jeon, and Won 2012). The components work together to set access rights, synchronize and update data, conduct remote wiping, handle VPN connections, execute scanning of harmful files, and generate event reports, [40]. MDM offers constraints over applications, cameras, and the use of cloud in workers' devices, [35].

MAM is a flexible choice that manages a certain group of applications on the mobile device, [35]. MAM helps the firm to adopt safety practices, lockdown, define access control regulations, configure software settings, wipe programs under its

control remotely, block access to unauthorized applications, and install approved apps. Applications stay secret and executed at the Worker's choice outside of MAM's boundaries, [41], [42]. When MAM is used in conjunction with containerization environments, it becomes much more powerful.

MIM: Data integrity and encryption are the primary concerns of MIM, which also defines the application and people's access and provides document synchronization across numerous devices while also managing security processes like scanning harmful files, [41]. A firm's data is stored in a single area, like in a cloud server, though it can only be accessible based on explicit consent standards set to the devices and applications that are requesting for it. Because data is stored in a virtual central location, MIM synchronizes data across devices in a similar way to cloud storage services, [8].

EMM: This is a broad method that incorporates the features of MDM, MAM, and MIM. EMM is a BYOD safety feature that keeps track of all devices, apps, and data, [43]. EMM's unique characteristics include the ability to separate business and individual data on the same device, as well as preventive attack detection and a corporate app store, [35].

NAC: This technology allows safe and restricted network connectivity for a broad variety of devices across multiple locations by controlling devices that joins the firm's network. NAC also offers additional controls such as authentication and encryption, as well as the integration of MDM technologies into a network architecture to govern connectivity, assets, and entire network surveillance. In addition to categorizing individuals according to access control strategies or roles, virtual LANs are utilized in this strategy to reduce network traffic, [44]. Besides the BYOD management techniques, there are other measures that are adopted to ensure information integrity, confidentiality, and authenticity are guaranteed in BYOD adoption in a workplace. These measures include;

Secure browsing

Even though a virtual private network is an excellent solution to protect firm security, managers can also use the AirWatch Browser on workers' devices to allow workers to access corporate intranet sites. Users can link the AirWatch Browser to workplace intranets and third-party Web filters using a single sign-on and app tunnelling, [45].

Separation Techniques

Techniques for separating enterprise and personal space based on virtualization and the operating system (OS) have shown promise. Private personal applications and data, as well as vital company apps and data, are confined and executed on the same device in a BYOD. A BYOD scheme must ensure that the individual worker space does not affect the company workspace's security. The enterprise workplace should never jeopardize the privacy of the personal user area. For a successful BYOD design, knowing how to effectively segregate the two environments on the same mobile device becomes critical. To achieve the separation goal, techniques such as virtual mobile platforms, dual boot, and virtualization need to be adopted, [45].

Consolidated control

BYOD control mechanisms encompass compliance control, data sanitization, and compacted configuration control. Furthermore, an administrator can efficiently detect all activities. Misuses of BYOD are detected via a dashboard. This makes it easier to enforce the BYOD policy. In terms of data preservation, the operator can wipe all data with a factory reset or selectively wipe data through a channel like Google Cloud Messaging for Android or another cloud-based solution, [10]. This approach aids in the fortification of s firm's information assets in the event that BYOD devices are lost or stolen. It is critical that an individual can request the operator to delete data via a communication channel. To identify users, a proper authentication technique is required. This is similar to how mobile banking transactions are authenticated. As previously stated, all such controls are totally centralized, and a device must be equipped with an agent that connects to the centralized control, [10].

Blocking and wiping remotely

Whenever individuals' devices are used to execute job-related tasks, certain restrictions are imposed to safeguard the company's intellectual and critical information. When a device is reported lost, a user violates the established policy, or a worker no longer works for the company, remote wiping and blocking are performed. However, Wiping or disabling a device may result in the destruction of the device or cause an individual's data to be. Workers must understand the ramifications of blocking and erasing data caused by software put on their own devices. All of these terms must be

mentioned in the personal device use policy and consent forms, [37]. Whenever a device is misplaced, seized, or the possessor leaves the firm, remote wiping is the last resort. The method entails logging onto the device, then deleting all firm's applications and data, [42]. Remote wiping methods are already included in certain commercially accessible MDM and MAM solutions, [32].

Antivirus, anti-malware, and spyware

These apps are necessary for bolstering BYOD security systems, [46]. It's vital that enterprises mandate the incorporation of safety procedures and that workers who use mobile devices for work motives have installed anti-malware programs to reduce the probability of compromising computers and other devices connected to the firm's network.

Data erasure destruction. Data erasure is required when the organization requires an updated configured device or when an individual wish to upgrade their own device. To avoid losing important data, the files of the preceding device must be wiped in both cases. By leaking critical firm data to the public, an unethical worker can hurt the company. Using Mobile Device Management software to remotely reset a worker's device is one way. These tools have the ability to delete data partitions. This clause must be included in the Worker's contract so that, if necessary, the gadget can be completely reset without causing him or her any inconvenience, [37]

III. METHODOLOGY

Descriptive research design was used in this study to solicit views of respondents on awareness of cybersecurity concerns as well as measures used by organizations to address related security challenges. The respondents were chosen from a non-governmental organization in Kenya through purposive sampling. Structured questionnaires were used to collect responses from the respondents. Out of the 150 questionnaires issued to the respondents, 100 questionnaires were returned. Collected data was analysed using descriptive statistical analysis.

Findings

a. Use of personal devices at work place

Participants were asked whether their organization allow them to use personal devices at work place. 88.6 percent of the participants indicated that they are allowed to use their personal devices, 11.4% of the participants who work in the departments such as finance and health indicated that they were not allowed to use personal devices at work place due to sensitivity of data they handle. These results attest to the growing acceptance of BYOD. Organizations cannot afford to buy computers for every employee due to cost implications.

b. Personal device used to accomplished assigned tasks

The results in Table 1 below show that 58.2% of the respondents use laptops, 19.8% use mobile phones, 6.0% Desktop computers, while 16% use both mobile phones and laptops. Majority of the participants prefer laptops due to portability and advanced technology. This means that workers can access the organization portal remotely.

Table I: Devices used

BYOD device used	Percent (%)
Mobile phone	19.8
Laptop	58.2
Desktop	6.0
Mobile phone and laptop	16.0

c. Awareness of BYOD Policy

We asked the participants if they were aware of any policies that governed the usage of BYOD. 21% of individuals answered they were unaware, compared to 79% who claimed to be. In addition to making sure that employees follow the BYOD regulations, the management team has a responsibility to ensure that all employees are aware of them.

d. Awareness of BYOD security challenges

In regards to awareness of BYOD security challenges, majority of the participants (74.72%) indicated that they were not aware of the security challenges while 25.28% were aware. There is low awareness of security issues related to information systems. Risks associated with BYOD are unknown to many people and this exposes them to data breaches.

e. BYOD security measures

The participants provided their responses on security measures necessary to address BYOD security issues. The table below shows the results

Table II: BYOD security measures

	SD	D	N	A	SA
1. For me, it is necessary to ensure that my cell-phone is encrypted to safeguard data	14.1%	32.1%	20.9%	17.7%	15.2%
2. My employer remotely wipes and block organization data from employees BYOD's who exit the company	90%	5.6%	3.25%	0.45%	0.7%
3.My organization deactivates email accounts of employees who exits	0.8%	0.5%	2.3%	25.9%	70.8%
4. It's necessary to install Antivirus, anti-malware, and spyware programs on BYOD devices	0.5%	1.0%	7.9%	30.1%	60.5%
5.Our organization enforces consolidated control of BYOD (compliance control, data sanitization, and compacted configuration control) to detect and prevent misuse of BYOD	20.8%	32.0%	14.2%	13.1%	19.1%
6.My device stores work related data and personal data separately	73.7%	10.4%	0.7%	10%	5.2%
7.I have put mechanisms in place to recover data in case the device is lost, stolen or damaged	10.8%	14.2%	20.6%	26.5%	27.9%

Key: SD=strongly disagree D=disagree, N=neutral, A=Agree, SA= strongly Agree

The Majority of the participants (32.1%) disagreed that it is necessary to ensure that their cell-phone is encrypted to safeguard data. 90% of the participants also strongly disagreed that their organization wipes and block data when an employee exit. Most of the respondents (70.8%) strongly agreed that an employee who exits the organization have their email accounts and portal accounts deactivated. A Majority of the respondents (60.5%) strongly agreed that it is necessary to install anti-malware programs on BYOD's. 32% of the respondents disagreed that their organization enforces consolidated control of BYOD to detect and prevent misuse. Most of the participants strongly disagreed that their devices stores work and personal data separately. This indicates that there is no separation of personal and work data. Majority of the respondents (27%) have put in place to back-up data while 10.8% disagreed.

IV. CONCLUSION

Inevitably, BYODs will always find their way in workplaces whether permitted by a firm or not. The safety concerns of BYODs can't be ignored and therefore firms must need to put safety measures in place to ensure that their information confidentiality, integrity, and authenticity are not compromised. Technical and non-technical measures have to be put in place to safeguard information assets. The study findings indicate that security measures in regards to BYOD have been ignored. It is imperative for organizations to formulate policies for regulating BYOD usage and enhance awareness of the dangers posed by BYOD since the knowledge of BYOD security challenges as per the research is low. Installation of intrusion prevention and detection systems, as well as close monitoring of BYOD usage, is significant in a BYOD scenario. Further research is needed regarding the secure adoption and implementation of BYOD in workplaces.

REFERENCES

[1] Forcepoint.com, "What is (BYOD)? Bring your own device security and policies," 2022. [Online]. Available: https://www.forcepoint.com/cyber-edu/bring-your-own-device-byod.

[2] A. Monnappa, "What is BYOD (Bring Your Own Device) and Why Is It Important?," 2021. [Online]. Available: https://www.simplilearn.com/what-is-byod-and-why-it-is-important-article.

[3] J. Holleran, "Building a better strategy for BYOD," Risk Management, vol. 61, no. 7, pp. 12-14, 2014.

[4] N. Singh, "B.Y.O.D. Genie Is Out Of the Bottle – "Devil Or Angel"," Journal of Business Management & Social Sciences Research (JBM&SSR), vol. 1, no. 3, pp. 1-12, 2012.

[5] A. Ghosh, P. K. Gajar and S. Rai, "Bring your own device (BYOD): Security risks and mitigating strategies," Journal of Global Research in Computer Science, vol. 4, no. 4, pp. 62-70, 2013.

[6] C. Brook, "The Ultimate Guide to BYOD Security: Overcoming Challenges, Creating Effective Policies, and Mitigating Risks to Maximize Benefits," 2020. [Online]. Available: https://digitalguardian.com/blog/ultimate-guide-byod-security-overcoming-challenges-creating-effective-policies-and-mitigating.

[7] Citric.com, "What BYOD (Bring Your Own Device)?," 2022. [Online]. Available: https://www.citrix.com/solutions/unified-endpoint-management/what-is-byod.html.

[8] M. Eslahi , M. V. Naseri, H. Hashim, N. M. Tahir and E. H. M. Saad, "BYOD: Current state and security challenges," in 2014 IEEE Symposium on Computer Applications and Industrial Electronics (ISCAIE), 2014.

[9] NCSC.gov.uk, "Device Security Guidance," 2022. [Online]. Available: https://www.ncsc.gov.uk/collection/device-security-guidance/bring-your-own-device.

[10] C. Vorakulpipat, S. Sirapaisan, E. Rattanalerdnusorn and V. Savangsuk, "A Policy-Based Framework for Preserving Confidentiality in BYOD Environments: A Review of Information Security Perspectives," Security and Communication networks, 2017.

[11] D. Sangroha and V. Gupta, "Exploring Security Theory Approach in BYOD Environment," in In: Kumar Kundu M., Mohapatra D., Konar A., Chakraborty A. (eds) Advanced Computing, Networking and Informatics, 2014.

[12] T. Maddox, "Research: 74 percent using or adopting BYOD," 2015. [Online]. Available: https://www.zdnet.com/article/research-74-percent-using-or-adopting-byod/.

[13] VMware.com, "What is Bring Your Own Device?," 2022. [Online]. Available: https://www.vmware.com/topics/glossary/content/bring-your-own-device-byod.html.

[14] J. Mont, "The Risks and Benefits of Allowing Employee-Owned Devices," 2012. [Online]. Available: https://www.complianceweek.com/the-risks-and-benefits-of-allowing-employee-owned-devices/4255.article.

[15] A. Pillay, H. Diak, E. Nham, G. Tan, S. Senanayake and S. Deshpande, "Does BYOD increase risks or drive benefits?," 2013.

[16] A. Calder, "Is the BYOD movement worth the risk," Credit control, vol. 34, no. 11, pp. 65-70, 2013.

[17] S. Stieglitz and T. Brockmann, "Increasing Organizational Performance by Transforming into a Mobile Enterprise.," MIS Quarterly Executive, vol. 11, no. 4, pp. 189-204, 2012.

[18] B. Alleau and J. Desemery, "Bring Your Own Device It's all about Employee Satisfaction and Productivity, not Costs!," 2013.

[19] C. Rose, "BYOD: An examination of bring your own device in business.," Review of Business Information Systems (RBIS), vol. 17, no. 2, pp. 65-70, 2013.

[20] A. G. Bello , . D. Murray and . J. Armarego , "A systematic approach to investigating how information security and privacy can be achieved in BYOD environments," Information and Computer Security, vol. 25, no. 4, 2017.

[21] Trustwave.com, "TW-Enterprise-Mobile-Risk-assesssment," 2014. [Online]. Available: https://www.datasecurity works.com/datasheets/TW-Enterprise-Mobility-Risk-Assessment.pdf.

[22] S. O'Dea, "Number of smartphone subscriptions worldwide from 2016 to 2027 (in millions)," February 2022. [Online]. Available: https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/.

[23] McAfee.com, "Mcafee ATR Threat report," 2021. [Online]. Available: https://www.mcafee.com/enterprise/en-us/lp/threats-reports/apr-2021.html.

[24] cisco.com, "Survey Report-BYOD: A Global Perspective Harnessing Employee-Led Innovation," cisco, 2012.

[25] M. Alazab, M. Alazab, A. Shalaginov, A. Mesleh and A. Awajan, "Intelligent mobile malware detection using permission requests and API calls.," Future Generation Computer Systems, vol. 107, pp. 509-521, 2020.

[26] A. B. Sallow, M. A. M. Sadeeq, R. . R. Zebari, M. B. Abdulrazzaq, M. R. Mahmood, H. M. Shukur and L. M. Haji, "An Investigation for Mobile Malware Behavioral and Detection Techniques Based on Android Platform," IOSR Journal of Computer Engineering (IOSR-JCE), vol. 22, no. 4, pp. 14-20, 2020.

[27] M. Potts, "The state of information security," Network Security, vol. 2012, no. 7, pp. 9-11, 2012.

[28] B. Gatewood, "The nuts and bolts of making BYOD work," Information Management Journal, vol. 46, no. 6, pp. 26-31, 2012.

[29] D. Sahu, S. Tripathi, S. Sharma and V. Dubey, "Cloud computing in mobile applications," International Journal of Scientific and Research Publications, vol. 2, no. 8, pp. 1-9, 2012.

[30] R. Nelson, M. María, C. Susana, V. Francisca, M. Adriana and V. Daniela, "Key aspects for the development of applications for Mobile Cloud Computing," Journal of Computer Science and Technology, vol. 13, no. 3, pp. 143-148, 2013.

[31] V. Samaras, S. Daskapan, R. Ahmad and S. K. Ray, "An enterprise security architecture for accessing SaaS cloud services with BYOD," in 2014 Australasian Telecommunication Networks and Applications Conference (ATNAC), 2014.

[32] A. M. French, C. Guo and J. P. Shim, "Current Status, Issues, and Future of Bring Your Own Device (BYOD)," Communications of the Association for Information Systems, vol. 35, no. 10, 2014.

[33] BussinessNewsDaily, "Using Your Smartphone for Work? You're Taking a Big Risk," 17 August 2012. [Online]. Available: https://mashable.com/archive/smartphone-security-lacking.

[34] M. Ratchford, P. Wang and R. O. Sbeit, "BYOD Security Risks and Mitigations," in Latifi S. (eds) Information Technology - New Generations. Advances in Intelligent Systems and Computing, 2017.

[35] B. Alotaibi and H. Almagwashi, "A Review of BYOD Security Challenges, Solutions and Policy Best Practices," in 2018 1st International Conference on Computer Applications & Information Security (ICCAIS), 2018.

[36] K. L. Thomson, "Information Security Conscience: a precondition to an Information Security Culture?," Journal of Information System Security, vol. 6, no. 4, pp. 5-19, 2010.

[37] M. Dhingra, "Legal Issues in Secure Implementation of Bring Your Own Device (BYOD)," Procedia Computer Science, vol. 78, no. 2016, pp. 179-184, 2016.

[38] D. Willis, "Bring Your Own Device: The Facts and the Future," Gartner.com, 2013.

[39] K. Rhee, W. Jeon and D. Won, "Security Requirements of a Mobile Device Management System," International Journal of Security and Its Applications, vol. 6, no. 2, pp. 353-358, 2012.

[40] G. Disterer and C. Kleiner, "BYOD Bring Your Own Device," Procedia Technology, vol. 9, pp. 43-53, 2013.

[41] A. Scarfo, "New Security Perspectives around BYOD," in 2012 Seventh International Conference on Broadband, Wireless Computing, Communication and Applications, 2012.

[42] N. Leavitt, "Today's Mobile Security Requires A new Approach," vol. 46, no. 11, pp. 16-19, 2013.

[43] P. Vaidya, P. Desai and M. Pande, "Some Important Features of Mobile Device Management – An Integral Part of BYOD," International Journal of Research, vol. 2, no. 10, pp. 427-435, 2015.

[44] A. B. Garba, J. Armarego, D. Murray and W. Kenworthy, "Review of the information security and privacy challenges in Bring Your Own Device (BYOD) environments," Journal of Information Privacy and Security, vol. 11, no. 1, pp. 38-54, 2015.

[45] J. . M. Chang, P.-C. Ho and T.-C. Chang, "Securing BYOD," IT professionals, vol. 16, no. 5, 2014.

[46] H. Romer, "Best practices for BYOD security," Computer Fraud & Security, vol. 2014, no. 1, pp. 13-15, 2014.