European Journal of
Technology
(EJT)

BYOD Systematic Literature review: A layered approach

Ntwari Richard, Annabella E Habinka, and Fred Kaggwa

European Journal of Technology
ISSN 4520-4738 (Online)
Vol.6, Issue 1, pp 69 - 85, 2022

www.ajpojournals.org

BYOD Systematic Literature review: A layered approach

[1*]Ntwari Richard, [2]Annabella E Habinka, and [3]Fred Kaggwa

[1,3]Department of Computer Science, Mbarara University of Science and Technology, Mbarara, Uganda.

[2]Department of Computer Science, Makerere University, Kampala, Uganda.

[*]Corresponding Author's Email: rntwari@gmail.com

ABSTRACT

Introduction: Bring your own device (BYOD) is a paradigm where employees use personal devices for organizational related activities. Various benefits accrued by both employees and organization. However, BYOD leads to risks and threats during their usage.

Purpose: The paper aimed at exploring benefits, risks, and suggested controls based on a systematic review of literature.

Methodology: A systematic review methodology was adopted for the study. A search using keywords was conducted to select peer-reviewed journal papers from 2010 to 2020 in ACM Digital Library, Emerald Insight, IEEE Explorer, Science Direct, and Taylor and Francis. Inclusion and exclusion criteria was applied, followed by quality appraisal on the selected articles, and then the data was extracted.

Results: According to the search results, BYOD research is on the rise. Benefits, risks, and controls associated with BYOD were also identified based on a layered approach. Findings indicate that user management is the weakest layer.

Originality/value: This paper adds to previous research on BYOD practices by highlighting key risks and suggesting practices that organizations can use to manage security and privacy risks in BYOD environments using a layered approach.

Keywords: *Briny Your Own Device, BYOD security, BYOD management, Security Controls*

1. INTRODUCTION

Bring your own device (BYOD) is a trend in business entities around the world (Shumate, Mohammed Ketel, 2014), (Alotaibi & Haya, 2018), where employees use personal devices such as smartphones, tablets and laptops among others to access organization networks, applications, and data (Alotaibi & Haya, 2018; Melva, Ratchford & Wang, 2019; Shumate & Ketel, 2014). BYOD's major benefit is mobility, which is made possible by increased mobile device adoption (Alotaibi & Haya, 2018; Palanisamy, Norman, & Mat, 2022). BYOD devices have features that are similar to those found in desktop computers, such as wireless communication interfaces, storage capabilities, high-power processors, and the ability to run a variety of data manipulation applications (Souppaya & Karen, 2013). Because of portability, people are increasingly preferring mobile devices to desktop computers(Harris & Karen, 2014). IT consumerization is a phenomenon in which certain technological advancements impose themselves on the general public before spreading within businesses. IT consumerization is exemplified by BYOD, or the use of personal mobile devices in a professional setting. The convenience with which these devices can be used, as well as the benefits of their various useful applications, are attributed to the inverted adoption logic concept (Harris & Karen, 2014).

Both the business and employees reap various benefits from BYOD (Shumate & Ketel, 2014; Olalere, Mahmod, Ramlan, & Azizol, 2015). From a business standpoint, there are several advantages: 1) technological advancements and the use of the most up-to-date software(Gupta, Garima, & Gurinder, 2019). 2) employee efficiency, as a result of employees' ability to work on the go, at any time and from any location (Baillette & Barlette, 2018). 3) Cost savings due to a reduction in the purchase of hardware and software for employees, as the cost is passed on to them. Employee benefits include mobility, which leads to work flexibility and, as a result, productivity. 2) Employee satisfaction as a result of using a personal and preferred device and 3) Increased productivity as a result of access to information at any time and from any location(Harris & Patten, 2014).

However, instead of new technologies emerging from companies first, BYOD technologies emerge from the consumer domain of the organization, which is a reversal of the traditional business innovation path (Baillette & Barlette, 2018). This reversal poses various threats and challenges to traditional Information Technology in business settings because it is not a corporate initiative but rather an employee preference(Zambrano & Glen, 2018). Shumate & Ketel (2014), Alotaibi & Haya (2018), and Eslahi, Maryam, Hashim, Tahir, & Ezril, (2014) list the following potential risks associated with BYOD: 1) Lack of BYOD policy in, IT policies to guide on user behaviour which may result in insecure, devices 2) Lack of network control in place for devices accessing the corporate network, and 3) Security of data in transit and stored on the mobile device. 4) The presence of malware on the device, and 5) Devices that have been misplaced or stolen.

As a means of overcoming the above-mentioned risks, both technical and non-technical means have been proposed by Harris & Karen (2014), Eslahi et al., (2014), Fani, Rossouw, & Mariana (2016), Olalere et al. (2015), Bello, David, & Jocelyn (2017), Cho & W (2018), Palanisamy, Azah, & Miss Laiha (2020). Technical models include mobile device management, network access control, mobile application management, and virtualization, as well as nontechnical methods such as awareness and training, and BYOD policies (Harris & Karen, 2014). However, each of these approaches have sets of flaws. This study aimed at making a methodological contribution by reviewing existing literature on BYOD and determine the benefits and risks involved based on systematic literature review combined

with a layered approach. In addition, existing BYOD security controls were reviewed, with strengths and weaknesses highlighted.

2. METHODOLOGY

This study aimed at identifying BYOD security risks and controls based on a systematic literature review and layered approach. A systematic literature review guide proposed by Kitchenham et al., (2009) was followed in carrying out the study. A major advantage of following a systematic literature review is the rigorous process involved in data collection, processing, and analysis. The key stages of the review are described in depth in the sections that follow.

2.1 Research Questions

The primary goal of this study was to identify literature for BYOD benefits and risks, as well as gaps in potential remedies to the identified concerns. To attain the aforementioned goal, three research questions were suggested to be investigated (see table 1).

Table 1. Research Questions

No.	Research Question	Motivation
RQ. 1	What benefits are accrued by using BYOD devices in a corporate environment?	Identification of benefits of BYOD to both employees and the organization
RQ. 2	What threats are faced while using BYOD devices in a corporate environment?	Determine the threats faced by all actors in BYOD
RQ. 3	What mitigation strategies can be used to overcome the identified threats in BYOD?	Identification methods used to minimize the occurrence of threats in the BYOD environment

2.2 Search Strategy

Automatic searches on selected databases were used to obtain comprehensive results. The research team created search strings to help them retrieve relevant results from the selected databases. To find articles, the search terms “Bring Your Own Device”, “BYOD”, “Bring Your Own Technology”, “BYOT”, “mobile devices”, “mobile devices security”, “IT consumerization”, “BYOD policy”, Theories and “BYOD solution” were used. The search terms were a combination of the key issues raised in the research questions in 2.1 above. The keywords were searched for in the title and abstract to get as many relevant publications as possible. Five digital databases (ACM Digital Library, Emerald Insight, IEEE Explorer, Science Direct, Taylor and Francis) were used to find relevant publications.

2.3 Search Process

A thorough literature search was conducted using relevant keywords on selected databases, yielding a total of 1425 studies. The resulting papers were then subjected to the inclusion/exclusion criteria before removal of undesired results. The purpose of this stage is to minimize irrelevant results, since the study was limited to peer review articles from a journal or conference. Hence non-academic works such as periodicals and white papers were excluded from the study. Furthermore, papers that were not written in English, or lacked full text, or fell outside the year of publication range of 2011 to 2020 were excluded too. At a total of 337 were eliminated at this point. The next step was to read through the titles and

abstracts to see if they were relevant to the research questions. The articles' contents were afterwards skimmed for screening reasons. Articles that did not articulately address BYOD risk and controls were eliminated at this stage, leading to the exclusion of 1008 articles. There were a total of 22 primary papers returned in the final results (see Figure 1). Table 4 shows the distribution of the number of studies retrieved from each database. The studies were chosen from ACM Digital Library (2), Emerald Insight (3), IEEE Explorer (10), Science Direct (4), Taylor and Francis (3).

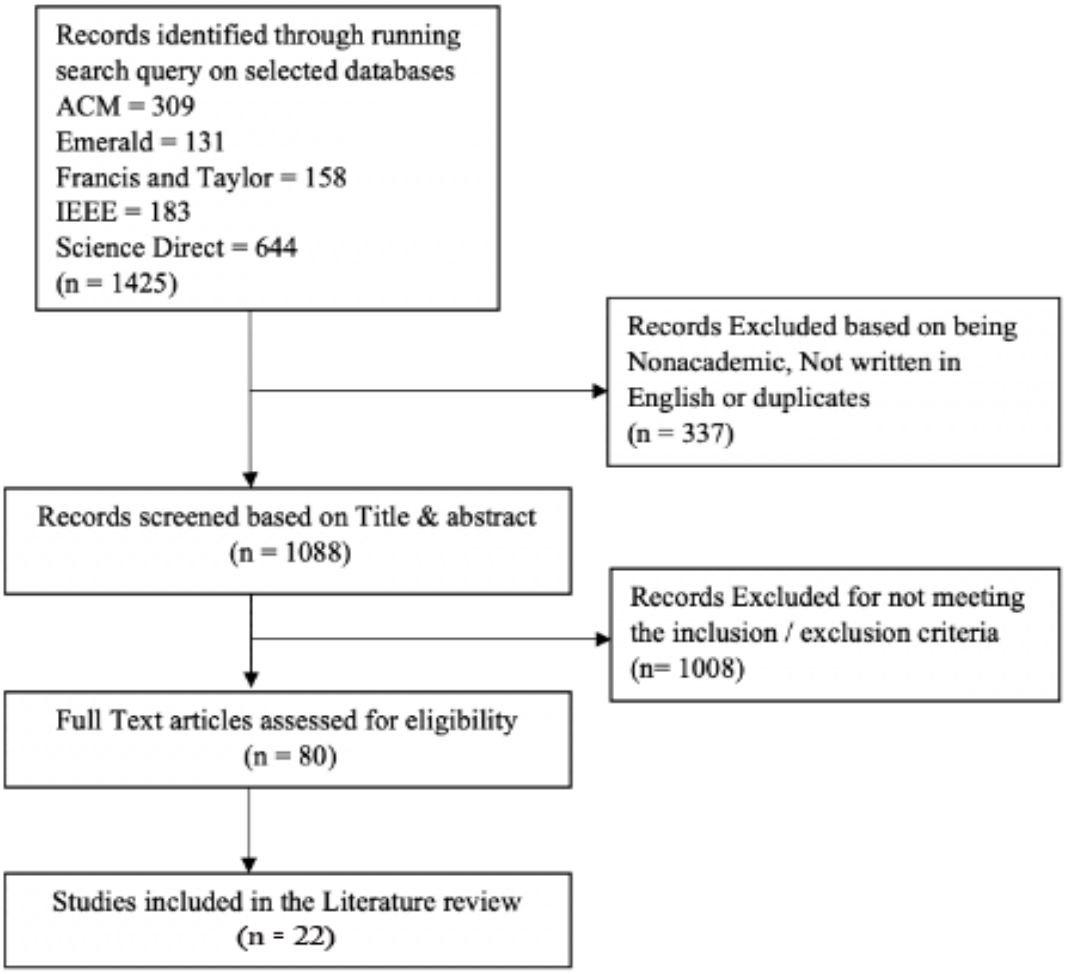

Figure 1. Flow diagram for studies selection

2.4 Inclusion and Exclusion Criteria

The inclusion / exclusion criteria were based on the guidelines (Kitchenham et al., 2009). The search mainly focused on mapping existing literature on BYOD risks and suggested controls in the business environment. Hence, papers that did not clearly describe the risks and controls were excluded. Poster papers were excluded too, from the review as they would have duplicated the information contained in the full text articles. The search spans the years 2011 to 2020, all articles outside the range were eliminated. The search focused on papers written in English language. A full description of the inclusion/ exclusion criteria is described in Table 2. The inclusion/exclusion criteria helped strengthen the search process quality for the purposes of data synthesis and analysis.

Table 2. Inclusion / exclusion criteria

No	Inclusion Criteria	Exclusion Criteria
1.	The paper must be in BYOD research context to well-defined methods and results	Any research that is out of the BYOD context
2.	The paper must be published in a peer-reviewed journal or conference proceedings	Non peer-reviewed published information
3.	The paper should be written and published in English language	Non English papers
4.	Full text available	Full text unavailable
5.	Published between 2011 and 2020	Outside the bracket of selected years

2.5 Quality Appraisal Criteria

A set of criteria were used to assess the quality of each selected study and to determine the relevance of the original study's findings and interpretation (Kitchenham et al., 2009). A quality evaluation was performed for this review based on the questions below to offer a measure of the extent to which a research is appropriate and can produce findings that will add to the scope of the inquiry. The grading technique for the article was established as Yes = 1, Partial = 0.5, and No = 0 or Unknown (information is not provided). To begin, if a research entirely meets the requirement, it was given a rating of 1. Secondly, if a research only partially met a quality requirement, it was given a grade of 0.5. Finally, if it failed to fulfill a quality requirement, it received a 0 rating. Grading for the research questions was as follows;

- QA1: Y (Yes), BYOD features and benefits are explicitly described in the study; P (Partly), BYOD features and benefits are implicit; N (No), BYOD features and benefits are not mentioned and cannot be inferred easily.
- QA2: Y (Yes), the study's threats and risks are well described; P (Partly), the study's threats and risks are either missing or not explicitly specified; N (No), the paper's threats and risks are missing or not defined.
- QA3: Y (Yes), mitigation strategies for identified risks are clearly defined; P (Partially), a few mitigation strategies for identified risks are defined or are unclear; N (No), mitigation strategies are lacking.

Based on the above quality assessment questions, as a score of Y=1, P=0.5, and N=0 was an award to each question, leading to the most qualifying papers scoring 3 points and the least qualifying scoring 0 points. The study selected papers whose scores ranged between 2.5 to 3 points.

2.6 Data extraction and Analysis

The following information was extracted from each study: the title of the study, the author(s), their institution, and the country in which it was conducted, the source (journal or conference), and full reference, and the study's research methods. The main research questions and their answers are summarized in this study. The data extraction results were tabulated in table 3 to show the following: The annual number of BYOD studies and their sources (addressing RQ1). Each paper discusses the features and benefits of BYOD

(addressing RQ1), the threats and solutions identified in each study (addressing RQ2 and RQ3).

Table 3. Summary of selected studies

Id	Author	Title	Year	Research Idea
A	(Palanisamy et al., 2020)	BYOD policy compliance: Risks and strategies in organizations	2020	Investigated factors that influence BYOD policy compliance using PPT model
B	(Wani, Antonette, & Kathleen, 2019)	BYOD in Hospitals-Security Issues and Mitigation Strategies	2019	Developed a mitigation strategy which can cater for BYOD security issues in hospitals
C	(Al-Harthy, Mohammed, Fiza, Rahim, Nor'Ashikin, & Amando, Singun, 2019)	Theoretical Bases of Identifying Determinants of Protection Intentions towards Bring - Your-Own-Device (BYOD) Protection Behaviors	2019	Protection intentions factors leading to BYOD protection behaviors
D	(Gupta et al., 2019)	Employee Perception and Behavioral Intention to Adopt BYOD in the Organizations	2019	Evaluated the employees' perceptions towards BYOD & their intentions to use their personal devices for organizational purpose.
E	(Ratchford & Yong Wang, 2019)	BYOD-Insure: A Security Assessment Model for Enterprise BYOD	2019	Proposed a comprehensive security assessment model, BYOD-Insure, that assesses the security of an organization's BYOD posture
F	(Doargajudhur & Peter, 2018)	The Effect of Bring Your Own Device (BYOD) Adoption on Work Performance and Motivation	2018	Investigated the effects of BYOD adoption on employees' motivation and perceived job performance
G	(Baillette & Barlette, 2018)	BYOD-related innovations and organizational change for entrepreneurs and their employees in SMEs	2018	Identified new risks arising from BYOD adoption in SMEs by entrepreneurs and their employees
H	(Giwah, 2018)	User Information Security Behavior Towards Data Breach in Bring Your Own Device (BYOD) Enabled Organizations - Leveraging Protection Motivation Theory	2018	Evaluated users behavior towards information security, based on the Protection Motivation Theory

I	(Alotaibi & Haya, 2018)	A Review of BYOD Security Challenges, Solutions and Policy Best Practices	2018	Reviewed BYOD security challenges and issues, security solutions and policy best practices in organizational perspective
J	(Kadimo, Masego, et al., 2018)	Bring-your-own-device in medical schools and healthcare facilities: A review of the literature	2018	Literature review of BYOD in health facilities
K	(Cho & W, 2018)	A Study of BYOD adoption from the lens of threat and coping appraisal of its security policy	2017	Investigated BYOD adoption issues based on Technology Threat Avoidance Theory
L	(Amoud & Roudies, 2017)	Experiences in Secure Integration of BYOD	2017	Systematic Literature Review on secure integration of BYOD in an Enterprise
M	(Bello et al., 2017)	A systematic approach to investigating how information security and privacy can be achieved in BYOD environments	2017	Explored best practices in managing BYOD
N	(Thompson, Tanya, & Xuequn, 2017)	"Security begins at home": Determinants of home computer and mobile device security behavior	2017	Comparison of security between home desktop users and mobile users
O	(Fani et al., 2016)	A framework towards governing "Bring Your Own Device in SMMEs"	2016	Proposed a framework for management of BYOD in organizations
P	(Hovav & Frida, 2016)	This is my device! Why should I follow your rules? Employees' compliance with BYOD security policy	2016	Employee compliance with BYOD policy
Q	(Ketel & Thomas, 2015)	Bring your own device: Security technologies	2015	Explored security techno-logies involved in BYOD
R	(Downer & Maumita, 2015)	BYOD Security: A New Business Challenge	2015	Described BYOD security challenges and available frameworks
S	(Zahadat, Paul, Timothy, & Bill, 2015)	BYOD security engineering: A framework and its analysis	2015	Examined BYOD risks and proposed a framework for overcoming them
T	(Harris & Karen, 2014)	Mobile device security considerations for small and medium sized enterprise	2014	Reviewed BYOD challenges in SMEs and suggested controls.

U	(Wang, Jinpeng, & Karthik, 2014)	Bring your own device security issues and challenges	2014	Summarized BYOD security issues and challenges and a comparisons of solutions.
V	(Shumate & Ketel, 2014a)	Bring your own device: Benefits, risks and control techniques.	2014	Discussed BYOD security related issues and explored the benefits, risks, available controls and solutions

3. FINDINGS

The 22 articles were research papers, since the inclusion/exclusion criteria targeted only journal or conference papers. Among these, 12 were based on qualitative research methodology, while 8 quantitative based paper and 2 used mixed methods. The publications were produced in high-income and middle-income countries as namely, USA (7), Australia (5), France (1), Hong Kong (1), India (1), Korea (1), Malaysia (1), Oman (1), Saudi Arabia (1) South Africa (1), Botswana (1), and Morocco (1). Although the search was limited to 2011 to 2020, the selected articles range from 2014 to 2020 as shown in Figure 2.

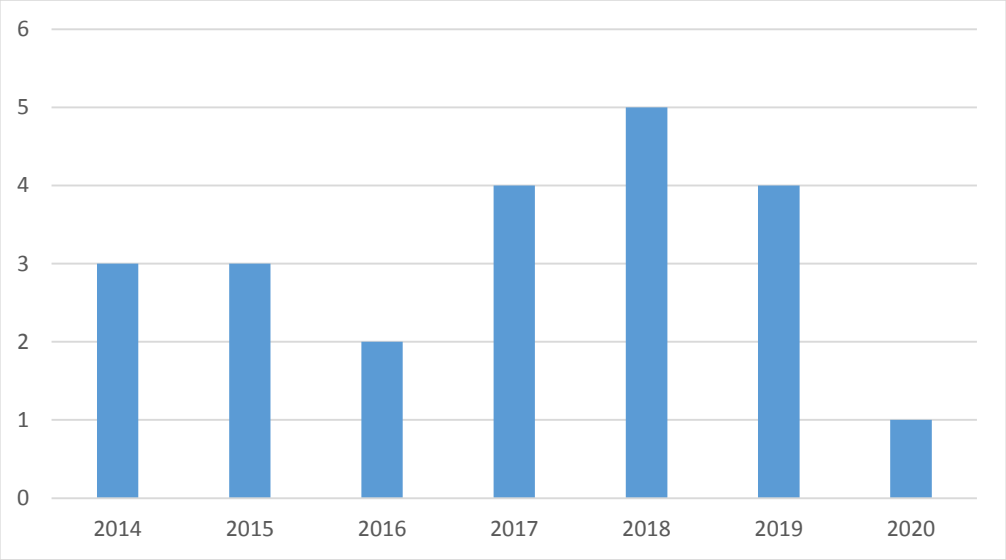

Figure 2. Publications by year

4. DISCUSSION

4.1 RQ1: What benefits are accrued by use BYOD?

Prior studies, Bello et al. (2017), Alotaibi & Haya (2018) , and Ratchford & Yong Wang (2019) indicate that implementation of BYOD programs benefits both the organization and individuals. Analysis of the literature suggests benefits to the organization include cost savings at workplace (Alotaibi & Haya, 2018). These costs relate to hardware and software purchases, which are transferred to employees, purchasing and maintaining their own devices, saving organisation costs that would have done the same (Gupta et al., 2019; Zahadat, et al., 2015). Cost cutting in BYOD supports the claim that organizations desire for technology that is simple to use and accessible while conserving or decreasing costs (Fani et al., 2016). Another significant aspect of cost saving includes the reduction of IT technical support and maintenance cost (Alotaibi & Haya, 2018a); (Ketel & Thomas, 2015). IT helpdesk support is limited in a BYOD setting because the employee owns the devices and

utilizes the devices with which they are familiar. However, Akin-Adetoro & Kabanda (2015) contrast that BYOD is costly for employees since they must cover related expenditures. In contrast, employees opt to overlook the cost because the perceived benefits outweigh the cost. Technological innovations are integrated into the organization (Doargajudhur & Peter, 2018) through use of the latest equipment and software (Gupta et al., 2019). Employees are motivated by these advances because they make organization data easier to utilize, process, and obtain. Furthermore, BYOD supports innovativeness by supporting employees to discuss and collaborate ideas at any time and from anywhere (Bello et al., 2017). Organizations with limited resources, such as small and Medium Enterprises, might profit from resource efficiency technologies(Harris & Karen, 2014).

Similarly, the benefits enjoyed by employees include satisfaction due to the use of personal devices (Amoud & Roudies, 2017). Allowing employees to choose and use the gadget of their choice leads to a sense of ownership (Thompson, et al., 2017), which leads to satisfaction. With BYOD, employees select familiar devices, reducing the time required to adapt to and learn new interfaces (Amoud & Roudies, 2017), which results in the device providing satisfaction while in use. Furthermore, using familiar devices boosts creativity (Bello et al., 2017), critical thinking, and problem-solving skills (Al-Harthy et al., 2019), because employees can use the most up-to-date technology to complete their tasks. Secondly, employees are productive when working on their own device (Alotaibi & Haya, 2018b; Thompson, McGill, & Xuequn, 2017), saving time spent carrying out a task (Al-Harthy et al., 2019). Similarly, using familiar gadgets reduces the training time and needs while increasing usability (Amoud & Roudies, 2017). Furthermore, BYOD incorporates mobility leading to increased accessibility and flexibility at work (Alotaibi & Haya, 2018). This strategy promotes working remotely or mobility by allowing secure access to information from any network connected to the Internet, keeping in touch with clients (Amoud & Roudies, 2017). Finally, employees are given the freedom to be adaptable. Employees have greater freedom in managing their time since they utilize the same device for personal and business duties, resulting in flexibility. This allows end users to communicate with their families, reducing stress (Baillette & Barlette, 2018).

4.2 RQ2: What threats are faced while using BYOD?

Literature review by Alotaibi & Haya (2018), Olalere et al. (2015), Harris & Karen (2014), Palanisamy et al. (2020) , Harris & Karen (2014) and Cho & W (2018) indicates that threat agents include the device connectivity of, the device the operating system and applications on, the device data stored or accessed by, the device and human factors. A mapping of threats to the literature has been illustrated using a novel layered approach in table 4.

Table 4. Identified risks for each layer from selected studies

Layer	Risk	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
Device	Stolen device/lost mobile device	✓	✓			✓			✓	✓		✓		✓		✓		✓		✓		✓	✓
	Jail broken/ rooted device		✓																		✓		
	Inadequate Controls	✓	✓	✓						✓	✓	✓		✓				✓	✓	✓			✓
	Wearable devices			✓																			
	Disposal of device								✓			✓								✓			

Data	Malware leading to data leakage	✓	✓	✓		✓		✓		✓	✓		✓	✓	✓	✓	✓	✓		✓	✓	✓	✓
	Third party apps		✓					✓	✓														
	Un-authorized access	✓	✓					✓	✓		✓	✓		✓		✓		✓	✓			✓	
Applications and OS	Out dated apps						✓														✓		
	Different variations / versions of software	✓		✓							✓		✓								✓		
	Apps from un-official stores		✓	✓							✓					✓					✓		
	Integrations (access and permissions)			✓				✓											✓	✓			✓
Network	Connection to rouge access points	✓		✓						✓	✓			✓				✓			✓		✓
	weak access controls	✓	✓																		✓		
	Inadequate Network resource, infrastructure			✓						✓	✓		✓										
	Un-encrypted channels	✓	✓								✓											✓	
Users	Lack of training / awareness	✓								✓				✓		✓							
	Lack of Knowledge																						
	social engineering	✓								✓				✓									
	Privacy - Company vs user data			✓						✓			✓										
	Compliance	✓	✓	✓			✓						✓		✓	✓	✓					✓	
	User behavior (eg Malicious insider)	✓		✓									✓		✓		✓	✓					
Policy	Non existent	✓	✓			✓		✓	✓	✓				✓		✓		✓					✓
	Inadequate policy		✓	✓																			
	Adherence to policy								✓					✓	✓								

Threats in each layer were carefully identified and are described as follows;

Device related risks: Mobile devices are known for their mobility (Al-Harthy, Mohammed et al., 2019), which allows users to communicate while on the go. However, because of their mobility, gadgets are susceptible to theft or loss (Palanisamy et al., 2020), (Wani et al., 2019), (Melva M Ratchford & Yong Wang, 2019), (Giwah, 2018), (Cho & W, 2018) and (Ketel & Thomas, 2015). The possessor of a stolen or misplaced phone with insufficient access control may gain access to private data saved on the device (Shumate & Ketel, 2014). Regrettably, the security rules that apply to traditional computing equipment like desktop PCs do not extend to these mobile devices (Palanisamy et al., 2020). Another danger is using jail-broken or rooted devices in a BYOD setting, because their security is compromised (Wani et al.,

2019) and (Harris & Karen, 2014). (Al-Harthy, Mohammed et al., 2019) raises concerns about the security of wearable gadgets, which are on the increase and include capabilities similar to other mobile devices. Another danger identified is improper mobile device disposal, which might expose the data stored on them to unauthorized persons (Cho & W., 2018; Giwah, 2018; Zahadat et al, 2015).

Connectivity risks: For data exchange, mobile devices include wireless interfaces such as Wireless Fidelity (Wifi), Bluetooth, near field communication (NFC), and Global Services for Mobile (GSM)(Souppaya & Karen, 2013). Users in a BYOD environment utilize these interfaces to access company data and applications while on the go. However, data sent over these channels can be intercepted by malevolent individuals using the following techniques; A user could be persuaded to utilize phony and malicious access points (Al-Harthy et al., 2019),(Palanisamy et al., 2020), (Bello et al., 2017; Cho & W, 2018; Harris & Karen, 2014; Kadimo, et al., 2018; Ketel & Thomas, 2015) and (Shumate & Ketel, 2014), giving the access point originator access. Some access points' security measures, such as Wifi's WEP, can be readily cracked or hacked(Harris & Karen, 2014), allowing unauthorized access to data. Because mobile devices can establish hotspots, a rogue employee could build an access point that attackers could exploit to get beyond security protections like firewalls in an organization (Al-Harthy et al., 2019; Bello et al., 2017; Cho & W., 2018; Harris & Patten, 2014; Kadimo et al., 2018; Ketel & Shumate, 2015; Palanisamy et al., 2022; Zahadat, et al., 2015).

Operating system and applications: User applications (apps) provide consumers access to the device's capabilities and accessibility on mobile devices. These apps are linked to the hardware and system resources via a mobile operating system (OS). A diversity of OS and apps, including multiple versions with varying security measures, exist as a risk connected with the operating system (Shumate & Ketel, 2014; Wang, Wei, & Vangury, 2014). This creates a quandary about how to properly manage and regulate them. Existence of out-of-date operating systems and apps with vulnerabilities that may be abused to obtain access to sensitive information (Doargajudhur & Peter, 2018), (Harris & Karen, 2014). Existence of jail-broken / rooted devices exposes their operating systems to vulnerabilities such as malware installation (Wani et al., 2019) and (Harris & Karen, 2014). Third-party app shops may include malware that may be exploited to get access to sensitive information(Shumate & Ketel, 2014a).

Data Risk: The most significant dangers connected with BYOD are data breaches or data loss. When data is leaked or lost, organizations risk serious consequences such as legal action, tarnished reputation, and financial fines, among other things (Palanisamy et al., 2020). The common causes of data loss include unauthorised access due to device loss or malware installed on the device (Palanisamy et al., 2020),(Wani et al., 2019) ,(Ratchford & Wang, 2019), (Giwah, 2018), (Cho & W, 2018), (Al-Harthy, Mohammed et al., 2019), (Baillette & Barlette, 2018), (Alotaibi & Haya, 2018) and (Ketel & Thomas, 2015). Malware is any harmful program that interferes with the normal operation of a mobile device and/or the apps loaded on the device. Malware is often placed in an infected program (Shumate & Ketel, 2014) whose functioning and data are jeopardized (Alotaibi & Haya, 2018). Attackers can use this flaw to gain easy access to edit or delete corporate data. Viruses, Trojan horses, spyware, and adware are only some of the types of malware that exist. These differences are determined by the malware's method of assault on the device (Harris & Karen, 2014). Malware is acquired through the download and installation of infected or fraudulent apps from third-party sources (Palanisamy et al., 2020).

User Attacks: These are non-technical attacks aimed at the use of a BYOD device. The user's unawareness and physiological condition are exploited in these attacks (Giwah, 2018). The most common approach is social engineering which involves psychological manipulation to get sensitive or secret data from the user (Palanisamy et al., 2020), (Alotaibi & Haya, 2018), (Bello et al., 2017). Methods of social engineering may also be used to trick people into installing malware on their devices. Another type of assault is a Denial-of-Service (DoS) attack, in which the attacker sends a corrupted text message to prevent the victim from using the device's services. The majority of user attacks are blamed on a lack of policy to guide users to regulations of BYOD usage(Wani et al., 2019),(Giwah, 2018) ,(Bello et al., 2017).

4.3 RQ3: What are the characteristics of the security models used in BYOD?

Organisations apply numerous techniques to mitigate the risks identified in B. above. Observations from the literature indicate that each technique identified secures a particular section of the BYOD process such as devices, network access points, access control, and software management. This section therefore, discusses the techniques and control of risk management in a BYOD based on the actors' perspective.

Device management: The Mobile Device Manager (MDM) approach includes utilizing two-component software to handle mobile devices. The server software is the first component, and it sends control commands to the mobile device via the agent program, which is the second component (Meisam, & Ezril, 2014); Downer & Maumita, 2015). Organizations use MDM to monitor, manage, and secure devices since it addresses the behaviour of the device as a whole (Wani et al., 2019). The MDM implements security regulations and monitors compliance among managed devices (Harris & Karen, 2014). Another technique is the enforcement of a mobile device's access control and permissions at the operating system level. In the event that a device is lost or stolen, these restrictions prohibit unauthorized access to device functionality. The use of screen locks, passwords, personal identification numbers (PINs), and biometric locks to open the device is the initial layer of restrictions (Ketel & Thomas, 2015), (Wani et al., 2019) , (Cho & W, 2018). The use of permission to allow apps access to certain services or data is the second layer of control. Allowing geo-tracking and remote management access to GPS services, for example, as a means of locating and controlling a misplaced gadget (Shumate & Ketel, 2014).

Operating system and Application management: The Mobile Application Manager (MAM) was identified as a tool for managing and protecting company apps that are installed on mobile devices (Alotaibi & Haya, 2018), (Ketel & Thomas, 2015). MAM, in contrast to MDM, which manages the entire device, only manages specific programs. Application, installation, updates, and deletions, as well as audit and policy enforcement, such as application whitelisting and blacklisting controls, are all key MAM operations (Harris & Karen, 2014), (Downer & Maumita, 2015), (Ganiyu & Rasheed, 2018). One of the MAM's flaws is that it cannot control personal apps that are not managed by it. The Enterprise Mobility Manager (EMM) is another option for managing software in a BYOD environment (EMM). This method combines the capabilities of MDM, MAM, and mobile information manager into a single solution (Alotaibi & Haya, 2018). As a result, hardware, software, and data are all managed simultaneously. EMM's ability to separate corporate and personal data allows for effective device management. Users, on the other hand, are hesitant to use it due to its strict policy monitoring and high costs.

Data Management: Mobile Information Manager (MIM) is a data management strategy in which data is managed centrally (Eslahi et al., 2014). Any authenticated device is given an encrypted link to the data. This strategy works well for isolating personal information from

corporate data. However, this strategy limits the number of business apps that can access data (Eslahi et al., 2014). Mobile desktop virtualization is another data management strategy. Security policies are also enforced by the server, which apply to all devices with access (Hovav & Frida, 2016). When a session is closed, all programs and data are saved on the server, not the device. This prevents data from being stored on the mobile phone (Ganiyu & Rasheed, 2018). The technique's limitations present challenges when installing old systems. Containerization is a secure method of storing organizational apps and data on a mobile device. The policies of the container determine how data can be accessed and used. Containerization allows the separation of corporate and personal data while having no effect on the device's functionality (Hovav & Frida, 2016). Another option is to use antivirus software to verify that the device is secure before allowing access. This assists in the elimination of malware that could lead to data leaks or tampering.

Network Management: Network Access Control (NAC) is a mechanism for regulating and managing access to organizational networks. Device authentication (Alotaibi & Haya, 2018a), controlling multiple devices in multiple locations at the same time, and data encryption in transit are all capabilities of this approach (Downer & Maumita, 2015). The NAC can also keep track of how users interact with the network and what resources they have access to (Ketel & Thomas, 2015). Policies, such as user access categorization based on policy definitions, can be applied in the NAC. However, there are drawbacks to this strategy, including the inability to detect malware-infected devices that could compromise the network.

User Management: A user policy is an important tool for ensuring compliance with BYOD regulations and legislation. Security measures such as acceptable employee behavior standards, device usage, network access, data management, and application management are all specified in the policy (Palanisamy et al., 2020), (Wani et al., 2019), (Ratchford & Wang, 2019). Technical controls and policy are inextricably linked such that if the policy is violated, the technical restrictions become ineffective, as pointed out by Alotaibi (Alotaibi & Haya, 2018). An incentive should be included in the policy to urge staff to follow it. The question of "what" should be included to make it comprehensive, on the other hand, is a major challenge for user policy formulation. Secondly, awareness and training programs should be included into the day-to-day operations of a business to increase awareness levels (Downer & Maumita, 2015; Palanisamy et al., 2020). According to Harris et. al. (Harris & Karen, 2014), awareness aids employees in becoming aware of the problem and how to respond to it, whereas training aids employees in gaining knowledge and ability to combat the problem.

5. CONCLUSION

This study set out to explore the literature to identify BYOD features, namely, advantages, risks, and solutions. A systematic review of 22 studies has revealed that many benefits are accrued when BYOD is permitted in an organisation. Findings indicate that benefits are achieved by both organisations and employees, including cost cutting, satisfaction, and productivity, among others. However, the same literature indicates that security risks are prevalent and continue to occur in organisations with greater possibility of exposing data to security breaches. Evaluation of the risks indicated risks being severe compared to those in traditional computing (Palanisamy et al., 2020). Risks were investigated based on a layered approach, identifying the respective layers such as device management, operating system and applications management, Data Management, Network Management, User management and Policy.

The findings indicate that lost or stolen devices, data leakage due to malware, connection to rouge access points are some of the key risks. A series of controls are suggested to combat the risks. However, a balance between control and user freedom is recommended, as an imbalance might lead to psychological repulsion. The attempt to find a balance between security management and BYOD may be difficult, since excessively strict control may negatively affect user experience and lead to reluctance to BYOD. Findings show that user management is the weakest layer, since other layers have technical controls in place. The study recommends an organisation to pay attention to the social factors through the implementation of BYOD policies. If not, users might turn to their social surroundings yet the outcome is unpredictable. Another recommendation is the use of awareness techniques such as training and helpdesks to provide users with insight and guidance.

The outcomes of this study point to the need for in-depth research into policy compliance and awareness programs that can solve BYOD security concerns. BYOD requires security knowledge and training since, with mobile devices, users make their own security decisions, which distinguishes it from conventional computing. In contrast to the conventional setting, leaving control in the hands of employees alone poses security issues. Technology-specific abilities should be incorporated into the training. Users are frequently ignorant of the dangers that these technologies pose, and even if they are aware, they need to know how to reduce those dangers.

According to the findings, policies should be utilized to achieve a balance between users' demand for convenience and network and system administrators' desire to enforce network limits. These guidelines controlling mobile device usage confront a variety of issues. However, the policy should be drafted carefully to enable positive adoption. The policies should ensure that mobile devices will continue to offer consumers with the convenience they seek once all laws and regulations have been implemented. There is a scarcity of research on the effectiveness of BYOD policies, making it impossible to understand how organisations have achieved the delicate balance of convenience and security.

To our best knowledge, this is the first time a layered approach has been used in a systematic literature review to conduct a critical review of selected BYOD studies. The evidence from the identified studies adds to our understanding of how to successfully implement BYOD in various domains. In addition, the review provides policymakers and implementers with recommendations for future improvements to these interventions.

6. FUTURE WORK / RECOMMENDATIONS

There are certain limits to this review, but they present opportunity for additional research. First, despite a comprehensive search, it is possible that some essential information was ignored owing to a lack of specified keyword strings. Using suitable synonym keywords to build search strings is an important aspect of the search process. Secondly, this research is confined to only two categories of documents: journal articles written in English and conference papers written in English. As a consequence, some articles may have been omitted. The key recommendations based on the findings and discussions are as follows: 1) Since employees are the weakest link in the BYOD eco system, there is a need to discover techniques that might promote BYOD compliance behaviour among them. 2) Before implementing a BYOD program, organizations should first design a BYOD policy. Policy is the basis, and policies are in place to guide users through the dos and don'ts that lead to compliance. 3) Future study should focus on the social aspects that impact employees' security in the workplace. 4) A paradigm that supports policy adherence, technological controls, and stakeholder management might assist to ease BYOD security problems. As a

result, future research should look into how policy, people, and technology security goals can be fulfilled in a BYOD environment.

REFERENCES

Ajzen, I., & Thomas, J. M. (1986). Prediction of goal-directed behavior: Attitudes, intentions, and perceived behavioral control. *Journal of experimental social psychology*, *22*(5), 453-474.

Akin-Adetoro, A., & Kabanda, S. (2015). Contextualizing BYOD in SMEs in developing countries. *In Proceedings of the Southern African Institute for Computer Scientist and Information Technologists*.

Alotaibi, B., & Haya, A. (2018). A review of BYOD security challenges, solutions and policy best practices. *1st International Conference on Computer Applications & Information Security (ICCAIS).*

Amoud, M., & Roudies, O. (2017). Experiences in secure integration of BYOD. *Proceedings of the 7th International Conference on Information Communication and Management.*

Baillette, P., & Barlette, Y. (2018). Baillette, P., & Barlette, Y. (2018). BYOD-related innovations and organizational change for entrepreneurs and their employees in SMEs. *Journal of Organizational Change Management*, *31*(4), 839-851.

Bello, A. G., David, M., & Jocelyn, A. (2017). A systematic approach to investigating how information security and privacy can be achieved in BYOD environments. *Information & Computer Security*, *25*(4), 475-492.

Cho, V., & W, H. I. (2018). A study of BYOD adoption from the lens of threat and coping appraisal of its security policy. *Enterprise Information Systems*, *12*(6), 659-673.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS quarterly*, 319-340.

Doargajudhur, M. S., & Peter, D. (2018). The effect of bring your own device (BYOD) adoption on work performance and motivation. *Journal of Computer Information Systems*, *60*(6), 518-529.

Downer, K., & Maumita, B. (2015). BYOD security: A new business challenge. *International Conference on Smart City/SocialCom/SustainCom (SmartCity).*

Eslahi, M., Maryam, V. N., Hashim, H., Tahir, N. M., & Ezril, H. M. (2014). BYOD: Current state and security challenges. *IEEE Symposium on Computer Applications and Industrial Electronics (ISCAIE).*

Fani, N., Rossouw, v. S., & Mariana, G. (2016). A framework towards governing "Bring Your Own Device in SMMEs. *Information Security for South Africa.*

Ganiyu, S. O., & Rasheed, G. J. (2018). Characterising risk factors and countermeasures for risk evaluation of bring your own device strategy. *International Journal of Information Security Science*, 49-59.

Giwah, A. D. (2018). User Information Security Behavior Towards Data Breach in Bring Your Own Device (BYOD) Enabled Organizations-Leveraging Protection Motivation Theory. *SoutheastCon.*

Gupta, R., Garima, B., & Gurinder, S. (2019). Employee Perception and Behavioral Intention to Adopt BYOD in the Organizations. *International Conference on Automation, Computational and Technology Management.*

Harris, M. A., & Karen, P. P. (2014). Mobile device security considerations for small-and medium-sized enterprise business mobility. *Information Management & Computer Security*, *22*(1), 97-114.

Hovav, A., & Frida, F. P. (2016). This is my device! Why should I follow your rules? Employees' compliance with BYOD security policy. *Pervasive and Mobile Computing*, *32*, 35-49.

Kadimo, K., Masego, B. K., Dineo, K., Lovie, E. S., Kagiso, B. S., Carrie, K., & Kutlo, B. (2018). Bring-your-own-device in medical schools and healthcare facilities: a review of the literature. *International journal of medical informatics*, *119*, 94-102.

Ketel, M., & Thomas, S. (2015). Bring your own device: Security technologies. *SoutheastCon.*

Kitchenham, B., & Stuart, C. (2007). uidelines for performing systematic literature reviews in software engneering .

Kitchenham, B., O. Pearl, B., David, B., Mark, T., John, B., & Stephen, L. (2009). Systematic literature reviews in software engineering–a systematic literature review. *Information and software technology*, *51*(1), 7-15.

Liang, H., & Yajiong, X. (2009). Avoidance of information technology threats: A theoretical perspective. *MIS quarterly*, 71-90.

Meisam, E., Maryam, V. N., H, H., N, M. ,., & Ezril, H. M. (2014). Byod: Current state and security challenges. *IEEE Symposium on*, (pp. 189–192).

Okoli, C., & Kira, S. (2010). A guide to conducting a systematic literature review of information systems research.

Olalere, M., Mohd, T. A., Ramlan, M., & Azizol, A. (2015). A review of bring your own device on security issues. *Sage Open*, *5*(2).

Palanisamy, R., Azah, A. N., & Miss Laiha, M. K. (2020). BYOD policy compliance: Risks and strategies in organizations. *Journal of Computer Information Systems*, 1-12.

Ratchford, M. M., & Wang, Y. (2019). BYOD-Insure: A Security Assessment Model for Enterprise BYOD. *Fifth Conference on Mobile and Secure Services (MobiSecServ).*

Rogers, W. R. (1975). A protection motivation theory of fear appeals and attitude change1. *Rogers, Ronald W. "A protection motivation theory of fear appeals and attitude change1." The journal of psychology*, *91*(1), 93-114.

Shumate, T. M. (2014). Bring your own device: benefits, risks and control techniques. *IEEE Southeastcon.*

Shumate, T., & Ketel, M. (2014). Bring your own device: Benefits, risks and control techniques. *IEEE Southeastcon.*

Souppaya, M., & Karen, S. (2013). *Guidelines for managing the security of mobile devices in the enterprise.* NIST special publication.

Straub, W. D., & Welke, J. R. (1998). Coping with systems risk: Security planning models for management decision making. *MIS quarterly*, 441-469.

Thompson, N., Tanya, J. M., & Xuequn, W. (2017). Security begins at home": Determinants of home computer and mobile device security behavior. *Computers & Security, 70*, 376-391.

Wang, Y., Jinpeng, W., & Karthik, V. (2014). Bring your own device security issues and challenges. *IEEE 11th Consumer Communications and Networking Conference* .

Wani, T. A., Antonette, M., & Kathleen, G. (2019). BYOD in hospitals-security issues and mitigation strategies. *Proceedings of the Australasian Computer Science Week Multiconference.*

Zahadat, N., Paul, B., Timothy, B., & Bill, A. O. (2015). BYOD security engineering: A framework and its analysis. *Computers & Security, 55*, 81-99.

Zambrano, F. R., & Glen, D. R. (2018). Bring your own device: a survey of threats and security management models. *International Journal of Electronic Business, 14*(2), 146-170.