12-2018

Bring Your Own Device (BYOD): Risks to Adopters and Users

Obinna G. Otti
ogotti@stcloudstate.edu

Bring Your Own Device (BYOD): Risks to Adopters and Users

by

Obinna Gerald Otti

A Starred Paper

Submitted to the Graduate Faculty of

St. Cloud State University

in Partial Fulfillment of the Requirements

for the Degree of

Master of Science

in Information Assurance

December, 2018

Starred Paper Committee
Abdullah Abu Hussein, Chairperson
Lynn A. Collen
Balasubramanian Kasi

Abstract

Bring your own device (BYOD) policy refers to a set of regulation broadly adopted by organizations that allows employee-owned mobile devices – like as laptops, smartphones, personal digital assistant and tablets – to the office for use and connection to the organizations IT infrastructure. BYOD offers numerous benefits ranging from plummeting organizational logistic cost, access to information at any time and boosting employee's productivity. On the contrary, this concept presents various safety issues and challenges because of its characteristic security requirements. This study explored diverse literature databases to identify and classify BYOD policy adoption issues, possible control measures and guidelines that could hypothetically inform organizations and users that adopt and implement BYOD policy. The literature domain search yielded 110 articles, 26 of them were deemed to have met the inclusion standards. In this paper, a list of possible threats/vulnerabilities of BYOD adoption were identified. This investigation also identified and classified the impact of the threats/vulnerabilities on BYOD layered components according to security standards of "FIPS Publication 199" for classification. Finally, a checklist of measures that could be applied by organizations and users to mitigate BYOD vulnerabilities using a set layered approach of data, device, applications, and people were recommended.

Keywords: BYOD, Security, Privacy, Risk, Mobile Device Management (MDM) Confidentiality, Availability & Integrity.

Dedication

This study is devoted to the Almighty and Ever-living God for all His blessings, sustenance grace, loveliness and for making this research effort and my masters master's program in St Cloud State University possible.

Acknowledgments

My genuine gratitude goes to my supervisor as well as committee members Dr. Abdullah Abu Hussein, Dr. Lynn Collen, and Dr. Balasubramanian Kasi for offering their invaluable and unreserved constructive criticism, suggestions, and supervision in the course of this research. In addition, earnest appreciation goes to the head of the department of Information Systems; Dr. Herath Susantha and my graduate advisor; Dr. Jim Chen for their support and guidance through my master's program. Distinct appreciations go to my wife; Priscilla Otti for her patience, understanding, and encouragement, and my parents; Chief and Mrs. Anthony Otti for their unflinching support throughout the course of my master's program in St Cloud State University. A special feeling of gratitude goes to my siblings, in-laws, relatives, and wonderful friends. At all times, I will continuously appreciate you all for being there for me.

Table of Contents

Chapter Page

List of Tables

List of Figures

Chapter I: Introduction

Bring Your Own Device, or BYOD, is a catchphrase that has gained wide adoption to denote to personnel who take their own mobile devices namely; laptops, laptops, smartphones, personal digital assistant and tablets to their place of work for use. Moreover, BYOD is a contraction from the perception of “IT Consumerization” which defines the rising trend of innovative information technologies emergence into the consumer market and other organizations (government and business) (Moreira, Cota, & Gonçalves, 2016). Olalere, Abdullah, Mahmod, and Abdullah (2015) in their work also referred to Bring Your Own Devices (BYOD) as the strategy of permitting the personnel/employees of an organization to work with their own personal mobile devices. Irrespective of the perceptions the society has about BYOD, the use of personal mobiles devices is swiftly increasing (Sundgren, 2017). BYOD came into existence since staff or employees of an organization started bringing their personal USB drive to work in order to accomplish the installation of programs and carry out their assigned task.

Apparently, security and privacy risks are increasing with the high rate spread of mobile devices and their increasing use by organizations to me meet their organizational goals. As mobility grows in the workplace, so do challenges from managing bandwidth and device access to handling the most pressing concerns of security (Shridhar, 2017). The 2017 Mobile Security Report focuses on these security challenges and offers fresh insights into the state of mobile threats and solutions (Shridhar, 2017).

Since the proliferation of cloud-based software and mobile devices, mobile computing has displaced internet computing (Olalere et al., 2015). BYOD enables staff or employees to connect to their organizations' IT infrastructure using their personal mobile devices. Based on reports acquired from research aimed at investigating the limitations and affordances of "Bring Your Own Device" for wide-ranging educational practices in higher education based on the teachers' viewpoints, effective ways of integrating BYOD into students' academic lives are being explored by academicians (Song & Kong, 2017). A survey in 2015 affirmed that about 70% of businesses have adopted BYOD. Only 50% of the employees use the security measure (e.g., password, passcode) installed on their devices and less than 20% uses additional security measure such as Anti-malware (Downer & Bhattacharya, 2015).

With the advancement in cloud technology, cloud security remains a major security concern for organizations and users that rely greatly on cloud infrastructures that is dependent on BYOD policy to deliver and support business service to its teaming clients. Additionally, cybersecurity challenges are very common to SMEs as well as large organizations and most interestingly some these organizations do not possess essential IT staff, expertise and knowledge to effectively avert, allay and challenge cybersecurity issues. "It is no accident that in 2015, over 74% of the SMEs faced at least one cybersecurity breach" (Kyriazis, 2018). To address challenge in cloud environments, Kyriazis (2018) presented an innovative architecture that enables users to bring their own security mechanisms in cloud environments. This innovative architecture depend on the deep-rooted Bring Your Own Device (BYOD) model and

implements it in the context of security and privacy which “obviates the need for on-site security-oriented resources (e.g. hardware, software, personnel), given that these security mechanisms will be offered, managed, selected, activated, deployed and monitored as plugins” (Kyriazis, 2018).

There are many benefits of adopting BYOD policy such as reducing organizational cost, the building-up of employee’s productivity, increased flexibility and employee satisfaction. Additional benefits of BYOD include maximizing profit in the purchase of hardware, applications, service agreements, licensing and insurance (Caldwell, Zeltmann, & Griffin, 2012). At the introduction of Apple iOS devices, the convenience and prevalence of these mobile devices made them extremely appealing to workers using them for work, off-location and on location (Zahadat, Blessner, Blackburn, & Olson, 2015). Even though both companies and their employees can benefit from various aspects of BYOD, there are also risks and concerns accompanying the adoption of BYOD (Vorakulpipat, Sirapaisan, Rattanalerdnusorn, & Savangsuk, 2017). In essence, the protection of corporate data stored in BYOD is important. As BYOD also connects to the corporate network, it is also crucial to secure the corporate network as well as the BYOD.

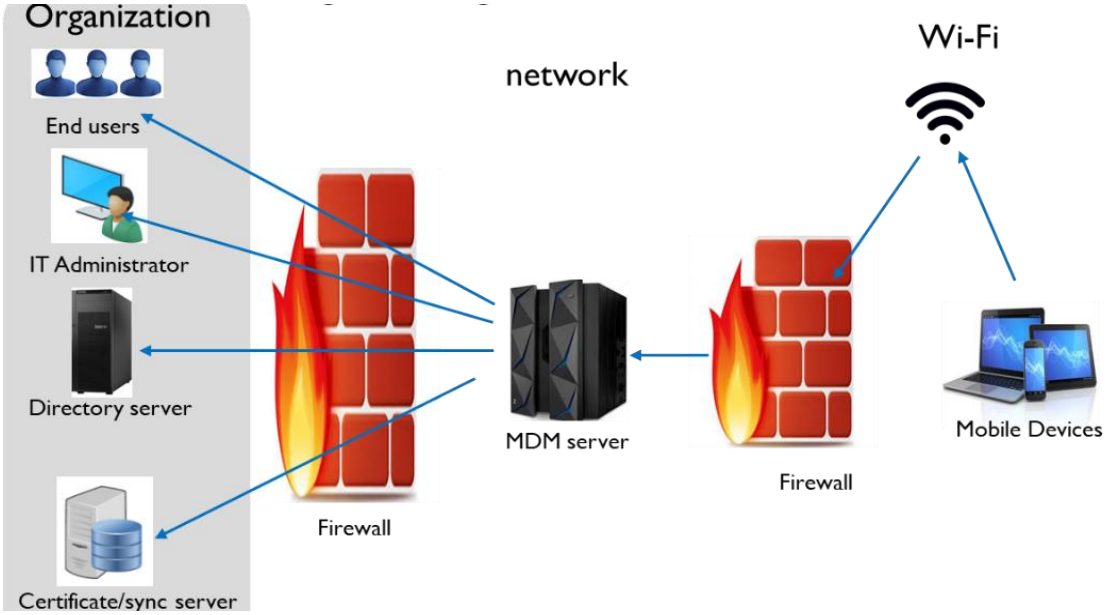

Figure 1. Diagram of BYOD Networks

Problem Statement

Ogie (2016) observed that there are numerous risks linked to Bring Your Own Device policy. The obvious wide gap in BYOD policies adoption by today's organizations demonstrates that there is knowledge deficiency in preferring solutions to BYOD challenges. Since there is a lack of standardized security metric, the process of evaluating the severity of the attacks has become harder (Zulkefli & Singh, 2018). This starred paper will launch a background to comprehend BYOD risks and threats to both adopters and users by taking a critical look into circumstances that aid the existence of these risks, attacks, and threats as well as its consequences.

Nature and Significance of the Problem

Based on IT consumerization concepts, BYOD solutions can benefit both users and adopters like the government and business organizations. For instance, management and administrative standards of BYOD in corporate organizations can be

adopted by higher education institutions (Saa, Moscoso-Zea, & Lujan-Mora, 2017). In view of this context, BYOD frameworks are being fashioned and adopted by some organizations such as university, for example, to achieve learning goals and keep its students connected. The security risks and threats posed by the implementation of BYOD to enterprises (adopters) and employees (users) can bring an organization to its kneels because adopters and users of BYOD policy stands the risk of data leakage or loss of information as well as the problem of control and management of mobile devices between adopters and users, BYOD policies should be constantly revaluated with a view to proposing a corresponding risk management solution.

The Objective of the Study

The objective of this study borders on the evaluation of the effectiveness of generally adopted BYOD policies, with the aim of identifying the BYOD security threats, risks, challenges as well as vital policy considerations for effective application by both users and adopters.

Study Questions

Some of the questions that have inspired this research study are:

1. What is BYOD policy and its advantages?
2. What are the security and privacy risks, threats, vulnerability and attacks that are intrinsic in the BYOD framework?
3. What are the causes of these security and privacy risks, threats, vulnerability, and attacks?

4. What possible control measures or solutions should be considered for confronting BYOD policy from risks, threats, vulnerability and attacks to information security and privacy?

Definition of Terms

To offer a considerate comprehension of the phrases, expressions, and terms used in in this study and to stick to industry standard terminology, underneath are the resulting terms, expressions and definitions taken from *User's Guide to Telework and Bring Your Own Device (BYOD) Security* (Souppaya & Scarfone, 2016) and SANS Institute website (SANS Institute, 2017)

- **Application Program Interface (API**): A crop of routines, protocols, and tools for developing software applications.
- **Advanced Persistent Threat (APT):** A targeted and cyber-attack in which an intruder gets access to a network and remains unnoticed for a prolonged period.
- **Authentication:** The method of checking the accuracy of a claimed identity.
- **Authenticity:** Conformance and legitimacy of the original information.
- **Availability:** Assurance of dependable access to information by an authorized person(s).
- **Blacklist**: List of senders of spam e-mails previously directed to a user.
- **Computer Network:** Assembly of host computer systems and sub-network through which data exchange is made possible.

- **Confidentiality:** Set standard that determines access limits to information by authorized persons.
- **Content Filtering:** The method of monitoring, examining communications and averting the distribution of malicious content to users through email and web pages.
- **Corporate Network:** A group of computer systems, connected within a building or area which are all owned by an organization.
- **Disinfect:** This simply means the removal of malware from file content.
- **Enterprise Mobility Software:** This is an application which allows the secure usage of mobile device and application by employees of an organization.
- **Integrity:** This is the safeguarding from inappropriate information obliteration or modification, including ensuring information non-repudiation and authenticity.
- **Malware or Malicious Code:** This is a program that is secretly positioned onto a computing device with the sole intention of compromising the integrity, confidentiality, and availability of the computer's operating system, data and applications.
- **Mobile Device:** A minor moveable computer namely PDA, tablet, and smartphones.
- **Personal Computer:** Laptop or desktop computer.

- **Personal Firewall:** A program with the capability of screening the flow of communications among computers and blocks unwanted communications.
- **Phishing:** A misleading computer-based tactic to trick people into revealing delicate personal information.
- **Popup Window:** A separate web browser windowpane that is instinctively triggered to open when a webpage gets loaded.
- **Quarantine:** A store of files that have malware, virus, trojan in segregation for impending inspection or disinfection.
- **Remote Access:** This refers to the ability users or employee of an organization to gain access to its organization's IT network from an external location.
- **Remote System Control:** The ability to remotely use a computer system of an organization from a telecommuting computer system.
- **Risk:** Refers to the possibility of a threat exploiting vulnerabilities of an entity of value thereby causing damage to the entity in question e.g. an organization.
- **Risk Assessment:** Refers to the method of identifying risks and determining its impact.
- **Security Controls:** Refers to the set of standards, algorithm, metrics, policy, procedure or other measures applied to minimize the rate of harm caused by vulnerability or threat.

- **Security Policy**: Refers to a course of action adopted to regulate or control how a system or organization offers safety measures to safeguard critical and sensitive resources.
- **Security Protections:** Refers to control measures to counter threats with an intention to recompense for a weakness in the security of a computer system.
- **Service Set Identifier (SSID):** Refers to a term or name given to a wireless access point (AP). Also, it is a type of identifier that exclusively recognizes a wireless local area network - WLAN.
- **Social Engineering:** Refers to generic term given to attackers with the intention to hoax people into performing some tasks like downloading and executing files which appears to be malicious or disclosing sensitive information.
- **Standard User Account:** An employee or user account that possess restricted privileges which are meant for some generalized specific tasks like browsing the web, sending and receiving e-mails.
- **SQL Injection**: A code injection method used by hackers with nefarious intention to embed a malicious code or program in an unsecured application and then conceded to the database backend.
- **Telecommuting:** Refers to the capability to perform work responsibilities from a remote location other than the organization’s premises by contractors, business partners, employees, vendors, and other users.

- **Threat:** Refers to a potential action or object that has the capacity to violate computer security and cause harm or security breach.
- **Virtual Private Network:** Refers to technology that connects the computing devices across a public network and enables employee or users to receives and sends information to the organization's private network.
- **Vulnerability:** Refers to a fault or flaw that exists in a system's design, application or operation which can be taken advantage of, to disrupt the security policy of a computer system.
- **Whitelist:** Refers to a list of email senders considered and known to be trustworthy and acceptable.

Summary

This chapter gives a summary of what BYOD means, its benefits and security challenges. Also, this chapter clearly defines the objective, nature, and significance of this study. In addition, some project related terms in this chapter were defined. The subsequent chapter discusses a brief description of the background and literature review of previous related work by other scholars.

Chapter II: Background and Review of Literature

Introduction

In this chapter, literature related to the study problem, questions and methodology were reviewed.

Background Related to the Problem

Security risk to BYOD casts substantial problems on organizations' computer technology resources. Interestingly, it is worthy to note that awareness of the risks and threats arising from BYOD policies is growing. Research has revealed the tendency of adopters and users of BYOD policies not paying close attention to the importance of security of BYOD models. Table 1 shows literature review of notable BYOD policy research efforts meanwhile Appendix A provides a broad-range of research efforts and their contributions that were very instrumental in this study. The cognizance of security and privacy of BYOD for organizations have obvious been studied in recent times. In a recent research (Singh, Chan, & Zulkefli, 2017), security and privacy risks were classified into privacy risks on BYOD (Saa et al., 2017); use of untrusted mobile OS and applications; malicious application installation on mobile device; lack of physical security controls; and the usage of insecure networks.

Table 1

Literature Review of Notable BYOD Policy Research Efforts

Study	Focus	Problem	Contribution
Zulkefli *et al.* (2018)	BYOD security metrics classification	The severity of BYOD security attacks	A taxonomy that contributes to providing a ranking list on the severity of various security attacks occurring in BYOD Higher Education.
Giwah (2018)	User behavior towards information security data breach in BYOD enabled organizations	Unpredictability in predicting users' intended information security data breach in organizations using a BYOD policy.	Proposed a theoretical approach based on the Protection Motivation Theory.
Alotaibi & Almagwashi (2018)	Evaluation of BYOD Policy Best Practices, Security Issues, and Solutions	Existing BYOD security issues, challenges, solutions and policy best control measures in an organization.	Presented an all-inclusive policy model for BYOD security.
Ketel (2018)	Enhancing BYOD Security Through SDN	Methods and solutions for alleviating BYOD security risks in an organization.	Proffered various network technologies and administration tools e.g. SDN, NFV and EMM that can be used to mitigate BYOD security challenges.
Olalere et al. (2015)	Theoretical Assessment of Bring Your Own Device on Security Challenges	Inadequate research efforts to address security issues confronting BYOD policy implementation	Provides a theoretic evaluation for future work which aids scholars to detect viable areas of research in BYOD.
Kadimo et al. (2018)	Literature Review of BYOD in healthcare facilities and medical schools	Identified components of BYOD policy e.g. guidelines, issues, and interventions that could hypothetically apprise BYOD policy creation, adoption and implementation in healthcare facilities and medical schools	Conceived and developed an exploration strategy for conducting search & review of themes, abstracts, and titles. Similarly, they analyzed the identified matrix for agreed and used emerging themes.

Apart from privacy risks and security controls of BYOD, there are other factors that could impede the successful implementation of BYOD solutions in organizations. Mishima, Sakurada, and Hagiwara (2018) believed that some risk factors could impede the rising growth of BYOD implementation in the institutions of higher learning. These risks include an upsurge in operation cost of the computer room, a price reduction of information equipment and modification of the atmosphere of information-based education (Mishima *et al*., 2018).

In business atmospheres, BYOD is widely used, and it entails great mandate for security in order to manage and administer business responsibilities in a secure and accurate method. For every BYOD environment, security and privacy of data is accorded great significance and priority. Therefore, Harthy, Shah, & Shankarappa (2018) in their paper, “proposed enhanced risk management for BYOD to improve security of BYOD environment which utilizes MDM system logs and risk management system and apply machine learning for identifying the malicious activity”.

Herrera, Ron, & Rabadão (2017) stated that the chief risk of BYOD is the network connection because these BYOD devices are used by workers to gain access to companies' information, but there is the lack of policy on cybersecurity that safeguards the network connectivity and the transmitted info. For this reason, the study of policies and strategies of cybersecurity that is focused on BYOD can be an alternative to guarantee the growth of a company where employees use their own devices from anywhere (Herrera et al., 2017).

Current authentication systems in many organizations typically targets separately devices or users, whereas the BYOD policy needs to guarantee that authorized users with the secured devices can only be granted access. Zheng, Cao & Chang (2018) research paper presented “a novel biohashing based user-device physical unclonable function (UD PUF) to provide a bipartite authentication of both user and device for the BYOD system”. Their initial research results depicts that “an honest (device, user, challenge) combination exhibits a very low equal error rate of 0.032, and tampering of

any elements of the tuple will cause the hamming distance between the “live” and enrolled templates to have nearly random distribution” (Zheng, Cao & Chang, 2018).

Ballagas, Rohs, Sheridan, and Borchers (2004) scrutinized the diverse types of user or employee communications and deployment issues neighboring large public displays. They came up a physical interface for communicating with big public presentations using mobile phones with empowered cameras. Ballagas et al. proposed that to support serendipitous interaction with large public displays, the interface should use both visual codes and optical-flow processing.

Olalere et al. (2015) discussed BYOD’s theoretical concepts, benefits, prevalence, probable security attacks, and challenges. They also reviewed findings of academic research on BYOD. This detailed review demonstrates that security problems contain the greatest important issue challenging BYOD policy and subsequently, little efforts have been made to address these security problems (Olalere et al., 2015).

Obviously, it appears that tabloid headlines across the world on a consistent basis transmit news of cyber-attacks leading to data breaches. In the United States, data breaches incidents increased by a significant 40% in 2016 (Timms, 2017). Considering the number of occurrences of cyber-attack on an international gauge, it further depicts only the increasing trends of cyber-attacks confronting business firms nowadays. Timms (2017) examined the security risks and challenges encountered by SMEs and summaries how these can be mitigated. According to Timms, SMEs remain often restricted by incomplete resources and minor IT industry players whose chief job

is to make uncomplicated systems functioning, rather than having an all-inclusive comprehension of the cyberthreat.

Koh, Oh, and Im (2014) opined that BYOD restrictions and users' demonstrative repugnance to the control of personal mobile devices are inadequate to mitigate risk factors trendy in a BYOD environment. They studied security problems that could possibly occur in the innovative IT environments of BYOD. Koh et al. also described some BYOD glitches which can't be mediated with the existing technical know-how and solutions. In addition, Koh et al. proposed an all-inclusive security system that can be applied in the resolution of emerging security threats by investigating the framework information that conducts an energetic access control.

French, Guo, and Shim (2014) summarized the board discussion which happened at the "2013 Americas Conference on Information Systems." They discussed the existing issues, position in addition to the future course of adoption and usage of Bring Your Own Device (BYOD), Bring Your Own Apps (BYOA) and Bring Your Own Service (BYOS). In addition, current use, adoption, pros and cons, real-world cases, issues of traditional security and privacy, and future directions were the covered BYOD topics.

Obviously, there are numerous benefits to employing BYOD policy; but since countless risks are associated with BYOD, it has become a new phenomenon poses a high level of difficulty for organizations to securely manage (Fani, Solms, & Gerber, 2016). The Fani et al. (2016) research provided a rudimentary guideline to management

executives on the method of managing and governing the emerging BYOD phenomenon in a secure and accountable manner.

Yevseyeva et al. (2015) was very instrumental in addressing the connected security vulnerabilities and risks of devices used within “Bring Your Own Device (BYOD)” framework. They argued that bearing in mind the decision-making atmosphere and the glaring truth that an employee might assume a better position to make a fitting choice, that nudging could be most appropriate than severe guidelines in conditions of the ambiguity of security-based conclusions (Yevseyeva et al., 2015). Several nudging examples were considered in their research.

Okigbo, Uwasomba, and Douglas (2016) stated BYOD is an original phenomenon which comes with the increased rate IT consumerization. Previous investigations showed that 70 % growth was felt in employee productivity, 40% price decrease on corporate-liable mobile devices in organizations that adopted BYOD (Okigbo et al., 2016).

Shumate and Ketel (2014) discussed security issues that are linked to BYOD frameworks. They noted BYOD has an increased prevalent choice for big business and small business that are similar and explored the inherent advantages, risks, obtainable controls measures and outcomes to allay the characteristic security worries specifically bedeviling BYOD frameworks and its associated devices.

Prashant, Arnab, and Shashikant (2013) provided numerous mobility approaches, control features, procedures, and defenses, administrative and management facet to achieve organizational implementation of BYOD policy. Their work

believed that BYOD naturally accompanies new opportunities but has several risks that also accompanies it.

According to Wang, Wei, and Vangury (2014), it is vital to safeguard BYODs thereby protecting organizations' networks because BYODs mobile devices constitute part of organizations' networks. This is apparently so because mobile devices are very prevalent in workplaces due to its enormous rewards such as growing users' productivity and plummeting companies' operational cost. Wang et al. (2014) explained, however, that IT consumerization brought various security challenges and issues owing to their requirements for adequate security. Their study recapitulates attacks and threats on BYODs and exposing its security challenges. Wang et al. additionally associates current BYOD frameworks and offers a security framework that guides enterprises in the adoption and implementation of BYOD policy.

Li and Yang (2017) analyzed the powerful factors of employing a BYOD policy in organizations, then identified some difficulties in the course of deploying the BYOD policy. Furthermore, they proposed a conforming management approaches of BYOD with the view to providing avenues for enterprises to achieve the mobile needs of their organizations (Li & Yang, 2017).

In addition, Kao, Chang, and Chang (2015) scrutinized some problems associated with the security of BYOD services provided within the university environment. They also analyzed current BYOD concepts that apply to wireless network framework, which demands from users the enrollment their mobile devices to client software for administration and control reasons. They discovered that passwords &

usernames were used several times a day to circumvent user identity verifications (Kao et al., 2015). Thus, a “BYOD service management system—EZ-Net” was proposed to enforce a fail-through authentication functionality to a mobility controller of current wireless local area network through numerous visibly conventional authentication servers (Kao et al., 2015). A typical 60 minutes of “authentication time per month” was saved for every user thereby saving a significant cost on licensing fees charged for EZ-Net management software by the studied university (Kao et al., 2015).

According to Jaha and Kartit (2017), to prevent stress and data leakage triggered by the BYOD trend, numerous solutions have been suggested which includes the use of authentication methods and Mobile Device Management (MDM). Several security control approaches can be selected to accomplish BYOD goals such as authentication techniques (Jaha and Kartit, 2017).

While a chunk of studies have engrossed their attention on BYOD policy in a teaching space condition, very minute fieldwork setting study seems to have been carried out on BYOD. Welsh et al. (2018) reported that students’ observations of the challenges and advantages of Bring Your Own Device in the context of fieldwork. The major discoveries of their work recommend that about one-fifth of students during fieldwork were not eager to use their own device quoting damage or loss as the chief motive for their unwillingness. Their study also discovered that some students thought that group work can be negatively impacted by BYOD (Welsh et al., 2018). Apparently, this study depicts a misconfiguration between practitioner (adopters) and student (users) discerning with earlier studies which recommend that BYOD policy adopters

have faith that group work can be enhanced by mobile smart devices (Welsh et al., 2018).

Information systems research in BYOD has demonstrated a growing demand to evaluate user information security behavior perception. Regrettably and in broad contexts, almost all the investigations carried out on user behavior towards information security have thus created a knowledge breach for a comparable study that emphasizes on organizational technological policies and specific concepts (Giwah, 2018). Relying on the rising pliability introduced by the Bring Your Own Device policy, Giwah (2018) examined the prevailing works by researchers, suggested an approach to conducting their study and a theoretical model founded on Protection Motivation Theory (PMT). Their research also climaxes findings made to the field of information security investigation (Giwah, 2018).

In a bid to advance employee organizational productivity and efficacy, organizations depend on policies such BYOD policy to encourage the IT consumerization in recent times. Ekpo & Fournier-Bonilla (2018) studied and sought to comprehend how the application of BYOD policies by companies or organizations bring about influencing issues otherwise observed as perceived threats that could constitute user's resistance to embracing emerging technologies. In addition, this study "goes to determine to what extent such concerns influence employee's decisions to either embrace a BYOD program or reject the BYOD program" (Ekpo & Fournier-Bonilla, 2018).

Benefits and security risks accompany BYOD policy adoption. The adoption and implementation of BYOD policies constantly pose some difficult problems because organizations need to circumvent security risks to ensure enhanced productivity by its employee. Nevertheless, risks that are linked with the security of “BYOD” devices could be controlled by creating a security policy that is functional and implementing some measures for technical security control (Alotaibi & Almagwashi, 2018). Alotaibi and Almagwashi (2018) reviewed the existing BYOD security issues and challenges, possible solutions and best security control measures from an organizational viewpoint. In addition, the Alotaibi and Almagwashi research presented a comprehensive security policy model for adoption.

To distinguish abnormal behaviors and recognize unauthorized access to resources through BYOD devices due to the proliferation of mobile devices such as laptops, smart phones and widespread internet access, Petrov & Znati (2018) presented a framework, which employs a twofold technique; the artificial neural networks (ANN) and decision tree (DT) machine learning (ML) techniques are intertwined to mitigate the risks of exfiltration or tampering, infiltration of delicate organizations’ information when retrieved on BYOD mobile devices. The framework enables active counter-measures control “against 3 types of intruders, who mimic the behavior of legitimate users in order to gain access to sensitive IT infrastructure and data in organizations’ Intranets” (Petrov & Znati, 2018).

Ketel’s (2018) research on enhancing BYOD security through Software Defined Networking (SDN) examined the various approaches and resolutions which can be

applied by organizations to lessen BYOD security risk to a bearable extent. Although BYOD adoption offers several organizational advantages, security risks still pose a critical problem for organizations (Ketel, 2018). Ketel's academic research efforts presented the solutions may include vast administration and network technological tools e.g., NFV, SDN, and EMM to resolve the prevalent BYOD problems.

Research by Kadimo et al. (2018) identified that there is a scarcity of literature on development, evaluation of BYOD policy and assessment of mobile device deployment plans. This theoretical assessment examined the available literature to recognize BYOD policy mechanisms (guidelines, problems, and interventions) that could hypothetically apprise BYOD policy creation, implementation and evaluation in healthcare facilities and medical schools (Kadimo et al., 2018). These researchers created an overview medium to identify the key facets of individual study and veiled the matrix for developing concepts (Kadimo et al., 2018). They also suggested a relative adoption of a method of applying interventions to 'chasing' problems, an extra possible method of attaining a benign environment for mobile device use through the creation of an all-inclusive BYOD policy that balances patient privacy and the users 'need for suitability with organizational security' (Kadimo *et al.,* 2018).

Literature Related to the Methodology

Identifying and responding to the emerging security challenges posed by BYOD adoption has led a lot of researchers into an intense methodical investigation with a view of proposing mitigation strategies to security and risks concerns posed by BYOD.

Li, Peng, Huang, and Zou (2013) outlined several BYOD security issues using a candid tactic of inspecting smartphones in a BYOD network intermittently to thwart any breach in security. The Li et al. (2013) research contributions were presented in three-fold: (a) identification of network security threats to organizations based on the exclusive smartphones features, (b) introduction of a technique for measuring security representative of smartphone in an organizations' network while relying on the owner's the co-location logs and interests, and (c) proposed a carefully planned but otherwise strategic sampling method of addressing BYOD security challenges between responsiveness to security incidents and convenience/cost-efficiency.

Amoud & Roudies (2017) scholarly investigation presented a Systematic Literature Review (SLR) of BYOD published research articles to answer the following question: "How to integrate securely a BYOD in an Enterprise?''. In addition, this study demonstrated that there's no one-size-fits-all solution to the inherent issues of BYOD, because BYOD brings new trend of challenges to organizations that adopts it (Amoud & Roudies, 2017). Moreover, Amoud & Roudies (2017) study noted that the prevailing security approaches to BYOD extensively covers the information assembly but, relative approaches do not define how to agree on a technique for executing adaptive security in BYOD or in what way to offer information input for adapting security.

Research efforts of Jaramillo, Newhook, and Smart (2013) related to the security of mobile devices in BYOD. Jaramillo et al. (2013) evaluated a security model that harmonizes software ecosystems and several heterogeneous mobile devices into a solitary flexible network for message dissemination and organization mobile device

management. This security model offers a basis for consideration of many security, energy, and connectivity challenges that are very dissimilar from issues inherent in a conventional organizational system (Jaramillo et al., 2013).

Saa et al. (2017) employed a pedagogical perspective in studying the adoption of BYOD in educational environments. Saa et al. (2017) research showed a vibrant knowledge of how an institution of higher learning can be unsympathetically affected if they permit mobile devices in classes by a student, and on the flip side, the issue of students worrying about being watched via their mobile devices by an employee of the university. Their research outcome showed that lots of students believe that a BYOD policy could help enhance learning methods in computer science-based programs.

As more corporate organizations adopt Bring Your Own Device (BYOD), the usage private networks for business dealings presents dangers such as illegal disclosure of corporate organizations employee's information or business details as depicted in Figure 1. Similarly, as BYOD initiatives and mobile device flexibility rise in the places of work, security concerns also increase (Shridhar, 2017). As depicted in Figure 2, data leakage or loss constitutes 69% of the principal security challenge to BYOD, the effect of malware on the organization's IT networks (63%) and download of insecure content or applications (64%) (Shridhar, 2017).

Tanimoto et al. (2016) discussed the risk evaluation of BYOD in a corporate organization. They explicitly evaluated risks that are integrated within the BYOD framework with a risk management technique such as risk matrix and risk breakdown

structure (RBS). Also, this assessment will support and add to the security, safe growth and advancement of BYOD in an organization (Tanimoto *et al.,* 2016).

The Bello, Murray, and Armarego (2017) systemic investigation focused on BYOD adoption, and its associated risks and mitigation strategies, investigating how both security and privacy of information can be efficiently attained in BYOD networks. Bello et al. (2017) expanded previous study investigating BYOD practices and provides a current best practice approach that can be used by organizations to systematically investigate and understand the manner in which privacy and security risks can be managed within a BYOD network.

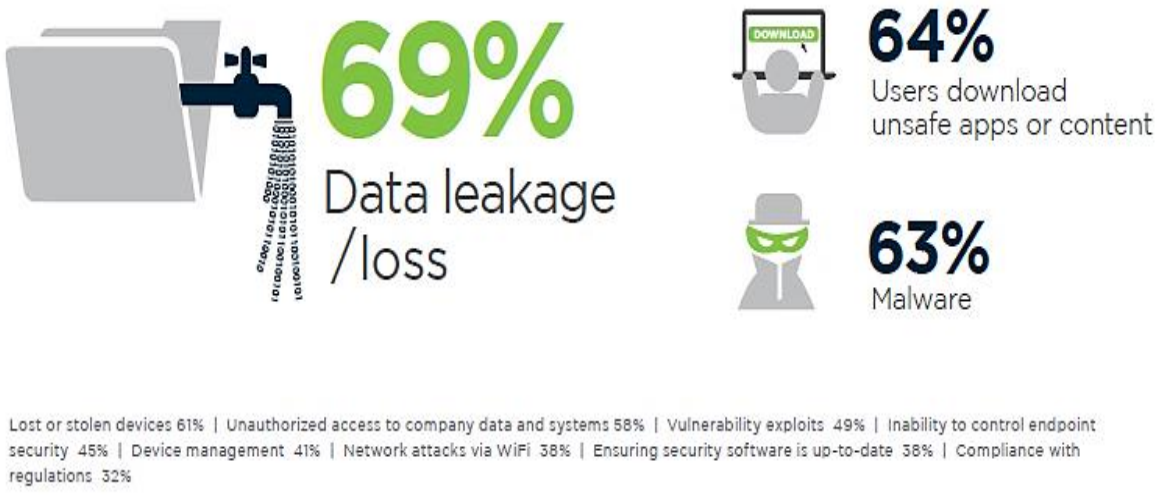

Figure 2. Main Security Concerns of BYOD (Shridhar, 2017)

Summary

There are vast research papers on BYOD with a view of creating awareness on the risks and benefits inherent in BYOD policy adoption and usage. This chapter presented the background, literature, and significance of this study. The concrete

methodology adopted for this research is discussed in the next chapter which would collaborate the guidelines for effective and secure adoption and use of BYOD.

Chapter III: Methodology

Introduction

This chapter describes the procedure or methodological concepts employed in capturing BYOD security and privacy risk and attacks by carrying out a review of literature from valued journals on research efforts by scholars in IT security.

Design of the Study

Despite the numerous benefits and advantages of BYOD adoption, users and adopters are still unaware of some the security issues and challenges of BYOD should that be examined before adopting BYOD. The qualitative research approach was used to identify the problem of this study by way of classification of data that can be converted into a functioning and working BYOD guidelines.

Table 2

Research/Study Questions Methodology

Research Questions	Approach/Design
Define BYOD and its advantages?	Study the existing research work from academic research databases like Springer, IEEE Xplore Digital library, Research Gate, Science Direct, Google Scholar and Semantic Scholar.
What are the privacy and security risks, threats, weakness and attacks that are intrinsic in the BYOD framework?	Study existing reports, the latest security breaches, etc.
What are the causes of these security and privacy risks, threats, vulnerability, and attacks?	Research existing reports, the latest security breaches, and research work from other scholars
What possible control measures or solutions should be considered for confronting BYOD policy from risks, threats, vulnerability and attacks to information security and privacy?	Research various BYOD models or solutions and generate a checklist of possible control measures using a layered approach of data, device, application, and people.

Data Collection

Information for this study was collected using purposive sampling. Purposive sampling was used to subjectively look for information relevant to the research variables of security and privacy risks inherent in BYOD framework. This research study searched and reviewed the literature on Bring Your Own Device (BYOD) relating to security and privacy risks, attacks, policy, challenges, checklist, and guidelines. Reference materials were analyzed from academic research databases like Springer, IEEE Xplore Digital library, Research Gate, Science Direct, Google Scholar, and Semantic Scholar. In addition, other sources like Gold Certified research papers from SANS, peer-reviewed articles, and journals, conference papers and presentations, government publications (bulletins), publications from research organizations, survey reports, publications from service providers, BYOD framework publications and news articles were also exploited in the course of this study.

Tools and Techniques

For this study, the following tools, standards, and techniques were utilized in the collection and analysis of data.

NIST FIPS Publication 199

“Federal Information Processing Standards (FIPS)” publication offers vital crop of rules that defines information systems and technology standards and information encryption algorithms and processing for use within government agencies, vendors and other contractors who worked directly or indirectly for various government establishments. FIPS ideals and rules are dispensed to create requirements for numerous reasons like ensuring interoperability and computer information security and

are envisioned for instances where appropriate industry values or standards are not in existence (National Institute of Standards and Technology, 2004).

This publication by the National Institute of Standards and Technology (NIST) was very instrumental towards the identification and classification of the impact of the common BYOD security and privacy risks/threats or attacks on BYOD layered approach architecture components of data, device, applications and people into security objectives of integrity, confidentiality and availability according to FIPS ideals for security classification of “Federal Information and Information Systems” grounded on Federal Information Security Management Act (FISMA). FISMA is a United States law enacted to define an all-inclusive approach to safeguard government operations, assets and information from threats and risks which can be man-made or natural (National Institute of Standards and Technology, 2004).

According to FISMA, three (3) security objectives for data/information and its systems are defined as follows:

Confidentiality:

> “Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information.”

Integrity:

> “Protecting against improper information modification or destruction and includes ensuring information non-repudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information.”

Availability:

"Ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information or an information system."

FIPS Publication 199 defines three levels of potential impact on organizations or individuals should there be a breach of security (i.e., a loss of confidentiality, integrity, or availability) (National Institute of Standards and Technology, 2004). The forfeiture of confidentiality, integrity, and availability predictably could take adverse effect on BYOD layered approach architecture components (device, applications, data and people).

Layered Approach of BYOD Framework

This study followed a layered approach as depicted in Figure 3 to recommend solutions that could be applied by organizations &and users to mitigate BYOD security and privacy risks/attacks and vulnerabilities. Business rule of the proposed layered approach of BYOD framework explains the dependency of different layers. This concept of layered approach also provides measures or conditions for making decisions on how possible solutions can be useful in resolving security and privacy risks of BYOD policy implementation as a result of IT consumerization. It is worthy to note that without people layer is dependent on the device layer, the device layer is dependent on the applications layer, while the applications layer is dependent on the data layer. This layered approach is designed to help identify and encapsulate security and privacy risks inherent in the different layers of BYOD framework.

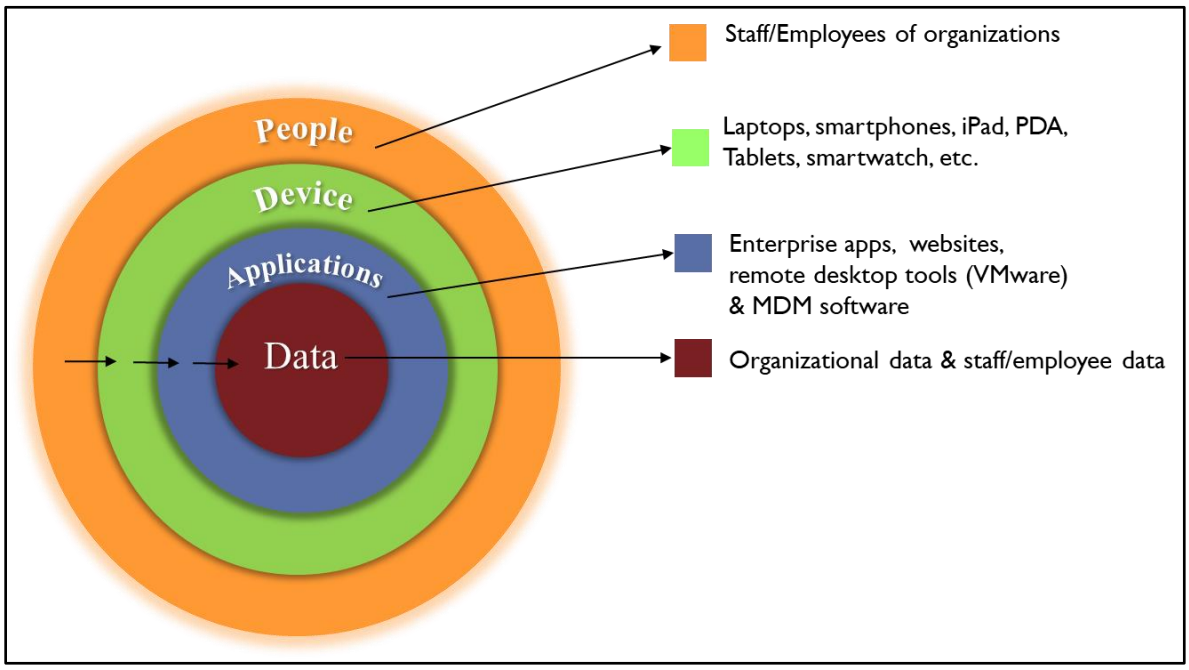

Figure 3. Layered Approach of BYOD Framework

The layered approach diagram (Figure 3) in this study portrays a characteristic attempt at integrating all the possible BYOD security and privacy risks solutions or measures into a single actionable idea. Each of these layers exposes the inherent or possible security and privacy risks, threat and attacks of BYOD framework. The Layered Approach of BYOD Framework is divided into four layers:

Data layer*:* This is the innermost layer which comprises the organizational data and end-users data, for instance, messages (e-mails and text, picture, and voice messages) files, etc. This layer presents data created, accessed or retrieved, modified, communicated, saved or used via a mobile device by an organization or its employee. This determines various types of data that can be accessed through the device and applications layer by different category of people in the people layer. Data in the BYOD framework is indispensable to an organizational objective and requires security and

privacy protection to meet legal and regulatory requirements for a successful BYOD policy implementation.

Applications layer*.* This layer comprises of the software (VMware, web apps, customized apps, firewalls, etc.) that are used to process data into information for organizational and end-users usage. The applications encompass security controls, irrespective of the device used for access to data. This layer harbors the responsibility of determining and reviewing all software/apps that are accessible through device layer to guarantee they conform with security and privacy standards and policy (e.g., storage limitations, encryption conditions, access permissions) that protects the components of the data layer. To ensure compliance in BYOD framework, the management and human resources of an organization will deploy a Mobile Device Management (MDM) tool which must align with the set standards and policies of the companies for monitoring to manage and control the functionality and operations of the employees/staff in the people layer.

Device layer: This layer is next to the outermost layer. It comprises moveable devices such as smartphones, laptops, iPads, personal digital assistant, tablets, smartwatch, etc. that are used to access applications or programs in the application layer for data processing. Mobiles devices in this layer need a cumulative variation of security and privacy controls due to the increased flexibility, functionality, choice and possibility of routine replacement of these mobile devices. In this layer, it is expedient to ensure that the types of mobiles devices that are used to access data, and how mobile

devices are secured to protect data or information to meet the requirements for security objectives in a BYOD framework.

People layer: This layer is the outermost layer which is made of organizational staff/employees that access and process data through the application layer via a diversity of mobile devices like laptops, smartphones, iPads, personal digital assistant (PDA), tablets, smartwatch, etc. The organizational staff/employees in the people layer require regular training and communications on the characteristic risks/threats, policies, standards and tools for securing the availability, confidentiality and integrity of data or information in within a BYOD framework.

Zotero

Zotero is a unique research computer application tool built for reference management. It allows users to acquire references from internet sources such as journal article webpage with a sole click, it then organizes them and uses the captured data to produce bibliographies and citations (Strothmann, 2018). The Zotero app is an easy and free tool. Zotero suggests to its users numerous of paths to generate, import and store data, files and information (Zotero, 2018). Zotero is most operative when used from the beginning of the writing of a research project. Zotero offers a book-length guide which apparently may be pointless to some users who like to explore computer applications on their own but this guide can be seen as one of the program's assets is its spontaneous interface (Strothmann, 2018); nevertheless, the new version of *Zotero: A Guide for Librarians, Researchers and Educators* (Fronk, 2018) is nonetheless to be treasured for the meticulousness employed in explaining the program's functionality. After going through the process of downloading, setting-up and adding Zotero to a word

processor such as MSWord, Zotero tool offers a power-driven and fascinating experience on data collection for a research literature review. to search for publications and articles that is related to my research problem. With Zotero, this study was able to collect data and information from journal articles, books and websites that are related to the research problem with one click and then archives related web links, PDFs and other files together with that data stored in Zotero collection. For beginners, it offers a clear, approach with directions to every Zotero's main functions, demonstrated with all-embracing screenshots (Strothmann, 2018). Below are some exciting tasks this study was able to achieve with Zotero that made data collection and analysis easier:

- Automatically capture bibliographic information from the web
- Archiving web pages
- Organizing and annotating items
- Finding and searching in Zotero
- Creating bibliographies in a word processor
- Expediently exports Zotero library or collection from one computer to the other and access your library from another computer.

Summary

This chapter offered a detailed design of this research effort. Purposive sampling was employed to subjectively look for information relevant to the research variables of security and privacy risks inherent in BYOD framework. The layered approach concept of data or information collection would be valuable and significant to a researcher with

similar research interest because conforming to the methodology used in this study is not difficult and could save researchers some time and effort forward.

Chapter IV: Presentation of Data and Analysis

Introduction

This chapter provides a thematic presentation and analysis of data and information collected from different literature domains search to identify and classify the impact of the risks, attacks, and vulnerabilities on BYOD using a layered approach. The classification process of risks, threats, and vulnerabilities is created using the “FIPS” standards for security classification of “Federal Information and Information Systems.” Also, this chapter presents a checklist of control measures that could be applied by organizations and users to mitigate BYOD risks, attack and vulnerabilities using a set layered approach of data, device, applications, and people as described in Figure 3.

Data Presentation

Data collected from this study was based on the effort of researchers in the field of BYOD security and privacy. This study identified possible BYOD risks, threats, and attack and suitable control measures to mitigate them using a layered approach of data, device, applications, and people. One hundred and ten academic research publications were chosen based on their abstracts and titles for this study. Correspondingly, the articles at that point were read and examined to define their importance. The remaining publications that were not applicable to this investigation were expunged. This investigation yielded 26 articles (Appendix A) that are important were identified and analyzed for security and privacy risks or attacks related to BYOD policy challenges as depicted in Figure 4.

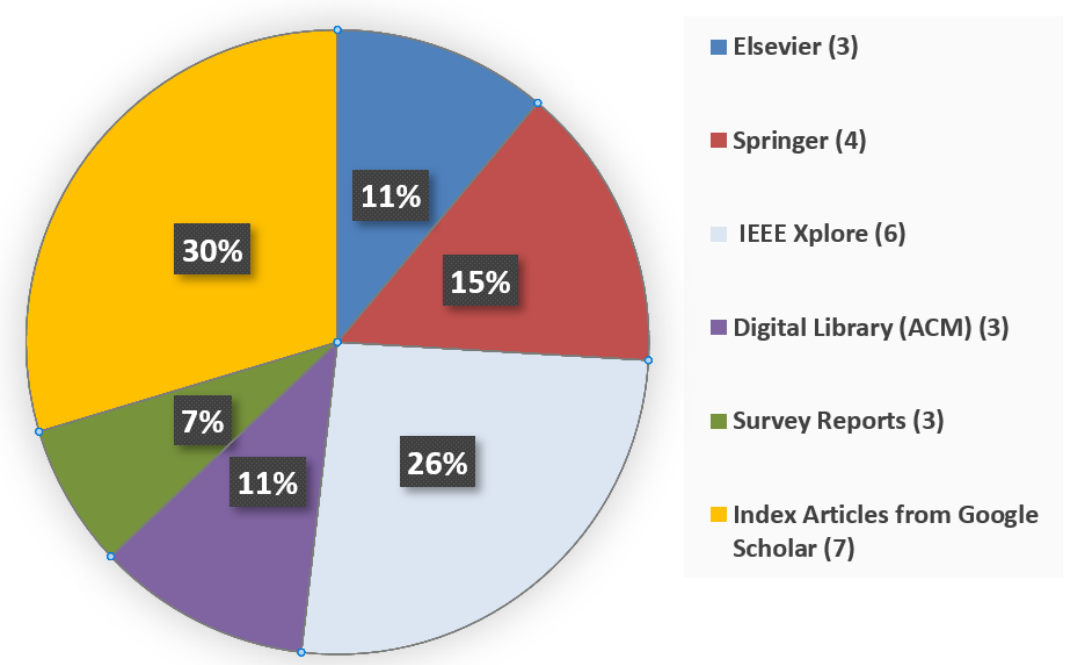

Figure 4. Proportion of Publications Chosen from Several Literature Database

Based on the data collected, common security and privacy risk, threat and attack impact on BYOD layered framework were presented in Table 4. Furthermore, this study followed a layered approach as depicted in Figure 3 to recommend solutions that could be applied by organizations and users to mitigate BYOD security and privacy risks, threat, attacks and vulnerabilities as shown in Tables 4, 5, and 6.

Table 3

Common Security and Privacy Risk, Threat and Attack Impact on BYOD Layered Framework.

Potential BYOD concerns	Data	Device	Applications	People
Advanced Persistent Threat (APT attacks)	X		X	X
Attack to back-end infrastructure to steal data/info		X		X
Bluetooth infection		X		X
Cryptocurrency mining	X	X		X
Data compromise/contamination	X			X
Data Deletion	X			X
Data exfiltration	X			X
Data Exposure (e.g. organizational data breach)	X			X
Data interception	X			X
Data loss/leakage	X			X
Data Modification/alteration	X			X
Data sniffing	X			X
DDoS attacks (Bandwidth issues)			X	X
Distribution of malicious code	X		X	X
Download illegal content (e.g.; unsafe app, malware)	X		X	X
Exposure to untrusted and malicious apps	X		X	X
Exposure to untrusted and unsecured networks	X		X	X
Identity theft (e.g., impersonation, fraud)	X			X
Poor authorization and authentication		X		X
Identity theft (e.g. impersonation, fraud, etc.)	X	X		X
Crypto-jacking, broken cryptography	X		X	X
Inadequate BYOD awareness				X
Informal BYOD adoption				X
Insecure usage e.g. phishing				X
Instantiation DDoS attack		X	X	X
Interactions with other untrusted and unsecured systems	X	X	X	X
Unreliable MDM solution purchases				X
Litigation & liability issues	X			X
Reduced technical controls		X		X
Privacy exploitation via hacking	X		X	X
Sale of data	X			X
Secure socket layer attacks		X	X	X
Social engineering attacks	X			X
SQL injection attacks	X			X
Steal company trade secrets	X			X
Support & maintenance issues		X		X
Targeted attacks through router/Wi-Fi	X	X		X
Virus or malware infection	X		X	X
Workplace deviant and illegal behaviors of employee				X

Table 4

A Layered Approach to BYOD Device Theft/Loss Potential Attacks

BYOD S&P Issues		Potential Attacks	C	I	A	Layered Approach
Device theft/loss	User	Data Exposure (e.g. organizational data breach, access to a network connected to devices)	X			• **Data:** Trigger data back-up & remote device wipe. Also, containerize data to protect and segregate organizational data from personally-owned data on BYOD devices. Restrict access privileges. • **Device:** Change the mobile device password regularly, limit access to the device and enforce device lockdown. Also, enforce authentication of password/passcode requirements, encryption & Screen locking settings. Create default plain text message-sending format and reading format. • **People:** Users must accept BYOD policy terms regarding information usage for device theft issues • **Applications:** Determine which types of apps are off-limits, enable phishing filter capabilities, block popup windows and avert automatic recall of passwords on a website. Also, run web apps with the least privileges possible.
		Data Deletion			X	
		Data Modification		X		
		Insecure usage e.g. phishing	X	X		
		Cryptocurrency mining		X		
		Download illegal content (e.g. unsafe app, malware)		X		
		Identity theft (e.g., impersonation, fraud, etc.)	X	X		
	Organization	Data Exposure (e.g. organizational data breach, access to network-connected devices)	X			• **Data:** Enforce encryption of data at rest, trigger data back-up & remote device wipe. Containerize organizational data. • **Device:** Increase the variety of security controls due to the increased mobility, choice, functionality, and replacement of BYOD devices • **People:** Carry out an information security risk assessment, set expectations clearly by defining policy terms regarding information usage for device theft issues regarding information usage for device theft issues. Provide training/support sessions dealing with a wide range of digital security threats associated with device theft/loss. • **Applications:** Deploy mobile device management (MDM) system covering all employee devices. Configure applications to support security. Deploy a secure VPN to keep data safe from data modification/deletion.
		Data Deletion			X	
		Data Modification		X		
		Fraudulent attacks	X			
		Instantiate DDoS attack			X	
		Data sniffing	X			
		Illegal Cryptocurrency mining e.g. crypto-jacking	X			
		Virus or malware infection		X	X	
		Attack to back-end infrastructure to steal information		X		
		Distribution of malicious code		X		

Note: *C = Confidentiality, I = Integrity and A = Availability.*

Table 5

A Layered Approach to BYOD Network Attacks

BYOD S&P Issues		Potential Attacks	C	I	A	Layered Approach
Network Attacks	User	Data interception	X			• **Data:** Trigger back-up of data & remote device data auto-wipe. Automatically initiate device lockdown. Containerize data to safeguard and segregate organizational information from personally-owned data/information on employee mobile devices. • **Device:** Incapacitate essential networking functionalities apart from when they are desired. Avoid jailbreaking devices. Limit access to the device. Periodically audit devices • **People:** Limit the use of remote access utilities. Install and configure antivirus software. Enable & configure content filtering on web-browsers. Use encrypted and protected networks that is reinforced and controlled by an organization to gain access the corporate services and data. • **Applications:** Keep device apps updated, employ the use of third-party plug-ins to enhance security, enable spam filtering. Determine which types of apps are off-limits, enable phishing filter capabilities, block popup windows and prevent website passwords from being recalled habitually. Only run apps downloaded from legitimate and secure app stores.
		Data Exposure	X			
		Data compromise		X	X	
		Identity theft (impersonation)	X	X		
		Bluetooth infection		X	X	
		Social engineering attacks Privacy exploitation via hacking		X	X	
		Exposure to untrusted and malicious apps	X			
	Organization	Targeted attacks through router/Wi-Fi	X	X		• **Data:** Keep your web filtering tools up to date. Enforce multi-factor authentication for verification mobile devices & its users. Containerize data to protect and segregate organizational data from personally-owned data on BYOD devices • **Device:** Ensure network segregation & segmentation for guest connection. Grant access for a specific secure wireless network. Forbid the use of rooted devices on organization's network. • **People:** Define a well-developed risk control policy for networks attacks and provide adequate training/support organization's staff. Document network attack incidents. Enforce compliance policy controls protocols. • **Applications:** Deploy virtual private network (VPN) infrastructure to keep data safe from interception. Sustain steady updates of anti-malware or firewall programs on organization's IT infrastructure with the most recent digital signatures. Always test firewall functionality to detect network intrusions. Blacklisting and whitelisting applications to modify the standard service set identifier (SSID). Also, deactivate the wireless Access point (AP) SSID broadcasts.
		Secure socket layer attacks		X		
		SQL injection attacks		X		
		Advanced Persistent Threat (APT attacks)		X		
		Data contamination		X		
		fraudulent attacks	X			
		Exposure to untrusted and malicious apps	X			
		DDoS (Bandwidth issues)			X	
		Interactions with other untrusted and unsecured systems	X		X	
		Exposure to untrusted and unsecured networks	X			
		Reduced technical controls	X	X	X	

Note: *C = Confidentiality, I = Integrity and A = Availability.*

Table 6

A Layered Approach to BYOD Control and Management issues

BYOD S&P Issues		Potential issues	C	I	A	Layered Approach
Control & Management issues	User	Data loss/leakage	X			• **Data:** Trigger data back-up & remote device data auto-wipe. Automatically initiate device lockdown. Containerize data to protect and segregate organizational data from personally-owned data on BYOD devices. • **Device:** Ensure BYOD devices conforms to security and privacy rules. • **People:** Comply with organizational security and privacy rules. Review and update BYOD policy as needed. • **Applications:** Deploy mobile device management (MGM) system covering all employee devices. Configure applications to support security. Deploy a secure VPN to keep data safe from data modification/deletion.
		Data Modification/alteration		X		
		Deletion			X	
		Sale of data	X			
		Download illegal content (e.g.; unsafe app)		X		
		Identity theft (e.g., impersonation, fraud)	X			
		Poor authorization and authentication	X	X		
		Data interception attack	X			
	Organization	Data contamination	X	X		• **Data:** Trigger data back-up & remote device data auto-wipe. Enforce auditing, Identification & access control policy establish User ID protocols. • **Device:** Ensure BYOD devices conforms to information security and privacy standards. Network segmentation & segregation to thwart attacks and unauthorized access via mobile devices • **People**: Provide technical support and Training Program. Require employees to cooperate if the organization needs to collect unique data pertaining to the subject matter of a legal hold from their personal devices. Address disciplinary action for violation of the BYOD Policy. Review and update BYOD policy as needed. • **Applications:** Deploy tested & credible MDM solution
		Vulnerability to fraudulent attacks			X	
		Data compromise	X			
		Steal company trade secrets	X			
		Data deletion			X	
		Reduced technical controls			X	
		Workplace deviant and illegal behaviors of the employee	X			
		Data exfiltration	X			
		Litigation & liability issues	X	X		
		Support & maintenance issues		X	X	
		Inadequate BYOD awareness & policy violations			X	
		Unreliable MDM software procurement	X	X	X	
		Informal BYOD adoption	X	X		

Note: *C = Confidentiality, I = Integrity and A = Availability.*

Data Analysis

The analysis of the data collected from reviewing diverse publications from various domains of literature related to BYOD security and privacy risk, threat, attacks and vulnerability, 26 papers were analyzed. Because of the complex nature of

qualitative methods, it was decided to apply thematic content analysis (Boyatzis, 1998) in this study, as it involves the classification of data into themes or patterns, as well as identifying connections and providing explanations of the themes and patterns (Bello *et al.,* 2017). The analyzed data acquired from the publications addressed: (a) device loss/stolen device; (b) network attacks; and (c) control and management, litigation issues.

These challenges bordering on BYOD policy adoption and implementation as revealed in Tables 4, 5, and 6. It is imperative to note that data acquired were also analyzed and classified by the generalized format by “FIPS standards for security classification of Federal Information and Information Systems” for communicating the security objectives category of *information type i.e. confidentiality, integrity and availability,* was used for classification as represented in Tables 4, 5, and 6.

Summary

This chapter presented a wide-ranging understanding of BYOD policy adoption by presenting an academic knowledge, challenges, benefits, security risks, attacks, threats, and effort by researchers in the area of BYOD policy development and adoption. Analysis of the qualitative data collected resulted in classifications of security and privacy risks, threats and attacks of BYOD. In addition, based on a layered approach as depicted in Figure 3, analysis of data collected resulted into a checklist of control measure or solutions that could be applied by organizations and users to mitigate BYOD security and privacy risks, threat, attacks, and vulnerabilities.

Chapter V: Results, Conclusion, and Recommendations

Introduction

In present times, more organizations now permit employee-owned mobile devices to gain access to an organizational network either remotely or within the organization's working environment. With the growing pace of advancement of mobile technology, BYOD policy has become a fundamental phenomenon and concept that is still thriving (Tu & Yuan, 2015). Thus, BYOD adoption pats several parts of people's daily life, be it economic, education or social with its numerous advantages and challenges (Boadi, Zhou, & Ioannis, 2018). Attacks to smart mobile devices can be carried out by exploiting weaknesses that may be present in the application software, operation system, system verification not appropriately set-up, personal device or server and abuse to a targeted component by users (Weintraub, 2016). The study's objective was to provide a theoretical groundwork, challenges, advantages, security risks, threats and research efforts by scholars in the area of BYOD security and privacy. This chapter gives an overall understanding of methodology and results obtained from this study. This chapter also presents the state each of the study questions, answers, and recommendation by this study.

Results

The viewpoints and the theme/classification generated from data analysis formed the foundation of the results and discussion in this research work. The research questions examined in this research are discussed with respect to the findings of BYOD literature review.

RQ1: What is Bring Your Own Device (BYOD) and its advantages?

Bring Your Own Devices (BYOD) policy denotes permitting employees of an organization to work with their own mobile devices (Olalere et al., 2015). Likewise, the perception of "consumerization" on which BYOD policy relies on describes the increasing advancement of information technologies, initially to the consumer market and then to corporation/organizations (government and private businesses) (Moreira et al., 2016). Based on literature from Olalere et al. (2015), Moreira et al. (2016), Zahadat et al. (2015), Saa et al. (2017), Song & Kong (2017), and Caldwell et al. (2012), there are many benefits of adopting BYOD policy. They are as follows:

- Increased Productivity: User being more comfortable with their personal device.
- Lowers cost to the organizations: No devices cost to the company because the employee uses his/her own device.
- New cutting-edge technology: Frequent and faster upgrades than the devices of the company. Also, BYOD makes the most of cloud technologies.
- Attract and retain talent: Using personal devices attracts talent.
- Ubiquitous access to information at any time.
- Increased customer satisfaction with users working with devices they prefer.

RQ2: What are the security and privacy risks, threats and attacks that are intrinsic in BYOD frameworks?

Security and privacy threats, risks, and attacks constitute the biggest BYOD objection worldwide. Perceived new risks and concerns associated with BYOD were

identified by organizations that did not allow BYOD and perceived and actual new risks and concerns were identified by organizations that do allow BYOD (Santee, 2017). From the employee and organization angle, what are risks, threats, and attacks in BYOD user/employee side and organization side? Tables 4, 5, and 6 illustrate the three classifications of security and privacy concerns of BYOD.

Device loss/stolen device: The theft/loss of an employee mobile device constitutes a devasting risk or vulnerability to both the organization and employee (user) when the lost device is being used to perpetrate malicious intentions such as data modification, exposure, alteration and deletion, information theft and download illegal content (e.g., unsafe app, malware) as shown in Table 5. Other potential BYOD attacks could consist of Identity theft (e.g., impersonation, fraud, etc.), data sniffing, instantiation DDoS attack, attack to back-end infrastructure to steal information and distribution of virulent codes. Many organizations' security and privacy breaches happen due to loss/theft of mobile devices. Table 5 shows potential risks and attacks that could emanate from device loss/theft to user and organization.

To alleviate these risks, a layered device infrastructure may be practical to deal with different grades of risks in some organizations. For example, mobile devices that are employed in the presentation sensitive financial information to the executive members through a customized application will perpetually be elusive to theft or loss than a mobile device that has access to receiving email. Device theft or loss depicts that organizations and its employee stand a greater risk of data/information loss or modification and alteration if appropriate control measures are not taken.

According to Donowan (2018), a medical equipment supplier based in Massachusetts reported to OCR that on September 1, 2018 a phishing attack orchestrated via a lost device of an employee exposed personal health information (PHI) of 21,311 persons. On the Reliable Respiratory company website, a notice read that on July 3 it found out a breach of an employee's email account that resulted from a successful phishing attack (Donowan, 2018). Based on an investigation by a third-party forensic specialist, the company determined that an unauthorized or barred person(s) had access to the employee email and possibly through a stolen work device between June 28 and July 2 (Donowan, 2018).

Similarly, Valley Hope Association, a Kansas-based group, reported that a laptop used for work responsibilities was stolen from an employee's vehicle on December 30, 2015 (LaPointe, 2016). Though Valley Hope Association was unable to list how many persons that were possibly affected by the security vulnerability created the device loss, however, the Office of Civil Rights (OCR) data breach tool outlined 52,076 persons that could be possibly affected (LaPointe, 2016). Also, names of patient linked with one or more private identifiers possibly would have been made visible to malicious entities (LaPointe, 2016). Data and information that might have been exposed consist of the following patient account information, medical information, medical record numbers, dates of birth, phone numbers, addresses, state identification or driver's license numbers, social security numbers, physician name, diagnoses, treatment and treatment location, disability codes, usernames and passwords, health insurance information, financial information, and tax identification numbers (LaPointe, 2016).

Network attacks: Mobile devices in BYOD framework can remotely link-up to an organization's networks from anyplace and at any time thereby placing the organizational network and conforming data at grave risk. Without proper protection, adversaries may be able to intercept corporate information or even impersonate legitimate employees and illegally gain access to networks and services (Vorakulpipat et al., 2017).

Unsafe networks can be problematic for any device in BYOD framework, as data transmitted via unsafe Wi-Fi networks are transmitted in an unencoded format which can be intercepted and opened by unauthorized persons linked directly or indirectly to that network. Wi-Fi or Bluetooth can simply be used to transmit malicious code/app to mobile devices (Gajar, Ghosh, & Rai, 2013). Wi-Fi or Bluetooth connections has the possibility of being intercepted by a malicious individual if these connections do not possess strong firewall from the connected devices. This could result in the theft of enterprise data and information. Insecure connections could pave way for rogue apps by an attacker which lead to denial of system services for genuine employee or users and organization's executives. IT professionals need to focus on a mixture of device security, layered protection and smarter provision in a bid to protect mobile endpoints network from exposure (Oyo-Ita, Utoda, & Asuquo, 2018). Some third-party application in 2017, was blamed for massive cryptocurrency breach of a cryptocurrency exchange company (Bithumb) in South Korea (Goldman, 2017). This breach was orchestrated by a hack attack via a computer in a Bithumb employee's house and about 30,000 customers' information was exposed in this attack (Goldman, 2017).

A potential entry point towards infecting mobile devices is through high-risk application or malicious application that acquire mobile device information and parades unsolicited adverts without the user's accord (TREND MICRO, 2015). An application with malicious intent may possess the capacity to sniff, alter, or snip inter-application communications thereby contaminating trusted apps on the mobile device as well as apps from authorized app stores may be infected. To this end, enabling location-based services or allowing push notifications should be discouraged. For instance, in 2015, a malware targeted developers' tool sets was created to infect iOS apps in the Apple app store (Hoelscher, 2017). To this end, it was reported that Apple Inc. removed well over 300 apps from the app store (Hoelscher, 2017).

Users or employees of organizations that employ the BYOD framework can compromise your BYOD network security and privacy by:

- *The Use of Weak Passwords.* An employee on BYOD framework that uses a password such as "123456" or "football" or "abcdfe" can easily grant access to a hacker thereby gaining access or control of an organization's network and treasured business data. Truthfully, it barely takes less than 10 minutes for a hacker to break a password in all lowercase of six alphabets.
- *Engaging in Social Media While at Work*. Virtually all employees of organizations implementing BYOD are possibly whiling away some time at work accessing Twitter, WhatsApp, Facebook, Snapchat, and other social media sites. In addition, employees via their mobile device might also

unintentionally post or transmit sensitive organizational information on these social media sites.

- Phishing. This is a deceitful tactic of sending emails claiming to have originated from a trustworthy organization with the sole aim of inducing people to disclose private information like bank account number, credit card numbers, social security number, and passwords. Some employees who work with their mobile device can jeopardize their organization network security is by opening an email sent by a fraudster. Cybercriminals frequently penetrate organizational networks through phishing drives. Social engineering attack methods and phishing can also be used to deceive BYOD users into downloading malware on their devices or trick them to divulge confidential information (Singh et al., 2014).

The use of weak passwords, engaging in social media while at work and phishing challenges increases the risk of an unauthorized individual gaining access to delicate information of an organization.

Control and management, litigation issues. Manager managers of organizations may not fully comprehend the probable security risk BYOD adoption brings to an organization because it is a new phenomenon and may not be cognizant of the types security measures that should be put in place to efficiently safeguard organizational information (Tu & Yuan, 2015). Owing to the different mobile devices that operate on various networks, vigilant deliberation must be made on the willingness of an organization to manage and control the issues that may arise from cross-platform

compatibility (Oyo-Ita et al., 2018). With unmanaged and unregulated BYOD devices, an employee or user that has an unregulated pass into organization network could carry out malicious or fraudulent activities thereby compromising or exposing the organization's business information.

There are potential risks linked with loss of control of any mobile device, be it company or employee-owned (Oyo-Ita et al., 2018). When an employee with a mobile device that is used for work walks out of the organization premises, it can obviously be problematic to regulate the type Wi-Fi connections the employee used to access the organization's network resources. Shielding laptop and mobile endpoints from compromise and exposure entail IT professionals to concentrate on a mixture of mobile device security, smarter provision and layered protection (Oyo-Ita et al., 2018).

A healthcare information/data breach in Washington on February 10, 2016, was orchestrated as a result of an employee error which resulted in the compromise of Medicaid patient files of 91,000 individuals (Heath, 2016). This information was gathered from the released statement by the Washington State Health Care Authority (HCA) explaining the data breach which happened after an employee of HCA mal-handled information of patients from a provider of free healthcare - Apple Health (Medicaid), for low-income people (Heath, 2016). Information jeopardized allegedly includes Apple Health client ID numbers, patients' social security numbers, private health information and dates of birth. Both individuals involved had their employment terminated. In addition, Steve Dotson (HCA Risk Manager) explained that their organization has no suggestion that their client files went outside the two employees

implicated, significant privacy laws were desecrated, and adequate thoroughness was given to the type of the information exposure (Heath, 2016).

In addition, a key contributor to several security and privacy risks that most organizations experience is lack of training/awareness of user/employee. Upholding a tradition of conducting routine awareness and training for handling device loss and other risks is vital to the security and privacy of organization business information.

In case there is litigation linking an organization that adopts BYOD policy, employees' mobile devices might be subjected to investigation. Regulations obviously vary from country to country, however, the unique regulation that all regions must have in common is that every employee must give clear and well-versed consent for their organization to access to employee personal data (Saa et al., 2017). In healthcare, there are strict legislative regulations that adopters of BYOD policies must obey when handling personal health information of patients. For instance, the Personal Health Information Protection Act (PHIPA) and other associated laws in Ontario, Canada, provides severe rules, as well as substantial penalties that are charged every time an organization's mobile device is stolen (Inside Counsel, 2013).

RQ3: What are the causes of BYOD security and risks, threats, vulnerability and attacks?

The results from the theoretical study revealed the BYOD issues depicted in Tables 4, 5, and 6 and as identified in the literature review. The outcomes from the review expose the numerous risk and attacks linked with BYOD in the fields of identification and access control, onboarding, communication, risk control, application

control, maintenance, and compliance. The underlying causes of BYOD risks, threats, vulnerability, and attacks are identified as follows:

- **Absence of policies.** Bello et al. (2017) recognized that though there are still organizations which do not have BYOD policies in existence, the ones which have a policy had exceptions for enforcing them on certain users or devices and treated BYODs as corporate-owned. To this end, organizations and employees are ever more susceptible to confidential data leakage or loss and compliance problems.
- **Policy violation***.* User policy violations can easily expose BYODs to numerous vulnerabilities (Masin, 2013). Therefore, technical control and user/employee access to organizations' IT infrastructure should be defined by the security objectives of availability, integrity and confidentiality.
- **Inadequate security controls***.* Based on previous investigation by researchers from literature like Bello et al. (2017), employee survey report showed that 75% of organizations did not direct BYOD users/employees to apply any counter or control measures on their mobile devices, such as password authentication, lock-screens, activating passwords, fixing of security software and making routine operating system updates.
- **Malicious insiders***.* BYOD users/employee that are malicious insiders can execute threats (Brdiczka et al., 2012) because they are employees and possess access to organizational IT infrastructure systems anytime and anywhere.

- **Inadequate security and privacy awareness**. According to Bello et al. (2017), some employees of organizations that deploy BYOD policy were found to lack knowledge of IT personnel to contact or preventive measures to take when their devices are exposed to risks or infected. Similarly, while some employees were uninformed of the level of privacy authorized to them in BYOD, the surveyed organizations have likewise botched to enforce the privacy levels of each employee. Furthermore, the organizations confirmed that BYODs have been lost and stolen and infected with viruses and malware. Confidential or private information have similarly been exposed and hackers exploited this vulnerability to orchestrate network attacks, identity theft, data sniffing and cyber-stalking through BYOD mobile devices.
- **Ineffective management issues**. Guan (2012) and Harris, Patten, and Regan (2013) research efforts reported a growth rate that is of concern for the inadequate availability of effective BYOD policies, standards, and procedures. The Bello et al. (2017) survey reported that senior management employee response from one of the case organizations surveyed showed the deficiency of effective policies that could be adopted to achieve optimum BYOD policy implementation. In this vein, the lack or deficiency of effective BYOD policies can result in some BYOD information security and privacy breach originating from the download of torrent files and infected mobile devices. Robust effective BYOD policies and measures must be readily made available to administer BYOD set standards and practices to prevent data or information

leakage and confidential data loss which could compromise BYOD policy effectiveness in the event of an attack through BYOD mobile devices.

RQ4: What possible control measures or solutions should be considered for confronting BYOD policy from risks, threats, vulnerability and attacks to information security and privacy?

In view of the increasing number of risks orchestrated with BYOD adoption, organizations should re-scrutinize the efficacy or worth of their organization's information security and privacy infrastructure over a variety of BYOD fundamental components which include: processes of identification & access control, onboarding, communication, risk control, application control, maintenance and compliance. Information security and privacy control standards encompass the "management, operational and technical safeguards/countermeasures prescribed to protect the confidentiality, integrity and availability of a system and its information" (National Institute of Standards and Technology, 2013). According to the review of BYOD literature by Garb, Armarego, Murray, and Kenworthy (2015), Dedeche, Liu, Le, and Lajami (2013) and Rivera, George, Peter, Muralidharan, and Khanum (2013), various security and privacy control measures that re-enforce BYOD management effectiveness in organizations were identified. The Bello et al. (2017) literature research review and the survey report acknowledged fitting BYOD control measures. The Bello et al. (2017) analysis were directed towards diverse control concepts for BYOD concerning the creation of unambiguous policies/procedures, device management, data control, employee access control, and network control. Apparent formation of information

systems security and privacy guidelines appeared as the principal measure to checkmate BYOD attacks, while also integrating other control methods for BYOD risk and attacks. Technical controls such as virtualization and containerization, in addition to awareness creation and training programs, BYOD-user perception and behavioral effects require consideration. Consequently, in view of the presented data in Table 6, this study proposes a layered approach to BYOD control and management issues.

Conclusion

Bring Your Own Device policy security and privacy potential problems assessment is a significant move towards safeguarding the effective BYOD adoption, implementation, and management of confidential information in its framework. This work proffers unambiguous understanding of BYOD security risks and threats to adopters and users by (a) identification and classification of possible list of threats/vulnerabilities of BYOD adoption and (b) identification and classification of impact on the threats/vulnerabilities of BYOD based on security objectives of availability, confidentiality and integrity, and presentation of a checklist of measures that should be applied by organizations and users to mitigate BYOD risks using a layered approach. Theoretically, this academic research effort has addresses foundational resources that buttress the understanding and identification of BYOD policy security and privacy risks, threats and vulnerability. According to the results of this study, notwithstanding that Bring Your Own Device is an influential idea with the vast potential to strengthen productivity and effectiveness, organizations should adopt policies, procedures, and standards that have the most fitting technical controls to avert organizational and

employee loss of confidential information. Technically, it is expected that the contribution of this research by implementation will be advantageous to employees/users and organizations that use BYOD policies in the course of accomplishing its organizational goals.

Recommendations

To create a holistic and effective BYOD framework that ensures the security and privacy objectives of confidentiality, integrity, and availability of information, BYOD architecture must elucidate the fundamental policies and standards of on-boarding, risk control, communication, application control, identification and access control, maintenance and compliance. Adopting and implementing an effective BYOD program is a responsibility that is not only restricted to IT network administrators but also it is a responsibility that should be undertaken by the organizations and its employee in general. Intrinsically, an all-inclusive BYOD policy is required to ensure that the program is not only efficacious but likewise secure. Here are some recommendations to aid organizations with their BYOD adoption and implementation.

Policy Considerations

Employee training on security and privacy awareness. Appropriate BYOD policy creation and employee training are vital to securing organization information technology infrastructure. Without adequate security and privacy consideration, cost of managing BYOD project could constitute a major problem. This will warrant organizations adopting BYOD to invest more time creating awareness and training on how their employees can secure their mobile devices from BYOD risks and attacks.

Furthermore, Employees of organizations should be encouraged to report challenges they may have with their devices. A grave risk or vulnerability might develop in light of unreported malware, virus attacks and data breach, while attacker remains sneakier and persistent in their methods of attacking mobile devices.

Routine risk audit. As most organizations adopt BYOD policy, mobile devices become channels for flow of information. It becomes imperative that organizations BYOD framework is audited routinely to check for vulnerability and apps that do not meet BYOD policy security and privacy requirements of centralized management, auditability, and reportability.

Regular policy update. Proper BYOD framework of organizations should enforce review and update of security policies for remote access, a virtual private network (VPN), web applications such as customer relationship management software, email, and portals. In addition, all mobile devices should have updated operating systems, strong antivirus software and web browser before connecting to the organization's IT network.

Enforce the authentication mechanism. The practice enforcing the use of robust and secure passwords by employees to gain access to an organization's IT infrastructure should be encouraged. Enforcement of two-factor authentication and personal identification number (PIN) mechanisms are the most reliable ways to achieve identity authentication. Also, devices of all employees need to be registered by the IT unit of organizations.

Enforce encryption of data. Enforcement of encryption of organization's data will prevent a data breach, data modification, and data exposure, as a result, the increased trend of device theft/loss. Mobile device theft is a major security concern for organizations. To this end, organizations should ensure that their employee secures their devices with a password lock because of any application that downloads and stores data on a mobile device should safeguard that data in the event of cracked PIN or passcode attack by a hacker.

Mobile Device Management Software Consideration

Mobile device management (MDM) tool is software that permits organizations' IT administrators or professional to enforce policies, regulate and secure mobile devices that are capture in a BYOD framework of an organization. Mobile device management software is a fundamental part of enterprise mobility management (EMM) software which has component features of identity authentication, access supervision and BYOD framework data sync and share.

MDM was developed to enhance security and functionality of mobile devices within BYOD framework while concurrently safeguarding organizational network. The producers of mobile devices and programmers of mobile operating systems determine what mobile device management software can accomplish on their mobile devices through their application program interface (API). Consequently, mobile device management software has turned out to be an essential product, with most software merchants selling MDM applications with a comparable set of fundamental features.

Characteristic features of mobile device management software include:

- organizational app store
- mobile device inventory
- mobile device tracking
- data encryption enforcement
- password and personal identification number enforcement;
- remote wipe
- app/website blacklisting and whitelisting

Operation mechanics of mobile device management (MDM). The functionality of the mobile device management software depends on enterprise mobility software such as VMware and a mobile device management server that is hosted in a data center - either in the cloud or on the premises of an organization. BYOD policies are configured via the mobile device management server's administration console by system administrators. Subsequently, the policies are transmitted by the server to the enterprise mobility software on the mobile device. The MDM agent or enterprise mobility software enforces the policies to the mobile device by interacting with application programming interfaces (APIs) deployed straight into the mobile device operating system. In the same way, through the MDM server, system administrators can deploy applications to monitor and control mobile devices.

This study, therefore, recommends the deployment of a Mobile Device Management (MDM) software to ensure the security of both organizations' and employees' mobile devices. It is imperative for an organization who wish to implement

BYOD policies to consider mobile device management software that has the capacity to secure organizational and employee applications like email and web browsers. Also, MDM software should have configuration, monitoring, remote wipe capability and over the air device application distribution capacity.

Mobile device management software may have its flaws; however, the significant benefits outweigh its risk. Therefore, appropriate and well-structured use must be accomplished to address the privacy concerns of the Bring Your Own Device policy implementation.

Moreover, corporate firms could also employ the use of a virtual private network (VPN) to permit employees that remotely to access organizational IT infrastructure, however, organizations need to apply caution in reaching this goal to avoid network attacks like SQL attacks, advanced persistent threat and cross-site scripting attacks.

Future Work

Future work will take its bearing from the outcomes and findings recognized through the data analysis stages in this academic research effort. A theoretical qualitative study cannot identify all possible security and privacy risk concerns of BYOD to both organizations and its employees. Holistically, this is exclusively accurate since various organizations or corporate organization have numerous information security and privacy requirements. Therefore, a quantifiable investigation will be very significant to evaluate this study through a survey to capture employee and organizations perception of the level of implementation, acceptance, and security and privacy compliance of BYOD policy in recent times.

Obviously, as the privacy phobia for BYOD policy adoption seems to be growing among employee or users, many organizations are yet to adopt a complete BYOD program. When it comes to BYOD policy security and privacy risk assessment, there is still much to be done. There is the need to develop a semantic based solution for security assurance in BYOD.

References

Alotaibi, B., & Almagwashi, H. (2018). A review of BYOD security challenges, solutions and policy best practices. In *2018 1st International Conference on Computer Applications Information Security (ICCAIS)* (pp. 1-6). doi.org/10.1109/CAIS.2018.8441967

Amoud, M., & Roudies, O. (2017). Experiences in Secure Integration of BYOD. In *Proceedings of the 7th International Conference on Information Communication and Management - ICICM 2017* (pp. 127–132). Moscow, Russian Federation: ACM Press. https://doi.org/10.1145/3134383.3134394

Ballagas, R., Rohs, M., Sheridan, J. G., & Borchers, J. (2004). BYOD: Bring your own device. *Procedia Technology*, *9*, 43-53. Retrieved from http://www.vs.inf.ethz.ch/publ/papers/rohs-byod-2004.pdf

Bello, A. G., Murray, D., & Armarego, J. (2017). A systematic approach to investigating how information security and privacy can be achieved in BYOD environments. *Information and Computer Security*, *25*(4), 475-492. doi.org/10.1108/ICS-03-2016-0025

Boadi, P. M., Zhou, S., & Ioannis K, K. (2018). Current BYOD security evaluation system: Future direction. *Journal of Information Technology & Software Engineering*, *8*(3), 1-6.

Boyatzis, R. E. (1998). *Transforming qualitative information: Thematic analysis and code development*. Thousand Oaks, CA: Sage Publications, Inc.

Brdiczka, O., Liu, J., Price, B., Shen, J., Patil, A., Chow, R., Bart, E., & Ducheneaut, N. (2012). Proactive insider threat detection through graph learning and psychological context. *IEEE Symposium on Security and Privacy Workshops (SPW)*, IEEE, San Francisco, CA, pp. 142-149.

Caldwell, C., Zeltmann, S., & Griffin, K. (2012). BYOD (bring your own device). *Competition Forum, 10(*2), 117-121

Dedeche, A., Liu, F., Le, M., & Lajami, S. (2013). *Emergent BYOD security challenges and mitigation strategy*. Melbourne, Australia: The University of Melbourne.

Donowan, F. (2018). *Reliable respiratory says phishing attack affected 21k individuals*. Retrieved from https://healthitsecurity.com/news/reliable-respiratory-says-phishing-attack-affected-21k-individuals

Downer, K., & Bhattacharya, M. (2015). BYOD security: A new business challenge. In *Smart City/SocialCom/SustainCom (SmartCity), 2015 IEEE International Conference* (pp. 1128-1133).

Ekpo, I. E., & Fournier-Bonilla, S. D. (2018). The Bring Your Own Device Trend in an Oil and Gas Sector. In *2018 IEEE Conference on Multimedia Information Processing and Retrieval (MIPR)* (pp. 218–219). Miami, FL: IEEE. https://doi.org/10.1109/MIPR.2018.00052

Fani, N., Solms, R. V., & Gerber, M. (2016). Governing information security within the context of #8220: Bring your own device in SMMEs #8221. In *2016 IST-Africa Week Conference* (pp. 1-11). doi.org/10.1109/ISTAFRICA.2016.7530586

French, A., Guo, C., & Shim, J. P. (2014). Current status, issues, and future of bring your own device (BYOD). *Communications of the Association for Information Systems*, *35*(1), 191-197.

Fronk, E. (2018). Zotero: A guide for librarians, researchers and educators. *Journal of Web Librarianship*, *12*(2), 145-146. doi.org/10.1080/19322909.2018.1448658

Gajar, P. K., Ghosh, A., & Rai, S. (2013). Bring your own device (BYOD): Security risks and mitigating strategies. *Journal of Global Research in Computer Sciences*, *4*(4), 62-70.

Garba, A. B., Armarego, J., Murray, D., & Kenworthy, W. (2015). Review of the information security and privacy challenges in bring your own device (BYOD) environments. *Journal of Information Privacy and Security, 11*(1), 38-54.

Giwah, A. D. (2018). User information security behavior towards data breach in bring your own device (BYOD) enabled organizations—leveraging protection motivation theory. In *SoutheastCon 2018* (pp. 1-5). doi.org/10.1109/SECON.2018.8479178

Goldman, J. (2017). B*YOD blamed for massive cryptocurrency breach*. Retrieved from https://www.esecurityplanet.com/endpoint/byod-blamed-for-massive-cryptocurrency-breach.html

Guan, L. (2012). Established BYOD management policies needed. *Government News, 32*(2), 9. Retrieved from http://search.informit.com.au/documentSummary;dn=521079283440573;res=IELHSS

Harris, M. A., Patten, K., & Regan, E. (2013). *The need for BYOD mobile device security awareness and training*. Americas Conference on Information Systems, AISeL, Chicago.

Harthy, k A., Shah, N., & Shankarappa, A. (2018). Intelligent Risk Management Framework for BYOD. In *2018 IEEE 15th International Conference on e-Business Engineering (ICEBE)* (pp. 289–293). https://doi.org/10.1109/ICEBE.2018.00055

Heath, S. (2016). *91K patients' data compromised in WA healthcare data breach*. Retrieved from https://healthitsecurity.com/news/91k-patients-data-compromised-in-wa-healthcare-data-breach

Herrera, A. V., Ron, M., & Rabadão, C. (2017). National cyber-security policies oriented to BYOD (bring your own device): Systematic review. In *2017 12th Iberian Conference on Information Systems and Technologies (CISTI)* (pp. 1-4). doi.org/10.23919/CISTI.2017.7975953

Hoelscher, P. (2017). *BYOD security: What are the risks and how can they be mitigated?* Retrieved from https://www.comparitech.com/blog/information-security/byod-security-risks/

Inside Counsel. (2013). *Inside Counsel - November 2013 - 61*. Retrieved from http://www.insidecounseldigital.com/insidecounsel/november_2013?pg=61&lm=1382505085000

Jaha, F., & Kartit, A. (2017). Pseudo code of two-factor authentication for BYOD. In *2017 International Conference on Electrical and Information Technologies (ICEIT)* (pp. 1-7). doi.org/10.1109/EITech.2017.8255248

Jaramillo, D., Newhook, R., & Smart, R. (2013). Cross-platform, secure message delivery for mobile devices. In *2013 Proceedings of IEEE Southeastcon* (pp. 1-5). doi.org/10.1109/SECON.2013.6567435

Kadimo, K., Kebaetse, M. B., Ketshogileng, D., Seru, L. E., Sebina, K. B., Kovarik, C., & Balotlegi, K. (2018). Bring-your-own-device in medical schools and healthcare facilities: A review of the literature. *International Journal of Medical Informatics*, *119*, 94-102. doi.org/10.1016/j.ijmedinf.2018.09.013

Kao, Y. C., Chang, Y. C., & Chang, R. S. (2015). Managing bring your own device services in campus wireless networks. In *2015 International Computer Science and Engineering Conference (ICSEC)* (pp. 1-7). doi.org/10.1109/ICSEC.2015.7401456

Ketel, M. (2018). Enhancing BYOD security through SDN. In *SoutheastCon 2018* (pp. 1-2). doi.org/10.1109/SECON.2018.8479230

Koh, E. B., Oh, J., & Im, C. (2014). A study on security threats and dynamic access control technology for BYOD, smart-work environment. *Proceedings of the International Multi Conference of Engineers and Computer Scientists, 2*, 634-639.

Kyriazis, D. (2018). BYOS: Bring Your Own Security in Clouds and Service Oriented Infrastructures. In *2018 32nd International Conference on Advanced Information*

Networking and Applications Workshops (WAINA) (pp. 374–379). Krakow: IEEE. https://doi.org/10.1109/WAINA.2018.00114

LaPointe, J. (2016). *Stolen laptop leads to possible healthcare data breach in KS.* Retrieved from https://healthitsecurity.com/news/stolen-laptop-leads-to-possible-healthcare-data-breach-in-ks

Li, F., Peng, W., Huang, C., & Zou, X. (2013). Smartphone strategic sampling in defending enterprise network security. In *2013 IEEE International Conference on Communications (ICC)* (pp. 2155-2159). doi.org/10.1109/ICC.2013.6654846

Li, P., & Yang, L. (2017). Management strategies of bring your own device. *MATEC Web of Conferences*, *100*, 02007. doi.org/10.1051/matecconf/201710002007

Masin, J. (2013). *Peer-To-Peer (P2P) file sharing risks*. Retrieved from https://www.securedocs.com/blog/2013/02/peer-to-peer-p2p-file-sharing-risks

Mishima, K., Sakurada, T., & Hagiwara, Y. (2018). Easy accessible virtual computer room for BYOD environment. In *2018 15th IEEE Annual Consumer Communications Networking Conference (CCNC)* (pp. 1-2). doi.org/10.1109/CCNC.2018.8319318

Moreira, F., Cota, M. P., & Gonçalves, R. (2016). Strategies for minimizing the influence of the use of BYOD and Cloud in organizations: 4CM model. In *2016 IEEE 11th Colombian Computing Conference (CCC)* (pp. 1-8). doi.org/10.1109/ColumbianCC.2016.7750785

National Institute of Standards and Technology. (2004). *Standards for security categorization of federal information and information systems* (No. NIST FIPS 199). Gaithersburg, MD: Author. doi.org/10.6028/NIST.FIPS.199

National Institute of Standards and Technology. (2013). *Security and privacy controls for federal information systems and organizations*. NIST Special Publication, 800, 53. Gaithersburg, MD: Author.

Ogie, R. (2016). Bring your own device: An overview of risk assessment. *IEEE Consumer Electronics Magazine*, *5*(1), 114-119. doi.org/10.1109/MCE.2015.2484858

Okigbo, A. C., Uwasomba, C., & Douglas, I. T. (2016). Security and privacy issues in BYOD: Analytical comparison between MDM and RMS solutions. *International Journal of Applied Research and Technology*, *5*(8), 85-91.

Olalere, M., Abdullah, M. T., Mahmod, R., & Abdullah, A. (2015). A review of bring your own device on security issues. *SAGE Open*, *5*(2). doi.org/10.1177/2158244015580372

Oyo-Ita, E. U., Utoda, R. A., & Asuquo, U. O. (2018). The impact of bring your own device (BYOD) on information technology (IT) security and infrastructure. In The Nigerian Insurance Sector. *American Journal of Engineering Research (AJER)*, *7*(5), 237-246.

Petrov, D., & Znati, T. (2018). Context-Aware Deep Learning-Driven Framework for Mitigation of Security Risks in BYOD-Enabled Environments. In *2018 IEEE 4th*

International Conference on Collaboration and Internet Computing (CIC) (pp. 166–175). https://doi.org/10.1109/CIC.2018.00032

Prashant, K. G., Arnab, G., & Shashikant, R. (2013). Bring your own device (Byod): security risks and mitigating strategies. *Journal of Global Research in Computer Science*, 4(4), 62-70. Retrieved from http://www.sans.org/resources/glossary.php

Rhodes, J. (2013). Building security around BYOD. *Managing Mobility, Rough Notes, 56*, 104-114.

Rivera, D., George, G., Peter, P., Muralidharan, S., & Khanum, S. (2013). *Analysis of security controls for BYOD (Bring Your Own Device)*. Melbourne, Australia: The University of Melbourne.

Rodríguez, N. R., Murazzo, M. A., Chavez, S., Valenzuela, F. A., Martín, A. E., & Villafañe, D. A. (2013). Key aspects for the development of applications for Mobile Cloud Computing. *Journal of Computer Science & Technology*, *13*.

Saa, P., Moscoso-Zea, O., & Lujan-Mora, S. (2017). Bring your own device (BYOD): Students perception—privacy issues: A new trend in education? In *2017 16th International Conference on Information Technology Based Higher Education and Training (ITHET)* (pp. 1-5). doi.org/10.1109/ITHET.2017.8067824

SANS Institute. (2017). *SANS glossary of terms used in security and intrusion detection.* North Bethesda, MD: Author.

Santee, C. (2017). An exploratory study of the approach to bring your own device (BYOD) in assuring information security. *CEC Theses and Dissertations*. Retrieved from https://nsuworks.nova.edu/gscis_etd/1005

Shridhar, M. (2017). *Mobile security: 2017 spotlight report* (pp. 1-22). Retrieved from https://www.cybersecurity-insiders.com/wp-content/uploads/2017/04/2017-Mobile-Security-Report-Zimperium_1.3.pdf

Shumate, T., & Ketel, M. (2014). Bring your own device: Benefits, risks and control techniques. In *IEEE SOUTHEASTCON 2014* (pp. 1-6). doi.org/10.1109/SECON.2014.6950718

Singh, M. M., Chan, C. W., & Zulkelfli, Z. (2017). Security and privacy risks awareness for bring your own device (BYOD) paradigm. *International Journal of Advanced Computer Science and Application, 8*(2). doi.org/10.14569/IJACSA.2017.080208

Singh, M. M., Siang, S. S., Ying, O., Hashimah, N., Malim, A. H., & Shariff, A. R. M. (2014). Security attacks taxonomy on bring your own devices (BYOD) model. *International Journal of Mobile Network Communications & Telematics (IJMNCT)*, *4*(5), 1-17.

Song, Y., & Kong, S. C. (2017). Affordances and constraints of BYOD (Bring Your Own Device) for learning and teaching in higher education: Teachers' perspectives. *The Internet and Higher Education*, *32*, 39-46. doi.org/10.1016/j.iheduc.2016.08.004

Souppaya, M. P., & Scarfone, K. A. (2016*). User's guide to telework and bring your own device (BYOD) security* (No. NIST SP 800-114r1). Gaithersburg, MD:

National Institute of Standards and Technology. Doi.org/10.6028/NIST.SP.800-114r1

Strothmann, M. (2018). Book review: Zotero: A guide for librarians, researchers and educators (2nd ed.). *Reference and User Services Quarterly*, *57*(3), 222-222. doi.org/10.5860/rusq.57.3.6619

Sundgren, M. (2017). Blurring time and place in higher education with bring your own device applications: A literature review. *Education and Information Technologies*, *22*(6), 3081-3119. doi.org/10.1007/s10639-017-9576-3

Tanimoto, S., Yamada, S., Iwashita, M., Kobayashi, T., Sato, H., & Kanai, A. (2016). Risk assessment of BYOD: Bring your own device. In *2016 IEEE 5th Global Conference on Consumer Electronics* (pp. 1-4). doi.org/10.1109/GCCE.2016.7800494

Timms, K. (2017). BYOD must be met with a wider appreciation of the cyber-security threat. *Computer Fraud and Security*, *2017*(7), 5-8. doi.org/10.1016/S1361-3723(17)30058-1

TREND MICRO. (2015). *Implementing BYOD: What are the risks to your corporate data?* (pp. 1-6). Retrieved from http://about-threats.trendmicro.com/cloud-content/us/ent-primers/pdf/Implementing_BYOD_Update_final2.pdf?_ga=2.46965031.1264716071.1539581465-1168375342.1537935127

Tu, Z., & Yuan, Y. (2015). Coping with BYOD security threat: From management perspective. In *Proceedings of Twenty-first Americas Conference on Information*

Systems (AMCIS), held 13-15 August 2015, Fajardo, Puerto Rico. (Vol. 5, pp. 1-6).

Vorakulpipat, C., Sirapaisan, S., Rattanalerdnusorn, E., & Savangsuk, V. (2017). A policy-based framework for preserving confidentiality in BYOD environments: A review of information security perspectives. *Security and Communication Networks*, 1-11. doi.org/10.1155/2017/2057260

Weintraub, E. (2016). Evaluating confidentiality impact in security risk scoring models. *International Journal of Advanced Computer Science and Applications*, *7*(12), 156-164. doi.org/10.14569/IJACSA.2016.071221

Welsh, K. E., Mauchline, A. L., France, D., Powell, V., Whalley, W. B., & Park, J. (2018). Would bring your own device (BYOD) be welcomed by undergraduate students to support their learning during fieldwork? *Journal of Geography in Higher Education*, 1-16. doi.org/10.1080/03098265.2018.1437396

Yevseyeva, I., Turland, J., Morisset, C., Coventry, L., Grob, T., Laing, C., & van Moorsel, A. (2015). Addressing consumerization of IT risks with nudging. *International Journal of Information Systems and Project Management*, *3*(3), 5-22. doi.org/10.12821/ijispm030301

Wang, Y., Wei, J., & Vangury, K. (2014). Bring your own device security issues and challenges. *2014 IEEE 11th Consumer Communications and Networking Conference (CCNC)*, 80-85. doi.org/10.1109/CCNC.2014.6866552

Zahadat, N., Blessner, P., Blackburn, T., & Olson, B. A. (2015). BYOD security engineering: A framework and its analysis. *Computers and Security*, *55*, 81-99. doi.org/10.1016/j.cose.2015.06.011

Zheng, Y., Cao, Y., & Chang, C. H. (2018). Facial biohashing based user-device physical unclonable function for bring your own device security. In *2018 IEEE International Conference on Consumer Electronics (ICCE)* (pp. 1–6). Las Vegas, NV: IEEE. https://doi.org/10.1109/ICCE.2018.8326074

Zotero. (2018). *Zotero 5.0.36: New PDF features, faster citing in large documents, and more*. Retrieved from https://www.zotero.org/blog/zotero-5-0-36/

Zulkefli, Z., & Singh, M. M. (2018). The “bring your own device” (BYOD) security metrics taxonomy. *Advanced Science Letters*, *24*(11), 8582-8590. doi.org/10.1166/asl.2018.12307

Appendix

Summary of BYOD Policy Research Efforts

No.	Researcher(s)	Research Focus	Knowledge Contribution
1	Zulkefli *et al.* (2018)	Security	A taxonomy that contributes to providing a ranking list on the severity of various security attacks occurring in BYOD Higher Education.
2	Giwah (2018)	Security	Proposed a theoretical approach based on the Protection Motivation Theory.
3	Alotaibi & Almagwashi (2018)	Security	Presented an all-inclusive policy model for BYOD security.
4	Ketel (2018)	Security	Proffered various network technologies and administration tools e.g. SDN, NFV and EMM that can be used to mitigate BYOD security challenges.
5	Olalere et al. (2015)	Security	Provides a theoretic evaluation for future work which aids scholars to detect viable areas of research in BYOD.
6	Ekpo & Fournier-Bonilla (2018)	Security & Privacy	Determined to what extent determinant factors had prevented users from adopting BYOD as well as to understand what factors subscribed users saw as challenging when adopting BYOD.
7	Amoud & Roudies (2017)	Security	This study presented a Systematic Literature Review (SLR) of BYOD published research articles to answer the following question: “How to integrate securely a BYOD in an Enterprise’’.
8	Herrera, Ron, & Rabadão (2017)	Security & Privacy	This research focused on a systematic review about BYOD’s actual situation, its trend, impact & a proposal of recommendations oriented to have a National Policy in Ecuador.
9	Zheng, Cao, & Chang (2018)	Security	Presented a novel biohashing based user-device physical unclonable function (UD

No.	Researcher(s)	Research Focus	Knowledge Contribution
			PUF) to provide a bipartite authentication of both user and device for the BYOD system.
10	Kyriazis (2018)	Security & Privacy	This paper presents an approach that proposes the use of security mechanisms, as plugins that are custom/tailored and potentially developed by the end users themselves.
11	Vorakulpipat, C., Sirapaisan, S., Rattanalerdnusorn, E., & Savangsuk, V. (2017).	Security & Privacy	The chief contribution of this study is to investigate recent trends concerning the preservation of confidentiality in BYOD from the perspective of information security and to analyze the critical and comprehensive factors needed to strengthen data privacy in BYOD. Also, this study provides a foundation for developing the concept of preserving confidentiality in BYOD and describes the key technical and organizational challenges faced by BYOD-friendly organizations.
12	Boadi, P. M., Zhou, S., & Ioannis K, K. (2018).	Security	This paper introduced a possible scoring framework purposefully for scoring related to BYOD vulnerability; this considers historic and intrinsic characteristics.
13	Mishima, K., Sakurada, T., & Hagiwara, Y. (2018)	Security	Implemented brand new concept virtual desktop system for computer lecture, TUAT Virtual Computer Classroom, which is based in virtual desktop technology and users can access the tools with any HTML5-compliant web browser, removing the differences for various operating systems.
14	Oyo-Ita, E. U., Utoda, R. A., & Asuquo, U. O. (2018).	Security	Proffered suggestions that will adequately maintain IT security and Infrastructure even in the face of an ever-improving trend in smart phones and intelligent devices in the Nigerian Insurance Sector.
15	Welsh, K. E., Mauchline, A. L., France, D., Powell,	Security	The key findings suggest that around one fifth of students were not willing to use their own device during fieldwork citing loss or damage as the main reason. Also, this study suggests that some students believe that

No.	Researcher(s)	Research Focus	Knowledge Contribution
	V., Whalley, W. B., & Park, J. (2018).		BYOD can have a negative impact on group work.
16	Harthy, Shah, & Shankarappa (2018)	Security & Privacy	This paper proposed a novel approach which utilizes MDM log file to proactively detect potential threats in BYOD environment and take preventive and mitigative measures in real time.
17	Petrov & Znati (2018)	Security	Contributions of this study include the formulation of the BOYD unauthorized access control problem, a framework that uses artificial neural networks (ANN) and decision tree (DT) machine learning (ML) techniques to detect anomalous behaviors and to identify unauthorized access to resources on BYOD devices.
18	Bello, A. G., Murray, D., & Armarego, J. (2017).	Security & Privacy	Provides a current best practice approach that can be used by organizations to systematically investigate and understand the manner in which privacy and security risks can be managed within a BYOD network.
19	Jaha, F., & Kartit, A. (2017).	Security & privacy	Proposed an improved algorithm in three phases to implement keystroke dynamics.
20	Li, P., & Yang, L. (2017).	Management Strategies	Proposed a conforming management approaches of BYOD with the view to providing avenues for enterprises to achieve the mobile needs of their organizations.
21	Saa *et al.* (2017)	Privacy	Their research outcome showed that lots of students believe that a BYOD policy could help enhance learning methods in computer science-based programs.
22	Song, Y., & Kong, S. C. (2017).	Security	Effective ways of integrating BYOD into students' academic lives were explored by academicians
23	Timms, K. (2017).	Security	Examines the security challenges faced by SMEs and outlines how these can be addressed.

No.	Researcher(s)	Research Focus	Knowledge Contribution
24	Weintraub (2016)	Security	Provided a theoretical groundwork, challenges, advantages, security risks, threats and research efforts by scholars in the area of BYOD security and privacy.
25	Fani, N., Solms, R. V., & Gerber, M. (2016)	Security	Provided a rudimentary guideline to management executives on the method of managing and governing the emerging BYOD phenomenon in a secure and accountable manner.
26	Zahadat, N., Blessner, P., Blackburn, T., & Olson, B. A. (2015).	Security & Privacy	The first is to address the security concerns of BYOD, which necessitate technology, policy management, and people integration instead of the traditional technology alone approach. The second is to propose a BYOD Security Framework as the solution to BYOD security concerns.