Journal of Advanced Research in Applied Sciences and Engineering Technology

Journal homepage:
https://semarakilmu.com.my/journals/index.php/applied_sciences_eng_tech/index
ISSN: 2462-1943

BYOD Security Policy Model: A Systematic Literature Review

Izzah Inani Abdul Halim[1,*], Alya Geogiana Buja[2], Jasni Mohamad Zain[3], Abdul Hafaz Ngah[4], Rohit Bansal[5]

[1] Department of Computer Science, Faculty of Computer, Media and Technology Management, University College TATI, Teluk Kalong, 24000 Chukai, Terengganu, Malaysia
[2] Computing Science Studies, College of Computing Studies, Informatics and Mathematic, Universiti Teknologi MARA (UiTM) Melaka Branch, Jasin Campus, Kampung Seri Mendapat, 77300 Merlimau, Melaka, Malaysia
[3] Institute of Big Data for Analytics and Artificial Intelligence, Universiti Teknologi MARA Shah Alam, 40450 Shah Alam, Selangor, Malaysia
[4] Faculty of Business, Economics and Social Development, Universiti Malaysia Terengganu, 21300 Kuala Terengganu, Terengganu, Malaysia
[5] Department of Management Studies, Vaish College of Engineering, Rohtak Station Diary Mohalla, Rohtak, Haryana 124001, India

ABSTRACT

In education sector, Bring Your Own Device (BYOD) Security Policy (BYOD-SP) was established as earlier in 2015 in foreign universities with the purpose to safeguard campus's network, system and confidential data and information. BYOD-SP is one of the strategic planning launched, aims to achieve maximum security for personally owned device through BYOD phenomenon. BYOD-SP acts as an official documentation that describes the detailed explanation of each component for the BYOD users to abide to all the components' requirement in BYOD-SP. In BYOD practice in education field, BYOD-SP must meet the education agenda where BYOD-SP need to be tailored following education strategic plans and eliminate potential attacks that might cause the universities in loss if BYOD-SP is launched without having a robust model to refer of its components. Hence, it is crucial as this will welcome unauthorized parties to get access, gain and steal campus corporate data in BYOD environment. This study aims to identify what the necessary components that could assist top management and policy makers to formulate the comprehensive BYOD-SP in future and BYOD can be one of mobile computing that being accepted to be practiced in secured environment. Existing studies were executed in many research designs, where the review fulfilled the Preferred Reporting Items for Systematic reviews and MetaAnalyses (PRISMA) publishing standard. Two common online databases, World of Science (WOS) and Scopus were utilized to observe articles for this study purposes where a total of 16 articles published from 2013-2022 were reviewed to answer the formulated research questions on BYOD-SP. This review includes a topic based on the thematic analysis which is the components in drafting BYOD-SP documentation. The findings from this study proved four main components to be emphasized in tailoring BYOD-SP which are Device, Process, People and Jurisdiction/Law. The research's findings here may drive the organization to have a reference model of BYOD-SP components and come out with the sturdy BYOD-SP to be adhered by all individuals in education premises. The top management in the organization need to involve in the procedures in each component of BYOD-SP to alleviate the case of security breach in BYOD activities.

Keywords:

Bring Your Own Device; BYOD; Security policy; Higher learning; Malaysia

[*] *Corresponding author.*
E-mail address: izzahinani.ah@gmail.com

https://doi.org/10.37934/araset.62.1.170186

1. Introduction

Bring Your Own Device (BYOD) had taken place in the corporate environment since 2012 when the employee is allowed to bring their personal technological devices to the workplace and this practice continues to be followed by various organizations after that. Following the COVID-19 pandemic, the education sector also transitioned to digital platforms, with educators at various levels agreeing on the necessity of integrating technological devices into the education system [1]. During the first three years of BYOD practice, scholars actively discussed the BYOD benefits to several parties; including the individual and the management of the organization. BYOD was preferable as it claimed to be the way of how productive the employee can deliver tasks anytime and anywhere using familiar personal devices. Even though it has widely been accepted, the discussion on the BYOD phenomenon had shifted to the potential threats and risks when information security is being targeted in a BYOD environment since its early implementation. The scholars had aggressively discussed the worst scenario, the consequences of missing/stolen devices and the ignorance of individuals to adhere to the security policy contribute to confidential data and private information being in crisis. The current analysis of the prevention method of securing the BYOD environment involves the blockchain [2], Software Defined Networking [3] and context aware approaches after the discussion on installing mobile device management (MDM) still lacking in the security technique although it is still needed [4]. With the emergence of advanced technology in the latest smart devices, organizations need to address potential security threats from intruders when implementing BYOD. This involves developing a technical solution to effectively block any such threats.

Releasing BYOD Security Policy (BYOD-SP) is a strategic initiative aimed at ensuring users adhere to the guideline and procedures for BYOD usage. The policy document is made available for download and easy accessibility. Before BYOD penetrated the social practice in the working environment, many organizations had established general information and communication technology (ICT) security; consisting of public rules of safeguarding the corporate network and system. As per standard policy, it is customary to review and update security measures with the latest information on an annual basis. The general ICT policies usually identified all aspects that touch on the usage of technology and emphasize the required action towards suspicious activities related to the IT field and environment. The final documentation of ICT policies had been filtered by the respective department and get approval from the top management before being published to the public. In Malaysia situation, there is differentiation existed in BYOD-SP concept and documentation. Our exploration before elaborated that the earlier version of BYOD-SP was released in 2019, and most of the institutions result in discouraged that motivates us to further extend our research and action to determine the reference model of comprehensive BYOD-SP with the suggestion of Scott, Mason and Szewczyk [5] that it should be formulated with more end-users in mind and readable, user-friendly and accessible.

1.1 Research Question

This study seeks to determine the critical components that should be emphasized in crafting the BYOD-SP documentation. In particular, it aims to identify the mandatory components to be gathered as a reference model in launching an appropriate BYOD-SP blueprint that meet current needs of securing information security. In achieving this, this research formulated two research questions which are:

RQ1: What are the specific components of BYOD security policies that differentiate them from general ICT policies within organizations?

RQ2: Which theoretical perspective on security components are employed on tailoring BYOD security policies?

The need for this study arises from the necessity to conduct a systematic review of existing studies on the characteristics of BYOD-SP, theories related to crafting BYOD-SP documentation, and influential factors of crafting BYOD-SP, in order to offer prospects for future research. As a result, this review paper makes the following contributions:

i. Recognition and exploration of the distinctive characteristics of BYOD-SP
ii. Examination and presentation of theories utilized in existing studies on BYOD-SP.
iii. Identification of components on crafting BYOD-SP.

This article is structured into various sections. The discussion commences by introducing the concept of BYOD-SP. Section 2 of the Literature Review then delves into the summarization of the 7 steps outlined in the Security Threat Reduction Policy (STRP) framework. Furthermore, it presents a comprehensive examination of existing BYOD Models/Frameworks in the literature, along with a brief exploration of Malaysia's approach to managing information technology initiatives and government strategies. The following section details the research methodology, the fourth section showcases the search results and ensuing discussions, and finally, the fifth section provides the concluding remarks for the review.

2. Related Work

A framework called Security Threat Reduction Policy (STRP) [6] had been elaborated featuring the seven steps in tailoring comprehensive BYOP-SP that controlled the possibility of security threats (see Table 1). We summarize the study of the framework to see the suggestions in each step to see how crucial each steps described and which party should take actions to empower the security practice in existing BYOD-SP. This framework asserts that addressing security policy factors effectively is a key factor in reducing the inherent security risks within the BYOD environment, in addition to technology and collaborative efforts of individuals. In addition, this article also supported this study as very articles have comprehensively analysed security issues and respective policies phase by phase. The initial two phases, Strategy and Recognition, addressed the policy aspect. The Strategy phase is of utmost importance, requiring prioritization by top management to establish a robust connection with individuals within the organization and create a dynamic and efficient BYOD model. Furthermore, it is essential for BYOD-SP guidelines to incorporate routine initiatives aimed at educating individuals about security features.

Table 1
The STRP Framework

7 steps	Description	Authority	Status
Strategy	✓ Design a strong and efficient BYOD model ✓ Establishing a strong relationship (managers, employees, shareholders, managerial authorities)	Higher Management	Crucial
Recognize	✓ Device registration ✓ Training about BYOD policy guidelines & security	Employee IT Department	-
Defend	✓ Passwords ✓ Patterns ✓ Biometric authentication ✓ One-time authenticate mechanism ✓ Incorporate both Internal application & software ✓ Network - high layer advanced encryption protocol	IT Department	-
Detect	✓ Clear understanding about BYOD security threats ✓ Proper knowledge of the security threats ✓ Install anti-malware and anti-virus ✓ Utilize visualization software ✓ Mobile Device Management (MDM) trace device loss	Employee	-
Retaliate	✓ Install high-security firewalls and anti-virus software ✓ Utilize MDM - wipe out all the corporate details with employee properties.	IT Department	-
Retrieve	✓ Prevent - shared or public data storage platforms for corporate details & activities. ✓ Utilize Virtualization - personal space of employee-owned devices is not used and employee can directly store and access information from the organization data storage centre	Organizations Employee	-
Evaluation & observe	✓ Regular checkup ✓ Security updates ✓ Feedbacks	Higher Management IT Department	Crucial

2.1 BYOD Security Model/Framework

Establishing BYOD-SP is guided by the security components and mandatory elements agreed upon by several parties including governments, agencies, security experts and top management of the organization. They identified every aspect of critical parts of security breaches in an organization. If cybersecurity is being neglected or is not in top consideration, higher chance the organization might experience the biggest loss of valuable and secretive data/information. Existing BYOD Model/Framework influenced the way of tailoring the BYOD-SP; identified the security issues that might appear. According to Chen, Hu and Cheng [7], security issues that stem from Bring Your Own Device (BYOD) policies are addressed less frequently than those related to IT, Management, Users, and Mobile Devices domain. In addition, organizations must be conscious of end-of-life (EoL) issues when designing and implementing BYOD policies, ensuring that they adequately address end-of-life data remanence issues with sufficient solutions and controls to mitigate this real risk [5]. Hence, the objectives of this study are to highlight the unique aspects of BYOD-SP that differentiate them from the broader ICT policies typically found in organizations and to identify components from a theoretical perspective shape the tailoring of future BYOD-SP customization.

We believe that this study can be utilized by any organization to tailor a comprehensive and suitable BYOD-SP in each field to accommodate the needs and mission of the different organization due to the fact that there is a similarity in previous discussions that encourage the top management level to involve in policy creation as result by Ratchford *et al.,* [8] inconsistent security policies exist across departments. Supported by Chen, Hu and Cheng [7] information security fatigue appears when there is a conflict between information security related and employees' adoption of BYOD practice. In the past, it was emphasized that having a well-defined policy framework is crucial for incorporating the local government laws into the organization's BYOD security policy [9].

2.2 BYOD-SP in Malaysia Context

Recent study in Malaysia emphasized the urgent need of having an assessment for mobile device security [10]. We believe that it could improve the usage of the mobile device in BYOD situation and BYOD performance as well. It investigates the feasibility of using information systems (IS) audit to assess the security of mobile devices by exploring the risks and vulnerabilities associated with these devices, as well as examining organizational information system (IS) security and management perception of mobile device security. The fact that Bring Your Own Device (BYOD) policies typically involve employees bringing their own devices, such as smartphones, means that there is a growing need to study the security and privacy implications of these devices. Specific examples, such as data leakage or loss, downloading unsafe apps or content, and lost or stolen devices, serve as evidence that security breaches can originate from the devices themselves. In addition, the findings from a systematic literature review discussion on compliance with BYOD-SP, Palanisamy, Norman and Mat Kiah [11] suggest that organizations should prioritize the development of BYOD security policies as a factor for improvement. Besides enhancing user compliance with the BYOD-SP, it is imperative to promptly establish a reliable reference model for formulating an effective BYOD-SP. Therefore, this study seizes the opportunity to examine the currently discussed models or frameworks for establishing the BYOD-SP within an organization.

With BYOD-SP yielding disparate outcomes across select public universities in and an ambiguous landscape within private institutions in Malaysia, immediate actions should be taken to meticulously orchestrate the crafting of BYOD-SP through astute planning. The implementation of Malaysia's BYOD security policy in higher education involves aligning with government education agendas, incorporating each university's strategic plan, and ensuring comprehension and acceptance of the policy by various stakeholders such as managerial and non-managerial personnel, staff, and students from both IT and non-IT backgrounds. Various technologies in modern age play important consideration and must be a part of consideration in BYOD-SP as more approaches and techniques of securing devices and network being aggressively discussed in latest research on BYOD protection [12]. In 2020, Government of Malaysia had launched MyDIGITAL and one of the strategic thrusts in MyDIGITAL [13] is *T6-Build trusted, secure and ethical digital environment* where it focuses to drive digital transformation and inclusion across the digital economy, emphasizing inclusivity among the rakyat (people) and all levels of businesses in Phase 2 (2023-2025). BYOD as a part of this thrust have to be positioned at the main consideration of secured environment as the phenomenon of bringing personal devices to the workplace and schools or universities is gaining popularity. In Saudi Arabia the study highlights the importance of implementing policies and standards to ensure security of device in BYOD practice. It also reiterates that having strict policies is necessary to document and manage risks, as exploiting vulnerabilities could weaken the infrastructures of government and corporate sectors [14].

3. Methodology

For this study, the review was guided by the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) statement. Conducting a systematic literature review (SLR) requires formulating specific research questions and using systematic and explicit methods to identify, select, evaluate, collect, and analyse data from relevant previous studies. PRISMA provides a comprehensive framework for conducting systematic reviews, covering a wide range of general concepts and topics [15]. In addition, Sierra-Correa and Kintz [16] highlighted three key benefits of using PRISMA:

i. it helps to define research topics for systematic investigation
ii. it generates inclusion and exclusion criteria
iii. it facilitates the analysis of a large database of scientific papers within a specific time limit.

Figure 1 illustrated the findings of related study from two primary online database:

i. Scopus
ii. Web of Science.

From the search string (defined in Table 2), we discovered a total of 70 articles initially, which underwent a screening process to filter and ensure they met the study's requirements. We have compiled a list of exclusion criteria from 70 articles, including the following:

i. publication date must fall between 2013 and 2022 to ensure the inclusion of the latest discussions on the BYOD model
ii. articles must be primarily in English language, excluding those in other languages
iii. articles not related to journals are excluded.

These three criteria were recommended to assist us narrow down our focus on articles closely aligned with our research contributions. From those, 30 articles were further evaluated to avoid redundancy and confirm their relevance to the BYOD model or framework. After excluding some based-on identification criteria, we ultimately obtained 16 articles that specifically discussed the BYOD model and framework in various sectors.

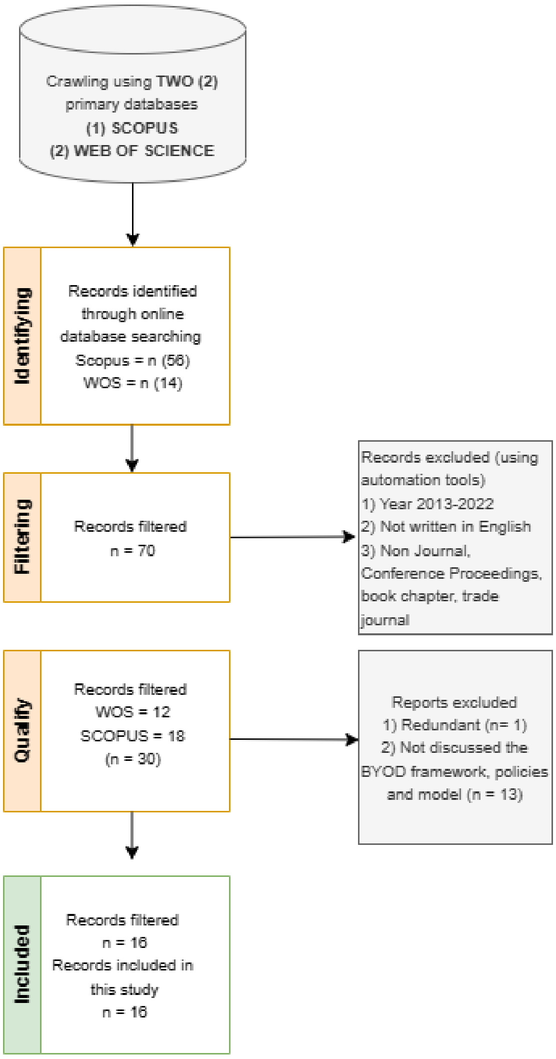
Crawling using TWO (2) primary databases
(1) SCOPUS
(2) WEB OF SCIENCE
Identifying
Records identified through online database searching
Scopus = n (56)
WOS = n (14)
Filtering
Records filtered
n = 70
Records excluded (using automation tools)
1) Year 2013-2022
2) Not written in English
3) Non Journal, Conference Proceedings, book chapter, trade journal
Qualify
Records filtered
WOS = 12
SCOPUS = 18
(n = 30)
Reports excluded
1) Redundant (n= 1)
2) Not discussed the BYOD framework, policies and model (n = 13)
Included
Records filtered
n = 16
Records included in this study
n = 16

Fig. 1. Flow Diagram Detailing the Application of PRISMA 2020 to Studies Published between 2013-2022

In Table 2, the keywords and strings were formulated for the search process. Both were retrieved based on the title Bring Your Own Device and Security Policy. In the searching process, the keywords were explored in the title to catch the relevant articles to the study. Two main online digital databases were utilized; Scopus and Web of Science (WOS) in this strategy of searching related papers.

Table 2
The Search String

Databases	Keywords Search
Scopus	(TITLE-ABS-KEY (bring AND your AND own AND device OR byod OR byo*) AND TITLE-ABS-KEY (security AND policy OR polic*) AND TITLE-ABS-KEY (model OR mode*))
Web of Science	Bring Your Own Device OR BYOD OR BYO* OR Mobile Device (Title) and Security Policy OR Polic* (Title) and Model (All Fields)

4. Results and Discussion

4.1 Dissemination of Studies

This study covered the research on BYOD-SP model or framework in last 10 years (2013-2022). Figure 2 summarized the total of articles in each year, where it identified zero contribution in 2013. The discussion's contributions have been consistently published, except for 2020, which we suspect may be due to regional COVID-19 lockdowns. The trend resumed in 2021, driven by the increased of mobile device usage and Work-From-Home (WFH) settings post-lockdown, and it continued to grow significantly in 2022.

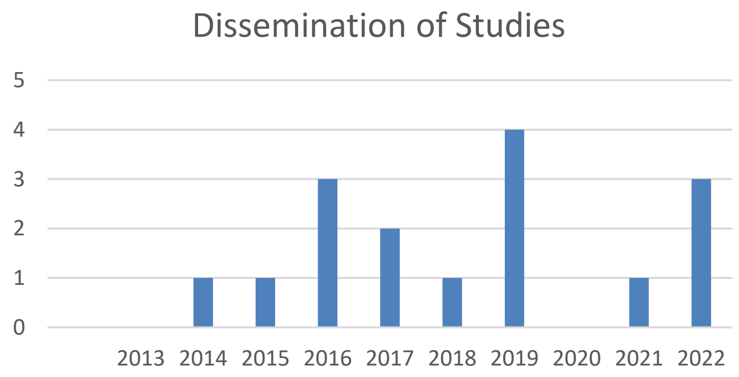

Fig. 2. Dissemination of Studies (2013-2022)

4.1.1 Summary on articles found

Table 3 summarized the methodology for each of the studies found. The utilization of questionnaire surveys as a quantitative approach significantly dominates the research pertaining to BYOD models/frameworks when contrasted with alternative methods like experimental, qualitative case studies and focus groups discussion. In 2019, quantitative approach conquered the research method other than use case and empirical study on BYOD-SP model. What piques our interest in advancing this study on the BYOD-SP when a study on the exploring the significance of the bring-your-own-device policy in shaping mobile learning behavioural patterns applied qualitative method with a specific focus on its implications within the education sector. The study wishes to gain insights from management using a qualitative approach regarding their readiness to implement a comprehensive BYOD-SP, which incorporates robust components.

Table 3
Article Details

Paper ID	Title, Year	Method
1	Requirement Engineering for Effective Mobile Learning: Modelling Mobile Device, 2014	Case Study
2	Formal modelling and automatic enforcement of Bring Your Own Device policies, 2015	Experimental Evaluation Partial Model Checking
3	This is my device! Why should I follow your rules? Employees' compliance with BYOD, 2016	Quantitative
4	Unintended consequences of a strategically ambiguous organizational policy selectively restricting mobile device use at work, 2016	Case study Focus group
5	Policy framework for adoption of bring your own device (BYOD) by institutions in Nigeria, 2016	Qualitative method Secondary data
6	Public trust in a mobile device and service policy in South Korea: The Mobile Device, 2017	Quantitative
7	A new conceptual model for BYOD organizational adoption, 2017	Purposive sampling Focus group (Discussions, Observations) Document analysis
8	A Review of BYOD Security Challenges, Solutions and Policy Best Practices. A Review, 2018	Articles, conference
9	Role of Perceived Value in Acceptance of Bring Your Own Device Policy, 2019	Questionnaire Survey
10	Policy Framework and Recommendations to Minimize the Usage of Stolen and Counterfeit or Substandard Mobile Communication Devices, 2019	Questionnaire survey
11	BYOD secured solution framework, 2019	Use Case
12	A security risk perception model for the adoption of mobile devices in the healthcare industry, 2019	An empirical study
13	ARANAC: A Bring-Your-Own-Permissions Network Access Control Methodology for Android Devices, 2021	Analysis:
14	BYOD Policy Compliance: Risks and Strategies in Organizations, 2022	Systematic Review
15	Understanding the role of the bring-your-own-device policy in mobile learning behavioural usage, 2022	Qualitative Focus group discussions, Direct observation Document analysis
16	A Theoretical Foundation for Explaining and Predicting the Effectiveness of a Bring Your Own Device Program in Organizations	Quantitative

4.2 Analysis of Existing Model (2013 – 2022)

Analysing the study type outlined in Table 3 motivated us to delve deeper into the BYOD Model/Framework, specifically its policy focus. We proceeded to extract the relevant discussions from each study, highlighting the emphasized components and exploring the various funding methods for the BYOD Model/Framework. The BYOD practice revolves around the device, and the obligatory discussion centres around the device itself, encompassing both hardware and software aspects. Based on early discussions on the BYOD trend, three components consistently emerge: Software, Hardware, and People. The convergence of these three elements demonstrates how BYOD is implemented securely, with fewer reported cases of criminal issues and risks to the BYOD environment. The rapid advancement of technology has made software and hardware crucial considerations in the discussion surrounding the BYOD phenomenon. With various devices having different operating systems and system settings, managing BYOD requires finding a unified solution [17]. When formulating a BYOD security policy, it is essential to address software components to prevent misuse and the presence of malicious software. Modern mobile applications come in various customizations and may potentially contain hidden malicious code designed for spying or theft on small devices. From the early stages of BYOD, both software and hardware have been integral components that require continuous attention and elaboration.

To the best definition of BYOD, it refers to the right of individuals to safeguard their privacy on personal devices, even if these devices store sensitive information belonging to an organization. Therefore, the implementation of laws or acts can protect the rights of both the organization and the device owner. Legal measures have been introduced to establish an agreement between both parties, ensuring accountability for protecting the company's sensitive information stored on the device while respecting the privacy of the individual's personal data. In addition to this situation of privacy matters, the organization has the right to protect its network and system in BYOD practice which include agreement of individual willing to adhere to any steps or precaution from revealing them to unauthorize party. Therefore, individual need to follow the procedures including sharing the cloud storage account where it might contain the corporate data, private email conversion, confidential files and documents etc. The agreement of accessing corporate data or storing them in personal cloud storage must been acknowledged by the managements side and they have the right to vanish the data for the situation of the individual suspicious action or leave the organization.

To reinforce the various aspects under discussion, such as risk knowledge, security awareness and education, promotion, and training, it is important to build a comprehensive and robust system for establishing BYOD security policies (BYOD-SP). Within an organization, there may be individuals from non-IT backgrounds or non-managerial positions, like casual worker who may have limited security knowledge or exposure to new techniques or malicious attack mechanisms. Hence, we are of the opinion that these elements offer supplementary assistance in formulating BYOD security policies by enhancing individuals' understanding of BYOD knowledge and associated risks. As supported by Bello, Murray, Armarego [18] to successfully implement BYOD, it is mandatory to deploy an efficient information security program specifically designed for BYOD. Alongside these supportive elements, the IT department within an organization should not overlook their responsibility of assisting non-technical employees in managing risk situations related to BYOD practices. Therefore, implementing a monitoring process for all activities within the BYOD environment can help organizations reduce the likelihood of potential attacks or other harmful activities.

One more crucial aspect BYOD-SP that should not be overlooked is the audit process. In the documentation of BYOD-SP from foreign universities, it was emphasized that policies should undergo annual reviews. This serves as a best practice to keep up with technological advancements, new device inventions, and the latest software releases. By regularly reviewing the policies, they can be updated to align with the most recent developments in security practices. Within the education sector, there are various avenues to access innovative teaching and learning methods, such as utilizing websites, online meetings, accessing online portals, or participating in discussions on virtual platforms [19]. In this context, individuals need to be aware of the necessary steps to develop good security habits which includes practices like employing strong passwords, avoiding clicking on suspicious links, not sharing the private activities etc. [20]. We believe that these analysis on existing BYOD model/framework answers RQ1 in this study.

4.3 Summary of Existing BYOD Model/Framework (2013/2022)

Table 4 presents the year-wise arrangement (from 2013-2022) of the research that investigates the early adopters of the BYOD model/framework. The objective of the study is to identify the key aspects highlighted in the published articles, including hardware, software, people, technology, and other related components that are essential. These findings were compiled to create a list of necessary components that should be considered before developing the BYOD-SP. Policies must ensure the protection of sensitive corporate data and information on mobile devices without compromising the device's usability and the resulting productivity from BYOD [21]. Since this study aims to propose a reference model for the BYOD-SP, it identifies the recurring components discussed to provide guidance for stakeholders in tailoring a comprehensive BYOD-SP for various fields.

Table 4
Retrieving Components

ID	BYOD Model/Framework	Components
1	Integrated artefact model architecture Mobile Learning Requirement Engineering (RE)	Software
2	BYODroid	Software Hardware
3	Reactance, Protection Motivation and Organizational Justice Theories	People – Employee, IT Support Team Software - Virtualization
4	Conceptual Model	People – Nonmanagerial Workers
5	BYOD Policy Framework	Hardware – Device Software – OS People – Role & Designation Law – Privacy (Employee)
6	Ordered Probit Model	Other – Knowledge Law – Act MDDI (Mobile Device Distribution Improvement DDI)
7	Conceptual Model	Other – Acceptable, Support
8	A comprehensive security policy model (3-tier policy model)	Legal – Agreement, Access, Privacy Software – MCM, OS Hardware – Ca Credential, Encryption, Diversity Other – Educate, Security, Awareness People – Employee Law – Employee Privacy
9	Research Model Benefits & Sacrifice	Technology People Other – Job Flexibility
10	Equipment Identity Registers (EIRs)	Other – Awareness Hardware – Blocking Mechanism (Stolen Device) Law - Regulations
11	A secure BYOD model	People – Access (Trusted/Untrusted) Other – Monitoring & Audit
12	A theory-grounded conceptual model	Other – Promote, Training, Risk, Behavioural Technology Hardware - Convenient
13	ARANAC Application Risk Assessment based Network Access Control) Android Devices	Hardware Other – Awareness, Privacy, Permission, Access, Risk Hardware - Behaviour
14	People, Process and Technology (PPT) Model	Process

		Other – Guidelines, Enforcement, Mandate, Awareness, Clear, Friendly
15	Actor network theory	Other – Promote Hardware – Appropriate, Integrate Software – Equitable Access
16	Knapp and Ferrante's Information Security Policy and Effectiveness (ISPE) model	Other – Awareness, Enforcement, Account

4.3.1 BYOD model/framework timeline

In the two years prior (2013-2014), the focus of the model was on mobile devices as people practiced BYOD with these devices. Emphasis was placed on the installation of software to detect legal applications while infiltrating the corporate network and system. Untrusted software could jeopardize sensitive data and information, as several applications were found to contain malicious software unbeknownst to users. The research continued over the next two years, incorporating various methods such as case studies, quantitative and qualitative approaches, to develop a more compatible BYOD model/framework that could align with security policies for BYOD implementation. This year, the research expanded to include hardware and software components as well as motivation theory, aiming to reinforce the published IT policy and provide additional support for the BYOD phenomenon. The discussion underscored the importance of empowering device privacy and legal applications when accessing corporate networks and systems. Furthermore, the authors also addressed non-professional individuals and their respective roles and designations.

Another component being emphasized here is the existence of laws. Any irresponsible actions taken while practicing BYOD in organizations, such as mishandling corporate data or engaging in illegal transactions that result in business losses, cannot be disregarded. Therefore, the BYOD-SP (BYOD Security Policy) can be strengthened by introducing acts and laws that prevent individuals from being ignorant of corporate responsibilities, even when practicing BYOD with their devices.

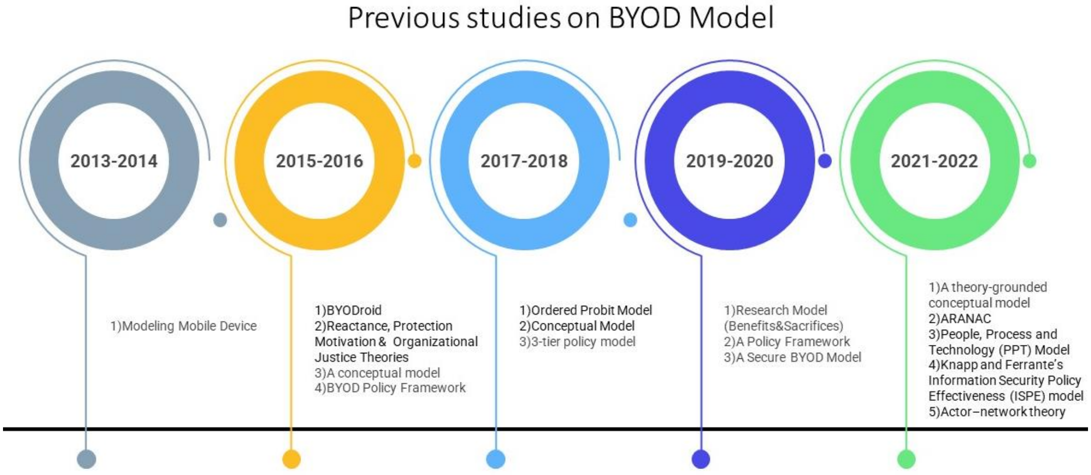
Previous studies on BYOD Model
2013-2014
2015-2016
2017-2018
2019-2020
2021-2022
1)Modeling Mobile Device
1)BYODroid
2)Reactance, Protection Motivation & Organizational Justice Theories
3)A conceptual model
4)BYOD Policy Framework
1)Ordered Probit Model
2)Conceptual Model
3)3-tier policy model
1)Research Model (Benefits&Sacrifices)
2)A Policy Framework
3)A Secure BYOD Model
1)A theory-grounded conceptual model
2)ARANAC
3)People, Process and Technology (PPT) Model
4)Knapp and Ferrante's Information Security Policy Effectiveness (ISPE) model
5)Actor–network theory

Fig. 3. BYOD Model/Framework Timeline

4.3.2 STRP framework + previous BYOD model/framework

In strategy step, the given points revolve around the concept of security policy within an organization. It mentions the importance of having clear policy interpretation, while also highlighting the value of maintaining some strategic ambiguity. It emphasizes that security requirements may vary depending on an employee's role and designation.

7 steps	Description	Paper ID
Strategy	Policy interpretation - Strategically ambiguous policy	8
	Security requirements based on employee role and designation	12
	Policy Specific Criteria	13
	Organization level	4
	Process Model (Policy)	6
	Security policy awareness	
Recognize	Policy interpretation - Mobile norms	8
	Which devices and operating systems to support	12
	Safeguards on mobile devices that are convenient for practitioners to	16
	adopt	11
	Enforcement	15
	Promoting appropriate mobile device use	
Defend	Software-intensive system	3
	BYODroid Server & Installer	1
	Application Level (MCM & Permission)	4
	Trusted User access and Untrusted Guest User access	14
	ARANAC (Application Risk Assessment based Network Access Control	10
Detect	Mobile virtualization	5
	The level of risk they are willing to tolerate	12
	Knowledge	7
	Device Level (CA Credentials & Encryption)	4
	Increasing user awareness	9
	Promote security policy compliance in mobile devices and safeguard	16
	information	15
	Actor–network theory	
Retaliate	Technology empowerment	2
	Establishing a proper blocking mechanism	9
Retrieve	Employee privacy concerns	12
	Job flexibility control	2
	Maintenance together account	11
Evaluation & observe	Having an IT support team	5
	Adding reforms to regulations	9
	Monitoring of the BYOD-User activity & Audit compliance	14

Additionally, it also highlights the role of the organization in developing policy and implementing a process model to ensure compliance with policies. While in recognize step, these points highlight the key areas that need to be addressed when implementing mobile device security policies. This includes policy interpretation and establishing mobile device norms, determining which devices and operating systems to support, implementing safeguards that are easy for practitioners to adopt, enforcing policies and promoting appropriate mobile device use among stakeholders.

4.3.4 References components on tailoring BYOD-SP

This study further extends from the findings to retrieve the components of BYOD-SP by Kang *et al.,* [4] and proposed a reference model for BYOD-SP to have a strong establish BYOD-SP in future, which being targeted to be implement in tertiary education. Figure 4 retrieved the common discussion of BYOD components:

i. BYOD-SP implementation in universities [22]
ii. existing BYOD-SP Model/Framework.

We matched each of the components to construct a reference model of future BYOD-SP. In the

i. we carry out the components in each of the procedures listed out in the official documentation released
ii. we did compare the components that being discussed from this systematic review.

Then, we proposed a theoretical perspective (conceptual framework) on security components were employed in answering our RQ2 (see Figure 4). In this study, we explore into two primary focal points that align with the BYOD reference component model, which should be the central considerations when formulating a BYOD-SP. The reference components will be compared to determine similarities and find suitable terminology for other components like "Knowledge," "Acceptable," etc., as well as elements within the Process components.

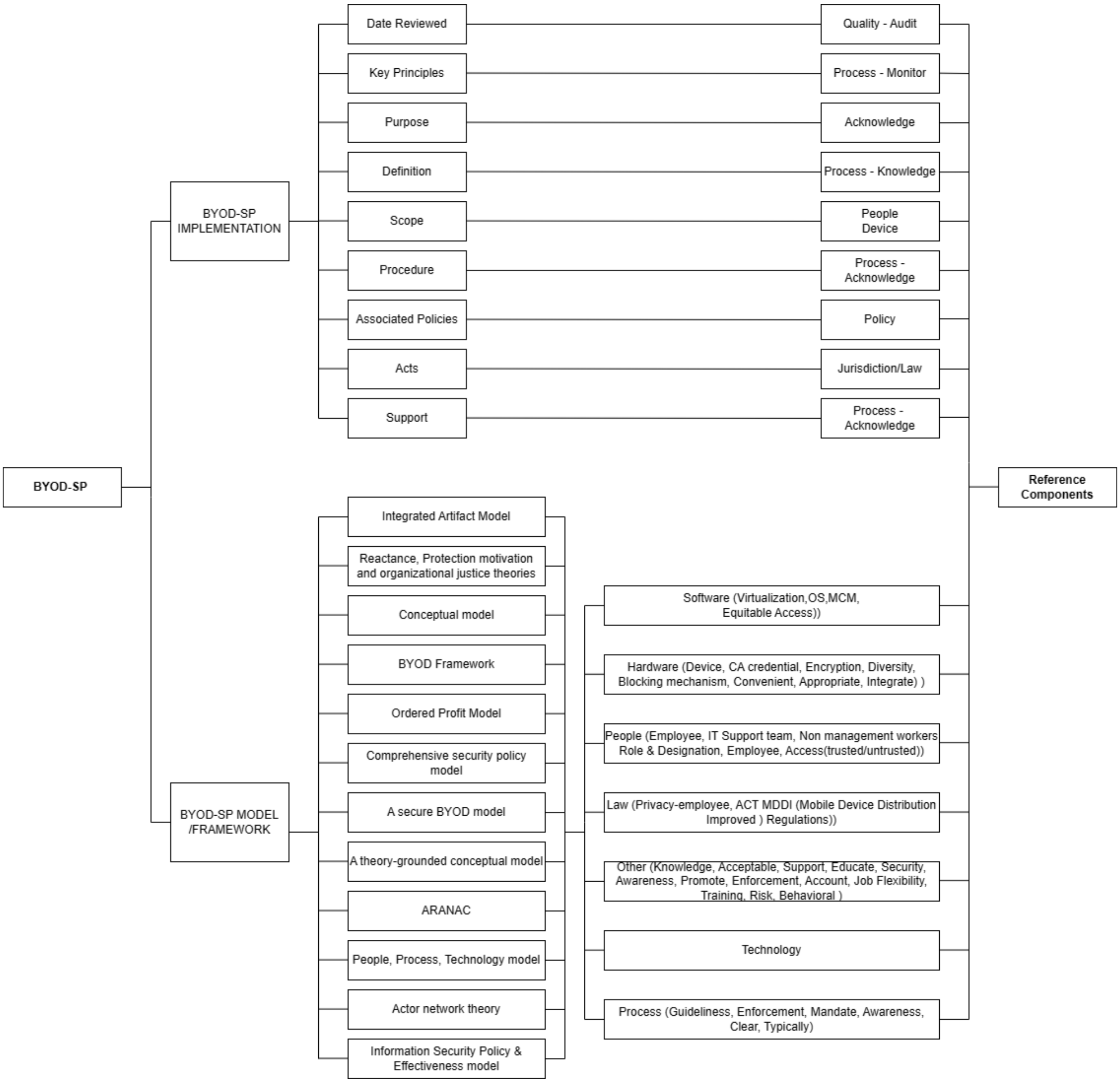
Date Reviewed
Key Principles
Purpose
Definition
BYOD-SP IMPLEMENTATION
Scope
Procedure
Associated Policies
Acts
Support
Quality - Audit
Process - Monitor
Acknowledge
Process - Knowledge
People Device
Process - Acknowledge
Policy
Jurisdiction/Law
Process - Acknowledge
BYOD-SP
Reference Components
Integrated Artifact Model
Reactance, Protection motivation and organizational justice theories
Conceptual model
BYOD Framework
Ordered Profit Model
Comprehensive security policy model
BYOD-SP MODEL /FRAMEWORK
A secure BYOD model
A theory-grounded conceptual model
ARANAC
People, Process, Technology model
Actor network theory
Information Security Policy & Effectiveness model
Software (Virtualization,OS,MCM, Equitable Access))
Hardware (Device, CA credential, Encryption, Diversity, Blocking mechanism, Convenient, Appropriate, Integrate))
People (Employee, IT Support team, Non management workers Role & Designation, Employee, Access(trusted/untrusted))
Law (Privacy-employee, ACT MDDI (Mobile Device Distribution Improved) Regulations))
Other (Knowledge, Acceptable, Support, Educate, Security, Awareness, Promote, Enforcement, Account, Job Flexibility, Training, Risk, Behavioral)
Technology
Process (Guideliness, Enforcement, Mandate, Awareness, Clear, Typically)

Fig. 4. Conceptual Framework (Reference Model of BYOD-SP)

5. Conclusion

This research conducted an examination of 16 studies and utilized a systematic literature review approach to identify the components of BYOD-SP. Additionally, the study uncovered relevant theories of BYOD-SP and a reference model that can be adapted to create a comprehensive security policy specifically tailored to the educational sector, with a focus on the situation in Malaysia, its implication and future directions of BYOD-SP topics and limitations in previous discussion.

5.1 Summary of Findings

Based on our understanding, the discoveries inspire us to delve deeper into the essential elements that must be taken into account when designing the BYOD-SP, especially in today's tech-savvy era where an array of technologies is integrated into the practice of BYOD. These elements should be robust and are seen as the building blocks of a reference model within BYOD-SP documentation. The official blueprint for BYOD-SP should be developed with a comprehensive list of identified features, encompassing Software, Hardware, Personnel, Legal aspects, Technology, Processes, or any other pertinent categories, which should be organized as distinct components integrated into the reference model for BYOD-SP.

This study also suggests that the top management should take significant steps to create a dedicated official documentation for BYOD-SP, considering the increasing prevalence of BYOD in teaching and learning sessions. Furthermore, it emphasizes that BYOD should not merely be treated as a subsection within general ICT policies. At present, only a limited number of higher education institutions in Malaysia have incorporated dedicated BYOD practices into their ICT policies, and the development of BYOD-SP may have been unclear, making it challenging for stakeholders to devise robust solutions.

5.2 Limitation & Future Directions

While we made an integrated effort to comprehensively create keywords and key phrases, it is believable that certain synonyms may have been overlooked. Glitch in the generation of keywords and key phrases could impact the search results during the SLR development process. Additionally, it is important to note that this study exclusively encompasses literature from English-language journals and conference articles, which potentially excludes other applicable articles not featured here. In future endeavours, this study intends to explore the perspective of management regarding the BYOD phenomenon and the development of BYOD-SP documentation, potentially aiming to establish a reference model for its components. Through the findings, gaps within the research field have been identified that can be proposed as future exploration.

Acknowledgement

This research was funded by grants from University College TATI under Short Term Grant No. GPJP2022 / 9001-2202 and Universiti Teknologi MARA under Geran Insentif Penyeliaan (GIP) Ref No. 600-RMC/GIP 5/3 (117/2023). We would like to express gratitude to University College TATI and Universiti Teknologi MARA for the grants of this study. We also sincerely appreciated the reviewers' valuable and constructive comments in helping us to produce this paper.

References

[1] Jie, C. Y., and N. Mat Ali. "COVID-19: What are the challenges of online learning? A literature review." *International Journal of Advanced Research in Future Ready Learning and Education* 23, no. 1 (2021): 23-29.

[2] Sushil, Gaikwad Sarita, Rajesh K. Deshmuk, and Aparna A. Junnarkar. "Security Challenges and Cyber Forensics For IoT Driven BYOD Systems." In *2022 IEEE 7th International conference for Convergence in Technology (I2CT)*, pp. 1-7. IEEE, 2022. https://doi.org/10.1109/I2CT54291.2022.9824368

[3] Kim, Kyong-jin, and Seng-phil Hong. "Study on enhancing vulnerability evaluations for BYOD security." *International Journal of Security and Its Applications* 8, no. 4 (2014): 229-238. https://doi.org/10.14257/ijsia.2014.8.4.20

[4] Kang, Qiao, Lei Xue, Adam Morrison, Yuxin Tang, Ang Chen, and Xiapu Luo. "Programmable {In-Network} security for context-aware {BYOD} policies." In *29th USENIX Security Symposium (USENIX Security 20)*, pp. 595-612. 2020.

[5] Scott, Ben, Raina Mason, and Patryk Szewczyk. "A snapshot analysis of publicly available BYOD policies." In *Proceedings of the 2021 Australasian Computer Science Week Multiconference*, pp. 1-6. 2021. https://doi.org/10.1145/3437378.3437394

[6] Soubhagyalakshmi, Pullagura, and Kalli Satyanarayan Reddy. "An efficient security analysis of bring your own device." *IAES International Journal of Artificial Intelligence* 12, no. 2 (2023): 696. https://doi.org/10.11591/ijai.v12.i2.pp696-703

[7] Chen, Yang, Hong-chao Hu, and Guo-zhen Cheng. "Design and implementation of a novel enterprise network defense system bymaneuveringmulti-dimensional network properties." *Frontiers of Information Technology & Electronic Engineering* 20, no. 2 (2019): 238-252. https://doi.org/10.1631/FITEE.1800516

[8] Ratchford, Melva, Omar El-Gayar, Cherie Noteboom, and Yong Wang. "BYOD security issues: A systematic literature review." *Information Security Journal: A Global Perspective* 31, no. 3 (2022): 253-273. https://doi.org/10.1080/19393555.2021.1923873

[9] Jamal, Fara, Mohd Taufik Abdullah, Azizol Abdullah, and Zurina Mohd Hanapi. "Enhanced bring your own device (BYOD) environment security based on blockchain technology." *International Journal of Engineering & Technology* 7, no. 4.31 (2018): 74-79. https://doi.org/10.14419/ijet.v7i4.31.23345

[10] Othman, Noor Ashitah Abu, Azah Anir Norman, and Miss Laiha Mat Kiah. "Information system audit for mobile device security assessment." In *2021 3rd International Cyber Resilience Conference (CRC)*, pp. 1-6. IEEE, 2021.

[11] Palanisamy, Rathika, Azah Anir Norman, and Miss Laiha Mat Kiah. "Compliance with Bring Your Own Device security policies in organizations: A systematic literature review." *Computers & Security* 98 (2020): 101998. https://doi.org/10.1016/j.cose.2020.101998

[12] Mahariya, Satish Kumar, Awaneesh Kumar, Rajesh Singh, Anita Gehlot, Shaik Vaseem Akram, Bhekisipho Twala, Mohammed Ismail Iqbal, and Neeraj Priyadarshi. "Smart campus 4.0: Digitalization of university campus with assimilation of industry 4.0 for innovation and sustainability." *Journal of Advanced Research in Applied Sciences and Engineering Technology* 32, no. 1 (2023): 120-138. https://doi.org/10.37934/araset.32.1.120138

[13] Minister's, Economic Planning Unit Prime. "Department,"Malaysia Digital Economy Blueprint,"." *Econ. Plan. Unit Prime Minist. Dep* (2021): 104.

[14] Bahaddad, Adel A., Khalid A. Almarhabi, and Ahmed M. Alghamdi. "Factors affecting information security and the implementation of Bring Your Own Device (BYOD) Programmes in the Kingdom of Saudi Arabia (KSA)." *Applied Sciences* 12, no. 24 (2022): 12707. https://doi.org/10.3390/app122412707

[15] Page, Matthew J., Joanne E. McKenzie, Patrick M. Bossuyt, Isabelle Boutron, Tammy C. Hoffmann, Cynthia D. Mulrow, Larissa Shamseer *et al.,* "The PRISMA 2020 statement: an updated guideline for reporting systematic reviews." *bmj* 372 (2021).

[16] Sierra-Correa, Paula Cristina, and Jaime Ricardo Cantera Kintz. "Ecosystem-based adaptation for improving coastal planning for sea-level rise: A systematic review for mangrove coasts." *Marine Policy* 51 (2015): 385-393. https://doi.org/10.1016/j.marpol.2014.09.013

[17] Rajapaksha, Nirusha. "Bring Your Own Device (BYOD): Existent State, Issues, and solutions."

[18] Bello, A. G., D. Murray, and J. Armarego. "Information & Computer Security Article Information." *Information & Computer Security* 23, no. 2 (2015): 145-60.

[19] Almaiah, Mohammed Amin, Sarra Ayouni, Fahima Hajjej, Abdalwali Lutfi, Omar Almomani, and Ali Bani Awad. "Smart mobile learning success model for higher educational institutions in the context of the COVID-19 pandemic." *Electronics* 11, no. 8 (2022): 1278. https://doi.org/10.3390/electronics11081278

[20] Chen, Hao, Ying Li, Lirong Chen, and Jin Yin. "Understanding employees' adoption of the Bring-Your-Own-Device (BYOD): the roles of information security-related conflict and fatigue." *Journal of Enterprise Information Management* 34, no. 3 (2021): 770-792. https://doi.org/10.1108/JEIM-10-2019-0318

[21] Shah, Nazaraf, and Arun Shankarappa. "Intelligent risk management framework for BYOD." In *2018 IEEE 15th International Conference on e-Business Engineering (ICEBE)*, pp. 289-293. IEEE, 2018.

[22] Halim, Izzah Inani Abdul, Alya Geogiana Buja, Mohd Shah Shafie Idris, and Nurul Jannah Mahat. "Implementation of BYOD Security Policy in Malaysia Institutions of Higher Learning (MIHL): An Overview." *Journal of Advanced Research in Applied Sciences and Engineering Technology* 33, no. 2 (2023): 1-14. https://doi.org/10.37934/araset.33.2.114