applied sciences

Article

Factors Affecting Information Security and the Implementation of Bring Your Own Device (BYOD) Programmes in the Kingdom of Saudi Arabia (KSA)

Adel A. Bahaddad [1,*], Khalid A. Almarhabi [2] and Ahmed M. Alghamdi [3]

[1] Department of Information System, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah 21589, Saudi Arabia
[2] Department of Computer Science, College of Computing in Al-Qunfudah, Umm Al-Qura University, Makkah 24381, Saudi Arabia
[3] Department of Software Engineering, College of Computer Science and Engineering, University of Jeddah, Jeddah 21493, Saudi Arabia
* Correspondence: dbabahaddad10@kau.edu.sa

Abstract: In recent years, desktop computer use has decreased while smartphone use has increased. This trend is also prevalent in the Middle East, particularly in the Kingdom of Saudi Arabia (KSA). Therefore, the Saudi government has prioritised overcoming the challenges that smartphone users face as smartphones are considered critical infrastructure. The high number of information security (InfoSec) breaches and concerns has prompted most government stakeholders to develop comprehensive policies and regulations that introduce inclusive InfoSec systems. This has, mostly, been motivated by a keenness to adopt digital transformations and increase productivity while spending efficiently. This present study used quantitative measures to assess user acceptance of bring your own device (BYOD) programmes and identifies the main factors affecting their adoption using the unified theory of acceptance and use of technology (UTAUT) model. Constructs, such as the perceived business (PT-Bs) and private threats (PT-Ps) as well as employer attractiveness (EA), were also added to the UTAUT model to provide the public, private, and non-profit sectors with an acceptable method of adopting BYOD programmes. The factors affecting the adoption of BYOD programmes by the studied sectors of the KSA were derived from the responses of 857 participants.

Keywords: bring your own device (BYOD); information security; Saudi Arabia

check for updates

Citation: Bahaddad, A.A.; Almarhabi, K.A.; Alghamdi, A.M. Factors Affecting Information Security and the Implementation of Bring Your Own Device (BYOD) Programmes in the Kingdom of Saudi Arabia (KSA). *Appl. Sci.* **2022**, *12*, 12707. https://doi.org/10.3390/app122412707

Academic Editors: João M. F. Rodrigues, Pedro J. S. Cardoso and Cristina Portalés Ricart

Received: 11 October 2022
Accepted: 9 December 2022
Published: 11 December 2022

1. Introduction

More countries worldwide are prioritising the adoption of digital transformations that help them develop strategic objectives and amenities. Digital transformations convert the existing models of private businesses and government institutions into new models that are based on human resource (HR) management, product manufacturing, and the provision of digital technology services. [1]. The primary objective of a basic digital transformation is to develop a business model that ensures that the organisation grows with the current technological trends, promotes operational competence, and reduces errors [2]. It also efficiently improves customer and employee satisfaction, increases income, and fosters creativity. [3]. The World Competitiveness Centre of the Institute for Management Development (IMD) in Lausanne, Switzerland developed the World Digital Competitiveness (WDC) index to gauge the rivalry and digitalisation status of every nation.

The advent of the coronavirus disease 2019 (COVID-19) forced the communications sector to look beyond its outdated methods of acquiring information. This is because the sector is not only responsible for controlling the use of data and digital platforms as well as the personal content of individuals, institutions, and states but also for guaranteeing the growth of social and economic activities despite the implementation of lockdowns and social distancing measures in most countries [4]. The KSA used the pandemic as an opportunity to hasten their digital migration by developing initiatives that improved the electronics trade and encouraged private businesses and government institutions to introduce digital amenities that meet consumer demands [5].

The government of the KSA has supported digital transformation in several ways. As outlined in the Saudi Vision 2030 Plan, the government endeavours to develop mutual amenities for all its administrative agencies [6] to increase quality, reduce costs, combine efforts, and form a positive work environment for every individual. The government will also support their adoption of online applications, such as HR management systems, cloud applications, and data-sharing platforms. Furthermore, the Supreme Royal Decree number 7/B/33181, which was established on 7 September 2003, aims to completely transform Saudi Arabian society into an information and technology (IT)-based society with electronic access to government services [7]. The KSA is also a member of the G20, which prioritises uniting unique and growing industrialised economies to deliberate on vital global issues. It also emphasises digitalisation, wherein information is converted into a computer-readable format by arranging the data into bits [8].

Bring your own device (BYOD) programmes are one of the most appropriate methods that a country can use to accomplish digital transformations on a national scale. The method, which allows employees to connect personal devices such as their smartphones, tablets, and personal computers to the setup and systems of the organisation [9], grew in popularity after Cisco Systems, Inc. implemented it in 2009 [10] and due to IT consumerism. Employers generally allow employees to use their own personal mobile phones as they have better features. Some of the advantages of BYOD programmes are less cost and increased user productivity. Additional advantages also include savings on procurement, software, hardware, service agreements, insurance, and licensing [11]. Bring your own device (BYOD) programmes significantly increase employee mobility, productivity, satisfaction, and flexibility. They also increase efficiency as most employees are experts at using their own personal devices, thereby reducing the need for training [12]. Apart from that, BYOD programmes also allow individuals in rural areas to access services at affordable rates. Employees who use their own personal devices are also more diligent for the most part [13]. Furthermore, BYOD programmes facilitate instantaneous information sharing and communication anywhere, without local area network (LAN) or wireless fidelity network (Wi-Fi) availability [14].

However, BYOD programmes are not without their challenges. This includes data breaches if the personal device is stolen or lost as well as a lack of protective safeguards, such as antivirus software and firewalls. The high IT cost of supporting personal devices is also a challenge. Furthermore, personal devices also lack network management and controls [15–17].

Another drawback of BYOD programmes, in both an organisational and state setting, occurs when multiple users request the same data at the same time. In such cases, leaders must consider these multiple requests simultaneously. This requires conceptualising the network processes that administrators, end-users, and organisations use. Leaders must also evaluate the incorporation of business devices with personal devices and the complexity of accessibility governance in instances where there is transfer in addition to the storage of end-user information.

Network expandability and the number of approved users further complicate the management of multiple business networks. Therefore, it is evident that the policies of BYOD programmes could present additional threats that complicate the security governance of the IT divisions that manage these complex networks.

Many researchers believe that it is essential to examine the advantages and disadvantages of adopting BYOD programmes as it will help various institutions manage information more efficiently. Nevertheless, studies on the security necessities and governance approaches of BYOD programmes remain limited. Therefore, organisations should prioritise identifying the factors that affect the willingness of employees to use their own personal devices for work-related purposes to recognise the benefits of BYOD policies.

This present study examined the critical concerns associated with BYOD policies by establishing a correlation between the various behavioural aspects that hinder end-users from integrating the multiple requirements and responsibilities of BYOD programmes. It also examined the BYOD solutions that appeal to end-users and the incentives that motivate BYOD adoption, in accordance with the current BYOD regulations. Numerous factors directly and indirectly affect the regional advancement of information and communications technology (ICT). Regional ICT growth is tricky as it requires the adoption of a multidimensional viewpoint. Furthermore, different ICT infrastructures, such as change management and leadership roles, have distinct features. Differences in regulatory and cultural environments also cause unusual challenges. This present study only evaluated the status of BYOD programmes in the KSA.

One of the main aims of this present study was to identify the factors that lead to the successful adoption of BYOD policies in instances where the technology improves and the policies become outdated. The disadvantages that this present study assessed were obtained from the end-users and were based on the factors that would motivate them to participate in a BYOD programme. The benefits of BYOD programmes, particularly their influence on staff productivity, as well as their limitations in terms of how individuals, particularly employees who are involved in critical infrastructure, utilise their personal devices, were also examined. Therefore, the primary objective of this present study was to develop a flexible and valid BYOD policy model that can be adapted to any form of critical infrastructure.

The following four sub-questions helped realise the primary objectives:

1. What are the factors affecting the adoption of BYOD programmes?
2. Which of these factors closely relate to security and privacy concerns?
3. To what extent do these factors affect the adoption of BYOD programmes by Saudi citizens?
4. Based on these factors, what criteria and policies do BYOD programmes have to adopt to become a reality?

For successful BYOD adoption to occur, the current BYOD policies for maintaining information security (InfoSec), facilitating BYOD adoption, and the degrees of enrolment warrant further investigation. The findings of this present study will benefit businesses and government institutions alike as both stakeholders are affected by mobile technology trends. Therefore, examining how different guidelines affect successful BYOD adoption will help pinpoint specific policies that significantly affect its implementation. This will provide stakeholders with valuable insights that can then be used to develop new BYOD frameworks dedicated to crucial infrastructures. A quantitative study that involved 857 participants from the public, private, and non-profit sectors was conducted to identify the factors that affect the perceived level of safety of participating in a BYOD programme at a Saudi Arabian organisation.

This present study begins with a brief description of the concept of digital transformation followed by an evaluation of the meaning and benefits of BYOD. The goals and questions of this study are also discussed. A thorough assessment of the factors affecting InfoSec and BYOD adoption in Saudi Arabia is then conducted. The results of this data analysis and the methodology are then explained before the main findings and conclusions are discussed.

The contributions of this study are primarily focused on measuring the level of PT-Bs and PT-Ps as well as the EA ability to track, which represent new entities that would be useful to add to the UTAUT model in order to measure the behavioural intention to provide the public, private, and not-for-profit sectors with an acceptable way to adopt a BYOD approach.

2. Literature Review

The reviewed studies provided various factors affecting user acceptance of BYOD programmes. This present study focused on two types of studies that aid the large-scale adoption of BYOD programmes. This included studies that used theories, such as Ground Theory, to examine the influencing factors as well as studies that applied specific theoretical frameworks. The theory-based studies conducted surveys to compile a list of factors that increase the confidence and willingness of a specific target audience to accept and participate in BYOD programmes while the theoretical framework-based studies conducted in depth examinations of frameworks and their deep structures across diverse fields and aspects of work to gather more knowledge and develop a better understanding of the applicable aspects of BYOD programmes. This was accomplished by studying the multiple factors of varying industries to ensure that they all have a similar degree of influence on BYOD programmes. This present study examined the types of studies to identify the relevant and irrelevant factors that directly affect user adoption and willingness to participate in BYOD programmes in the light of their increased adoption by government sectors and concerns over InfoSec. These results were then used to develop a flexible framework that can be adapted to address the concerns of the public and private sectors.

Some studies focused on identifying the potential risks then developed frameworks and policies for BYOD programmes [18,19], focused on the adoption of BYOD programmes in the private sector, and identified multiple risks that average employees and decision-makers perceive. As observed, most private organisations adopt BYOD programmes as it lowers cost and increases employee productivity. However, weak BYOD restrictions and policies as well as a failure to develop better security measures negatively affect the growth and efficacy of BYOD programmes at organisations [18,19]. Meanwhile, Sadiku et al. [20] identified the challenges and benefits of using personal laptops, smartphones, tablets, and USB drives at work [21]; however, they also established the importance of developing BYOD policies that mitigate security risks and increase employee productivity. The study also developed generally applicable best practices and policies that organisations can use to overcome the challenges of BYOD programmes [21]. According to Downer and Bhattacharya [22], the increased adoption of BYOD programmes is one of the main challenges of the InfoSec industry. As such, the study used frameworks and policies that are currently practised in the security industry to develop comprehensive frameworks as well as security, growth, integrity, and data privacy solutions for BYOD programmes [22].

One of the biggest challenges that BYOD programmes faced at the beginning of this decade was privacy and the protection of confidential and sensitive data from breaches and leaks. As such, multiple studies have developed various solutions that help increase privacy levels. Saa et al. [23] developed solutions for the higher education sector of Ecuador by focusing on the four main axes that directly correlate with BYOD programmes, namely, prior BYOD knowledge, preferred methods of using BYOD programmes in the education industry, security and network vulnerabilities, and work efficiency by adopting BYOD programmes in the higher education system [23]. Musarurwa [24], however, implemented BYOD programmes in the education and medical sectors of Zurich University Hospital to increase organisation and work efficiency and manage medical, nursing, and administrative processes in an optimal way [24]. Multiple studies indicate the importance and flexibility of using BYOD programmes in the higher education sector and focus on the implications of data breaches or loss, how to raise awareness to preserve and protect data, and technical security solutions with clear policies that help improve BYOD control [25–28].

Other BYOD-related studies examine its use in diverse applications, such as electronic payment and other electronic services. For instance, [29] outlined the importance of developing software and privacy policy frameworks that increase the adoption and acceptance of mobile electronic payment methods such as e-wallets. It also examined how to use e-wallets during the COVID-19 pandemic and provided mobile application ideas that can be used to expand the marketplace of mobile payment service providers. It also proposed the use of e-wallets that are not linked to bank accounts and that rely, instead, on loyalty-based electronic payment methods at companies and large stores than can be converted into cash in the future [29]. Meanwhile, Jamal et al. compared the current BYOD authentication techniques and classified them according to the level of security. They examined 25 proposals from multiple industrial and academic fields that implement BYOD policies that enhance security and detect data leaks in organisations. The outcome of this study could increase the adoption of BYOD programmes by both profit and non-profit organisations [30]. Ubene et al. examined the insurance sector of Nigeria, which works with multiple partners and serves diverse clients from the public and private sectors. The study found that some of the technical levels of these insurance organisations used data that was primarily collected via telephone interviews and questionnaires. This could negatively impact data entry operations in the system infrastructure and their clients [31].

Multiple studies combined theoretical and practical aspects to develop theory–practical frameworks that bridge the gap between the importance of BYOD adoption and innovative solutions that benefit commercial and non-commercial sectors. For instance, [18] used the plan–do–check–act (PDCA) cycle to formulate BYOD policies that benefit users and the organisation [18]. Both [29] and Retnowardhani et al. [32] examined the benefits of a BYOD policy that activates encryptions for e-wallets and other electronic payment methods. Meanwhile, Neves and Mello [33] used common enterprise frameworks, such as ISO 27002:2005, and the practical controls of the Centre of Internet Security (CIS) to develop adequate BYOD policies. Shrestha and Thakur suggested using multiple additional institutional cybersecurity frameworks, such as those outlined by the National Institute of Standards and Technology (NIST), the European Network and Information Security Agency (ENISA), the Control Objectives for Information Technologies (COBIT 5), and the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) (ISO / IEC 27001), to fine-tune the handling of BYOD programmes [34]. Koesyairy et al. [35,36], similarly, focused on the application of institutional cybersecurity frameworks in the Indonesian and South African banking sectors, respectively. The Indonesian banking sector adheres to the POJK 1/POJK.07/2013 regulations of the Otoritas Jasa Keuangan (OJK) to decrease the number of security incidents and ensure compliance with internal security policies, which need to be implemented in BYOD programmes. This is because the InfoSec rules of BYOD programmes must be standardised to ensure the continued safe use of BYOD programmes, sensitive data, InfoSec, and data security frameworks [33].

Meanwhile, other extant studies have examined the status of BYOD acceptance and methods of increasing user acceptance. Krey [26] proposed using a BYOD programme for enterprise mobility management (EMM) in the medical sector. The study developed a new method of introducing mobile strategies to the closely intertwined organisational and social structures of hospitals as well as measured user acceptance using a BYOD and EMM framework [26]. Gupta et al. [37], however, used the technology acceptance model (TAM) framework and structural equation model (SEM) to identify and quantify the factors that affect the acceptance and willingness of healthcare professionals to participate in a BYOD programme based on the BYOD policies of an organisation. Moore examined the perceived usefulness and perceived ease of using a BYOD programme to better understand its adoption by a specific American governmental sector [38]. Multiple studies have also used theoretical frameworks that are more advanced than the extended technology acceptance model (TAM 2) and contain more precise determinants of organisational acceptance and user acceptance of BYOD programmes. For instance, El-Gbouri and Mensch [39] used the unified theory of acceptance and use of technology (UTAUT) model to examine themes, such as convenience, personal data security, privacy, and trust in the organisation, that most organisations seriously consider before adopting a BYOD programme [39]. Similarly, [40] used an improved coping model of user adaptation (CMUA) framework to explore behaviours related to the perception of business results with IT and the strategies that organisations use to address threats or mistrust of the devices that are used in BYOD programmes [40].

3. Theoretical Framework

As seen in the literature review, many practices and theoretical frameworks have been developed using standards and rules to comprehensively address the concerns that governmental and semi-governmental organisations have prior to BYOD adoption [26]. Many studies have also developed standards and rules as theoretical frameworks for BYOD adoption. However, few have outlined the practices, factors, restrictions, standards, and rules that increase user acceptance and willingness to participate in a BYOD programme in a work environment [41]. There is an overlap between studies that examine the standards and rules of working in a BYOD programme, user acceptance of BYOD standards and rules, and the positive and negative effect of BYOD standards and rules on BYOD growth as well as identifying and using the factors that affect stakeholder acceptance of BYOD in a proper framework. Nevertheless, this could simultaneously increase the credibility of BYOD programmes and user acceptance [42].

The first question to be addressed in this literature review was, "What are the factors affecting the adoption of BYOD programmes by employees at Saudi Arabian organisations?" Therefore, the intention of employees to participate in a BYOD programme daily had to be evaluated. This was accomplished by using leads to identify the basic and dependent variables that were then used to build the hypotheses and calculate the relevant variables [26]. The TAM model that Davis developed, and which multiple studies have since used, is one of the most popular models for demonstrating and understanding behavioural intent (BI) to accept or reject an innovative technology [37]. It is also one of the most well-established models in research due to its simplicity and adaptability [42]. Several studies have concluded that the TAM model is of tremendous quality and provides statistically reliable results [26,37,38]. Therefore, the TAM model is a great framework for gauging user acceptance of new technologies and serves the purposes of this present study.

As BYOD programmes increase employee productivity and flexibility at work as well as reduce the organisation's capital expenditure on projects and service programmes regardless of industry, organisations can tout BYOD programmes as beneficial initiatives to their employees [21]. Multiple studies that have investigated the importance of employee compliance with BYOD InfoSec policies have concluded that self-efficacy, response effectiveness, threat severity, and the cost of compliance influence the motivations of employees to comply with BYOD policies. Meanwhile, other studies have examined BYOD programmes in multiple countries and proven that the UTAUT model is well suited to explaining the adoption of technology-related services across multiple cultures and traditions [42].

Of the many theoretical frameworks that have been used to examine BYOD programmes, a few have used the UTAUT model as it is examines consumer behaviour and the level of knowledge in terms of the acceptance of modern technologies. The UTAUT model, which supersedes the TAM model, was developed by [43] and examines the benefits of using a technology and the factors that motivate its adoption as well as influence BI and behaviours when using a technology. Therefore, this present study adopted the UTAUT model as it is the ideal for measuring theoretical structures according to moderators such as gender, age, and level of experience, which are essential factors when gauging acceptance and interest levels, especially in the governmental, semi-governmental, and non-profit sectors [43]. Multiple studies have also proven that the UTAUT model provides a highly accurate measure of the level of acceptance of electronic systems as shown in Figure 1. As such, the following eight basic constructs of user adoption of IT may affect the theoretical framework:

- Performance expectancy (PE)—three factors;
- Effort expectancy (EE)—three factors;
- Social influence (SI)—three factors;
- Perceived threats (PTs)—three factors;
- Perceived business threats (PT-Bs)—three factors;
- Perceived private threats (PT-Ps)—three factors;
- Employer attractiveness (EA)—three factors;

- Behavioural intention (BI)—three factors;

The four moderators that can be implanted in the UTAUT framework include gender, age, level of experience, and willingness to use [43]. Many fields have recently taken to using the UTAUT model [28,44]. As such, multiple studies have proven its efficacy in gauging the adoption of mobile innovations [45–47]. It has also been used to identify the potential factors that may motivate employee adoption of BYOD programmes in the future [48] as well as what organisations can do to increase employee willingness to adopt technical services [49,50]. Therefore, it is recommended to develop a UTAUT framework that can potentially increase the level of acceptance while simultaneously examining BYOD-related security issues and the potential acceptance and consumer effects from a security and InfoSec standpoint.

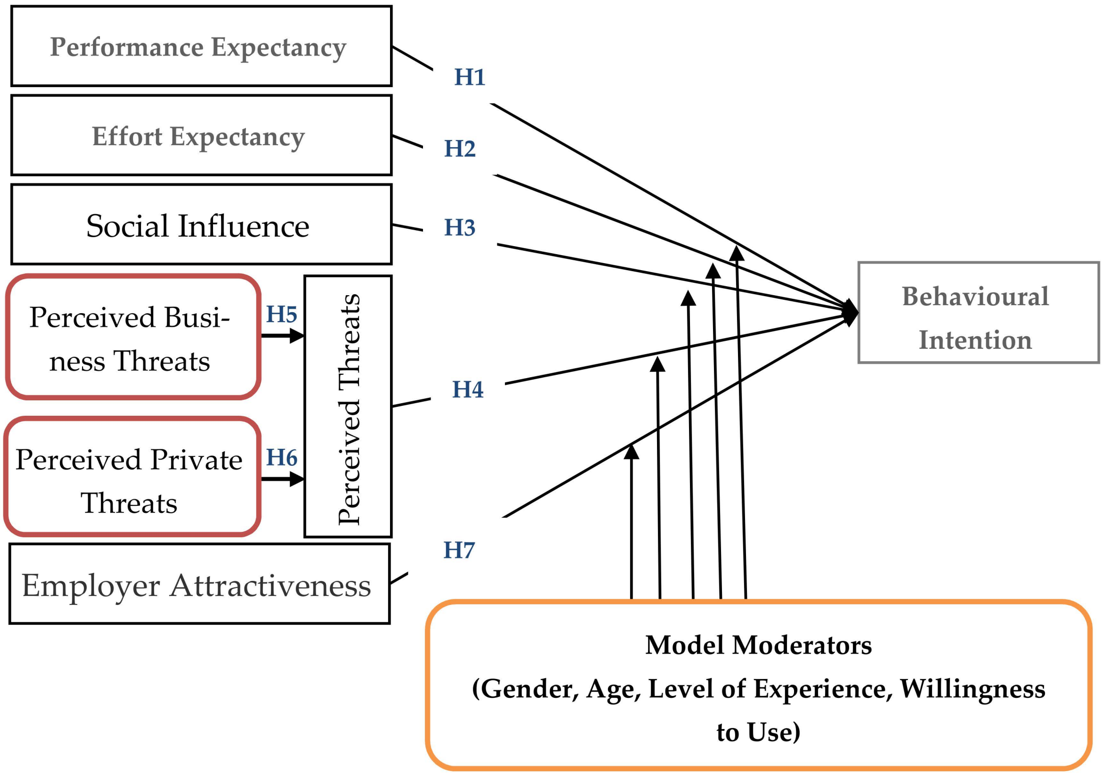

Figure 1. The modified UTAUT model for BYOD programmes.

As seen, the model depicts the influence of individual BIs on technology use [43], which directly depends on the four main factors of the UTAUT theoretical framework. Apart from the main constructs, gender, age, level of experience, and willingness to use moderate the correlation between these constructs and BI. More recently, [51] made two main modifications to the UTAUT model to adapt it to BYOD programmes and their requirements. These modifications excluded facilitating conditions, as the UTAUT model does not examine BYOD use behaviours, and included the addition of perceived threats (PTs) to examine the negative aspects of BYOD adoption and the use of personal devices to access work-related systems [44]. This present study further extended these modifications [51] by also examining how the factors of the theoretical framework affect the BI to adopt BYOD programmes across multiple industries, such as the military, education, commercial, and non-commercial sectors, that have varying uses and knowledge of BYOD programmes. This adds to the existing body of BYOD-related literature by providing useful insights on how to increase BYOD adoption globally.

According to the PTs, innovations may not always be beneficial. As the UTAUT model does not examine the negative factors that hinder BYOD adoption, the PTs were added according to the social cognitive theory (SCT) [52,53] and other major resistance theories in information-system-related literature [54–56]. Based on the concept of technology adoption and use disincentives, PTs are the degree to which an employee believes that participating in a BYOD programme carries threats that elicit anxious or emotional reactions, which, consequently, negatively affect adoption behaviours and acceptance. According to Niehaves et al., these threats can be distinguished into two main dimensions: threats that affect the PT-Ps and threats that affect the PT-Bs. Examples of PT-Ps include the loss of private data, the recovery of the private data of the organisation, and the blurring of the boundaries between private life and work. Therefore, any form of encroachment into the property of an individual could increase administrative corruption among the users [57]. Examples of PT-Bs include the loss of business data, damaging the corporate network with malware, and violating corporate policies [57]. As such, it is recommended to examine the PT-Ps and PT-Bs that generally affect intentions to adopt BYOD programmes.

Studies have also shown that adopting BYOD programmes may affect the motivations of an organisation to hire or reject future employees. For instance, if BYOD programmes influence the decisions of an individual decision-maker, it can be used as a reason to hire new employees or to retain existing employees by extending their employment contracts. Therefore, BYOD programmes can be used to increase the attractiveness of an organisation, which may increase the acceptance of BYOD programmes. Employer attractiveness (EA) is defined as the degree to which an individual is attracted to and accepting of an organisation or sector that adopts BYOD programmes. The BI of attractive work correlates positively with individuals who tend to adopt BYOD programmes. Therefore, the BI to adopt BYOD programmes is expected to be positive and will increase BYOD acceptance when opportunities for attractive work in an organisation that adopts BYOD programmes arise. Table 1 provides detailed definitions of the constructs and relevant hypotheses.

Table 1. Hypotheses and items.

Construct	Definition	Hypothesis No.	Hypothesis	Related Framework	Type	No. of Items
Performance Expectancy (PE)	The degree to which an individual believes that BYOD programmes increase their job performance	H1	PE factors will positively affect the BI to adopt BYOD programmes in the KSA	PE → BI	Reflective	3
Effort Expectancy (EE)	The degree of ease that an individual believes BYOD programmes will provide	H2	EE factors will positively affect the BI to adopt BYOD programmes in the KSA	EE → BI	Reflective	3
Social Influence (SI)	The degree of importance that an individual places on the opinions that others have of their participation in BYOD programmes	H3	SI factors will positively affect the BI to adopt BYOD programmes in the KSA	SI → BI	Reflective	3
Perceived Threats (PTs)	The degree of anxiety- and emotion-evoking threats that an individual associates with BYOD programmes	H4	PT factors will positively affect the BI to adopt BYOD programmes in the KSA	PT → BI	Formative	3
Perceived Private Threats (PT-Ps)	The degree to which an individual believes that BYOD programmes threaten their job	H5	PE factors will positively affect the PTs of adopting BYOD programmes in the KSA	PT-Ps → PT	Formative	3
Perceived Business Threats (PT-Bs)	The degree to which an individual believes that BYOD adoption threatens their private life	H6	PE factors will positively affect the PTs of adopting BYOD programmes in the KSA	PT-Bs → PT	Formative	3

Table 1. *Cont.*

Construct	Definition	Hypothesis No.	Hypothesis	Related Framework	Type	No. of Items
Employer Attractiveness (EA)	The degree to which an individual believes the attractiveness of an organisation increases if it adopts BYOD programmes	H7	EA factors will positively affect the BI to adopt BYOD programmes in the KSA	EA → BI	Reflective	3

In summary, a number of measurement elements were used from previous studies, and a number of elements were created based on discussion sessions with a number of interested employees who are working in the BYOD field and spreading awareness about this approach.

4. Methodology

An empirical study was conducted using employees from multiple government organisations as well as private organisations that have significant experience in government and semi-government transactions. As such, the population of the study included employees from the military, education, private, and non-profit sectors. The purpose of the study was to measure the efficacy of the proposed methods of increasing BYOD acceptance among existing and future employees. These proposed methods were obtained from extant studies. A survey was conducted as it best captures the opinions and perceptions of a target audience. The participants of this present study were technical or non-technical employees who were willing to adopt BYOD programmes and policies. To ensure that the participants could thoroughly and credibly evaluate BYOD programmes, only participants with years of BYOD knowledge and experience were invited to participate in the survey.

To retain scalability, some of the items were extracted from multiple extant technical studies. To link the elements of BYOD programmes with the theoretical framework of this present UTAUT-model-based study, the contexts of the questions of the theoretical framework were modified to better suit the survey. Multiple industry experts then reviewed the survey to determine if the measurement elements were able to answer and measure the combinations. A pre-pilot study was conducted to determine if all the indicators were clear and if all parts of the survey captured the verbal instructions. A pilot study was then conducted to ensure that the survey questions were easily understood and unambiguous. A standardised survey was then designed using integrated measuring elements and distributed via Google Forms to gather the required data. A total of 857 responses were obtained and reviewed to ensure that each respondent completed the entire survey. The number of incomplete responses did not exceed 5%. As such, the total number of complete responses was 822.

The survey contained closed-ended question that measured participant perceptions using a five-point Likert scale where 5 indicated strong agreement and 1 indicated strong disagreement. The survey consisted of three main components and collected the following: (1) demographic information, (2) the prevalence of using personal devices at work, and (3) the acceptance of BYOD practices in in-office and out-of-office settings. The samples were analysed and described using IBM® SPSS® Statistics 24 and IBM® SPSS® Amos™ 24, which are best suited for analysing complicated data and conducting an exploratory factor analysis (EFA) and confirmatory factor analysis (CFA).

5. Data Analysis and Main Findings

5.1. Data Sampling

According to the General Authority for Statistics (GaStat), in 2021, 8.09 million employees from various government and private sectors were registered at both the Social Insurance Pension Service and Public Pension Agency of the KSA (shorturl.at/elJP4). Workplaces in the KSA are distributed between the government, private, and non-profit sectors. Government sectors are completely supported by the state budget while semi-government sectors are business sectors that are completely under the purview of a government sector and work to support some of the tasks of the government sector in question. Meanwhile, the private sector consists of many companies and organisations that provide the KSA with reliable economic and commercial movement. The non-profit sector, however, comprises charitable societies that do not receive permanent financial support from the government or private sector of the KSA. Employees from three basic sectors, government, private, and non-profit, were the population of this present study.

As the participants had to be able to complete the survey, they had to possess some BYOD-related skills and knowledge as well as work with mobile devices. Therefore, prior to participating in the survey, potential participants were required to answer the following three questions: (1) Do you use your personal device to access the systems of the organisation? (2) Do you sometimes bring your personal device to work to complete some work on it? and (3) Do you possess basic BYOD-related knowledge and experience? The Raosoft formula was used to determine the minimum sample size required based on the number of employees at the time of the study (8.09 million) within a 5% margin of error and at a 99% confidence level. Therefore, the survey required at least 664 participants [58]. The actual number of participants was 857.

To ensure that the participants in the questionnaire represented the required sample in the best way, the conditional questions were set at the beginning page, which helped to nominate the right segment for the survey. Additionally, using the snowballing technique helped the survey reach the largest possible segment who were willing to participate based on the conditional criteria that were set at the beginning. Moreover, the participation in the questionnaire was voluntary so that the participant could leave to complete the participation at any time, and one of the conditions for accepting participation in the analysis stage in the participation was that 95% should be completed as a minimum.

After completing the data collection of the participants, all the results and analysis outcome were stored in the external repository for access at any time by the interested people to the results of this study. The link to the external repository is https://data.mendeley.com/datasets/3kkrsw92s8/1 (15 August 2022).

5.2. Appropriateness of Questions for the Target Audience

Two steps were used to ensure that the questions were correctly scaled for the relevant factors and clearly understood by the target audience. Firstly, a pilot study was conducted on 5% of the final sample size and the internal consistency between the answers was calculated to confirm that the observed percentage exceeded 0.6 (Table 2). Secondly, the survey was distributed on a larger scale using the snowball technique to reach the minimum required number of participants (664). The first section of the survey briefly outlined the purpose of the study, its research objectives, and the definition of BYOD programmes. Participants were also informed that participation was voluntary and that they could withdraw their participation without providing a reason.

Table 2. Frequency of responses of the examined means, SDS, skewness, and kurtosis.

Factor Code	Mean	SD	Skew	Kurtosis	Cronbach's Alpha	CR	AVE	Rotated Factor Loadings
PE1	3.81	0.927	−0.726	−0.278	0.766	0.6325	0.7821	0.689
PE2	3.65	0.873	−0.631	−0.474				0.827
PE3	3.91	0.943	−0.978	0.578				0.693
EE1	3.44	0.810	−0.372	−1.052	0.877	0.6111	0.8249	0.779
EE2	3.31	0.907	−0.235	−1.170				0.775
EE3	3.70	0.745	−0.751	−0.498				0.790

Table 2. *Cont.*

Factor Code	Mean	SD	Skew	Kurtosis	Cronbach's Alpha	CR	AVE	Rotated Factor Loadings
SI1	3.92	0.718	−0.859	0.302	0.619	0.6143	0.8266	0.807
SI2	3.71	0.704	−0.642	−0.221				0.781
SI3	4.29	0.878	−1.372	1.890				0.761
PT1	4.37	0.788	−1.340	2.058	0.699	0.6684	0.858	0.799
PT2	3.88	0.976	−0.862	0.471				0.843
PT3	4.02	0.926	−0.927	0.784				0.809
PT-B1	3.65	0.773	−0.631	−0.474	0.609	0.6513	0.7089	0.827
PT-B2	4.37	0.711	−1.340	2.058				0.279
PT-B3	3.88	0.976	−0.862	0.471				0.833
PT-P1	4.32	0.876	−1.429	2.016	0.639	0.6214	0.7693	0.673
PT-P2	4.16	0.938	−1.148	1.122				0.690
PT-P3	4.02	0.926	−0.927	0.784				0.809
EA1	4.32	0.876	−1.429	2.006	0.601	0.6392	0.6848	0.563
EA2	4.00	0.980	−0.998	0.727				0.792
EA3	4.29	0.878	−1.372	1.890				0.578
BI1	3.44	0.810	−0.372	−1.052	0.881	0.6191	0.8297	0.789
BI2	3.31	0.707	−0.235	−1.170				0.775
BI3	3.70	0.845	−0.751	−0.498				0.795

5.3. Demographic Questions and Content

The demographic questions were divided into five main sections. The first section collected basic characteristics, such as gender, age, and education level, while the second section collected job- and workplace-related information, such as whether the participant works in the government or private sector. The third section collected information on the nature of the participant's job at the organisation and their knowledge of the importance of adopting BYOD programmes in their sector. The fourth section collected information on the employment status of the participant and determined if any of the participants were not from the government or private sectors. Lastly, the fifth section collected information on the types of devices that the organisation provided the participants and the personal devices that the participants used to access the systems of the organisation (Table 3).

In summary, the demographic section of the survey collected the gender, age, employment status, and education level of the participants as well as the types of devices that the organisation provided them and the personal devices that they used to access the systems of the organisation. It also examined the use of personal devices in the workplace and work-completion behaviours outside of the workplace. The amount of missing data in any survey should not exceed 5% of its total questions [59,60]. Only 3.8% of the data in this present study were missing. This included participants who failed to complete the survey for technical reasons or left one or more entire sections of the survey unanswered. These responses (12) were excluded from the present study.

Table 3. The Total Variance Explained including Initial Eigenvalues and Sums of Squared Loadings.

Component	Initial Eigenvalues			Extracted Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	11.676	48.652	48.652	11.676	48.652	48.652
2	03.339	13.913	62.565	03.339	13.913	62.565
3	01.688	07.035	69.600	01.688	07.035	69.600
4	01.292	05.384	74.983	01.292	05.384	74.983
5	01.104	04.599	79.582	01.104	04.599	79.582
6	00.784	03.265	82.847	00.784	03.265	82.847
7	00.739	03.079	85.926	00.739	03.079	85.926
8	**00.586**	**02.443**	**88.369**	**00.586**	**02.443**	**88.369**
9	00.558	02.323	90.693			
10	00.527	02.197	92.890			

Note: Extraction method: PCA—eight components extracted.

5.4. Assessment of Standard Deviation (SD) and Normal Distribution

The standard deviation (SD) and the normal distribution are calculated to determine the level of data dispersion and the distance between the mean curve and the direction of the deviation [61]. The SD must not exceed 1.0. A low SD indicates that the values are spread out over a small area of the mean curve and that the sample size is a good representation of the target audience. Skewness and kurtosis tests are commonly used to determine normal distribution [60]. These values should range from 0 to 2.50 [59]. The skewness and kurtosis values of this present study ranged from −0.235 to 1.429 and −1.170 to 2.058, respectively, which were within the recommended range.

5.5. Reliability Scale

A reliability test was conducted using the quantitative data to ensure their reliability and the internal consistency of the structures of the proposed research model, which is a basic requirement when adapting a theoretical framework to ensure that abnormal elements are removed. As recommended by multiple meta-analyses [59,62], this present study used a minimum of 0.75. Table 2 depicts the Cronbach's alpha (α) of the eight constructs in the UTAUT framework. The α ranged from 0.601 to 0.880, indicating the internal consistency and reliability of the survey.

5.6. Exploratory Factor Analysis (EFA)

Exploratory factor analysis (EFA) helps determine the strength as well as the correlations between the items in a study [59]. Tests included in an EFA, namely, the Kaiser–Meyer–Olkin (KMO), Bartlett's B, and eigenvalue, determine how the elements of a construct correlate to each other, eliminate weak elements, and build an integrated model.

The KMO of this present study was 88.37%, which exceeds the recommended 68.13% for a sample test. The Bartlett's B appropriate level of correlation was also statistically significant at 0.001. Therefore, all 24 factors satisfied the original EFA tests. As seen in Table 3, which illustrates the structures, the next stage included internal rounds to extensively test the theoretical framework of the present study.

5.7. Confirmatory Factor Analysis (CFA)

A critical measurement test of a theory, CFA examines the links between structures and searches for important correlations between them [59,63]. As testing the validity of the constructs is a primary aim of data analysis, a CFA was conducted after internal consistency and reliability testing to fully assess the theoretical framework of this present study. One of the primary advantages of CFA is structural equation modelling (SEM), which is a subset that generates a more rigorous interpretation of a theoretical framework than EFA [59,64]. The results of the CFA refined and supported the conceptual framework of this present study.

5.8. Assessment of Model Fit and Measurement Model

A CFA enhances the measurement of the acceptance or rejection of a form. As such, it confirms the validity of a theoretical framework and identifies indicators that are unsatisfactory or that require improvement (Table 4). A CFA also contains the validity and reliability of SEM and specific measurement criteria that were used to assess the factors of BYOD programmes. Therefore, SEM was used to test the validity of the theoretical framework by examining and evaluating linear correlations between the constructs, which, in turn, was reflected in the hypothesis testing. Furthermore, the method test of a CFA ensures that a theoretical framework can be reused by other similar studies in the future [65]. As seen in Table 4, the internal measurements were calculated accurately. Composite reliability (CR) and the average variance extracted (AVE) are the most accurate tests of reliability and variance between factors. They can also be used in complex constructs and address the reliability of relevant constructs [66]. According to [67], the AVE should be used to measure the validity of model discrimination. The constructs of this present study correlated closely and are shaded in Table 4. A standardised CR of more than 0.6 [68] and an AVE of more than 0.5 are considered satisfactory [59]. Table 3 presents the AVE of this present study.

Table 4. Correlation matrix and discriminant validity of the measurement model, path coefficients, *t*-values, and *p*-values of the hypotheses.

Relationship or Path	PE	EE	SI	PT	PT-B	PT-P	EA	BI	Hypothesis No.	Estimate	*t*-Value (R^2)	Path	*p*-Value
PE	**0.796**								H1	0.739	8.722	PE → BI	***
EE	0.739 **	**0.823**							H2	0.888	6.168	EE → BI	***
SI	0.691 **	0.586 **	**0.803**						H3	0.644	10.020	SI → BI	***
PT	0.686 **	0.545 **	0.742 **	**0.847**					H4	0.697	8.596	PT → BI	***
PT-B	0.825 **	0.673 **	0.754 **	0.898 **	**0.853**				H5	0.845	9.718	PT-B → PT	***
PT-P	0.644 **	0.569 **	0.710 **	0.823 **	0.731 **	**0.870**			H6	0.698	11.598	PT-P → PT	***
EA	0.612 **	0.488 **	0.772 **	0.673 **	0.673 **	0.789 **	**0.84**		H7	0.732	10.086	EA → BI	***
BI	0.739 **	0.673 **	0.586**	0.565 **	0.673**	0.569 **	0.482 **	**0.843**					

** $p < 0.05$, *** $p < 0.001$.

5.9. Testing the Main Hypotheses

Three tests, *t*-value, *p*-value, and the standardised regression coefficient, were used to test the correlation between the constructs. The previous tests were conducted to identify weaknesses in the hypotheses (Hs) of this present study. The baseline values of H1 to H7 ranged from 0.888 to 0.644 and were statistically significant (0.001) while the coefficient of determination (R^2) ranged from 11.598 to 8.722, which exceeded the recommended 1.96. As seen in Table 4, all the factors met the acceptance criteria for the modulus structure model, a requirement of SEM. The results of the entire construct indicated the positive effects of using BYOD programmes in different environments as well as mobile devices and smartphones. Furthermore, the correlation between the structures of the theoretical framework and the constructs was significant (Table 4).

5.10. Testing the Moderator Hypotheses

One of the main reasons of using mediators in a UTAUT model is to investigate their effect on the acceptance and use of an electronic system as well as BYOD acceptance and adoption. According to Badwelan [69], different mediators influence different aspects that increase the acceptance of a technical system. The use of mediators is also one of the main aspects of theoretical models as they are based on the unique characteristics of a particular community [69]. A related previous study completed the basic analytical requirements and focused on the reliability and stability of the theoretical framework. It highlighted the four mediators: gender, age, level of experience, and willingness to use. The dataset was divided into two main groups for each mediator. Therefore, the participants were divided according to gender (male or female) as well as age (below or more than 40 years old as 40 is the midpoint of the working years). The participants were then divided according to level of experience (high = more than three years or low = less than three years) and willingness to use (high or low). Table 5 presents the participants according to the divisions.

The purpose of these guidelines was to identify differences between the characteristics of the participants and features of BYOD programmes according to individuals in the service and non-service industries. The correlation coefficients, critical ratios, and *p*-values of each construct were used to identify differences in the correlations between the constructs. The chi-square (χ2) and degree of freedom (df) are also necessary when calculating differences between vector groups. To calculate the path of the differences between the median groups, the gender, age, level of experience, and willingness to use of all 28 hypotheses had to be calculated to determine which path was significant to the model. Insignificant pathways were then removed and the effective pathways in the moderator groups were found. The χ2 and df of the restricted and unconstrained models were then calculated to determine the level of change in the ensemble model Δ ($df = 1$) and to identify significant pathways [65]. The participants were grouped according to the division of the mediators in the theoretical model. Table 5 presents the total number of participants in each division. The correlation between the constructs in terms of gender was:

$$\mathbf{PE \rightarrow BI;\ EE \rightarrow BI;\ SI \rightarrow BI;\ PT \rightarrow BI;\ PT\text{-}P \rightarrow PT;\ PT\text{-}B \rightarrow PT;\ EA \rightarrow BI}$$

Table 5. Sample distribution across four moderator groups.

Moderator	**Group Level**	**Sample Distribution by Moderator Group**	
		Numbers	**Percentage**
Gender	Male	745	86.94%
	Female	112	13.06%
Age	Over 40 Years old	431	50.29%
	Below 40 years old	426	49.71%
Experience	High	334	38.94%
	Low	523	61.06%
Voluntariness of Use	High	579	67.55%
	Low	278	32.45%

As all the correlations were significant, gender reflected high interest in using laptops and smartphones in BYOD programmes in the government, private, and non-profit sectors. The results of the restricted and unrestricted tests indicated insignificant differences between men and women and significant correlations between PE, EE, SI, PT, PT-P, PT-P, and EA with BI in both men and women.

Age was an important moderator of BYOD acceptance as well as laptop and smartphone use; which was 50.3% and 49.71%, respectively. The age of more or less than 40 years old is the midpoint of working life. Reflective correlations based on the experience of the mediator indicated some differences between the older ages and those unwilling to conduct work on their personal devices. As such the PT → BI, PT-B → PT, and PT-P → PT correlations were insignificant. By contrast, the under 40 group indicated that technical aspects were an important part of their lives. Therefore, there were significant results in all the hypotheses and differences between the characteristics of these two groups (Table 6).

Level of experience was a key moderator due to its importance in BYOD acceptance as well as laptop and smartphone use. As many as 38.98% and 61.06% of the participants reported high and low levels of experience with BYOD programmes, respectively. The reflected correlations of the level of experience mediator were similar with those of the gender mediator. The correlations between participants who reported high and low levels of experience were all significant.

The willingness to use laptops and smartphones is a main factor that increases productivity and flexibility. However, the participants reported that they wanted educational applications that teach them how to use BYOD programmes and that it would increase their desire and willingness to learn. An analysis of the willingness to use moderator showed that 67.57% and 32.45% of the participants indicated high and low readiness, respectively. The correlations between PE → BI, EE → BI, and SI → BI were insignificant with respect to both high and low willingness to use but other putative correlations were significant (Table 6). As seen, most of the putative pathways for gender, age, level of experience, and willingness to use were significant and meaningful with respect to the sample. Furthermore, EA, PT-B, and PT-P were also significant in both sections of each of the four moderators.

Table 6. Summary of path coefficients, *t*-values, and *p*-values of gender and experience moderators.

Gender		Male, N = 745, 86.94%			Female, N = 112, 13.07%			Constrained Model		Unconstrained Model		Δ (*df* = 1)	Testing Result
		Estimate	*t*-Value	*p*	Estimate	*t*-Value	*p*	2	*df*	χ2	*df*		
H1	PE → BI	0.563	5.012	***	0.652	6.560	***	3545.3	57	3650.9	50	4.4	Supported
H2	EE → BI	0.645	4.992	***	0.640	6.150	***	3335.8	55	3251.2	51	6.6	Supported
H3	SI → BI	0.725	6.445	***	0.515	7.231	***	3440.5	56	3451.1	52	7.8	Supported
H4	PT → BI	0.653	5.850	***	0.612	5.395	***	3296.2	58	3284.6	53	8.6	Supported
H5	PT-B → PT	0.695	6.845	***	0.601	7.210	***	3460.8	58	3449.9	52	10.9	Supported
H6	PT-P → PT	0.605	6.145	***	0.632	7.054	***	3170.8	57	3159.9	53	10.9	Supported
H7	EA → BI	0.622	5.012	***	0.752	6.801	***	3256.8	59	3243.9	54	12.9	Supported
Age		Old—More Than 40 Years Old, N = 431, 50.03%			Young—less Than 40 Years Old, N = 426, 49.71%			Constrained Model		Unconstrained Model		Δ (*df* = 1)	Testing Result
		Estimate	*t*-Value	*p*	Estimate	*t*-Value	*p*	χ2	*df*	χ2	*df*		
H8	PE → BI	0.674	6.712	***	0.585	5.112	***	3479.7	51	3473.3	49	6.4	Supported
H9	EE → BI	0.662	6.162	***	0.667	5.092	***	3339.7	52	3323.3	48	16.4	Supported
H10	SI → BI	0.537	7.331	***	0.747	6.545	***	3409.7	51.5	3398.3	48.5	11.4	Supported
H11	PT → BI	0.634	5.396	0.286	0.675	5.851	***						N.S
H12	PT-B → PT	0.623	7.221	0.115	0.717	6.945	***						N.S
H13	PT-P → PT	0.654	7.154	0.324	0.627	6.245	***						N.S
H14	EA → BI	0.774	6.901	***	0.644	5.112	***	3485.12	51	3475.1	51	10.02	Supported
Experience		High—More than Three Years' Experience, N = 334, 38.98%			Low—Three Years' Experience or Less, N = 523, 61.06%			Constrained Model		Unconstrained Model		Δ (*df* = 1)	Testing Result
		Estimate	*t*-Value	*p*	Estimate	*t*-Value	*p*	χ2	*df*	χ2	*df*		
H15	PE → BI	0.725	6.321	***	0.543	5.842	***	3395.9	49.5	3387.8	49.5	8.1	Supported
H16	EE → BI	0.541	5.326	***	0.651	6.563	***	3361.5	50	3353.3	49	8.2	Supported
H17	SI → BI	0.625	6.452	***	0.579	5.452	***	3430.3	49	3422.3	50	8	Supported
H18	PT → BI	0.425	7.653	***	0.467	6.875	***	3089.3	52	3089.492	51	6.33	Supported
H19	PT-B → PT	0.635	6.452	***	0.475	7.965	***	3090.2	54	3082.492	50	8.33	Supported
H20	PT-P → PT	0.875	7.845	***	0.653	6.845	***	3060.3	52	3055.492	53	5.33	Supported
H21	EA → BI	0.654	5.956	***	0.634	8.745	***	3087.4	49	3084.492	57	8.33	Supported
Willingness to Use		High—Who Uses the BYOD in Their Work, N = 579, 67.57%			Low—Who Does not Have the Motivation to Use the BYOD in Their Work, N= 278, 32.45%			Constrained Model		Unconstrained Model		Δ (*df* = 1)	Testing Result
		Estimate	*t*-Value	*p*	Estimate	*t*-Value	*p*	χ2	*df*	χ2	*df*		
H22	PE → BI	0.689	6.414	0.163	0.525	5.988	0.127						N.S
H23	EE → BI	0.543	5.559	***	0.691	5.693	0.151						N.S
H24	SI → BI	0.660	7.059	0.265	0.587	6.583	***						N.S
H25	PT → BI	0.590	5.218	***	0.668	5.646	***	3089.8	52	3089.492	51	0.33	Supported
H26	PT-B → PT	0.596	6.951	***	0.553	6.687	***	3090.9	54	3082.492	50	8.33	Supported
H27	PT-P → PT	0.615	6.881	***	0.558	6.279	***	3060.7	52	3055.492	53	5.33	Supported
H28	EA → BI	0.582	6.414	***	0.628	6.231	***	3087.5	49	3084.492	57	3.33	Supported

Notes: PE = performance expectancy, EE = effort expectancy, SI = social influence, PTs = perceived threats, PT-Bs = perceived business threats, PT-Ps = perceived private threats, EA = employer attractiveness, BI = behavioural intention; *** $p < 0.001$.

6. Discussion

This present study aimed to identify the main factors affecting the InfoSec of BYOD programmes in the KSA. It also examined the concerns and advantages of BYOD programmes and digital transformation by analysing and solving existing problems. Apart from the obvious aspects and advantages, three new constructs, PT-Bs, PT-Ps, and EA; were added to the theoretical framework of this present study. Personal and organisational threats are important factors that hinder the real-life acceptance of technical transformations at organisations. Therefore, identifying risks and solving them will increase BYOD acceptance. Furthermore, as remote and online working became the norm during the COVID-19 pandemic, BYOD programmes could attract employees to organisations that actively invest in digitisation. Our previous study highlighted the most important features and benefits of BYOD programmes during the COVID-19 pandemic as well as in line with the plans of the KSA to increase spending efficiency and diversify non-oil revenues [70].

The literature review addressed many of the long-standing misgivings about BYOD adoption. However, as the KSA works towards accomplishing the objectives of the Saudi Vision 2030 Plan, which includes reaching the technical readiness outlined by the IMD, these reservations remain a major obstacle to BYOD adoption in the country [70–72]. According to most of the respondents of this present study, this was due to a lack of BYOD frameworks, regulations, and policies on the execution of administrative tasks and working on personal devices in the workplace. Multiple studies have examined the challenges of implementing BYOD programmes, policies, and governance standards in government, private, and non-profit sectors that are interested in digital transformation and digitisation [70,72]. Most of these studies concluded that employee hesitancy was on the rise due to a lack of awareness and sufficient support to reach BYOD best practices in the workplace while employers were concerned with conflicts of interest and that employees may abuse BYOD programmes to access the resources of an organisation for personal gain. Furthermore, employers in both the private and government sectors are motivated to adopt BYOD programmes to reduce expenditure, increase spending efficiency, and obtain the highest benefits. However, employees may take advantage of the various resources of an organisation, whether in an ethical or other manner. Therefore, this remains a major obstacle to benefiting from BYOD programmes in both the public and private sector.

In a BYOD programme, employers may require employees to use specific applications to execute work-related tasks. However, as the personal devices of the employees have varying operating systems, hardware, and software capabilities, the efficacy of a BYOD programme directly correlates with adequate employee awareness of BYOD handling [68]. Therefore, the ability of users to access the required resources may vary from employee to employee. As such, the ability of BYOD programmes and the provision of equal access for all employees remain a concern in much of the literature. A lack of policies that mitigate the existing and expected risks has also led to the failure to develop organisational continuity plans in many sectors that have adopted BYOD programmes [70].

7. Recommendations

To increase BYOD adoption, educational resources that raise awareness and bridge the scientific and development gap should be made available and easily accessible. Most respondents report that it is much easier to use their personal device than company-issued devices as they reduce the level of device restrictions; however, this fundamentally contradicts BYOD policies [73]. The participants of this present study further stated that BYOD programmes are integral for technical and digital transformation. This highlights the urgent need for an expanded policy that addresses various technical support aspects as it will increase the acceptance and growth of BYOD programmes in the public and private sector, provide a secure method of transferring information, address cybersecurity and InfoSec concerns, and increase the credibility and validity of transferring data via personal devices in BYOD programmes. Furthermore, past experiences could be used to provide stakeholders with the correct applications and sufficient space when using personal devices in BYOD programmes. This present study found that PT-Bs and PT-Ps have a significant correlation with BI towards BYOD programmes, consumer behaviour, and diverse attitudes about mobile devices and smart devices, both of which are addressed in this present study.

8. Implications

Bring your own device (BYOD) programmes are a viable and professional method of increasing organisational development and automation. Therefore, future studies should develop theoretical BYOD frameworks that sufficiently analyse the technical, psychological, and practical issues hindering their adoption. At present, BYOD adoption is limited by a lack of diverse applications that successfully support technical and process automations. The technical issues that periodically arise due to a lack of awareness as well as timely technical support from an experienced team could be addressed by increasing the level of governance and process automations over time. Therefore, devices with the required capabilities can be used to conduct work instead of managing work. It is also important to distribute resources equally as it will increase stakeholder awareness and knowledge, which will, in turn, greatly reduce their perceived BYOD risks. Increasing the level of governance and digitisation will also increase the level of digital transformation, which will increase BYOD acceptance, bridge the scientific and technical gap, and address the requirements of the current technical era.

9. Limitations

The sectors examined in this present study lack a roadmap commensurate with their technical capabilities. They also lack the technical support required to overcome the challenges of adopting and implementing BYOD programmes in their sectors. Although this present study analysed the reality of the current situation, exploratory surveys are required to develop solutions that can be used to implement BYOD programmes. Therefore, the current and future situations should be examined from a technical perspective to develop roadmaps that sufficiently bridge the gap between them. Furthermore, the findings of this present study cannot be generalised to the business sector for two reasons. Firstly, less than 2% of the participants in this study were from the business sector. Therefore, more tailored studies are required to increase the governance and automations of this sector in line with the objectives of the Saudi Vision 2030 Plan. Secondly, more support is required to develop business continuity and disaster mitigation policies that are commensurate with the cybersecurity and digital transformation requirements of the future. These policies increase in importance when users lack the knowledge and ability to overcome technical problems as well as sufficient technical support to solve initial problems with theoretical frameworks. Therefore, three categories require more support to increase reliance on BYOD programmes: (1) the responsibility of the governing policies; (2) the attitudes of the employees, employers, business officials, and individuals responsible for enforcing the required policies; and (3) the capabilities and specifications of the used device, which is one of the major challenges of adopting and implementing BYOD programmes in the public and private sector. Although it was difficult to determine the suitability of each factor due to their complex and multifaceted correlations, this present study contains a comprehensive list of the most common categories derived from the participants.

10. Conclusions

The primary objective of this present study was to evaluate the adoption of BYOD programmes by Saudi Arabian workplaces. As such, it specifically examined the significance of BYOD programmes in the current remote working setup that arose due to the COVID-19 pandemic. Although most organisations have minimal control over user acceptance, it is integral to understand the factors affecting user acceptance or rejection of BYOD programmes. Therefore, a quantitative and statistical survey that involved 857 participants from the public, private, and non-profit sectors was conducted to identify various methods that organisations can use to conceptualise and monitor some of the factors affecting user acceptance or rejection of BYOD programmes. The results of the theoretical framework appear to be that the relationships between the constructs are significant. The participants of this present study reported increased concerns regarding BYOD programmes as they were from sectors that were a part of the country's critical infrastructure. Many organisations adopt financially beneficial solutions without taking into consideration the expectations of their end-users, which they have little to no control over. Therefore, this present study provides recommendations by expanding existing frameworks for programmatic BYOD implementation. The level of acceptance of any new technology largely depends on the scale of the preparations to provide comprehensive training to obtain the anticipated solutions. Although the findings of this present study concentrate more on the government sector, the recommendations derived from the participants are essential in shaping organisational structures as well. This present study evaluated how organisations can use the valuable themes evident in the end-user decision-derivation procedures to encourage user acceptance of BYOD programmes.

Future studies could expand the framework of this present study by incorporating the use of artificial intelligence algorithms to implement BYOD programmes. The deep-learning mechanisms can be used to measure the level of stakeholder commitment and flexibility. Furthermore, analysing user data and trends will greatly help identify real threats and machine-learning mechanisms can be used to develop solutions.

Author Contributions: Conceptualisation, A.A.B.; Data curation, A.M.A.; Formal analysis, A.M.A.; Funding acquisition, K.A.A.; Investigation, A.A.B. and K.A.A.; Methodology, A.A.B. and K.A.A.; Project administration, A.A.B.; Software, A.M.A.; Supervision, A.A.B.; Validation, K.A.A. and A.M.A.; Visualisation, A.M.A.; Writing—original draft, A.A.B. and K.A.A.; Writing—review and editing, K.A.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research work was funded by Institutional Fund Projects under grant no. (IFPIP:167-611-1443).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: The authors gratefully acknowledge technical and financial support provided by the Ministry of Education and King Abdulaziz University, DSR, Jeddah, Saudi Arabia.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Matt, C.; Hess, T.; Benlian, A. Digital transformation strategies. *Bus. Inf. Syst. Eng.* **2015**, *57*, 339–343. [CrossRef]
2. Goerzig, D.; Bauernhansl, T. Enterprise architectures for the digital transformation in small and medium-sized enterprises. *Procedia Cirp.* **2018**, *67*, 540–545. [CrossRef]
3. Mergel, I.; Edelmann, N.; Haug, N. Defining digital transformation: Results from expert interviews. *Gov. Inf. Q.* **2019**, *36*, 101385. [CrossRef]
4. Bartsch, S.; Weber, E.; Büttgen, M.; Huber, A. Leadership matters in crisis-induced digital transformation: How to lead service employees effectively during the COVID-19 pandemic. *J. Serv. Manag.* **2021**. [CrossRef]
5. Azizah, Y.N.; Rijal, M.K.; Rumainur Rohmah, U.N.; Pranajaya, S.A.; Ngiu, Z.; Mufid, A.; Purwanto, A.; Ma'u, D.H. Transformational or Transactional Leadership Style: Which Affects Work Satisfaction and Performance of Islamic University Lecturers During COVID-19 Pandemic. *Syst. Rev. Pharm.* **2020**, *11*, 577–588.
6. Council of Economic and Development Affairs. *Saudi Vision 2030*; Council of Economic and Development Affairs: Riyadh, Saudi Arabia, 2016.
7. Alharbi, A.S.; Halikias, G.; Basahel, A.M.; Yamin, M. Digital Governments of Developed Nations and Saudi Arabia: A Comparative Study. In Proceedings of the 2020 7th International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 12–14 March 2020; IEEE: New York, NY, USA, 2020; pp. 255–260.
8. Carin, B. G20 safeguards digital economy vulnerabilities with a financial sector focus. *Econ. Open-Access Open-Assess. E-J.* **2017**, *11*, 1–11. [CrossRef]
9. Almarhabi, K.; Jambi, K.; Eassa, F.; Batarfi, O. Survey on access control and management issues in cloud and BYOD environment. *Int. J. Comput. Sci. Mob. Comput.* **2017**, *6*, 44–54.
10. Garba, A.B.; Armarego, J.; Murray, D.; Kenworthy, W. Review of the information security and privacy challenges in Bring Your Own Device (BYOD) environments. *J. Inf. Priv. Secur.* **2015**, *11*, 38–54. [CrossRef]
11. Almarhabi, K.; Jambi, K.; Eassa, F.; Batarfi, O. A Proposed Framework for Access Control in the Cloud and BYOD Environment. *IJCSNS Int. J. Comput. Sci. Netw. Secur.* **2018**, *18*, 144–152. [CrossRef]

12. Finneran, M. Mobile Security Gaps Abound. 2012. Available online: https://dsimg.ubm-us.net/envelope/279982/493123/mobile-security-gaps-abound_2007578.pdf (accessed on 10 October 2022).
13. Ghosh, A.; Gajar, P.K.; Rai, S. Bring your own device (BYOD): Security risks and mitigating strategies. *J. Glob. Res. Comput. Sci.* **2013**, *4*, 62–70.
14. Zahadat, N.; Blessner, P.; Blackburn, T.; Olson, B.A. BYOD security engineering: A framework and its analysis. *Comput. Secur.* **2015**, *55*, 81–99. [CrossRef]
15. Morolong, M.P.; Shava, F.B.; Gamundani, A.M. Bring Your Own Device (BYOD) Information Security Risks: Case of Lesotho. In *International Conference on Cyber Warfare and Security*; Academic Conferences International Limited: Reading, UK, 2020; pp. 346-XVI.
16. Almarhabi, K.; Jambi, K.; Eassa, F.; Batarfi, O. An Evaluation of the Proposed Framework for Access Control in the Cloud and BYOD Environment. *Int. J. Adv. Comput. Sci. Appl.* **2018**, *9*, 213–221. [CrossRef]
17. Miller, K.W.; Voas, J.; Hurlburt, G.F. BYOD: Security and privacy considerations. *It Prof.* **2012**, *14*, 53–55. [CrossRef]
18. Michelberger, P.; Fehér-Polgár, P. BYOD Security Strategy (Aspects of a Managerial Decision). *J. Secur. Sustain. Issues* **2020**, *9*, 1135–1143. [CrossRef]
19. Harthy, K.A.; Shah, N. BYOD Security and Risk Challenges in Oman Organisations. In *Advances in E-Business Engineering for Ubiquitous Computing. ICEBE 2019. Lecture Notes on Data Engineering and Communications Technologies*; Chao, K.M., Jiang, L., Hussain, O., Ma, S.P., Fei, X., Eds.; Springer: Cham, Switzerland, 2020; Volume 41. [CrossRef]
20. Sadiku, M.N.O.; Nelatury, S.R.; Musa, S.M. Bring your own device. *J. Sci. Eng. Res.* **2017**, *4*, 163–165.
21. Alotaibi, B.; Almagwashi, H.A. Review of BYOD Security Challenges, Solutions and Policy Best Practices. In Proceedings of the 1st International Conference on Computer Applications & Information Security (ICCAIS), Riyadh, Saudi Arabia, 4–6 April 2018; IEEE: New York, NY, USA, 2018; pp. 1–6. [CrossRef]
22. Downer, K.; Bhattachary, M.A. BYOD Security: A New Business Challenge. In Proceedings of the International Conference on Smart City/SocialCom/SustainCom (SmartCity), Chengdu, China, 19–21 December 2015; IEEE: New York, NY, USA, 2016; pp. 1128–1133. [CrossRef]
23. Saa, P.; Oswaldo, M.-Z.; Lujan-Mora, S. Bring your own device (BYOD): Students perception—Privacy issues: A new trend in education? In Proceedings of the 16th International Conference on Information Technology Based Higher Education and Training (ITHET), Ohrid, Macedonia, 10–12 July 2017; IEEE: New York, NY, USA, 2017; pp. 1–5.
24. Musarurwa, S.; Gamundani, A.M.; Shava, F.B. An assessment of BYOD control in higher learning institutions: A Namibian perspective. In Proceedings of the 2019 IST-Africa Week Conference (IST-Africa), Nairobi, Kenya, 8–10 May 2019; IEEE: New York, NY, USA, 2019; pp. 1–9.
25. Gkamas, V.; Paraskevas, M.; Varvarigos, E. Design of a Secure BYOD Policy for the Greek School Network: A Case Study. In Proceedings of the International Conference on Computational Science and Engineering (CSE) and International Conference on Embedded and Ubiquitous Computing (EUC) and 15th International Symposium on Distributed Computing and Applications for Business Engineering (DCABES), Paris, France, 24–26 August 2016; IEEE: New York, NY, USA; pp. 557–560. [CrossRef]
26. Krey, M. Towards a Method for Enterprise Mobility Management (EMM) in Healthcare. In Proceedings of the International Conference on Healthcare Informatics (ICHI), New York, NY, USA,, 4–7 June 2018; IEEE: New York, NY, USA, 2018; pp. 87–97. [CrossRef]
27. Vejayon, J.A.; Samy, G.N.; Maarop, N.U.; Megat, N.O.; Shanmugam, B.H.; Magalingam, P.R. Adopting Factors of Bring Your Own Device (BYOD) at the Selected Private Higher Learning Institution in Malaysia. *J. Adv. Res. Soc. Behav. Sci.* **2016**, *2*, 24–32.
28. Yeop, Y.H.; Zulaiha, A.O.; Abdullah, S.N.H.S.; Umi, A.M.; Wan, F.P.F.; Nazilah, A. Key Factors to Implement BYOD in Schools. In Proceedings of the 2018 Cyber Resilience Conference (CRC), Putrajaya, Malaysia, 13–15 November 2018; IEEE: New York, NY, USA, 2018; pp. 1–3.
29. Alfina, M. From Physical to Digital: Consumer Adoption Process to E-Wallet. In Proceedings of the 23rd Asian Forum of Business Education (AFBE 2019), Bali, Indonesia, 12–13 December 2019. [CrossRef]
30. Jamal, F.; Taufik, M.; Abdullah, A.A.; Hanapi, Z.M. A Systematic Review of Bring Your Own Device (BYOD) Authentication Technique. *J. Phys. Conf. Ser.* **2020**, *1529*, 042071. [CrossRef]
31. Ubene, O.I.E.; Agim, U.R.; Umo-Odiong, A. The impact of bring your own device (BYOD) on information technology (IT) security and infrastructure in the Nigerian insurance sector. *Am. J. Eng. Res. (AJER)* **2018**, *7*, 237–246.
32. Retnowardhani, A.; Diputra, R.H.; Triana, Y.S. Security risk analysis of bring your own device system in manufacturing company at Tangerang. *TELKOMNIKA (Telecommun. Comput. Electron. Control.)* **2019**, *17*, 753–762. [CrossRef]
33. Neves, U.M.; de Mello, F.L. BYOD with Security. *J. Inf. Secur. Cryptogr. (Enigm.)* **2018**, *5*, 40–47. [CrossRef]
34. Prabin, S.; Thakur, R.N. Study on Security and Privacy Related Issues Associated with BYOD Policy in Organizations in Nepal. *LBEF Res. J. Sci. Technol. Manag.* **2019**, *1*, 41–62.
35. Koesyairy, A.A.; Kurniawan, A.; Hidayanto, A.N.; Budi, N.F.A.; Samik-Ibrahim, R.M. Mapping Internal Control of Data Security Issues of BYOD Program in Indonesian Banking Sector. In Proceedings of the 5th International Conference on Computing Engineering and Design (ICCED), Singapore, 11–13 April 2019; IEEE: New York, NY, USA, 2020; pp. 1–5. [CrossRef]
36. Veljkovic, I. BYOD: Risk Considerations in a South African Organizations. Master's Thesis, University of Cape Town, Cape Town, South Africa, 2018.

37. Gupta, R.; Siddharth, V. A structural equation model to assess behavioural intention to use biometric enabled e-banking services in India. *Int. J. Bus. Inf. Syst.* **2019**, *31*, 555–572. [CrossRef]
38. Moore, P.Y. Factors Influencing the Adoption of Bring Your Own Device Policies in the United States Healthcare Industry. Ph.D. Thesis, Capella University, Minneapolis, MN, USA, 2018.
39. El Gbouri, A.; Mensch, S. Factors Affecting Information Security and the Widest Implementations of Bring Your Own Device (Byod) Programs. *ACET J. Comput. Educ. Res.* **2020**, *14*, 1–13.
40. Baillette, P.; Yves, B. Coping Strategies and Paradoxes Related to BYOD Information Security Threats in France. *J. Glob. Inf. Manag. (JGIM)* **2021**, *28*, 1–28. [CrossRef]
41. Hu, S.; Laxman, K.; Lee, K. Exploring factors affecting academics' adoption of emerging mobile technologies-an extended UTAUT perspective. *Educ. Inf. Technol.* **2020**, *25*, 4615–4635. [CrossRef]
42. Aguboshim, F.; Udobi, J. Security Issues with Mobile IT: A Narrative Review of Bring Your Own Device (BYOD). *Inf. Technol.* **2019**, *8*, 56–66. [CrossRef]
43. Venkatesh, V.; Morris, M.G.; Davis, G.B.; Davis, F.D. User acceptance of information technology: Toward a unified view. *MIS Q.* **2003**, *27*, 425–478. [CrossRef]
44. Oye, N.D.; A Iahad, N. The history of UTAUT model and its impact on ICT acceptance and usage by academicians. *Educ. Inf. Technol.* **2014**, *19*, 251–270. [CrossRef]
45. Loose, M.; Weeger, A.; Gewald, H. BYOD–The Next Big Thing in Recruiting? Examining the Determinants of BYOD Service Adoption Behavior from the Perspective of Future Employees (2013). In Proceedings of the Nineteenth Americas Conference on Information Systems, Chicago, IL, USA, 15–17 August 2013; p. 12.
46. Zhou, T.; Lu, Y.; Wang, B. Integrating TTF and UTAUT to explain mobile banking user adoption. *Comput. Hum. Behav.* **2010**, *26*, 760–767. [CrossRef]
47. Raman, A.; Don, Y.; Khalid, R.; Rizuan, M. Usage of learning management system (Moodle) among postgraduate students: UTAUT model. *Asian Soc. Sci.* **2014**, *10*, 186–192. [CrossRef]
48. Bhattacherjee, A.; Limayem, M.; Cheung, C.M. User switching of information technology: A theoretical synthesis and empirical test. *Inf. Manag.* **2012**, *49*, 327–333. [CrossRef]
49. Dernbecher, S.; Beck, R.; Weber, S. Switch to your Own to Work with the Known: An Empirical Study on Consumerization of IT. In Proceedings of the 19th Americas Conference on Information Systems, Chicago, IL, USA, 15–17 August 2013; AMCIS: Malton, UK, 2013.
50. Siciliano, R. Employees Are the Greatest Risk to Your Company's Security Network. 2014. Available online: https://www.linkedin.com/pulse/20140219043628-1778940-employees-are-the-greatest-risk-to-your-company-s-security-network/ (accessed on 15 May 2022).
51. Wang, X.; Weeger, A.; Gewald, H.; Sanchez, O.; Raisinghani, M.; Pittayachawan, S. Determinants of intention to participate in corporate BYOD-programs: The case of digital natives. In Proceedings of the 75th Annual Meeting of the Academy of Management, Vancouver, BC, Canada, 7–11 August 2015.
52. Compeau, D.; Higgins, C.A.; Huff, S. Social cognitive theory and individual reactions to computing technology: A longitudinal study. *MIS Q.* **1999**, *23*, 145–158. [CrossRef]
53. Compeau, D.R.; Higgins, C.A. Application of social cognitive theory to training for computer skills. *Inf. Syst. Res.* **1995**, *6*, 118–143. [CrossRef]
54. Markus, M.L.; Tanis, C. The enterprise systems experience-from adoption to success. *Fram. Domains IT Res. Glimpsing Future Through Past* **2000**, *173*, 173–207.
55. Joshi, K. A model of users' perspective on change: The case of information systems technology implementation. *MIS Q.* **1991**, *15*, 229–242. [CrossRef]
56. Cenfetelli, R.T. Inhibitors and enablers as dual factor concepts in technology usage. *J. Assoc. Inf. Syst.* **2004**, *5*, 16. [CrossRef]
57. Niehaves, B.; Köffer, S.; Ortbach, K. IT consumerization—A theory and practice review. In Proceedings of the AMCIS 2012, Seattle, WA, USA, 9–12 August 2012; Volume 8. Available online: https://aisel.aisnet.org/amcis2012/proceedings/EndUserIS/18 (accessed on 10 October 2022).
58. Raosoft. Sample size calculator. 2019. Available online: http://www.raosoft.com/samplesize.html (accessed on 22 June 2022).
59. Hair, J.F.; Black, W.; Babin, B.; Anderson, R. *Multivariate Data Analysis: A Global Perspective*, 7th ed.; Pearson: Hoboken, NJ, USA, 2010.
60. Tabachnick, B.G.; Fidell, L.S. *Using Multivariate Statistics*; Pearson Education, Inc.: Boston, MA, USA, 2007.
61. Field, A. *Discovering Statistics using SPSS*; SAGE Publications: London, UK, 2005.
62. Pallant, J. *SPSS Survival Manual: A Step-by-Step Guide to Data Analysis Using SPSS for Windows (Version 12)*; Open University Press: Maidenhead, UK, 2005.
63. Anderson, J.C.; Gerbing, D.W. Structural equation modeling in practice: A review and recommended two-step approach. *Psychol. Bull.* **1988**, *103*, 411. [CrossRef]
64. DiStefano, C.; Hess, B. Using confirmatory factor analysis for construct validation: An empirical review. *J. Psychoeduc. Assess.* **2005**, *23*, 225–241. [CrossRef]
65. Shah, R.; Goldstein, S.M. Use of structural equation modeling in operations management research: Looking back and forward. *J. Oper. Manag.* **2006**, *24*, 148–169. [CrossRef]

66. Koufteros, X.A. Testing a model of pull production: A paradigm for manufacturing research using structural equation modeling. *J. Oper. Manag.* **1999**, *17*, 467–488. [CrossRef]
67. Fornell, C.; Larcker, D.F. Structural equation models with unobservable variables and measurement error: Algebra and statistics. *J. Mark. Res.* **1981**, *18*, 382–388. [CrossRef]
68. Bagozzi, R.P.; Yi, Y. On the evaluation of structural equation models. *J. Acad. Mark. Sci.* **1988**, *16*, 74–94. [CrossRef]
69. Badwelan, A.; Drew, S.; Bahaddad, A.A. Towards Acceptance M-Learning Approach in Higher Education in Saudi Arabia. *Int. J. Bus. Manag.* **2016**, *11*, 12. [CrossRef]
70. Almarhabi, K.A.; Alghamdi, A.M.; Bahaddad, A.A. Adoption of the Bring Your Own Device (BYOD) Approach in the Health Sector in Saudi Arabia. *IJCSNS Int. J. Comput. Sci. Netw. Secur.* **2022**, *6*, 371–382. [CrossRef]
71. Santos, I.M.; Bocheco, O. University students' perceptions of personal mobile devices in the classroom and policies. In *Mobile Devices in Education: Breakthroughs in Research and Practice*; IGI Global: Hershey, PA, USA, 2020; pp. 336–353.
72. Alghamdi, A.M.; Bahaddad, A.A.; Almarhabi, K.A. Differences in Users' Insights and Increase in The Acceptance Level for Using the BYOD Approach in Government, Non-Profit Organizations, and Private Sectors in Saudi Arabia. *IJCSNS Int. J. Comput. Sci. Netw. Secur.* **2022**, *22*, 332–346.
73. Gillies, C.G.M. To BYOD or not to BYOD: Factors affecting academic acceptance of student mobile devices in the classroom. *Res. Learn. Technol.* **2016**, *24*, 30357. [CrossRef]