South African Journal of Information Management
ISSN: (Online) 1560-683X, (Print) 2078-1865

Extending unified theory of acceptance and use of technology with ISO/IEC 27001 security standard to investigate factors influencing Bring Your Own Device adoption in South Africa

Author:
Thembekile Mayayise[1]

Affiliation:
[1]Department of Information Systems, Faculty of Commerce, Law and Management, University of the Witwatersrand, Johannesburg, South Africa

Corresponding author:
Thembekile Mayayise,
Thembekile.Mayayise@wits.ac.za

Dates:
Received: 09 Feb. 2021
Accepted: 26 Aug. 2021
Published: 09 Nov. 2021

How to cite this article:
Mayayise, T., 2021, 'Extending unified theory of acceptance and use of technology with ISO/IEC 27001 security standard to investigate factors influencing Bring Your Own Device adoption in South Africa', *South African Journal of Information Management* 23(1), a1376. https://doi.org/10.4102/sajim.v23i1.1376

Background: As the use of mobile computing devices such as smartphones increase in developing countries, some employees in organisations prefer using their privately owned mobile devices for work purposes by following the Bring Your Own Device (BYOD) practice. However, the actual factors that influence the adoption of this practice are limited.

Aim: This study aimed to investigate the factors that positively influence the employee's behavioural intention to adopt the BYOD practice in organisations.

Setting: The focus of the study is workers in various industries in South Africa.

Method: A model is proposed which extends components of the Unified Theory of Acceptance and the Use of Technology (UTAUT) model by certain elements of the ISO/IEC 27001 security standard and an organisational factor. It is a quantitative study. Through a snowball method, a sample of 130 South African workers participated in the study by completing an electronic survey where 106 valid responses were received.

Results: The data analysis was conducted through the SPSS data analysis tool. The results revealed that performance expectancy, effort expectancy, awareness and training, and policy existence positively influence the behavioural intention to adopt the BYOD Practice.

Conclusion: The outcome of this study will benefit practitioners considering the implementation of BYOD and also researchers seeking to expand the scope of existing technology adoption frameworks.

Keywords: Unified Theory of Acceptance and the Use of Technology; Bring Your Own Device; adoption; security standard; International Organization for Standardization/International Electrotechnical Commission 27001; information security; behavioural intention.

Introduction

As a tradition, organisations of different business practices have provided employees with the necessary business tools such as mobile computing devices to perform their jobs. This practice allowed organisations to retain ownership of mobile devices and the information contained therein, as information is regarded as a valuable asset by most organisations (Madzima, Moyo & Abdullah 2014). This model of information asset management had its affordances and shortcomings for employees and organisations alike. Organisations often struggled with the financial burden to acquire, insure, maintain and replace the computing devices. For this reason, some organisations have adopted the Bring Your Own Device (BYOD) practice. In certain instances, employees use their privately owned devices out of convenience, which often leads to unreasonable expectations by employers for employees to stay available for work purposes even though it may come at a cost. The employers' expectations regarding the employee's use of personally owned devices, if unmanaged, could negatively affect the behavioural intention to adopt BYOD by employees. The BYOD practice has over the years allowed for some flexibility, which allowed employees to use their privately owned devices for work purposes, whilst companies have been able to save some costs of acquiring computer assets (Romer 2014).

According to Hovav and Putri (2016), BYOD is defined as an environment that permits its employees the use of their privately owned devices to access corporate network to perform their tasks. Another definition emphasises bringing a user's device to the workplace for official business use (Vignesh & Asha 2015). The common theme with both these definitions is that the user/employee privately owns the device. According to Morrow (2012), the 'D' in BYOD refers to more than the physical device. It extends to employees accessing Outlook Webmail and SharePoint, and other applications that are hosted on the cloud.

In this research's context, BYOD refers to employees using their privately owned devices such as cell phones, laptops, tablets to access work information and store such information on personal cloud storage.

According to Dang-Pham and Pittayachawan (2015), the increased risks of malware and information security incidents make implementing BYOD practices an option that must be thoroughly investigated to minimise any security vulnerabilities. Furthermore, because cybercrime is a global problem affecting various countries worldwide, companies stand to have their information stolen, destroyed or altered because of cybercrime. Therefore, any access to company information needs to be safeguarded.

Different types of cyber-attacks can be experienced when a device is exposed to unsafe environments when downloading software from untrusted sources. The BYOD devices are vulnerable to cyber threats when not configured securely based on the organisation's security standards (Yang, Hong-Chao & Guo-Zhen 2019). It poses more significant risks to the organisation's information when BYOD is ungoverned from the point of view of policy, strategy, and technical controls. Employees can use their devices to access company information through unsafe means.

The BYOD empirical studies in the past have focused on BYOD adoption from other framework dimensions which did not necessarily look at the factors that influenced the behavioural intention (BI) to adopt BYOD with a combination of factors emanating from a scholarly perspective and the practitioner side (Musarurwa, Flowerday & Cilliers 2018). This study aimed to look at the factors that positively influence employees' BIs to adopt BYOD in organisations. The unified theory of acceptance and use of technology (UTAUT) model and the International Organization for Standardisation (ISO)/International Electrotechnical Commission (IEC) 27001 security standard will be used as a lens in the study. The study was conducted using South African participants working in different industries. As South Africa is one of the developing countries, the results of this study will give insights into the level of awareness regarding BYOD practices by employees in organisations and the factors that drive BYOD adoptions in organisations.

This article makes the following contributions:

- It adds to the existing body of knowledge regarding the factors affecting BYOD practices in developing countries.
- It makes a significant theoretical contribution to the existing technology adoption frameworks.
- Organisations will get to understand the factors that influence employees to adopt BYOD in corporate environments.

The remainder of the article has been structured as follows: The second section is literature review, the third and fourth sections focus on research design and methodology, the fifth section presents the findings and discussion, and the sixth section concludes the study.

Literature review

Background

The adoption of BYOD policy is a strategic decision, which an organisation may formally choose to undertake for various reasons. Some of these reasons include: cost savings, improved efficiency and productivity (ISACA 2020). There are many aspects, which ought to be considered when organisations adopt a BYOD programme.

The strategy must cover all dimensions, which must be translated into a plan to operationalise the strategy. The policies, procedures and standards must be developed to ensure governance of BYOD (Fani, Von Solms & Gerber 2016). The other aspect is the technology and also the risks related to the multi-sharing of devices. The adoption of BYOD policy in an organisation is usually associated with introducing privacy and security risks because of a lack of information security awareness among employees and BYOD policy (Alotaibi & Almagwashi 2018).

Various studies have been conducted around developing relevant organisational BYOD policies to adequately address risks associated with the use of personally owned devices for work purposes (Herrera, Ron & Rabadao 2017). However, there is another aspect to BYOD implementation, which many researchers rarely discuss that is, whether BYOD practices are formalised from a policy governance perspective. The SysAdmin, Audit, Network and Security (SANS) institute conducted a study where they surveyed companies to establish their view of BYOD.

The results of the survey revealed that 97% of the 1000 surveyed companies deemed BYOD important. However, a further study revealed that 36% of these organisations stated that BYOD policies are not formalised, 23% of the companies do not allow BYOD, and 14% confirmed that they inform their employees to secure and monitor their devices (Vignesh & Asha 2015). The proposed study gives a view in terms of the South African industries where BYOD is adopted.

Bring Your Own Device risks and associated breaches

There are various benefits that organisations stand to gain from implementing the BYOD programme, such as cost

reductions and improved productivity. However, there are also certain risks associated with the use of BYOD in organisations. Risk is the combination of the likelihood of an event and its consequence.

Risks such as security misconfiguration of devices and failure to restrict URL access are prevalent in BYOD environments (Lennon 2012).

Security breaches

The BYOD has both advantages and disadvantages. One of its shortcomings is that it can lead to many data security breaches, such as device theft or malicious data deletions. The use of personal devices to access emails, social media platforms and the downloading of different applications can potentially open doors to cybersecurity attacks. Security mistakes that happen in a non-work context could adversely compromise the security of information in an organisation. It is thus paramount that before an organisation adopts BYOD, a proper risk assessment is done to determine the existence of adequate controls (Dang-Pham & Pittayachawan 2015).

The corporate information that is stored on personal cloud storage services such as iCloud and Dropbox stand to be exposed if such services are compromised. For example, in 2016 Dropbox was hacked, and usernames and passwords were exposed and if employees store company information at their discretion in such platforms, such information can get exposed during a hack (Gibbs 2020).

Malware attacks

There are many risks related to the use of BYOD. According to (Dang-Pham & Pittayachawan 2015; Ameen et al. 2020), Malware is a common risk faced by any institution that seeks to implement BYOD. Malware refers to malicious software that gains access to the user's machines through phishing scams, email attachments and file sharing.

Data leakage

The risk of data leakage increases with the use of personal devices for work purposes. Data leakage risk is worsened because most devices are exposed to many dangers through private use when users access platforms such as the Internet and social media. Data leakage can result in reputational damages in an organisation. Some of the devices might not have more robust security controls such as encryption, which could help minimise data leakage risk. In organisations, such as tertiary institutions, where BYOD affects a higher number of users, insecure volumes of end-points have to be considered when determining the impact of potential risk.

By adopting BYOD, an organisation is merely undertaking that even the mistakes that can happen outside the working environment can ultimately impact the organisation's online safety because of its opening. Measures such as awareness and training (AT) often minimise the risks associated with data security attacks (Bauer, Bernroider & Chudzikowski 2017; Dang-Pham & Pittayachawan 2015). Other major drawback concerning BYOD include the invasion of privacy. An organisation can monitor the use of a user device without the user being aware and this could result in some of their personal information also being monitored (Bann, Singh & Samsudin 2015).

Theft of mobile device

When personally owned devices get stolen with no controls to enable remote data wiping, the corporate information is likely to be exposed, which could ultimately cause reputational damage (Bongiovanni 2019).

Downer and Bhattacharya (2015) identified several other challenges associated with BYOD. They include technical issues such as the compatibility of privately owned devices and policy challenges that could arise as a result of the lack of policies and standards which regulate the use of BYOD devices in organisations. It is important for the organisations that seek to adopt BYOD to consider these issues methodically.

Benefits of Bring Your Own Device

Despite the risks posed by the introduction of BYOD in an organisation, there are various benefits that the organisations and employees can expect to gain. The reduction in the purchases of computer devices such as laptops, cell phones and tablets can be expected by the companies that adopt and implement BYOD policy. This financial saving can be channelled into other areas where financial resources are most needed. Other benefits include increased productivity and efficiency, mobility, job satisfaction and reduced information, communication and technology (ICT) support (Vignesh & Asha 2015). In organisations where there is no compensation in the form of allowances to employees for the use of BYOD, some employees may refuse the financial burden of BYOD and use the company-owned devices for business purposes which potentially affects their behavioural intention to adopt BYOD. It is when the benefits of implementing BYOD are seen to outweigh any risks that it gets implemented (Baillette, Barlette & Leclercq-Vandelannoitte 2018).

The gap in the existing literature regarding BYOD is that only a few empirical studies have been conducted on BYOD adoptions to identify factors that influence adoption. A study conducted by Lennon (2012), focused on employee attitudes towards using BYOD devices. Still, it is a study with specific gaps, that is, it is unclear how many participants took part in the survey. Another study by Ameen et al. (2020) focused solely on the employee's intention to comply with the BYOD policy, but it does not include evaluating factors that influence BYOD adoption holistically. A study that identified key traits for the behavioural intention to adopt BYOD was conducted to propose a BYOD intentional model (Musarurwa et al. 2018). The study's limitation is that it only focused on participants from one organisation and looked at BYOD controls and not necessarily adoption.

Theories and hypothesis development

Theoretical background

There are various frameworks that have been used in the past to determine the adoption of multiple technologies. Models such as the motivational model, theory of planned behaviour, social cognitive, motivation diffusion theory and the unified theory of acceptance are some of the models which have been used in technology adoption related studies (Rahi, Ghani & Ngah 2019).

This study investigates the factors that hold from the UTAUT, ISO/IEC 27001 security standard and the organisational requirement perspective that positively influences BYOD adoption in the South African context. The UTAUT was deemed the most appropriate framework to use because it comprehensively looked at the factors that are important to consider from a behavioural perspective.

Unified theory of acceptance and use of technology

The UTAUT is a model used across various research studies that sought to investigate or identify the factors that impacted BYOD adoption in different research settings. It has been used to determine the factors that influenced the adoption of technologies and services, such as internet banking and mobile banking (Baishya & Samalia 2020). The UTAUT consists of the following elements: performance expectancy (PE), effort expectancy (EE), social influence (SI) and user behaviour which impact or influences the BI. In a study by Boonsiritomachai and Pitchayadejanant (2018), UTAUT was combined with Technology Acceptance Model (TAM) to identify the most important factors determining mobile banking adoption. The results revealed that the hedonic aspects were the most critical determinants for mobile banking adoption by generation Y. The original UTAUT Framework is depicted in Figure 1.

International Organization for Standardisation/ International Electrotechnical Commission 27001 security standard

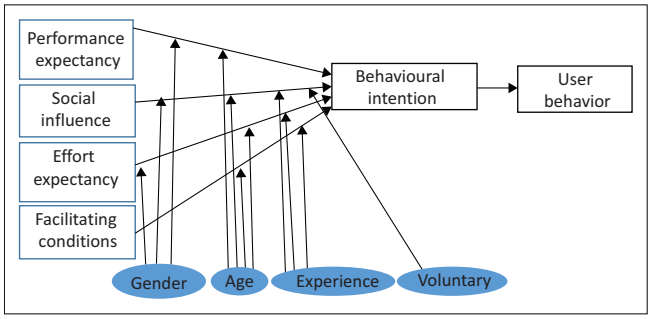
The ISO/IEC27001 is an information security techniques standard, which like many ISO standards, often get revised to align with the developments within the ICT industry. The ISO/IEC 27001:2015 version consists of seven main clauses with the first clause being the one that requires a full definition of the context in so far as information security is concerned. Based on the requirements of this security standard, an organisation must have a policy which governs information security. In addition to that requirement, employees need to be made aware of the content of such a policy. It is from those requirements that the policy and AT constructs were selected for this study as BYOD would need such aspects to be included as security requirements embedded in the practice. Other ISO/IE 27001 clauses include: leadership, planning, support, operation, performance evaluation, and ensuring continual improvement. Leadership support is vital for security governance because leadership provides direction and resources for planning information security initiatives in an organisation. The support clause looks at the activities necessary to operationalise the information security strategy; performance evaluation focuses on reviewing the effectiveness of the key security processes so that any weaknesses can be identified to ensure continual improvement.

The ISO/IEC 27001:2015 is combined with the UTAUT to produce the proposed model as depicted in Figure 2. The main aim of incorporating this standard is to look at the specific security related aspects which mobile technology users should be aware of when using their personal devices to access their corporate work information.

The proposed model consists of the following parts, that is, UTAUT and the ISO/IEC 27001:2015 and an additional construct named organisational requirement which emanates from the literature. The constructs and hypothesis statements are further detailed in the following section.

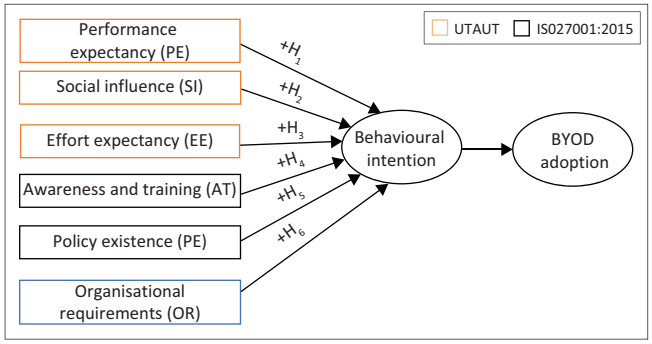
Hypothesis development

There are a number of factors which contribute to employees using their privately owned devices or cloud storage services for work purposes. In this section, six (6) hypothesis statements are formulated for the six constructs which emanate from the proposed model as depicted in Figure 2.



Source: Adopted from Rahi, S., Abd. Ghani, M. & Hafaz Ngah, A., 2019, 'Integration of unified theory of acceptance and use of technology in internet banking adoption setting: Evidence from Pakistan', Technology in Society 58(February 2018), 101120. https://doi. org/10.1016/j.techsoc.2019.03.003

FIGURE 1: The original unified theory of acceptance and use of technology framework.



BYOD, bring your own device; UTAUT, unified theory of acceptance and use of technology.

FIGURE 2: The proposed model – unified theory of acceptance and use of technology + International Organization for Standardisation/International Electrotechnical Commission 27001:2015.

Constructs from UTAUT

H1-Performance expectancy positively influences the behavioural intention to adopt BYOD

When technology is deployed, it is expected to perform at a certain level which will satisfy the user's needs. The better the performance, the more likely the technology is going to be used. Performance expectancy has previously been linked to technology adoption in different studies such as mobile banking adoption. It has thus been hailed as a driving force to technology adoption (Cao & Niu 2019). This hypothesis aims to confirm: if PE positively influences the behavioural intention to adopt BYOD.

H2-Social influence expectancy positively influences the behavioural intention to adopt BYOD

Social influence measures the external impact that users could have from their peers, colleagues, friends, and anyone within their circle of influence. The greater the level of SI, the more likely the technology will be adopted. There will be a lot of people out there to learn from and offer support and motivation regarding technology use. In other studies, individuals have been influenced by their social cycles in adopting certain technologies (Wang, McGill & Klobas 2020). In this study, it has been hypothesised that SI positively influences the behavioural intention to adopt BYOD.

H3-Effort expectancy positively influences the behavioural intention to adopt BYOD

Different technologies require different effort levels. Effort expectancy refers to the expected effort required to use the technology. The effort is usually evaluated based on the following elements: the perceived ease of use and complexity (Patil et al. 2020). The less complicated the technology is, the more likely it will be adopted. Effort expectancy has positively impacted the adoption of certain technologies; hence this hypothesis has been developed.

ISO/IEC 27001:2015 constructs

H4-Awareness and training positively influences the behavioural intention to adopt BYOD

The support clause of the ISO/IEC standard requires that AT be conducted to support entrenchment of an information security policy. Awareness and training are regarded as essential elements in providing support from a policy compliance perspective as per the requirements set out in the support section of the ISO/IEC 27001:2015 security standard. Users of information technology need to be aware of the risks involved with personally owned devices for work purposes.

Previously, researchers have used the ISO/IEC 27001:2015 security standard in various studies because of its best practice controls used to mitigate the BYOD related risks (Bounagui, Mezrioui & Hafiddi 2019; Hajdarevic, Allen & Spremic 2017).

Awareness and training are essential aspects that contribute to making employees aware of the adoption of technologies and how they work (Musarurwa et al. 2018). Bann et al. (2015) posited that the lack of awareness on the policies has often led to abuse of data as the users are not usually aware of information security risks. Based on this, the hypothesis on AT has been formulated to determine the employee's BI to adopt BYOD.

H5-Policy existence positively influences the behavioural intention to adopt BYOD

A policy that outlines management direction regarding the use of personally owned devices for work purposes has not been specifically looked at in the previous BYOD adoption studies. This research aims to determine if this construct influences BYOD adoption; hence this hypothesis formulation.

The leadership clause sets out the requirement that management of an organisation must give direction in terms of their information security stance regarding BYOD adoption from a strategic perspective. Consequently, an information security policy must be developed for an organisation and communicated to the relevant parties through AT on the support clause.

For this study, a BYOD security policy will be used as a model construct to determine if the existence of a BYOD policy influences the BI to adopt BYOD or not. The use of mobile devices and personal cloud services in the workplace can pose severe challenges if there is no guiding policy that helps manage the environment (Kadimo et al. 2018).

Additional construct from literature

H6-Organisational requirements positively influences the behavioural intention to adopt BYOD

The BYOD can be implemented by employees deciding to do so because of the organisation's lack of guidance on the adoption strategy. Retrospectively BYOD can also be adopted as a result of organisational requirements (OR_OR) (Fani et al. 2016; Ruxwana, Msibi & Mahlangu 2018). For instance, because of the COVID-19 outbreak, some organisations in South Africa required their employees to work from remote locations using their privately owned devices.

Suppose an organisation requires its employees to use their personally owned devices for work purposes. In that case, this hypothesis will confirm if such requirements are the only way employees can adopt BYOD or only through their preferences.

Research design and methods

Research design

A quantitative research approach was used in this study, and the IBM SPSS software was used for statistical data analysis.

The survey monkey online tool was used to develop an electronic survey for data gathering. The snowball method was used for the identification of participants and the distribution of the survey questionnaire. The survey link was e-mailed, sent to professional contacts on the LinkedIn website, and distributed via WhatsApp messages. The contacts were further requested to send to other relevant participants in their circle of influence.

Sampling

In South Africa, BYOD is implemented in various organisations, and it was not practical to identify the actual population of all the companies or employees who have adopted BYOD. Instead, a guideline of sample size selection in line with Krejcie and Morgan (1970) was used. A sample of 130 professional workers from different industries participated in the study. Only 106 responses were valid.

Results discussion

Table 1 consists of the participant's demographic information. The majority (56%) of the survey participants were over 40 years old with the younger respondents were between the ages of 19 and 25, making 6.6% of the participants. Participants worked in diverse industries such as health, construction and mining. The majority of the respondents were from unspecified sectors, followed by participants who worked within the health sector. The mining and the wholesale sectors were the least represented, with only 2.8% of the responses emanating from there, respectively.

TABLE 1: Demographic information.

Biographical details	Frequency	%
Age		
19–25	7	6.6
26–32	11	10.4
33–39	28	26.4
40+ years	60	56.6
Total	**106**	**100.0**
Gender		
Female	64	60.4
Male	42	39.6
Total	**106**	**100.0**
Experience		
1–5 years	11	10.4
6–10 years	17	16.0
11–15 years	23	21.7
16 years +	52	49.1
Less than 1 year	3	2.8
Total	**106**	**100.0**
Industry		
Mining	3	2.8
Wholesale and retail sector	3	2.8
Construction	4	3.8
Energy	6	5.7
Engineering	6	5.7
Education	8	7.5
Financial/Banking	12	11.3
Government Department/ Parastatal	14	13.2
Health	22	20.8
Other	28	26.4
Total	**106**	**100.0**

The correlation analysis was conducted to determine the correlation between two variables also referred to as the bivariate correlation where the relationship can either be positive or negative. The Pearson correlation co-efficient ranges between -1 and 1. The outcome of this analysis is outlined in Table 2, where the assessment of correlation of the following attributes: PE, BI, Pex, OR_OR, AT, EE and SI was conducted.

According to the results reflected in Table 2, the BI to adopt BYOD is highly correlated with the following constructs as r is a lot closer to 1: PE ($r = 0.854$, $n = 106$, $p < 0.01$), AT ($r = 0.68$, $n = 106$, $p < 0.01$), EE ($r = 0.63$, $n = 106$, $p < 0.01$) and moderately correlated to Pex ($r = 0.45$, $n = 106$, $p < 0.01$) and has a lower correlation with OR_OR ($r = 0.239$, $n = 106$, $p < 0.05$) and SI ($r = 0.259$, $n = 106$, $p < 0.01$).

Table 3 outlines a summary of the results of the multiple regression analysis and the variance analysis of the variables.

Multiple regression indicates each independent variable's relative contribution and further describes how much of the variance the dependent variable can explain in the independent variables. Internal reliability of the constructs is directly assessed through Cronbach alpha scores. A Cronbach's alpha value of 0.7 is deemed an acceptable threshold for reliability. The Cronbach alpha values that were acceptable for independent variables are: PE = 0.721; Pex = 0.781; AT = 0.774; EE = 0.729. The Cronbach alpha value for OR_OR = 0.317 which is unreliable.

The results of hypothesis test are depicted in Table 4 and Figure 3. Only four out of the six hypothesis statements were supported

The diagrammatical representation of the final model is illustrated in Figure 3, showing the results of hypothesis tests 1–6.

Based on the results depicted in Table 4 and Figure 3, it is evident that OR_OR and SI do not positively influence workers' decision to adopt BYOD in their organisations.

Performance expectancy in a bring your device context does have a strong influence in professional workers behavioural intention to adopt BYOD.

Performance and EE is dependent on several factors. The amount of effort required to use personally owned devices has also been found to influence the employee's BI to adopt BYOD. In terms of effort, the easier it is to use their privately owned mobile devices, the more likely the BI to adopt BYOD.

It is evident that with PE being strongly supported compared to the other three constructs, employees enjoy using a personally

TABLE 2: Correlation analysis results.

Constructs	Performance Expectancy (PE)	Behavioural Intention (BI)	Policy Existence (Pex)	Organizational Requirements (OR_OR)	Awareness and Training (AT)	Effort Expectancy (EE)	Social Influence (SI)
Performance Expectancy (PE)							
Pearson Correlation	1	0.854**	0.449**	0.577**	0.592**	0.752**	0.142
Sig. (2-tailed)	-	0.000	0.000	0.000	0.000	0.000	0.147
N	106	106	106	106	106	106	106
Behavioural Intention (BI)							
Pearson Correlation	0.854**	1	0.450**	0.239**	0.683**	0.632**	0.259**
Sig. (2-tailed)	0.000	-	0.000	0.014	0.000	0.000	0.007
N	106	106	106	106	106	106	106
Policy Existence (Pex)							
Pearson Correlation	0.449**	0.450**	1	0.318**	0.293**	0.390**	0.291**
Sig. (2-tailed)	0.000	0.000	-	0.001	0.002	0.000	0.002
N	106	106	106	106	106	106	106
Organizational requirements (OR OR)							
Pearson Correlation	0.577**	0.239*	0.318**	1	0.195*	0.697**	-0.120
Sig. (2-tailed)	0.000	0.014	0.001	-	0.045	0.000	0.222
N	106	106	106	106	106	106	106
Awareness and Training (AT)							
Pearson Correlation	0.592**	0.683**	0.293**	0.195*	1	0.839**	0.284**
Sig. (2-tailed)	0.000	0.000	0.002	0.045	-	0.000	0.003
N	106	106	106	106	106	106	106
Effort Expectancy (EE)							
Pearson Correlation	0.752**	0.632**	0.390**	0.697**	0.839**	1	0.142
Sig. (2-tailed)	0.000	0.000	0.000	0.000	0.000	-	0.148
N	106	106	106	106	106	106	106
Social Influence (SI)							
Pearson Correlation	0.142	0.259**	0.291**	-0.120	0.284**	0.142	1
Sig. (2-tailed)	0.147	0.007	0.002	0.222	0.003	0.148	-
N	106	106	106	106	106	106	106

*, Correlation is significant at the 0.05 level (2-tailed).

**, Correlation is significant at the 0.01 level (2-tailed).

In understanding the correlation results, the following thresholds are applicable: *r*-value of less 0.1 is insignificant; *r*-value of less than 0.3 is low; *r*-value of less than 0.5 is medium or moderate & *r*-value of greater than 0.7 is high (Steyn 2001).

owned device for work purposes because they are used to the functionality hence they can perform their tasks optimally.

Awareness and training was also tested in the model was found to influence BYOD's BI to adopt by workers.

Policy existence was also found to be of positive influence in making workers adopt BYOD in their organisations. Social factors were not found to have any influence on the worker's decision's to adopt BYOD.

Based on the outcome of H6, it is evident that OR_OR have a negative influence on the employee's BI to adopt BYOD.

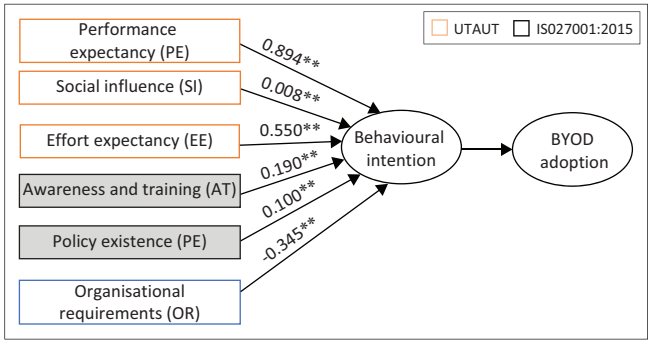
These results offer insight into the key constructs, which are important to be considered in order to promote BYOD adoption in different organisations. On the other hand, a balance is required when setting out OR_OR for BYOD adoption as these can discourage employees from adopting BYOD. It appears that employees would prefer to use their personally owned devices for work purposes instead of being forced into BYOD adoption.

Conclusion

This study aimed to investigate the factors influencing BYOD adoption using UTAUT and ISO/IEC 27001 security standard as a base plus an additional factor, the organisational requirement – a construct drawn from the reviewed literature. The factors investigated are PE, SI, EE from the UTAUT model and AT, policy existence (Pex) from the ISO 27001 security standard. Six hypotheses statements were formulated based on the proposed model constructs, and four were supported, and two were not

TABLE 3: Coefficients analysis.

Model	Independent Variables	Unstandardized coefficients		Standardised coefficients	*t*	Sig.
		B	Std. Error	Beta		
1	(Constant)	-0.415	0.243	-	-1.704	0.092
	Performance expectancy (PE)	1.224	0.082	0.894	15.006	0.000
	Policy existence (Pex)	0.086	0.038	0.100	2.259	0.026
	Organisational requirements (OR_OR)	-0.404	0.057	-0.345	-7.044	0.000
	Awareness & training (AT)	0.168	0.044	0.190	3.863	0.000
	Effort Expectancy (EE)	0.097	0.067	0.550	8.863	0.000
	Social influence (SI)	0.008	0.044	0.008	0.180	0.857



BYOD, bring your own device; UTAUT, unified theory of acceptance and use of technology.
**, Correlation is significant at the 0.01 level (2-tailed).

FIGURE 3: Final model of unified theory of acceptance and use of technology + International Organization for Standardisation/International Electrotechnical Commission 27001:2015.

supported as depicted in Table 4 and Figure 3 The factors that positively influence employee's BI to adopt BYOD in South African organisations are PE, EE, AT, and Pex. The PE had the most decisive influence on employee's BI to adopt BYOD, which clearly shows that professional workers choose to adopt BYOD because they firmly believe that they will perform exceptionally well in their jobs. The SI construct did not influence the employee's decision to adopt BYOD in this context. The OR_OR construct that may be in the form of stipulated requirements by organisations to adopt BYOD proved to negatively impact if BYOD adoption was to be a voluntary practice.

Notwithstanding this study's outcome, the outcome is beneficial in practice as it gives guidance regarding the drivers of BYOD adoption from UTAUT and ISO/IEC 27001 perspective. The novelty of the proposed framework, as depicted in Figure 2, is that it contributes academically by expanding the UTAUT framework with an industry practice security standard, ISO27001. Future research should focus on investigating factors which positively influence BYOD adoption using other technology adoption frameworks or by expanding the scope of UTAUT.

The model can be extended to include other variables such as privacy and constructs from other models such as TAM or Technology-Organisation-Environment (TOE). The sample size can be increased, and the participants from other countries can be used to test the model and see if it yields the same or different results. The moderating effect of variables can also be tested to determine their impact on the endogenous variable.

TABLE 4: Summary of results.

Hypothesis statements	Result	Outcome
H_1- Performance expectancy (PE) positively influences the behavioural intention to adopt BYOD	$\beta = 0.894$ $p < 0.05$	Supported
H_2- Social influence (SI) positively influences the behavioural intention to adopt BYOD	$\beta = 0.008$ $p < 0.05$	Not supported
H_3- Effort expectancy (EE) influences the behavioural intention to adopt BYOD	$\beta = 0.550$ $p < 0.05$	Supported
H_4- Awareness and training (AT) positively influences the behavioural intention to adopt BYOD	$\beta = 0.190$ $p < 0.05$	Supported
H_5- Policy existence (Pex) positively influences the behavioural intention to adopt BYOD	$\beta = 0.100$ $p < 0.05$	Supported
H_6- Organisational requirements (OR_OR) positively influences the behavioural intention to adopt BYOD	$\beta = -0.345$ $p < 0.05$	Supported negatively not positively

BYOD, Bring Your Own Device.

Limitations of the study are that participants were from South Africa, which could constrain the generalisability of the results. In addition, it was a quantitative study that might have limited certain views that participants could have given if it were a qualitative study.

The findings of this study can assist management of various organisations to identify strategies that can assist in encouraging employees to adopt BYOD, which will see employees benefit as well.

Acknowledgements

This research was only made possible through the willing Participants who agreed to participate in the study and respond to the survey questionnaire in full.

Competing interests

The author declares that she has no financial or personal relationship(s) that may have inappropriately influenced her in writing this article.

Author's contributions

The author contributed to this study from planning, execution and conclusion of the research study.

Ethical considerations

The researcher obtained ethical clearance from the University of the Witwatersrand's ethics committee before conducting this study, where the researcher was affiliated at the time.

Funding information

The author received no external financial support for the research, authorship and or publication of this article.

Data availability

The survey monkey platform was used for data collection. Access to this platform is restricted to only authorised users. However, arrangements can be made to provide the data to the requestor upon a reasonable request to the author.

Disclaimer

The views and opinions expressed in this article are those of the author and do not necessarily reflect the official policy or position of any affiliated agency of the author.

References

Alotaibi, B. & Almagwashi, H., 2018, 'A review of BYOD security challenges, solutions and policy best practices', in *1st International Conference on Computer Applications and Information Security*, ICCAIS, IEEE, 2018.

Ameen, A., Tarhini, A., Shah, M.H. & Madichie, M.O., 2020, 'Employees' behavioural intention to smartphone security: A gender-based, cross-national study', *Computers in Human Behavior* 104(March 2020), 106184. https://doi.org/10.1016/j.chb.2019.106184

Baillette, P., Barlette, Y. & Leclercq-Vandelannoitte, A., 2018, 'Bring your own device in organizations: Extending the reversed IT adoption logic to security paradoxes for CEOs and end users', *International Journal of Information Management* 43(June), 76–84. https://doi.org/10.1016/j.ijinfomgt.2018.07.007

Baishya, K. & Samalia, H.V., 2020, 'Extending unified theory of acceptance and use of technology with perceived monetary value for smartphone adoption at the bottom of the pyramid', *International Journal of Information Management* 51(April 2020), 102036. https://doi.org/10.1016/j.ijinfomgt.2019.11.004

Bann, L.L., Singh, M.M. & Samsudin, A., 2015, 'Trusted security policies for tackling advanced persistent threat via spear phishing in BYOD environment', *Procedia Computer Science* 72, 129–136. https://doi.org/10.1016/j.procs.2015.12.113

Bauer, S., Bernroider, E.W.N. & Chudzikowski, K., 2017, 'Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks', *Computers and Security* 68(4), 145–159. https://doi.org/10.1016/j.cose.2017.04.009

Bongiovanni, I., 2019, 'The least secure places in the universe? A systematic literature review on information security management in higher education', *Computers and Security* 86(September 2019), 350–357. https://doi.org/10.1016/j.cose.2019.07.003

Boonsiritomachai, W. & Pitchayadejanant, K., 2018, 'Determinants affecting mobile banking adoption by generation Y based on the unified theory of acceptance and use of technology model modified by the technology acceptance model concept', *Kasetsart Journal of Social Sciences* 40(2), 1–10. https://doi.org/10.1016/j.kjss.2017.10.005

Bounagui, Y., Mezrioui, A. & Hafiddi, H., 2019, 'Toward a unified framework for cloud computing governance: An approach for evaluating and integrating IT management and governance models', *Computer Standards and Interfaces* 62(September 2018), 98–118. https://doi.org/10.1016/j.csi.2018.09.001

Cao, Q. & Niu, X., 2019, 'Integrating context-awareness and UTAUT to explain Alipay user adoption', *International Journal of Industrial Ergonomics* 69(September 2018), 9–13. https://doi.org/10.1016/j.ergon.2018.09.004

Dang-Pham, D. & Pittayachawan, S., 2015, 'Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university: A protection motivation theory approach', *Computers and Security* 48, 281–297. https://doi.org/10.1016/j.cose.2014.11.002

Downer, K. & Bhattacharya, M., 2015, 'BYOD security: A new business challenge', *Proceedings – 2015 IEEE International Conference on Smart City, SmartCity 2015, Held Jointly with 8th IEEE International Conference on Social Computing and Networking, SocialCom 2015, 5th IEEE International Conference on Sustainable Computing and Communications,* IEEE, pp. 1128–1133.

Fani, N., Von Solms, R. & Gerber, M., 2016, 'A framework towards governing "Bring Your Own Device in SMMEs"', *2016 Information Security for South Africa – Proceedings of the 2016 ISSA Conference*, IEEE, pp. 1–8.

Gibbs, S., 2020, Dropbox hack leads to leaking of 68m user passwords on the internet. viewed 24 May 2020, from https://www.theguardian.com/technology/2016/aug/31/dropbox-hack-passwords-68m-data-breach.

Hajdarevic, K., Allen, P. & Spremic, M., 2017, 'Proactive security metrics for Bring Your Own Device (BYOD) in ISO 27001 supported environments', in *24th Telecommunications Forum, TELFOR 2016, Institute of Electrical and Electronics Engineers Inc*, IEEE.

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

Hovav, A. & Putri, F.F., 2016, 'This is my device! Why should I follow your rules? Employees' compliance with BYOD security policy', *Pervasive and Mobile Computing* 32, 35–49. https://doi.org/10.1016/j.pmcj.2016.06.007.

ISACA, 2020, *The benefits of allowing business use of personal mobile devices*, viewed 24 May 2020, from https://www.isaca.org/resources/isaca-journal/past-issues/2013/jonline-using-personal-mobile-devices-in-a-business-setting%0D.

ISO/IEC, 2015, *ISO/IEC 27001. Information technology – Security techniques – Information security management systems – Requirements*, South African National Standard, SABS Standards Division, Pretoria.

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

Krejcie, R.V. & Morgan, D.W., 1970, 'Determining sample size for research activities', *Educational and Psychological Measurement* 30, 607–610.

Lennon, R.G., 2012, 'Changing user attitudes to security in bring your own device (BYOD) & the cloud', *Proceedings – 2012 5th Romania Tier 2 Federation Grid, Cloud and High Performance Computing Science, RQ-LCG 2012*, IEEE, pp. 49–52.

Madzima, K., Moyo, M. & Abdullah, H., 2014, 'Is bring your own device an institutional information security risk for small-scale business organisations?', *2014 Information Security for South Africa – Proceedings of the ISSA 2014 Conference*, IEEE.

Morrow, B., 2012, 'BYOD security challenges: Control and protect your most sensitive data', *Network Security* 2012(12), 5–8. https://doi.org/10.1016/S1353-4858(12)70111-3

Musarurwa, A., Flowerday, S. & Cilliers, L., 2018, 'An information security behavioral model for the bring-your-own-device trend', *SA Journal of Information Management* 20(1), 1–9. https://doi.org/10.4102/sajim.v20i1.980

Patil, P., Tamilmani, K., Rana, N.P. & Raghavan, V., 2020, 'Understanding consumer adoption of mobile payment in India: Extending Meta-UTAUT model with personal innovativeness, anxiety, trust, and grievance redressal', *International Journal of Information Management* 54(October 2020), 102144. https://doi.org/10.1016/j.ijinfomgt.2020.102144

Rahi, S., Abd.Ghani, M. & Ngah, A.H. 2019, 'Integration of unified theory of acceptance and use of technology in internet banking adoption setting: Evidence from Pakistan', *Technology in Society* 58(August 2019), 101120. https://doi.org/10.1016/j.techsoc.2019.03.003

Romer, H., 2014, 'Best practices for BYOD security', *Computer Fraud and Security* 2014(1), 13–15. https://doi.org/10.1016/S1361-3723(14)70007-7

Ruxwana, N., Msibi, M. & Mahlangu, T., 2018, 'Bring your own device adoption readiness in a South African University', *South African Review of Sociology* 49(3–4), 78–95. https://doi.org/10.1080/21528586.2019.1580218

Steyn, H., 2001, 'Practical significant relationships between two constructs', *South African Journal of Industrial Psychology* 28(3), 10–15.

Vignesh, U. & Asha, S., 2015, 'Modifying security towards BYOD', *Procedia Computer Science* 50, 511–516.

Wang, X., McGill, T.J. & Klobas, J.E., 2020, 'I want it anyway: Consumer perceptions of smart home devices', *Journal of Computer Information Systems* 60(5), 437–447. https://doi.org/10.1080/08874417.2018.1528486

Yang, C., Hong-Chao, H. & Guo-Zhen, C., 2019, 'A software-defined intranet dynamic defense system', *International Conference on Communication Technology Proceedings, ICCT, IEEE*, 2019–October, pp. 849–854.