International Journal of Science Annals, Vol. 7, No. 2, 2024
print ISSN: 2617-2682; online ISSN: 2707-3637; DOI:10.26697/ijsa

SOCIAL AND BEHAVIORAL SCIENCES. Health Care Sciences

ORIGINAL RESEARCH

An Information Security Assessment Model for Bring Your Own Device in the South African Healthcare Sector

Authors' Contribution:
A – Study design;
B – Data collection;
C – Statistical analysis;
D – Data interpretation;
E – Manuscript preparation;
F – Literature search;
G – Funds collection

Moeketsi C. B.[1 ABCDEFG], **Adeyelure T. S.**[1 ABCDEFG], **Segooa M. A.**[1 ABCDEFG]

[1] *Tshwane University of Technology, South Africa*

Received: *29.06.2024;* ***Accepted:*** *30.07.2024;* ***Published:*** *25.12.2024*

Abstract

Background and Aim of Study: *The healthcare sector stands at the forefront of industries embracing personal-device usage for professional tasks. Permitting to Bring Your Own Device (BYOD) for healthcare professionals presents information security hurdles that pose challenges for decision-makers in the healthcare field, despite the considerable benefits associated with BYOD. The aim of the study: to develop an information-security assessment model for BYOD in the South African healthcare sector to guide healthcare decision-makers.*

Material and Methods: *The main focus of the study was the South African private healthcare sector, Gauteng Province. The target population size of 170 with a sample size of 118 with the feedback responses with additional 10, which were also included in the analysis data statistics that was done for 128 received responses. The instrument used for the closed-ended questionnaire was SPSS 28.0.1.1 and the expert judgement technique for the validation questionnaire. Factors from the diffusion of innovation theory, the electronic protected health information security framework, cybersecurity knowledge, skills, abilities and external variables were adapted to inform the conceptual model.*

Results: *The following factors have the most significant contributions to the development of an information security assessment model for BYOD in the South African healthcare sector: training is the most influential factor with a predictive power of 64.0% ($\beta=0.640$) at $p=0.001$; security threats with 61.3% ($\beta=0.613$) significance level $p=0.020$; conversely, security controls had a predictive power of 50.9% ($\beta=0.509$) at $p=0.001$.*

Conclusions: *This study has developed a contextual information-security assessment model for BYOD within the South African healthcare sector. In practical terms, this model offers guidance to healthcare decision-makers in seamlessly integrating BYOD practices into daily operations; and aids in cautious planning, guided by the insights provided by the security-assessment model for BYOD.*

Keywords: *healthcare, private, information security, bring your own device, South Africa.*

DOI: *https://doi.org/10.26697/ijsa.2024.2.1*

Conflict of interests: *The authors declare that there is no conflict of interests*

Peer review: *Double-blind review*

Source of support: *This research did not receive any outside funding or support*

Information about the authors: ***Moeketsi Catherine Botlwaelo*** *(Corresponding Author) – https://orcid.org/0009-0006-4120-7691; cthmoeketsi@gmail.com; Master of Computing, Department of Informatics, Tshwane University of Technology, Pretoria, South Africa.*

Adeyelure Tope Samuel *– https://orcid.org/0000-0002-6138-4285; Doctor of Computing Science and Data Processing, Senior Lecturer, Department of Informatics, Tshwane University of Technology, Pretoria, South Africa.*

Segooa Mmmatshuene Anna *– https://orcid.org/0000-0002-4190-8256; Doctor of Computing, Lecturer, Department of Informatics, Tshwane University of Technology, Pretoria, South Africa.*

Introduction

Information Communication Technology (ICT) plays a vital role in facilitating various business solutions, by offering a wide range of technical and software application platforms for organizations to enhance their operational efficiency. With the continuous evolution of technology, organizations are harnessing these advancements to stay competitive in the market. This has led to a gradual shift towards digital platforms and products for day-to-day operations, transforming information technology (IT) from a mere service provider into a strategic asset driving current business operations (Omboga et al., 2021; Pypenko, 2019). Additionally, there is a rising trend of mobility adoption, in which employees utilize their personal devices for both personal and professional tasks. Some organizations, especially in developing countries, have implemented permissive policies allowing the use of personal devices for business purposes (Pypenko, & Melnyk, 2021; Wani et al., 2021).

The utilization of personal devices, such as cellphones, computers, laptops, and tablets in business operations has been proven to boost employee morale, enhance work performance, and save costs (Mahat & Ali, 2018). Employees feel more flexible and comfortable using familiar devices anytime, anywhere. Smart mobile devices are increasingly prevalent in workplaces as organizations embrace Bring Your Own Device (BYOD) policies (Downer & Bhattacharya, 2022). This practice positively impacts business processes, necessitating strategic planning, user awareness, and training (Kholoanyane, 2020). BYOD adoption brings multiple benefits, including improved performance, enhanced business processes, cost-efficiency, and heightened employee morale, leading to increased productivity (Coker, 2021). Leveraging personal devices enables organizations to realize numerous advantages, ranging from cost savings to enhanced productivity and morale. This approach fosters a more agile and connected workforce, particularly crucial in sectors such as healthcare where rapid access to information can be lifesaving (Ujakpa et al., 2019).

In South Africa, the healthcare sector faces challenges in delivering timely services due to inadequate technology support for digital health platforms, mobile health, and smart technology such as BYOD. Such technologies could benefit both the public and private sectors, including medical aid schemes (Ali et al., 2021). The increasing demand for BYOD as a service underscores its importance in organizational infrastructure, given its agility, business flexibility, boosted employee morale, improved productivity, and enhanced employee satisfaction (Abdulkarim & Binord, 2021). These factors highlight the potential of BYOD to enhance workplace productivity and efficiency.

Despite the acknowledged benefits of BYOD in enhancing organizational efficiency, there is a critical need for an information-security assessment model specifically tailored for the South African healthcare sector. This sector, already grappling with inadequate technology support, urgently requires a contextualized model to assess and mitigate security risks associated with BYOD adoption. Developing such an information-security assessment model is essential to ensure the overall operational efficiency of healthcare providers in South Africa. To address this research gap, the study developed an information-security assessment model for Bring Your Own Device in the South African healthcare sector.

The aim of the study. To develop an information-security assessment model for BYOD in the South African healthcare sector from the perspective of behavioral science, specifically within the niche of Business Information Systems.

This research diverges from the traditional pure computing system approach, focusing instead on understanding the factors that influence information security in BYOD environments. By examining the interactions between the identified factors, the study aims to create a contextual model that addresses the unique security challenges within the domain of the study. This approach underscores the importance of integrating human-centered insights with technical solutions to enhance security measures within the South African healthcare sector.

Materials and Methods

The study employed design science research methods, which aimed to develop artefacts to address research problems. This process involves five iterative steps (Kuechler & Vaishnavi, 2011). Firstly, there is awareness of the problem, influenced by preliminary investigations that identified the absence of a contextual information-security assessment model for BYOD in the South African healthcare sector. Next, the suggestion of the artefact as a potential solution is made based on existing theories. Following that is the development phase, in which the artefact is created using various theories to formulate an assessment-security model for guiding BYOD implementation in the South African healthcare sector.

Validation involves measuring the validity of the developed artefact through expert judgment. Finally, in the conclusion phase, the results obtained through expert judgment are presented. A group of selected experts validated the developed model, contributing to the validation process of the artefact. Kuechler and Vaishnavi (2011) commented that the results of an artefact or developed model are reflected in the conclusion stage of design-science research.

Design science research (DSR) functions as a problem-solving paradigm focused on advancing human understanding by creating innovative solutions (vom Brocke et al., 2020). In essence, DSR seeks to enhance knowledge domains in technology and science by crafting new artefacts that tackle challenges and improve their respective environments. This study adhered to the principles of design science research in line with its overarching objective: the development of an information-security assessment model tailored for BYOD implementation in the South African healthcare sector.

In this study, the researcher collaborated with the ICT directorate, who facilitated the distribution of the questionnaire to employees and IT subject matter experts in the healthcare sector. Before distributing the questionnaire, a permission letter was issued, and the contact person was assured that data collection would be anonymous, private, and solely for research purposes. A Google Form was created, and a link was sent to the ICT directorate to aid in distributing it to healthcare staff.

The research adopted a mixed-method approach, integrating both quantitative and qualitative analyses. In line with this methodology, a survey questionnaire was adopted, gathering data from a total of 128 randomly selected individuals. Expert Judgement was used in this study, and the validity of the developed artefact was determined by the experts' responses to the developed model validation questionnaire.

The reliability of the measuring instrument was tested and was reliable based on the output in Table 1.

Table 1

Overall Reliability Statistics of the Measuring Instrument: Reliability Statistics

Cronbach's alpha	Number of items
0.959	54

According to Yin (2014), measuring instrument with values above 0.7 threshold are acceptable and deemed reliable. The overall reliability of the questionnaire with 54 items as demonstrated in Table 1 was found to be 0.959, which reliability was considered good since it was above the recommended threshold of 0.7, and comparing the number of items in the questionnaire.

Results

The results demonstrated indicated that all hypotheses were supported after data analysis at an acceptable at the p value with a significant value less than 0.05, which is acceptable; and therefore, the conceptual model was not iterated before it was taken to the experts for validation. The reliability statistics table demonstrated relationships between constructs were supported.

The sample size of 128 respondents was considered and therefore, Part one focused on gathering demographic information such as organization, age, gender, profession, race, educational level, and years of service. Part two centered on assessing participants' knowledge of computers, information security, and BYOD. Participant's demographics are shown in Table 2, which is broken down into the relevant categories.

Table 2

Frequencies of Participants' Demographics

Variables		Frequency			
		Person	Percent	Valid percent	Cumulative percent
Organisation	Public healthcare	18	14.1	14.1	14.1
	Private healthcare	88	68.8	68.8	82.8
	Pharmaceutical	11	8.6	8.6	91.4
	Clinical services	11	8.6	8.6	100.0
	Total	128	100.0	100.0	–
Years in the organisation	2 years or less	10	7.8	7.8	7.8
	3-5 years	24	18.8	18.8	26.6
	6-10 years	56	43.8	43.8	70.3
	10 years+	38	29.7	29.7	100.0
	Total	128	100.0	100.0	–
Highest level of education	Matric/Certificate	19	14.8	14.8	14.8
	Diploma	54	42.2	42.2	57.0
	Bachelor's degree	37	28.9	28.9	85.9
	Postgraduate	15	11.7	11.7	97.7
	Other	3	2.3	2.3	100.0
	Total	128	100.0	100.0	–
Gender	Male	65	50.8	50.8	50.8
	Female	58	45.3	45.3	96.1
	Other	5	3.9	3.9	100.0
	Total	128	100.0	100.0	–
Age	<25 years	8	6.3	6.3	6.3
	26-35 years	40	31.3	31.3	37.5
	36-45 years	59	46.1	46.1	83.6
	46-55 years	17	13.3	13.3	96.9
	55+ years	4	3.1	3.1	100.0
	Total	128	100.0	100.0	–

The outcomes in Table 2 take the individuals' operational space into account. Some of participants (14.1%) work within the public sector; these are individuals who have partnered with the private sector. About 68.8% of participants work within the private sector space. Some of responses (8.6%) were received for both pharmaceutical and clinical services that are also partnering with the private healthcare sector. More responses were attained from the private healthcare sector, at about 68.8% responses.

The outcomes in Table 2 take the individuals' years within the organization into account. Some of participants (7.8%) had 2 years or less of service. About 18.8% of participants had between 3-5 years of service. About 43.8% of the largest group of participants had 6-10 years of experience within the organization; and 29.7 % of participants had 10 years + of service.

There were 14.8% of participants with matric/certificate. Participants with a bachelor's degree made up 28.9% of the group, while those with a post-graduate degree made up 11.7%. Participants with "other" numbered 2.3%, while the 42.2% of survey respondents with a diploma yielded the highest percentage.

Both genders participated in the survey, according to the findings. The percentage of male participants was 50.8%, while the percentage of female participants was 45.3% and 'other' made up 3.9% of participants. The highest number of responses was from male participants at 50.8%.

Participants who were under 25 years made up 6.3% of the total. Some 31.3% of participants were between the ages of 26 and 35; 46.1% were between the ages of 36 and 45; and 13.3% were between the ages of 46 and 55. Participants who were 55 and above made up 3.1% of the total. According to the table, individuals who were between the ages of 36 and 45 made up the highest percentage of participants at 46.1%.

Pearson's Correlation of the Constructs

Correlation, in a general sense, assesses the connection between variables; and quantifies the degree of association between two variables (Talaat & Gamel, 2023). When two variables change in magnitude, they do so either in the same direction (positive correlation) or in the opposite direction (negative correlation) in correlated data. This technique gauges the relationship between continuous variables that are both dependent and independent. Additionally, this method can have both advantages and drawbacks. A negative correlation suggests that, as the value of one variable increases, the value of the other variable decreases; whereas a positive correlation indicates that as one variable's value increases, the value of the other variable also increases. Table 3 indicates factors grouped together with a positive and a significantly high correlation with one another. Correlation coefficient values, as outlined by Schober et al. (2018), range from -1 to 1, with -1 indicating a perfect negative correlation; and 1 indicating a perfect positive correlation. Pearson's correlation approach was employed in this study to represent the relationship between the constructs. According to Xiong et al. (2020), if p is greater than 0.01 but less than or equal to 0.05, a strong assumption about the null hypothesis must be made. If p is less than or equal to 0.01, it indicates a very strong assumption about the null hypothesis. The correlation between the constructs utilized in this study is depicted in Table 3, which illustrates the relationship between the constructs employed in this study.

Table 3
Pearson's Correlation of the Constructs

Constructs		ISA	SECT	POL	SECC	COMP	COMPL	TRN	SECM
ISA	Pearson Correlation	1.000	–	–	–	–	–	–	–
SECT	Pearson Correlation	0.655**	1.000	–	–	–	–	–	–
POL	Pearson Correlation	0.465**	0.691**	1.000	–	–	–	–	–
SECC	Pearson Correlation	0.420**	0.648**	0.705**	1.000	–	–	–	–
COMP	Pearson Correlation	0.324**	0.527**	0.694**	0.635**	1.000	–	–	–
COMPL	Pearson Correlation	0.358**	0.558**	0.556**	0.631**	0.704**	1.000	–	–
TRN	Pearson Correlation	0.498**	0.583**	0.606**	0.675**	0.490**	0.459**	1.000	–
SECM	Pearson Correlation	0.676**	0.793**	0.812**	0.828**	0.753**	0.741**	0.763**	1.000

Note. ISA – information-security abilities factors; SECT – security-threats factors; POL – policy factors; SECC – security-controls factors; COMP – compatibility factors; COMPL – complexity factors; TRN – training factors; SECM – information security assessment model for BYOD; ** Correlation is significant at the 0.01 level (2-tailed); * Correlation is significant at the 0.05 level (2-tailed).

The table shows that information-security abilities (ISA) factors have a significant relationship of 0.655 (2-tailed) with security threats, with a significant relationship at the 0.01 level.

Policy factors have a significant relationship of 0.465 (2-tailed), with ISA factors; and security threats with a significant relationship of 0.691 (2-tailed) both at the 0.01 level.

Furthermore, the security control factor has a significant relationship with ISA of 0.420 (2-tailed), a significant relationship with security threats of 0.655 (2-tailed), and policy factor with a significant relationship of 0.648 (2-tailed) both at the 0.01 level.

Meanwhile, the compatibility factor has a significant relationship with the ISA factors of 0.324 (2-tailed), with security threats of 0.527 (2-tailed), with the policy factor of .705 (2-tailed), and a significant relationship with security controls of 0.625 (2-tailed) and all at the 0.01 level.

Moreover, the complexity factor has a significant relationship with ISA factors of 0.358 (2-tailed), with security threats of .558 (2-tailed), with policy of 0.556 (2-tailed), with security control of 0.631 (2-tailed), and lastly a significant relationship with compatibility of 0.704 and all at the 0.01 level.

Furthermore, the training factor has a significant relationship with information-security ability factors of 0.498 (2-tailed), with security threats of 0.583 (2-tailed), with policy of 0.606 (2-tailed), with security controls of 0.675 (2-tailed), with compatibility of 0.490 (2-tailed) and with complexity of 0.459 (2-tailed) and all at the 0.01 level.

Furthermore, there is high value concerning the correlation of security controls and policy of 0.705 (2-tailed) that is at the 0.01 level.

For this reason, an information-security assessment model for BYOD can be integrated into day-to-day operations of the healthcare sector.

The variables show a positive significant relationship at a 2-tailed which is supported by Pearson correlation at a *R* value of 96.9% prediction and a p value less than 0.05.

Regression Analysis

In addition to descriptive analysis, a regression analysis was performed to assess the predictive capability of the overall model and the individual contributions of each independent variable to this prediction.

The analysis revealed a robust predictive power for the model at 94.0% (R^2=0.940).

The specific contributions of each independent variable to this prediction are detailed in the results presented in Table 4.

Table 4

*Regression Coefficients**

Model	Unstandardized coefficients		Standardized coefficients	*t*	Sig.	Collinearity statistics	
	B	Std. Error	Beta			Tolerance	VIF
(Constant)	0.867	0.561	–	3.155	0.002	–	–
ISA	0.207	0.152	0.242	7.944	0.001	0.429	1.630
SECT	0.613	0.259	0.091	2.362	0.020	0.434	1.602
POL	0.273	0.305	0.164	4.172	0.001	0.257	1.887
SECC	0.509	0.279	0.208	5.403	0.001	0.353	1.836
COMP	0.124	0.259	0.162	4.344	0.001	0.369	1.712
COMPL	0.298	0.246	0.181	5.281	0.001	0.453	1.408
TRN	0.640	0.112	0.187	5.723	0.001	0.475	2.107

Note. *Dependent variable: SECM – information security assessment model for BYOD; ISA – information-security abilities factors; SECT – security-threats factors; POL – policy factors; SECC – security-controls factors; COMP – compatibility factors; COMPL – complexity factors; TRN – training factors.

The results presented in Table 4 reveal significant contributions of various factors to the development of an information security assessment model for BYOD in the South African healthcare sector.

Training emerged as the most influential factor, with a predictive power of 64.0% (β=0.640) at p=0.001, followed by security threats at 61.3% (β=0.613) significance level p=0.020.

Conversely, security controls exhibited a predictive power of 50.9% (β=0.509) at p=0.001. According to Ahamed et al. (2023), a Variance Inflation Factor (VIF) exceeding 10 indicates problematic multicollinearity. However, Table 3 indicates that all VIF values were below 5, indicating an absence of multicollinearity.

Testing of the Hypotheses

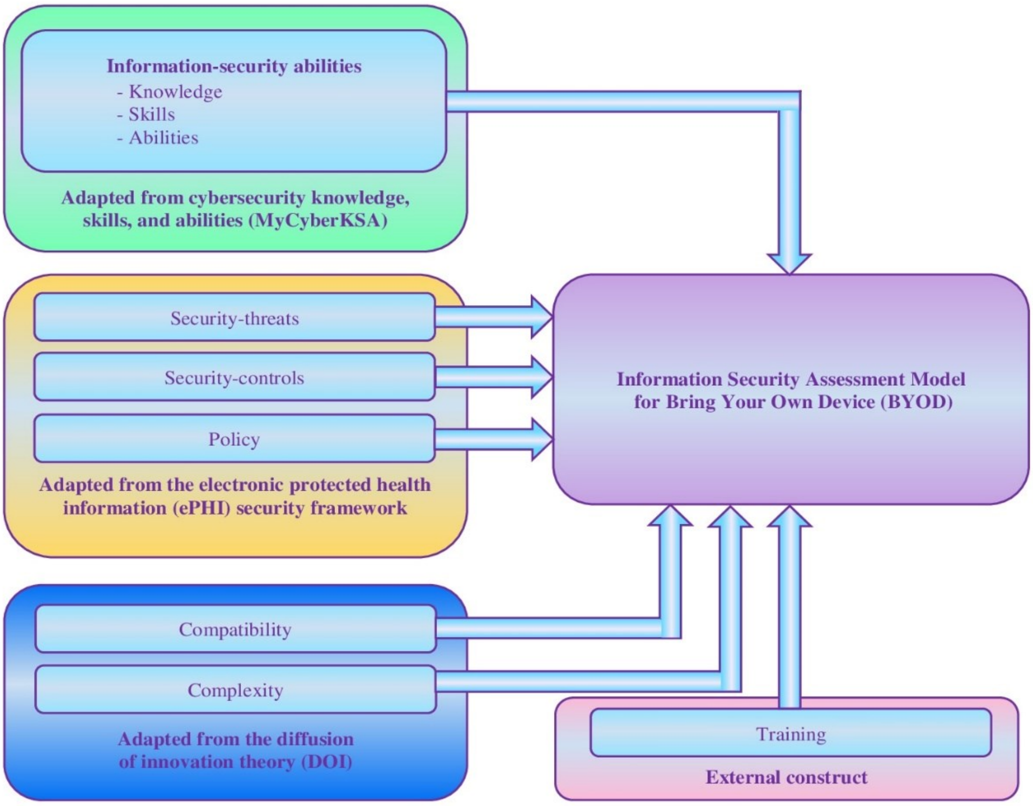
Based on the regression and correlational analysis, the set hypotheses were tested; and the results are presented in Table 5.

Table 5
Testing of the Hypotheses

Hypotheses	Results	Action
H1-Information-security abilities factors, skills, and knowledge in the organisation influence the development of an information-security assessment model for BYOD	P=0.001<0.05	Supported
H2-Security-threats factors in the organisation influence the development of an information-security assessment model for BYOD	P=0.020<0.05	Supported
H3-Policy factors in the organisation influence the development of an information-security assessment model for BYOD	P=0.001<0.05	Supported
H4-Security-controls factors in the organisation influence the development of an information-security assessment model for BYOD	P=0.001<0.05	Supported
H5-Compatibility factors in the organisation influence the development of an information-security assessment model for BYOD	P=0.001<0.05	Supported
H6-Complexity factors in the organisation influence the development of an information-security assessment model for BYOD	P=0.001<0.05	Supported
H7-Training factors in the organisation influence the development of an information-security assessment model for BYOD	P=0.001<0.05	Supported

Based on these findings, a conceptual model for an information security assessment model for BYOD in the South African Healthcare Sector was developed, as illustrated in Figure 1.

Figure 1
An Information Security Assessment Model for Bring Your Own Device in the South African Healthcare Sector


Information-security abilities
- Knowledge
- Skills
- Abilities
Adapted from cybersecurity knowledge, skills, and abilities (MyCyberKSA)
Security-threats
Security-controls
Policy
Adapted from the electronic protected health information (ePHI) security framework
Information Security Assessment Model for Bring Your Own Device (BYOD)
Compatibility
Complexity
Adapted from the diffusion of innovation theory (DOI)
Training
External construct

Model Validation

The validation of the proposed information-security assessment model for BYOD in the South African healthcare sector was conducted with seven experts who provided comprehensive feedback. The reviewers, possessing diverse qualifications and extensive experience in information security, unanimously agreed on the model's relevance, suitability, and significance. They indicated that the model is highly appropriate for improving business productivity, guiding decision-makers, and enhancing security measures within the healthcare sector. The feedback from the experts highlighted that the model effectively addresses the necessary constructs and requires no modifications, confirming its adequacy and applicability. From the feedback obtained from the seven experts' review, the model is considered relevant, suitable, and significant, and it will serve as a guide for decision-makers in assessing information security for BYOD in the South African healthcare sector. The developed artifact was not modified as all the constructs were supported.

Discussion

The results of this study, all 7 variables were all supported and found to be significant to be integrated into the day-to-day healthcare operations.

Information-Security Abilities Factors

It was predicted that H1-Information-Security Abilities Factors will have a significant influence on the information-security assessment model for BYOD integration into the South African healthcare sector. The findings of this study, depicted in Figure 1, supported the hypothesis. Information-security abilities emerged as influential and significant factors in developing an information-security assessment model for BYOD integration. Dash and Ansari (2022) underscored the necessity of considering extensive competencies such as skills, experience, and knowledge, along with their interrelationships, to craft a practical security model. Within the healthcare sector, information-security abilities for BYOD signify the depth of skills and knowledge relevant to the information-security domain. These assessment models are typically constructed and upheld by experts within the security domain.

As noted by Chowdhury and Gkioulos (2023), the escalating demand within modern enterprises for proficient security professionals has spurred the proliferation of various programmes and initiatives aimed at imparting security skills and knowledge. Despite increased awareness among enterprise staff regarding security threats, the incidence of successful attacks against companies has shown little to no decline over the years.

Security-Threats Factors

It was predicted that H2-Security-Threats Factors will have a significant influence on the information-security assessment model for BYOD integration into the South African healthcare sector. This hypothesis predicted a positive correlation between the security threats factor and the integration of the information-security assessment model for BYOD in this study. The questionnaire was designed to evaluate the organization’s readiness regarding mitigation plans for information-security breaches and employee awareness. Vulnerabilities in hardware, software, and networks, along with tactics such as phishing scams and social-engineering techniques, are frequently exploited by attackers. These threats often propagate through channels such as drive-by downloads, malicious email attachments, and deceptive applications (Aslan et al., 2023). The hypothesis confirmed that the security factor significantly influences the integration of an information-security assessment model for BYOD into the South African healthcare sector. Furthermore, this influence can be strengthened through preventive measures such as established protocols, training programmes, tailored policies, and mitigation strategies.

Policy Factors

It was predicted that H3-Policy Factors will have a positive influence on the information-security assessment model for BYOD integration into the South African healthcare sector. This hypothesis was validated, impacting the development of the information-security assessment model for BYOD integration. Farid et al. (2023) define an information-security policy as a widely recognized foundational framework for organizational information security, serving a pivotal role in communicating both acceptable and unacceptable actions concerning the organization’s assets to employees. Consequently, this hypothesis bolsters the information-security assessment model for BYOD integration.

Security-Controls Factors

It was predicted that H4-Security-Controls Factors will have a significant influence in the information-security assessment model for BYOD integration into the South African healthcare sector. The hypothesis received support based on the findings presented in Figure 1 of this study. Access control measures are indispensable for safeguarding the information and assets of the healthcare sector against both internal and external threats, thereby reducing vulnerability to physical and cyberattacks (Ayedh et al., 2023). Alshurideh et al. (2023) aver that security measures within computer systems include various techniques such as speech analysis, firewalls, and digital signatures, aimed at protecting software, devices, and data contained within the system. However, the security of BYOD technology faces contemporary challenges, including inadequate security controls on devices commonly used by healthcare professionals, concerns regarding device locking and authentication; and issues related to the security of mobile-device applications (Wani et al., 2020). Consequently, the validated hypothesis indicates that the security-controls factor significantly influences the integration of an information-security assessment model for BYOD into the South African healthcare sector. Furthermore, this influence can be augmented by implementing robust access-control mechanisms for personal devices to safeguard confidential patient information in the healthcare sector.

Compatibility Factors

It was predicted that H5-Compatibility Factors will have a significant influence in the information-security assessment model for BYOD integration into the South African healthcare sector. The hypothesis was validated as per Figure 1 in the study. This indicates that employees and experts in the healthcare sector indeed perceive their daily activities to impact the information-security assessment model for BYOD. Neves and Mello (2018) posit that security models compatible with a company’s technologies and infrastructure should remain under the company’s control; and devices with unfixable vulnerabilities should be prohibited. Additionally, according to Liao et al. (2021), the compatibility perspective is predominantly utilized and particularly relevant for understanding users’ technology usage behaviour. Four compatibility principles compatibility with established work practices, chosen work style, prior experience, and value are linked to IT innovation within the enterprise context. The compatibility factor demonstrates a substantial influence on the integration of the information-security assessment model for BYOD into the South African healthcare sector.

Complexity Factors

It was predicted that H6-Complexity Factors will significantly influence the information-security assessment model for BYOD integration into the South African healthcare sector. Complexity refers to how difficult it is to comprehend or utilize a particular system or technology, which impacts perceptions of innovation. Almaiah et al. (2022) suggest that when technology is less complex and characterized as simple, it is perceived as highly sophisticated and advantageous, especially if it includes new technologies and inventive features. The complexity of the developed model needed validation by a group of experts to ensure its integration into the healthcare sector's daily operations and services would not be overly complex. The validation process involved experts, who positively responded to the model. Testing and validation of newly designed models are crucial, as stated by Hao et al. (2021), necessitating thorough examination by a group of individuals or a pilot group before deployment across the organization. Complex systems, as highlighted by Freund et al. (2021), offer significant opportunities for innovation within existing and potential fields of application. Strategic complexity management frameworks or models for system deployment encapsulate the complexity of IT systems. A survey questionnaire was developed to gather information about the complexity of integrating a developed artefact into existing processes.

Training Factors

It was predicted that H7-Training Factors will positively influence the information-security assessment model for BYOD integration into the South African healthcare sector. The hypothesis found support in the study's findings, as illustrated in Figure 1. Beltempo et al. (2022) stressed ongoing research aimed at improving security training across the healthcare sector for all employees. This study gave precedence to the training factor, evaluating the number of healthcare-sector employees undergoing information-security and BYOD training. The survey questionnaire specifically targeted the information-security-awareness training posture among healthcare-sector employees. Alahmari et al. (2023) underscored the critical role of effective security training as the primary defence against security breaches. These researchers advocated for the IT department to prioritize delivering information-security awareness training, with regular updates on security risks and fraudulent methods, ensuring that employees maintain vigilance and prevent unauthorized access to organizational information systems, whether using personal or organizational devices.

The supported hypothesis highlights the importance of the training factors, which may sometimes be overlooked, but nevertheless significantly enhances employees' vigilance when using personal and organizational devices for work-related tasks. In conclusion, all seven supported constructs contribute to an information-security assessment model for BYOD integration, indicating its potential success in the South African healthcare sector. Decision-makers can effectively integrate this model into their day-to-day operations and services, bolstering overall security measures. Furthermore, future studies should also explore the financial aspects of BYOD. This study only focused on identifying factors that influence the development of the artefact, excluding the financial aspects. The developed model can be the baseline for additional factors to be incorporated into the type of research to be undertaken.

Conclusions

Adopting new technology platforms presents significant challenges for daily business operations, but it is essential for maintaining competitiveness. Successful integration of new systems requires ongoing support, monitoring, and maintenance. This study developed an information-security assessment model for BYOD in the South African healthcare sector, with a focus on equipping stakeholders with the necessary knowledge for the secure use of personal devices. The research involved 128 respondents and 7 experts, all data collected was valid and used for analysis. The study followed the design science research process to identify key factors, and develop, and validate the model. The validity of the model within the research domain was confirmed by the experts. However, the study proposed further investigation into the financial implications of BYOD, which may influence security measures.

Acknowledgments

The authors wish to acknowledge all those that participated in this study. Thank you so much for support.

Ethical Approval

The study obtained ethical clearance from the institution Ethics Committee (Ref. No. FCRE/ICT/2022/08/002(1).

Funding Source

This research did not receive any outside funding or support.

References

Abdulkarim, S., & Binord, F. (2021). The psychological effects of Bring Your Own Device (BYOD). *OIRT Journal of Information Technology, 1*(2), 6–9. https://doi.org/10.53944/ojit-2103

Ahamed, M. I., Biswa, A., & Phukon, M. (2023). A study on multicollinearity diagnostics and a few linear estimators. *Advances and Applications in Statistics, 89*(1), 29–54. https://doi.org/10.17654/0972361723050

Alahmari, S., Renaud, K., & Omoronyia, I. (2023). Moving beyond cyber security awareness and training to engendering security knowledge sharing. *Information Systems and e-Business Management, 21*(1), 123–158. https://doi.org/10.1007/s10257-022-00575-2

Ali, R. F., Ali, S. E. A., Rehman, M., & Sohail, A. (2021). Information security behavior and information security policy compliance: A systematic literature review for identifying the transformation process from noncompliance to compliance. *Applied Sciences, 11*(8), Article 3383. https://doi.org/10.3390/app11083383

Almaiah, M. A, Alfaisal, R., Salloum, S. A., Hajjej, F., Shishakly, R., Lutfi, A., Alrawad, M., Al Mulhem, A., Alkhdour, T., & Al-Maroof, R. S. (2022). Measuring institutions' adoption of artificial intelligence applications in online learning environments: Integrating the innovation diffusion theory with technology adoption rate. *Electronics, 11*(20), Article 3291. https://doi.org/10.3390/electronics11203291

Alshurideh, H. M., Alquqa, E., Alzoubi, H., Kurdi, B., & Hamadne, S. (2023). The effect of information security on e-supply chain in the UAE logistics and distribution industry. *Uncertain Supply Chain Management, 11*(1), 145–152. https://doi.org/10.5267/j.uscm.2022.11.001

Aslan, Ö., Aktug, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics, 12*(6), Article 1333. https://doi.org/10.3390/electronics12061333

Ayedh, M. A. T., Wahab, A. W. A., & Idris, M. Y. I. (2023). Systematic literature review on security access control policies and techniques based on privacy requirements in a BYOD environment: State of the art and future directions. *Applied Sciences, 13*(14), Article 8048. https://doi.org/10.3390/app13148048

Beltempo, E., Karvonen, J., & Rajamaki, J. (2022). ECHO CyberSkills Framework as a Cyber-Skills Education and Training Tool in Health and Medical Tourism. *Proceedings of the 21st European Conference on Cyber Warfare and Security, 21*(1), 434–437. https://doi.org/10.34190/eccws.21.1.274

Chowdhury, N., & Gkioulos, V. (2023). A personalized learning theory-based cyber-security training exercise. *International Journal of Information Security*, *22,* 1531–1546. https://doi.org/10.1007/s10207-023-00704-z

Coker, T. E. (2021). *What human factors are associated with the adoption of BYOD in an organization?* [Preprint]. https://doi.org/10.31234/osf.io/ey4qm

Dash, B., & Ansari, M. F. (2022). An effective cybersecurity awareness training model: First defense of an organisational security strategy. *International Research Journal of Engineering and Technology* (IRJET), *9*(4), 1–6. https://www.irjet.net/archives/V9/i4/IRJET-V9I401.pdf

Downer, K., & Bhattacharya, M. (2022). BYOD security: A study of human dimensions. *Informatics, 9*(1), Article 16. https://doi.org/10.3390/informatics9010016

Farid, G., Warraich, N. F., & Iftikhar, S. (2023). Digital information security management policy in academic libraries: A systematic review (2010-2022). *Journal of Information Science*. https://doi.org/10.1177/01655515231160026

Freund, L., Al-Majeed, S., & Millard, A. (2021). Towards the definition of a strategic complexity management framework for complex industrial systems. *Proceeding of the 16th International Conference of System of Systems Engineering,* pp. 210–215. IEEE. https://doi.org/10.1109/SOSE52739.2021.9497491

Hao, X., Xiao, Y., Wu, Y., Zhang, Q., & Atkin, G. E. (2021). Low complexity suboptimal constellation design for multi-user multiple access. *Proceeding of the 2020 IEEE International Conference on Electro Information Technology,* pp. 259–264. IEEE. https://doi.org/10.1109/EIT48999.2020.9208302

Kholoanyane, M. E. (2020). *Security awareness and training policy guidelines to minimize the risks of BYOD in a South African SME* [Thesis, Northwest University]. http://hdl.handle.net/10394/36906

Kuechler, B., & Vaishnavi, V. (2011). On theory development in design science research: anatomy of a research project. *European Journal of Information Systems, 17*(5), 489–504. https://doi.org/10.1057/ejis.2008.40

Liao, X., Wu, D., Zhang, Q., & Han, G. (2021). How to improve users' loyalty to smart health devices? The perspective of compatibility. *Sustainability, 13*(19), Article 10722. https://doi.org/10.3390/su131910722

Mahat, N. B., & Ali, N. B. (2018). Empowering employees through BYOD: Benefits and challenges in Malaysian public sector. *International Journal of Engineering & Technology, 7*(4.35), 643–649. https://doi.org/10.14419/ijet.v7i4.35.23077

Neves, U. M., & de Mello, F. L. (2018). BYOD with security. *ENIGMA – Journal of Information Security and Cryptography, 5*(1), 40–47. https://doi.org/10.17648/jisc.v5i1.70

Omboga, S. O., Mukisa, M. T., & Cyprian, R. M. (2021). A bring your own device risk assessment model *International Journal of Security, 12*(2), 15–34. https://www.cscjournals.org/manuscript/Journals/IJS/Volume12/Issue2/IJS-158.pdf

Pypenko, I. S. (2019). Digital product: The essence of the concept and scopes. *International Journal of Education and Science, 2*(4), 56. https://doi.org/10.26697/ijes.2019.4.41

Pypenko, I. S., & Melnyk, Yu. B. (2021). Principles of digitalisation of the state economy. *International Journal of Education and Science, 4*(1), 42–50. https://doi.org/10.26697/ijes.2021.1.5

Schober, P., Boer, C., & Schwarte, L. A. (2018). Correlation coefficients: Appropriate use and interpretation. *Anesthesia & Analgesia, 126*(5), 1763–1768. https://doi.org/10.1213/ANE.0000000000002864

Talaat, F. M., & Gamel, S. A. (2023). Predicting the impact of no. of authors on no. of citations of research publications based on neural networks. *Journal of Ambient Intelligence and Humanized Computing, 14*, 8499–8508. https://doi.org/10.1007/s12652-022-03882-1

Ujakpa, M. M., Heukelman, D., Mutasa, L., & Rodríguez-Puente, R. (2019). Perceived use of mobile devices at the workplace and its perceived effect on performance. *Proceeding of the 2019 Global Trends in Management, IT and Governance in an e-World* (pp. 195–198).

Vom Broke, J., Hevner, A., & Maedche, A. (2020). Introduction to design science research. In vom Brocke, J., Hevner, A., Maedche, A. (Eds.), *Design Science Research. Cases. Progress in IS* (pp. 1–13). Springer. https://doi.org/10.1007/978-3-030-46781-4_1

Wani, T. A., Mendoza, A., Smolenaers, F., & Gray, K. (2021). Bring-Your-Own-Device usage trends in Australian hospitals – A national survey. In M. Merolli, Ch. Bain, & L. K. Schaper (Eds.), *Studies in Health Technology and Informatics, Vol. 276: Healthier Lives, Digitally Enabled* (pp. 1–6). https://doi.org/10.3233/SHTI210002

Xionga, O. L, Nasric, F., Leanna, M. W. Luic, L. M. W, Gillc, H., Phanc, L., Chen-Lic, D., Iacobuccic, M., Ho, R., Majeedc, A., & McIntyre, R. S. (2020). Impact of COVID-19 pandemic on mental health in the general population: A systematic review. *Journal of Affective Disorders, 277,* 55–64. https://doi.org/10.1016/j.jad.2020.08.001

Yin, R. K. (2014). *Case study research design and methods* (5th ed.). SAGE. https://search.worldcat.org/title/Case-study-research-:-design-and-methods/oclc/835951262

Cite this article as:
Moeketsi, C. B., Adeyelure, T. S., & Segooa, M. A. (2024). An information security assessment model for bring your own device in the South African healthcare sector. *International Journal of Science Annals, 7*(2), 57–66. https://doi.org/10.26697/ijsa.2024.2.1