Journal of Positive School Psychology
2022, Vol. 6, No. 10, 2448-2459 http://journalppw.com

Information Technology Risks Associated With Employee Non-Compliance With The Organizational "Bring-Your-Own-Device" Policy

C Kreeft[1*], K K Govender[2]

*[1]*Regensys Business School*

[2]*University of KwaZulu-Natal*

***Corresponding Author: C Kreeft**

Abstract
Bring Your Own Device (BYOD) practices which allow employees to use their personal mobile devices for work purposes from anywhere and at any time, are fraught with cyber security risks and small and medium enterprises (SMEs) are most at risk due to the lack of resources and knowledge on how to mitigate these security risks and threats. This study aimed to determine if the sampled SMEs in South Africa have a BYOD policy, their level of awareness of the security risks associated with not having a BYOD policy, and non-compliance with a BYOD policy, where such policy existed. An on-line study was conducted using two separate questionnaires to survey 27 SME owner-managers and 94 of their employees, who were selected through stratified random sampling.

It was ascertained that a high level of awareness of security risks and threats existed amongst the sampled SME management and employees. No identifiable relationship could be found between the level of security risk awareness and BYOD policy non-compliance behaviour exhibited by management and the employees.

The vast majority of the management representatives indicated that they did not have a BYOD policy. The absence of such a policy or effective implementation thereof where such existed, leaves organizations open to IT security risks and threats that could highly impact the organization's future. Further research is recommended to establish why organizations which are fully aware of BYOD security risks and threats, delay implementation of the BYOD policy.

Keywords: Covid-19; Information Technology; SMEs; cybersecurity risks

INTRODUCTION

The popularity of the Internet of Things (IoT), an increase in wireless bandwidth, and hybrid working models necessitated by the Covid-19 pandemic have seen a significant rise in Bring Your Own Device (BYOD) practices amongst organizations in South Africa. BYOD is a practice where an organization allows its employees to use their own mobile devices for work-related purposes, since personal and workplace integration of mobile devices is convenient, increases productivity, offers greater flexibility, and contributes to job satisfaction (Annansingh, 2021:1). However, significant security risk is associated with allowing mobile devices onto organizational network platforms, which includes malware, viruses, knowledge leakage, cybers attacks, information security fatigue, and naïf acts. "When organization-critical and sensitive data is downloaded to personal devices, it can leave the organization and may be accessible to anyone" (Annansingh, 2021:1). Safeguarding the organization and maintaining information security has become an information technology management (IT) challenge, and often, "small and medium enterprises are the ones most affected, as they lack the resources and knowledge to mitigate the challenges" (Annansingh, 2021:1). BYOD policies allow an organization to mitigate security risks by implementing strategic IT management strategies such as controlling access rights, personal devices, data storage, and apps.

The Covid-19 pandemic has triggered an increase in the adoption of hybrid working models and a combination of hybrid working, internet-ready cloud, and mobile technology advancements find employees more readily using their personal devices to perform organizational tasks. According to Ali, Dominic, Ali, Rehman, and Sohail (2021:1), few studies focus on actual compliance behaviour, and therefore, there is a need to explore actual compliance with policies, rather than the intention to comply.

Adclick Africa (2018:16) points out that SMEs are continuously adapting due to the decentralisation of technology services and SMEs view BYOD practices as cost-saving measures, and employees are free to use their preferred mobile devices, operating systems, and hardware (Rose, 2013:65). Security management of a wide range of mobile devices, variations in operating systems, data allocation, network accessibility, and access to corporate data is but a few management problems experienced when implementing BYOD practices (Rose, 2013:65). Silva, de Gusmão, Poleto, e'Silva and Costa (2014:733) assert that "Information is considered to be the primary assets of an organization, and as such, it needs to be protected against constant security risks such as information security leaks and abuses.'

It is against the above background that this study will investigate the reasons for organizational non-compliance as well as the level of organizational understanding of the security risks associated with non-compliance with the BYOD policies and procedures of an organization. The objectives of the study were to explore the reasons for non-compliance with BYOD policy within SMEs; analyse the awareness of security risks associated with BYOD practices within SMEs, assess the potential impact of non-compliance with BYOD policy on SMEs and to analyse the relationship between security risk awareness and BYOD policy non-compliance behaviour.

LITERATURE REVIEW

Staff accessing their organization's data without authorisation, downloading unsafe applications, and lost and stolen devices form part of the primary barriers to BYOD adoption (Chen et al., 2021: 771). Chen et al. (2021: 771) cite Vorakulpipat, Sirapaisan, Rattanalerdnusorn and Savangsuk (2017), who state that researchers have identified an apparent conflict amongst employees concerning the adoption of BYOD practices and work-life conflict is the most identifiable conflict between organizational security demands and personal user habits.

Downer and Bhattacharya (2016:1) confirm that although organizations are becoming aware of the risks associated with implementing BYOD, in comparison with IT security concerns, BYOD concerns are still underrated. Staff experience conflict within the workplace when they decide to adopt BYOD practices since this decision results in a trade-off between personal use habits, ownership, and rights as set against organizational security demands (Chen et al., 2021: 771).

Kholoanyane (2020:13) explains BYOD technology as presenting a solution for SMEs which saves costs and alleviates budget constraints. Organizations permitting employees to use their own mobile devices save a daily an average of 58 minutes per personal device user, thus increasing productivity by 38% (N-able, 2021). Lowry and Moody (2015:433) believe that organizations are at risk due to an increased reliance on information and its' related systems. Employee actions, as they move between corporate and their personal devices, introduce risk that needs careful management and mitigation (N-able, 2021). Lowry and Moody (2015:433) believe that employees pose the greatest threat to information in an organization because they are a common source of information security breaches.

Sing (2012:2) explains that BYOD is not a simple practice since it places information security at risk, since implementing BYOD diminishes the hardware and asset costs but increases information technology expenditure. Noluvuyo et al. (2016:1) advise that due to the consequences of threats, the security of information should receive preference and SMEs should strongly consider the importance of BYOD policy compliance.

ORGANIZATIONAL AWARENESS AND POLICIES

Implementing corporate policies can contribute towards building and maintaining BYOD awareness. However, managing numerous employee devices, customer networks, and policy implementation has become a complex task (N-able, 2021). Lowry and Moody (2015:433) confirm that the lack of information security policy (ISP) compliance is a common organizational issue. ISPs are partially effective as employees often bypass and disregard information security policies (Lowry and Moody, 2015:433). These researchers believe that strict information security policies need to be implemented to curb employee information misuse.

Although BYOD devices hold benefits for the organization and the stakeholders since employees have immediate access to personal applications and services due to the merger of personal and organizational devices (Noluvuyo et al., 2016:2), BYOD is a complex policy inclusive of potential issues and drawbacks. Organizational information security can become compromised when dealing with unknown applications and services accessing the network. A clear, well-structured BYOD policy will assist an organization in establishing an organizational device usage framework, which will steer the organization towards implementing acceptable procedures in support of BYOD adoption.

INFORMATION AND COMMUNICATION TECHNOLOGY IN SMES

Adclick Africa's (2018:4) research focuses on the underreported reality of SMEs which constantly adapt alongside the ever-changing technological landscape, and the decentralisation of technological services has enabled SMEs to access new markets, reduce business costs, and increase efficiency. DeShield (2017:1) lists data retrieval, privacy, and legal concerns as key security risk factors and indicates that there are identifiable challenges to the adoption of BYOD by SMEs. Data protection on both organizational, employee, and third-party mobile devices, legal and privacy compliance, security measures, and employee uptake of a BYOD policy are viewed as part of these security concerns.

SECURITY RISKS ASSOCIATED WITH BYOD PRACTICES

Van Niekerk (2017:115) states that the South African online privacy and security legislation has expanded and as such, mitigating organizational security risks requires a BYOD policy inclusive of legislative measures such as those contained in The National Cybersecurity Policy Framework (NCPF) enacted in 2015 and the Protection of Personal Information (POPI) Act of 2013 enacted in 2021. Kholoanyane (2020:14) states that compliance with security and privacy legislation seems to be challenging for SMEs, and any non-compliance will leave organizations at risk.

Sing (2012:1) cites CompTIA and explains security risks as the most significant drawback of implementing BYOD and this researcher identified security threats such as litigation, unauthorised users, leakage of confidential data, and viral infection were identified. "The complexity of IT systems creates operational risks such as unauthorised use, access, disclosure, disruption or changes to the information system, and the outsourcing of IT services also have the potential to increase risks because confidential information is flowing outside the organization" (Institute of Directors in Southern Africa, 2015:32). Downer and Bhattacharya (2016:1) mention that the incorporation of security measures to address BYOD threats and risks is complicated, and security measures need constant adjustment to protect all devices and constant manoeuvring becomes resource-intensive for both the employees and the organization.

DeShield (2017:28) acknowledges that failure to address security risks could cause a gambit of security risks for organizations, since IT is dynamic, fast-paced, and ever-changing in nature. Mobile technology and devices offer a wide variety of options for organizations and employees alike, and IT departments are expected to mitigate security risks associated with BYOD practices. Noluvuyo et al. (2016:2) list BYOD risks as data leakage, hacking, and device theft, and small organizations are more susceptible to the risks accompanying BYOD practices.

Both SMEs and large organizations are exposed to BYOD security risks (Kholoanyane (2020:15), and changing non-compliant behaviour will be beneficial to the organization. Biscoe (2018) identifies the motives behind the decision of staff to not to comply, as there being no apparent reason to comply, compliance cost is high, and the way to compliance is frustrating and obstructive.

Employees accessing organizational data without consent, downloading unsafe applications, and lost and stolen devices form part of primary barriers to BYOD adoption (Chen et al., 2021: 771). These researchers cite Vorakulpipat, Sirapaisan, Rattanalerdnusorn and Savangsuk (2017) as stating that researchers have identified an apparent conflict amongst employees concerning the adoption of BYOD practices. Work-life conflict is the most identifiable conflict seen between organizational security demands and personal usability habits.

BYOD Policy Non-compliance

Risk management is more than an organizational policy document since it should be evident in the day-to-day corporate activities (Institute of Directors in Southern Africa, 2015:26). An initial organizational challenge when choosing to implement a security policy is determining how and where BYOD will be required, which is an initial challenge for organizations (Downer and Bhattacharya's, 2016:1).

In South Africa, reporting cyber-incidents is not yet mandatory and thus hampers in-depth assessments of the composition of threats and their impact (Van Niekerk, 2017:128). Most studies emphasise security risks and challenges associated with BYOD practices being intensified due to non-compliant behaviour with reference to BYOD policy and procedures. There is a common thread in the literature that organizational practices with respect to BYOD increase security concerns amongst Chief Information Officers (CIOs) and information technology managers. DeShield (2017:28) emphasises that non-compliance behaviour relating to BYOD, such as the lack of a comprehensive implementation strategy, will further increase organizational security risks. This researcher emphasized that access to an organization's resources using personal mobile devices constitutes a definite security risk and that BYOD practices should be integrated within all organizational policies.

Since BYOD practices are unique to each organization, country, region, and industry, additional academic knowledge is required to gain a better understanding of South African SME's in terms of their IT risk awareness associated with BYOD policy non-compliance behaviour. Research needs to be undertaken to understand better the reasons for non-compliance with BYOD policy implementation and the incidence of levels of non-compliance amongst SMEs in South Africa. Thus, this study was conducted among a sample of SMEs in South Africa to address the aforementioned issues, following the methodology discussed next.

RESEARCH METHODOLOGY

The research problem was addressed through descriptive research and probability sampling, more specifically, stratified random sampling, was used to ensure non-bias. The different strata were selected by identifying diverse managerial occupations and employees participating in BYOD practices. The first sample comprised 27 companies across various SME sectors and the survey targeted either the manager/director or owner. The second group surveyed comprised employees from the same 27 organizations, who used their mobile devices for work purposes and those who used the company Wi-Fi and network infrastructure for private purposes.

The quantitative research approach was best-suited to address the research objectives. The organizational gatekeepers granted research permission and identified the staff members within the organization who could be surveyed. Two questionnaires were developed and the first targeted managerial level employees and owner-managers, and the second focused on the organizational employees.

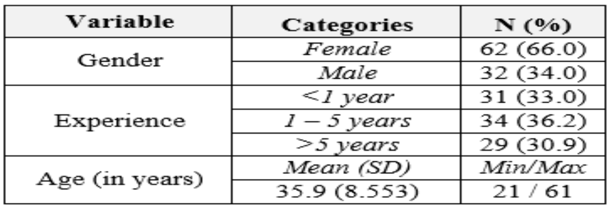
Cochran's sample size formula/calculator was used to calculate the number of employees needed to complete the survey from each organization (Glen, 2021). By focusing on the 27 businesses, a randomly selected group of employees were requested via e-mail, to participate in the survey and direct to the questionnaire link housed in Google Forms. For tracking and data allocation, email addresses were logged against the organizations, differentiating management from employees through survey responses.

The questionnaire used Likert-type and semantic differential scales to gauge the participant's attitude towards and awareness of BYOD security risks and policy implementation. Descriptive and inferential statistical analysis was conducted.

Internal validity was achieved through actively addressing any confounding variables within the research instrument. External validity was achieved by using Cochran's formula to determine the sample size since studying the entire population is impossible, and therefore a subset was studied (Stumpfegger, 2017). Reliability was addressed by calculating the Cronbach's alpha.

FINDINGS

Table 1 reflects that 66% of the employee respondents were female and 34% male. The respondents' ages varied between 21 and 61 years of age, with the mean age being 36 years.



Variable	Categories	N (%)
Gender	*Female*	62 (66.0)
	Male	32 (34.0)
Experience	*<1 year*	31 (33.0)
	1 – 5 years	34 (36.2)
	>5 years	29 (30.9)
Age (in years)	*Mean (SD)*	*Min/Max*
	35.9 (8.553)	21 / 61

Table 1: Employee Respondents' Demographic Data

The demographics of the owner-manager respondents is depicted in Figure 1.

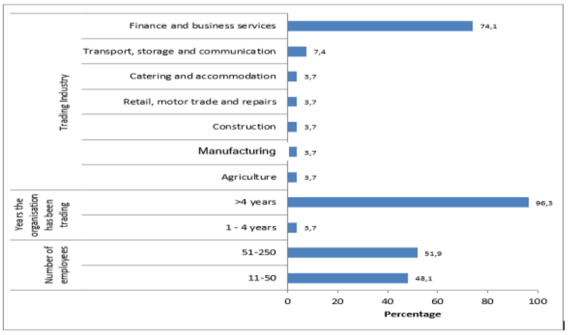
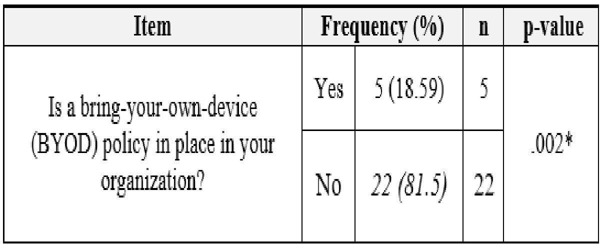


Figure 1: Organizational characteristics

Figure 1 reveals that 48% of the SMEs had between 11–15 employees, and 52% of organizations had between 51–250 employees. One organization has been trading for less than a year, whereas the remaining 26 have been trading for more than four years. The vast majority (74%) of the responders represented the finance and business services industry.

BYOD policy

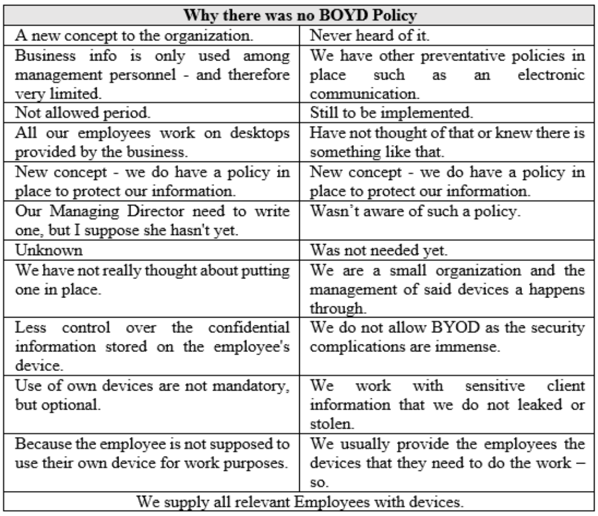
Table 2 represents the feedback from the managerial respondents regarding the availability of a BYOD policy in their organizations. The binomial test result indicates that a significant (81.5%) of respondents indicated that there is no BYOD policy in their organizations.



Item	Frequency (%)		n	p-value
Is a bring-your-own-device (BYOD) policy in place in your organization?	Yes	5 (18.59)	5	.002*
	No	*22 (81.5)*	22	

Table 2: Existence of a BYOD policy in the organization

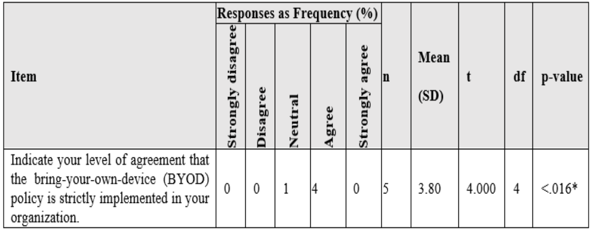
By using an open-ended question, the respondents were asked why there is no BYOD policy in the organization, and their responses are captured in Table 3.



Why there was no BOYD Policy	
A new concept to the organization.	Never heard of it.
Business info is only used among management personnel - and therefore very limited.	We have other preventative policies in place such as an electronic communication.
Not allowed period.	Still to be implemented.
All our employees work on desktops provided by the business.	Have not thought of that or knew there is something like that.
New concept - we do have a policy in place to protect our information.	New concept - we do have a policy in place to protect our information.
Our Managing Director need to write one, but I suppose she hasn't yet.	Wasn't aware of such a policy.
Unknown	Was not needed yet.
We have not really thought about putting one in place.	We are a small organization and the management of said devices a happens through.
Less control over the confidential information stored on the employee's device.	We do not allow BYOD as the security complications are immense.
Use of own devices are not mandatory, but optional.	We work with sensitive client information that we do not leaked or stolen.
Because the employee is not supposed to use their own device for work purposes.	We usually provide the employees the devices that they need to do the work – so.
We supply all relevant Employees with devices.	

Table 3: Reasons for not having a BYOD Policy

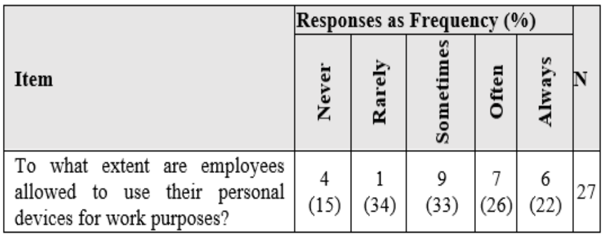
Table 4 summarises the respondents' level of agreement regarding the implementation of the organizational BYOD policy and the one-sample t-test results indicate that, where BYOD policies are in place, these are strictly implemented.



Item	Responses as Frequency (%)					n	Mean (SD)	t	df	p-value
	Strongly disagree	Disagree	Neutral	Agree	Strongly agree					
Indicate your level of agreement that the bring-your-own-device (BYOD) policy is strictly implemented in your organization.	0	0	1	4	0	5	3.80	4.000	4	<.016*

Table 4: Implementation of the BYOD policy

The observable frequencies reflected in Table 5 show that only a minority (15%) of organizations do not allow employees to use their personal devices for work purposes, implying that the majority do allow the employees to do so.



Item	Responses as Frequency (%)					N
	Never	Rarely	Sometimes	Often	Always	
To what extent are employees allowed to use their personal devices for work purposes?	4 (15)	1 (34)	9 (33)	7 (26)	6 (22)	27

Table 5: Use personal devices for work purposes

Owner and managerial respondents representing the organizations were asked to rate their level of agreement as to why they do not have a BYOD policy or strictly implement a BYOD policy in their organizations where such a policy existed. Figure 2 depicts the responses which clarify why they do not have a BYOD policy or strictly implement such a BYOD policy within their organization.

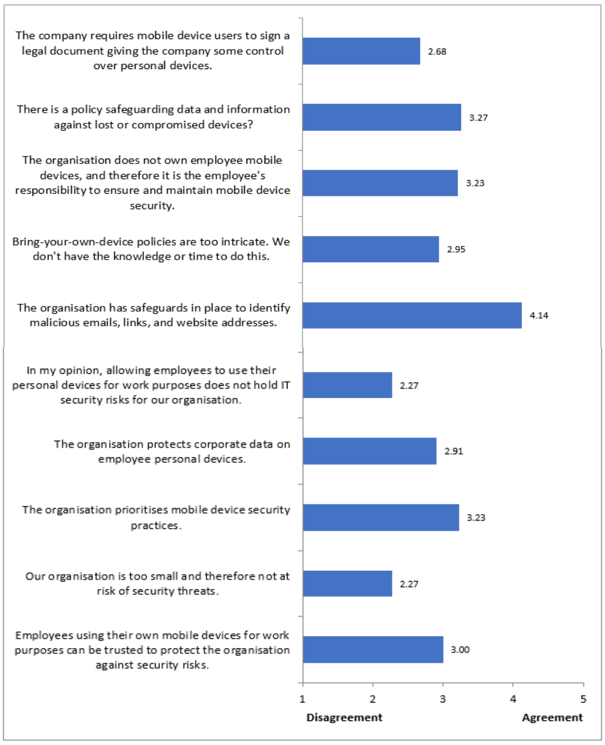


Figure 2: Reasons why organizations do not have a BYOD policy or strictly implement the policy

Table 6 reflects further responses with respect to non-existence or non-compliance with a BYOD policy at an organizational level.

Item	Responses as Frequency (%)					N	Mean (SD)	t	df	p-value
	Strongly disagree	Disagree	Neutral	Agree	Strongly agree					
Employees using their own mobile devices for work purposes can be trusted to protect the organization against security risks.	3 (14)	5 (23)	6 (27)	5 (23)	3 (14)	22	3.00	.000	21	1.000
Our organization is too small and therefore not at risk of security threats.	8 (36)	6 (27)	3 (14)	4 (18)	1 (5)	22	2.27	-2.667	21	<.014*
The organization prioritises mobile device security practices.	1 (5)	6 (27)	3 (14)	11 (50)	1 (5)	22	3.23	1.000	21	.329
The organization protects corporate data on employee personal devices.	4 (18)	5 (23)	5 (23)	5 (23)	3 (14)	22	2.91	-.318	21	.754
In my opinion, allowing employees to use their personal devices for work purposes does not hold IT security risks for our organization.	9 (41)	2 (9)	8 (36)	2 (9)	1 (5)	22	2.27	-2.748	21	<.012*
The organization has safeguards in place to identify malicious emails, links, and website addresses.	0	0	2 (9)	15 (68)	5 (23)	22	4.14	9.514	21	<.001*
Bring-your-own-device policies are too intricate. We don't have the knowledge or time to do this.	2 (9)	5 (23)	7 (32)	8 (36)	0	22	2.95	-.213	21	.833
The organization does not own employee mobile devices, and therefore it is the employee's responsibility to ensure and maintain mobile device security.	1 (5)	6 (27)	5 (23)	7 (32)	3 (14)	22	3.23	.925	21	.365
There is a policy safeguarding data and information against lost or compromised devices?	0	7 (32)	6 (27)	5 (23)	4 (18)	22	3.27	.266	21	.266
The company requires mobile device users to sign a legal document giving the company some control over personal devices.	3 (14)	9 (41)	4 (18)	4 (18)	2 (9)	22	2.68	.231	21	.231

Table 6: Reasons for non-compliance with or non-existence of a BYOD Policy

Employee security risk awareness

Table 7 reflects the binomial test results of the feedback from the employees regarding the availability of a BYOD policy within their organizations.

Item	Frequency (%)		n	p-value
	Yes	No		
Is a bring-your-own-device (BYOD) policy in place in your organization?	30 (31.9)	*64 (68.1)*	94	<.001*

Table 7: Availability of a BYOD policy in the organization

A one-sample t-test was used to analyse the respondents' level of agreement with that statement ‘’the existing BYOD policy is strictly implemented within their organization”. This is captured in Table 8 below.

Item	Responses as Frequency (%)					n	Mean (SD)	t	df	p-value
	Strongly disagree	Disagree	Neutral	Agree	Strongly agree					
Indicate your level of agreement that the bring-your-own-device (BYOD) policy is strictly implemented in your organization.	-	-	13 (13.8)	10 (10.6)	7 (7.4)	30	3.80 (0.805)	5.442	29	<.001*

Table 8: Implementation of BYOD policy by employees

The one-sample t-test result indicates significant (95% level) agreement by the employees that where BYOD policies are in place, these are strictly implemented.

All employee respondents were asked to indicate the extent to which they are allowed to use their personal devices for work purposes and the results are captured in Table 9.

Item	Responses as Frequency (%)					n	Mean (SD)	t	df	p-value
	Never	Rarely	Sometimes	Often	Always					
To what extent are you allowed to use your personal devices for work purposes?	2 (2.1)	7 (7.4)	30 (31.9)	16 (17)	39 (41.5)	94	3.88	7.742	93	<.001*

Table 9: Flexibility allowed to employees to use their personal devices for work purposes

Figure 3 depicts the personal mobile technologies respondents used for work purposes.

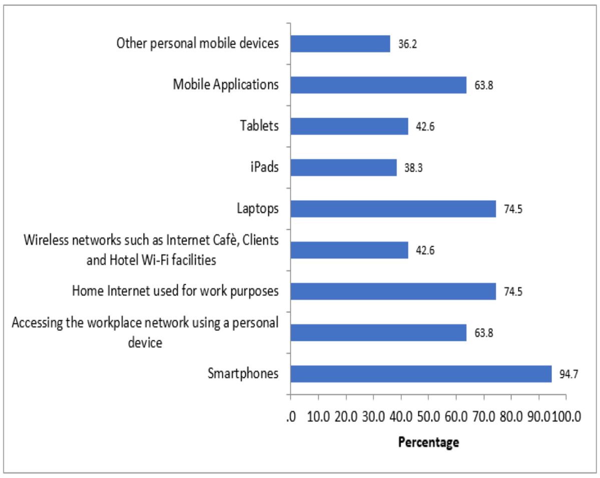


Figure 3: Types of personal mobile technologies used for work purposes

Table 10 which reports the security risk behaviour linked to personal mobile device practices reveals that 59% of the respondents indicated that they never use their personal laptops or desktops for work purposes. Respondents seemed to be most aware of the risks associated with allowing someone else to use their personal devices for work, without supervision and the vast majority (83%) of the respondents stated that they never allow such behaviour.

Item	Responses as Frequency (%)					n	Mean (SD)	t	df	p-value
	Never	Rarely	Sometimes	Often	Always					
Indicate how often you use your personal laptop or desktop for work purposes, even when you are not supposed to.	55 (59)	7 (7)	17 (18)	5 (5)	10 (11)	94	2.02	-6.784	93	<.001*
Indicate how often you use your personal smartphone or tablet for work purposes, even when you are not supposed to.	14 (15)	14 (15)	21 (22)	20 (21)	25 (27)	94	3.30	2.066	93	<.042*
Indicate how often you allow someone else to use your personal device that you use at work without supervision.	78 (83)	11 (12)	3 (3)	1 (1)	1 (1)	94	1.26	-25.209	93	<.001*

Table 10: Security risk behaviour associated with use of personal mobile devices

Organization's security risk awareness

Table 11 reflects of the owner-managers with respect to their awareness of the security risks associated with BYOD practices in the workplace.

Item	Responses as Frequency (%)					n	Mean (SD)	t	df	p-value
	Not at all aware	Slightly aware	Moderately aware	Very aware	Extremely aware					
Device Theft	0	1 (4)	2 (7)	12 (44)	12 (44)	27	4.30	8.688	26	<.001*
Data Loss and Leakage	1 (4)	0	3 (11)	11 (41)	12 (44)	27	4.22	6.802	26	<.001*
Breaching of Company rules	1 (4)	0	4 (15)	13 (48)	9 (33)	27	4.07	6.088	26	<.001*
Hacking	1 (4)	0	0	13 (48)	13 (48)	27	4.37	8.488	26	<.001*
Introduction of malicious software (e.g., viruses)	1 (4)	0	3 (11)	12 (44)	11 (41)	27	4.19	6.684	26	<.001*
Unauthorised Network Access	1 (4)	2 (7)	3 (11)	11 (41)	10 (37)	27	4.00	4.837	26	<.001*
The undermining of Critical Business Obligations	1 (4)	0	5 (19)	8 (30)	13 (48)	27	4.19	6.150	26	<.001*
Intellectual Property Leak	1 (4)	0	3 (11)	10 (37)	13 (48)	27	4.26	6.929	26	<.001*
Phishing	1 (4)	0	4 (15)	10 (37)	12 (44)	27	4.19	6.400	26	<.001*

Table 11: Management's feedback regarding security risks associated with BYOD practices

From the results in Table 11, it may be surmised that an overwhelming conflated response indicates that >80% of the owner-managers are aware of data theft, data loss, and leakage, the breaching of company rules, followed by hacking.

Factor analysis with promax rotation was applied to the eight security risk awareness items contained in Table 11 to determine the structure of the data. A Kaiser-Meyer-Olkin measure of sampling adequacy (KMO) value of .814 and a significant Bartlett's test (p<.05) indicates that the data was adequate for successful and reliable factor extraction. One factor was extracted, which accounts for 72.86% of the variance in the data. The factor loadings are summarised in Table 12.

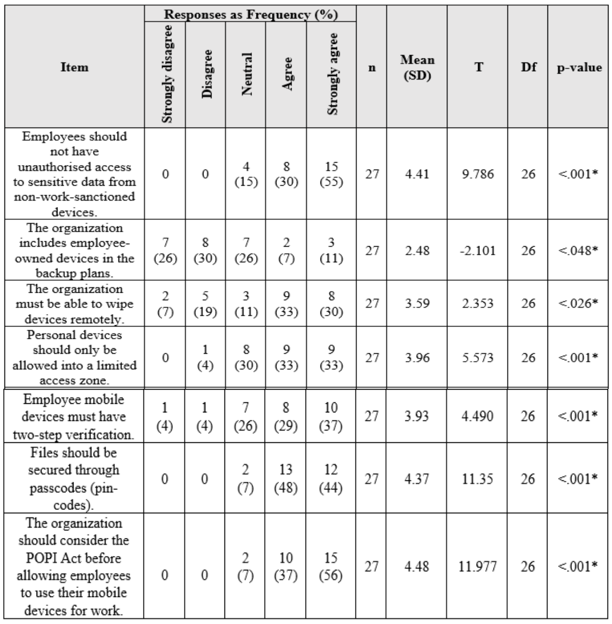
Factor Loadings	Factor
	1
Breaching of Company rules	.936
Introduction of malicious software (i.e. viruses)	.930
Phishing	.926
Intellectual Property Leak	.900
Hacking	.857
The undermining of Critical Business Obligations	.843
Device Theft	.792
Data Loss and Leakage	.791
Unauthorised Network Access	.671

Table 12: Factor loadings – security risk awareness associated with BYOD practices

A composite measure is formed by calculating the average of the agreement scores for the items included in the factor. The Cronbach's alpha score for this composite measure is .957, which indicates reliability was attained.

The results from a one-sample t-test show that with respect to the management, there is significant awareness of security risks associated with BYOD practices, M=4.20, p <.001.

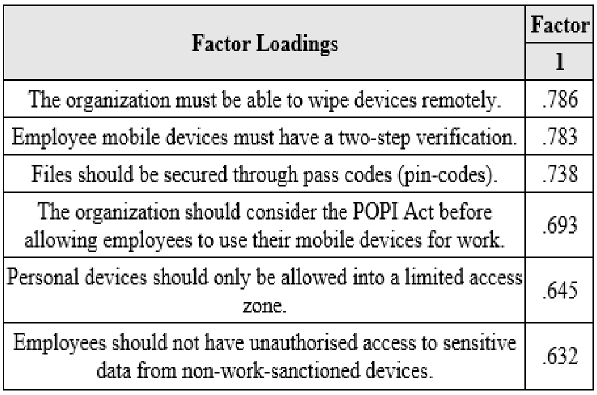
Organizational respondents, as represented by the owner or management, were provided with seven statements focused on security risks associated with BYOD practices. Table 13 contains the data analysed using the one-sample t-test, which represents a summary of the owner and managerial respondent's level of agreement regarding security threats associated with BYOD practices.



Item	Responses as Frequency (%)					n	Mean (SD)	T	Df	p-value
	Strongly disagree	Disagree	Neutral	Agree	Strongly agree					
Employees should not have unauthorised access to sensitive data from non-work-sanctioned devices.	0	0	4 (15)	8 (30)	15 (55)	27	4.41	9.786	26	<.001*
The organization includes employee-owned devices in the backup plans.	7 (26)	8 (30)	7 (26)	2 (7)	3 (11)	27	2.48	-2.101	26	<.048*
The organization must be able to wipe devices remotely.	2 (7)	5 (19)	3 (11)	9 (33)	8 (30)	27	3.59	2.353	26	<.026*
Personal devices should only be allowed into a limited access zone.	0	1 (4)	8 (30)	9 (33)	9 (33)	27	3.96	5.573	26	<.001*
Employee mobile devices must have two-step verification.	1 (4)	1 (4)	7 (26)	8 (29)	10 (37)	27	3.93	4.490	26	<.001*
Files should be secured through passcodes (pin-codes).	0	0	2 (7)	13 (48)	12 (44)	27	4.37	11.35	26	<.001*
The organization should consider the POPI Act before allowing employees to use their mobile devices for work.	0	0	2 (7)	10 (37)	15 (56)	27	4.48	11.977	26	<.001*

Table 13: Security threats associated with BYOD practices

Factor analysis with promax rotation was applied to the seven items contained in Table 13 to determine the structure of the data. A Kaiser-Meyer-Olkin measure of sampling adequacy (KMO) value of .813 and a significant Bartlett's test (p<.05) indicates that the data was adequate for successful and reliable factor extraction. One factor was extracted, which accounts for 51.21% of the variance in the data. The factor loadings are summarised in Table 14.



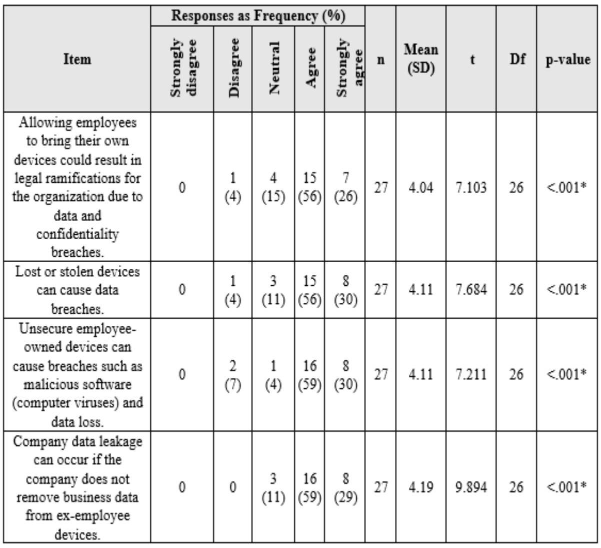
Factor Loadings	Factor
	1
The organization must be able to wipe devices remotely.	.786
Employee mobile devices must have a two-step verification.	.783
Files should be secured through pass codes (pin-codes).	.738
The organization should consider the POPI Act before allowing employees to use their mobile devices for work.	.693
Personal devices should only be allowed into a limited access zone.	.645
Employees should not have unauthorised access to sensitive data from non-work-sanctioned devices.	.632

Table 14: Factor loadings – security threats associated with BYOD practices

A composite measure is formed by calculating the average of the agreement scores for the items included in the factor. The Cronbach's alpha score for this composite measure is .844, which indicates reliability is attained. The results from a one-sample t-test show that there is significant agreement that specific security measures need to be practiced, M=4.12, p <.001.

Impact on SMEs of non-compliance with BYOD policy

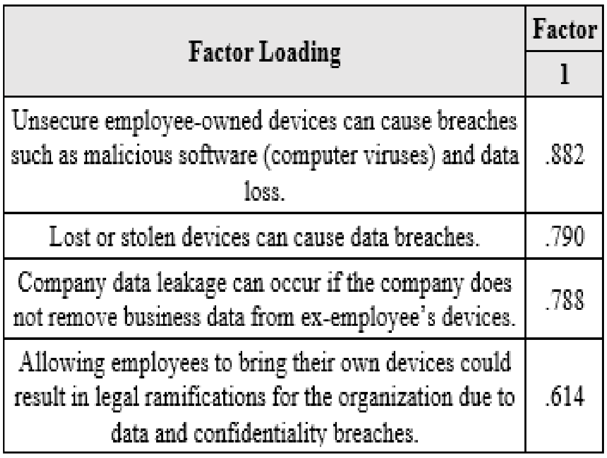
Table 15 contains the organizational owner and managerial respondents' feedback regarding the perceived potential impact on the organization of non-compliance with BYOD policy. The one-sample t-test data analysis revealed overwhelming (82%) agreement among the respondents that allowing employees to bring their own devices could result in legal ramifications for the organization due to data and confidentiality breaches. The vast majority (89%) of the respondents ''agreed'' that unsecure employee-owned devices can cause breaches such as malicious software (computer viruses) and data loss.



Item	Responses as Frequency (%)					n	Mean (SD)	t	Df	p-value
	Strongly disagree	Disagree	Neutral	Agree	Strongly agree					
Allowing employees to bring their own devices could result in legal ramifications for the organization due to data and confidentiality breaches.	0	1 (4)	4 (15)	15 (56)	7 (26)	27	4.04	7.103	26	<.001*
Lost or stolen devices can cause data breaches.	0	1 (4)	3 (11)	15 (56)	8 (30)	27	4.11	7.684	26	<.001*
Unsecure employee-owned devices can cause breaches such as malicious software (computer viruses) and data loss.	0	2 (7)	1 (4)	16 (59)	8 (30)	27	4.11	7.211	26	<.001*
Company data leakage can occur if the company does not remove business data from ex-employee devices.	0	0	3 (11)	16 (59)	8 (29)	27	4.19	9.894	26	<.001*

Table16: The potential impact of non-compliance on the organization

Factor analysis with promax rotation was applied to the four items contained in Table 15 to determine the structure of the data. A Kaiser-Meyer-Olkin measure of sampling adequacy (KMO) value of .644 and a significant Bartlett's test (p<.05) indicates that the data was adequate for successful and reliable factor extraction. One factor was extracted, which accounts for 60.02% of the variance in the data. The factor loadings are summarised in Table 16.

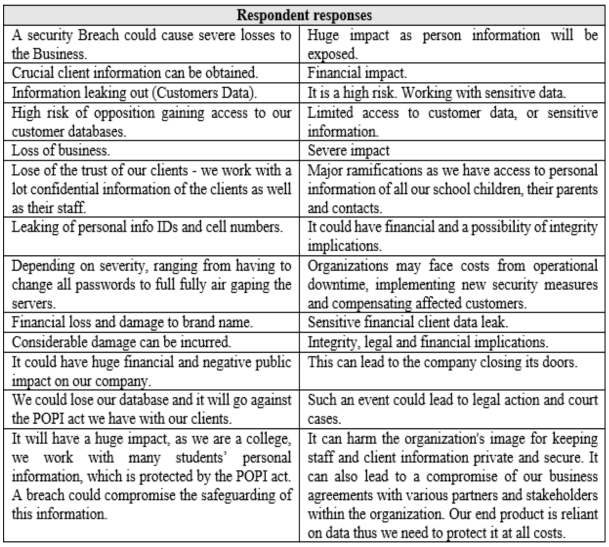


Factor Loading	Factor 1
Unsecure employee-owned devices can cause breaches such as malicious software (computer viruses) and data loss.	.882
Lost or stolen devices can cause data breaches.	.790
Company data leakage can occur if the company does not remove business data from ex-employee's devices.	.788
Allowing employees to bring their own devices could result in legal ramifications for the organization due to data and confidentiality breaches.	.614

Table16: Factor loadings – perceived potential impact

A composite measure is formed by calculating the average of the agreement scores for the items included in the factor. The Cronbach's alpha score for this composite measure is .847, which indicates reliability is attained. The results from a one-sample t-test show that there is significant agreement that they perceive there to be a potential impact of non-compliance on the organization associated with BYOD practices, M=4.11, p <.001.

Using an open-ended question, the organizational respondents, represented by the owner or management, were requested to indicate the impact of a security breach on the organization and the responses are captured in Table 17.

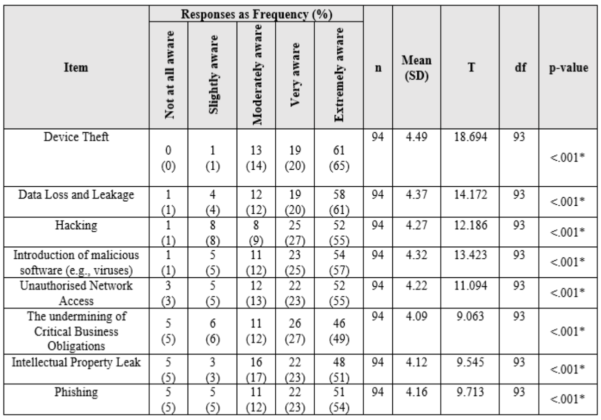


Respondent responses	
A security Breach could cause severe losses to the Business.	Huge impact as person information will be exposed.
Crucial client information can be obtained.	Financial impact.
Information leaking out (Customers Data).	It is a high risk. Working with sensitive data.
High risk of opposition gaining access to our customer databases.	Limited access to customer data, or sensitive information.
Loss of business.	Severe impact
Lose of the trust of our clients - we work with a lot confidential information of the clients as well as their staff.	Major ramifications as we have access to personal information of all our school children, their parents and contacts.
Leaking of personal info IDs and cell numbers.	It could have financial and a possibility of integrity implications.
Depending on severity, ranging from having to change all passwords to full fully air gaping the servers.	Organizations may face costs from operational downtime, implementing new security measures and compensating affected customers.
Financial loss and damage to brand name.	Sensitive financial client data leak.
Considerable damage can be incurred.	Integrity, legal and financial implications.
It could have huge financial and negative public impact on our company.	This can lead to the company closing its doors.
We could lose our database and it will go against the POPI act we have with our clients.	Such an event could lead to legal action and court cases.
It will have a huge impact, as we are a college, we work with many students' personal information, which is protected by the POPI act. A breach could compromise the safeguarding of this information.	It can harm the organization's image for keeping staff and client information private and secure. It can also lead to a compromise of our business agreements with various partners and stakeholders within the organization. Our end product is reliant on data thus we need to protect it at all costs.

Table 17: Managements' feedback

Security Risk Awareness and BYOD Policy Non-compliance Behaviour

In summary, it became evident that the overwhelming majority (98%) of the respondents agreed that they understood the importance of maintaining a secure IT network and believed that the IT infrastructure is secure and not at risk. The vast majority (73%) of respondents implemented mobile device and security practices and most (68%) of the respondents agreed that they protect their devices according to the requirements set out by the organization. Table 18 reflects the data with respect to the level of awareness of BYOD security risks.

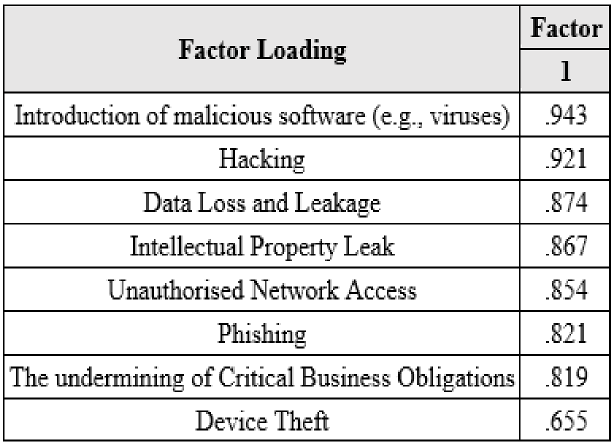


Item	Responses as Frequency (%)					n	Mean (SD)	T	df	p-value
	Not at all aware	Slightly aware	Moderately aware	Very aware	Extremely aware					
Device Theft	0 (0)	1 (1)	13 (14)	19 (20)	61 (65)	94	4.49	18.694	93	<.001*
Data Loss and Leakage	1 (1)	4 (4)	12 (12)	19 (20)	58 (61)	94	4.37	14.172	93	<.001*
Hacking	1 (1)	8 (8)	8 (9)	25 (27)	52 (55)	94	4.27	12.186	93	<.001*
Introduction of malicious software (e.g., viruses)	1 (1)	5 (5)	11 (12)	23 (25)	54 (57)	94	4.32	13.423	93	<.001*
Unauthorised Network Access	3 (3)	5 (5)	12 (13)	22 (23)	52 (55)	94	4.22	11.094	93	<.001*
The undermining of Critical Business Obligations	5 (5)	6 (6)	11 (12)	26 (27)	46 (49)	94	4.09	9.063	93	<.001*
Intellectual Property Leak	5 (5)	3 (3)	16 (17)	22 (23)	48 (51)	94	4.12	9.545	93	<.001*
Phishing	5 (5)	5 (5)	11 (12)	22 (23)	51 (54)	94	4.16	9.713	93	<.001*

Table 18: Level of awareness of BYOD security risks

From Table 18, it may be surmised that the respondents indicated high (extreme) awareness of data theft (65%), data loss and leakage (61%), hacking (55%), the introduction of malicious software (57%), undermining of critical business obligations (49%), intellectual property leakage (51%) and phishing (54%).

Factor analysis with promax rotation was applied to the eight security risk awareness items contained in Table 19 to determine the structure of the data. A Kaiser-Meyer-Olkin measure of sampling adequacy (KMO) value of .878 and a significant Bartlett's test (p<.05) indicates that the data was adequate for successful and reliable factor extraction. One factor was extracted, which accounts for 71.95% of the variance in the data. The factor loadings are summarised in Table 19.



Factor Loading	Factor
	1
Introduction of malicious software (e.g., viruses)	.943
Hacking	.921
Data Loss and Leakage	.874
Intellectual Property Leak	.867
Unauthorised Network Access	.854
Phishing	.821
The undermining of Critical Business Obligations	.819
Device Theft	.655

Table 19: Factor loadings – employee respondents' security risk awareness

A composite measure is formed by calculating the average of the agreement scores for the items included in the factor. The Cronbach's alpha score for this composite measure is .951, which indicates reliability is attained. Results from a one-sample t-test show that there is significant awareness of security risks associated with BYOD practices, M=4.25, p <.001.

DISCUSSION OF KEY FINDINGS

A significant finding is that the overwhelming majority (81.5%) of organizations surveyed do not have a BYOD policy in the workplace. The absence of a policy or effective implementation thereof (if one existed) leaves organizations open to IT security risks and threats. N-able (2021) confirms employee actions as introducing risks, as they move between the corporate and their personal devices, and that this needs careful management and mitigation. The following were reasons identified as to why the organization does not have a BYOD policy:

- This is a new concept, unknown to the organization, and that they have never heard of such a policy, nor have they thought of implementing a BYOD policy.
- A policy is unnecessary because business information is only used amongst management and is therefore limited.
- A BYOD policy is not needed because the use of personal mobile devices is not allowed.
- They have other preventative policies in place, such as an electronic communications policy.
- Since organizations provide the resources employees need, they do not need to use their own personal devices.
- BYOD policies are still to be implemented.
- Employees are not supposed to use their own devices for work purposes.
- The use of personal devices is not mandatory, only optional.

The Institute of Directors in Southern Africa (2015:26) explains risk management as being more than an organizational policy document and should be evident in the day-to-day corporate activities. Thus, even in cases where a BOYD policy exists, management should ensure that it is being implemented.

The literature explains that BYOD is an information technology trend (Downer and Bhattacharya, 2016:1) that allows employees to use laptops, tablets, and smartphones in the workplace. The research confirms that mobile technologies such as smartphones, laptops, and home internet use for work purposes are allowed by the participating organizations. All three of these technologies carry potential IT risks and threats to the organization, more especially since the 'human'' element is involved, since Kholoanyane (2020:23) assert that organizational owners and management sometimes secure their network infrastructure by relying on technology, whilst ignoring human vulnerabilities.

It is unknown if organizations don't understand the real impact of IT security risks and threats, or they select not to currently focus on policy creation and will act reactively when needed, or are too trusting of their employees, or assume that because employees own these devices, they will take the responsibility to ensure and maintain mobile device security, or they might not have thoroughly considered the impact of BYOD policy non-compliance.

A good proportion (68%) of the employee participants responded that there is no BYOD policy in their organization. However, what raises concern is that of those who confirmed the availability of a BYOD policy, almost 50% indicated that the BYOD policy is not strictly implemented.

The majority of employee respondents confirmed that they are allowed, in various degrees, to use their personal devices for work purposes. However, not all respondents seemed to be fully aware of the risks associated with allowing someone to use their personal devices for work without supervision. Sing (2021:1) explains that today's technology-savvy generation is exposed to most technologies, which is confirmed by the data since most respondents indicated being aware of the associated risks. The literature also suggests that staff accessing their organization's data without authorisation, downloading unsafe applications, and lost and stolen devices form part of the primary barriers to BYOD adoption (Chen et al., 2021: 771).

It was ascertained that the vast majority (80%) of the organizational owner and managerial representatives agree that the BYOD policy is strictly enforced in the organization. However, a mismatch is observed when comparing the employee respondents' feedback since only 57% of the employee's reported agreement that the BYOD policy is strictly implemented within their organizations.

Owner and managerial organizational respondents seemed to be extremely aware of the security risks associated with BYOD practices. Organizational awareness was exhibited through the organizational owner and management respondents' feedback confirming organizational awareness of security risks associated with BYOD practices. This confirms Downer and Bhattacharya's (2016:1) finding that recent publications confirm organizations being aware of the risk associated with implementing BYOD.

It became evident that the employee respondents clearly understood what is needed to exhibit BYOD compliance behaviour. Initially, it was considered that BYOD policy non-compliance is due to a lack of knowledge of IT security risks and threats. However, the literature (Biscoe, 2018) identifies the reasons why staff do not comply as there being no apparent reason to comply, compliance cost is high, and compliance is frustrating and obstructive. In this study, there is no identifiable relationship between the level of security risk awareness and BYOD policy non-compliance behaviour. Lowry and Moody (2015:433) believe that employees pose the greatest threat to information in an organization because they are a common source of information security breaches.

CONCLUSION

No identifiable relationship was established between the level of security risk awareness and BYOD policy non-compliance behaviour could be established. From the awareness levels ascertained, it can be deduced that there is a high level of security risk awareness amongst the SME owner-managers. However, being fully aware of IT risks and threats, owners and management still did not implement BYOD policies. This is a reason for great concern. Owners and management should strongly consider establishing an organizational culture of BYOD compliance behaviour through implementing a BYOD policy.

Initially, it was considered that BYOD policy non-compliance is due to a lack of IT security risk and threat knowledge. However, from the findings it could be observed that both the owner and managerial and employee respondents are aware of IT security risks and threats.

There is no identifiable relationship between the level of security risk awareness and BYOD policy non-compliance behaviour. Thus, the question which needs to be answered is if there is an awareness of BYOD behaviour security risks and threats, why do owners and management of organizations delay implementing a BYOD policy?

RECOMMENDATIONS

Although the owners and management of the SMEs as well as their employees, fully understand the risks associated with BYOD behaviour and practices, both groups still exhibit BYOD non-compliance behaviour. Further research is needed to determine the reasons behind thedisconnect between high-level organizational management and employee awareness of IT security risks and threats and electing not to implement BYOD policies. Research is recommended into the owner and managerial level awareness of the importance and purpose of organizational policies. Determining why owners and management of organizations allow these practices without adequate compliance regulations will add much-needed value to the existing body of knowledge.

REFERENCES

[1]. Adclick Africa. 2018, 'An Assessment of South Africa's SME Landscape: Challenges, Opportunities, Risks & Next Steps' Report', 2018/2019 Reports and Surveys, SME South Africa, https://smesouthafrica.co.za/resources/, (assessed 17 September 2021).

[2]. Ali, R.F., Dominic, P.D.D., Ali, S.E.A., Rehman, M., and Sohail, A. 2021, 'Information Security Behaviour and Information Security Policy Compliance: A Systematic Literature Review for Identifying the Transformation Process from Noncompliance to Compliance', Appl. Sci., 11, 3383. https://doi.org/ 10.3390/app11083383.

[3]. Annansingh, F. 2021, 'Bring your own device to work: How serious is the risk?', Journal of Business Strategy, 42 (6), 392-398, https://doi.org/10.1108/JBS-04-2020-0069.

[4]. Chen, H., Li, Y., Chen, L., and Yin, J. 2021, 'Understanding employees' adoption of the Bring-Your-Own-Device (BYOD): the roles of information security-related conflict and fatigue'. Journal of Enterprise Information Management, 34 (3), 770-792, https://doi.org/10.1108/JEIM-10-2019-0318.

[5]. DeShield, L. 2017, 'The Challenges of Implementing Bring Your Own Device', Walden Dissertation and Doctoral Studies, Walden University, College of Management and Technology.

[6]. Downer, K. and Bhattacharya, M. 2016, 'BYOD Security: A New Business Challenge', accepted for publication in Proceedings of the 5th International Symposium on Cloud and Service Computing (SC2 2015), IEEE CS Press, Computer Science, Cryptography and Security, https://arxiv.org/ftp/arxiv/papers/1601/1601.01230.pdf, (accessed 30 September 2021).

[7]. Glen, S. 2021, 'Cronbach's Alpha: Simple Definition, Use and Interpretation', StatisticsHowTo.com, Elementary Statistics for the rest of us! https://www.statisticshowto.com/probability-and-statistics/statistics-definitions/cronbachs-alpha-spss/, (assessed 21 September 2021).

[8]. Institute of Directors in Southern Africa. 2015, 'Governance in SMEs. A guide to the application of corporate governance in small and medium enterprises', [pdf], https://cdn.ymaws.com/www.iodsa.co.za/resource/resmgr/Docs/GovernanceinSMEsGuidelowres.pdf, (accessed 17 October 2021).

[9]. Kholoanyane, M. E. 2020, 'Security awareness and training policy guidelines to minimise the risks of BYOD in a South African SME', Dissertation, Northwest University, https://repository.nwu.ac.za/bitstream/handle/10394/36906/Kholoanyane_ME.pdf?sequence=3&isAllowed=y, (accessed 16 September 2021).

[10]. Lowry, P.B and Moody, G.D. 2015, 'Proposing the control-reactance compliance model (CRCM) to explain opposing motivations to comply with organizational information security policies', Information Systems Journal, 25 (5), 433-463, DOI: 10.1111/isj.12043.

[11]. N-able. 2021, 'The Top 7 Risks of Bring Your Own Device (BYOD) MSPs Should Remember', [blog], Security, https://www.n-able.com/blog/the-top-7-risks-of-bring-your-own-device-msps-should-remember (accessed 16 September 2021).

[12]. Noluvuyo, F., von Solms, R. and Gerber, M. 2016, 'A framework towards governing "Bring Your Own Device in SMMEs"', Conference: 2016 Information Security for South Africa (ISSA), Center for Research in Information and Cyber Security, Nelson Mandela Metropolitan University, DOI:10.1109/ISSA.2016.7802922.

[13]. Rose, C. 2013, 'BYOD: An Examination of Bring Your Own Device in Business'. Review of Business Information Systems (RBIS), 17 (2), 65-70, https://doi.org/10.19030/rbis.v17i2.7846.

[14]. Silva, M.M., de Gusmão, A.P.H., Poleto, T., e'Silva, L.C., and Costa, A.P.C.S. 2014,'A multidimensional approach to information security risk management using FMEA and fuzzy theory', International Journal of Information Management, 34, 733-740, doi:10.1016/j.ijinfomgt. 2014.07.005.

[15]. Sing, N. 2012, 'B.Y.O.D. Genie Is Out of the Bottle – "Devil or Angel"', Journal of Business Management & Social Sciences Research, 1 (3), 1-12.

[16]. Stumpfegger, E. 2017, 'Trustworthiness of Research', Munich Business School, https://www.munich-business-school.de/insights/en/2017/trustworthiness-of-research/, (accessed 9 December 2021).

[17]. Van Niekerk, B. 2017, 'An analysis of cyber-incidents in South Africa'. The African Journal of Information and Communication (AJIC), 20, 113-132. https://doi.org/10.23962/10539/23573.