Employee Usage of Mobile Devices Within South African Municipalities, Implications on Policy and Employee Training

https://doi.org/10.3991/ijim.v14i20.15747

Patrick Otto, Job Dubihlela (✉), Henrie Benedict
Cape Peninsula University of Technology, Cape Town, South Africa
dubihlela@cput.ac.za

Abstract—This paper focuses on the importance of policies, procedures and employee training and awareness as aid to manage risks associated with the usage of mobile devices in local government entities in the Namakwa District of the Northern Cape region. A quantitative research method was applied in the study by obtaining responses from a sample of participants in the Namakwa District of the Northern Cape region, using closed-ended questions in the questionnaire, which provided the participants with a predetermined list of coded responses. The results were analyzed and indicated that the majority of the respondents do utilize mobile devices in their organizations. In general, these entities make more use of laptops than any other types of mobile devices. The results indicate that these organizations also still apply the traditional approach of providing their employees with specifically approved types of mobile devices (corporate-owned device) and therefore, do not support the Bring-Your-Own-Device or Choose-Your-Own-Device strategy. There is a clear indication that more efforts are required to ensure improvement, specifically relating to the development of a privacy and security policy and/or procedures as well as providing user training and awareness within municipal organizations.

Keywords—Mobile devices; mobile usage, mobile risks; employee training, South Africa municipalities

1 Introduction

The introduction of mobile devices has resulted in offices not being the only place where business is conducted, as access to the enterprise's network is now possible with such devices. Employees have started to utilize mobile devices for business and personal use, which comes with potential risk exposure to organizations. Therefore, effective risk management practices are pivotal within such organizations. The study aims to ascertain whether these organizations that permit the use of mobile device connections to their networks is managing the associated risks (Singh et al. 2018). The study specifically looked at whether these organizations developed and implemented an approved privacy and security policy and/or procedure to guide their employees, as well as educate them on security awareness and offer them with training (El-Sofany & El-Haggar, 2020). This research includes a literature review as well as

an in-depth investigation to determine the management of risks associated with the utilization of mobile devices within these entities.

The government structures within South Africa are in three (3) spheres; namely National, Provincial and Local government (The Constitution of the Republic of South Africa, 1996). The government sphere, specifically relating to Local Government, is a make-up of Municipalities in accordance with Chapter Seven (7) of the Constitution. Municipalities are responsible for managing their administration, planning and budgeting processes in such a way that they deliver basic needs (services) as well as promote social and economic development within their communities (The Constitution of the Republic of South Africa, 1996). The structures of municipalities within South Africa is further divided into three (3) categories; namely, Category A (metropolitan municipalities), Category B (Local Municipalities) and Category C (District Municipalities) (The Constitution of the Republic of South Africa, 1996).

According to an online overview of the research focus area (Municipalities of South Africa, 2020: online), the Namakwa District equates to 126 836km² and consist of seven (7) entities; one (1) District Municipality and six (6) Local Municipalities. Furthermore, considering the usage of mobile devices by employees within these municipalities in the Namakwa District during their day-to-day activities, an increased probability exists on the associated risk exposures materializing. Therefore, guidance to employees in the form of approved policies and/or procedures, as well as user training and awareness (education) is fundamental within these entities, and could not be overemphasized.

2 Literature Review

2.1 Risks associated with mobile device usage

Based on previous research reports (Zidoun et al. 2016; Phillips, 2014; Lydon, 2014; Adedolapo, 2016; De Shield, 2017), the usage of mobile devices as an organisational strategy, comes with potential associated risks about the entity. These include risks pertaining to User Privacy, Physical Security, Organisational and User Information Security as well as Compliance.

User privacy risk: In recent years, employees could utilize their privately owned devices for work-related activities which however increases concerns relating to the individual's privacy, according to Ames *et al.* (2016) as well as Miller *et al.* (2012). In cases where an investigation is required for whatever reason, personal devices are retained, resulting in the capturing of personal information on the devices. No access is granted to the devices during the investigation, and personal information might be retrieved from the device, resulting in possible breach of user privacy (Dhingra, 2016). Since the employee's private information is known to the employer in such an instance, it could result in it being used against an employee (Alhalafawy & Zaki, 2019). Loose *et al.* (2013) allude that the loss of, as well as retrieval of, personal information by organizations; are considered as a threat in such a strategy. Therefore, great care must be taken in instances where private/personal information stored on

devices are being accessed; as it could result in claims against the organization as well as possible embarrassment to such a user (Hinkes, 2014).

Physical security risk: By nature, smart devices are mobile, and are utilized in different locations. Therefore, such devices are at risk of being lost or stolen and could put sensitive organizational information at risk (Ames *et al.*, 2016). In agreement, Souppaya *et al.* (2013) indicate that mobile devices are generally utilized at many different locations, not necessarily always in the control of the organization. Furthermore, van Kessel et al. (2013) confirm that there is a growing trend in the access of information on mobile devices being lost or stolen. There is an indication that it is important to develop and implement mitigations to minimize potential damage in cases of devices being lost or stolen. According to Khan *et al.* (2015); the physical security of mobile devices is not an easy task. Devices being lost and having minimal access safeguards such as password controls could pose a potential risk to the organization (Alhalafawy & Zaki, 2019). Bellamy (2014) further confirms the risk in a study where almost 50% of the entities, in a survey for the previous year, have lost mobile devices. Therefore, physical securing of mobile devices is very important (Disterer & Kleiner, 2013).

Organizational and user information security risk: Information stored on mobile devices should be safeguarded and considered just as important as the actual physical device in itself. According to Ames *et al.* (2016), data stored on these devices are at risk of being compromised where the suitable security is not being considered and put in place. Another concern is instances where security on such devices are being lowered by users, opening the door for potential attacks (Alhalafawy & Zaki, 2019). Mobile devices are also utilized to make use of networks outside the organization for activities amongst others, such as internet access. Since the organization usually do not have control over the security of such networks, information that is communicated could be compromised (Souppaya *et al.*, 2013). Where users are utilizing Virtual Private Network (VPN) connections, the information could be compromised in instances where such devices are being lost or stolen, and such channels are used by unwanted people (van Kessel *et al.*, 2013). According to Dhingra (2016), the practice of the usage of personal mobile devices within the organization also pose a lot of risks. Still, the risk of losing data is one of the biggest threats. Pereira *et al.* (2017) agree with this sentiment in that this tendency, within businesses in recent times, brought about an increase in security risks in their view. In addition, security-related issues are considered high on the list when considering the usage of personal mobile devices, as employees take sensitive information away from the organization opening the door for unauthorized utilization or alteration (Jamaluddin *et al.*, 2015).

According to Singh et al. (2018) and Hetting (2014) the utilization of such as a strategy, could pose a risk of information loss in an event of the device being lost. Another concern raised regarding this strategy by Pillay *et al.* (2013) is that in the event of employees making a device change, critical information might be landing in the hands of unauthorized individuals. To support this sentiment, Siddiqui (2014) indicates that sensitive information might get lost or compromised where employees dispose of their devices, sharing it with family or in the event of them exiting the organization. Lost business information may result in unfavourable publicity which

could negatively affect stakeholder's confidence in the organization's systems and controls, as well as its ability to manage its affairs (Hinkes, 2014). Therefore, the benefits associated with this strategy could be outweighed in instances where the organization's information is not effectively managed (Garba *et al.*, 2015).

Compliance risk: As an organization, the entity should comply with laws, regulations, policies and procedures to improve stakeholder confidence and continue their operations to increase investor's value. Therefore, based on the strategy implemented with regards to the usage of mobile devices; an organization will be required to implement the necessary mitigations to minimize the possibility of the realization of compliance risks.

2.2 User training and awareness

The employees within municipalities in the Namakwa District make use of mobile devices in general during their day-to-day activities. Whist the trend in work habits shifted as employees can work from outside the office, this increases the probability of risks (pertaining to the organization) materializing. When referring to the role of the Accounting Officer in line with the MFMA Section 62 (1) (c) and Section 95 (c) (i); the importance of an effective, efficient and transparent risk management system is emphasized, in aid to enhance the achievement of organizational objectives.

Therefore, organizations should develop and implement a privacy and security policy; to provide guidance to employees, as well as protect organizational information where mobile device usage is permitted to manage associated risks (Garba et al. 2015). A privacy and security policy/procedure are a set of rules, known throughout the organization, which should be followed and complied with (by employees) in search of protection against associated risks. According to Sanelli (2018), policies address essential matters such as acceptable behaviour while procedures define what steps should be followed for consistency purposes. Watson (2016) agree with this sentiment, indicating that policies and procedures are fundamental in ensuring consistency within an organization.

According to Neideck (2016), the importance of having policies and procedures within an entity includes benefits such as:

- Setting and defining expectations
- Keeping managers accountable to set standards
- Driving compliance with laws
- Assisting in defence against employee claims [against the organization]
- Making employees aware of what to do and where to turn to for help

However, the implementation of a new policy/procedure document should be launched appropriately to ensure that the awareness concerning the process is communicated to the relevant audience as well as the necessary training provided. According to Chand (n.d), training refers to the mastering of a skill to the desired level, against a set standard. Benton (2014) opines that a lack of employee training comes at

a cost, as these are often unhappy employees. O'Neill (2020) opines that the value of having employees trained within entities provides benefits such as:

- Improvement in performance
- Enhanced communication
- Improvement in staff retention
- Creating consistency in how to do things
- Reducing recurring errors

According to Hanlin et al. (2013); through the performance of training and awareness relating to the usage of mobile devices, users would be more vigilant about security. This was also confirmed by Disterer and Kleiner (2013) as well as by Siddiqui (2014), indicating that comprehensive training and awareness is essential for users when implementing a new policy or procedure document and format it with the styles.

3 Research Design and Methodology

The research conducted included an empirical study through the collection of data using a quantitative research method. Based on previous studies, more work on the management of risks emanating from the operational level was an area identified which warrants additional research work. The quantitative research method followed included the surveying of a research questionnaire to obtain quantitative data on the views from respondents who adhere to the relevant demarcation criteria. The research questionnaire utilized during the survey comprises of closed questioning, therefore providing the participants with a predetermined list of responses coded in advance, from which to make a selection. According to an online overview of the research focus area (Municipalities of South Africa, 2020), the Namakwa District consists of seven (7) entities as previously discussed. Therefore, the total number of individuals employed within the administrative functions of these entities, making use of mobile devices, were considered the targeted population. The non-random (non-probability) sample selection options were applied during the research and more specifically included the Snowball as well as the Convenience options. Information obtained from the respondents in the form of the completed research questionnaires received was recorded within a Microsoft Excel template and analysed using the Statistical Package for Social Sciences (SPSS) software.

The study followed appropriate ethical considerations. These include the explanation of research objectives to participants, not including minors in the sample of required respondents, informing respondents that participation is voluntary as well as obtaining the required consent while clarifying that withdrawal from participation is allowed without any implications. Furthermore, the participants were informed that a research questionnaire to be answered will be the tool used in the data gathering process and that such data obtained will be used for academic purposes and anonymously included in a master's thesis document and an academic journal as a summary of all information received and not being identified as single respondent's information.

4 Results and Discussion

Results emanating from the study is based on responses from individuals employed within the Local Government entities in the Namakwa District, with the following information:

Table 1. Profile of Respondents

Respondent's age	**Frequency**	**%age**	**Respondent's Average Years of Experience**	**Frequency**	**%age years**
Below 26 yrs	6	12.0	Senior Management	18.33	43.2
From 26-35 yrs	17	34.0	Middle Management	15.85	37.3
From 36-45 yrs	18	36.0	Non-management	8.27	19.5
From 46-55 yrs	8	16.0			
55 yrs +	1	2.0			
Total	50	100	Total	42.45	100
Respondent's position	***Frequency***	***%***	***Respondent's Gender***	***Frequency***	***%***
Senior Management	9	18.0	Male	32	64.0
Middle Management	16	32.0	Female	18	36.0
Non-management	25	50.0			
Total	50	100	Total	50	100

When respondents were asked, whether management within the Local Government entities in the Namakwa District deems mobility of employees as necessary in delivering on organizational objectives, it is evident from the responses obtained that it is considered imperative; and corroborated by the fact that 39.58% of responses indicate it as being very important and 41.67% as important. However, the usage of a mobile device within these entities include mostly laptops (70.18%); while minimum usage of other mobile devices such as tablets (17.54%) and smartphones (10.53%) occur. The majority (72.73%) of smartphones and tablets users is more senior officials (senior management and middle management). Furthermore, a substantial amount of participants confirmed that their organizations do not allow the usage of personal mobile devices, with only 20.93% confirming use. Therefore, these entities are generally still making use of the traditional approach of providing their employees with their specifically approved types of mobile devices and not supporting the Bring-Your-Own-Device (BYOD) or Choose-Your-Own-Device (CYOD) strategy.

Furthermore, when respondents were asked whether formal policies/procedures are in place guiding users/employees, and whether training and awareness are available to users/employees in instances where mobile device usage is allowed within Local Government entities in the Namakwa District; it is evident that significant improvement is required in this area.

The following factors, as per below, corroborate those mentioned above:

Table 2. Existence of policies and training - mobile device usage

Existence of Policies / Procedures	Frequency	%	Training provided	Frequency	%
Yes	15	30.0	Yes	6	12.0
Not sure	17	34.0	Not sure	9	18.0
No	18	36.0	No	35	70.0
Total	50	100	Total	50	100

In limited instances (30.00%), participants were confident that their organization have a formal policy/procedure in place on mobile devices and confirm the need for improvement. A significant number of responses (70.00%) confirmed that formal training is not being provided in their organizations and confirm the requirement for improvement.

Stemming from the results discussed above, it is evident that improvement is necessary relating to the development and / or creating of awareness about a formal privacy and security policy / procedure, and the need to provide user/employee training and awareness; affecting the management of associated risks as highlighted in the literature review previously discussed. This was also validated by the fact that when respondents were asked whether risks pertaining to mobile devices utilized within the Local Government entities in the Namakwa District, is managed; only 36.11% confirmed that there is satisfactory management of these risks (16.67% - Very good, and 19.44% - Good).

5 Conclusion and Recommendations

5.1 Concluding remarks

According to the literature study performed, it became evident that risks relevant to an organization not effectively managed, influence the achievement of the organizational objectives. Based on the results, it is evident that employees and management of Local Government Entities within the Namakwa District of the Northern Cape consider the usage of mobile devices as essential and necessary in the achievement of organizational objectives. After testing whether policies/procedures to guide users/employees, as well as training and awareness for users/employees, is performed (on the usage of mobile devices) within Local Government entities in the Namakwa District; it is evident based on results obtained, and analyses performed that these are areas requiring improvement, and if enhanced could impact on effective management of associated risks.

The majority of respondents (84.00%) indicated that their organisation makes use of mobile devices, and a substantial number of respondents confirmed that mobile devices are considered vital by themselves (64.58%) as well as their management (81.25%). In contrast, 9 out of 10 respondents agree that mobile devices enhance their efficiency and productivity. These results confirm the statement of Shackles (2016), who stipulated that the usage of mobile devices became important in the modern business world and had an effect on productivity. Jamaluddin *et al.* (2015) corroborate

that the usage of mobile devices by employees give them access to organisational information while being away from the office, and therefore increase productivity. This is also aligned to the conclusion by Sheldon (2013) as well as Ludwig (2018) that the usage of mobile devices impact efficiency and productivity of employees.

Many participants (62.79%) confirmed that their organisations do not allow the usage of personal mobile devices. This conservative approach is followed to minimise the risk of information being accessed or altered by unauthorised individuals. It is aligned to the opinions of Pillay *et al.* (2013) as well as Miller *et al.* (2012) and Hetting (2014). They all concluded that the utilisation of a strategy where employee's mobile devices are being utilised pose a risk of information loss to the organisation. These results also corroborated the statement made by Siddiqui (2014), who stipulated that sensitive information might get lost or compromised where employees dispose of their devices, sharing it with family or in the event of them exiting the organisation.

Processes about the management of risks within these entities require improvement, explicitly relating to policies/procedures to guide users/employees as well as training and awareness provided to users/employees to ensure vigilant users. These results are corroborated by the statements of other researchers, as mentioned below:

Name of author (s)	Research focus area	Findings
Garba *et al.* (2015)	Managing information security and privacy risks about mobile devices.	Organisations should develop and implement a privacy and security policy where mobile devices are being utilised.
Yevseyeva *et al.* (2014)	Managing user risks on mobile devices.	Privacy and security policy should be complied in search of protection against security risks
Harris *et al.* (2013)	Mobile device security awareness and training.	Training and awareness of users are important where mobile devices are being utilised.
Siddiqui (2014)	Mobile device security awareness and training.	Training of users is essential where mobile devices are being used.
Hanlin *et al.* (2013)	Mobile device education, training and awareness pertaining to security.	Training and awareness will ensure that users would be more vigilant with regards to security while utilising mobile devices.

Based on the discussions mentioned above, it is evident that the processes on the management of associated risks within these entities require improvement, specifically pertaining to the development and roll-out of a privacy and security policy/procedure, and conducting of employee/user training and awareness where mobile devices are utilized at Local Government entities in the Namakwa District of the Northern Cape.

5.2 Recommendations

The following recommendations were made pertaining to the research performed:

i. Developing a privacy and security policy/procedure: Management should compile a privacy and security policy or procedure document on the usage of mobile devices, approved by the relevant officials and committees, which guide employees.
ii. Providing user training and awareness: Management should invest more time and resources to provide employees with the necessary training periodically, creating security awareness with regards to the associated risks about the usage of mobile device; and training and awareness procedure should be revisited to account for amendments where required.

6 Limitations and Suggestions for Further Research

You The research exposed certain constraints. The major limiting factors experienced relate to challenges in receiving a written consent letter from the leadership of all entities within the scope of the study, granting the researcher permission to approach employees within their entities during the data collection phase. Participant's daily tasks (at work) taking preference, resulting in a slow response rate relating to the completion and return of Research Questionnaire documents.

Another limitation is the fact that this study exclusively focused on the municipalities in the Namakwa District of South Africa. Further research opportunities do exist which could research on 1.) Improvement of internal controls (i.e. use of matrixes) governing the risks associated with the utilization of mobile devices; 2.) Worthiness and cost relation with regards to the usage of mobile devices by organizations; 3.) Verification of other security solutions associated with the utilization of mobile devices; and 4.) Development of a methodology relating to risk assessment while using mobile devices, in order to prioritize the treatment of higher-risk exposures before spending time on the remaining risks.

7 Acknowledgements

Authors appreciate the Cape Peninsula University of Technology for the literary resources, the research opportunity provided. Dr Benedict and Prof Dubihlela spared their time and support from demanding academic duties to offer guidance during this research study. The special services of Cheryl Thomson for professional editing is appreciated.

8 Authors' Contributions

The material of this publication was introduced with the intention of Mr Otto's pursuance of his master's degree, a co-supervised collaboration. Both Dr Benedict (principal supervisor) and Prof. Dubihlela (co-supervisor) significantly contributed to the research conceptualization and further collaborated as supervisors. Their duties were to assist with the completion of the research project, conduct all reviews and

guide the direction of the research project, the data analysis and overall academic write-up.

9 References

[1] Adedolapo, A. 2016. Bring your own device (BYOD) adoption in South African SMEs. https://open.uct.ac.za/bitstream/.../thesis_com_2016_akin_adetoro_adedolapo.pdf [10 March 2020].

[2] Alhalafawy, W.S. Zaki, M.Z.T. 2019. The effect of mobile digital content applications based on gamification in the development of psychological well-being. International Journal of Interactive Mobile Technologies, Vol. 13 (8), 107-123. https://doi.org/10.3991/ijim.v13i08.10725

[3] Ames, B., Brown, F., Bogert, J., Creer, M., Lourens, J., Patel, R., Rai, S. & Stein, S. 2016. An internal auditor's guide to understanding and auditing smart devices. https://na.theiia.org/standards-guidance/Member%20Documents/GTAG-Auditing-Smart-Devices.pdf [09 May 2019].

[4] Bellamy, F.D. 2014. Enterprises without strong BYOD policies risk major data breach. https://search-proquest-com.libproxy.cput.ac.za/docview/15605/ [14 February 2019].

[5] Benton, B. 2014. Importance of Employee Training: 6 Reasons Why It Saves You Money. https://www.autodesk.com/redshift/importance-of-employee-training/ [16 April 2020].

[6] De Shield, L. 2017. The challenges of implementing Bring Your Own Device. https://scholarworks.waldenu.edu/cgi/viewcontent.cgi? [10 March 2019].

[7] Dhingra, M. 2016. Legal issues in secure implementation of Bring Your Own Device (BYOD).http://www.sciencedirect.com/science/article/ [08 March 2019]. https://doi.org/10.1016/j.procs.2016.02.030

[8] Disterer, G. & Kleiner, C. 2013. BYOD Bring Your Own Device. http://www.sciencedirect.com/science/article/pii/S221201731300159X [08 March 2020]. https://doi.org/10.1016/j.protcy.2013.12.005

[9] El-Sofany, H.F. & El-Haggar, N. 2020. The Effectiveness of Using Mobile Learning Techniques to Improve Learning Outcomes in Higher Education. International Journal of Interactive Mobile Technologies, Vol. 14 (8), 4-18. https://doi.org/10.3991/ijim.v14i08.13125

[10] Garba, A., Armarego, J. & Murray, D. 2015. A policy-based framework for managing information security and privacy risks in BYOD environment. http://www.ijettcs.org/Volume4Issue2/IJETTCS-2015-04-23-122.pdf [11 March 2019].

[11] Hanlin, C., Jiao, L., Thomas, H. & Xiaowei, L. 2013. Security challenges of BYOD: A security education, training and awareness perspective. https://minerva-access.unimelb.edu.au/handle/11343/33347 [11 March 2019]

[12] Harris, M., Patten, K. & Regan, E. 2013. The need for BYOD mobile device security awareness and training. http://aisel.aisnet.org/amcis2013/ISSecurity/GeneralPresentations/14/ [11 March 2019].

[13] Hetting, C. 2014. Mitigating security & compliance risks with EMM. https://us.blackberry.com/content/dam/blackBerry/pdf/business/english/Heavy_Reading-Mitigating_Security_and_Compliance_Risks_with_EMM.pdf [14 May 2018].

[14] Hinkes, A. 2014. BYOD policies: A litigation perspective. http://www.americanbar.org/content/dam/aba/administrative/litigation/materials/2014_sac/2014_sac/byod_policies.pdf [11March 2019].

[15] Jamaluddin, H., Ahmad, Z., Alias, M. & Simun, M. 2015. Personal Internet use: The use of personal mobile devices at the workplace. www.sciencedirect.com/science/article/pii [20 April 2019].
[16] Khan, J., Abbas, H. & Al-Muhtadi, J. 2015. Survey of mobile user's data privacy threats and defence mechanisms. http://www.sciencedirect.com/science/article/pii/S1877050915017044 [20 April 2019]. https://doi.org/10.1016/j.sbspro.2015.01.391
[17] Loose, M., Weeger, A. & Gewald, H. 2013. BYOD – the next big thing in recruitment? Examining the determinants of BYOD service adoption behaviour from the perspective of future employees. http://aisel.aisnet.org/amcis2013/EndUserIS/GeneralPresentations/12/ [11 March 2019]. https://doi.org/10.1016/j.procs.2015.07.223
[18] Ludwig, S. 2018. Why organizations should still care about BYOD. https://search-proquest.com.libproxy.cput.ac.za/docview/2052775065? rfr[14 February 2019].
[19] Lydon, E. 2014. The benefits and threats of BYOD in a SME enterprise. www.diva-portal.org/smash/record.jsf?pid=diva2:1022207 [06 March 2019].
[20] Neideck, S. 2016. 5 Key Reasons Why It's Important to Have Policies and Procedures. https://community.hrdaily.com.au/profiles/blogs/5-key-reasons-why-it-s-important-to-have-policies-and-procedures [16 April 2020].
[21] Miller, K., Voas, J. & Hurlburt, G. 2012. BYOD: Security and privacy considerations. https://s3.amazonaws.com/academia.edu.documents/30666416/MVH2012.pdf?AWSAccessKeyId [09 October 2018].
[22] Municipalities of South Africa. 2020. Municipalities. https://municipalities.co.za/ [24 January 2020].
[23] O'Neill, E. 2020. The Importance of Training Employees for your Business. https://www.learnupon.com/blog/importance-of-training-employees/ [16 April 2020].
[24] Pereira, T., Barreto, L. & Amaral, A. 2017. Network and information security challenges within Industry 4.0 paradigm. Procedia Manufacturing, 13:1253–1260. [12 September 2019].
[25] Phillips, C. 2014. Information security governance implementation within the mobile device environment. https://open.uct.ac.za/bitstream/handle/.../thesis_com_ [06 March 2019]. https://doi.org/10.1016/j.promfg.2017.09.047
[26] Pillay, A., Diaki, H., Nham, E., Senanayake, S., Tan, G. & Deshpande, S. 2013. Does BYOD increase risks or drive benefits? https://minerva-access.unimelb.edu.au [11 March 2019].
[27] Sanelli, A. 2018. The importance of policy & procedure. https://www.convercent.com/blog/the-importance-of-policy-procedure [16 April 2020].
[28] Shacklett, M. 2016. Mobile devices in the workplace: Three situations that could get awkward. https://www.techrepublic.com/article/mobile-devices-in-the-workplace-three-situations-that-could-get-awkward/ [18 February2019].
[29] Sheldon, R. 2013b. Wearable computing devices could have enterprise prospects. http://searchmobilecomputing.techtarget.com/opinion/Wearable-computing-devices-could-have-enterprise-prospects [06 March 2019].
[30] Siddiqui, R. 2014. Bring Your Own Device (BYOD) in higher education: Opportunities and challenges. http://scholar.google.co.za/scholar?start=10 &q=byod&hl=en&as_sdt=0,5&rlz=1Y1XIUG_enZA513ZA513 [11 March 2019]. https://doi.org/10.1016/c2012-0-07723-x
[31] Souppaya, M. & Scarfone, K. 2013. Guidelines for managing the security of mobile devices in the enterprise. http://nvlpubs.nist.gov/nistpubs/SpecialPublications [07 March 2019]. https://doi.org/10.6028/nist.sp.800-124r1

[32] Singh, S., Zolkepli, I.A., & Kit, C.W. 2018. New Wave in Mobile Commerce Adoption via Mobile Applications in Malaysian Market: Investigating the Relationship Between Consumer Acceptance, Trust, and Self Efficacy. International Journal of Interactive Mobile Technologies., 12 (7), 112-128. https://doi.org/10.3991/ijim.v12i7.8964

[33] Van Kessel, P., Layman, J., Blackmore, J., Burnet, I. & Harada, S. 2013. Bring your own device: Security and risk considerations for your mobile device program. http://www.ey.com/Publication/vwLUAssets/EY_-

[34] Watson, K. 2016. The Importance of Policies and Procedures. https://www.excelbenefitconsulting.com/the-importance-of-policies-and-procedures/ [16 April 2020].

[35] Yevseyeva, I., Morisset, C., Turland, J., Coventry, L., Grob, T., Laing, C. & Van Moorsel, A. 2014. Consumerisation of IT: Mitigating risky user actions and improving productivity with nudging. www.sciencedirect.com/science/article [20 April 2019]. https://doi.org/10.1016/j.protcy.2014.10.118

[36] Zidoun, Y., El arroum, F.Z., Talea, M., Dehbi, R. 2016. Students' Perception About Mobile Learning in Morocco: Survey Analysis. International Journal of Interactive Mobile Technologies, 10 (4), 80-84. https://doi.org/10.3991/ijim.v10i4.5947

10 Authors

Patrick Otto is the Lead Internal Auditor at PetroSA, who completed his master's degree in Internal Auditing in the department of Financial Information systems at the Cape Peninsula University of technology.

Prof Job Dubihlela is a financial expert turned-academic with a wealth of over 15 years in industry. He is currently head of Internal Auditing & Financial Info Systems at the Cape Peninsula university of Technology. He sits on various research committees and trustee boards. He has published extensively in internal reputable journals.

Dr Henri Benedict is a senior lecturer in the faculty of business and management sciences at the Cape Peninsula university of Technology. He is widely published in internal reputable journals.

Article submitted 2020-05-26. Resubmitted 2020-09-18. Final acceptance 2020-09-18. Final version published as submitted by the authors.