Mobile Device Usage in Higher Education Institutions in South Africa

Ryan De Kock and Lynn A. Futcher
Center for Research in Information and Computer Security, School of ICT, Nelson Mandela Metropolitan University
Email: s211109940@nmmu.ac.za, Lynn.Futcher@nmmu.ac.za

***Abstract*— Cyber security threats are on the rise as the use of personally owned devices are increasing within higher education institutions. This is due to the rapid adoption of the Bring Your Own Device (BYOD) trend. In 2014, 92% of students used laptops globally for academic purposes, 44% used tablets, and 68% used smart phones. In addition, 89% of higher education institutions in the United States and United Kingdom allow students, faculty and non-academic staff to access their network using personally owned mobile devices.**

A great concern is that although BYOD is widely accepted in higher education institutions, security is somewhat lacking. In addition, cyber-security threats have switched their focus to mobile devices. Therefore, the number of new mobile vulnerabilities reported each year has increased. Furthermore, in 2014, 10% of global cyber security breaches took place in the education sector with a total of 31 breaches resulting in the exposure of 1,359,190 identities. This placed the educational sector at the top of the list with the third most cyber-security breaches in 2014, behind the healthcare and retail sectors.

A literature survey, together with a single explanatory case study involving a higher education institution in South Africa were used to determine typical mobile device usage in an academic context. As a result of completing the study, it is clear that there is a high demand for the use of BYOD in higher education institutions in South Africa and that BYOD is vital to the academic success of its students. This paper discusses mobile device usage in higher education institutions in South Africa. In addition, it provides some key factors for higher education institutions to consider when dealing with the increased demand for BYOD usage.

Keywords*— *Mobile Device Usage; Bring Your Own Device (BYOD); Higher Education Institutions

I. INTRODUCTION

Gartner [1] defines Bring Your Own Device (BYOD) as:

"*An alternative strategy that allows employees, business partners and other users to use a personally selected and purchased client device to execute enterprise applications and access data. It typically spans smartphones and tablets, but the strategy may also be used for PCs. It may or may not include a subsidy.*"

BYOD was first introduced in 2009 by Malcolm Harkins, Intel's chief information security officer, after realizing that more and more employees wanted to use their own mobile devices in the workplace [2]. Intel's leaders did not dismiss the possibility of this new trend due to the risks involved. Instead, they embraced the technology by setting up effective employee-owned device policies, resulting in increased connectivity to Intel's network, greater employee productivity and improved security measures.

As the adoption of the BYOD trend is increasing in today's organizations of different sectors, higher education institutions also encourage students and staff to use their own devices in exchange for the benefits offered by this trend. Furthermore, it is predicted that BYOD will become the leading practice for all educational environments by the year 2017 [3]. This highlights the overwhelming increase in the BYOD paradigm in the education sector.

The purpose of this paper is to determine mobile device usage in higher education institutions in South Africa. This is achieved through a case study of a South African higher education institution, implementing BYOD. The following section discusses the research design implemented in this study followed by background information on the use of BYOD in higher education institutions. Thereafter, the case study data is presented and discussed followed by key factors derived from the literature and the case study data.

II. RESEARCH DESIGN

In addition to the literature survey conducted to gain a better understanding of mobile device usage in higher education institutions, this study also makes use of a case study. The case study was used to gather a large amount of data and information required to determine the current state of mobile device usage in South African higher education institutions.

Yin [4] suggests that there are three different types of case studies. These include explanatory, exploratory and descriptive case studies. However, this research makes use of the descriptive case study. This type of case study is used when the researcher is seeking describe a natural phenomenon which occurs within the data in question [4]. As for this research, a descriptive case study is used to describe how a South African higher education institution is implementing BYOD.

In addition, there is more than one type of case study design. In fact, Yin [4] proposes that there are two types of case study

designs, the single- and multi-case design (which involves cases within cases). The design used for this study makes use of the single case study design, as it focuses on a single case.

Therefore, a single descriptive case study involving a higher education institution in South Africa was used to determine typical mobile device usage in an academic context. The following section discusses mobile device usage in higher education institutions.

III. BACKGROUND

Although the concept of BYOD was only first introduced in 2009 [2], organizations and higher education institutions have shown an increasing interest in and tolerance for employees and students using their own mobile devices for work and academic purposes.

Liz Gosling, director of Information Technology (IT) services at Auckland University of Technology, states that the IT demands in higher education institutions differ from the technology requirements within an enterprise organization [5]. Therefore, to draw a comparison between higher education institutions and enterprise organizations, the BYOD users within each of these need to be compared to determine where they are similar and where they differ. Fig. 1 illustrates this comparison.

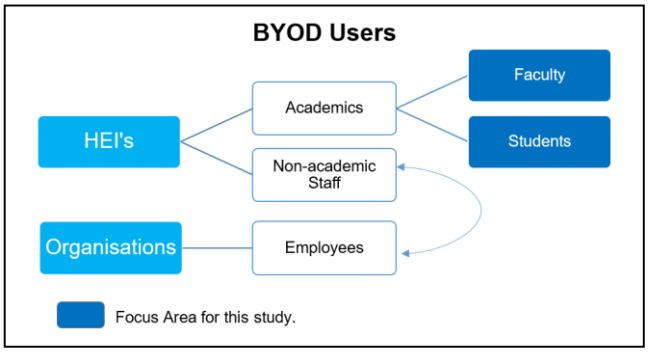

Figure 1: A comparison between BYOD users in organizations and HEI's.

As depicted in Fig. 1, the BYOD users in higher education institutions differ from organizations since they comprise students, non-academic staff and faculty, whereas organizations only include various employees. Furthermore, the employees within an organization are similar to the non-academic staff members within a higher education institution. These include human resources, marketing, accounting and finance, management, employees, etc. Throughout this paper, faculty refers to any academic staff such as lecturers, professors, etc.

Higher education institutions are realizing the importance of addressing the demand of BYOD within their institutions. This is supported by the findings in a survey conducted by Bradford Networks [6]. The survey questioned professionals representing over 500 higher education institutions in the United States and United Kingdom. It was found that 85% of higher education institutions allow students, faculty and non-academic staff to use their personal devices on their network, while 6% of the respondents reported that they have no plans to implement BYOD in the future. Furthermore, they found that 84% of the institutions that do not allow BYOD receive requests to use personal devices on their networks [6]. From Fig. 2, it is clear that there is a high demand for mobile device usage in higher education institutions. Fig. 2 is based on the results of an international survey conducted by Educause in 2014 [7]. The survey was sent to 213 higher education institutions across 15 countries.

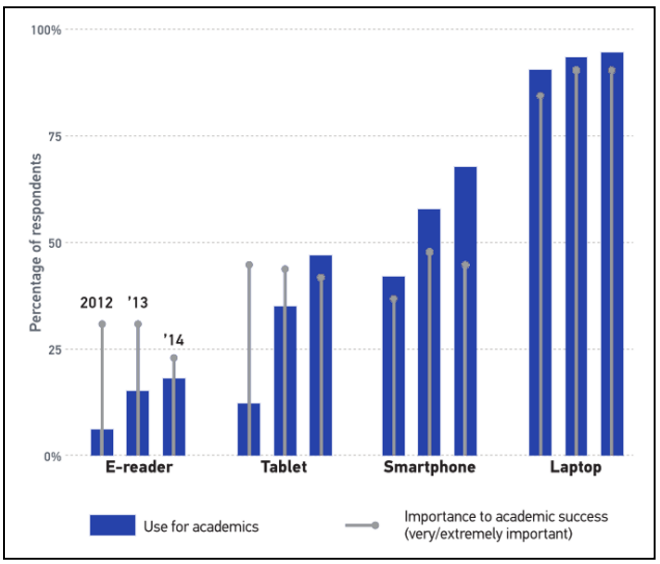

Figure 2: Use and importance of devices for academics [7].

Fig. 2 illustrates how important the use of BYOD is within the education sector as well as the percentage of students and staff that use personally owned devices for educational purposes. As illustrated in Fig. 2, 92% of students used laptops for academic purposes in 2014, 44% used tablets, 68% used smart phones, and 16% used e-readers [7]. An additional figure extracted from the international survey conducted by Educause in 2014, shows students' experiences with various types of technology for academic purposes. This is depicted in Fig. 3.

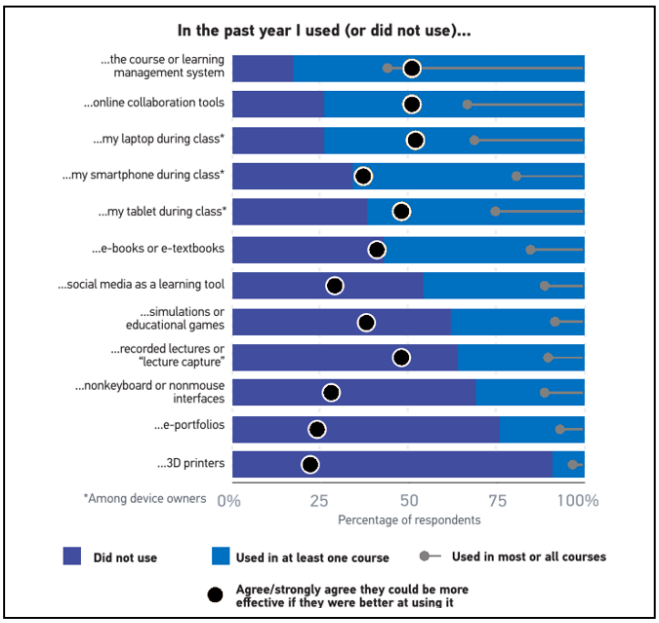

Figure 3: Use of technology for academic purposes [7].

Fig. 3 shows students' experiences with various types of technologies and their opinions about being more effective if they were better skilled at using certain technologies. Although students are skilled in most technologies, the use of e-books and recorded lectures should be considered. Furthermore, higher education institutions should provide enough online content to support their course content. Most students have used the learning management system (LMS) in at least one course (83%), but only just over half (56%) have used it in most or all of their courses, as depicted in Fig. 3. An LMS is a fundamental component in higher education. These systems function as digital learning environments, administrative systems for course management, and enterprise systems for institutional analytics and other purposes [8].

The above mentioned surveys clearly reflect a wide acceptance of BYOD in higher education institutions. Stavert [9] therefore, suggests three main reasons for why education institutions transition to BYOD. These include:

1. Financial pressure – Not all higher education situations can afford state of the art personal technology for all its students and staff. However, with the use of BYOD, students, faculty and non-academic staff can use their own mobile devices.
2. Pressure from students and staff – Higher education institutions are pressured by students, faculty and non-academic staff to use their own mobile devices for work and academic purposes.
3. Digital device ownership and use – Mobile devices have become more affordable over the last couple of years. These devices provide students, faculty and non-academic staff with 24/7 access to ideas, resources, people and communities. This has led to a large increase in ownership of mobile devices.

In addition, the reasons behind the great levels of acceptance in higher education institutions may be due to the fact that the purpose of an educational institution is to provide knowledge which is achieved by providing information regarding a particular subject. Today the internet is a major source of information on almost any subject. Higher education institutions may also have subscriptions to online journals and libraries which most of them provide for free to students. With the use of BYOD, students can easily access these sources of information from anywhere [10].

A great concern is that although BYOD is widely accepted in higher education institutions, security is somewhat lacking. Most higher education institutions have allowed some form of BYOD mostly via network access control (NAC) without implementing any BYOD policy [10]. This is very risky as higher education institutions are exposing their networks to various threats like unauthorized access, attacks of malware and viruses from student devices connected to the institution's network, loss of data, etc. This is also supported by an international survey conducted by the SANS Institute in 2014. They found that 60% of higher education institutions are concerned with the use of faculty and non-academic staff owned mobile devices while 30% are concerned with the use of student owned mobile devices on their networks [11].

The greater concern over faculty- and non-academic staff-owned mobile devices makes sense, since they handle large amounts of sensitive data, whereas students typically only handle their own. However, it was specifically the exposure of this type of data that landed Iowa State University in trouble in April 2014, when it was discovered that nearly 30,000 student records between 1992 and 2012 were exposed on 5 departmental servers [12]. While the servers where taken over by attackers wanting the computing power to create Bitcoins, the fact remains that privacy-protected data subject to regulatory compliance was inadvertently exposed on their servers.

It is therefore clear that there is a high global demand for mobile device usage in higher education institutions and that security is somewhat lacking. The following section discusses mobile device usage in South African higher education institutions.

IV. CASE STUDY

In accordance with the case study approach, a representation of any population was not intended, but rather a single case was chosen [13]. For this purpose, only South African higher education institutions implementing BYOD where eligible. According to the South African Higher Education Act 101 [14], a higher education institution can be defined as an institution that provides higher education on a full-time, part-time or distance basis which is:

a) Merged, established or deemed to be established as a public higher education institution under this act;

b) Declared as a public higher education institution under this act;

c) Registered or provisionally registered as a private higher education institution under this act.

Given the above mentioned definition of what a higher education institution is, a prominent higher education institution within South Africa, was selected as the single case for this case study.

The Nelson Mandela Metropolitan University (NMMU) opened on 1 January 2005, due to the merging of three very different institutions as a result of the South African government's countrywide restructuring of higher education. Therefore, NMMU brings together the traditions of both technikon and university education, and draws on more than a century of quality higher education in an institution that offers a wide range of academic, professional and technological programs at varying entrance and exit levels. Furthermore, the NMMU has approximately 26 602 students and approximately 4 515 (1 702 faculty and 2 813 non-academic staff) permanent and contracted staff members, based on six campuses in the Nelson Mandela Metropole and George.

The mission statement of the NMMU is "*to offer a diverse range of quality educational opportunities that will make a critical and constructive contribution to regional, national and global sustainability*". This can only be achieved through the deployment and use of appropriate Information and Communication Technologies (ICT). The NMMU must furthermore also operate and be perceived as a safe and reliable

institution that ensures the security and proper use of its information assets.

The NMMU provides Wi-Fi access to students, faculty, non-academic staff and guests on their campuses. They also recognize the value of personal devices used for work and study purposes. In the past few years, NMMU has invested R7 000 000 on Wi-Fi across all seven campuses, and a further R750 000 to improve the quality of the Wi-Fi coverage. They have also upgraded 70 traditional lecture venues to enable faculty and students to use modern technology and provided support for NMMU's Learning Management System (Moodle). In addition, the university handed over 250 computing devices using selection criteria that covered all campuses and all faculties but with a focus on off-campus students. Furthermore, they estimate that an additional R2 000 000 will be spent on modernizing the remaining venues in 2016. Due to this, mobile device usage at the NMMU has increased over the past few years.

The case study data was obtained from key ICT staff members from the NMMU. They were asked to supply BYOD related documents and archival records where available. Several freely available documents were also obtained from internal systems within the NMMU. The documents obtained include network logs, a list of suggested software, survey results, information security awareness and training initiatives, policies and procedures.

Fig. 4 illustrates mobile device usage among students, faculty and non-academic staff at the NMMU. These percentages refer to the number of users who used their smartphones, laptops and tablets to access the NMMU network 3 or more times per week in 2014.

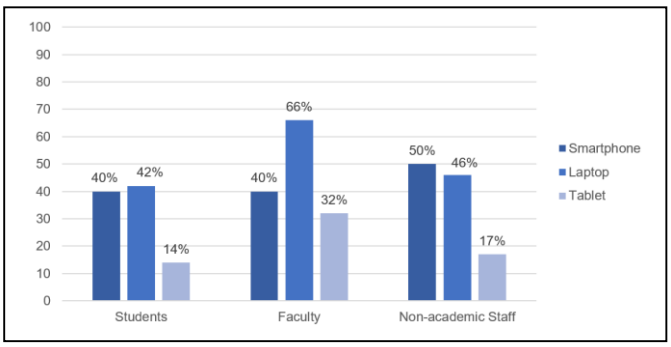

Figure 4: Mobile device usage for 3 or more times per week in 2014.

In 2014, faculty and non-academic staff accessed the NMMU network using mobile devices more frequently than students, as depicted in Fig. 4. Furthermore, students and faculty primarily used laptops when accessing the NMMU network, while non-academic staff primarily used smartphones. Tablets where not used very often by any of the user groups in 2014, as depicted in Fig. 4. However, Fig. 5 illustrates an enormous increase in tablet usage by students in 2015. In fact, tablet usage among students increased by approximately 55% from 2014 to 2015, as depicted in Fig. 5.

It can also be seen that student smartphone usage increased from approximately 40% in 2014 to approximately 85% in 2015. Furthermore, laptops which were primarily used by students in 2014, were surpassed by smartphones and tablets in 2015.

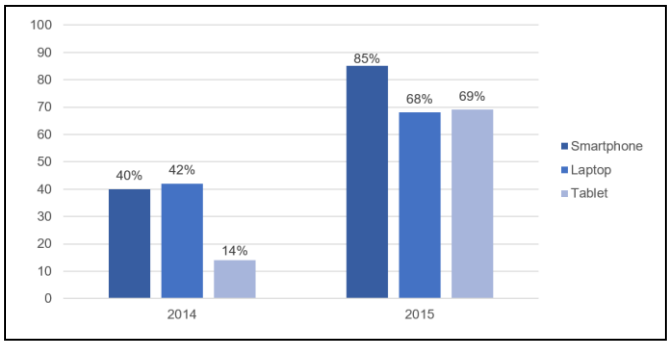

Figure 5: Student mobile device usage for 3 or more times per week.

Smartphone usage among faculty and non-academic staff also increased in 2015, as depicted in Fig. 6. However, the increase in smartphone usage resulted in a decrease in laptop and tablet usage among faculty and non-academic staff in 2015. Fig. 6 refers to both faculty and non-academic staff. However, the figure only depicts mobile device usage for 3 or more times per week, therefore only illustrating the frequent use of mobile devices accessing the NMMU network.

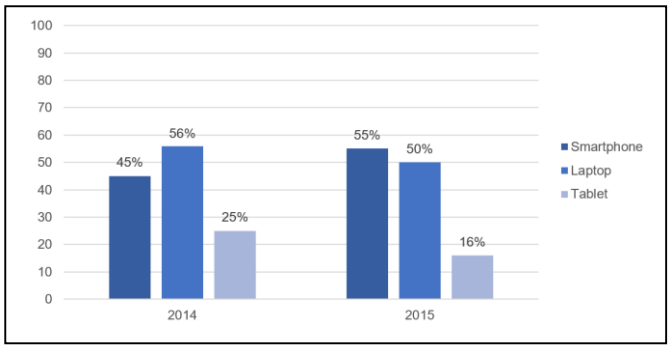

Figure 6: Staff mobile device usage for 3 or more times per week.

Smartphone usage among faculty and non-academic staff increased by approximately 10% from 2014 to 2015, while laptop usage decreased slightly by approximately 6% and tablet usage decreased by approximately 9%, as depicted in Fig. 6.

The frequent use of mobile devices at the NMMU increased significantly among students in 2015. However, the frequent use of mobile devices among faculty and non-academic staff has decreased slightly with the exception of a slight increase in smartphone usage. Figs. 7, 8 and 9 illustrate what the mobile devices depicted in Figs. 4, 5 and 6 were used for in 2015, therefore only depicting the frequent use (3 or more times per week) of mobile devices.

Fig. 7 illustrates what students, faculty and non-academic staff used their smartphones for in 2015.

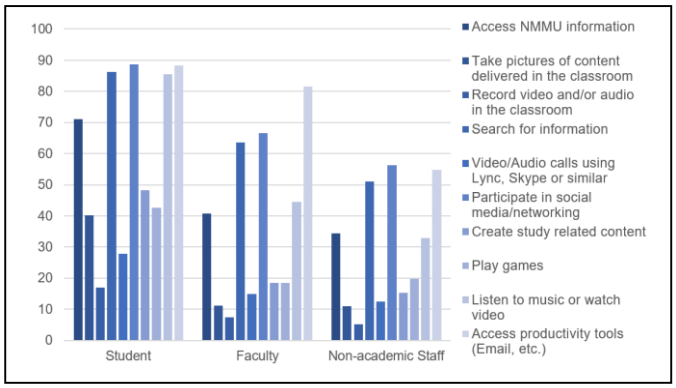

Figure 7: Student, faculty and non-academic staff smartphone usage for 3 or more times per week in 2015.

In 2015, students and non-academic staff primarily used their smartphones to participate in social networking followed by accessing productivity tools, such as emails, and to search for information. However, faculty primarily used their smartphones to access productivity tools followed by participating in social networking, and searching for information. Therefore, students and non-academic staff used their smartphones for similar purposes, while faculty shows a slight exception of accessing productivity tools more frequently than participating in social networking. The use of smartphones to access NMMU related information is also relatively popular among students, faculty and non-academic staff, as depicted in Fig. 7.

Fig. 8 illustrates what laptops were used for among students and staff in 2015. In Fig. 8 staff refers to both faculty and non-academic staff at the NMMU.

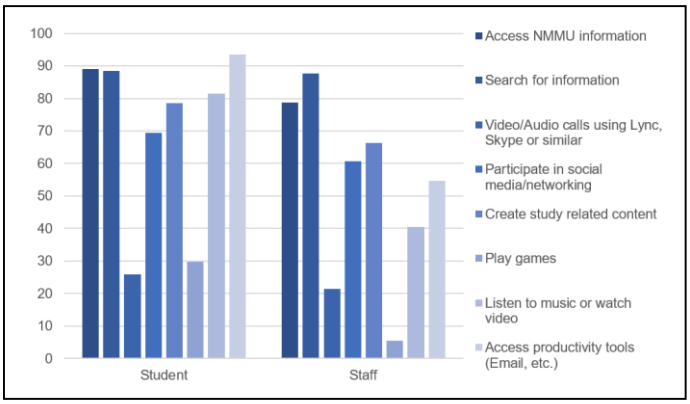

Figure 8: Student and staff laptop usage for 3 or more times per week in 2015.

In 2015, students primarily used their laptops to access productivity tools and NMMU related information as well as to search for information, as depicted in Fig. 8. Faculty and non-academic staff, however, mainly used their laptops to search for information, access NMMU related information and to create study related content such as presentation slides and worksheets, etc. Therefore, both students and staff used their laptops to frequently access NMMU related information and to search for information on the internet, as depicted in Fig. 8.

Fig. 9 illustrates what tablets were used for among students and staff in 2015, where staff refers to both faculty and non-academic staff.

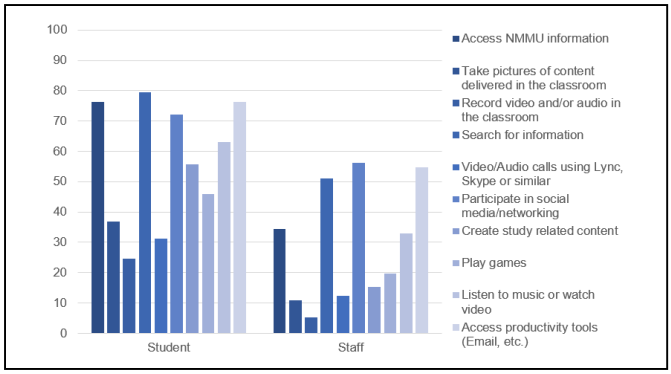

Figure 9: Student and staff tablet usage for 3 or more times per week in 2015.

In 2015, students primarily used their tablets to search for information followed by accessing productivity tools and NMMU related information, as well as participating in social networking. Whereas faculty and non-academic staff primarily used their tablets to participate in social networking followed by accessing productivity tools, searching for information, and accessing NMMU related information. Therefore, both students and staff primarily used tablets for similar reasons in 2015, as depicted in Fig. 9.

Fig. 10 illustrates which tools and technologies NMMU faculty are interested in using for academic purposes.

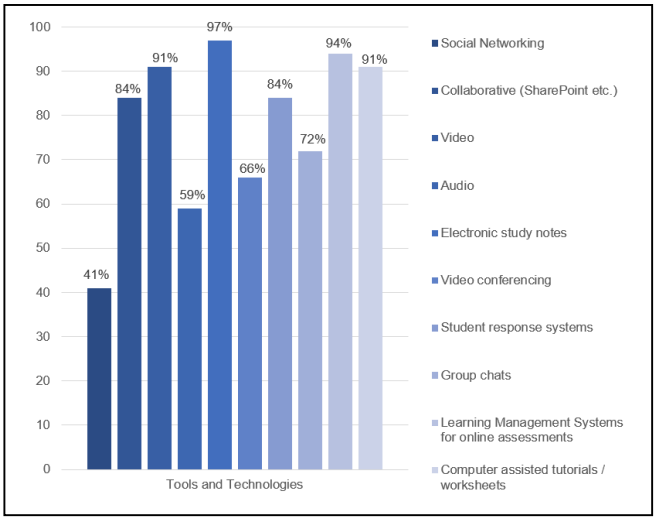

Figure 10: Faculty interest in technology usage for academic purposes in 2015.

This graph illustrates various teaching and learning assessment methods and the percentage of faculty interested in using them for academic purposes.

According to Fig. 10, faculty are mostly interested in using electronic study notes, learning management systems for online assessments, videos, and computer assisted tutorials and worksheets to aid teaching and learning methods at the NMMU. In 2014, 83% of students found that faculty are using technology to enhance their learning experience. This increased fractionally in 2015. Furthermore, students at the NMMU are currently receiving study material in various forms from faculty. Fig. 11

illustrates how NMMU students received their study material in 2015.

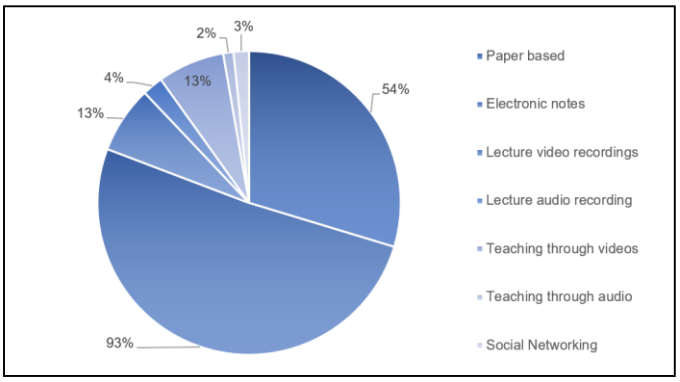

Figure 11: How students received study material from faculty in 2015.

In 2015, students primarily received their study material in the form of electronic notes, followed by paper-based study material. However, paper-based study material decreased by 7%, while electronic notes increased by 4% from 2014 to 2015. Teaching through videos and lecture video recordings were also relatively popular, but insignificant in comparison to electronic and paper based study materials.

From these results, it can be concluded that faculty are currently integrating technology into the curriculum to enhance students learning experience. In addition, there has been a significant increase in BYOD demand. The following section discusses key factors that higher education institutions should consider when dealing with this increased demand for BYOD usage.

V. KEY FACTORS

Given the predicted increase in mobile device usage at South African higher education institutions and the integration of technology into the curriculum, higher education institutions need to consider several key factors when dealing with the increased demand for BYOD usage as discussed in this section. These factors are derived from both literature and the case study data.

Mobile Device Management (MDM) – Some higher education institutions may consider adopting an MDM solution. Although not a new technology, MDM is only starting to gain in sophistication due to the invasion of employee-owned devices into the workplace [15] and because the number of confidential business information leakages via mobile devices has continued to rise [16]. An MDM solution can be seen as a partial system for the management of BYOD risks, such as data leakages, loss of organizational control and visibility, and ease of mobile device loss [15]. This is achieved through comprehensively managing mobile devices by monitoring their status and controlling their functions remotely using wireless communication technology such as Wi-Fi or Over-the-Air (OTA), as well as managing the required organizational resources [16]. Although relatively expensive, higher education institutions that can afford to implement an MDM solution should do so. However, it is essential for higher education institutions to realize that the implementation of an MDM solution is not necessarily sufficient to cope with the proliferation of devices on their campuses. Therefore, higher education institutions need to make sure their technology and policies deliver the data security and management efficiency they seek [17].

Since there are no commercial off-the-shelf solutions for MDM that work on every platform [18], and that all MDM solutions offer the same basic capabilities, choosing an MDM solution should not be based on technical security needs alone. Instead, it should be supported by non-technical elements of information security such as policies and processes [15].

Develop a concise and inclusive acceptable use policy (AUP) – Higher education institutions face a unique set of challenges when implementing BYOD [19]. These challenges are differentiated according to student, faculty and non-academic staff. Each user group brings with it a unique set of demands. Before developing an AUP, higher education institutions first need to determine the intended goals and results of the policy document [20]. These include outlining authorized use, prohibited use, systems management, policy violation procedures, policy review and specifying limitations of liability [21]. In addition, higher education institutions need to determine what systems, services, and sensitive data students, faculty and non-academic staff need to access using their personal mobile devices [19]. Furthermore, the policy needs to accommodate the uncertainty of emerging technologies that will continue to end up on campuses [19]. Therefore, institutions need to find a way to draft a policy that is sufficiently broad to allow for future technologies yet sufficiently detailed to be enforceable.

Data security – Higher education institutions need to review and implement appropriate safety measures to protect their students, faculty, non-academic staff, and databases populated with sensitive information [22]. However, for higher education institutions to achieve this, they need to consider various threats [23]. These include unauthorized access to sensitive data stored on the mobile devices; unauthorized access to data stored on the institution's network; attacks from malicious software; and the ability to impersonate an authorized user. In addition, sensitive data should be classified and encrypted [11].

Network infrastructure – Opening a higher education institution's network to student, faculty and non-academic staff mobile devices increases the strain on the institution's network [20]. Therefore, institutions need to ensure that their network infrastructure is capable of meeting the BYOD demands. To achieve this, institutions need to determine how many mobile devices students, faculty and non-academic staff have and ensure sufficient bandwidth is available to accommodate these devices [9]. In addition, they need to ensure that their network is maintained by the IT department [11]. Ease of access and quality of service also plays a major role, since students, faculty and non-academic staff will most likely expect 24/7 network access [9]. Several higher education institutions use network segmentation to improve performance and increase security [20]. This allows them to provide a network for students and a separate network to be used by faculty and non-academic staff, thereby avoiding data and security conflicts and protecting student information.

Develop a software infrastructure – In a BYOD environment, students, faculty and non-academic staff will use a variety of mobile devices. A significant challenge for any higher education institution is to provide software tools that can be utilized by their users on any device [20]. This requires considerable planning. Therefore, institutions need to make use of platform-independent tools, cloud-based storage, and web-based applications.

Develop a portal – Higher education institutions need to create a central location that collects software tools and other resources [20]. This provides students, faculty and non-academic staff with a central location from where they can access web applications, general information, distinct-licensed software and other educational resources.

Build a curriculum – Higher education institutions need to find a way to incorporate technology into the curriculum [20]. This will enable students to learn and complete assignments anywhere, anytime. Furthermore, students will most likely be encouraged to bring their personal devices to campus if the curriculum supports their use. In addition, faculty should be able to grade assignments quicker and send feedback to students using the LMS.

Provide ongoing education and training – Higher education institutions should find ways to educate students, faculty and non-academic staff of the dangers associated with the use of BYOD [24]. They should be made aware of ways to access and use data safely, as well as how they can protect sensitive information. Education and training should also include social media usage, personally identifiable information, strong passwords and privacy settings [25]. Without training and education, users could inadvertently put personal data as well as the institutions' data at risk. Furthermore, students, faculty and non-academic staff should clearly understand the appropriate and inappropriate use of their personal devices [3].

Address equity – Higher education institutions need to maintain equity among students by ensuring that no student is disadvantaged through the lack of available technology [3]. Several higher education institutions allow students who cannot afford their own mobile devices to loan devices from them [9]. It is essential that all students have equal opportunities in this regard.

Plan financially for sustainability – Higher education institutions need to be well-prepared for the possible challenges introduced by BYOD. Financial sustainability allows higher education institutions to plan ahead for mobility [22]. This will allow them to add devices to their network without adding strain. In addition, the allocation of funds is essential to enabling higher education institutions to follow through on their BYOD projects, plans, and the integration of technology [22]. Sufficient investment in bandwidth, infrastructure, personnel, and new technology is needed to provide a robust and scalable network infrastructure to support the increasing number of devices [3].

Help desk – A well run help desk is central to the smooth operation of a BYOD program. The role of the help desk should be expanded to cater for multiple devices and operating systems [26]. Furthermore, higher education institutions should ensure that processes, procedures and systems are in place so that technical support can be provided promptly and efficiently to students, faculty and non-academic staff [9].

Higher education institutions should consider these key factors when dealing with the increased demand for BYOD usage on campus.

VI. CONCLUSION

It is clear that higher education institutions in South Africa are observing a tendency in faculty and students that use their laptops, smart phones, tablets, e-readers and other mobile devices as a resource for enhancing their learning experience [10]. Furthermore, some higher education institutions may consider adopting an MDM solution to address the potential breach points associated with the implementation of BYOD. However, while MDM has some level of protection, the use of MDM alone is an insufficient resource for the implementation of BYOD [27]. Therefore, higher education institutions need to find more innovative and effective ways to safeguard valuable information and protect students, faculty and non-academic staff from security violations and data loss. The key factors discussed in this paper serves as a good starting point for higher education institutions. The ultimate goal should be for higher education institutions to safely provide enhanced learning resources to its students and to safeguard faculty and non-academic staff within their comfort zone. The explosion of mobile devices in higher education institutions is clearly cause for both celebration and concern.

Since this study only includes a single case, further research could include performing such a case study on other higher education institutions in South Africa. Furthermore, future research will consider the development of a framework to aid South African higher education institutions with the implementation of BYOD.

VII. ACKNOWLEDGEMENTS

The financial assistance of the National Research Foundation (NRF) towards this research is hereby acknowledged. Opinions expressed and conclusions arrived at, are those of the authors and are not necessarily to be attributed to the NRF.

REFERENCES

[1] Gartner, Inc., "Gartner Predicts by 2017, Half of Employers will Require Employees to Supply Their Own Device for Work Purposes," 1 May 2013. [Online]. Available: http://www.gartner.com/newsroom/id/2466615. [Accessed 28 May 2015].

[2] J. Roman, "BYOD: Get Ahead of the Risk," 1 November 2012. [Online]. Available: http://www.bankinfosecurity.in/byod-get-ahead-risk-a-4394. [Accessed 2 May 2015].

[3] T. Probert, "BYOD – an educational revolution?," *Educational Technology*, pp. 72-73, 2012.

[4] R. K. Yin, Case Study Research: Design and Methods 5th Edition, United States of America: SAGE Publications, Inc., 2013.

[5] C. Sliep, "Bring Your Own Device and Information Technology Service Delivery: A Higher Education Intitution Case Study," p. 165, 2013.

[6] Bradford Networks, "The impact of BYOD in education," May 2013. [Online]. Available: http://th-ebooks.s3.amazonaws.com/The_Impact_of_BYOD_in_Education.pdf. [Accessed 27 August 2015].

[7] J. Bichsel and E. Dahlstrom, "ECAR Study of Undergraduate Students and Information Technology, 2014," Educause, Louisville, 2014.

[8] M. Brown, J. Dehoney and N. Millichap, "What's Next for the LMS?," *Educause Review*, 22 June 2015.

[9] B. Stavert, "Bring your own device (BYOD) in schools," *NSW Department of Education and Communities*, 2013.

[10] K. R. Afreen, "Bring Your Own Device (BYOD) in Higher Education: Opportunities and Challenges," *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)*, pp. 233-236, 2014.

[11] R. Marchany, "Higher Education: Open and Secure?," *SANS Institute*, June 2014.

[12] Iowa State University, "Iowa State IT staff discover unauthorized access to servers," 22 April 2014. [Online]. Available: http://www.news.iastate.edu/news/2014/04/22/serverbreach. [Accessed 23 November 2015].

[13] K. M. Eisenhardt and M. E. Graebner, "Theory building from cases: Opportunities and challenges," *Academy of Management Journal*, vol. 50, no. 1, pp. 25-32, 2007.

[14] Republic of South Africa, "Higher Education Act 101 of 2003," 2003.

[15] A. Dedeche, S. Lajami, M. Le and F. Liu, "Emergent BYOD Security Challenges and Mitigation Strategy," *The University of Melbourne*, pp. 1-17, 2013.

[16] W. Jeon, R. Keunwoo and D. Won, "Security requirements of a mobile device management system," *International Journal of Security and its Applications*, vol. 6, no. 2, pp. 353-358, 2012.

[17] M. Davis, "BYOD: Why Mobile Device Management Isn't Enough," 20 11 2012. [Online]. Available: http://www.informationweek.com/it-leadership/byod-why-mobile-device-management-isnt-enough/d/d-id/1107487?. [Accessed 7 August 2015].

[18] D. Baranwal, S. Ravindran and R. Sadana, "BYOD in the Enterprise — A Holistic Approach," *ISACA Journal*, pp. 1-8, 2013.

[19] S. Difilipo, "The policy of BYOD: Considerations for higher education," *Educause Review*, pp. 60-61, 1 April 2013.

[20] Intel Education, "BYOD Planning and Implementation Framework," 2012. [Online]. Available: http://www.k12blueprint.com/sites/default/files/BYOD -Planning-Implementation.pdf. [Accessed 30 November 2015].

[21] A. Green, "Management of security policies for mobile devices," *Proceedings of the 4th annual conference on information security curriculum development*, 2007.

[22] A. S. Ackerman and M. L. Krupp, "Five Components to Consider for BYOT/BYOD," *International Conference on Cognition and Exploratory Learning in Digital Age*, pp. 35-41, 2012.

[23] I. Bernik and B. Markelj, "Mobile devices and corporate data security," *International Journal of Education and Information Technologies*, pp. 97-104, 2012.

[24] N. Hockly, "Tech-savvy teaching : BYOD Technology Matters," *Journal of Modern English Teachers*, vol. 21, no. 4, pp. 44-45, October 2012.

[25] S. Emery, "Factors for Consideration when Developing a Bring Your Own Device (BYOD) Strategy in Higher Education," *University of Oregon*, pp. 1 - 111, July 2012.

[26] B. Dixon and S. Tierney, "Bring Your Own Device To School," *Report by Microsoft Corporation*, pp. 1-16, 2012.

[27] E. B. Koh, J. Oh and C. Im, "A Study on Security Threats and Dynamic Access Control Technology for BYOD , Smart-work Environment," in *International Multi-conference of Engineers and Computer Scientists*, Hong Kong, 2014.