Available online at: http://journal.uinsgd.ac.id/index.php/kh
Khazanah Hukum, Vol. 5 No. 2: 105-129

DOI: 10.15575/kh.v5i2.28723

Navigating Legal Implications: The Impact of Enhanced Smartphone Integration on Security in Organizational Networks

Kenneth Ohei
Mangosuthu University of Technology, South Africa
Email: kennethohei@gmail.com

ABSTRACT

The escalating integration of smartphones within organizational frameworks has been driven by their augmented functionality, especially pertinent during the global pandemic. However, this surge in device utilization has concurrently amplified concerns surrounding security, as sensitive data becomes increasingly susceptible. In this context, the study conducted a survey to assess the security implications of smartphone integration while considering the legal aspects. The findings unequivocally substantiate the notion that smartphones pose substantial security risks, particularly when users stray from established protocols, potentially leading to legal consequences. Drawing from prior research emphasizing mobile devices' vulnerability, we advocate for a preemptive legal stance, suggesting the installation of anti-malware software on smartphones as a legally sound countermeasure. By doing so, organizations can thwart potential hacking endeavors, thereby not only fortifying network security but also mitigating legal liabilities and shielding sensitive information in compliance with relevant regulations. The implications of this study extend to organizational management and legal teams, enabling them to enact effective policies that reinforce network security and adhere to evolving legal challenges. This research underscores the significance of striking a balance between technological integration and safeguarding confidentiality within the boundaries of the law, offering essential insights for organizational resilience in an increasingly digitized landscape while avoiding legal pitfalls.

Keywords: Compliance regulations, Information technology (IT), Network security, Attacks, Security concerns, Telecommunication

ABSTRAK

Meningkatnya integrasi ponsel pintar ke dalam kerangka organisasi didorong oleh peningkatan fungsionalitasnya, terutama selama pandemi global. Namun, lonjakan penggunaan perangkat ini juga meningkatkan kekhawatiran seputar keamanan, karena data sensitif menjadi semakin rentan. Dalam konteks ini, penelitian ini melakukan survei untuk menilai implikasi keamanan dari integrasi ponsel cerdas dengan tetap mempertimbangkan aspek hukum. Temuan ini secara tegas memperkuat anggapan bahwa ponsel pintar menimbulkan risiko keamanan yang besar, terutama ketika pengguna menyimpang dari protokol yang sudah ditetapkan, sehingga berpotensi menimbulkan konsekuensi hukum. Berdasarkan penelitian sebelumnya yang menekankan kerentanan perangkat seluler, kami menganjurkan sikap hukum preventif, menyarankan pemasangan perangkat lunak anti-malware pada ponsel cerdas sebagai tindakan penanggulangan yang sah secara hukum. Dengan melakukan hal ini, organisasi dapat menggagalkan potensi upaya peretasan, sehingga tidak hanya memperkuat keamanan jaringan tetapi juga mengurangi tanggung jawab hukum dan melindungi informasi sensitif sesuai dengan peraturan terkait. Implikasi dari penelitian ini meluas ke manajemen organisasi dan tim hukum, sehingga memungkinkan mereka untuk menerapkan kebijakan efektif yang memperkuat keamanan jaringan dan mematuhi tantangan hukum yang terus berkembang. Penelitian ini menggarisbawahi pentingnya mencapai keseimbangan antara integrasi teknologi dan menjaga kerahasiaan dalam batas-batas hukum, memberikan wawasan penting untuk ketahanan organisasi dalam lanskap yang semakin digital sambil menghindari jebakan hukum.

Kata Kunci: Kepatuhan terhadap peraturan, Teknologi informasi (TI), Keamanan jaringan, Serangan, Masalah keamanan, Telekomunikasi

---

Received: May 20, 2023; Revised: August 10, 2023; Accepted: August 24, 2023

INTRODUCTION

Colin (2019) agrees that organisations network security experts need a written security policy. This will ensure that there is confidentiality and trust between organisations and mobile users, where data lose, and sabotage is avoided. The set of policies that are being implemented are to be used by the administration of IT in organisations. However, maintaining these policies may cause a lot of friction and pointless arguments which leads to nothing useful (Collin, 2019).

Mobile devices have effective abilities, more than personal computers (PCs), which can be found in people's pockets, purses, and bags (Chun & Maniatis, 2009). According to Schaeffer-Filho, Smith, Mauthe, & Hutchison (2014), mobile devices security has been neglected to the state of being attractive targets for attackers. Smartphone securities have not been up to date with traditional computer security (Schaeffer-Filho et al., 2014). The probing issue is that smartphones security has not kept bound with modern computer security (Holmes, Byrne, & Rowley, 2013). Mobile devices are likely to being attacked easily and cultured mobile malware that can be a threat to the confidential, integrity and availability (CIA) of the corporate system and the data in it. Mobile social networking applications sometimes lack detailed privacy controls (Jansen & Grance, 2011).

Jansen and Grance (2011) stated that, while mobile devices are taking on more abilities that were formerly available to technical security solutions, they keep failing network security. This means most mobile phone security depends on the user to make intelligent, cautious choices. Even the most careful users can still fall victim to attacks on their mobile phones.

Various smartphones have a password feature that locks the device but with the network attacks that exist, users can be hacked, and unlawful users can still access personal information (Aviv, Sapp, Blaze, & Smith, 2012). Permitting features, and by choosing a reasonably multifaceted password at the same time, can empower encryption, remote wipe capabilities, and antivirus software. Invaders can generate deceptive WiFi hotspots for the purpose of attacking mobile devices and may round public WiFi networks for indiscreet devices (Gherbi, Aliouat, & Benmohammed, 2017).

Network security model mostly needed to ensure security policies on mobile devices (Enck, Ongtang, & McDaniel, 2009). Mobile devices are defenseless to network security that run on them and in need of security policies because of the valuable resources that can monitor the devices (Parkinson & Khan, 2018). This is because of a lack of network security policies transparency. In certain African countries, it is difficult to identify a specific aspect of the university policy affecting users.

The high rate of policy changing that is frequently done without consulting with the users or making them aware, makes it easier for mobile devices to be attacked (Mukhopadhyay, Chatterjee, Bagchi, Kirs, & Shukla, 2019). This shows that, if the device is susceptible to several vulnerabilities, it will be at risk of network and cross-service attacks. Garfinkel, Juels, & Pappu (2005) mention that, equivalent policies that mobile devices undergo, create issues and risks that need to be carefully considered along with data retention and disposal issues that the network has.

At the crossroads of mobile device integration and organizational security, this research delves into critical legal aspects while investigating essential questions surrounding user awareness, institutional communication, and the potential of software administrative empowerment in the context of a university. The central inquiry goes beyond mere technological considerations and delves into whether users possess a comprehensive understanding of legally binding pre-configured policies governing mobile device usage for university-related tasks, emphasizing the potential legal implications of non-compliance. In the midst of escalating concerns over data leakage due to misuse or loss, the study also rigorously examines whether

the university effectively disseminates legally sound information about Mobile Device Management policies, elucidating the extent to which users are cognizant of protective measures within the boundaries of relevant data protection laws.

Furthermore, the research takes a legal perspective to analyze whether conferring software administrative privileges aligns with prevailing legal frameworks and enhances the university's capacity to bolster network security within lawful limits. By addressing these questions from a legal standpoint, the study aims to unveil potential gaps in policy awareness, communication strategies, and administrative empowerment that could have legal implications. This process sheds light on critical legal issues affecting organizational security and user compliance in the mobile device era, offering insights that can guide universities in navigating legal complexities while ensuring robust security measures and adherence to applicable laws and regulations.

LITERATURE STUDY

Cyber Security

Effiong (2013) pointed out how technology complicates the environment, whereby new treats and harmful activities are experienced with a limited focus and budget on security. There is no doubt in what mobile device can do nowadays which make them more acceptable and easier to work with rather than computers like in the early days. Lamey (2018) mentioned that people are currently living in a technological era where they can share information in an instant and are able to get information quickly. Without a doubt the Internet has made things lot possible to be done within a short period of time. Information can be easily accessed, however, with the availability of information on the Internet this has provided cyber criminals with a platform to take advantage of people. In many tertiary institutions, different crimes are being witnessed going from misconducts of examination, forgery of admission, theft, assault, and cultism amongst others . Based on recent studies cybercrime is currently experienced as a form of crime in tertiary institutions, which is reducing and exposing the economy of the nation (Shinde, 2002). With this happening as experienced in regions of Nigeria and many Western countries, commercial credibility is not recognised in employees who are appropriately using eCommerce.

Cyber Security in Universities

Higher education is different to what had been years ago, which now offers students and employees engagement through online learning systems and other supporting ones (Bandara, Ioras, & Maher, 2014). Today, understanding information systems and information technology is not an issue whereby learning strategies are provided within the internet. Balacheff et al (2009) has assured that wireless network platform is given to people in universities, therefore there are demand that comes with been able to access information on the net like how to be protected from all the mischievous activities that comes with it.

Furthermore, the focus on open data indicates a trend where raw underlying data is made more available through the net and with appropriate licensing, for reuse by third parties to increase its efficacy. Open data illustration needs appropriate data management practices throughout the lifecycle so that data is excellently conserved and published to be used by others. For online collaborative learning which included essential security properties such as availability, integrity, identification, access control, confidentiality can still control network from failure by using the approach based on the public key infrastructure models (Moneo, Caballe, & Prieot, 2012).

The identification and levelling of security controls at assured types of data can simply be accomplished with active association of data managers. These individuals are best positioned to identify properties, measure which kinds of controls will be most appropriate, that will ultimately be responsible for maintaining the integrity of systems and data (Ferman & İlhan, 2019).

Research in all fields for innovation and universities carry quantities of sensitive information to help advance and viable programs in areas such as healthcare, engineering, and technology and national defence (Mirzajani, Mahmud, Fauzi Mohd Ayub, & Wong, 2016). Universities are victims of cybercrime as they have become more established in society, which will make universities feel their share of the impact. Serious data will become a natural target for cyber-attacks.

Therefore, the danger will always be high for information to fall into the wrong hands. However, majority of universities have experienced damage to status and had to stop important projects or their work due to attack. As information or system breach can occur, this has the potential of impacting national security, due to possible sensitive nature of the information which could been compromised (Chen & He, 2013). This shows that individuals and organised people targeting the university and development data for a purpose also determined to get the information can compromise the institute to get to access on what they are looking for and universities must respond to this.

Knowledge/Information security

Universities should begin to conduct in-house audits of the network system risks, management priorities and systems when using mobile devices to do university work. The role of the IT department continues been important in protecting growth and reputation. IT department needs to work closely with the rest of the university departments so that the network system can be protected against hacking, cyber theft, and unforeseen activities (Von Solms, 2001).

Strange behaviours with the usage of mobile devices were observed by information security specialists (Talib, Clarke, & Furnell, 2010). They are all aware of the threats that could be unprotected but still there is no methods in strengthening the security of employees' phones. Androulidakis & Kandus (2011) also expressed causes for the harmful behaviour at hand, by looking at the mobile users and the fact that they are unaware of the possible measures that can be taken or even implemented for them to avoid security breaches.

Regardless the claims with these problems in hand and thinking if the security controls had been correctly placed this would have been avoided but there is a larger issue that is highlighted by these (Talib et al. 2011). These can take only one employee to be compromised or their device to be lost and without proper protection to their mobile devices they can easily be victims of malicious attacks. For the system to be attacked it only need one malicious insider to steal privileged information. Handling a problem space with many people can be difference between success and failure in an intimidating task (Bauman & Del Rio, 2006). As an alternative, these experts will tell the university the loss should be planned by explaining the on how the insurance and recovery options woks.

There are cases where application of security measure could work to reduce security rather than improve it. Hence, only the calculation of factors associated with information assets and seeing how much an investment would return, sadly this is easier said than done (Talib et al., 2011).

According to Kritzinger and Smith (2008) mobile phones are today's necessity for everyone even more important for employees of the university as the duties can be done through different devices. However, it also makes them vulnerable to security threats that may result in a loss of information. There

 ISSN 2715-9698 (online)

are many employees that are at disadvantaged just because there is a limited access to information relating to information security threats for them to be knowledgeable (Puhakainen & Siponen, 2010). Puhakainen and Siponen (2010) also mentioned how unlikely for competitors in more developed societies.

As there are ever-increasing security threats to mobile device information, Lacey (2010) continued by stating that users are not only the cause of security cases, then again also the prime means of checking, discovering, and determining security problems. Lacey (2010) further recommended a change in the use of an approach when making people aware of the security threats using interferences such as changing people's responsiveness, approaches and behaviour when coming to the use of technology. The Information Security Behaviour Profiling Framework (ISBPF) by Ngoqo and Flowerday (2015) proposed the framework to have better understanding and suggestions between awareness, attitudes and employees' information security behaviour.

Security Risks

According to Tweneboah-Koduah, Skouby, & Tadayoni (2017), mobile devices will continue to be targets to security threats whereby it may be physical device loss or misuse of application. Reality is this device now store or they are used for accessing sensitive data especially in workplaces. In educational environment, electronic learning system and it's concerned about their privacy and security when using the system. Robinson (2014) stated that often in higher institutions data is accessible to faculties and staff private data that can be reaches in many ways in which this day mobile device is one of the gadgets they use.

Therefore, guidance is needed as to security risks surrounding mobile devices on how to address various security risks at the university (Gordon, 2015). With connection of the Internet that can be accessed in multiple unsecure ways, and different security applications that users can make use of in accessing information that was only accessed by the desktop computers, this makes the mobile devices the subject of security breaches (Botha, Furnell, & Clarke, 2009). For safety on the devices there should be considerate to possible security risks related with mobile devices to progress a complete approach to mobile device security (Gordon, 2015).

Mobile wireless networks are usually exposed to security threats. The likelihood of eavesdropping, spoofing, and denial-of-service attacks should be carefully considered. Current link security techniques often apply within wireless networks reducing security threats. With the use of technology, employees have effects in term of integrity, confidentiality, and privacy (Ott, 2014). Therefore, information should always be secure as records, e-portfolio data, and should be safeguarded when using mobile devices in higher institutions. With security challenge university should ensure that employees have access only to required learning material and instruction regardless of the location.

Network attacks

Networks rely on numerous lines of protection, but with the use of mobile devices there are security concerns that keep expanding and organisation's system cannot bypass those traditional network securities (Goyal, Jabbari, Kearns, Khanna, & Morgenstern, 2016). Mobile devices are often exposed to malware and viruses that may be malicious to the network, this if objectively modified copies even delete important files to the point of compromising the server of the organisation (Guido et al., 2013). There are network attacks that are mainly found on mobile devices that comes as programs such as Cabir, Skulls,

DroidKungFu and many more which were written specifically to attack mobile phones in case of steeling files (Rogers, 2013).

At times recognising all devices and connections on network can be a tricky as per credentials a person can be connected on multiple devices. Each limit should be appraised to determine the kind of security controls necessary and how they can be best organised (Meidan et al., 2018). Boundaries between organisation's systems and others organisation that are nearby, and applying controls to ensure there are no misuse, or denial-of-service events that are rapidly contained and recovered from if they do occur. Without taking into considerations terms of service with all cloud service employees to ensure that organisation's information and activities are protected with the same amount of security that would intend to provide on personal devices.

Denial-of-service attacks may be directed at the web server or its supporting network infrastructure to prevent or hinder your website users from making use of its services. This can include preventing the user from accessing e-mail, websites, online accounts, or other services (Goyal et al., 2016). The most common attack occurs when the attacker floods a network with information, so that it can't process the user's request. Sensitive information on backend databases that are used to support interactive elements of a web application may be compromised through the injection of unauthorized software commands.

Cyber criminals may gain unauthorized access to resources elsewhere in the organization's network via a successful attack on the web server. Cyber criminals may also attack external entities after compromising a web server. According to Hoffman (2013) these attacks can be launched directly from the compromised server against an external server or by indirectly placing malicious content on the compromised web server that attempts to exploit vulnerabilities in the web browsers of users visiting the site. The server may be used as a distribution point for attack tools, pornography or illegally copied software.

Mobile Device Management

Although mobile devices are effective in business areas as it makes the day to be more productive, it creates IT security challenges and increase risks. In relation to using mobile devices for work related activities that workers have adopted, employees carry out important information, whereby the IT have no control of it (Henderson, 2011). Implementing Mobile Device Management is to enhance security and reduce the risk of an information breach of organisation information.

This service helps protect University information on smart phones quickly and easily. Whether it's a university-owned phone or a personal phone, if it's used to access campus information or e-mail, it must be securely configured. In a study conducted by Osterman et al (2012), a lot of employees are expected to use their mobile devices for work purpose whereby organisations cannot afford to buy employees devices. With Mobile device management it is not only secure also gives employees the opportunity to work anytime from anywhere, which will give satisfaction to the companies' benefits.

However, no principles have been established yet to evaluate whether such Mobile Device Management systems correctly provide the basic security functions needed by enterprises and whether such functions have been securely developed. Therefore, security requirements of a Mobile Device Management system by modelling a threat and applying a security requirement should be taken into consideration (Layland et al., 2012). The number of cases of confidential organisation information leakage through mobile devices has continued to rise.

 ISSN 2715-9698 (online)

Security Culture

Mobile devices have developed to the point that it became a personal behaviour to people owning them. The Increased productivity numbers to the organisation which moved the IT culture showing there is more embracement to it Cheng, Li, Li, Holm, & Zhai (2013). With more flexibility to the organisation, these portable devices of employees can control the workflow at the same time approaching the security issues that are regularly address. Although the majority of organisation avoid the use of mobile devices for work related activities. According to Muogboh and Ojadi (2018) to avoid altering security protocols and roaming to new policies reducing the risk increased exposure to cyber threats and data breaches.

When implementing security culture in organisations or high institutions, strategies need to be determined know how to support employees and secure its network (Karlsson, Denk, & Åström, 2018). This will illustrate which departments or employees will participate in the program, whereby functions that are beneficiary to strategies will be recognised by organisations. Backup and recovery are important as are to be addressed in the instance of a lost or stolen device. This is important to organisational security and for getting employee back to work and performing good in their duties (Muogboh & Ojadi, 2018).

Network Application

Advances in technologies have resulted in momentous progress towards approaches, requests, and development of applications (Beghriche & Bilami, 2018). Therefore, newly developed applications possibilities of considerably benefits for emerging of mobile networks allowing designers, developers, and researchers to manage and create mobile network applications. Sharma and Ramkuma (2017) mentioned that with wireless connections for mobile devices technology, connectivity of Mobile Ad hoc Networking (MANET) should progressively adapt mobile networking technology to effectively manage ad hoc network groups which can operate independently on them.

Mobile Application

Mobile application supply channels which transform mobile devices into App Phones, having the capability of downloading countless applications in an instant. There is support of ecommerce within organisational boundaries which benefits organisations and their employees in understanding the value of mobile applications (Murray, 2019).

Many organisations that try to find recruitment for social media in their employees' achievement efforts begin by uploading; promotion and educational material on YouTube, Facebook, or providing information about specific topics (Picazo-Vela, Fernández-Haddad, & Luna-Reyes, 2016). Engagement might be simply with information being reachable to others or might interact with sharing from kind of applications. These activities can help to create responsiveness and change attitudes among potential people.

According to Murray (2019), modern mobile phones are incorporated with browsing applications such as Opera Mini, Internet Explorer, Mozilla Firefox, used for sharing information resources through Infrared, Bluetooth, and WiFi. Mobile devices incorporate a sequence of structures used in several educational environments. Lecturers in higher education make use of SMS as quick access to students for course requirements, conduction of classes, pop quizzes to students and sending information about timetable and reminding students about important dates (Gikas & Grant, 2013).

AirWatch

AirWatch is a type of mobile device management which allows better security for smartphones, tablets, and most mobile devices that employees of the university are now privileged to use for their work (Kaufman, 2009). This is to secure the devices operation even when they are connected to secure WiFi networks (Pottie & Kaiser, 2000). The service is used to make sure that the existing university network will only enable you to access your data and e-mails therefore it needs credentials for information to be accessed.

Mobile devices have become more advanced the use of it is powerful even in the workplace. There is no longer much difference between mobile devices and traditional computers therefore the actions that are taken towards computers regarding securities must be considers with mobile devices (Osterman et al., 2012). This is to make sure that there would not be any experiences of data breach, the same way that is done with the computers of the higher institutions. According to (Kaufman, 2009) mobile devices with iOS, Android, and windows operation system Airwatch give it the ability to secure any data that may be sensitive information about the university.

Wireless Technology

Wired technologies have been in use for years, where lecturers, administration and students communicated though with either learning or teaching. However, universities are moving towards the use of wireless technologies (Abowd & Sterbenz, 2000). Wired technology provides limited access for usage because of its lack of mobility. This clearly shows, wired technologies cannot provide anytime, anywhere functionality benefit offered by mobile wireless technologies (Pottie & Kaiser, 2000). Zheng et al (2013) also stated that Although with the use of wireless technology there are security issues that people can experience. The use of unknown Wi-Fi settings, where unidentified applications can be downloaded connecting with untrusted sites.

RESEARCH METHOD

This study employs a quantitative research design, utilizing a structured questionnaire administered to 200 participants selected through purposive sampling from Northwest University (NWU). The questionnaire gathers data on universal factors influencing NWU employees, featuring both closed-ended and Likert-scale questions (Creswell & Creswell, 2017). The collected data are analyzed using descriptive and inferential statistics to uncover patterns, relationships, and trends. Findings are then systematically interpreted to derive meaningful insights, followed by the formulation of comments and recommendations aimed at addressing the identified factors. Ethical considerations are upheld throughout the research process, ensuring participants' informed consent, anonymity, and confidentiality. While acknowledging limitations, such as the chosen data collection method and sample size, this approach provides a comprehensive exploration of the employee-related dynamics at NWU.

RESULT AND DISCUSSION

Research Findings and Analysis

Out of the total of 200 questionnaires that were sent out to respondents, only one 162 were received back. Statistical insinuations and figures were used to discuss data collected (Creswell & Creswell, 2017).

 ISSN 2715-9698 (online)

With the attempt of getting all questionnaires back only 80% was received and that made the study compatible. The statistical sample illustrates that the sample meet rigorous rules that are randomly selected. All names were allocated a number and numbers were drawn. If somebody did not complete a questionnaire, the next number was drawn, and the person used. In this way the samples could be regarded as being representative.

Demographics

The focus of this study is on permanent employees owning mobile devices. On distributing questionnaires, 162 respondents both male and female participated in the study and were between the age of 25 and 65 years. Questionnaires were distributed amongst employees from the age of 25 -65 years including several departments in the university. Findings show that age groups 20-35 years and 36-45 years both had 49 respondents. Forty of the study respondents were between the age 46 -55 years, the remaining 24 of the respondents were between the age of 56-65 years.

Below age frequency table observations contained a total of 162 employees. Of those employees they fall in categories of age 25 to 35, 36 to 45, 46 to 55 and 56 to 65. Employees that are aged between 20 and 35 were (30.2%). The same percentage of 30.2 was age group from 36 to 45. Age group of 46 to 55 years had 40 employees who participated on the study which was 24.7% of them. The least employees that took part on the study were aged 56 to 65 years. Valid percent on the table below shows no difference between the column and the percentage column. This simply validates that there are non -missing respondents in the results. Hence cumulative percent column shows a 100% result of respondents.

Table 1. Gender Anova Table

ANOVA						
Gender	Sum of Squares	Df	Mean Square	F	Sig.	Bayes Factor[a]
Between Groups	2.060	4	.515	2.120	.081	.007
Within Groups	38.138	157	.243			
Total	40.198	161				

Table 1 above is a model showing different approaches in a regression command. This table show the break down features of gender and of which amongst male and female have the most working hours. The sum of square between the groups if 2.060 and within the groups is 38.138 showing that indeed male employees have the most working hours. The total of them all is 40.198. Degree of freedom is derived by the total number variables minus one. The study shows that between groups in frequency of 2.120 there is a slight (0.81) change of females having more working hours. This verifies the significance in results obtained.

Table 2. Bayesian Estimates of coefficients for working hours

Bayesian Estimates of Coefficients[a,b,c]					
Parameter	Posterior			95% Credible Interval	
	Mode	Mean	Variance	Lower Bound	Upper Bound
Working Hours = 1	1.800	1.800	.025	1.492	2.108
Working Hours = 2	1.545	1.545	.022	1.252	1.839
Working Hours = 3	1.415	1.415	.005	1.281	1.549
Working Hours = 4	1.484	1.484	.004	1.363	1.606

Working Hours = 5	1.292	1.292	.010	1.093	1.490

Table 2 shows than all variances are below 0. The credible interval is not relatively significant to the p-values this shows that the results are statistically significant.

Table 3. Employees having the most working hours.

			Working hours per week					
			10 or less	11 to 20	21 to 30	31 to 40	40 or more	Total
Gender	Male	Count	2	5	31	33	17	88
		Expected Count	5.4	6.0	28.8	34.8	13.0	88.0
		% within Gender	2.3%	5.7%	35.2%	37.5%	19.3%	100.0%
		% within Working hours per week	20.0%	45.5%	58.5%	51.6%	70.8%	54.3%
		% of Total	1.2%	3.1%	19.1%	20.4%	10.5%	54.3%
	Female	Count	8	6	22	31	7	74
		Expected Count	4.6	5.0	24.2	29.2	11.0	74.0
		% within Gender	10.8%	8.1%	29.7%	41.9%	9.5%	100.0%
		% within Working hours per week	80.0%	54.5%	41.5%	48.4%	29.2%	45.7%
		% of Total	4.9%	3.7%	13.6%	19.1%	4.3%	45.7%
Total		Count	10	11	53	64	24	162
		Expected Count	10.0	11.0	53.0	64.0	24.0	162.0
		% within Gender	6.2%	6.8%	32.7%	39.5%	14.8%	100.0%
		% within Working hours per week	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
		% of Total	6.2%	6.8%	32.7%	39.5%	14.8%	100.0%

The verdicts in table 3 reveal that 54% of respondents were male. This however is not in-line with the actual gender composition at Northwest university whose total workforce employment. 38% of male participants was from the working group of 31-40, which is the same as female participants with 42%.

Findings highligh the average working hours of employees per week. This was to compare working hours between employees of all age groups from 25-65 in North West University Mafikeng Campus. Discoveries shows that majority of employees between age group of 25-35 works more than 31 hours per week which is 23% of employees, hence it shows that they have the most working hours out of all groups.

As the age groups vary in the higher institutions, findings from the study shows the older the employees the less working hours obtained. Therefore, between ages of 36-55, employees' peak working hours is more than 21 hours per week whereby age group from 36-45 is leading with 21%.

According to Morrow (2012), escalation in web applications cloud computing contributes to employees' daily work, which increases access of information on devices without management by IT departments. Results show that many employees save their information on the mobile device as it is easy access in making them more productive regarding their work. Most of the respondents were from the Faculty of Economics and Management Sciences (FEMS) with 37 participants and 31 of them used their mobile devices as a form of information storage and the other 6 participants did not.

The support employees and employees from Faculty of Natural and Agricultural Sciences (FNAS) each with respondents of about 30 participants only 27 of them agreed that they use mobile device as a source of data storage in case of their work and 3-4 other participants did not prefer storing their information in their mobile devices. Faculty of Education with a total of 30 participants only 5 of them did

not store information on their mobile devices. With Faculty of Humanities, 23 employees took part in the study and 21 of them stored information in their devices whereby only 2 did not.

The least participants were from Faculty of Engineering and all 10 employees used their mobile devices as a form of storage for university information that they use daily. This simply shows that majority of employees in North West University are technically advanced and this makes them more productive in their daily work routines.

From all the 162 questionnaires distributed amongst six faculties in NWU Mafikeng campus, the above table 4 and 5 shows that about 142 respondents do store information on their mobile devices. Hence the remaining 20 respondents do not store information on the mobile devices this shows that the faculty does have an influence as seen in figure 3 that faculty of engineering all agreed.

Table 4 below is the independent sample test that shows the significant between two variables. As assumed in the Hypothesis that Storing of information on mobile device is influenced by respondents. Hence the frequency is higher that signification it is accepted to be true.

Table 4. Independent sample test for influence of faculty in storing on mobile devices 4.4.5

Independent Samples Test										
		Levene's Test for Equality of Variances		t-test for Equality of Means						
		F	Sig.	t	Df	Sig. (2tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference	
									Lower	Upper
Faculty	Equal variances assumed	.832	.363	-1.361	160	.175	-.595	.437	-1.458	.268
	Equal variances not assumed			-1.463	25.918	.156	-.595	.407	-1.431	.241

It is very essential that employees know what risks are there when using mobile devices in the framework of their daily lives. Currently many mobile devices can offer users the ability to check their e-mail status. Godwin-Jones (2017) argues that although this technology provides user convenience, there are problems that have raised.

Based on table 3 above, 88.86% of respondents that took part in the study agrees that they are familiar with threats that can attack their mobile devices. Along those respondents only 18.52% do not have a clue on threats that are harmful to mobile devices. 0.62% which is approximately 2 candidates that took part on the questionnaire did not answer the question.

In 162 respondents in table 5 that took part in the study, observations above shows whether employees are familiar with threats that can attack mobile devices. Of individuals that answered in the questionnaire some said Yes, No and other preferred not to answer. 18.5% of employees was not familiar with mobile device threats, which is 30 of them that said no. With percentage of 80.9 was respondents that where familiar with the threats. 0.6% which was only 1 participant preferred not to answer. 99.4% of employees answered. As there is no missing questionnaire, just 1 respondent preferred not to answer, hence 100% results in the cumulative percent column.

Table 5. Threats that employees are familiar with.

Which Threats Are You Familiar With					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Unsecure WiFi	40	24.7	24.7	24.7
	Network Spoofing	26	16.0	16.0	40.7
	Phishing Attacks	47	29.0	29.0	69.8
	Spyware	23	14.2	14.2	84.0
	Not aware	26	16.0	16.0	100.0
	Total	162	100.0	100.0	

SIM use toolkits have ability to allow applications admission functions and phone book entries to spread viruses with message sending. Wu, Chen, Wu, & Cardei (2007) stated that mobile users can easily be intercepted during message broadcast and could be modified by unauthorized parties after they reach data storing centre. For example, when a user clicks a link provided by the phishing mail, they may be connected to a website provided by the phishing mail and be tricked to download malware onto their devices.

In taking part in questionnaire respondents had to choose one of the familiar threats between phishing, spoofing, unsecure WiFi, spyware or if they are not aware. Twenty-four-point seven percent (24.7%) of respondents, which is 40 participants were familiar with Unsecure WiFi where is popular following phishing attack which leads by 29.0%. Respondents that were aware of network spoofing were 26 which is 16% of them that knew the attack. Only 14.2% of the respondents chose spyware as the familiar threat and about 16% where unaware of all the threads that were mentioned in the questionnaire.

Table 6. Case processing summary

Scale: Mobile Device for Work Purpose

Case Processing Summary			
		N	%
Cases	Valid	155	95.7
	Excluded[a]	7	4.3
	Total	162	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability table is commonly used for multiple questions in a questionnaire that uses a form of scale to determine if the scale is reliable. Table 6 above is a case summary of the use of mobile devices for work purposes, this was distributed to 162 employees. Of those participants 95.7% of them took part on the section and 4.3% which is 7 participants shows that they did not take part in the section.

The reliability statistics table provides the actual value for Cronbach's alpha that normally ranges from 0 and 1. For this section on whether mobile device is important for work purposes, it shows 0.516 alpha whereas the greater the coefficient, the higher the internal consistency of the variables.

Table 7. Univariate statistics table

Univariate Statistics							
	N	Mean	Std. Deviation	Missing		No. of Extremes[a]	
				Count	Percent	Low	High
Satisfaction	161	2.34	1.112	1	.6	0	0
Get Work Done	159	2.38	.884	3	1.9	0	0
Access Services	156	2.52	1.068	6	3.7	0	1
Gender	162			0	.0		

ISSN 2715-9698 (online)

In table 7 Variables that were codes in SPSS were of multiple question that are under the section of how purposeful it is for mobile devices to be used in the workplace. Employees were to answer if they get satisfaction from using mobile devices because mobile devices are always at reach, it is user friendly, consistent or for its flexibility. Therefore, 161 respondents, answered this question with only 1 participant that preferred not to answer. Between 98.1% of respondents 46.9% thought it is because using mobile devices user friendly and can get more work done where ever the person in. hence 18.0% thought it was because of the flexibility the mobile device has.

With whether the university will get more work done based on the new information technology 159 answered the question and only 1.9% did not take part in the question. 156 respondents answered the question where they were asked on whether the university policies using mobile devices, system quality can allow employees access to all services. In this case 43.2% of employees thought it will be user friendly for them to be able to access the systems, 34.6% which is 56 respondents thought it will show consistency in the university systems that they are being updated and that they will be able to access all systems.

Table 8. Use mobile devices for work purposes.

Item	**I get satisfaction from using mobile devices for my work because it is?**				**University will get more work done based on the new technology systems for reasons that it is?**				**With current policies and usage of mobile devices, all systems can be accessed allowing employees access information because it is?**			
Scale Range (1 - 4)	At reach	User Friendly	Consistent	Flexible	At reach	User Friendly	Consistent	Flexible	At reach	User Friendly	Consistent	Flexible
Percentage	34%	26%	21%	18%	13%	48%	19%	15%	20%	22%	15%	38%

According to Seppala and Alamaki (2003), the goal of innovative preliminary projects is to create flexible teaching solutions, which will enable access to information using different devices, and support learning in a variety of situations. Some promising approaches are looked at in considering limitations. Several issues to be dispensed from three essential properties of mobile computing: communication, mobility, and portability (Seppälä & Alamäki, 2003). Of course, special-purpose systems may avoid some design pressures by doing without certain desirable properties.

Table 8 above shows the usage of mobile device for work purpose, three questions were asked and had to be answered with a scale range. The range is based on mobile devices in whether it as at reach, user friendly consistent or flexible to use it for work purposes. 34% of respondents believed that they get satisfaction when using mobile devices for work purposes because it is always at reach most of the time. 26% of the participants thought because it is user friendly. Because people are always on their mobile devices and checking their e-mails, it becomes consistent to keep doing their work and 21% of respondents agrees with that. With mobile devices, as it is portable, 18% of respondents thinks that it is flexible and gets satisfaction in getting work done.

University will get more work done based on the new technology systems, majority of respondents thought that it is user friendly with 48%. 13% of respondents thought that their mobile devices are always at reach and are smarter can also install latest technology systems. People are always checking their mobile devices; it becomes consistent to keep working and 19% of respondents approves so. With mobile devices being smarter 15% of respondents thinks that it is flexible getting more work done. With current policies and usage of mobile devices one must be careful in protecting themselves from being victims of cyber-attacks. Especially with the use of bring your own device to work policy all systems can be accessed in mobile devices and can access all information regardless how fragile it is. In case of promoting e-learning this is a good opportunity to higher institutions as employees will be able to access the workload or whatever information needed at that point. In 162 participants that took part on the questionnaire 20% of them thought that this was best as the devices are at reach most of the time. 22% of them thought it was because the systems were made to be user friendly to employees. With the consistent option only 15% opted for that category. Nowadays everyone wants to work at their own comfort so 38% of respondents thought being able to access the system was a sign of flexibility.

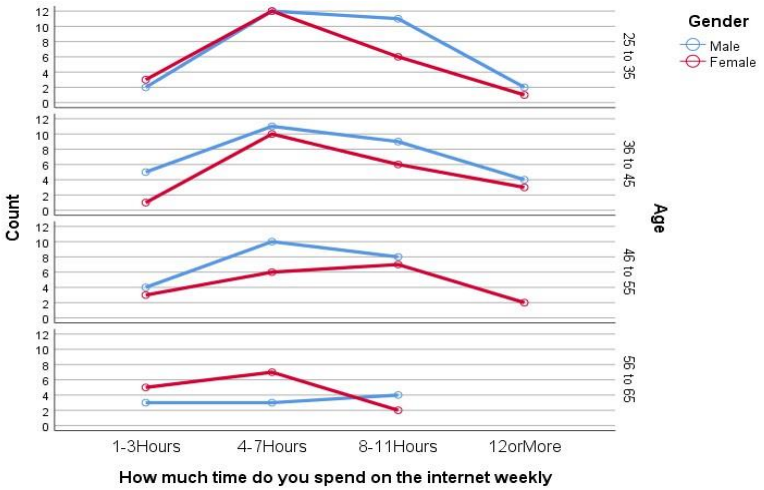

Figure 1. Time spend on the internet weekly.

Above is Figure 1 where it shows time spent on the internet weekly is categorized according to age groups of respondents that took part on the study. It shows that the older you became the less time you spend on the internet according to this research group. In 162 respondents that took part on the study based on all age groups and gender the usage of internet starts to increase rapidly from 1-3 hours of internet use.

All groups reach their peak point between 4-7 hours of internet usage whereby age group between 25-35 both gender-race are the highest. In all age groups majority of male participants uses internet especially between 8-11 hours. The internet usage deceases from 12 hours and more and between age group of 46-55 and 56-65 is shows that only female participants use the Internet.

The Pearson correlation table shows little relationship between age and working hours and whether the two variables have an influence on time spend on the internet weekly. The sample size is of 162 respondents that took part on the study with no missing response. It shows that in all the variables Pearson correlation has a strong relationship as seen on Table 13 the matrix of all variables is 1.

With working hours as a variable that has an influence on time spend using the internet there is a positive correlation as it is 0.149 showing that both times spend on the internet and working hours

 ISSN 2715-9698 (online)

increase in value. Age also influence time spend on the internet by -0.160 it shows a negative correlation whereby when one variable increases the other decreases in value. The statistically significant correlation is 0.05 that shows that the variables are related and strongly correlates.

Table 9. Reliability Statistics

Reliability Statistics	
Cronbach's Alpha	N of Items
.516	3

Table 10. frequency table where employees verify applications before downloading.

	N	Minimum	Maximum	Mean	Std. Deviation
Do you verify application before downloading them	162	1	3	1.56	.510
Valid N (list wise)	162				

Employees where asked if they do verify applications before downloading them. With only three participants that decided not to respond. Table 9 and 10 above shows that the statistics that were collected during the study is significant and proven by the standard deviation. As most people are becoming victims especially in phishing attack this can sometime be because they are not careful enough in protection themselves when installing or downloading applications. Figure 1 above shows how the respondents answered on whether they verify application before downloading them. This question was to look at if people are just downloading application or knows the proms that comes with the application. About 89 of the respondents out of the 162 that took part agreed on verifying the applications to be downloaded before taking feather actions. Seventy-two (72) of the respondents did not check when installing a downloaded application on their mobile devices.

Figure 2 discuss the types of databases whereby employees can back up their information. In all 162 respondents that took part in the study 19 of them stored or backed up their information regardless of if it was work based or not on Cloud-Based. Majority of respondents used Drop-Box for backing up their information and this is 64 of them. With Google-Drive based on the response that was collected 41 of participants made their back up on that type of database. As this one is mostly assessable to employees of the university on their work desktops, 37 of respondents used it for backing up the data.

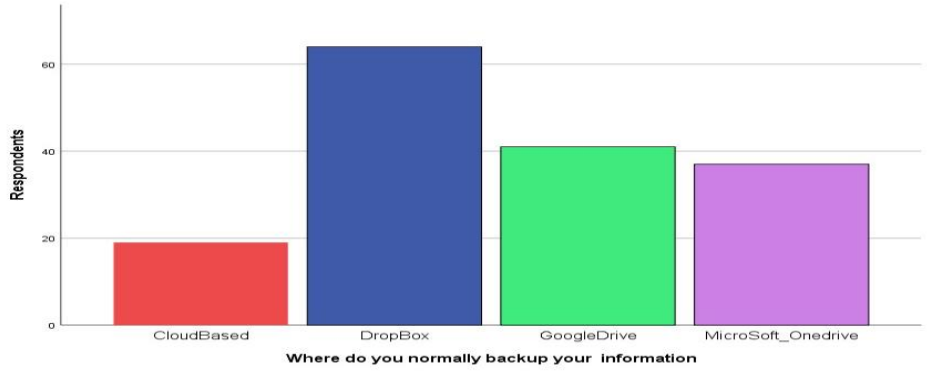

Figure 2. were employees normally backup information.

In guidance to security risk surrounding mobile devices, the is a way in which vulnerabilities are to be addressed and various security risks at the university Gordon (2015). With connection of the internet

that can be accessed in multiple unsecure ways, and different security applications that users can make use of in accessing information that was only accessed by the desktop computers, this makes the mobile devices the subject of security breaches (Botha et al., 2009).

Table 11 above shows vulnerabilities in usage of mobile device in whether employees are aware of the security risks aligned using devices for work purposes. Three questions were asked to look at the level of knowledge the employees have and had to answered with a scale range of if they agree, strongly agree, disagree, or strongly disagree. It was asked if mobile device security should increase for flexible mobile device usage and 63 participants strongly agreed on that point, followed by 72 of them which also agreed that security should be increased. 26 of the rest of the participants did not think it was necessary for the security to increase, with which 20 of them strongly disagreed and only 6 of the disagreed.

Respondents were asked on the awareness that they had in whether they were supposed to protect the university data even in the use of mobile devices for work purpose. Majority of the respondents said they were aware of having the responsibility to protect the university data on the use of their mobile devices. Hence 21 of them strongly agreed on been aware of this condition. 65 of the respondents agreed on knowing about the data protection. Some of the respondents were not aware that they are supposed to protect the university data. In which 32 of them strongly disagreed on this and 44 disagreed on this condition.

As mobile devices need to constantly be updated participants were asked if updating anti-virus on the devices reduces the risks of cyber-attacks. Most employees thought keeping mobile device updated was a good thing to do to reduce security vulnerabilities. 56 of the respondents strongly agreed on updating anti-virus regularly and 70 of them agreed on this condition. Only a few of them disagreed on this matter in which only 22 of them strongly disagreed and 14 disagreed.

Correlation between these variables was to check if there is a relationship on whether 162 employees that participated are aware of the vulnerabilities that they can face when using mobile devices. The Pearson correlation in Table 11 shows only 161 responded on the relationship between two variables of flexible access and vulnerabilities which is clear that they strongly correlate by 0.517 while increasing in value.

The significance of these two variables is 0.13, concluding that there is inflation in both variables. On being aware of protecting university data while using mobile devices, the response was compared to the vulnerabilities the university faces. Therefore, it shows in the above table that the variables had 0.21 correlations which represented weak correlation between the two variables. Significance of 2 tailed between protecting university data and its vulnerabilities is 0.795, concluding that there is no statistical significance as the means of increase variable does not relate to the other.

Pearson correlation for all three variables is from 0.5 as the vulnerability column is the average answer to all the questions as answered in the questionnaire, hence the strong correlation relationship between the variables. The variables are statistically correlated with 0.01 and 0.05 showing the relation and inflation in the variables. The correlation table answers the research question: Is the university network vulnerable to modern mobile devices? Clearly showing that employees think that using mobile devices university network is indeed vulnerable.

Table 12 above discusses communication safety of mobile devices especially when dealing with a large group of people. Morrow (2012) stated that valuable information should be protected, organisations must stop making distinction between devices in the complex network and outside of it. The question was analysed based on the faculty and how the agree or disagree with this condition. Higher population of employees agreed that mobile devices are safer even when dealing with a large group of people in this case

 ISSN 2715-9698 (online)

students. Seventy (70) respondents agreed on the safety of the devices whereby majority of them was from Support. It was a tie between faculty of economics and management sciences and faculty of natural agricultural sciences with 9 respondents from both departments and this came up to 33 respondents that strongly agreed on this condition. Twenty-two (22) respondents strongly disagreed on mobile devices being safe for communication in large groups of people and 36 disagreed.

Data show that if by restricting access to application that are not work related will reduce security threats mobile devices can undergo. Between two variables that was evaluated, 161 employees who answered questions of whether the university should restrict mobile devices from accessing other applications not related to university work ethics, and if mobile devices should be safe from all the security threats even on employee-owned devices through storing corporate data and retrieving it from corporate network.

The relationship between the two was detained using Pearson correlation, showing 0.001. This means first variable did not correlate with the changes of the second variables, hence the weak correlation between the two. Table 19 shows a positive correlation which is both variables decrease in value. There is no statistical significance between the two variables because the 2 tailed value is 0.995 as of the decrease in the employee-owned devices does not relate to restricting mobile devices.

Correlation was amongst the questions related to how mobile devices should be safe from all the security threats even on employee-owned devices, through storing corporate data and retrieving it from corporate network, in whether the university restrict mobile devices from accessing other applications not related to university work ethics and University should make it part of the employee package to ensure that they get more security for their mobile devices. Evaluate to check whether there is a relationship between these questions that were answered by employees. Above in Table 4.20 is the Pearson correlation showing how these variables have an influence on each other. Of all the respondents of 162 employees, only 1 employee preferred not to take part.

With Employee-Owned Devices being a dependent to University Issue Own Devices and Employee Package decrease in value with a positive correlation of 0.133 and 0.135. For two variables, there are not statistically significant between the variables. Although University Issue Own Devices being a dependent to Employee-Owned Devices with a person correlation of 0.138 there is a positive correlation even though it was a weak one. Employee Package variables strongly correlated with each other with the value of 0.364, as both variables increased in value. There is a statistically significance with 0.000 showing inflation of variables relates. The statistically significant correlation is 0.01 that shows that all variables are related and strongly correlates.

With the BYOD policy being at use certain actions needs to be taken to protect the critical data of a person's workplace. The research question on if current policies ensure mobile devices security in Mafikeng Campus, as perceived on the above table 10 employees did not fully agree on this condition. Mobile devices are often classified as smart; their operating systems and security characteristics have quickly progressed as has the trust upon them by organizations to conduct business (Banks, 2010). The infrequent blend of personal and business use for these devices creates numerus challenges to managing their risk. This study shows in Figure 8 that 95% of respondents that took part agreed on ha ving a yearly awareness in security issues to be educated on how they can reduce risks of been attacked or being victims of cyber-crime. Five percent (5%) of respondent felt like there was no need of awareness in security risks facing users of mobile devices.

Table 11. Bayesian Estimates of Coefficientsa,b,c on Employees need awareness in mobile device security threats

Bayesian Estimates of Coefficients[a,b,c]					
Parameter	Posterior			95% Credible Interval	
	Mode	Mean	Variance	Lower Bound	Upper Bound
Familiar With Treats = 1	1.267	1.267	.013	1.041	1.493
Familiar With Treats = 2	1.374	1.374	.003	1.266	1.482
Familiar With Treats = 3	3.000	3.000	.398	1.761	4.239
a. Dependent Variable: Yearly Awareness					
b. Model: Familiar With Treats					
c. Assume standard reference priors.					

Table 11 shows that all variances are above 0, therefore the above table concludes that the hypothesis is alternative. This is to show the claimed hypothesis of the researcher is true employees agreed that there is a need of awareness to make them be alert of the securities. The credible interval is relatively significant to the p-values this shows that the results are statistically significant. This answers one of the measures to be taken for mobile security issues to be avoided in university.

Are university policies protecting you if the device is being under attack Table 4.22 above reveals how employees feel about this condition whereby most of them disagreed on being protected by the university if they were to experience an attack and lose the data. Sixty-eight (68) of those respondents said they disagree on feeling protected and 32 strongly disagreed. However, 48 agreed that there was protection from current policies if they were to lose data and 12 of them strongly agreed. 4.7.18

In those participants that took part on the study mostly agreed on the fact that the university should have a stronger firewall for software-based network security system that allows or block traffic into network based on a set of rules. Eighty-five (85) respondents strongly agreed on having a firewall and 64 agreed this is about 92% of employees that agreed that for the university to have secure information they should have a stronger firewall, hence only 8% disagreed on that manner where 8 respondents strongly disagreed, and 5 respondents disagreed.

Summary of The Results

Because of the large amount of misuse occurrences, it important to understand how to reduce possibility of being attacked while using mobile devices and how to protect work ethics of corporate environments. General restriction can be suggested on certain levels to control work and be restrictive by reducing alleged threat of punishment for IS misuse. Although services through mobile devices can be convenient, it still has many security issues, which is a huge problem when sensitive information gets leaked.

The concept of electronic learning, which is a products or services using computer networks, is particularly well suited for use within mobile computing. Mobile learning, a branch of electronic commerce, refers to the transmission of data through wireless technology. It includes the use of mobile information terminals to participate in various activities, which is a new kind of an e-learning capability to get more work done in ones working space. This chapter captured and presented the data according to the statistical analysis. From the findings, it is evident that deficiencies exist in the overall management of mobile device security and must be addressed to educate employees on how to be cyber-attack free.

Answering to Research Questions

How is the university network vulnerable to modern mobile devices?

 ISSN 2715-9698 (online)

Universities are finding employees more productive when using mobile devices, and benefits are too great to ignore. The liberation factors impose on mobile device security issues, the security risks within the university administration which is important in the case of promoting intelligence in Information technology and its massive growth of modern mobile devices (Gordon, 2015).

Users are three times more likely to respond to a phishing attack on a mobile device than a desktop, according to Gordon (2015), in part simply because a phone is where people are most likely to first see a message. While of users click on phishing-related links, according to Freiberger-Verizon & Watts-Verizon (2018). Corporate mobile devices use Wi-Fi almost three times as much as they use cellular data. Nearly a quarter of devices have connected to open and potentially insecure Wi-Fi networks, and of those devices a man-in-the-middle attack in which someone maliciously intercepts communication between two parties within the most recent month. As mobile devices need to be updated constantly, participants were asked if updating anti-virus on the devices reduces the risks of cyber-attacks. Most employees thought keeping mobile device updated was a good thing to do to reduce security vulnerabilities.

Which measures are to be taken for mobile security issues to be avoided at the university?

In those participants that took part on the study mostly agreed on the fact that the university should have a stronger firewall for software-based network security system that allows or block traffic into network based on a set of rules. Eighty-five (85) respondents strongly agreed on having a firewall and 64 agreed this is about 92% of employees that agreed that for the university to have secure information they should have a stronger firewall.

This study shows in Figure 2 in chapter 4 that 95% of respondents that took part agreed on having a yearly awareness in security issues to be educated on how they can reduce risks of been attacked or being victims of cyber-crime. Five percent (5%) of respondent felt like there was no need of awareness in security risks facing users of mobile devices. Therefore, there university should consider these measures to ensure the safety of their data.

What are the perspectives of current policies ensuring mobile devices security at Mafikeng Campus?

Table 4.20 in chapter 4 answers the last research question whereby, with the BYOD policy being at use certain actions needs to be taken to protect the critical data of a person's workplace. The research question on if current policies ensure mobile devices security in Mafikeng Campus, as perceived on the above table 12 employees did not fully agree on this condition.

Murtagh & Legendre (2014) mentioned that with network attacks in universities, the likelihood of controlling them is commonly failed to be addressed, with security issues where mobile devices have made it easier for hackers to exploit systems which may compromise sensitive data. According to Seppala and Alamaki (2003), the goal of innovative preliminary projects is to create flexible teaching solutions, which will enable access to information using different devices, and support learning in a variety of situations.

With current policies and usage of mobile devices one must be careful in protecting themselves from being victims of cyber-attacks. Especially with the use of bring your own device to work policy all systems can be accessed in mobile devices and can access all information regardless how fragile it is. In case of promoting e-learning this is a good opportunity to higher institutions as employees will be able to access the workload or whatever information needed at that point. In 162 participants that took part on the questionnaire 20% of them thought that this was best as the devices are at reach most of the time. 22% of them thought it was because the systems were made to be user friendly to employees.

Discussion

The major objective of the study was to investigate whether NWU employees are aware of security concerns associated with mobile devices. Therefore, to fully understand the purpose of the study, the researcher drew questions that will fulfil and explain the meaning behind each of the above research objective.

To Determine the Impact of Network Securities That can be Improved in NWU Mafikeng Campus to Ensure the Safety of Mobile Devices.

The first objective stresses the impact of network securities that can be improved to ensure the safety of mobile devices. From the findings, it is evident that most respondents were aware and familiar with mobile device threats and only few had no clue of these threats. Also, at least 50 respondents mentioned that they spend at least 8 to 11 hours on the internet weekly which can leave them vulnerable to online attacks. Until NWU can make their employee's mobiles devices against security threats, they cannot risk spending a lot of time on the internet.

This action will give attackers enough time to track their devices and access their information. Therefore, the university should take measure in ensuring safety from all the security threats even on employee-owned devices through storing corporate data and retrieving it from corporate network. Shammar and Zahary (2020) stated there are serious concerns about the danger on the growth of technology, particularly regarding privacy and security; hence the university should start addressing these concerns. Findings revealed that respondents agree that if the university could create yearly awareness of security issues associated with mobile devices, this will reduce the risks of the attacks.

To Consider Influential Network Policies Available in NWU for Protecting the Security of Mobile Devices.

The second objective shows concerns about policies that are and should be in place, which influences the protection for network security of mobile devices. The findings presented demonstrates that many employees disagree that the university hasn't bothered in taking measures to protect their data when allowing its employees to use personal owned devices. Respondents therefore believe that their information will be secure if they were accessing their data from devices issued by the university.

Personal owned mobile devices of NWU employees' poses threats because they do not restrict users from any sites, even those that appear to be harmful ones. According to (Tamin, 2017) users should trust Information security management in context of mobile commerce. Therefore, if the university were to issues its own devices to access only university data, the devices wouldn't allow users to access unknown sites or anonymous sites that may harm university data. Preventing possible infection would mainly rely on mobile users' appropriate behaviour (Dang-Pham & Pittayachawan, 2015). The devices would also keep track of user ID, what sites they visited, how long were they online, what files were accessed and so on. Since the university isn't issuing its own devices to their employees for security measure purposes, for now it should have a strong firewall for software-based network security that allows or block traffic into a network based on a set of rules. Furthermore, employees also agree that the university should make it part of the employee package to ensure that they get more security for their mobile devices.

 ISSN 2715-9698 (online)

To Assess the Vulnerabilities of the Modern Mobile Devices in Network Security.

The third objective is apprehensive with network security concerns that may pose threats to mobile devices of NWU employees. The finding presented in Chapter 4 show that more than 130 respondents agrees that mobile devices security should be increased and made flexible for access to university data. This proves many are finding the university security weak with large room for improvement. This causes, or rather lead and spark an idea in each individual employee in the NWU Mafikeng campus that they should be alarmed of protecting their own university data stored in their mobile devices. An adversary can eavesdrop, delay, drop, replay, and modify messages and masquerade as any sender (Egners, Marschollek, & Meyer, 2012), hence the university needs to improve security approaches addressing attacks against the network. This means there should be an implementation of a virtual machine manager which will become the trusted base.

Since the university is dragging their feet in implementing an advance security measure against vulnerabilities of mobile devices in network security, their employees cannot keep on depending on them to keep their personal information safe. Hence, they use their own personal mobile devices to keep some of their information.

Other findings presented in the previous chapter that support the third objectives are of those related to employees updating their mobile device anti-malware. This, however, enables their mobile devices to be more secure from network vulnerabilities, enabling them so securely access their university information without having to worry about unauthorized users.

Legal Implications and Recommendations: Safeguarding University Mobile Device Security

In the evolving landscape of mobile device integration within university settings, it is imperative to comprehend the legal dimensions of ensuring data protection and security (Dwivedi et al., 2020). This section delves into the legal implications arising from potential breaches, examines legal awareness and compliance, discusses the alignment of Mobile Device Management (MDM) policies with data protection laws, evaluates Bring Your Own Device (BYOD) policies in terms of legal considerations, and explores the role of legal safeguards in enhancing security.

A fundamental facet illuminated by this study is the need for heightened legal awareness among university employees. The findings underscore that a substantial proportion of respondents lack a comprehensive understanding of the legal ramifications associated with security breaches linked to mobile device usage. Universities have a duty to promote legal education and awareness programs that enlighten staff about the legal risks entailed in mishandling data or engaging in unsafe online practices (O'Connell & DiFonzo, 2018). Transparent communication of legal obligations can significantly boost compliance, fostering a more secure digital environment.

The research accentuates the significance of effectively disseminating MDM policies. However, this dissemination must be coupled with policies that stand up to legal scrutiny and adhere to data protection regulations such as the General Data Protection Regulation (GDPR) or Health Insurance Portability and Accountability Act (HIPAA), depending on jurisdiction. Collaboration between legal and IT departments is paramount to crafting policies that safeguard sensitive information while respecting users' rights and privacy. The integration of legal expertise in policy formulation ensures that data security is promoted within the boundaries of the law.

While Bring Your Own Device (BYOD) policies offer flexibility, they introduce complex legal considerations. The research underscores the necessity for universities to harmonize convenient access to information with the protection of critical data. Legal teams must review BYOD policies to encompass the legal implications related to staff accessing university data on personal devices. With the potential for unauthorized access and data leakage, legal experts should collaborate with IT departments to draft policies outlining acceptable use, data handling, and security measures, all aligned with pertinent laws.

The study identifies a prevalent sentiment among respondents advocating for a stronger firewall for network security. Legal collaboration with IT departments is vital to assess the legal implications of implementing advanced security measures such as firewalls. These measures must not only uphold the university's interests but also safeguard the rights of users. In addition, legal professionals can play a pivotal role in framing clauses within employment contracts or service agreements that require staff to adhere to security protocols. This proactive step minimizes legal risks arising from potential negligence.

In the intersection of mobile device integration and organizational security, legal considerations stand as a linchpin (Goggin, 2021). This research underscores the pivotal role of universities in embracing not only technological measures but also legal awareness, compliance, and alignment with data protection regulations. By weaving legal expertise into the fabric of policy development and practices, universities navigate the intricate realm of mobile device security with finesse, thereby mitigating potential legal liabilities. This collaborative approach ensures that organizational security is bolstered within the contours of the law, ultimately fostering a safer digital environment that is conducive to both academic excellence and efficient administrative functions.

CONCLUSION

In an era characterized by rapid mobile device evolution, this study's focus on bolstering mobile device security within the NWU context underscores the paramount importance of aligning security practices with legal considerations. The study's findings reveal alarming gaps in user awareness and familiarity with data protection technologies, which necessitate immediate attention. The overarching strategy recommended herein entails raising user awareness about security risks while concurrently implementing legally compliant anti-malware software to proactively counter potential threats. NWU's journey within the digital landscape necessitates a harmonious convergence of technological innovation and legal safeguards. The study's insights underline the significance of informed users fortified with legally sound anti-malware solutions, effectively erecting a resilient defense against security breaches. By executing this multifaceted strategy, NWU not only fulfills its commitment to technological advancement but also adheres to legal and ethical standards, thereby cultivating a secure digital environment. In conclusion, this research underscores the intrinsic connection between legal compliance, user awareness, and robust security, offering NWU a pathway to navigate the digital frontier with confidence and legal acumen.

REFERENCES

Abowd, G. D., & Sterbenz, J. P. G. (2000). Final report on the inter-agency workshop on research issues for smart environments. *IEEE Personal Communications*, *7*(5), 36–40.

Androulidakis, I., & Kandus, G. (2011). Mobile phone security awareness and practices of students in budapest. *Proceedings of the 6th International Conference on Digital Telecommunications*, 17–22.

Aviv, A. J., Sapp, B., Blaze, M., & Smith, J. M. (2012). Practicality of accelerometer side channels on smartphones. *Proceedings of the 28th Annual Computer Security Applications Conference*, 41–50.

Balacheff, N., Ludvigsen, S., De Jong, T., Lazonder, A., Barnes, S.-A., & Montandon, L. (2009). *Technology-enhanced learning*. Springer.

Bandara, I., Ioras, F., & Maher, K. (2014). Cyber security concerns in e-learning education. *ICERI2014 Proceedings*, 728–734. IATED.

Banks, L. (2010). Mobile devices pose security dilemma for CIOs. Retrieved May 13, 2023, from Ananalysis based on PCT patent applications website: http://www.cio.com.au/article/346474/mobile_devices_pose_security_dilemma_cios

Bauman, S., & Del Rio, A. (2006). Preservice teachers' responses to bullying scenarios: Comparing physical, verbal, and relational bullying. *Journal of Educational Psychology*, *98*(1), 219.

Beghriche, A., & Bilami, A. (2018). A fuzzy trust-based routing model for mitigating the misbehaving nodes in mobile ad hoc networks. *International Journal of Intelligent Computing and Cybernetics*, *11*(2), 309–340.

Botha, R. A., Furnell, S. M., & Clarke, N. L. (2009). From desktop to mobile: Examining the security experience. *Computers & Security*, *28*(3–4), 130–137.

Chen, Y., & He, W. (2013). Security risks and protection in online learning: A survey. *The International Review of Research in Open and Distributed Learning*, *14*(5).

Cheng, L., Li, Y., Li, W., Holm, E., & Zhai, Q. (2013). Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. *Computers & Security*, *39*, 447–459.

Chun, B.-G., & Maniatis, P. (2009). Augmented smartphone applications through clone cloud execution. *HotOS*, *9*, 8–11.

Collin, R. (2019). *The Theory of Conscious Harmony*. Lulu. com.

Creswell, J. W., & Creswell, J. D. (2017). *Research design: Qualitative, quantitative, and mixed methods approaches*. Inggris: Sage publications.

Dang-Pham, D., & Pittayachawan, S. (2015). Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university: A Protection Motivation Theory approach. *Computers & Security*, *48*, 281–297.

Dwivedi, Y. K., Hughes, D. L., Coombs, C., Constantiou, I., Duan, Y., Edwards, J. S., … Prashant, P. (2020). Impact of COVID-19 pandemic on information management research and practice: Transforming education, work and life. *International Journal of Information Management*, *55*, 102211.

Effiong, A. (2013). Developing meaningful outcome measures for advanced care planning in the context of end stage renal disease (ESRD): going beyond randomised clinical trials (RCTs). *BMJ Supportive & Palliative Care*, *3*(2), 246.

Egners, A., Marschollek, B., & Meyer, U. (2012). Hackers in your pocket: A survey of smartphone security across platforms. *RWTH Aachen, Tech. Rep. AIB-2012-07*.

Enck, W., Ongtang, M., & McDaniel, P. (2009). On lightweight mobile phone application certification. *Proceedings of the 16th ACM Conference on Computer and Communications Security*, 235–245.

Ferman, A. M., & İlhan, D. O. (2019). An Evaluation Model Based on Sustainable Development for the Istanbul Shopping Center Market. *Aurum Journal of Social Sciences*, *4*(2), 129–154.

Freiberger-Verizon, M., & Watts-Verizon, M. T. (2018). Low latency networks: future service level use cases and requirements. *2018 Optical Fiber Communications Conference and Exposition (OFC)*, 1–3. IEEE.

Garfinkel, S. L., Juels, A., & Pappu, R. (2005). RFID privacy: An overview of problems and proposed solutions. *IEEE Security & Privacy*, *3*(3), 34–43.

Gherbi, C., Aliouat, Z., & Benmohammed, M. (2017). A survey on clustering routing protocols in wireless sensor networks. *Sensor Review*, *37*(1), 12–25.

Gikas, J., & Grant, M. M. (2013). Mobile computing devices in higher education: Student perspectives on learning with cellphones, smartphones & social media. *The Internet and Higher Education*, *19*, 18–26.

Godwin-Jones, R. (2017). *Smartphones and language learning*.

Goggin, G. (2021). *Apps: From mobile phones to digital lives*. John Wiley & Sons.

Gordon, C. J. (2015). *Addressing security risks for mobile devices: What higher education leaders should know*. The University of Nebraska-Lincoln.

Goyal, S., Jabbari, S., Kearns, M., Khanna, S., & Morgenstern, J. (2016). Strategic network formation with attack and immunization. *Web and Internet Economics: 12th International Conference, WINE 2016, Montreal, Canada, December 11-14, 2016, Proceedings 12*, 429–443. Springer.

Guido, M., Ondricek, J., Grover, J., Wilburn, D., Nguyen, T., & Hunt, A. (2013). Automated identification of installed malicious Android applications. *Digital Investigation*, *10*, S96–S104.

Henderson, T. (2011). How mobile device management works. In *IT WORLD*. IT WORLD.

Holmes, A., Byrne, A., & Rowley, J. (2013). Mobile shopping behaviour: insights into attitudes, shopping process involvement and location. *International Journal of Retail & Distribution Management*, *42*(1), 25–39.

Jansen, W., & Grance, T. (2011). *Guidelines on security and privacy in public cloud computing*. US Department of Commerce, National Institute of Standards and Technology ….

Karlsson, M., Denk, T., & Åström, J. (2018). Perceptions of organizational culture and value conflicts in information security management. *Information & Computer Security*, *26*(2), 213–229.

Kaufman, L. M. (2009). Data security in the world of cloud computing. *IEEE Security & Privacy*, *7*(4), 61–64.

Kritzinger, E., & Smith, E. (2008). Information security management: An information security retrieval and awareness model for industry. *Computers & Security*, *27*(5–6), 224–231.

Lacey, D. (2010). Understanding and transforming organizational security culture. *Information Management & Computer Security*, *18*(1), 4–13.

Lamey, D. (2018). The evolution of technology: past, present and future. In *Discover Tech*. Discover Tech.

Layland, R., Wexler, J., Datoo, A., George, A., Rege, O., Marshall, J., … Duckering, B. (2012). The 2011 Mobile Device Management Challenge–Defusing Mobile Anarchy in the Enterprise. *Network World and Robin Layland Present. Http://Solutioncenters. Networkworld. Com/Mobile_management_challenge. Accessed*, *29*.

Meidan, Y., Bohadana, M., Mathov, Y., Mirsky, Y., Shabtai, A., Breitenbacher, D., & Elovici, Y. (2018). N-baiot—network-based detection of iot botnet attacks using deep autoencoders. *IEEE Pervasive Computing*, *17*(3), 12–22.

Mirzajani, H., Mahmud, R., Fauzi Mohd Ayub, A., & Wong, S. L. (2016). Teachers' acceptance of ICT and its integration in the classroom. *Quality Assurance in Education*, *24*(1), 26–40.

Moneo, J. M., Caballe, S., & Prieot, J. (2012). *Security in learning management systems*. Spain: eLearning Papers.

Morrow, B. (2012). BYOD security challenges: control and protect your most sensitive data. *Network Security*, *2012*(12), 5–8.

Mukhopadhyay, A., Chatterjee, S., Bagchi, K. K., Kirs, P. J., & Shukla, G. K. (2019). Cyber risk assessment and mitigation (CRAM) framework using logit and probit models for cyber insurance. *Information Systems Frontiers*, *21*, 997–1018.

Muogboh, O. S., & Ojadi, F. (2018). Indigenous logistics and supply chain management practice in Africa. In *Indigenous Management Practices in Africa* (Vol. 20, pp. 47–70). Emerald Publishing Limited.

Murray, M. (2019). Tutorial: A descriptive introduction to the blockchain. *Communications of the Association for Information Systems*, *45*(1), 25.

Murtagh, F., & Legendre, P. (2014). Ward's hierarchical agglomerative clustering method: which algorithms implement Ward's criterion? *Journal of Classification*, *31*, 274–295.

Ngoqo, B., & Flowerday, S. V. (2015). Information Security Behaviour Profiling Framework (ISBPF) for student mobile phone users. *Computers & Security*, *53*, 132–142.

O'Connell, M. E., & DiFonzo, J. H. (2018). Reprinted from Vol. 44 No. 4 in Honor of Professor J. Herbie DiFonzo. The Family Law Education Reform Project Final Report. *Family Court Review*, *56*(1), 18–55.

Osterman, A., Vizoso Pinto, M. G., Haase, R., Nitschko, H., Jäger, S., Sander, M., … Baiker, A. (2012). Systematic screening for novel, serologically reactive Hepatitis E Virus epitopes. *Virology Journal*, *9*(1), 1–9.

Ott, D. (2014). Android* Security: Issues and Future Directions. *Intel Technology Journal*, *18*(2), 34–49.

Parkinson, S., & Khan, S. (2018). Identifying irregularities in security event logs through an object-based Chi-squared test of independence. *Journal of Information Security and Applications*, *40*, 52–62.

Picazo-Vela, S., Fernández-Haddad, M., & Luna-Reyes, L. F. (2016). Opening the black box: Developing strategies to use social media in government. *Government Information Quarterly*, *33*(4), 693–704.

Pottie, G. J., & Kaiser, W. J. (2000). Wireless integrated network sensors. *Communications of the ACM*, *43*(5), 51–58.

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: an action research study. *MIS Quarterly*, 757–778.

Robinson, T. (2014). Study reveals only 56 percent of employees get awareness training. *SC Magazine*.

Rogers, D. (2013). *Mobile Security: A Guide for Users*. Lulu. com.

Schaeffer-Filho, A., Smith, P., Mauthe, A., & Hutchison, D. (2014). Management Patterns for Network Resilience: Design and Verification of Policy Configurations. *Cyberpatterns: Unifying Design Patterns with Security and Attack Patterns*, 85–95.

Seppälä, P., & Alamäki, H. (2003). Mobile learning in teacher training. *Journal of Computer Assisted Learning*, *19*(3), 330–335.

Shammar, E. A., & Zahary, A. T. (2020). The Internet of Things (IoT): a survey of techniques, operating systems, and trends. *Library Hi Tech*, *38*(1), 5–66.

Sharma, I., & Ramkumar, K. R. (2017). A survey on ACO based multipath routing algorithms for ad hoc networks. *International Journal of Pervasive Computing and Communications*, *13*(4), 370–385.

Shinde, D. L. (2002). *Cybercrime Scene of the Computer Forensics Handbood*.

Talib, S., Clarke, N. L., & Furnell, S. M. (2010). An analysis of information security awareness within home and work environments. *2010 International Conference on Availability, Reliability and Security*, 196–203. IEEE.

Tweneboah-Koduah, S., Skouby, K. E., & Tadayoni, R. (2017). Cyber security threats to IoT applications and service domains. *Wireless Personal Communications*, *95*, 169–185.

Von Solms, B. (2001). Corporate governance and information security. *Computers & Security*, *20*(3), 215–218.

Wu, B., Chen, J., Wu, J., & Cardei, M. (2007). A survey of attacks and countermeasures in mobile ad hoc networks. *Wireless Network Security*, 103–135.