IOSR Journal of Mobile Computing & Application (IOSR-JMCA)
e-ISSN: 2394-0050, P-ISSN: 2394-0042.Volume 1, Issue 1 (May.-Jun 2014), PP 39-47
www.iosrjournals.org

Mobile computing application risks in Zimbabwe

Cuthbert Muza[1], Andelcah Muza[2]
[1](Department of Accounting, Banking and Finance, Zimbabwe Open University, Zimbabwe)
[2](Department Of Computer Science and Information Technology, Midlands State University, Zimbabwe)

Abstract: *Mobile technology has now become the order of the day. Everyone seems to own one or more mobile devices. Everyone is so excited because this has made life easier for a lot of people. Though mobile technology has brought many benefits to people's lives, its application has some risks that come with it. This paper therefore looked at mobile computing application areas in Zimbabwe, the risks brought about by mobile computing application in Zimbabwe and how mobile computing application risks are mitigated in a developing country like Zimbabwe where the technology level seems to be behind. The study findings showed that mobile application areas in Zimbabwe include paying bills, social networking and playing games. Most Zimbabweans revealed that they do not know how to mitigate mobile computing application risks. The study finally recommended that mobile computing application risks should be taught in schools as well as in televisions and radios so that everyone is aware of them.*

Keywords: *application risks, mobile computing, mobile device,mobile technology*

I. Introduction

This paper looked at the mobile application risks associated with a developing country like Zimbabwe. The paper sought to bring about the mobile applications common in Zimbabwe, the risks they bring about and how to overcome such risks. This study will help everyone who uses mobile technology at large to be aware of mobile application risks. The paper looked at what led to the study, gives details on how the study was conducted as well as results and conclusions of the study.

II. Background of study

Nowadays access to information worldwide is easier than it used to be long back. The information is progressively absent from offices but everywhere. Exceptional communication and production are being brought about by mobile computing but at the same time mobile computing brings risks to businesses and private/personal information. Mobile computing should be comprehensively protected to make sure that the mobile environment is managed and to ensure that corporate infrastructure and data are not put at risk. Most mobile devices have a greater tendency of being lost or stolen. They are also a bull's eye for hackers, malicious applications and all sorts of intimidating content. Organisations and individuals should make it a priority to secure connectivity and guard against mobile computing threats. Though mobile computing enhances the certainty of business success in organisations, it has a lot of risks which it carries along. There are financial risks associated with mobile computing applications. Use of smart phones or other mobile devices for online banking or online purchases can make the user's credit card information to be stolen and the user's bank's database to be hacked into. There are also information security risks where one could download corrupted applications which could access the user's email addresses and other data stored in the device. Viruses can attack an organisation's network via e-mails, the organisation's network can be obstructed by corrupted applications. If a mobile computing device is stolen or lost, the organisation's private information or personal identity is also lost.

According to UN telecom Agency's current report, in 2012 there were approximately 6billion mobile subscribers, which is about 87% of the world's population. Last year the sales of smart phones were roughly 40% of all mobile phone sales. Tablet sales were anticipated to surpass personal computer sales by some industry analysts by 2016.This shows how mobile computing use is increasing each day. Mobile device use is expanding beyond email. Most organisations are developing applications specifically for mobile computing. Much attention is focused on the advantages or benefits of mobile computing applications but little consideration on the risks associated with mobile computing applications.

In developed countries like France and USA, tablets and smart phones have distorted the boundaries between companies and their staff, partners and clients. Banks are also attacked on a large scale. A lot of businesses/organisations are working in the darkness when it comes to the remarkable risks they face with mobile computing. The attackers are usually cybercriminals who will be working for gain, protestors who will be violent for the sake of their ideology or hackers whose drive is often the entire challenge of the hack. Pirates now have no need to interrupt the organisation's network. All they need is to find an account ID online. They can have straight access to a lot of passwords/secret codes and credit card numbers if they are able to make their

way into the management system of a cloud. In 2011, about 24million Sony's customers' accounts were compromised.

According to Aljazeera news on the 8th of August, a teenage British girl by the name Hannah Smith hanged herself because she was being bullied on a social network called ask.fm. The ask.fm website has a question and answer format which enables its users not to disclose their identity as they post messages. The ask.fm website is rated the 9th most popular social networking site in the world created in 2010 and based in Latvia. It has about 13.2 million daily users. There is a high possibility that even in Zimbabwe there are people who use it. The researcher was so disturbed by these stories. This left a gap on the study of the mobile computing application risks in Zimbabwe. When we look at a situation in Zimbabwe, most parents are buying mobile phones and other mobile devices for their children at a very tender age. Even in primary schools you find pupils with mobile phones for different purposes. The researcher was left with some questions as to whether parents and their children in Zimbabwe are aware that mobile phones have such risks as stated above where children can be bullied on social websites leading to suicide. Internet abuse has been the headline of Britain where women received threats of rape and death on twitter. Can this be happening in a country like Zimbabwe?
In Aljazeera news, it was lately mentioned that a lot of people's information was compromised as their data was hacked through the use of Google website.

Recently, there was a panic among NUST students as they learnt that the university website had been hacked and results altered. Most students were able to see their results even if they had not paid the fees. Some of those who owed the school found that their accounts had been cleared and no longer owed the university anything while others who had paid their fees in full now owed the school large amounts. The other students found that they had failed the courses that they had never registered for. This had come as a result of the new software called Navision which had been bought by the university but the technicians were failing to use it which created loopholes for hackers. With the increase of mobile computing application in Zimbabwe, anyone can access any website anywhere and do anything to affect the website.

In February 2013, the ZRP warned people not to accept free key holders from the service stations and parking lots as these contained tracking device chips which criminals used to follow and rob/kill people. This criminal event was actually happening in Harare and Chitungwiza.
All the above issues prompted the research to pursue the proposed study.

III. Problem Statement

Looking at developing countries like Zimbabwe where technology seems to be behind compared to developed countries, the risks of mobile computing are of great concern. Organisations and people at large have welcomed mobile computing with wide open arms because mobile computing has made lives easier in the sense that mobile computing devices can store large amounts of data and are very portable. With all the benefits of mobile computing application, one wonders if Zimbabweans or Zimbabwean organisations are aware of the risks associated with mobile computing application.

IV. Importance of the Study

The researcher will review documents, journals, articles as well as interviewing people to find out the mobile computing application risks that are common in a developing country like Zimbabwe. This study will help the researcher to come up with knowledge on how Zimbabwean people view risks of the mobile computing application and the actions they take to mitigate these risks. With the level of technology in Zimbabwe, the researcher is curious to know how mobile computing application risks are taken care of as well as the security measures taken to protect users from mobile computing application risks.

Everyone who uses mobile computing will benefit from this study because the study will help people to be careful as they always look at benefits of mobile computing unaware of the risks brought about by applying it for different purposes. All this has prompted the researcher to carry a study to analyse the mobile computing application risks in Zimbabwe.

V. Research Objectives

- To come up with mobile computing application areas in Zimbabwe
- To explain the risks brought about by mobile computing application in Zimbabwe
- To determine if Zimbabweans are aware of these mobile computing application risks
- To attain knowledge on how mobile computing application risks are overcome, taken care of or mitigated in a developing country like Zimbabwe where the level of technology is behind.

VI. Research questions

- Which mobile computing application areas are common in Zimbabwe?
- What risks are brought about by mobile computing application in Zimbabwe?

- Are the people of Zimbabwe aware of the mobile computing application risks?
- With the level of technology in Zimbabwe, how are these mobile computing application risks overcome, taken care of or mitigated?

VII. Literature review

Literature review focuses mainly on investigation of literature that is related to mobile computing application risks. It takes note of the previous researches by different scholars in the area of study. The researcher will also make reference to various views expressed in journals, magazines, newspapers and other print media in relation to mobile computing application risks. Quite a number of terms will be used in this study and they will be better understood when defined.

7.1 Mobile computing definition

Asrani (2013, p.606) defined mobile computing as "an information management platform that is independent of location and time-based constraints." He further explained that the independence of this platform enables users to access data wherever at any time.

7.2 Mobile computing application

Deepak and Pradeep (2012, p.177) described mobile computing application as "the use of computing devices which usually interact in some fashion with the central information systems while away from the normal, fixed workplace." The mobile devices enable users to generate, get, store and transfer information anywhere, anytime and in any form as long as they have internet access. Deepak and Pradeep (2012, pp.179-180) gave areas where mobile computing is applied as follows:

7.2.1 Estate agents – Mobile computing enables estate agents to be flexible and productive. It enables them to work from anywhere, that is, at home, in the car, in the office or in the field. Mobile computing also helps the agents to dedicate more time to their customers. They can also give their customers instant response in regard to the information that might be needed by the customers.

7.2.2 Emergency Services- Most ambulances use mobile computing. This helps in cases of emergences like accidents. Ambulances can receive information while on the move which is very important in emergence incidents. The Cellular Digital Packet Data (CDPD) system used by some of the mobile devices helps to attain information about the location and other facts about the emergency incident to be posted or mailed fast to the mobile units that are nearer to the incident.

7.2.3 In courts – Mobile computing can be used in courts by lawyers. In a case where the conflicting lawyer mentions an incident or case they do not know they use the mobile computing devices to obtain direct contact the online legal database services so as to collect information about the case and the linked instances. Mobile computing application thereby makes people to access information anytime.

7.2.4 In companies- Companies apply mobile computing for different purposes such as advertising, selling, communicating to customers, meetings for discussions and presentations revision anywhere. Mobile computing also helps companies to gain a competitive advantage. Companies say that they get a faster response through use of mobile computing for advertising (Asrani 2013).

7.2.5 Mobile commerce - Mobile computing devices enable customers and organisations to purchase and advertise. Users can get access to their bank account details and be able to buy goods and to pay bills. There are shops and supermarkets that have Point of Sale terminals that allow their customers to use credit cards to buy. The Point of Sale terminals communicates with the bank central computer to verify the card usage. This happens rapidly and securely on cellular networks through mobile computing devices (Asrani 2013; Deepak &Pradeep 2012).

The 'bargaining power of buyers' increases due to mobile computing application. Mobile computing application may also lead to creation of market niches for new competitors. Adding to that, mobile computing applications lead to impulse buying due to ubiquitous markets (Ladd et al. 2010).

Mobile phones can be used to send mobile vouchers or tickets to users through mobile computing devices. These mobile vouchers are then shown at the ticket counter when checking in. People are also able to respond to stock market changes regardless of where they are (Asrani 2013)

7.2.6 Healthcare Services - Mobile computing devices leads to superior care for patients as data needed to help the patient is easily and quickly accessed. Through the use of mobile computing devices, health practitioners can monitor patients at any time and wherever. The emergency system is alerted by health-aware devices after detection of pulse rate and blood pressure. Mobile computing application in healthcare facilities help to reduce overcrowding as well as reducing costs. (Asrani 2013)

7.2.7 Social networking- Users can interact with each other through social networks like Facebook, Twitter, WhatsApp and Skype where they exchange photos, videos, messages and music.

7.2.8 GPS- Mobile computing is also used for providing geographical location services like finding nearby hotels, roads and for weather.

Mobile computing applications are said to provide safe, immediate and anytime, anywhere access to information. Mobile computing devices such as smartphones, flash drives and laptops are easy and convenient for use.

7.3 Mobile computing application risks

Oja (2012) argues that even if the use of mobile computing has been embraced by different users, it 'does not come without risks'.

- **Loss of device -** Most mobile devices are portable so they can be easily lost by accident or malicious intent. The mobile computing devices may be containing very sensitive information. They can store the owner's list of bank passwords, social security numbers on spread sheets or private information of an organisation. These mobile devices also act as entryways to a company's network resources. For example, a lost laptop with a Virtual Private Network (VPN) user and a saved password can cause the organisation's network to be vulnerable (Brooks 2005)

- **Social Engineering attack** – the attacker calls the user and poses as a company superior demanding the user's logon information to solve an urgent issue.

- **Access attacks** - Carrying out tasks like email checking, working on corporate documents and discussion of delicate matters by means of Voice Over Internet Protocol (VOIP) from mobile devices that are not safeguarded well gives attackers the ability of monitoring and gaining access to what was being accessed. Business rivals, hackers and restrictive governments take advantage of this by creating users' activities profiles and their identities.

- **Denial of service (DOS) attacks** – This is whereby a network is overpowered as a way of preventing legitimate users from receiving and sending information (Sawyer, n.d).

Locally stored information of an organisation is also at risk if the mobile devices are connected to the company's internal network because of untrusted links. Bluetooth, Wi-Fi and wireless Wide Area Networks (WANs) cause sensitive packets to be piped over the air where 'malicious sniffers' will be waiting (Brooks 2005).

Lum (2013) stated that mobile computing application can lead to other several risks. The brand status of the company can be damaged, company/customer and employee data can be lost and the company can lose customer trust if their information has been attacked. Data can be consolidated and the company may have to pay for regulatory fines and costs to comply with the regulations after an attack.

- **Phishing** - The email on the mobile device can be phished. Sawyer (n.d ,p8) defined phishing as 'the practice of creating a fraudulent e-mail which looks identical to a legitimate email from a bank or other company … in order to capture the user's login credentials.' The attacker usually creates a fake website which is looks equally to the real website. The user will then be asked to login using his/her username and password and also security number and credit card numbers may be requested. After the user has entered all this, the information is then sent to the attacker who in turn sells it for profit or uses it for identity theft. Some of the emails threaten to terminate the user's account if they do no update their information. Such emails are usually fraudulent.

- **Shoulder-surfing** – According to Sawyer (n.d, p9) shoulder-surfing is the 'practice commonly used by attackers in mobile settings as well as in any location where users are in close proximity to one another.' This risk enables the user to be observed by the attacker as he/she uses the mobile device. The attacker thereby catches all the private information entered by the user such as passwords. The keyboard and the screen of the device are usually monitored so as to get the information.

Other risks according to Oja (2012) include Unsecured Wi-Fi connections, Malware, Spam, Insecure or malicious applications and Viruses.

7.4 Mitigating/ overcoming the mobile computing application risks

Mobile computing risks can be avoided securing application of mobile computing (Sawyer, n.d).

- **Use of privacy filters** – Sawyer (n.d) mentioned use of privacy filters as one of the ways of preventing or avoiding shoulder-surfing especially when using mobile devices in 'close proximity environment.' He

further explained that Privacy filters restrict the viewing angle of the mobile device screen to the view of the user only to disable any nearest person from analysing the screen details.

- **Hand covering** – As users type their passwords they can cover with the hand to prevent attackers from observing how the keys are stroked (Sawyer, n.d)

- **Tailor made software** - According to the Controller's Report (2011) Company software for mobile can be tailor-made so that it does what is allowed by the company policy in terms of accessing data and applications. It further explains that there is software that can block the downloading of certain application programs as well as separating company information from personal information for security reasons. When the mobile computing device is stolen or lost these programs can remotely erase the data in these devices.

- **Encryption -** Brooks (2005) notes that since mobile devices are portable they should be encrypted to protect the information they carry from malicious acts. He further argues that even if the information is encrypted, fragile or compromised authentication can hinder even the best encryption schemes. This makes it crucial and wise to ensure integrity of the security boundary. Information can be sniffed as it travels over wireless networks so there is need for 'strong over-the-air encryption.' Sawyer stated that encryption is the answer to all mobile computing application attacks and that it makes users impenetrable by these attacks. He explains further that encryption alone is insufficient because if not used well, encryption can be breached or bypassed by social engineering, wireless monitoring, key-logging, electromagnetic interception, physical media analysis and use of Trojans. After all has been said and done, encryption alone cannot be relied on even if it is properly used.

- **Educating the user -** According to Sawyer, the user can be tricked or convinced by the attacker to render access to the attacker. This makes all security measures useless so the best way of defence against attacks is educating the user about these mobile computing risks as well as security of the mobile computing application.Sawyer (n.d) keeps emphasising that to defeat pishing users should be taught to monitor their emails strongly to sure they are from the real people they know. The mobile computing risks can also be reduced by updating antivirus software to defend against malware and viruses.

VIII. Research Methodology

Research methodology outlines how the researcher conducted the study, the design and tools that were applied as well as data collection techniques that were used. Various aspects of research methodology could be applied, that is, types of research strategies, data collection methods, sampling techniques and data analysis procedures. The researcher used a descriptive survey method for the study.

8.1 Descriptive survey method

This was defined by Cohen and Manion (1990, p.6) as "the process of gathering data at a particular point in time with the intention of describing the nature of existing condition". This method was chosen because it gives detailed descriptions of specific situations using interviews, observations and questionnaires. The researcher used questionnaires as the research instrument to gather primary data. This instrument was used to dig out information from the respondents which was beyond the surface or beyond that which could be ordinarily perceived by the observer (Leedy, 1985).The researcher used questionnaires because they reduce bias as personal contact with the respondent is not necessary and the fact that respondents have no need to disclose their names made it possible for respondents to freely give their views thus enhancing high chances of getting true or genuine answers concerning the research. Clear and simple language was used on the questionnaires to enable all respondents to understand.

The questionnaire had questions that included where the respondents applied mobile computing, whether they are aware of risks associated with mobile computing application, the risks of mobile computing they have experienced, the effects of mobile computing and how they mitigate mobile computing risks. The respondents were required rank and give comments on certain questions. The researcher used this to establish the significance of each question towards analysing the risks associated with mobile computing application. The questions in the questionnaire were either open-ended (where respondents were required to answer in their own words) or multiple choice (where respondents were to choose one or more answers from those provided). The questions were distributed to different people who were using mobile computing for different purposes.

8.2 Population and sampling

Borg and Gall (1989) defined population as a large group of individuals and objects that are considered useful in providing the required information in the area of study. A sample is a representative of a population.

The researcher sampled the population to avoid expenses of surveying the whole population and this assisted the researcher to have a correct description of the whole population considered for the study. The other reasons why the researcher sampled the population for the study include time saving, quicker availability of results, obtaining more detailed information better manageability of collected data and it gave more time to check data accuracy preceding analysis.

The sample was selected using simple random sampling. The researcher used simple random sampling for the study because it enabled each population member to be represented in the sample. The researcher took a sample of individuals in Harare who use mobile computing because Harare is the capital city of Zimbabwe where everyone from around Zimbabwe is assumed to be represented. About 50 individuals who apply mobile computing were selected. According to Newsday (2012, Dec), Harare has a population of 2 098 199 people.

Table 1: Population and sample size

Population size	2 098 199
sample size	50

50 questionnaires were issued to a variety of individuals who use mobile computing for different purposes. The questionnaires were issued through email or hand delivery. Of all the 50 questionnaires that were issued out, only 41 were delivered back to the researcher. This gave the response rate of 82 per cent which was not bad.

IX. Results, data analysis and Discussion of Results

To find out where people of Zimbabwe normally apply mobile computing, the respondents were requested to tick on the mobile computing application they make use of from the ones given on the questionnaire. If their area of mobile computing application was not there, they were requested to write it on the space for 'other' which was just under the listed mobile computing applications.

9.1 Applications of mobile computing

Table 2: Applications of Mobile computing

Application	Frequency	Percentage (%)
Estate Agency	6	14.6
Emergency services (ambulance, fire brigade)	3	0.07
In courts	0	0
Advertising, Purchasing, Marketing	33	80.5
Paying bills	22	53.7
Meeting discussions	11	26.8
Video conferencing	11	26.8
Presentation revision	12	29.3
Games	38	92.7
Health services	0	0
Social networking (WhatsApp, Facebook, etc.)	40	97.6
GPS	8	19.5
Banking	18	43.9

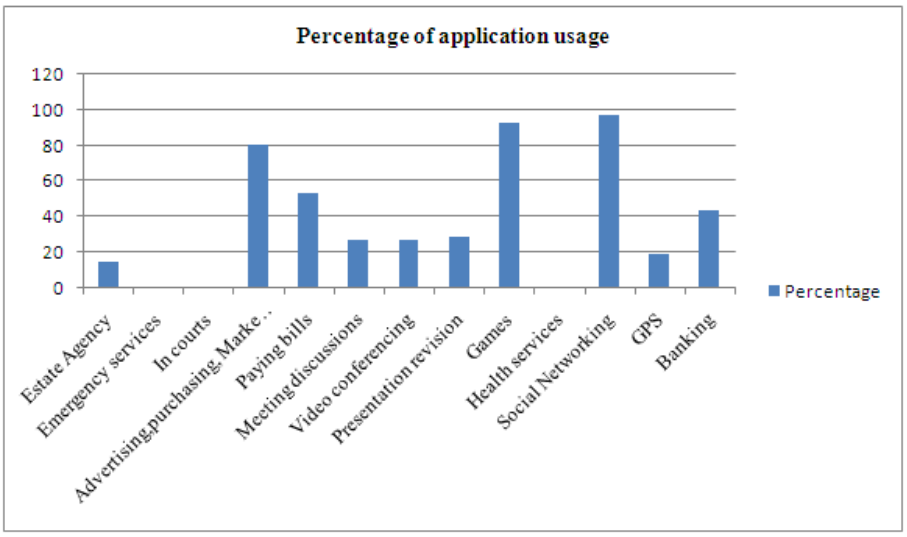

Figure 1:Applications of Mobile computing

The research findings show that 3 of the presented areas of mobile computing application are the mostly used by respondents because they have percentage usage of 50% and above. There is social networking with the highest percentage of 97.6, followed by games with 92.7%, then comes advertising, purchasing, marketing with 80.5% and finally paying bills with 53.7%. These results show that in Zimbabwe most people apply mobile computing in social networking. On the other hand, some of the areas of mobile computing application had very low response which shows that they are not commonly used in Zimbabwe. These include banking with 43.9%,video conferencing with 26.8%, GPS with 19.5%,presentation revision with 29.3% and emergency services with 0.07%. The results on the graph show that Health services and courts had 0 respondents which shows mobile computing in these areas may not be applied in Zimbabwe.

9.2 Awareness of mobile computing application risks

The respondents were requested to tick on 'yes', 'no' or 'not sure' whether they were aware of the risks associated with mobile computing application.

Table 3: Awareness of mobile computing application risks

response	Yes	No	Not sure
frequency	11	17	13
Percentage (%)	26.8	41.5	31.7

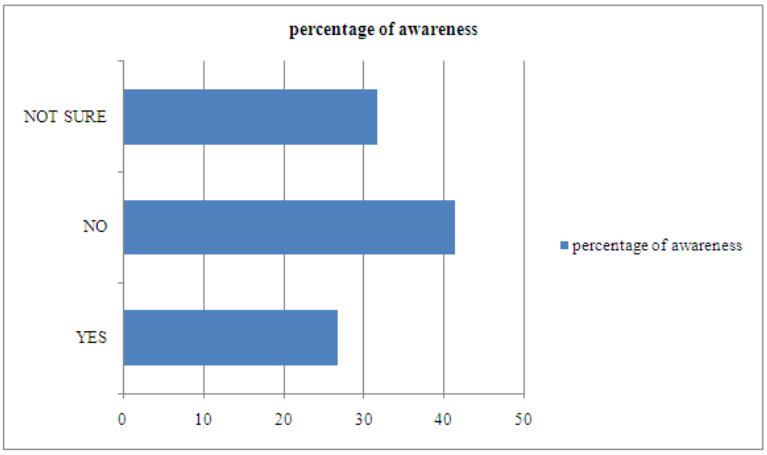

Figure 2: Awareness of mobile computing application risks

According to the graph in Figure 2, 41.5% of the respondents are not aware of the risks that are conveyed by application of mobile computing, 31.6% are not sure of their awareness of these risks and only 26.8% of the respondents indicate d that they were aware of the mobile computing application risks. This shows that a majority of the people of Zimbabwe are not aware of the mobile computing application risks. Most people apply mobile computing without knowing that it carries some risks with it that may put these people in danger. There are respondents who indicated that they are not sure about these risks which made the researcher to assume that these respondents did not know what these risks are all about or what they are.

9.3 Mobile computing application risks in Zimbabwe

On the questionnaire, respondents the requested to write down the risks or dangers they have come across due to applying mobile computing in different areas. Only a few respondents listed the risks and a majority of the respondents left spaces blank. The researcher assumed that the respondents who did not give feedback on the risks or dangers they have come across due to application of mobile computing, were not sure what these risks were all about or they did not know about these risks at all.

Nevertheless, the respondents who listed the risks gave a few different risks. Viruses had the highest frequency among all the mobile computing application risks stated by the respondents. The other risks that were given are theft of the mobile devices and money theft from their bank accounts. One of respondents mentioned that he once nearly lost his job due to application of mobile computing. He said was no longer productive at work as he spent most of working time on social networks like Facebook and WhatsApp. The other respondent revealed that she nearly got herself into Satanism by accepting whoever friend requested her on Facebook. She said that she would also get messages in her inbox from people she did not know who wanted various details concerning her. The other risk that was given by the respondents was the issue of Fraud where some of the respondents stated that they once fell into the hands of imposters on social networks like Facebook where the imposters would pose as great man of God who requested money from the users to help the needy. The users

would deposit money into the account details of these imposters only to discover later that these imposters were cheats or pretenders. The other issue mentioned was robbery where one of the respondents talked about being robbed after he was given a free key-holder that had a tracking device at a certain service station around Harare. The risks that the respondents mentioned, gave an insight to the researcher on the dangers or risks that people in Zimbabwe are facing due application of mobile computing. From the overall view of the results, the researcher found out that even though there are risks associated with the application of mobile computing on various areas, most people in Zimbabwe know nothing about these risks which leaves most Zimbabweans exposed to danger brought about by something that is handy to them and they seem to trust so much.

9.4 Mitigation of risks conveyed by application of mobile computing in Zimbabwe

Respondents were asked to state the ways they lessen, overcome or avoid the risks of applying mobile computing. Most of the respondents mentioned use of antivirus software and the use of passwords as the ways they use to mitigate risks conveyed by applying mobile computing. The other respondents stated that they back up information contained in their mobile devices to avoid disappointments if anything happens to their devices. However, there are about 30 of the respondents who revealed that they know nothing about how to lessen, overcome or avoid the mobile computing application risks.

The information given by the respondents concerning the issue of mitigating mobile computing application risks made the researcher realize that many Zimbabweans have little knowledge about mitigating risks brought about by applying mobile computing. The researcher recognised that the most common mitigation ways against mobile computing application risks are the use of passwords, antivirus software and backing up of information. This shows that Zimbabweans really need to be taught about a lot of different mitigation ways against mobile computing application risks.

X. Conclusion

This paper aimed at analysing mobile computing application risks in Zimbabwe. It looked at the applications of mobile computing used in Zimbabwe, the risks of mobile computing application or use in Zimbabwe as well as how the mobile computing application risks are mitigated in Zimbabwe. The paper also sought to check if Zimbabweans are aware of the mobile computing application risks or not. Questionnaires were used to collect data from 41 respondents.

Zimbabwe is a developing country where mobile computing use is increasing everyday and people are welcoming it so much. Almost everyone of every age group has a mobile device. The research results show that most people in Zimbabwe use mobile computing for social networking, games, paying bills, advertising, purchasing and marketing. Banking, video conferencing, GPS, presentation revision and emergency services are rarely used by people of Zimbabwe. The results also showed that mobile computing is not used in Health services and courts in Zimbabwe. A majority of Zimbabweans are not aware of mobile computing application risks and how these risks can be mitigated.

According to the research results, it is concluded that though mobile computing use is becoming common in Zimbabwe, people are not aware that it carries with it some risks that may put them at a disadvantage. The other thing is most people in Zimbabwe do not know how to protect themselves against the mobile computing application risks.

XI. Recommendations

The research recommends that people in Zimbabwe should be taught about the risks associated with mobile computing application as well as how to avoid, get rid of or even lessen these risks because many people seem to be ignorant when it comes to the risks that the use of mobile computing may bring. This can be done in schools and in companies as well as on television, newspapers and radios so that the knowledge about mobile computing application risks and mitigation techniques can reach and benefit everyone who uses or intends to use mobile computing.

For future studies a research on effects of mobile computing application in Zimbabwe is recommended.

References

[1]. Asrani, P. 2013, 'Mobile Cloud Computing', International Journal of Engineering and Advanced Technology, vol. 2, no. 4.
[2]. Borg, W.R. & Gall, M.D. 1989, Educational Research: An Introduction, 5th edn, Longman.
[3]. Brooks, J. 2005, 'Mobile computing risks are rising', eWEEK.com, 13 June, pp. 43-45.
[4]. 'Cameron castigates cyber bullying websites', Aljazeera, 08 August, http://aljazeera.com/news/europe/2013/08/20138814183245539.html.
[5]. Cohen, L. & Manion, L. 1990, Research Methods in education, 3rd edn.
[6]. Creswell, J.W. 1998, Qualitative, Quantitative and Mixed Methods Approaches, 2nd edn.
[7]. Daymon, C. & Holloway, I. 2002, Qualitative Research Methods in Public Relations and Marketing Communications, Routledge.
[8]. Deepak, G. & Pradeep, B.S. 2012, 'Challenging issues and limitations of Mobile Computing', International Journal Computer Technology and Applications, vol. 3, no. 1, pp. 177-181.

[9]. Denzin, N.K. 1970, The Research Act: A Theoretical Introduction to Sociological Methods, Aldine, Chicago.
[10]. Gill, J. & Johnson, P. 2002, Research Methods for Managers, 3rd edn, SAGE Publications, London.
[11]. Ladd, D.A. et al. 2010, 'Trends in Mobile Computing within the Information Systems: A ten year Retrospective', Communications of the Association for Information Systems, vol. 27, no. 17, pp. 285-306.
[12]. Leedy, P.D. 1985, Practical Research: Planning and Designing, 3rdedn, Macmillan, New York.
[13]. Lum, A. 2013, 'Mobile Computing risks- What you need to know', Control Solutions International, 13 April.
[14]. Oja, D. 2012, 'Addressing security risks of Mobile Computing', The ruggedized computing Blog, 7 August.
[15]. Saunders, M., Lewis, P. & Thornhill, A. 2009, Research Methods for Business Students, 5thedn, Pitman.
[16]. Stojmenovic, I. (ed) 2002, Handbook of Wireless Networks and Mobile Computing, Wiley-Interscience Publication.