Implementations of Network Security in the Internet Cafés around Pretoria, South Africa

Alfred Thaga Kgopa, and Prof Ray M Kekwaletswe

***Abstract*--**Although owners of Internet cafés extend the freedom use of Internet access to the users, but they fail to design a strong computer network security to prevent risk arising through computer access by users and external attacks. The aim of this study is to provide a conceptual framework for improving network security in the Internet Cafe strategically to ensure data privacy, data integrity, risk management and information security (IS) good behavior. The study investigated the challenges by Internet café owners to implementing network security and how information security can be implemented or improved in the Internet cafés. The follow-up interview was setup with the Internet café owners from all the Internet café were questionnaire of the first paper (*information security issues that are faced by Internet café users*) was conducted.

***Keywords*--**Information, Information Security, Internet, Network

I. Introduction

THIS study deals with the implementations of network security in the Internet cafés around Pretoria, South Africa. The first paper of this study identified information security issues that are faced by Internet café users, now this paper will focus on the challenges faced by Internet café owners in terms of implementing security tools in order to cover all angles of data confidentiality, integrity and availability. Framework is conceptualized based on the objective of this paper and the first paper of information security issues that are faced by Internet café users.

It is argued that Internet usage is likely to increase due to the increasing availability of network infrastructures, faster connection speeds, and lower connection costs in terms of Internet technologies such as asymmetric digital subscriber line (ADSL), third generation networks (3G) and so on [1]. Most businesses today have systems that also operate on the Internet for customer self-services. These systems offer businesses many advantages such as online marketing, advertising, purchasing and sales. So, Internet cafés play an important role in businesses that engage in e-business [10]. In order for customers to do online transactions, they must have access to the Internet so that they can log on to different e-business systems or websites to get help. Those who do not have Internet access from home or their place of work need to go to an Internet café in order to use the Internet.

Alfred Kgopa was with telecommunication company Telkom SA, Centurion 61 Oak Avenue. He is now employed and study at Tshwane University of Technology, in South Africa (SA), Pretoria. Phone: +2782 094 6339; email: kgopaat@tut.ac.za. His study leader is Prof Ray Kekwaletswe who is currently with Witwatersrand University, in SA

Internet cafés are increasingly providing Internet opportunities for ordinary people who can't afford to have Internet access at their homes. Many people use the Internet café to access their webmail, engage in instant messaging, to keep in touch with friends and families via social networks such as Facebook, Twitter, and other social network media [7]. Apart from engaging in social networks, many also go to Internet cafés to perform different actions such as online research, accessing online systems to perform their business transactions, while others use it to do their online banking and shopping.

II. Research Goal And Question

The goal of this study is to conceptualize a framework to Implementations network security in the Internet cafés.

A. Research Question

1) What challenges that Internet café owners face in implementing network security and how can network security be implemented or improved in the Internet cafés?

III. Data Collection Method

The data was collected from a variety of sources to ensure that the researcher had enough information to work from. For the purpose of this research and in order to answer the question and to achieve the goal of this research, both primary and secondary data was collected. The following data collection method has been used.

A. Follow-up Interview

The researcher decided to interview the Internet café administrators or owners in all Internet cafes where the questionnaire of first paper (*information security issues that are faced by Internet café users)* was distributed. The aim of this interview was to follow-up the questionnaire results due to there was suspicious information and also to find out the challenges Internet cafés to implement network security. So the researcher did not want to follow the principle of suspicion because it might give false suspicion thus according to [5]. Instead, the researcher wanted to find the actual findings to be discussed in relation with users findings.

Unstructured interview with both closed and open ended questions were used. The interview was conducted face to face in three of Internet cafes that the questionnaire where distributed.

IV. Sampling

Table 5 is sampling of follow-up interview that the researcher did face to face with the responsible people in all Internet cafe where user questionnaires was distributed.

TABLE I
SAMPLING OF FOLLOW-UP INTERVIEW

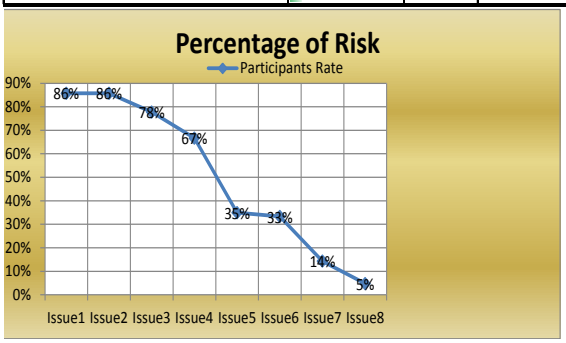
Follow-up Interview Sampling	
Number of Participants is 3	**Participants role**
Internet Café 1 (PTA Central)	Cashier **Qualification:** Public Admin
Internet Café 2 (PTA Central)	Owner and Administrator **Qualification:** A+
Internet Café 3 (Sunnyside)	Administrator and Technician **Qualification**: A+ and N+

V. Finding and Data Analysis

Results from previous paper *"Information Security Issues Facing Internet Café Users [4]"*

TABLE II
ISSUES FACING INTERNET CAFE USERS

Issues that affected Internet café users in Pretoria.			
No of participants		63	
Existance of Issues	**Participants Rate**	**Action Status**	**Comments**
Viruses	86%		High risk
Lack of Information Privacy	86%		High risk
Online Harassment	78%		High risk
Scam	67%		High risk
Poor Administrations	35%		Average risk
Slow Computers	33%		Average risk
No Enough Computers	14%		Low risk
Computer Crashing	5%		Low risk



The results of table 2 shows the issues that affect the users of Internet cafés in Pretoria, They are important as it was the objective of this study to find out what issues regarding the use of Internet cafes affect users. It was found that most users have been affected by issues in terms of information security at Internet cafes and it was also found that most users did not feel comfortable transmitting any personal information when using the computers in Internet cafés [4].

VI. Follow-up Interview Results

This section deals with the first part of research question "*What challenges that Internet café owners face in implementing information security*" and the second part "*how can information security be implemented or improved in the Internet cafés?*" will be discussed in the section of recommendations.

It is found that there are some certain challenges the Internet café owners need to address for the success of their businesses. The Internet cafés are using trial software and some they don't even use firewalls and they don't have servers in their network setup. The following issues have been noticed as challenges that Internet café owners need to address.

TABLE III
USAGE OF INFORMATION SECURITY PER INTERNET CAFÉ

	Information security used per Internet café		
	Café 1 (Pretoria Central)	**Café 2 (Pretoria Central)**	**Café 3 (Sunnyside)**
Computer and Network	Antivirus Password	Antivirus Password	Antivirus Password Monitoring system
Physical Security	-	-	Security cameras

A. Lack of Information Security Policy

During the research study it is found that the Internet café around Pretoria they don't have any existing information security policy for their business. Each and every Internet café has its own way of running day to day business. The owners are the solo owners and they are not franchised. So in this way it end-up as challenge of how should the business run because every owner is only doing business just to make their living. So this way of solo owner business it is committed to set the ineffective information security policies.

As stated by [8], without a clear understanding of the organization's policies and their scope, individuals does not have a good basis for making decisions about information security issues. [8] Continuing by saying that the best way to ensure the viability of the information security policy is to conduct training systems that detail the policy for the users and teach them how to perform securing procedures that are required by the information security policy.

B. Lack of Financial Management

It is also found that the owners of the Internet cafés they don't budget the money for their business maintenance and upgrading. All the Internet cafés that were visited they have poor network setup excluding the one in Sunnyside. The one in Sunnyside has better information security measures as compare to the one visited in Pretoria central. One of the owner clearly specified that they spend their business money in business premises rentals and to their personal life because Internet cafés is their only source of income. They should be aware that even Internet café is their source of income they should take care of them by making sure that the customer are

happy at all the times. Customers will go somewhere if they don't feel that their confidential information is secure when they use their Internet café.

So Internet cafe owners need to make budge to implement their business. They have to open a saving account, and the money for that account will only be used for business maintenance and any arising emergences of their business not for personal matters.

C. Lack of Technical Skills

Employing the person who doesn't have technical skill in the Internet café can ruin the business financially and the customer can go because they always don't get assisted when they have technical problems. Internet café owners need to take their employees to the training to gain knowledge and to learn more about new technologies. They must be aware that when the new security system is launched the hackers also develop or plan the new attack. Table 3 shows all the information security technologies they are used in the Internet café that where visited. The result shows that there is lack of knowledge on how to protect valuable data of business and customers from the malicious people.

VII. Recommended Implementations of Internet Cafés

This section deals with the second part of research question "*how can information security be implemented or improved in the Internet cafés?"* The section recommend on how can information or Network securities be implemented or improved in the Internet cafes.

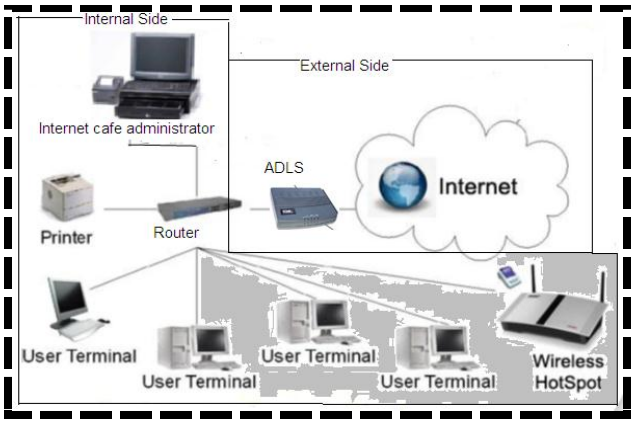


Fig. 1 Internet cafes network layout modified from ARINDA network layout)

The network setup layout in figure 1, is suitable for Internet cafés around Pretoria because most of them they run their business in the traditional way; in other words there is an administrator to accept payment from users and who logs on for users on available computers. Once the user has made the payment then they can go to the user terminal and use the computer to access the Internet. Figure 1 layout is thus recommended for all Internet cafés in Pretoria who run their business in traditional way.

The setup can be implemented as follow: Suppose you planned to build a home and wished to make it extremely secure against a vandalism or break-in and cost was no obstacle. You might investigate complicated alarm systems, building material, door locks and construction techniques. You will probably install electronic systems to interior and exterior light. You may also include surveillance cameras, video recording system and motion detector to prevent crime. These defenses could scale up to any size of home, but they are also common and therefore can be defeated by well-informed burglars.

Same to the Internet cafe they need be plan their information computer security when they plan to start Internet cafe business or they may implement this security recommendation to their existing Internet cafes. They can protect their computers from uninvited quest by putting up the firewall, which will prevent malicious people from taking control of your computers and from unwanted software to be installed. These include pop-up advertisement and viruses that are discussed in their previous sections. Firewall comes in to different types, there is hardware firewall and software firewall. The information about the firewalls was discussed in chapter two, but it will be also discussed on these section based on the network setup diagram so that those who want to implement their security based of these diagrams will have better understanding.

A. How Hardware Firewall Works

The hardware firewall in the diagram is the router, how it work? for instance if someone call you at home by dialing your home telephone numbers while you're at work, chances are someone or voice mail system will accept the call, and determine if they should forward the call to you. This is how hardware firewall work, in brief any information or email messages that comes to your computer will stop at the router. The router will determine if that incoming message of information has been requested by you. If it is the webpage you asked for or is your email, then the router sends it to your computer. If it is something that you did not requested, then the router will reject it [2].

Technically, your unique public internet address called your IP address, stops at the router and is converted into an addressing scheme that only the router and your computer understand, and that no one on the internet can get directly to your computer.

B. How Software Firewalls Work?

According to [2], software firewall is a computer program that inspects your incoming and outgoing information including emails sending and receiving emails. The software will determine what should be allowed to pass, similar to a router does. With software firewall you can specify which traffic form what side will be allowed to pass and which one shouldn't pass. You can setup the browse not to allow some certain website, for instance you can block the entire porn site

not to be accessible to prevent sexual harassment in the Internet cafe. There are numerous software fire walls including windows firewall.

If you are using windows XP, windows Vista or 7 and windows 8, there is no need to purchase the separate firewall software. All of these windows include firewall that is easy to configure and they should protect you very well. The simplest way to implement the windows firewall is to make sure your computers are up to date and the software is turned on as recommended. If you chose to purchase the separate firewall software there are numerous vendors who make them, including most of major antivirus builders such as Notorn Symantec, Macafee and Zone Alarms [3]

C. Unauthorised Access

What will happen if the attacks gain access to your network security?, just similar to your home, like it said that it is common that your sophisticated home security can be defeated by well-informed burglars. Still in you secure network setup there are still attacks that can gain access. The attackers can be informed by internal people or former employee about the network security of your Internet cafe. So you need to be prepared for any malicious action that comes to disrupt your network. If this happen at your home you might have a gun to defense yourself and your family against the attackers or press panic button for security call up.

So in terms of computer information security, Internet café owners they must have a plan to protect their data and customer data if the attackers have manage to break into their network [6]. Internet cafe owners can use updated antivirus software, and strong pass words can be used for all computer. When the users need to use the computer the administrator will log on behalf of the users once the payments has been received. Once the all computers need user name and password and the unknown user has gain access, that user should be treated as guest user. Once the user is treated as guest user would have limited access, would not be able to maintain other user's confidential data and will not be able to install any software on the computer.

VIII. RECOMMENDATIONS FOR INFORMATION SECURITY

The following layout is the review of best practice of information security that the study went through. This section will quickly summarize all important information that needs to be taken in consideration when someone wants to plan for information security. These entire important information security requirements are show in figure 2. The security requirements information is group together to form a layout and the researcher decided to called it Bullet of Information Security (IS) Hackers. Just like it said that you might use the gun to short burglars who will defeat your sophisticated home security. So Internet cafés owners can also use this layout as their gun bullet to kill all the threatening computer hackers.

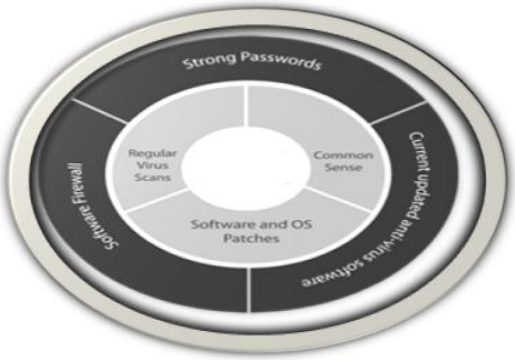


Fig. 2 Bullet of IS Hackers (source: google IS images)

- **Strong Password:** this is the most basic protection methods for your computer to ensure you have a strong and difficult to guess password.
- **Software Firewall:** A software firewall can be used to prevent oncoming traffic from contacting your computer without your request. Windows XP, Vista, 7 and 8 comes with a built-in, easy configured firewall that can perform this basic protection. Best idea is to leave it turned on and updated [3].
- **Antivirus Software:** The latest antivirus software is now so much more secure than just before. It is often a complete End-Point-Security Solution that can protect you from all this virus problems [10].
- **Software & Operating System Patches:** These are updates issued by software companies that fix known, and unknown, problems, security holes and vulnerabilities in their programs. Often these patches will fix a security hole that could allow remote attackers to access your computer. Install them often [9].
- **Regular Virus Scans:** Even though good antivirus programs detect in real-time, it is still a good idea to

manually run a scan of not only your computer hard drive, but also any external storage devices you may have [9].

- **Common Sense:** All the technology in the world cannot protect you when you do silly things like opening un-trusted email attachments, clicking on links you do not trust, downloading files over Peer-To-Peer networks etc. If you do dumb things, bad things could happen. Technology cannot prevent that

IX. Functions of Internet Café Security (FICS) Model

The Functions of Internet Café Security (FICS model is the conceptualised framework for incorporating key research findings in an integrative manner to support the research objectives. The model used to make recommendations based on the management of information security in Internet cafés.

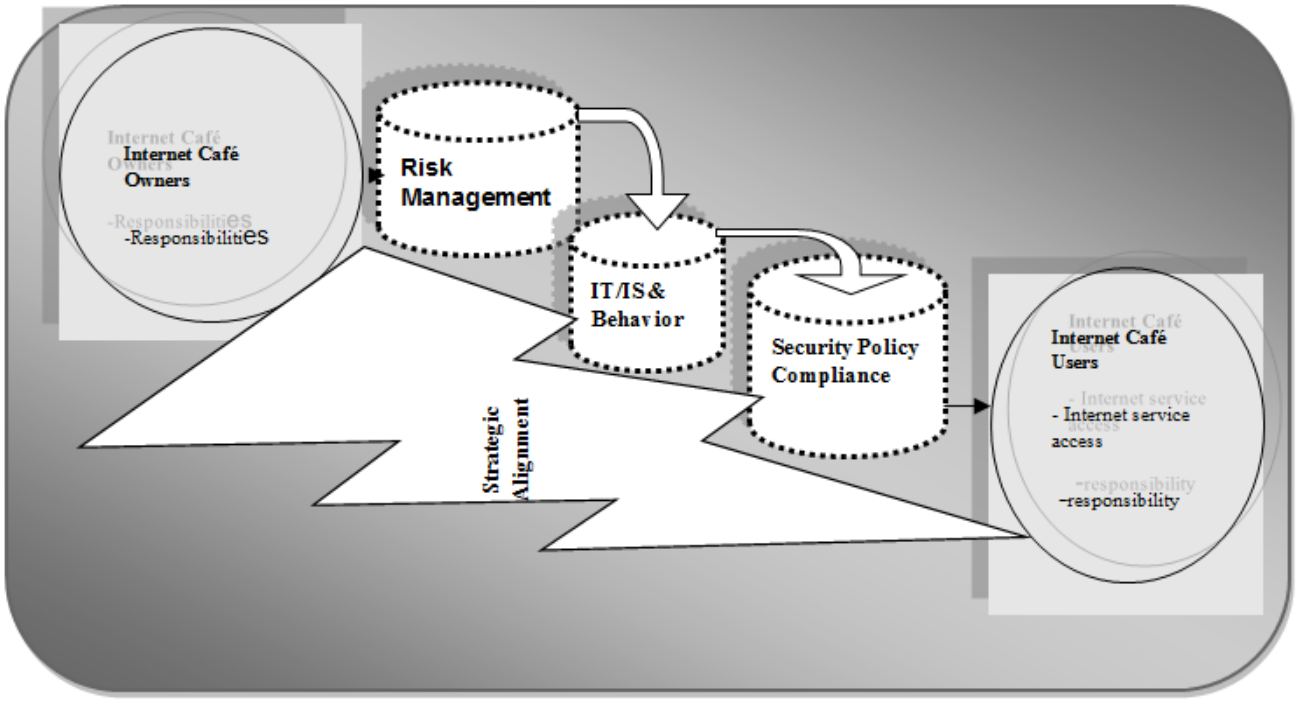


Fig. 3 FISC model: Conceptual framework for addressing Internet cafe issues

FICS model adds a new dimension to information security control. It differentiates between an Internet cafe owner's function of information security which is focused on information that is legally owned by the Internet cafe and the deliverable of customer services. The Internet cafe user's function, on the other hand, deals with the privacy of their own data that is available through a technical interface by means of which the user accesses and downloads/uploads data from and to the Internet. This section will not touch the users and owners responsibilities because they are already stated in pervious sections of recommendations.

A. Risk Management

Risk management requires an understanding of the source of threats, action of threats and how to manipulate that source in order to protect the Internet cafés from such threats [1]. Data that is stored on the networked computer is vulnerable to risks from external and internal sources that must be assessed [10]. It is thus important that guidelines to risk assessment be established with concomitant objectives. Assessment of risk involves an analysis and identification of the relevant risks in order to achieve the assigned objectives. Investigations show that most of the information security threats are caused by poor networking, physical security and administrations, e.g. a lack of technical skills by Internet cafe administrators and owners, also by the Internet cafe users who don't protect their data very carefully.

Users who do not feel comfortable using their personal information in the Internet cafe must make intensive efforts to improve their physical information security when using the Internet. Once the owners of Internet cafés know what information sources need protection, information security principles can be implemented and developed. Information security principles are the minimum acceptable security that should be provided to protect any personal information.

When users in Internet cafes download information from the Internet, some save the information on the computers of the Internet cafe before they send it to their memory sticks. It is thus easy for computers in Internet cafes to get viruses from this data, and it is the Internet cafe's responsibility to make sure that the data is secured. In other words, it is the user's responsibility to make sure that the data is deleted from the Internet cafe's computers before their Internet access expires. So by implementing the recommended network layout that is

discussed in section vii it will help to manage risk in the Internet cafes.

B. IT/IS Behaviour

According to [6], the success of information system security depends on the user's behavior, and that computer users must be proactive with regard to information security. If all the Internet cafés implement high levels of information security, the level of information security could be increased and this would be of benefit to the business of Internet cafes.

Like it said in the previous section, all the technology in the world cannot protect you when you do silly things like opening un-trusted email attachments, clicking on links you do not trust, downloading files over Peer-To-Peer networks etc. If you do dumb things, bad things could happen. Technology cannot prevent that.

Security technologies such as antivirus software need to be used in a correct behaviour and be updated continuously, and the practice of creating strong passwords is recommended to all users to protect unauthorised access of information [9]. Antivirus software needs to be scheduled for virus scanning at least once a day. Both software and hardware firewalls can be used to tighten security measures

C. Security Policy Compliance

The information security policy is an essential first step in providing an Internet café with adequate protection against possible threats and attacks. The findings of this study shows that poor implementation and enforcement of technical measures to protect user's information from malicious cybercrime, consequence in users of Internet cafes been concerned about using their confidential information in the Internet cafes.

For the successful assessment practice the following can be said:

- For effective and valuable results of information security policy, assessment must be thorough and it cannot leave out possible vulnerabilities because the results of the assessment may give a false picture of the information security policy status.
- It must also be repeatable to provide a consistent perspective on the Internet cafés security practice.
- Security policy assessment will initially increase the workload for any Internet café administrator by its nature.

Once the information security policy is implemented one should comply, this include Internet café owners, employees and users.

REFERENCES

[1] Ahmad, B. & Zuraini, I. 2012. Users as the Biggest Threats to Security of Health Information Systems: International Journal of Communications and Information Technology, 1(2), 1-16.

[2] Beal, V. The Differences and Features of Hardware and Software Firewalls. Online information security Article. published by Webopedia 2010

[3] HERATH, T. 2009. Encouraging information security behaviours in organizations. Journal of Decision Support System, Publisher: Elsevier. 47(2), 154-165

[4] Kgopa, AT. Information Security Issues Facing Internet Café User, Proceeding of the International Journal Conference on Computer Networks and Data Security (IJCCNDS'13).To be published by ISAET: Bali: Indonesia 2013,

[5] Klein, H & Myers, M. 1999. A Set of Principles for Conducting and Evaluating Interpretive Field Studies in Information Systems: MIS Quarterly Special Issue, 1(23), pp. 67–94

[6] Koskosas, C. 2011. Examining the linkage between information security and end-user trust. International Journal of Computer Science & Information Security, 9(2), 21-31.

[7] Rangaswamy, N. 2005. ICT for development and commerce: A case study of Internet cafés in India. International Conference on Social Implications of Computers in Developing Countries. Available from: http://research.microsoft.com/apps/pubs/default.aspx?id=143983 [Accessed 14 May 2012].

[8] Subramanian, K. A global challenge and integrated enterprise. India: National Informatics Centre Government of India 2012. Available from: http://www.i4donline.net/issue/jan04/gobal_challenge_integrated_full.htm.[Accessed: 11 October 2012].

[9] Venter, Coetzee and Labuschangne. Information Security for South Africa. Proceedings of ISSA conference. Published by ISSA. Johannesburg, 2009.

[10] Wikibooks. "Fundamentals of Information Systems Security/Information Security and Risk Management". 2012. Available from: http://en.wikibooks.org/wiki/Fundamentals_of_Information_Systems_Security/ Information_Security_and_Risk_Management [Accessed: 20 October 2012]

Alfred Kgopa was with telecommunication company Telkom SA, Centurion 61 Oak Avenue. He is now employed and study at Tshwane University of Technology, in South Africa (SA), Pretoria.
Phone: +2782 094 6339; email: kgopa80@gmail.com. His study leader is Prof Ray Kekwaletswe who is currently with Witwatersrand University, in SA.