Research Inventy: International Journal of Engineering And Science
Vol.6, Issue 2 (February 2016), PP -21-26
Issn (e): 2278-4721, Issn (p):2319-6483, www.researchinventy.com

An Overview of Information Systems Security Measures in Zimbabwean Small and Medium size Enterprises

[1]Kundai Oliver S. Sai, [2]Caleb Manjeese, [3]Talent Mawere, [4]Prosper T.Denhere
[1, 2, 3] Department of Mathematics and Computer Science - Great Zimbabwe University
Box 1235 Masvingo, Zimbabwe
[4]Department of Computer Science and Information Systems - Midlands State University
P Bag 9055 Gweru, Zimbabwe

ABSTRACT-*This paper reports on the Information Systems (IS) securitymeasures implemented by small and medium size enterprises (SMEs) in Zimbabwe. A survey questionnaire was distributed to 32 randomly selected participants in order to investigate the security measures and practices in their respective organisations. The results indicated that over 50% of the respondents had installed firewalls, while more than 80% carried out regular software updates and none of the respondents had intrusion detection systems. The researchers recommended that SMEs work to enhance their knowledge on the different IS threats in order to enable the implementation of preventive measures.*

Keywords *- Information, Information Systems, Measures, Security, SMEs*

I. Introduction

In a bid to improve efficiency and service delivery, most SMEs in Zimbabwe have since moved from the use of manual sales systems and cash registers to the use of electronic Point of Sale Systems (POS)(Sai, et al., 2015).On a daily basis, attackers are indisputably penetrating companies with a constant Internet connection and Zimbabwean SMEs are not an exception.This paper is aimed at identifying how these SMEs have been protecting their information systems and more importantly their data.Traditionally, computer facilities have been physically protected for three main reasons: To prevent theft of or damage to the hardware, to prevent theft of or damage to the information and to prevent disruption of service(Alkandary & Alhallaq, 2016).

II. Literature Review

This section provides a theoretical background towards answering the question:

What are the security measures currently implemented by Zimbabwean SMEs?

According to Keller et al. (2005) there are at least eight recommended security measures for small businesses:

Install and Properly Configure a Firewall

A firewall is a software program or piece of hardware that helps screen out hackers, viruses, and worms that try to reach your computer over the Internet(Microsoft, 2014). Firewalls are a business'sfirst line of defense and must be deployed irrespective of the size of the organisation(Khakpour & Liu, 2012). As growing numbers of businesses expose their networks to Internet traffic, firewalls are becoming a necessity (Laudon & Laudon, 2014).Attackers on a daily basis are undoubtedly probing companies witha constant Internet connection.Firewalls shield access to internal network services, and block certain kinds of attacks through packet filtering(Alkandary & Alhallaq, 2016).It is important to note that firewallsdo not protect against malicious traffic thattravels through legitimate communicationchannels. Software firewalls offer a good backupto a hardware solution, but only work onthe computer on which it is installed(Microsoft, 2014).

Update Software

Updating of software includes all applicationsand operating systems and leads to the issue ofpatch management. In 2002, 70 percent of successfulattacks exploited application vulnerabilities.Of those attacks, 35 percent resultedfrom defects for which a patch had been issuedand 65 percent from misconfigured applications (Keller, et al., 2005). The patching processis one in which the patch issuer provides a disclosurethat details the very nature of the vulnerabilitythat it is about to correct. Becausepeople do not patch quickly enough, it giveshackers the time to exploit that vulnerabilityand infect systems before the patch is installed(Paul Lin, 2006). This makes it incredibly importantto keep all software updated to preventsecurity incidents. In the case of anti-virus andspyware applications, the program is only asgood as the last update (Erlanger, 2003). An updateis necessary to capture the signatures ofthe latest and greatest threats.

Protect against Viruses, Worms, and Trojans

Anti-virus software consists of computer programs that attempt to identify, thwart and eliminate computer viruses and other malicious software (malware)(Alkandary & Alhallaq, 2016).Anti-virus software should be installed on allmachines to protect against security threats. Itis important to note that historically these programshave been largely reactive and respondto new threats by updating the known list of virussignatures(Hubbard & Forcht, 1998). They do not block new threatswithout a program update and offer no protectionagainst previously unknown threats. Somesoftware vendors now push the updates out tousers, which may offer better protection forshort-handed staffs. Some companies in theanti-virus industry are developing productsthat provide a more proactive defense. The bestnew products are providing a variety of securityprotection, including monitoring for spam, viruses, and spyware (Keller, et al., 2005).

Implement a Strong Password Policy

Even though these newer technologies are being gradually adopted, the user name and password authentication method remains the most widely used procedure for protecting data (Sun, et al., 2011).Implementing a strong password policy includesnot only developing and enforcing thepolicy, but also educating employees abouthow they should be protecting their passwords.Thorough control of passwords is aneasy and effective first step in maintaining informationsecurity (Keller, et al., 2005). Passwordsshould never be written down by employees orposted in any public or commonly accessibleplace, but users frequently do.According to Sun, et al.(2011), the level of protection offered by passwords is directly related to their complexity.A strong password is defined as havingmore than eight characters, at least one changeof case, a number that is not at the end, and anon-alphanumeric character such as # or * thatis also not at the end of the password (Helkala & Bakås, 2014).

Implement Physical Security Measures to Protect Computer Assets

Physical security measures can be as simple asputting locks on doors and adopting a DisasterRecovery Plan (Abu Musa, 2007). Steps towardachieving better physical security begin withmaking a record of equipment serial numbers foridentification and limiting access to equipmentsuch as servers and fax machines (Microsoft, 2014). This also includes trash management toensure that all secure documents are disposedof properly, which should be enforced by companypolicy. Sensitive areas should have accesspoints for identification of personnel, andcould include guarded entrances and exits.Backup storage sites are another physical securitymeasure, and are effective when used regularly.A network infrastructure map shows howthe network is set up and the devices that protectit, and should be treated as a sensitiveitem. Such knowledge in the hands of a hackeris equivalent to a roadmap to the system’s frontdoor.

Implement Company Policy and Training

As mentioned previously, employees and thoseinternal to the company generate a significant risk to the business. It is logical to assume thata company would address the biggest risk to informationsecurity by implementing employeeawareness and training. This is not, however,statistically the case. Employee training andawareness were the lowest on the list of toppriorities for information security spending, at16 and 13 percent, respectively (Keller, et al., 2005), and 70 percent of the respondentsto the Ernst and Young 2004 security surveydid not mention security training as a topinitiative (Keller, et al., 2005). Similarly, inthe 2004 CSI survey of mid- and large-sized companies, most respondents believed that securitytraining is very important, but many donot believe their company is spending enoughon security training (Gordon, et al., 2004). Unfortunately,training and security awareness aregenerally the first areas cut in times of budgetreductions, largely because the direct benefitof security training is difficult to determine(Schultz, 2004).

Connect Remote Users Securely

The remote access technology has advanced corporate productivity, provided online information, facilitated flexible work schedule, and improved business communication (Chou, et al., 2005). Both public and private networks provide the means by which information can be accessed.Many companies have mobile employees thatneed to access the company’s intranet or network infrastructure from a remote location, such as from home(Harris & Patten, 2014). Virtual private network (VPN)technology has been a tool to accomplish thiscommunication over the Internet through securetunnels, which contain encrypted data.The use of VPNs requires authentication toidentify legitimate users(Chou, et al., 2005).

Lock Down Servers

Management of servers is critical in today’sworld. Limiting what a server can do and whatit will allow is an effective way to protect thiscrucial network component. First of all, limitingexposure to the server is always a goodidea. Blocking ports that are not needed for operationsalso limits exposure. Internet-facing serversshould also be hardened. Servers can also beused to limit administrative privileges. Serverscan control PC operation and prevent userswho do not have administrative privileges fromdownloading unauthorized programs. This isan important tool that some companies haveutilized to limit vulnerability to viruses that attachthemselves in programs.

Implement Identity Services (Intrusion Detection)

Intrusion Detection Systems (IDSs) are designed to detect network attacks in progress and assist in post-attack forensics, whileaudit trails and logs serve a similar function for individual systems(Alkandary & Alhallaq, 2016). Typically, an intrusion detection device is a networkappliance that sits on a mirrored networkswitch port and inspects traffic betweenswitches in search of malicious bit patterns. It uses statistical anomaly or pattern-matching detection(Jain, et al., 2014). These systems can alsobe host based. It is a good idea to use intrusiondetection systems along with access controlsbecause access controls alone can be fooled byauthorized yet malicious users (Keller, et al., 2005).According to the 2004 CSI survey, 68 percentof respondents indicated the use of intrusiondetection systems and another 45 percent have invested in the more proactive technologycalled intrusion prevention (Gordon, et al., 2004).

III. Methodology

The sample for the study was drawn from a selection of SMEs who use point of sale systems for their daily transactions. A survey questionnaire was distributed to 32 randomly selected participants in the city of Kwekwe CBD. The objective of the Questionnaire was to investigate the security measures and practices in the organisations. The issues covered included firewalls, antivirus software, software updates and configurations, passwords, physical security and connection to remote servers.

IV. Results

The main objective of this study was to investigate the implemented security measures and practices in Zimbabwean SMEs. A list of 8 recommended measures was drawn from the review of literature. The questions in this section were structured and asked in order to investigate whether the recommended measures have been implemented. The statistical results for each investigated measure shall be presented.

Install and Properly Configure a Firewall

The following questions were presented in order to investigate if a firewall had been installed and properly configured:

1. *Do you have a firewall installed?*

2. *If the response in (1) above is yes, is the firewall properly configured?*

i. *How often is the firewall reconfigured?*

14 respondents, representing 46.7% of the research sample, indicated that they had no fire wall installed while 16 respondents, representing 53.3% of the research sample, indicated having firewalls installed. 9 respondents, representing 30% of the research sample, indicated that they had firewalls which had not been properly configured while 7 respondents, representing 23.3% of the research sample, indicated having properly configured firewalls. In terms of the frequency of reconfiguration, respondents qualified their response with the general indication that reconfigurations were only done when it was thought to be necessary.

Update Software

The following questions were presented to the respondents in order to investigate if software updates were carried out and the frequency of the updates:

3. *Do you carry out software updates?*
i. *How often?*

4 respondents, representing 13.3% of the research sample, indicated that they did not perform software updates while 26 respondents, representing 86.7% of the research sample, indicated that they carried out software updates. Responding to the frequency of updates question, 3 respondents, representing 10% of the research sample, indicated carrying out weekly updates. 21 respondents, representing 70% of the research sample, indicated carrying out updates once a month and 4 respondents, representing 13.3% of the research sample indicated carrying out software update when need arises.

Protect against Viruses, Worms, and Trojans

The following questions were presented to the respondents in order to investigate if their systems had protection against Viruses, Worms and Trojans:

4. *Does your system have antivirus software?*
    i. *How often do you update the software*?

5 respondents, representing16.7% of the research sample, indicated that they had no antivirus software installed while 25 respondents, representing 83.3% of the research sample, indicated that they had antivirus software installed. 2 respondents, representing 6.7% of the research sample, indicated that they carried out antivirus updates weekly. 20 respondents, representing 66.7% of the research sample, indicated that they carried out antivirus updates monthly. 3 respondents, representing 10% of the research sample, indicated caring out antivirus updates on a yearly basis

Implement a Strong Password Policy

The following questions were presented to the respondents in order to investigate if they had a strong password policy.

5. *Do you have a password policy?*
   i. *How long should be the password?*
   ii. *What characters constitute your passwords?*
   iii. *What other additional measures are included in your password policy? Please specify.*

11 respondents, representing 36.7% of the research sample, indicated that they did not have a password policy while 19 respondents, representing 63.3% of the research sample, indicated that they had a password policy. 20 respondents, representing 66.7% of the research sample, indicated that they had no specified password length. 5 respondents, representing 16.7% of research sample, indicated that their password ranged between 5 and 8 characters in length. 5 respondents, representing 16.7% of the research sample, indicated having password lengths of 8 characters and greater. 11 respondents, representing 36.7% of the research sample, indicated that their password consisted of numbers only while 19 respondents, representing 63.3% of the research sample, indicated that their passwords consisted of letters and numbers.

Implement Physical Security Measures to Protect Computer Assets

The following question was presented to the respondents in order to investigate if they had implemented security measures to protect their computer assets:

6. *Are there any physical security measures to protect computer assets?*

9 respondents, representing 30% of the research sample, indicated that they had not implemented any physical security measures to protect their computer asserts while 21 respondents, representing 70% of the research sample, indicated that they had implemented physical security measures to protect their computer assets.

Implement Company Policy and Training

The following questions were presented to the respondents in order to investigate if they had an IT policy and whether they offered training on the policy or not:

7. *Does your organisation have an IT policy*
8. *If the response is yes above does it offer training on the policy?*

All of the respondents (100%) indicated that their organisations did not have an IT policy. In observed cases, respondents indicated that the absence of an IT policy was mainly due to the organisations not being able to have a dedicated IT unit/department

Connect Remote Users Securely

The following questions were presented to the respondents in order to investigate if they connected remote users securely:

9. *Do you have remote users?*
10. *If the response is yes above, do you connect remote users securely?*

All the respondents (100%) indicated that they did not have remote users. It was however noted during observation that some respondents had remote connections to a back office for posting reports and day end reports. Because of this, secure connection to remote users may, to some extent, be considered an unreliable data item in this research.

Lock Down Servers

The following question was presented to the respondents in order to investigate if the servers were secured

11. *Is the server room secured?*

8 respondents, representing 26.7% of the research sample, indicated having secured server rooms. 6 respondents, representing 20% of the research sample, indicated that they did not have secured server rooms. 16 respondents, representing 53.3% of the research sample, did not have servers thus had no need for secured server rooms

Implement Identity Services (Intrusion Detection)

The following questions were presented to the respondents in order to investigate if the organisation had a properly configured intrusion detection system:

12. *Does the organisation have an intrusion detection mechanism?*
    i. *How often is the mechanism configured?*

All the respondents (100%) indicated that they did not have intrusion detection systems. In the observed cases the majority of respondents were not even aware of the existence of such systems.

V. Conclusion

Most of the recommended IS security measures for small businesses that were identified in the literature review have been implemented in SMEs though with varying consistency. However, three measures have been identified which none of the respondent SMEs have implemented and these are;

i. Company IT policy and training,
ii. Secure connection to remote server and
iii. Installation of intrusion Detection systems.

With most of the SMEs in the country not having constant connectivity to the internet and external LANs it can be admissible in the Zimbabwean context for the security measures not to be implemented as it is not a necessity. But however, with the increasing rate of Broadband penetration in the country and decreasing costs of internet connectivity the above scenario may not remain admissible. Also, it can be noted that most of the respondents do not have connections to remote servers or remote data entry points thus justifying the absence of secure remote connections. An issue of concern, however, is the absence of an IT policy and training for all the respondents. It can be noted that this is in line with the fact earlier alluded to, in the literature review, that SMEs lack the financial, operational and technical resources to make their organisation electronically secure.

VI. Recommendations

As a result of the literature review and survey findings, broad recommendations have been made to enable the Zimbabwean SMEs to make their organisations more electronically secure. The recommendations are that SMEs:

- Form consortiums to enable them to outsource IT expertise for the development of IT policy and training
- Formalise the on the job training process to include professional tutors/trainers
- Enhance their knowledge on the different threats to enable the implementation of preventive measures.
- Carry out software and antivirus updates frequently (i.e. whenever a patch or an update is available).

References

[1] Sai, K. O. S., Gumbo, R., Mzikamwi, T. & Ruvinga, C., 2015. Classification of Point of Sale nformation Security Threats: Case of Smes In Zimbabwe.. *Research Inventy: International Journal of Engineering And Science,* 5(9), pp. 33-36.

[2] Alkandary, Y. H. A. & Alhallaq, F. M. A., 2016. Computer Security. *International Journal of Advanced Research in Computer and Communication Engineering,* 5(1), pp. 1-6.

[3] Keller, S. et al., 2005. Information Security Threats and Practices in Small Businesses. *Information Systems Management: Security, Ethics, and Legal Issues,* 1(1), pp. 7-18.

[4] Microsoft, 2014. *Microsoft Safety & Security Center.* [Online] Available at: https://www.microsoft.com/security/pc-security/firewalls-whatis.aspx [Accessed 2 February 2016].

[5] Khakpour, A. & Liu, A., 2012. *First Step toward Cloud-Based Firewalling.* Irvine, CA, IEEE, pp. 41-50.

[6] Laudon, K. C. & Laudon, J. P., 2014. *Management Information Systems: Managing the Digital Firm.* 14 ed. Essex: Pearson Education Limited.

[7] Paul Lin, P., 2006. System Security Threats and Controls. *The CPA Journal,* pp. 58-66.

[8] Erlanger, L., 2003. *Top Five Myths About Safe Surfing.* New York: PC Magazine.

[9] Hubbard, J. C. & Forcht, K. A., 1998. Computer viruses: how companies can protect their systems. *Industrial Management & Data Systems,* 98(1), pp. 12-16.

[10] Sun, J., Ahluwalia, P. & Koong, K. S., 2011. The more secure the better? A study of information security readiness. *Industrial Management & Data Systems,* 111(4), pp. 570-588.

[11] Helkala, K. & Bakås, T. H., 2014. Extended results of Norwegian password security survey. *Information Management & Computer Security,* 22(4), pp. 346 - 357.

[12] Abu Musa, A. A., 2007. Evaluating the security controls of CAIS in developing countries: An examination of current research. *Information Management & Computer Security,* 15(1), pp. 46-63.

[13] Gordon, L. A., Loeb, M. P., Lucyshyn , W. & Richardson, R., 2004. *2004 CSI/FBI Computer Crime and Security Survey,* New York: Computer Security Institute.

[14] Schultz, E., 2004. Security training and awareness – Fitting a square peg in a round hole. *Computers and Security,* 23(1), pp. 1-2.

[15] Chou, D. C., Yen , . D. C. & Chou, A. Y., 2005. Adopting virtual private network for electronic commerce. *Industrial Management & Data Systems,* 105(2), pp. 223 - 236.

[16] Harris, M. A. & Patten, K. P., 2014. Mobile device security considerations for small- and medium-sized enterprise business mobility. *Information Management & Computer Security,* 22(1), pp. 97-114.

[17] Jain, A., Verma, B. & Rana, J. L., 2014. Anomaly Intrusion Detection Techniques: A Brief Review. *International Journal of Scientific & Engineering Research,* 5(7), pp. 1372-1383.