IRA-International Journal of Education & Multidisciplinary Studies
ISSN 2455–2526; Vol.06, Issue 02 (2017)
Pg. no. 181-190
Institute of Research Advances
https://research-advances.org/index.php/IJEMS

An Analysis of Point of Sale Systems Physical Configurations and Security Measures in Zimbabwean SMEs

Kundai Oliver Shadwell Sai

Lecturer, Department of Mathematics and Computer Science, Great Zimbabwe University, Masvingo, Zimbabwe.

Type of Review: Peer Reviewed.
DOI: http://dx.doi.org/10.21013/jems.v6.n2.p5

How to cite this paper:
Sai, K. (2017). An Analysis of Point of Sale Systems Physical Configurations and Security Measures in Zimbabwean SMEs. *IRA International Journal of Education and Multidisciplinary Studies* (ISSN 2455-2526), 6(2), 181-190. doi:http://dx.doi.org/10.21013/jems.v6.n2.p5

Disclaimer: The scholarly papers as reviewed and published by the Institute of Research Advances (IRA) are the views and opinions of their respective authors and are not the views or opinions of the IRA. The IRA disclaims of any harm or loss caused due to the published content to any party.

ABSTRACT

This paper undertook to establish the correlation between the Point of Sale configurations (setup) employed by Small and Medium Enterprises and the security controls and measures implemented for the prevention and detection of possible security threats. Quantitative data was collected from 30 Small and Medium Enterprises in the retail sector using a self-administered questionnaire. The participants were selected using purposive sampling. The data was analysed using descriptive statistics and the Chi square test was used to test for correlation between the variables. The research showed that only three of the recommended security measures for Small and Medium Enterprises are directly affected by the Point of Sale configuration in use and these are: Password Policy; Physical Security and Antivirus.

Key Words: Configuration, Point of Sale, POS, Security Measures, Setup, SMEs

Introduction

Small and medium enterprises (SMEs) represent a substantial part of retail businesses in Zimbabwe. Most of these enterprises have since migrated from the use of cash registers and manual sales systems to the use of electronic systems known as Point of Sale (POS) Systems. This change has ominously enriched check-out counter services, improved efficiency and accountability and also enhanced the stock taking aptitudes of merchants. The introduction of electronic POS systems has, conversely, presented new risks in terms of guaranteeing the security and integrity of data.

Small businesses usually have smaller amounts of resources as well as accessible money and technical proficiency with which to make their business electronically secure (Mills & McCarthy , 2014; Business Security Information, 2013). This suggests that Point of sale (POS) Systems for SMEs face a great threat of security breaches. The majority of Information Systems (IS) controls, which can also be applied to POS Systems, are built upon two fundamental ideologies of the need to protect against loss or damage and the need to ensure data accuracy (Hardcastle, 2011).

According to Abu-Musa (2008) technology has been, more often than not, advanced faster than the progression in control practices and this technological advancement has not been combined with similar improvement of the employees' knowledge, skills, awareness, and compliance. Zimbabwe is not an exceptional case as in most cases the introduction of new systems is not automatically reinforced by required skills and educational improvements. This research undertakes to establish if there is a relationship between the POS configuration adopted by an SME and the security controls and measures implemented for the prevention and detection of possible security threats. With the results of the research we can be able to identify the subgroups within the SMEs that are more vulnerable to security threats.

Literature Review

Point Of Sale System Definition

A point of sale (POS) can be generally defined as a point at which a sale is made, the ownership (and usually the possession) is conveyed from the retailer to the buyer, and indirect taxes (such as VAT) become payable. A point of sale is, commonly, a retail outlet. Kim & Kim (2007) define a point of sale system as a "supply net administration system for customer management" which delivers real time control of merchandise in stock and sale analysis. According to Ellram, et al. (1999), POS systems deliver valuable, near-real-time information on sales, such a system can be used to update inventory stock status and generate purchase orders as needed. POS systems can make effective use of consumer's sale data which is essential to introduce Customer Relationship Management (CRM) and Supply Chain Management (SCM).

Pos Categories

According to Kim & Lim (2011) there are a number of POS system categories. A typical POS system comprises of several client computers connected through privately owned connection lines, such as the electronic data exchange (EDI), with local servers at one or more stores (Figure 1). The server runs all data processes for these on-line POS systems, while the client computers provide the user-interface operations. Stemming from this strong, server-dependent design is the need to maintain the connection between the server and the clients throughout the processing of a sales transaction as disconnection will result in data loss and force the client(s) to suspend all transactions (sales/entries) until the link is re-established. Subsequently, in this type of POS system, disconnection from the server can be a major hazard, and small business owners, who are vulnerable to the frustrations of their customers, may have to bear the expense of having an in-house server at each store location.

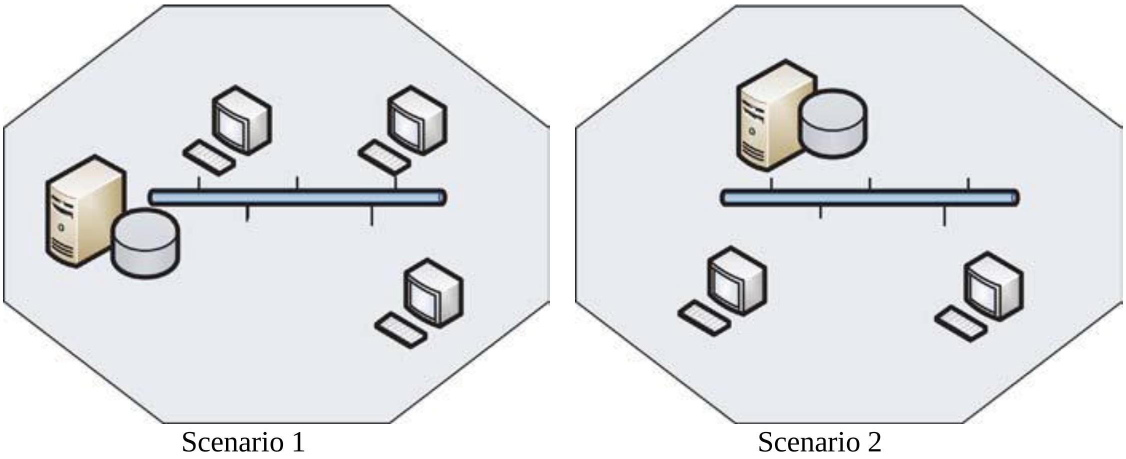

Figure 1: Local client server model for POS system.

Another type of POS system is an off-line, batch-based POS system. In this system, all clients are capable of processing all transactions with their local data cache, and processed transactions can be transmitted to the server periodically or on demand. For example, salespersons would upload the records of transactions in their handheld POS terminals (clients) when they go off duty. Since this type of off-line POS system is naturally immune to the hazard of being disconnected from the server and does not collect real-time information from its clients, the system will be adequate for certain a business environment in which there is weak or limited network connectivity.

Recommended Security Measures for SMEs

Install and Properly Configure A Firewall

According to Microsoft, firewalls are a business's first line of defence. As growing numbers of businesses expose their networks to Internet traffic, firewalls are becoming a necessity (Laudon & Laudon, 2006, p. 340). Attackers on a daily basis are undoubtedly probing companies with a constant Internet connection. The two basic types of firewalls are hardware and software firewalls. They work by blocking all traffic that is not explicitly allowed. These rules should reflect the company's security policy. It is important to note that firewalls do not protect against malicious traffic that travels through legitimate communication channels. Software firewalls offer a good backup to a hardware solution, but only work on the computer on which it is installed (Microsoft, 2004 in (Keller, Powell, Horstmann, Predmore, & Crawford, 2005)).

Implement A Strong Password Policy

Implementing a strong password policy includes not only developing and enforcing the policy, but also educating employees about how to protect their passwords. Thorough control of passwords is an easy and effective first step in maintaining information security (Phillips, (2002) in (Keller, Powell, Horstmann, Predmore, & Crawford, 2005)). Employees should be discouraged from the usual practice of writing down passwords or posting them in any public or commonly accessible place. A password can be considered to be strong if it consists of more than eight characters, a number that is not at the end, at least one change of case, and a non-alphanumeric character such as # or * that is also not at the end of the password (Panko, 2003)

Protect against Viruses, Worms and Trojans

Anti-virus software should be installed on all machines to protect against security threats. It is important to note that historically these programs have been largely reactive and respond to new threats by updating the known list of virus signatures. Anti-virus software has no ability to block new threats without a program update and do not offer protection from previously unknown threats. Some software vendors now push out the updates to users, which may offer better protection for short-handed staffs. Some companies in the anti-virus industry are developing products that provide a more proactive defence. The best new products are providing a variety of security protection, including monitoring for spam, viruses, and spyware (Robbins, 2004 in (Keller, Powell, Horstmann, Predmore, & Crawford, 2005)).

Update Software

Updating of software includes all applications and operating systems and leads to the issue of patch management. In 2002, 70% of successful attacks exploited application vulnerabilities while 65% resulted from misconfigured applications and 35% resulted from defects for which a patch had been issued (Desmond, 2004). During the patching process, the patch issuer provides an exposé of the very nature of the vulnerability that it is about to correct. Hackers are afforded the time to exploit that vulnerability and infect systems before the patch is installed as users do not patch quickly enough (Berinato, 2003). Thus it becomes extremely imperative to keep all software updated in order to prevent security incidents. In the case of spyware and anti-virus applications, the program is only as good as the last update (Erlanger, 2003 in (Keller, Powell, Horstmann, Predmore, & Crawford, 2005)). An update is necessary to capture the signatures of the latest and greatest threats.

Implement Physical Security Measures to Protect Computer Assets

Physical security measures can be as simple as putting locks on doors and adopting a Disaster Recovery Plan (Abu-Musa, Investigating the security policies of computerized accounting information systems in the banking industry of an emerging economy: the case of Egypt, 2004). Steps toward achieving better physical security begin with making a record of equipment serial numbers for identification and limiting access to equipment such as servers and fax machines (Microsoft, (2004) in (Keller, Powell, Horstmann, Predmore, & Crawford, 2005)). This also includes trash management to ensure that all secure documents are disposed of properly, which should be enforced by company policy. Sensitive areas should have access points for identification of personnel, and could include guarded entrances and exits. Backup storage sites are another physical security measure, and are effective when used regularly. A network infrastructure map shows how the network is set up and the devices that protect it, and should be treated as a sensitive item. Such knowledge in the hands of a hacker is equivalent to a roadmap to the system’s front door.

Implement Company Policy and Training

As mentioned previously, employees and those internal to the company generate a significant risk to the business. It is logical to assume that a company would address the biggest risk to information security by implementing employee awareness and training. This is not, however, statistically the case. Employee training and awareness were the lowest on the list of top priorities for information security spending, at 16% and 13%, respectively (Ernst and Young, 2003), and 70% of the respondents to the Ernst and Young 2004 security survey did not mention security training as a top initiative (Ernst and Young, 2004). Similarly, in the 2004 CSI survey of mid- and large-sized companies, most respondents believed that security training is very important, but many do not believe their company is spending enough on security training (Gordon et al., 2004). Unfortunately, training and security awareness are generally the first areas cut in times of budget reductions, largely because the direct benefit of security training is difficult to determine (Schultz, 2004).

Connect Remote Users Securely

Many companies have mobile employees that need to access the company's intranet or network infrastructure from a remote relocation, such as the home. Virtual private network (VPN) technology has been a tool to accomplish this communication over the Internet through secure tunnels, which contain encrypted data. The use of VPNs requires authentication to identify legitimate users.

Lock Down Servers

In today's world Server Management is a critical task (Keller, Powell, Horstmann, Predmore, & Crawford, 2005). The server is a crucial network component that can be effectively protected by limiting what it can do and what it will allow. Servers can control the operation of PCs and inhibit users without the requisite administrative privileges from downloading unauthorised programs. This is an important tool that is utilised by some enterprises in an effort to limit vulnerability to viruses that attach themselves to programs (Keller, Powell, Horstmann, Predmore, & Crawford, 2005).

Implement Identity Services (Intrusion Detection)

An intrusion detection device is typically a network appliance that sits on a mirrored network switch port inspecting traffic between switches and searching for malicious bit patterns using statistical anomaly or pattern-matching detection (Wexler, 2004).Access controls alone, can be fooled by authorised yet malicious users hence it is advisable to use them along with intrusion detection systems (IDS) (Liu, Jajodia, & McCollum, 2000). According to the 2004 CSI survey, 68% of respondents indicated the use of intrusion detection systems and another 45% have invested in the more proactive technology called intrusion prevention (Gordon, Loeb, Lucyshyn, & Richardson, 2004).

Methodology

The Quantitative Research approach was utilised in this study. Data was generated in quantitative form so as to subject it to quantitative analysis. The data was collected using a self-administered questionnaire with close-ended type questions. The questionnaire was administered to 32 SMEs and 30 complete questionnaires were returned representing a 93.75 response rate. The respondents were selected using purposive sampling. The questionnaires were analysed using descriptive statistics and the Chi Square test.

The following hypothesis is developed to test for the relationship:

> H0: Implemented POS setup has no effect on the implemented security measure for Zimbabwean SMEs.

Results and Discussion

Functional Point of Sale Stations

A total of 18 respondents, representing 60% of the research sample had 1 functional POS station, 8 respondents representing 26.7% of the research sample had 2 functional POS stations and 4 respondents representing 13.3% of the research sample had 3 functional POS stations. None of the respondents indicated having more than 3 functional POS stations. Given the financial and resource limitations facing small businesses it is logical that most of the respondents (86.7%) had less than 3 functional POS stations. Table 4.2 below gives a summary of the results.

Table 1: POS Stations

	Frequency	Percentage	Valid Percentage	Cumulative Percentage
1 Station	18	60.0	60.0	60.0
2 Stations	8	26.7	26.7	86.7
3 Stations	4	13.3	13.3	100.0
Total	30	100.0	100.0	

Pos Setup

14 respondents, representing 46.7% of the research sample, indicated having a client server setup, 8 respondents representing 26.7% of the research sample had standalone setup while 8 respondents, representing 26.7% of the research sample, indicated that they had a standalone with a back-office link. Table 4.3 below gives a summary of the results.

Table 2: POS Setup

	Frequency	Percentage	Valid Percentage	Cumulative Percentage
Client Server	14	46.7	46.7	46.7
Stand Alone	8	26.7	26.7	73.3
Stand Alone with Back Office Link	8	26.7	26.7	100.0
Total	30	100.0	100.0	

Security Measures against POS Configuration

Table 3 below shows the summary of results for the security measures for each POS set-up. None of the surveyed SMEs indicated having Intrusion Detection Systems, an IT policy are any form of IT policy training.

Table 3: Security Measures against POS Configuration

		setup		
		client server	stand alone	stand alone with back office link
		Count	Count	Count
INTRUSION DETECTION UPDATE FREQUENCY	never	14	8	8

INTRUSION DETECTION SYSTEM	no	14	8	8
	yes	0	0	0
SERVER ROOM SECURED	no	11	8	6
	yes	3	0	2
REMOTE CONNECTION SECURE	no	0	0	0
	yes	0	0	0
	n/a	14	8	8
REMOTE USERS	no	14	8	8
IT POLICY TRAINING	no	14	8	8
IT POLICY	no	14	8	8
PHYSICAL SECURITY MEASURES	no	4	2	3
	yes	10	6	5
PASSWORD CHARACTERS	numbers	6	2	3
	letters and numbers	8	6	5
PASSWORD LENGTH	unspecified	10	5	5
	more than 5 characters but less than 8	1	2	2
	more than 8 characters	3	1	1
PASSWORD POLICY	no	4	3	4
	yes	10	5	4
ANTIVIRUS UPDATE FREQUENCY	never	3	2	0
	weekly	0	2	0
	monthly	8	4	8
	yearly	3	0	0
ANTIVIRUS INSTALLED	no	3	2	0
	yes	11	6	8
SOFTWARE UPDATE FREQUENCY	weekly	1	1	1
	monthly	10	4	7
	yearly	0	0	0
S/W UPDATES	no	3	1	0
	yes	11	7	8
CONFIGURATION DONE	never	11	5	6
	other	3	3	2
FIREWALL CONFIGURED	no	4	4	1
	yes	2	2	3
	n/a	8	2	4
HAS FIREWALL	no	8	2	4
	yes	6	6	4

Physical Security Measures

Of the surveyed SMEs, only 3 respondents with the client server POS configuration had a secured server room while 2 of the respondents with a standalone POS setup with a back office link had secured server rooms. The majority of respondent across the 3 POS setup classes considered for this research indicated that they had implemented some sort of physical measures ranging from burglar bars, rapid response systems and enlisting the services of security personnel.

Password Policy

8 respondents with the client-server setup indicated having a mixture of numbers and letters for their passwords while 6 respondents from the same category indicated the use of numbers only for their

passwords. 6 respondents with standalone POS systems indicated having a mix of words and numbers foe their password while 2 respondents indicated that they only used numbers for their passwords. For the respondents with the back office link setup, 3 indicated using numbers only while 5 indicated using both numbers and letters for their passwords. It was however noted that none of the respondents across the divide indicated the inclusion of special characters in their passwords.

Anti-Virus Protection

11respondents with client server setup, 6 respondents with standalone and 8 respondents with back office link indicated that they had installed antivirus software. However 3 respondents with client server setup indicated carrying out updated at least once a year while 8 respondents carried out monthly antivirus updates. 2 respondents with standalone setup had weekly updates while 4 respondents updated monthly.

Firewalls

Of all the respondents with the client server setup, 6 indicated having firewalls while 6 respondents with standalone setup and 4 respondents with back office link indicated the same. 2 respondents with the client server setup had their firewall was properly configures while 2 and 3 respondents with the standalone and back office link setups also indicated that their firewalls were properly configured

Chi Square Analysis

The table below show the results of the Chi Square tests conducted on the data. The decision to accept or reject the null hypothesis was done at 5% level of significance (reject H0 if X^2calculated > X^2 critical).

Table 4:Pearson Chi-Square Tests

		setup
SERVER ROOM SECURED	Chi-square	6.88
	df	2
	Critical Chi-square	6.00
PHYSICAL SECURITY MEASURES	Chi-square	.323
	df	2
	Critical Chi-square	6.00
PASSWORD CHARACTERS	Chi-square	6.702
	df	2
	Critical Chi-square	6.00
PASSWORD LENGTH	Chi-square	1.875
	df	4
	Critical Chi-square	9.50
PASSWORD POLICY	Chi-square	.010
	df	2
	Critical Chi-square	6.00
ANTIVIRUS UPDATE FREQUENCY	Chi-square	12.643
	df	6
	Critical Chi-square	12.60
ANTIVIRUS INSTALLED	Chi-square	8.229
	df	2
	Critical Chi-square	6.00
SOFTWARE UPDATE FREQUENCY	Chi-square	3.865
	df	4
	Critical Chi-square	9.50
S/W UPDATES	Chi-square	2.030

	df	2
	Critical Chi-square	6.00
HAS FIREWALL	Chi-square	2.162
	df	2
	Critical Chi-square	6.00

From the Chi square analysis above it can be concluded that the POS configuration utilised by the respondent is related to the following security measures: Password Policy; Physical Security and Antivirus. However the test showed no statistical correlation between the POS configuration and the following security measures: Intrusion Detection Systems, IT policy, Firewall, Software Updates, Server Room Security and Firewalls. No meaningful results were obtained for issues to do with remote connections as all respondents indicated not having any remote connections or VPNs.

Conclusion

The research showed that only three of the recommended security measures for SMEs are directly affected by the POS configuration in use and these are: Password Policy; Physical Security and Antivirus. This study did not further elaborate on the reasons why the said factors are seen to be dependent on the POS configuration and why the rest are not. An exposition of those reasons may be subject to further study.

BIBLIOGRAPHY

Abu-Musa, A. A. (2004). Investigating the security policies of computerized accounting information systems in the banking industry of an emerging economy: the case of Egypt. *The Business Review of Information Systems, 8*(3), 83-102.

Abu-Musa, A. A. (2008). Information technology and its implications for internal auditing: An empirical study of Saudi organizations. *Managerial Auditing Journal, 23*(5), 438 - 466.

Berinato, S. (2003). FrankenPatch. *CIO.*, 100-110.

Business Security Information. (2013). *Business Security Information*. Retrieved January 26, 2016, from http://www.businesssecurityinformation.com/2013/06/business-security-why-small-businesses-should-take-action/

Desmond, P. (2004, May 17). *All Out Blitz against Web App Attacks*. Retrieved January 22, 2016, from http://www.nwfusion.com/techinsider/2004/0517techinsidermain.html

Ellram, L. M., La Londe, B. J., & Weber, M. M. (1999). Retail Logistics. *International Journal of Physical Distribution & Logistics Management, 29*(7), 477 – 494.

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Richardson, R. (2004). *CSI/FBI Computer Crime and Security Survey*. Computer Security Institute.

Hardcastle, E. (2011). *Business information Systems* (1st ed.). Venturus Publishing.

Keller, S., Powell, A., Horstmann, B., Predmore, C., & Crawford, M. (2005). Information Security Threats and Practices in Small Businesses. *Information Systems Management-SECURITY, ETHICS, AND LEGAL ISSUES*, 12-14.

Kim, S.-s., & Kim, T.-h. (2007). POS System Design in Security Level 1st. *International Journal of Multimedia and Ubiquitous Engineering, 2*(3), 131-136.

Kim, Y.-G., & Lim, J. (2011). A POS system based on the remote client-server model in the small business environment. *Management Research Review, 34*(12), 1334-1350.

Laudon, K. C., & Laudon, J. P. (2006). *Management Information System: Managing the digital firm* (9th ed.). New Jersey: Prentice-Hall.

Liu, P., Jajodia, S., & McCollum, C. D. (2000). Intrusion confinement by isolation in information systems. *Journal of Computer Security - Special issue on database security, 8*(4), 243-279.

Mills, K. G., & McCarthy , B. (2014). STATE OF SMALL BUSINESS LENDING:CREDIT ACCESS DURING THE RECOVERY AND HOW TECHNOLOGY MAY CHANGE THE GAME. Havard Business School.

Panko, R. R. (2003). *Business Data Networks and Telecommunications.* New Jersey : Prentice Hall.

Wexler, J. (2004). *ComputerWorld*. Retrieved January 22, 2017, from http://www.computerworld.com/article/2574323/networking/sidebar--security-and-qos-lexicon.html