Research Inventy: International Journal of Engineering And Science
Vol.5, Issue 9 (September 2015), PP -33-36
Issn (e): 2278-4721, Issn (p):2319-6483, www.researchinventy.com

Classification of Point of Sale Information Security Threats: Case of Smes In Zimbabwe.

[1]Kundai Oliver S. Sai, [2]Raviro Gumbo, [3]Tinomuda Mzikamwi
[4]Caroline Ruvinga
[1]*Department of Mathematics and Computer Science, Faculty of Agriculture and Natural Sciences, Great Zimbabwe University, Masvingo*
[2,3,4]*Faculty of Science & Technology, Dept. of Computer Science & Information Systems, Midlands State University, Gweru, Zimbabwe.*

Abstract : This paper reports on the classification of information security threats to Point of Sale Systems in Zimbabwean small and medium enterprises (SME's). The classification was done according to the frequency of occurrence of the threat and recommendations were given on how to secure POS to ensure maximum benefits are achieved. An empirical survey on twenty retail SMEs was carried out using self administered questionnaires. The analyses of results revealed that eleven possible security threats with varying magnitude of occurrence. The rate of occurrence of each of the eleven prevalent security breaches was found to be dependent on duration under consideration. According to daily occurrence accidental entry of bad data and power loss are the most prevalent with creation of fictious /incorrect output being the least prevalent, weekly recording reveal that creation of fictious /incorrect output is the most prevalent and accidental entry of bad data and power loss the least predominant, intentional destruction of data by employees is the most prevalent in monthly classification whilst creation of fictitious/incorrect output is the most prevalent annually.The researchers recommended intensive formalization of on the job training and awareness workshops on information security so as to strike a balance between technical and non-technical security measures.
Key words: *Point of sale (POS), information security, threats, small and medium enterprises (SMEs)*

I.INTRODUCTION

Small and medium enterprises (SMEs) constitute a significant part of retail businesses nowadays and play a pivotal role in developing countries (Economy, 2004) . In a bid to improve efficiency and service delivery, most of these enterprises have since moved from the use of manual sales systems and cash registers to the use of electronic Point of Sale Systems (POS). Philppott (1974) alludes that cash registers are dead if not yet buried by the advent of the electronic era. This has seen point of sale systems becoming an integral part of retail systems in creating an exciting and compelling retail experience (Yeh 2006). The embracing of this technology by the retail businesses has significantly improved checkout counter services, increased accountability and also improved the stock taking capabilities of retailers. Some retailers report that they have experienced better stock replenishment, speeding up of checking out of customers and up-dating of stock records (1977). Modern point-of-sale (POS) system can record and track sales by a customer or employee, process credit and debit cards, connect to other systems over a network, and manage inventory (Sarrel, 2007). One can conclude that the adoption of POS by retailers has indeed availed numerous merits and business opportunities.

Electronic data processing has evolved overtime, Philpott (1974) states that retailing is not new. Point of sale systems vary in type (Whitley, 2000). A typical POS system generally consists of a computer, a cash drawer, a receipt printer, a monitor, a customer display (also known as a pole display), some applications, a database, and I/O devices such as barcode readers, scales, magnetic stripe readers, check readers, finger print readers, or keyboards (Sarrel, 2007). In this research paper a retail point of sale system was considered as comprising of a computer, monitor, cash drawer, receipt printer, customer display, a barcode scanner and debit/credit card reader. Point of sale systems have a lot of power beyond its basic use of capturing data and receipting, they help control costs and help build sales when used to their fullest (Peters, 2007). These POS can also record and track sales by customer or employee, process credit and debit cards, connect to other systems over a network and manage inventory (Sarrel, 2007). According to Strazewski (1996) new computerized and networked point-of-sale (POS) systems do more than record sales and issue register receipts: they help control inventory, monitor employee performance, manage customer loyalty programs and sometimes share information with other franchise stores.

The POS systems have become the centrepiece of retail store management (Strazewski 1996). However modernized information systems (IS) have brought retail enterprises not only enormous benefits, but have also exposed them to information threats (Yeh 2006). Statistics reveal the continues rise in magnitude and severity of information security related incidents (Yeh 2006). Retailors are not an exempted they also face a high risk of security breaches. In order to reap huge benefits related with implementation of POS, SMEs need to ensure adequate information security (Fitzgerald 1995). Information security aims at providing tools and mechanisms for protecting the confidentiality, integrity, and availability of information in the face of attacks (Pieters 2011). Loch et al (1992) defines information security threats as a "broad range of forces capable of producing adverse consequences". The Federal Financial Institutions Examinations Council (FFIEC) (2002) defines a threat as any entity that can take action against the computer system or the data. Information security threats can be put into several broad categories as follows: accidents, natural disasters, sabotage (industrial and individual), vandalism, theft, unauthorized use (hacking) and computer viruses (Hardcastle, 2011). According to Loch et al (1992) and Davis (1996) the list of possible security threats to POSs includes; accidental entry of bad data by employees, intentional entry of bad data by employees, accidental destruction of data by employees, intentional destruction of data by employees, unauthorized access to data/system by employees, inadequate control over media (disks and tapes), poor control over manual handling of input /output, access to data/system by outsiders (hackers), access to data/system by outsiders (competitors), entry of computer viruses and worms into computer system, weak ineffective or inadequate physical control and natural disaster: fire, flood, loss of power, loss of communications.

Most enterprises solve their IS security-related problems using technical means and managerial controls.(Yeh 2006). General avoidance of breaches rests on three pillars people, processes and technology (Krausz, 2010). Numerous ways of mitigating these information security threats can be employed such as physical security, policies, laws and many other ways to secure information (Abu-Musa, 2007, Tipton, 2012, Whitman, 2011). But in most cases, technology has been developed faster than the advancement in control practices and this advancement has not been combined with similar development of the employees' skills, knowledge, awareness, and compliance (Abu Musa, 2001). Zimbabwe is not an incomparable case as in most cases the introduction of new systems is not necessarily supported by necessary educational and skill improvements. This research sought to make Zimbabwean SMEs aware of the potential threats that can challenge their POS systems and provide knowledge on information security controls that can be implemented to counter or prevent the threat.

II. METHODOLOGY

Questionnaire

A random sample of twenty questionnaires were distributed to SME owners in the retail sector in order to find out information security threats being faced by their Point of Sale Systems in Zimbabwe.

III RESULTS

Table1. Demographic data

Respondents Gender		*Respondents Age (years)*			
		18-25	26-30	31-40	Above 40
Male	13	3	7	2	1
Female	7	1	3	2	1

The demographic data reflects that there are more male SME owners than females. The majority of the owners fall within the age group of 26-30 years and very few owners are above 40 years.

Table 2. SME threat experience.

Threat	**No**	**Yes**
Accidental entry of bad data by employees	0	20
Power Loss	0	20
Employees sharing passwords	5	15
Entry of computer viruses into system	1	19
Suppression/destruction of the output	1	19
Intentional entry of bad data by employees	2	18
Creation of fictitious/incorrect output	6	14
Accidentaldestruction of data by employees	2	18

Intentional destruction of data by employees	9	11
Sensitive documents handed to non-security personnel for destruction/shredding	5	15
Unauthorized document visibility	7	13

Table 2. Rate of threat occurrence

Threat	*Occurrence %*			
	Daily	*Weekly*	*Monthly*	*Annually*
Accidental entry of bad data by employees	100	0	0	0
Power	100	0	0	0
Employees sharing passwords	87	13	0	0
Entry of computer viruses into system	84	16	0	0
Suppression/destruction of the output	68	16	16	0
Intentional entry of bad data by employees	83	17	0	0
Creation of fictitious/incorrect output	7	65	21	7
Accidental destruction of data by employees	95	5	0	0
Intentional destruction of data by employees	45	10	45	0
Sensitive documents handed to non-security personnel for destruction/shredding	87	13	0	0
Unauthorized document visibility	54	15	31	0

According to daily occurrence rate, accidental entry of bad data and power loss are the most prevalent with creation of fictious /incorrect output being the least prevalent. Weekly recording reveal that creation of fictious /incorrect output as the most prevalent and accidental entry of bad data and power loss the least predominant. Intentional destruction of data by employees is the most prevalent in monthly classification whilst creation of fictitious/incorrect output is the most prevalent annually.

Table 4. Classification Position/ Ranking

The results reveal that threat occurrence varies with time dependent. All threats have some probability of occurrence.

Threats	*Daily Ranking Position*	*Weekly Ranking Position*	*Monthly Ranking Position*	*Annual Ranking Position*
Accidental entry of bad data by employees	1	10	5	2
Power Loss	1	10	5	2
Employees sharing passwords	4	6	5	2
Entry of computer viruses into system	6	3	5	2
Suppression/destruction of the output	8	3	4	2
Intentional entry of bad data by employees	7	2	5	2
Creation of fictitious/incorrect output	11	1	3	1
Accidental destruction of data by employees	3	9	5	2
Intentional destruction of data by employees	10	8	1	2
Sensitive documents handed to non-security personnel for destruction/shredding	4	6	5	2
Unauthorized document visibility	9	5	2	2

IV. Conclusion

Threats vary in the rate of prevalence according to duration under consideration. Out of the numerous security threats, eleven were found to have been experienced by the retailors. The results reveal that all the threats vary in probability of occurrence. SME owners need to be made aware on the risks posed by these threats to their current businesses. Information security breach by any one of these threats can result in a wide spectrum of

effects ranging from trivial to catastrophic. Hence there is need to formalise the on the job training process of employees to enhance their knowledge on the different information security threats. This will enable the effective implementation of preventive and counter measures since they are all hinged on human support. The owners also need to be educated on control measures that can be set up within a company since they are influential and at the center of the implementation of IS. Knowledge on information security will go a long way towards ensuring the growth and success of SMEs.

References

[1] Abu-Musa, Ahmad A., (2002), "Computer crimes: how can you protect your computerized accounting information system", The Journal of American Academy of Business, Vol. 2 No. 1, pp. 91-101.

[2] Abu-Musa, Ahmad A., (2004a), "The threats of computerized accounting information systems: an empirical study on Saudi organizations", The Public Administration Journal, Vol. 44 No. 3, pp. 509-70.

[3] Abu Musa, Ahmad A.,, (2006), "Exploring perceived threats of CAIS in developing countries: the case of Saudi Arabia", Managerial Auditing Journal, Vol. 21 Iss: 4 pp. 387 – 407

[4] Ahmad A. Abu-Musa, (2007),"Evaluating the security controls of CAIS in developing countries: an empirical investigation", Information Management & Computer Security, Vol. 15 Iss 2 pp. 128 - 148

[5] Davis, Charles E, (1996), "Perceived security threats in todays Accounting Information Systems: A survey of CISAs". IS Audit &Control Journal, Vol. 3, pp. 38-4.

[6] Davis, Charles E., (1997), "An assessment of accounting information security." CPA Journal, 07328435, Mar 1997, Vol. 66, Issue 3.

[7] ECONOMY, I. A. G. (2004). "PROMOTING SMEs FOR DEVELOPMENT."

[8] FFIEC, (2002), "FFIEC Audit Handbook", The Federal Financial Institutions Examination Council (FFIEC), Source: http://www.ffiec.gov

[9] Hardcastle, E. (2011), "Business information Systems." VenturusPublishing

[10] Kevin J. Fitzgerald, (1995),"Information security baselines", Information Management & Computer Security, Vol. 3 Iss 2 pp. 8 – 12

[11] Locke, L., Silverman, S., &Spirduso, W. (2010), "Reading and Understanding Research." 3rd Edition. Los Angeles, Sage.

[12]

[13] Philpott, W. J. (1974). "CAPTURING DATA AT THE POINT OF SALE." Retail and Distribution Management **2**(2): 14-16.

[14] Pieters, W. (2011). "The (Social) Construction of Information Security." Information Society **27**(5): 326-335.

[15] Strazewski, L. (1996). "Point-of-sale system: Retail's high tech aid." Franchise Times **2**(4): 26.

[16] Yeh, A. J.-T. C. Q.-J. (2006). "On security preparations against possible IS threats across industries." Emerald Insight **14**(4): 343 - 36

[17] (1974). "THE EXPLOSION AT THE POINT OF SALE." Retail and Distribution Management **2**(1): 36-41.

[18] (1977). "Data capture at point of sale." Retail and Distribution Management **5**(1): 34-35.