Universal Journal of Accounting and Finance 1(1): 9-18, 2013 http://www.hrpub.org
DOI: 10.13189/ujaf.2013.010102

Computerized Accounting Information Systems and Perceived Security Threats in Developing Economies: The Nigerian Case

Tijani Oladipupo Muhrtala[1,*], Mathias Ogundeji[2]

[1]Elizade University, Ilara-Mokin, Ondo-State, 23401, Nigeria
[2]72/82, Kudirat Abiola Way, Suite A1, Humuani Shopping Mall, Oregun, Ikeja, Lagos, Nigeria
*Corresponding Author: oladipupotijani@gmail.com

Abstract The concept of IT as a business enabler is enshrined in the widespread use of computerized accounting information system the world over. However, this milestone in accounting portends imminent challenges in terms of the integrity of underlying accounting transactions processed by IT equipment and facility, an important question arises: what are the likely threats to computerized accounting information systems resulting from the deployment of IT in business and how can these challenges be overcome especially in developing economies? To analyse this area of interest, Nigerian companies has been chosen as reference. An empirical study was conducted through a structured survey directed to the users of computerized accounting systems. Information was collected in order to explain the perceived threats common to CAIS's as well as determine what categories of threats were most significant. Results show that employees and outsiders constitute key threats to information assets used in computerized accounting when not controlled effectively. This suggests that management should put in place authorization procedures on a "need to know basis" only. Authorized users should have access to only applications and data required to perform specific tasks only. Also, there should be regular logging and monitoring of logical access to systems and data, policies and procedures on segregation of duties, access and transaction logs.

Keywords CAIS's, Information Assets, Threats, Employees, Nigeria

1. Introduction

Computerized Accounting Information Systems (CAIS) handles both financial and non-financial transactions that directly affect the processing of financial transactions. When changes are made to customers' data, for instance change in next of kin and/or address, these changes provide vital information for processing of future sales to such customers. The widespread adoption of user-friendly systems and the great desire to automate business processes has made organizations to acquire and implement systems and software which could come in form of turnkey systems (e.g. generalized accounting systems, special-purpose systems, and office automation systems); backbone systems; vendor-supported systems; and Enterprise Resource Planning (ERP) systems. The trend of technology has promoted the sophistication of these commercial packages away from construction and delivery of in-house packages. Essentially, the application of software to accounting has been further engendered by the growth of commercial software market which have relatively low cost as compared to customized software; emergence of industry-specific vendors who targets their software to the needs of particular types of businesses; growing demand for software by businesses; and the trend toward downsizing of organizational units and the resulting move toward distributed data processing environment, which has made commercial software options more appealing to larger organizations**.** Subsequently, accounting tasks has been made much easier, faster and accurate.

This advancement in technology has created significant risk implications on accounting information systems. The underlying technology appears to develop faster as compared to the relative advancement in control practices which had not been combined with professional accountants' knowledge, skills and attitudes in the use of computing technologies (Abu-Musa, 2005) [1]. Information technology operates as a double-edged sword. Where the power is properly harnessed in serving virtuous purpose, it has produced tremendous improvement to organizational and human performances. At the same time when IT is exploited for malicious purposes, the threats it possess to individuals, organization and the society as a whole can be quite significant as many forms of malicious IT such as viruses, worms, e-mail spam, spyware, adware, and Trojan horses can affect personal utility computers as well as enterprise computing technologies might result. These events are

capable of leading into large scale productivity and financial losses to IT infrastructure (Liang & Xue, 2009) [8]. consequently, financial accounting information is exposed to the risks of failure of computing facility, equipment and software and/or applications common amongst which are hardware failure, workstation access penetration, theft of data services, password failure, program changes, computer virus, data leakage, unauthorized access to data, threat of service, unauthorized access, information modification, denial of service, and traffic analysis. These threats are generally classified as hardware, software, data and communication lines as well as network threats. Organizations must put in place adequate measures to ensure the protection of information assets through effective policy, controls, and standardized procedures and control testing. This would ensure the reduction in threats to CAIS. Although some studies revealed that managers have shown considerable effort to ensure security of information access, others argue that increased effort is necessary.

While a handful of information have been revealed on the magnitude of financial losses experienced by companies around the world on security breaches of IT systems, there have only been few academic studies identified in this area on their implications for accounting information systems especially in developing economies. This study intends to reveal the likely threats identified with the application of IT to accounting information systems in developing economies with particular reference to Nigeria. In addition it should be noted that this report present findings on peculiar security implications for accounting information systems from the point of view of professional accountants and IT specialists who are responsible for IT security. Hence, there is a combined relationship between the enabling role of IT and security implications for computerized accounting systems.

As a first step towards exploring the degree and types of threats faced by companies' use of CAIS's, the research focused on the use of computerized accounting system and the likely threats which might affect their security. This survey is the result of some modifications of the survey conducted by Abu-Musa (2005) [1], a study about perceived threats to CAIS in developing economies with particular reference to companies in Saudi Arabia. One of the most important advantages of applying this survey is that it provides a pattern that allows for international comparison. Following from this, typical statistical and descriptive information as well as other analytical techniques were used to examine the most challenging threats in organizations CAIS.

We collected formal information from companies in order to identify relevant factors related to CAIS threats which are most fundamental. These factors will form the basis for strategic decisions aimed at encouraging and improve underlying systems from our recommendations.

1.1. Aim and Objectives of the Study

The aim of the study is to provide evidence on the existence of threats in the CAIS's of companies in Nigeria, by investigating the perception of selected respondents. To achieve this aim, the study tries to:

i. investigate the respondents' perception on the existence of security threats on CAIS's in Nigeria;

ii. determine which amongst the perceived information security threats constitute the most significant elements.

1.2. Research Questions

In order to achieve the aforementioned objectives, the study shall provide answers to the underlisted questions:

i. to what extent does respondents' perception on the existence of security threats to computerized accounting information systems in Nigeria differ?

ii. what kinds of security threats are most significant to CAIS's in Nigeria from the standpoint of respondents?

1.3. Research Hypotheses

We have identified the following hypotheses in order to provide answers to the questions raised earlier:

H_{01}: there is no significant difference on the perception of respondent groups on the existence of security threats to CAIS's in Nigerian companies.

H_{02}: there are no perceived threats which are significant to the security of CAIS's in Nigerian companies.

2. Previous Studies

Cases in research and practice have increasingly made apparent the need for security of CAIS. Security threats and challenges for IT systems must be studied both in the context of IT systems and the formal/informal systems of organizations. Businesses must begin to develop environments in which cultures that foster responsibility by means of knowledge and conformance to rules and regulations, employee integrity, moral and ethical expectations for engagement at workplaces with regards to CAIS usage (Dhillon & Blackhouse, 1996) [5]. They must continually recognize the function of IT in accounting systems as a business enabler.

There are studies that used empirical approaches to explore the significance and threats to Computerized Accounting Systems in emerging economies. For instance, in U.S. (Ko & Dorantes, 2006; Liang & Xue); Malaysia (Tarmidi, Abdul Rashid, Deris & Roni, 2013), Malami, Zainol & Nelson, 2012); Kenya (Polo and Dima, 2013); Jordan (Hanini, 2012; Al-ma'aitah & Shatat, 2011); and Egypt (Abu-Musa, 2012).

Abu-Musa (2005) [1], provided empirical evidence of significant perceived threats of CAIS's in Saudi organizations, using a sample of 400 firms. The study covered companies in manufacturing, banks, insurance, retail merchandising, oil and gas, services, healthcare, government units amongst others. From a list of identified

CAIS's likely security threats provided, his conclusion was that factors such as employees' accidental and intentional entry of bad data, accidental destruction of data, introduction of computer viruses and other malicious programs, sharing of log-in credentials (ID's and passwords), suppression and destruction of output, unauthorized document visibility, misdirecting prints and distributing information to unauthorized persons were discovered to hold most significantly to perceived threats to CAIS's security.

On the social engineering hazards associated with IT resources, Hanini (2012) [6] examined the risks identified with CAIS's in Jordanian banks, reasons and ways of preventing such risks. In this study covering 63 responding officials of Jordan banks, findings revealed threats to information systems result from employees' lack of experience in securing organization's information systems mainly due to absence of training on how to protect accounting systems prior to resuming their jobs and lack of effective recruitment processes for accounts executives. As a result of these, employees were discovered to engage in intentional entry of inappropriate data during input, unauthorized access to output, and man-made disasters affecting information systems.

With similar purpose, there have also been studies as regards online transactions which encourage customers to make payments virtually. With reference to online payment for products and/or services ordered from companies, it is expected that the accounting systems capture, record and maintain such transactions and ultimately leading into accountability and reporting in the financial statements. Studies have also shown that customers of such companies are often worried and unwilling to carry out their transactions via such platforms due to perceived threats from actions of hackers, crackers and internet interlopers who might steal their access information. Therefore, companies which provide e-commerce platforms should endeavour to make available secure systems capable of enhancing customers' perception and encourage them to transact as such (Al-ma'aitah & Shatat, 2011) [2]. This undoubtedly would augment their competitive advantages provided by IT infrastructure.

On another very similar angle, a study on financial implications of information security fissures was carried out by Ko and Dorantes (2006) [7] when they investigated the impact of information security breaches on firm performance in Texas, U.S. The authors enquired into the financial performance of firms where their information systems security was breached following the breach. Using a matched sample comparison analysis, the study compared financial performance of the breached firm with that of company that have not experienced the breach and thereafter determine if the breached firm's performance has decreased compared to that of the control firm four quarters thereafter. Findings of the study revealed that although there was no significant reduction in the bottom-line of the breached firm, however a number of financial ratios experienced significant decline compared to prior periods.

In order to explore security threats to CAIS's in the banking industry, Malami, Zainol and Nelson (2012) [9] examined the system in Malaysia. Using a sample of 201 bank branches operating in Kuala Lumpur on which questionnaire copies were administered and subsequently analysing the input revealed the major threats challenging the computerized accounting systems of banks in Malaysia were human unintentional threats, human intentional threats, technological threats, environmental threats, and natural threats in that order. In other to obtain similar view in public services, Tarmidi, Rashid, Sakarnor bin Deris and Abdul Roni (2013) [12] investigated the security threat issues in Malaysian public services. Data was obtained via 500 copies of questionnaire distribution to CAIS users in Jabatan Akauntan Negara Malaysia (Accountant General Department). The study concluded after thorough analysis of 19 computerized accounting threats listed in the survey question that most of CAS security threats originate from internal sources (employees).

3. Research Design and Method

In this survey, we have adopted purposive sampling design. Consequently, the structure survey was designed based on the questionnaire that Abu-Musa (2005) [1] applied on Saudi organizations to study the main threats that actually face CAIS's, and the relative materiality of each threat. However, some other items peculiar to other emerging countries reality were adjusted for. Likewise, several filter questions were included as considered important. These include degree of qualification and their experience in information systems security. Accordingly, a 5-point Likert-scale was used with metric and dichotomous questions to analyse the variables as well as evaluate precise conditions.

A pilot survey was conducted delivering a value of 0.793 Cronbach's Alpha coefficient on internal consistency estimation. When the 19 items in the final survey instrument were evaluated, it produced a Cronbach's Alpha coefficient of 0.604 the survey run between May and June, 2013. In the final sampling error, an estimate of 9.23% was also obtained and considered acceptable for the investigation without previously existing factors. To provide support for descriptive analysis, survey tabulation was carried out in accordance with the category of questions and metrics were delivered to the statistical analysis, finally dichotomous questions were served to the descriptive analysis. Finally the filter questions were adopted in authenticating two items: tendencies obtained in the survey; and behaviour of subjects in the face of certain variables produced as input.

Subsequently, data collected were analysed using both descriptive and inferential statistics. While the descriptive method was used to describe the demography of respondents using percentages, analysis of variance was used to determine the relationship between respondents' perspectives while logistic regression model was adopted in

measuring the factors which were most significant as threats to the organizations CAIS's. Analyses were carried out using SPSS for Windows version 18.

3.1. Measure of Constructs

The instrument was divided into two (2) sections. Section A was designed to obtain information on respondents' demographic and subject details, while questions from a list of perceived threats indicated on a five-point Likert-scale frequency was considered in section B. The aim of section B was to obtain the view of respondents by rating each identified variable alongside the scale provided. Respondents were required to indicate their perception of the frequency of each of those threats in their respective organizations ranging from "never" represented by 1, to "every-time" denoted by 5.

3.2. Data Collection Procedure

Respondents were grouped into various sectors of the working industries in Nigeria ranging from manufacturing, banking, insurance, healthcare, retail merchandizing, and wholesale merchandizing. Accordingly, there was further re-classification for professionalism as the list included internal auditors, staff accountant, IS auditors, finance personnel, and IT professionals. A sample of forty (40) was targeted for each category of respondents. The choice of this sample size is guided by literature on the maximum and minimum number as prescribed by Balian, (1994) [3] and Denscombe (2003) [4], where they prescribed a size of not less than thirty (30) subjects per group category for any statistical test. Two-hundred copies of questionnaire were administered while a total of one-hundred and eighty one (181) were successfully retrieved. Out of this figure, 4 respondents indicated the use of manual accounting system; in addition, 6 were found incomplete and inadequate for analytical purpose while 13 others failed to complete the instrument indicating sensitivity of their companies' information disclosure due from their duty of confidentiality. Finally, the number of questionnaire copies identified as valid and usable were 158. This represents an overall response rate of seventy-nine (79%) percent for all groups. Subsequently, the responses were used in providing answers to hypotheses raised in the study. Information on responses categorized by group is as presented in Table 1.

Table 1. Questionnaire distribution and responses

Respondent Group	Number of Survey	Number of Responses	% of Responses
Internal Auditors	40	33	82.5%
Staff Accountants	40	31	77.5%
IS Auditors	40	31	77.5%
Finance Personnel	40	30	75.0%
IT Personnel	40	33	82.5%
Total	**200**	**158**	**79.0%**

Source: Analysis of survey data (2011).

4. Analysis and Results

In the first instance, preliminary results were performed using survey tabulation. This was aimed at gathering results in accordance with the topic of interest. It also allow for comparative analysis and to contrast tendencies of different variables under study.

Secondly, Analysis of Variance (ANOVA) was used to draw conclusions regarding relationship amongst respondents' perception about security threats to CAIS's in the companies under survey. This provided answer to the first hypothesis formulated in earlier section.

In the final analysis aimed at answering hypothesis two, Logistic regression was applied in order to analyse the influence of those factors perceived as threats on CAIS's. These were identified as the independent variables. The dependent variable on the other hand is the perception of security threats indicated by respondents. Respondents were requested to indicate whether or not they have perceived security threats in recent past (one year or less) due from likelihood of security breaches to their CAIS's. According to the questionnaire results, 132 respondents representing 83.5% responded to the affirmative. These perceived threats were mainly due from either insider abuse (present employee), and/or aggrieved past employee; or from remote locations by outsider. The independent variables however were the various perceived accounting information systems threats listed in the survey instrument (see: Appendix 2).

4.1. Test of Research Hypotheses

H_{01}: there is no significant difference in the perception of respondent groups on the existence of security threats to CAIS's in Nigerian companies.

For the purpose of this analysis, respondents were categorized into five (5) groups as revealed in Table 1 above. The 19 items from the questionnaire were associated with this hypothesis. The results of the hypotheses is as presented in the appendix I. Table 2 revealed that the first two statements used in validating the proposition made on the existence of differences in respondents' perception both have F-ratios of 1.144 and 0.363 respectively with p-values higher than 0.05 i.e. 0.338 and 0.835. Consequently, we conclude that there are no significant differences in the perception of respondent groups in areas of accidental and intentional entry of bad data by employees during the course of using CAIS's. However, the last two statements in the table have F-ratios of 3.038 and 5.645, and p-values of 0.019 and 0.000 which are both lesser than 0.05. Hence, we conclude that there exist significant differences amongst respondents' perception in areas of accidental and intentional destruction of data by company employees. These might be due to the possibilities that companies have different security policies and procedures in their information systems assets security as regards employees access levels on a "need to know basis" as well as access to data and information.

Table 3 revealed the result conducted on the next group of threats listed in the survey instrument. Respondent groups

share similar opinions as regards unauthorized access to data or systems by employees (F-ratio 1.421; p-value 0.230); unauthorized access to data or systems by outsider (hackers) (F-ratio 1.567; p-value 0.186); and natural disaster such as flooding and loss of power (F-ratio 0.501; p-value 0.735), with all p-values greater than 0.05 indicating that there are no significant differences in their perceptions. Conversely, as regards employee sharing of passwords with F-ratio of 6.043 and p-value of 0.000, respondents differ significantly as the p-value is less than 0.05. This might also be in line with significantly different security policies in areas of information access security with particular reference to identification and authentication procedures. Controlling access to CAIS's to guarantee authorized access is fundamental to information systems security. Some organizations operate systems with weak authentication methods, potential for users to bypass the authentication mechanisms in place, lack of confidentiality and integrity for the stored authentication information, as well as lack of encryption for authentication of information transmitted over the network.

Results in **Table 4 showed that** responding organizations all share similar opinions in areas of manmade and disasters such as fire and flood (F-ratio 0.490 and p-value 0.743); introduction of computer virus to the system (F-ratio 1.447 and p-value 0.221); Suppression or destruction of output (F-ratio 1.001; p-value 0.4090); and creation of fictitious or incorrect output (F-ratio 0.739; p-value 0.567). This might support the probability that security concerns with respect to data are broad encompassing availability, confidentiality and integrity. In the case of availability, the concern is with the destruction of data files, which can occur either accidentally or from aggrieved employees.

Under **Table 5** following, result of ANOVA on theft of data or information (F-ratio 0.758; p-value 0.554) and suppression or destruction of output (F-ratio 1.001; p-value 0.739) cleared the conclusion that respondents share similar view on both statements. Their views were however dissimilar under unauthorized copying of output (F-ratio 51.450; p-value 0.000). This might be associated with the fact that some organizations especially banking and insurance often dislodged users' access to external disk compartment (i.e. the CD drive) in other to discourage the use of external output devices such as flash disks and similar devices to prevent unauthorized copying of output from user systems.

Data in **Table 6** revealed that "unauthorized documents visibility through the display on monitors or on paper" has an F-ratio of 3.038 and p-value of 0.019.; the shredding of documents by unauthorized persons (F-ratio 3.361; p-value 0.011) and data interception from remote locations (F-ratio 3.106; p-value0.017) indicating that subjects share significantly different views as regards these variables. On the issue of security of documents, this may be due to factors such as size and type of office spaces, relationship amongst employees, existence of non-formal groups in the organization and other factors which might differ across companies.

H_{02}: there are no perceived threats which are significant to the security of CAIS's in Nigerian companies.

In the last stage of the study, a logistic regression was performed to establish which of the factors had the greatest incidence on the security of CAIS used in the firms evaluated. For that purpose in providing a response to hypothesis 2, the selected independent variables identified as the "perceived security threats" provided in the list of survey items were regressed against the dependent factor (perception of security threats to their CAIS's in recent past – one year or less). Regarding the independent variables, the resulting values of the factorial analysis were gathered for each one of the 158 observations in the survey, according to the recorded by the SPSS during the study. The final result was that the optimal variables for the model that represented significant relationship with the dependent variable out of the list of 19 items in the survey instrument were: (a) accidental entry of bad data by employees (p=0.023); (b) accidental destruction of data by employees (p=0.016); (c) employees sharing of password (p=0.001); (d) introduction (entry) of computer viruses to the system (p=0.031); (e) unauthorized copying of output (p=0.006); (f) unauthorized document visibility by displaying on monitors or printed on paper (p=0.0000). Tables 8 through to 12 in appendix II detailed the logistic regression results. Consequently, propensity in the significance of the perceived threats to the non-significance is greater when the accidental entry of bad data (Exp (B) = 1.048); accidental destruction of data by employees (Exp (B) = 0.930); employees sharing of passwords (Exp (B) = 0.402); introduction/entry of computer viruses to the system (Exp (B) = 0.882); unauthorized copying of output (Exp (B) = 5.432); and unauthorized document visibility by displaying on monitors or printed on paper (Exp (B) = 0.967). Conclusively, there are perceived threats which are significant to CAIS's in Nigerian companies contrary to hypothesis 2.

5. Conclusion and Recommendations

5.1. Conclusion

The study investigates the perception of Nigerian accountants and IT executives on the perceived security threats to CAIS's. Majority of respondents agree with the statement that CAIS's are exposed to security threats both within and outside the organization. The study found that factors such as accidental entry of bad data by employees, accidental destruction of data by employees, employees sharing of log-on credentials, introduction of virus, unauthorized access to information systems and unauthorized documents visibility via display on monitors and hardcopy documents are the most significant security threats to computerized accounting information systems. This findings agree substantially with prior studies (Abu-Musa, 2005) [1]; Hanini, 2012) [6], conducted in

Saudi-Arabia and Jordan respectively. The authors concluded that activities of employees (both intentional and unintentional) were primarily responsible as security threats to the protection of information assets in the organization.

5.2. Recommendations

Based on the findings and conclusion reached, we recommend that organizations should endeavour to implement substantial security measures to protect IT infrastructure through the use of physical, logical, environmental and administrative (policies, guidelines, standards, and procedures) controls. Management should monitor physical controls in place designed to safeguard CAIS's and to guide access to facilities, computers, and telecommunications equipment that supports information assets processing. Physical security controls should include use of security guards where appropriate. Where perceived benefit outweigh associated costs, use of biometric devices (retina, scanners, hand geometry, fingerprint scanners), electronic card readers should be used extensively. Physical access controls to computer equipment and facility enabling CAIS's should be monitored and reviewed periodically to ensure their effectiveness.

Management must educate and continue to put employees on strict awareness of their confidentiality duty as social engineering is mostly capable of defeating physical security controls. Social engineering activities include those psychological tricks on authorized users by unauthorized persons to gain access to the computerized processes. Employees must be contentiously educated on activities involving social engineering such as shoulder surfing (watching over the shoulder of authorized users to identify key codes that provides access to information assets); claiming to have lost badges or key cards and persuading an authorized user to permit access; or piggybacking behind authorized users with valid key card.

Although the maintenance of logical security seems more complex to implement and maintain, management should put in place authorization procedures on a "need to know basis" only. This implies that authorized users should have access to only applications and data required need to perform specific tasks only. Also, there should be regular logging and monitoring of logical access to systems and data. Policies and procedures should include segregation of duties and access and transaction logs.

Personnel responsible for securing CAIS's must continually become cautious of probable unauthorized users to information systems who are capable of gaining access to applications and data and then educate users as appropriate. These might include but not limited to aggrieved internal employees, contracted employees, suppliers or vendors, cleaning and maintenance contractors, partners, remote users as well as entities which have access to external information systems such as the general public.

Companies should put in place effective security programs and associated controls. To ensure continuity, regular penetration tests must be conducted. Such tests might include breaking into access points through persuasion or brute force, or gaining admission as a visitor and trying to access areas for which someone is not authorized.

Finally, there should be regular reviewing, monitoring and testing of physical, logical and environmental security controls to protect information assets. Those who hold IT security responsibilities should be made to define incidence response procedures and provide detailed guidelines for identification, notification, evidence collection, continued protection, and reporting of such disruptive events.

Appendix I

Table 2. Results of ANOVA

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
Accidental Entry of Bad Data By Employees	Between Groups	8.206	4	2.052	1.144	.338
	Within Groups	274.401	153	1.793		
	Total	282.608	157			
Intentional Entry Of Bad Data By Employees	Between Groups	2.306	4	.577	.363	.835
	Within Groups	242.909	153	1.588		
	Total	245.215	157			
Accidental Destruction Of Data By Employees	Between Groups	26.643	4	6.661	3.038	.019
	Within Groups	335.465	153	2.193		
	Total	362.108	157			
Intentional Destruction Of Data By Employees	Between Groups	37.785	4	9.446	5.645	.000
	Within Groups	256.012	153	1.673		
	Total	293.797	157			

Table 3. Results of ANOVA

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
Unauthorized Access To Data And Or System By Employees	Between Groups	5.380	4	1.345	1.421	.230
	Within Groups	144.804	153	.946		
	Total	150.184	157			
Unauthorized Access To Data And Or System By Outsiders Hackers	Between Groups	12.089	4	3.022	1.567	.186
	Within Groups	295.126	153	1.929		
	Total	307.215	157			
Employees Sharing Of Passwords	Between Groups	34.788	4	8.697	6.043	.000
	Within Groups	220.181	153	1.439		
	Total	254.968	157			
Natural Disaster Such As Fire Flooding Loss Of Power	Between Groups	3.907	4	.977	.501	.735
	Within Groups	298.276	153	1.950		
	Total	302.184	157			

Table 4. Results of ANOVA

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
Man Made Disasters such as Fire Loss of Power	Between Groups	3.013	4	.753	.490	.743
	Within Groups	235.171	153	1.537		
	Total	238.184	157			
Introduction Entry of Computer Virus to the System	Between Groups	12.068	4	3.017	1.447	.221
	Within Groups	318.976	153	2.085		
	Total	331.044	157			
Suppression or Destruction of Output	Between Groups	5.989	4	1.497	1.001	.409
	Within Groups	228.720	153	1.495		
	Total	234.709	157			
Creation of Fictitious or Incorrect Output	Between Groups	7.674	4	1.919	.739	.567
	Within Groups	397.243	153	2.596		
	Total	404.918	157			

Table 5. Results of ANOVA

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
Theft of Data or Information	Between Groups	2.347	4	.587	.758	.554
	Within Groups	118.362	153	.774		
	Total	120.709	157			
	Within Groups	49.378	153	.323		
	Total	115.797	157			
Unauthorized Copying of Output	Between Groups	107.497	4	26.874	51.540	.000
	Within Groups	10.225	153	.067		
	Total	117.722	157			
Suppression or Destruction of Output	Between Groups	5.989	4	1.497	1.001	.739
	Within Groups	228.720	153	1.495		
	Total	234.709	157			

Table 6. Results of ANOVA

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
Unauthorized Document Visibility	Between Groups	26.643	4	6.661	3.038	.019
	Within Groups	335.465	153	2.193		
	Total	362.108	157			
Shredding of Sensitive Documents by Unauthorized Persons	Between Groups	27.695	4	6.924	3.361	.011
	Within Groups	315.222	153	2.060		
	Total	342.918	157			
Data Interception from Remote Locations	Between Groups	26.189	4	6.547	3.106	.017
	Within Groups	322.495	153	2.108		
	Total	348.684	157			

Table 7. Result of ANOVA

Contrast Coefficients

Contrast	Group				
	1 Internal Auditor	2 Staff Accountant	3 IS Auditor	4 Finance Personnel	5 IT Professional
1	-1	-1	-1.5	2	1.5

Appendix ii

Table 8. Results of Logistics Regression.

Variables in the Equation

								95% C.I.for EXP(B)	
		B	S.E.	Wald	df	Sig.	Exp(B)	Lower	Upper
Step 1[a]	Accidental Entry of Bad Data By Employees	.047	.184	.065	1	.023	1.048	.731	1.503
	Intentional Entry Of Bad Data By Employees	.268	.197	1.850	1	.914	1.307	.889	1.922
	Accidental Destruction Of Data By Employees	-.073	.157	.218	1	.016	.930	.684	1.264
	Intentional Destruction Of Data By Employees	-1.123	.332	11.457	1	.001	.325	.170	.623
	Constant	5.894	1.818	10.512	1	.001	362.891		

a. Variable(s) entered on step 1: 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.

Table 9. Results of Logistics Regression.

Variables in the Equation

								95% C.I.for EXP(B)	
		B	S.E.	Wald	df	Sig.	Exp(B)	Lower	Upper
Step 1[a]	Unauthorized Access To Data And Or System By Employees	-.127	.240	.282	1	.795	.880	.550	1.409
	Unauthorized Access To Data And Or System By Outsiders Hackers	-.482	.167	8.280	1	.804	.618	.445	.858
	Employees Sharing Of Passwords	-.912	.274	11.048	1	.001	.402	.235	.688
	Natural Disaster Such As Fire Flooding Loss Of Power	-.088	.166	.280	1	.596	.916	.661	1.268
	Constant	7.188	1.581	20.662	1	.000	1323.193		

a. Variable(s) entered on step 1: Unauthorized Access To Data And Or System By Employees, Unauthorized Access To Data And Or System By Outsiders Hackers, Employees Sharing Of Passwords, Natural Disaster Such As Fire Flooding Loss Of Power.

Table 10. Results of Logistics Regression.

							95% C.I.for EXP(B)	
		B	S.E.	Wald	df	Sig.	Exp(B)	Lower	Upper
Step 1[a]	Man Made Disasters such as Fire Loss of Power	-.161	.190	.715	1	.398	.852	.587	1.236
	Introduction Entry of Computer Virus to the System	-.125	.159	.620	1	.031	.882	.646	1.205
	Suppression or Destruction of Output	-.127	.177	.510	1	.475	.881	.622	1.247
	Creation of Fictitious or Incorrect Output	-.014	.138	.010	1	.921	.986	.752	1.293
	Constant	2.990	1.060	7.961	1	.005	19.877		

a. Variable(s) entered on step 1: Man Made Disasters such as Fire Loss of Power, Introduction Entry of Computer Virus to the System, Suppression or Destruction of Output, Creation of Fictitious or Incorrect Output.

Table 11. Results of Logistics Regression.

Variables in the Equation

								95% C.I.for EXP(B)	
		B	S.E.	Wald	df	Sig.	Exp(B)	Lower	Upper
Step 1[a]	Theft of Data or Information	-.154	.358	.185	1	.667	.857	.424	1.730
	Unauthorized Copying of Output	-9.533	3969.102	.000	1	.006	5.432	.000	.
	Prints and Distribution to Unauthorized Persons	-10.280	3820.736	.000	1	.998	.000	.000	.
	Unauthorized Printing and Distribution	-.322	.220	2.140	1	.144	.725	.471	1.116
	Constant	80.940	12451.771	.000	1	.995	1.419E35		

a. Variable(s) entered on step 1: Theft of Data or Information, Unauthorized Copying of Output, Prints and Distribution to Unauthorized Persons, Unauthorized Printing and Distribution.

Table 12. Results of Logistics Regression.

Variables in the Equation

								95% C.I.for EXP(B)	
		B	S.E.	Wald	df	Sig.	Exp(B)	Lower	Upper
Step 1[a]	Unauthorized Document Visibility	-.033	.817	.002	1	.000	.967	.195	4.794
	Shredding of Sensitive Documents by Unauthorized Persons	-.089	.427	.044	1	.834	.915	.396	2.112
	Data Interception from Remote Locations	.086	.787	.012	1	.913	1.090	.233	5.096
	Constant	1.742	.531	10.776	1	.001	5.707		

a. Variable(s) entered on step 1: Unauthorized Document Visibility, Shredding of Sensitive Documents by Unauthorized Persons, Data Interception from Remote Locations.

REFERENCES

[1] Abu-Musa, A. Investigating the Perceived Threats of Computerized Accounting Information Systems in Developing Countries: An Empirical Study on Saudi Organizations, Computer and Information Science, Vol. 18, pp. 1-26, 2005.

[2] Al-ma'aitah, M., and Shatat, A., Empirical Study in the Security of electronic Payment Systems, International Journal of Computer science Issues, Vol. 8 (4), pp. 393-401, 2011.

[3] Balian, E., The Graduate Research Guidebook: A practical approach to doctoral/masters research, University Press of America, Maryland-U.S., 1994.

[4] Denscombe, M., The good research guide for small-scale social Research projects (2nd ed.), Open University Press, Maidenhead-Philadelphia.

[5] Dhillon, G., & Blackhouse, J., Risks in the use of information technology within organizations, International Journal of Information Management, Vol. 16(1), pp. 65-74, 1996.

[6] Hanini, E., The Risks of Using Computerized Accounting Information Systems in the Jordanian Banks; their reasons and ways of Prevention, European Journal of Business and Management, Vol. 4(20), pp., 53-63, 2012.

[7] Ko, M., & Dorantes, C., The Impact of Information Security

Breaches on Financial Performance of the Breached Firms: An empirical Investigation, Journal of Information Technology Management, Vol. XVII (2), pp. 13-22.

[8] Liang, H., & Xue, Y., Avoidance of Information technology Threats: A Theoretical Perspective, MIS Quarterly, Vol. 33(1), pp. 71-90, 2009.

[9] Malami, A., Zainol, Z., & Nelson, S., Security Threats of Computerized Banking Systems (CBS): The Managers' Perception in Malaysia, International Journal of Economics and Finance Studies, Vol. 4(1), pp. 21-30, 2012.

[10] Polo, J., & Oima, D., Effects of Computerized Accounting Systems on Audit Risk Management in Public Enterprises: A Case of Kisumu County, Kenya, International Journal of Education and Research, Vol. 1(5), pp. 1-10, 2013.

[11] SPSS 18 for Windows Evaluation Version Release, 18.0, 2009.

[12] Tarmidi, M., Rashid, A., Deris, M., & Roni, R., Computerized Accounting Systems Threats in Malaysian Public Services, International Journal of Finance and Accounting, Vol. 2(2), pp. 109-113, 2013.