The Key Issues Surrounding Electronic Commerce Information Security Management

Simon Nderitu Watuthu, Michael Kimwele, George Okeyo

Abstract- The purpose of this study was to identify the key issues surrounding electronic commerce information security management. A descriptive survey research design was conducted to gather primary data. Information about the current status of ecommerce information security practices and the impediments of these approaches was also collected. A structured questionnaire was used to collect secondary data. Once all the instruments were collected, they were validated edited and then coded. In the validation process, the collected instruments were checked to determine whether an acceptable sample was obtained in terms of proportion of the issued instrument. Descriptive statistics such as frequency distribution, percentages, means and standard deviations were calculated. This was facilitated by use of the statistical package for social science (S.P.S.S). The observations made from this study are that In Kenya, ecommerce faces numerous information security challenges. Confidentiality and Privacy issues was the top security issue of concern to the respondent's with 60.7% of the respondents admitting to it. Respondents further considered viruses and malicious software at 46.4%, human errors at 28.6% and also system or software errors at 17.9% as the top three main causes of confidential threat their organizations. Further the study revealed 85.7% of the respondents admitted that their organisation did not use any framework in managing information security.

Keywords: electronic commerce, information security ecommerce security

I. INTRODUCTION

Trepper (2000) described e-commerce as simply any business transaction that takes place via digital processes over a network. E-commerce however is really much more than just exchanging products or services for money over the internet. E-commerce also includes enabling technology that allows business to increase the accuracy and efficiency of business transaction process. E-commerce is also a way for organizations to exchange information with customers and vendors to the benefit of everyone involved. According to Horak (2002), E-commerce essentially involves the purchasing of goods and services over the web, usually through a secure credit card transaction.

Information security is the protection of information assets that use, store or transmit information from risk through the application of policy, education and technology (Whitman & Mettord, 2012). According to Ciampo (2012), information security is that which protects the integrity, confidentiality, and availability of information on the device that store, manipulate and also transmit the information through products, people and procedures.

There are several types of information security. These are personal security, operation security, communication security, network security and information security. Personal security deals with protecting the individual or group of individuals who are authorized to access the organization and its operations, Operations security deals with to protecting the details of a particular operation or series of activities, Communications security involves protecting communications media, technology, and content, Network security deals with protecting networking components, connections, and contents and Information security involves protection of information assets (Whitman & Mettord, 2012). According to Ciampo (2012), the main goals of information security are to prevent data theft, and thwart identity theft, avoid the legal consequences of not securing information, maintain productivity, and foil cyber terrorism. Computer security depends on a combination of physical barriers, software defenses and security procedures. E-commerce security is the protection of e-commerce assets from unauthorized access, use, alteration, or destruction. Ecommerce security threats range from intellectual property theft and business disruption to brand and reputation damage. Information security is a business enabler that is strictly bound to stakeholder trust, either by addressing business risk or by creating value for an enterprise, such as competitive advantage (Whitman & Mettord, 2012). According to Ward (2010), data breaches produce unwelcome publicity that can have a severe negative impact on a retail organization's brand and reputation. The damage from a data breach often extends well beyond losing the trust of only those customers directly impacted by the incident—and negative public perceptions can persist for years after a breach.

II. STATEMENT OF THE PROBLEM

According to Norman and Yasin (2010), development sectors and commercial enterprises in Africa and all over the world have been faced with serious challenges arising from massive computer application such as stolen data, viruses and saboteurs. Electronic commerce has not been spared by this information insecurity. Curtis and Cobham (2005) observe that several notable breaches of security have caused organizations to be cautious about implementing electronic commerce. Despite the rapid growth witnessed by electronic commerce with the growth of internet, there have been insufficient research efforts concerning the status of information security challenges facing it. Furthermore, research in understanding people issues in electronic commerce is one of the research gaps that need to be address in researches (Norman and Yasin, 2010). In effort to secure electronic commerce, organizations tend concentrate

Manuscript Received on February 16, 2015.

Simon Nderitu Watuthu, Jomo Kenyatta University of Agriculture and Technology, Kenya.

Dr. Michael Kimwele, Jomo Kenyatta University of Agriculture and Technology, Kenya.

Dr. George Okeyo, Jomo Kenyatta University of Agriculture and Technology, Kenya.

more on technology. Despite the use of these technologies, companies continue to lose billions due to information security breaches. This suggests that technology alone cannot achieve information security. Companies should therefore compliment these technologies with proper policies, procedures, and standards. For this purpose, organizations should have a comprehensive information security framework (Patil, 2008). This study aimed at developing a security framework to enhance electronic commerce. This was developed from information that was obtained from online tour and travel companies.

III. OBJECTIVE

The purpose of the study was to identify the key issues surrounding electronic commerce information security management.

IV. RESEARCH FOCUS

The study mainly focused on ecommerce information security threats and challenges faced by tour and travel companies in Nairobi. The study looked at the current status of ecommerce information security practices and the impediments of these approaches. The study made recommendations on how ecommerce information security can be improved in Kenya. A security framework was developed to provide a support tool to help security managers to enhance security in ecommerce.

V. METHODOLOGY

a) Research Design

This study used a descriptive survey design. Descriptive survey design was appropriate in this study because it enabled the researcher to explore the information security challenges faced by tour and travel companies practicing e-commerce and also help in identifying the requirements for the information security framework appropriate for this kind of business.

b) Target Population

The study was carried out in Nairobi where most tour and travel companies are located. There about 57 tour and travel companies in Nairobi (Telkom, 2013). Therefore Nairobi region was purposively selected for this study. The population of this study was obtained from a list that was obtained from a list of the official Nairobi 2013 yellow pages directory published by Telkom Kenya.

c) Sample Size and Sampling Procedure

To select the sample randomly the researcher wrote the names of all Tour and travel companies obtained from official Nairobi 2013 yellow pages on similar pieces of papers. The papers were evenly folded, put in a container and shuffled. Then the researcher then picked 17 of the papers at random. This was equivalent to 30% of the 57 companies to be involved in this study. This constituted the random sample to be used in this research. Two the employees in the IT department of the sampled companies filled in a questionnaire

d) Research instruments

A descriptive survey research design was conducted to gather primary data. The research was conducted using questionnaires.

e) Data Collection Procedure

The researcher got an introduction letter from Jomo Kenyatta University of Agriculture and Technology. Before going to the field, the researcher also obtained a research permit from the commission of higher education

After obtaining the research permit the researcher visited the sampled companies to inform the managers of the companies about the study. Then the researcher then went back to distribute the questionnaires to the relevant respondents.

f) Data Analysis

Once all the instruments were collected, they were validated edited and then coded. In the validation process, the collected instruments were checked to determine whether an acceptable sample was obtained in terms of proportion of the issued instrument.

Descriptive statistics such as frequency distribution, percentages, means and standard deviations were calculated. This was facilitated by use of the statistical package for social science (S.P.S.S). The data was then presented in tables.

VI. FINDINGS OF THE STUDY

In line with the objective of the study, the researcher sought to determine key issues surrounding electronic commerce information security management. The researcher presented a number of items to solicit responses that would address this objective. Firstly, the researcher sought to establish what the respondents' considered the top security issue of concern to their organisations, the responses are summarised in figure 1 below. The respondents considered confidentiality and privacy as the top security issue of concern to their organisations at 60.7% followed by integrity at 21.4%. The issue of availability was mentioned by the least, 17.9% of the respondents. This implies that indeed confidentiality and privacy is an important security issue in ecommerce organizations, hence a lot emphasis ought to place on addressing it. These findings echo what Nivan et al. (2013) observed. They observed that Privacy and security are major concern for electronic commerce.

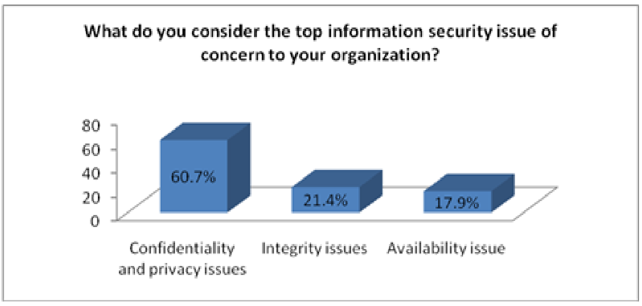

Figure 1: The top security issue of concern to your Organization

The researcher further sought to establish what the respondents considered to be top three main causes of security incidents in their organizations table 1 presents the findings. The study revealed that the respondents considered viruses and malicious software at 46.4%, followed by human errors also at 28.6% and lastly system or software errors at 17.9% as the top three main causes of security incidents in their organizations. Loudon, Loudon and Das (2010), indicate that sharing files over peer-to-peer (P2P) networks, such as those for illegal music sharing, may transmit malicious software or expose information on either information on either individual or corporate computers to outsiders this can occur through Trojan horse. Furthermore E-mails may contain attachments that serve as springboards for malicious software. These findings reflect what was observed by Nivan et al. (2013). They observed that trojan horse programs launch against client systems pose greatest threat to ecommerce because they by pass or subvert most of the authentication an authorization mechanisms used in an ecommerce transaction. Viruses are a nuisance threat in ecommerce.This implies that any effort geared towards address information insecurity security should lay emphasis on these three issues.

Table 1: Top three main causes of security incidents in your organization?

What do you consider to be top three main causes of security incidents in your organization?		
	Frequency	Percent
Viruses and malicious software	13	46.4
Human errors and omissions	8	28.6
System or software errors	5	17.9
Hardware failure	2	7.1
Total	28	100.0

Further the respondents were required to state whether their organizations' network has ever experienced any of the following problems since they began using it. The first problem was unauthorized access or interception of data. Their responses are summarized in table 2 below. Results in table 2 shows that 60.7% of the respondents reported that their networks had experienced the problem of unauthorized access to or interception of data with 21.4% reporting they had never while the least 17.9%, reporting they didn't know if such a problem had occurred. Hence from the responses, unauthorized access to or interception of data is a security threat to ecommerce organizations. These findings reflect what was observed by Arabjafari (2012). He observed that malicious code is one of the most common security threats.

Table 2: Unauthorized access to or interception of data

Unauthorized access to or interception of data		
	Frequency	Percentage
Yes	17	60.7
Never	6	21.4
Do not know	5	17.9
Total	28	100

Further the respondents were required to sate if the username or password leakage had been a problem in their organizations. An overwhelming majority (89%) of the respondents' organizations had experienced username or password leakage with a just 11% reporting not to have experienced this problem. This implies that this is a big problem to ecommerce organizations, hence there is need to address the issue as it affects an overwhelming number of ecommerce organizations. These finding are consistent with what was observed by Keanini (2014). He observed that more individuals on the net are having their email, social media and other accounts compromised because of weak passwords.

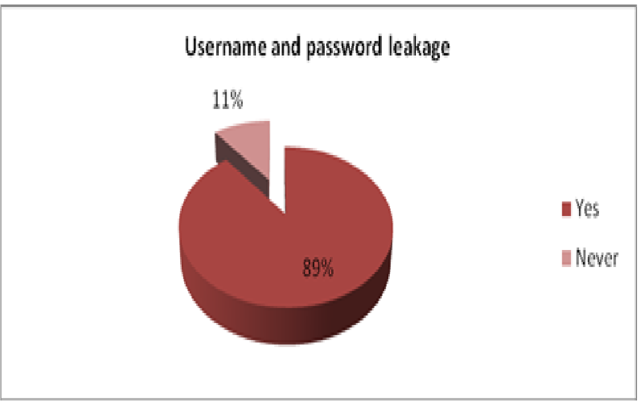

Figure 2: Username and Password leakage

Hacking was reported to have occurred as an overwhelming majority reported that their organization networks had been hacked before, figure 3 provides a summary of the results. Results in figure 3 revealed that 71.4% of the respondents reported having had their organizations' networks hacked while the least, 28.6% reported never having had their networks hacked. These responses imply that hacking is a big information security issue as it has been experienced by an overwhelming number of ecommerce organizations as shown above; hence emphasis has to be placed on finding ways of addressing it. These finding echoes what happened in Kenya where a leading media house's payroll information for April 2012 was published online. Soon after in May, 2012 sensitive information from a leading NSE listed company were also published online after their systems were hacked (Serianu, 2012).

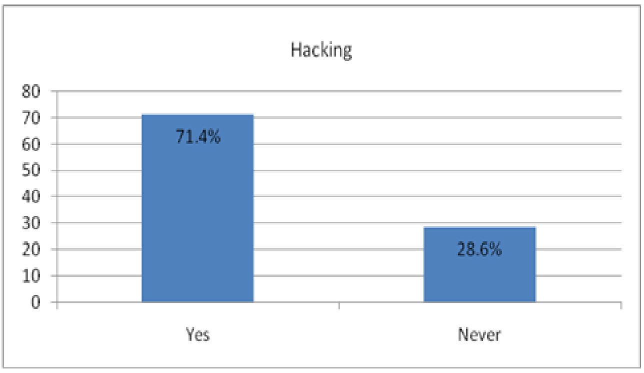

Figure 3: Hacking

In an effort to establish key issues in information security, the researcher further sought to determine whether the respondents had experienced theft of business as well as sensitive customer information from their organizations' websites. The responses are summarized in figure 4. Figure 4 reveals that indeed theft of business as well as sensitive customer information from respondents' organization websites takes place with a majority at 50% admitting it had happened followed by 32% who said this has never happened to their networks. The least at 18% reported that they did not know if such a thing had ever occurred. This findings are in line with what Manktelow (2013) reported. He observed that data theft and security issues are increasing each year, leading to financial losses, intellectual property theft, identity fraud, and compromised reputations. According to Roman (2013), Adobe's 2.9 million customers' personal information, including encycrypted payment card numbers were accessed by attackers. The attackers also removed from the system certain information on 2.9 million customers, including names, encrypted credit or debit numbers, cards expiration dates and other information relating to customers order.

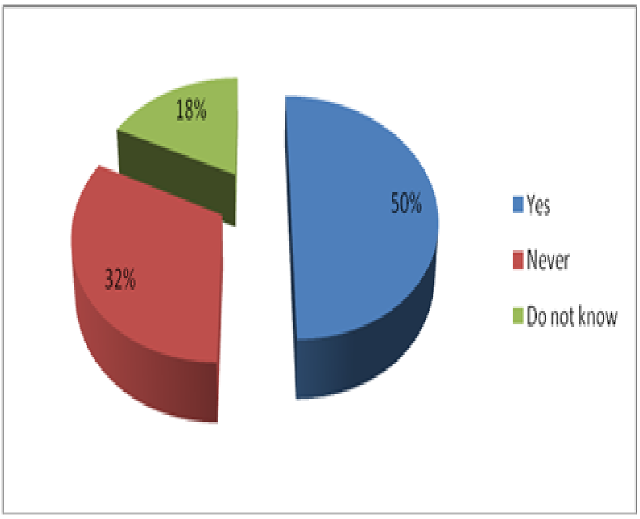

Figure 4: Theft of business as well as sensitive customer information from organization websites.

The respondents further reported that indeed it was true that they had received e-mail messages that looked like those of legitimate business partners or financial institution they bank with yet in the real sense they were fake. Table 3 gives a summary of the responses: Table 3 reveals that receiving e-mail messages that look like those of legitimate business partners yet in real sense they are fake had occurred with a majority at 64.3% agreeing with it. Only 32.1 % said this had not happened to them with the least, 3.6% reporting that they did not know if such a thing had ever taken place in their organizations. Hence this is a real issue that affects ecommerce organizations as shown by the overwhelming majority who said it has happened to them. This is in line with a report by Telecoms (2013). According to the report, a research and information centre director has warned bankers of the increasing incidence of internet fraud, committed by hackers who are able to overwrite passwords and make unauthorised intrusions into corporate websites.

Table 3: Receiving e-mail messages that look like those of legitimate business partners or financial institution you bank with but in the real sense they are fake

Receiving e-mail messages that look like those of legitimate business partners or financial institution you bank with but in the real sense they are fake		
	Frequency	Percent
Yes	18	64.3
Never	9	32.1
Do not know	1	3.6
Total	28	100.0

The researcher also sought to establish if employees have ever been tricked to give confidential information about their organizations or about their customer by people claiming to be legitimate authorities. Table 4 shows that the majority of the respondent's organizations, at 46.4% had encountered this problem while 35.7 % reported not having encountered this problem. Only 17.9% reported that they did not know if such a problem had been encountered by their organizations.

Table 4: Employees ever been tricked to give confidential information about their organization or about a customer by people claiming to be legitimate authorities

Employees being tricked to give confidential information about your organization or about your customer by people claiming to be legitimate authorities		
	Frequency	Percent
Yes	13	46.4
Never	10	35.7
Do not know	5	17.9
Total	28	100.0

A majority of the respondents at 64% further reported not being aware of the fact that sacked employees reveal confidential information about their organizations and customers. The results in figure 5 reveal that only 18% of the respondents agreed that sacked employees reveal confidential information about their organizations or about customers with another 18 % saying they did. Hence this is not a major information security concern as only a small percentage thought it was an information security problem with a majority, 64%, reporting they are not aware of it. These findings disagree with those Patil, (2008), who revealed that in an effort to secure electronic commerce, organizations tend concentrate more on technology, yet despite the use of these technologies, companies continue to lose billions due to information security breaches by current and former employees. This suggests that technology alone cannot achieve information security. Companies should therefore compliment these technologies with proper policies, procedures, and standards for employees.

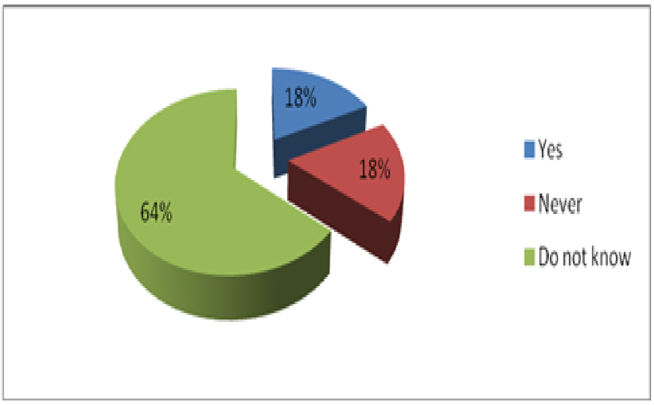

Figure 5: Sacked employees revealing confidential information about their organizations and customers

Results in table 5 revealed that most respondents, at 53.6% reported that their organizations had never encountered with disgruntled employees revealing confidential information about a customer. Only 25% of the respondents said that they had witnessed it while the least, 21.4% reported they did not know if disgruntled employees had ever revealed confidential information about a customer. The findings also do not agree with (Norman and Yasin, 2010) who reported that employee/people issues in electronic commerce is one of the research gaps that need to be address in researches (Norman and Yasin, 2010).

Table 5: Disgruntled employees revealing confidential information about a customer

Disgruntled employees revealing confidential information about your customer		
	Frequency	**Percent**
Yes	7	25.0
Never	15	53.6
Do not know	6	21.4
Total	28	100.0

Further the researcher sought from the respondents if the ecommerce organizations had experienced attacks using malicious software such as viruses, worm or Trojan horse, the responses are summarized in table 6. Table 6 reveals that the most, 64.3% of the respondents, agreed that attacks using malicious software such as viruses, worm or Trojan horse was an information security issue while the least 32.1% reported that this had never been an issue. The least, 3.6% reported they did not know if this was an issue. These findings reflect what various scholars have observed. According to Nivan et al. (2013), Trojan horse programs launch against client systems pose greatest threat to ecommerce because they by pass or subvert most of the authentication an authorization mechanisms used in an ecommerce transaction. Arabjafari (2012) observes that malicious code is one of the most common security threats. Further, according to Hoodrick and Temassia (2011), despite knowledge and infrastructure defenses, many viruses and worms have broken out regularly in the internet over the years.

Table 6: Attacks using malicious software such as viruses, worm or Trojan horse

Attacks using malicious software such as viruses, worm or Trojan horse		
	Frequency	**Percent**
Yes	18	64.3
Never	9	32.1
Do not know	1	3.6
Total	28	100.0

The researcher further sought to determine if users of respondents' organization web sites would be redirected to bogus web pages even when they typed in the correct webpage into their browser. Results in figure 6 reveal that majority (60.7%) of the respondents reported that they had never encountered such a problem with only 21.4% reported that such a problem had been encountered. The least, 17.9% said they did not know if such a problem had ever occurred. Thus the issue of users of respondents' organization web sites being redirected to bogus web pages was not a major problem encountered by ecommerce organizations as justified above.

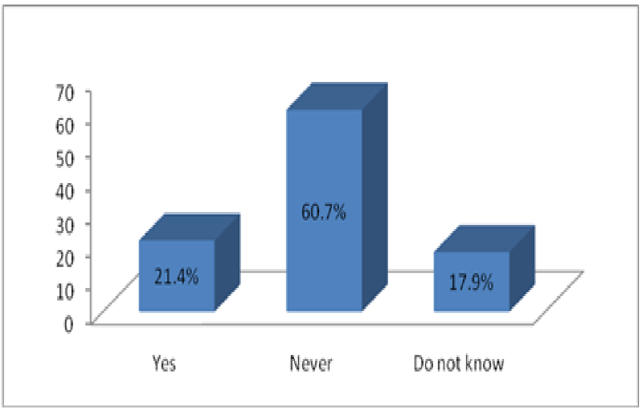

Figure 6: Users of organization website being redirected to bogus web pages even when they type the correct webpage into their web browser

VII. CONCLUSIONS

Confidentiality and Privacy were the top security issues of concern to the respondents followed by integrity. Respondents further considered viruses and malicious software, system or software errors and human errors as the top three main causes of security incidents in their organizations. Unauthorized access, username or password leakage, hacking and theft of business as well as theft of sensitive customer information from respondents' organization websites were also cited as issues. Other issues included: Receiving e-mail messages that look legitimate yet they are fake, employees being tricked to give confidential information about their organization or about a customer by people claiming to be legitimate authorities and attacks using malicious software such as viruses and worm or Trojan horse.

VIII. RECCOMENDATIONS OF THE STUDY

The recommendations of the study based on the findings:

- Organisations practicing ecommerce should formulate policies that promote information confidentiality. Such policies were found lacking.
- Each organisation practicing ecommerce should increase the funds allocated for managing threats against information confidentiality.
- A Risk assessment framework should be developed necessary to assess confidentiality threats in ecommerce.
- Information security experts globally should come up with a unified approach to fight threats against confidentiality.
- Creation of awareness and train staff and consumers on information security services.

g) Recommendation for further Research

- This research is on information security challenges faced by tour and travel companies in Kenya. Additional research concerning other sectors of ecommerce is recommended.
- Research could be done to determine the characteristics of effective security managers.
- The research found that integrity issues were ranked second after confidentiality issues surrounding ecommerce. We therefore suggest that research should be done to address integrity issues surrounding ecommerce.

REFERENCES

1. Arabjafari, M. (2012). *Security in E-commerce.* Available at:
2. http://www.slideshare.net/mohsinq1/security-for-e-commerce?related=1
3. Ciampo, M. (2012). *Security & Guide to Network Security Fundamental, International Edition.*Mexico: Cengage Learning
4. Curtis, G. & Cobham.D. (2005*). Business Information System: Analysis, design and practice Fifth edition*. England: Pearson Education Limited Edinburgh hate Harlow.
5. Hoodrick, M.T. &Temassia, R. (2011).*Introduction to Computer Security*. Delhi : Pearson Education
6. Horak, R. (2002). *Communications Systems and Networks, 3rd Edition*. New Delhi: Wiley Dreamtech India (P) Ltd
7. Norman, A. A.&Yasin, N.M. (2011).*An Analysis of Information Systems Security Management (ISSM): The Hierarchical Organizations vs. Emergent Organization*. *International Journal of Digital Society (IJDS*), (2010). 1(3)
8. Patil, J. (2008). *Information Security Framework: Case Study of a Manufacturing Organization.*
9. Seleanu, D. (2013).*Cyber security in Canada: Finance industry, government seek ways toshare Data.* Available at: http://blogs.reuters.com/financial-regulatory-forum/2013/07/18/cybersecurity-in-canada-finance-industry-government-seek-ways-to-share-data/
10. Trepper, C. (2000). *E-commerce Strategies*.Asoke K Ghosh, Prentice Hall of India Private Limited, Connaught Circus, New Delhi.
11. Ward T. (2010). *Strategies for Reducing the Risk of eCommerce Fraud.First Data*
12. Whitman M. E. &Mettord H. J. (2012**).***Principles of Information Security***, ***4th Edition.Course technology*, Cengage learning