Journal of Theoretical and Applied Information Technology
15th July 2019. Vol.97. No 13
© 2005 – ongoing JATIT & LLS

ISSN: **1992-8645** www.jatit.org E-ISSN: **1817-3195**

PRIVACY ISSUES IN E-COMMERCE

[1]MOHAMMAD AWNI AHMAD MAHMOOUD, [2]ABEER ATALLAH ALOUDAT,[3]LAITH TALAL KHRAIS, [4]SUKINAH ALJISHI, [5]YOSRA HAMZA, [6]MOHAMED NOURELDIN SAYED
[1]Imam Abdulrahman Bin Faisal university, Department of MIS, KSA
[2-4-5]Imam Abdulrahman Bin Faisal university, Department of Accounting, KSA
[3]Imam Abdulrahman Bin Faisal university, Department of Business administration, KSA
[6]Imam Abdulrahman Bin Faisal university, Department of finance, KSA
E-mail: [1]maamahmoud@iau.edu.sa, [2]aaaloudat@iau.edu.sa, [3]lakhris@iau.edu.sa, [4]saaljishi@iau.edu.sa, [5]yehamza@iau.edu.sa, [6]mnsayed@iau.edu.sa

ABSTRACT

The sales and purchase of goods and services through online platforms is increasingly gaining prominence around the globe. Most businesses are currently adopting e-commerce as an option of increasing the profitability of their goods and services. The internet has been an important channel for consumers to source for goods and services, and also as convenient way of making payments. Security of the online business is very important for its success. The research, therefore intends to identify and discuss various privacy and security issues within e-commerce. The research found that there were different causes of security breaches which can compromise the safety of e-commerce operations. The study also found out that there were numerous measures that businesses can implement to counter the rising threat to the security of online-based businesses.

Keywords: *Privacy, E-Commerce, Cyber Law, Technology, Cyber Attacks*

1. INTRODUCTION

Electronic commerce can be described as a way of conducting business through online platform. The security of e-commerce is a wider part of online risks that is being undertaken by many businesses while enforcing safety in business transactions (Gai, Qiu, Sun & Zhao 2016). The practice of e-commerce has an influential effect on the success of the business. Currently, individuals, organizations and multinationals have realized positive results on trade and development because of increased e-commerce transactions (Vakeel, Das Udo & Bagchi 2017). E-commerce has also eased business by enhancing, encouraging and making it convenient and possible for undertake inter-border trading.

However, the development of online transactions has increased security breaches (Aljifri, Pons & Collins, 2013). The amount of economic gains based on online trade has attracted hackers who have financially gained from online theft (Gai,Qiu, Sun & Zhao 2016). Cybercriminals continually develop malicious programs to gain access to online platforms and use them to steal from unsuspecting customers and online merchants. As a result, the e-commerce platform experiences an annual loss that run into millions of dollars each year.

Different measures have been put in place to help curb the rise in cyber-attacks. The aim is to increase the privacy, security and efficiency of e-commerce. Different players have initiated creative measures to enhance e-commerce efficiency (Vakeel, Das Udo & Bagchi 2017). The introduction of cyber laws by different countries is one of the biggest steps in enhancing cyber security and prompting safer online transactions. Besides, as technologies increases, online companies have also created technologies that protect them from marooning cyber criminals.

Research Aim and objectives

The research aims to;

To explore the main underlying security issues and how they affect e-commerce.

The research objective is to;

1. Identify significant threats to e-commerce trade,
2. To identify effective security measures to counter e-commerce threats,
3. To delineate the theoretical and practical implications that emerge from the research for future decision-making in talent management.

1.1 Statement Of The Problem

The emergence of e-commerce technology has had a significant effect on firms' export marketing. However, limited knowledge exists as to how e-commerce drivers influence an organization's import as well as export business strategy. Original outright outcome indicate that internal online marketing drivers such as e-commerce assets and ability to transfer ownership influences a company's level of promotion, increase communication facilitates greater distribution support.

Consistent with Bingi, Mir and Khamalah (2015), the adoption of e-commerce trade platforms by businesses has led to numerous safety concerns. According to Aljifri, Pons & Collins (2013), most e-commerce companies and users have reported incidences of data misuse. In line with the thoughts of Aljifri, Pons and Collins (2013) financial losses have also been reported by both the businesses and customers. The number of online hacking has been on the rise (Galanxhi-Janaqi & Fui-Hoon Nah, 2014). Therefore, in spite of the many advantages of e-commerce transactions, the extent of security breaches continues to increase.

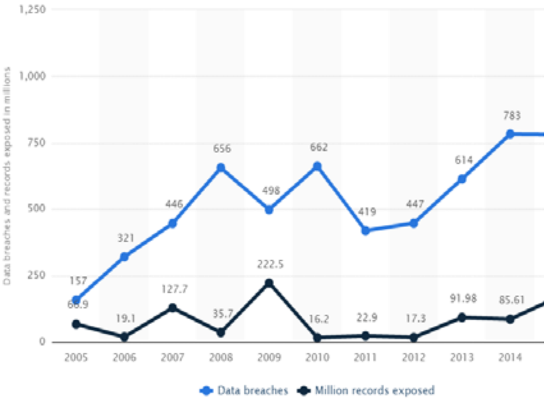
2. LITERATURE REVIEW

The literature review provides an overview of the analysis of different authors' perspectives on the topic of e-commerce security. The analysis gives the variations in thoughts while still providing the common areas where different authors agree. A study by Vakeel, Das Udo & Bagchi (2017), provides a model connecting confidentiality policy, trustworthiness, to online trust, and loyalty of clients and their ability to give trustworthy information. The research engaged 200 volunteers. The results show that the trust of online clients in a company is closely associated to an organization's perception and value for the customer's privacy (Vakeel, Das Udo & Bagchi 2017). Gai, Qiu, Sun and Zhao (2016) agree that trust inversely is associated to increased customer satisfaction and loyalty. This is that confirmed through increased purchases, openness to trying new products, and willingness to participate in programs that engages personal information. Hence, in line with the opinion of Motti and Caine (2015 privacy in the current e-commerce dispensation is an integral part of any e-commerce strategy and investment. Further, privacy security encourages consumer's spending, trustworthiness and loyalty.

Privacy in e-commerce is a critical issue that has attracted attention from different online players. According to Vakeel, Das Udo and Bagchi (2017), the privacy of an e-commerce platform is a very serious issue that requires regulatory and other measures to ensure safety. Vakeel, Das Udo and Bagchi (2017) also noted that 40percent of online users have complained about their online security based on the amount of personal data that they are required to give. The findings are supported by Chou and Chen (2016) who argues that online security was the single most issue that makes people fear using e-commerce platforms. Chou and Chen (2016) stated that the security of merchants and customers is always their priority concern when doing online-based transactions. The above findings also reflected Chatterjee (2015) opinion that 57% of online shoppers were not satisfied with the level of security and thus wanted a regulatory framework to enhance e-commerce transactions. Spiekermann, Grossklags and Berendt (2011) also argue that there is need to establish measures aimed at promoting online user safety. The major of privacy issues that were mentioned by the author was the possible loss and illegal compromise of personal data that the customers are asked when subscribing to the online-based platforms. Niranjanamurthy and Chahar (2013), however refutes the findings, observing that there was a need to come up with personal security measures as opposed to the development of policy guidelines. According to Niranjanamurthy and Chahar (2013), the implementation of security policies is not adequate enough since the development in technology could not be easily eradicated through oversight. All the arguments of the authors proved relevant as they all sought to explore the current privacy issues in e-commerce.

The issue of online privacy insecurity can be traced back to the evolution of e-commerce. According to Gai, Qiu, Sun and Zhao (2016), by 1998, when the online business had begun to pick up, most of the business and players had not enacted adequate measures to protect and enhance the privacy of the users. Gai, Qiu, Sun & Zhao (2016) also theorize that at the time, the level of data leaks to hackers was rampant. The findings of Gai, Qiu, Sun & Zhao (2016) were also supported by Motti & Caine (2015) whose research focused on the earlier development of cybercrime and the e-commerce sector. Motti and Caine (2015) acknowledged that the problems related to e-business privacy have existed since the beginning of online-based commerce. Further, Motti & Caine (2015) noted that the persistency of privacy issues has only surged in recent years despite the increased measures that have been implemented. However, Stead and Gilbert (2011) disagreed with the findings of the other studies, taking the position that the problem of online security threats on e-commerce websites has largely been contained. Stead and Gilbert (2011) also acknowledged the efforts by the e-commerce companies in trying to curb the security threats without fully relying on external interventions. Despite the many detailed observations by the authors, the view of Gai, Qiu, Sun & Zhao (2016) can be considered more detailed as they provide more historical developments on privacy issues.

Figure 1.0: the annual number of data breaches in the US between 2005 and 2016 (millions)



Source: Global Cyber Security centre

The above graph shows that there has been a gradual increase in the number of data breaches in the country. The findings on the graph are in agreement with Aljifri, Pons and Collins (2013) who argued that the number of security breaches within the e-commerce context had been steadily rising over the years.

However, Akter and Wamba, (2016) disagree in regards to the development of privacy issues in e-commerce. The authors argued that the onset of e-commerce did not bring with it privacy concerns. However, the authors acknowledged that the lack of proper mechanisms to protect buyer and seller information led to the subsequent change in online sales. Akter & Wamba, (2016) argued that by early 2000 many years after e-commerce practices had begun, the problems related to privacy began. Majorly, the author attributed the issues of online information theft to the increased technological awareness that led to issues such as hacking. However, despite the disagreement in ideas, both authors proved to have adequate arguments on the development of privacy issues within the e-commerce field.

Despite the numerous privacy issues, there are a number of studies arguing that there are no major privacy concerns within the e-commerce systems if proper measures could be instituted. Gai, Qiu, Sun & Zhao (2016) mentioned that the modern rise in the levels of technology could be one of the best methods that can be used to reduce the rising security threats in the e-commerce industry. Further, Gai, Qiu, Sun & Zhao (2016) stated that the companies can always rely on updated software applications and other technologically advanced tools to counter the rising e-commerce security challenges. Gai, Qiu, Sun & Zhao (2016) also acknowledged the existing skills gap in terms of the number of personnel who can effectively deal with the emerging security challenges. Kokolakis (2017) also argues that by mentioning that hackers were largely using the evasive forms of data breaches on online-based sites to gain unauthorized access. The author further pointed out that hackers were very quick to act on the modern changes in technology as well as any emerging trends in the security world of e-commerce. Thus, Kokolakis (2017) noted that hackers have always had an advantage in countering the new security measures that are implemented by the e-commerce players.

2.1.1 Forms of privacy breaches

The breach of personal privacy is one of the biggest forms of online breaches in the e-commerce sector. According to Kokolakis (2017), the e-commerce platforms provide avenues for hackers to gain access to personal information of people who use such platforms. Kokolakis (2017) noted that the breach of personal security includes access to very personal data which include the names, emails, mobile phone numbers, bank accounts and the location of a person. Vakeel, Das Udo and Bagchi (2017) supports the findings by noting that most online hackers primarily endeavour to acquire personal information and data of the users. Studies exist that point out that personal data can be used maliciously to promote personal security breach and even possible loss of funds. The findings of Akter & Wamba, (2016) were also in agreement with those of Vakeel, Das Udo & Bagchi (2017) who argued that a lot of financial losses in e-commerce transactions results from the theft of personal data relating to financial information of users in e-commerce platforms.

Privacy of communication was also identified as one of the biggest forms of concerns in e-commerce transactions. According to Akter & Wamba, (2016), communication is an important part of the conduct of e-commerce activities. The author also noted that some of the security breaches happen during the communication process. Vakeel, Das Udo & Bagchi (2017) also agreed with the findings by noting that the communication platforms in e-commerce expose a lot of customers to security breaches. Vakeel, Das Udo & Bagchi (2017) stated that most e-commerce websites have communication platforms which allow the customers to communicate directly with the e-commerce companies. However, some hackers take advantage of the poor security process and gain access to communication platforms. Further, Gai, Qiu, Sun & Zhao (2016) admitted that 40% of e-commerce customers have always expressed reservations in expressly using the e-commerce platforms in communication. Gai, Qiu, Sun & Zhao (2016) mentioned that most of the customers have fears that such platforms can always expose their identity to third parties and contribute to potential security breaches. All the three authors provided ideas that were relevant to the study and that sought to answer the research questions.

Location based security breaches is also a case of concern within the e-commerce forum. According to Gai, Qiu, Sun & Zhao (2016), the e-commerce platform has also been subjected to location-based security privacy compromise. Security concerns arise when a certain e-commerce platform is used to identify the location of a user. Further, Gai, Qiu, Sun & Zhao (2016) also noted that technology assistance such as website cookies which many sites ask users subscribe always expose the location of the user. Motti & Caine (2015) supports the assumption that in any e-commerce framework the factors of data integrity, customer and client authentication and non-repudiation are critical to the success of any online business. Further, Motti & Caine (2015 states that hackers are able to trace the exact location and have access to the computer information that operated by a user. The author was concerned that past security breaches have even led to the unauthorised withdrawal of information from the computers of customers which were later misused. Bagchi (2017) posits that the hackers use complex computer programs to trace the location and gain access to some of the personal data and information of users. Bagchi (2017) attributes the problem on the poor security protocol that is implemented by most of the e-commerce companies in a bid to protect their customers. Further, Bagchi (2017) mentioned that most customers were no longer finding it safe to use the online-based e-commerce platforms in conducting tractions since they feared being tracked by cyber criminals.

Frequently, e-commerce security breaches have been fuelled by the need for monetary gains. Galanxhi-Janaqi & Fui-Hoon Nah (2014) and Gai, Qiu, Sun & Zhao (2016) argues that most of the people who seek unauthorised entry onto the company of e-e-commerce websites do so with the belief that they will make some money. Gai, Qiu, Sun & Zhao (2016) posits that the security breaches always target the customer and the company. Galanxhi-Janaqi & Fui-Hoon Nah (2014) noted that one of the biggest threats to the e-commerce business was the unauthorised transfer of funds or diversion of payment from the customers into the individual accounts of criminals. That way, the company end up losing huge sums of money to wrong hands. Galanxhi-Janaqi and Fui-Hoon Nah (2014) comments that some of the cyber criminals gain entry into the systems and post fictitious orders and items. In most case, such orders would be delivered to physical addresses that are set up by the fraudsters. Such actions, Galanxhi-Janaqi & Fui-Hoon Nah (2014) notes, have led to millions of dollars in losses across the e-commerce industry. Finally, Vakeel, Das Udo & Bagchi (2017) also wrote that some of the online frauds and authorised hacks are undertaken by competitors. The study noted that due to increased competition within the e-commerce field, some companies were involving unethical business practices. Vakeel, Das Udo & Bagchi (2017) specifically noted that one of the business practices that was being undertaken by competitors was to bring down their online platforms or create security interference as a way of reducing customer dependence and trust on such companies. All the authors provided a detailed analysis. However, the views of Vakeel, Das Udo & Bagchi (2017) differed since they argued based on different sources of security threats within an organization.

2.2 Organizational Issues In E-Commerce Security

The solution to threats to organizational security is only based on the implementation of stringent security processes. According to Gai, Qiu, Sun & Zhao (2016) internal organizational rules and policies are important in meeting the daily security needs of a business that operates within the e-commerce space. Galanxhi-Janaqi and Fui-Hoon Nah (2014) also supports the need for organizational involvement in promoting e-commerce security. Galanxhi-Janaqi and Fui-Hoon Nah (2014) argues that the e-commerce business should be the first respondent in analysing and implementing security measures that would help in the development of comprehensive and secure online platforms. All the arguments by the three authors give insightful information on the different ways of enhancing providing security processes.

Organizations which participate in e-commerce business need to come up with proper mechanisms for dealing with online threats. In the view of Galanxhi-Janaqi and Fui-Hoon Nah (2014), the best approach that must be adopted by organizations is to set up integrated security systems and employ security experts to manage the systems. This argument is supported by Gai, Qiu, Sun & Zhao (2016) who stated that within the current business environment, e-commerce businesses must specially consider employing full-time security experts who can handle all the rising online-based security threats. Galanxhi-Janaqi and Fui-Hoon Nah (2014) also supports the point that the success of any future online businesses can only be based on developing stronger anti-hacking technology that would promote the security and privacy of all the customers.

The development of effective internal organizational systems would be useful in handling online-based security threats. According to Gai, Qiu, Sun & Zhao (2016), the installation of risk management processes within the business would help to maintain integrity of any online business. Gai, Qiu, Sun & Zhao (2016) further argued that the separation of tasks within the security management system would also help to prevent internal security breaches. This view is supported by Vakeel, Das Udo & Bagchi (2017) who acknowledged the rise in the incidences of collusion between internal business operatives and external hackers to breach the e-business systems. Gai, Qiu, Sun & Zhao (2016) also contributed to the research by adding that limiting the access control within the security system would form an important basis for enhancing system security and preventing possible attacks.

Finally, ensuring proper security upgrade would form a very useful step in the reduction of security breaches within the online platforms. According to Gai, Qiu, Sun & Zhao (2016), technology, especially within the security arena is a fast-changing phenomenon. Das Udo & Bagchi (2017) also appreciate that dealing with emerging security threats would require proper and adequate security upgrade based on new developments. Das Udo & Bagchi (2017) also further acknowledged the pace at which hackers are quick to update their technology and increase their illegal online presence.

2.2.2 Implementation Of E-Commerce Security Technologies

With the increase in security technologies, there are different approaches that can be used in managing e-commerce security threats. According to Das Udo & Bagchi (2017), the most effective security technology for increasing safety of e–commerce platforms is encryption algorithms. Das Udo & Bagchi (2017) stated that there are many approaches to security encryption through the above method. Galanxhi-Janaqi & Fui-Hoon Nah (2014) also contributed to the research by adding that one of the most effective approaches is the use of Public Key Infrastructure (PKI). Gai, Qiu, Sun & Zhao (2016) also acknowledged the research by defining KPI as the layer of online security which is useful in preventing successive security breaches. Hsu (2019) observes that the trend by e-e-commerce companies to reward spenders has increased online criminal activities.

Niranjanamurthy and Chahar (2013) observes that the creation of digital signatures and security keys were important approaches in the promotion of e-commerce security. The findings were also supported by Spiekermann, Grossklags & Berendt (2011) who acknowledged that the e-commerce stability was increasingly being achieved through online certification processes. Spiekermann, Grossklags & Berendt (2011) noted that online signatures had increasingly been used as a means of locking out potential hacks who seek entry into the system. Further, Gai, Qiu, Sun & Zhao (2016), also appreciated the adoption of single security points within online platforms as a means of narrowing the risk of online manipulations. Gai, Qiu, Sun & Zhao (2016) concludes by positing that all the above processes and methods have helped to increase customer confidence and lower possible financial losses associated with e-commerce security threats.

3. METHODOLOGY

The research methodology section provides a clear and detailed analysis of the approaches and methods in this study. Specifically, this section entails data collection and analysis methods (Gai, Qiu, Sun & Zhao 2016). The methodology also includes an exclusive examination into the various data research limitations that could have influenced the outcome of the study. The study also discussed the various assumptions that existed while conducting the research.

3.1. Data analysis approach

Specifically, the study adopted a qualitative data analysis approach.

3.1.1 Qualitative data analysis approach

According to Quinlan, Babin, Carr & Griffin, (2019), the qualitative analysis method is used in the collection and analysis of data. Quite often, qualitative data provides non-numeric information that a study will use while undertaking the research. The study used the following approaches in the analysis:

Content analysis: The approach was used in making inferences by enhancing the interpretation of data and research findings in as far as e-commerce are concerned.

Narrative analysis: The narrative method is used as a data analysis method, especially when analysing data which come from respondents. The methodology applies experiences from people and shared knowledge to support the analysis. The study used the approach to analyse the primary data that was collected from the field.

3.2. Data and data collection methods

The study relied on both primary and secondary data which formed the basis of the research information.

3.2.1 Primary data

The research utilized 50 respondents for the interview and 50 for taking part in the providing answers in the form of questionnaires. The approaches used to gather the data are discussed below:

Questionnaires: The study identified relevant respondents who provided information regarding the privacy issues in e-commerce.

The people who took part in the research were drawn from the different professional and social background. The study ensured that the composition of respondents would provide authenticity and reliability on the final research.

A total of 50 participants took part in the research. Of the total number of participants, the study ensured that there was a balance in representation. The highest number of respondents consisted of 25 e-commerce customers. The reason for having high representation of the customers in the research was based on the nature of business since the customers are the most affected within the e-commerce industry. In addition, the group is also crucial for the success of the electronic businesses and their security guarantees sales. The study also included 10 e-commerce business executives as part of the respondents. The executives formed an important part of the response teams as they have a clear operational background of the online-based businesses. In addition, the executives had a clear knowledge of the security issues facing the business. The study also included 15 online security experts. It was important to have views on the professionals on how best to promote efficiency in doing business.

Interviews:

The study sampled 50 respondents who took part in the interview process. The interviews consisted of 25 affected customers who gave views about their level of experience and confidence on the e-commerce platforms. The interviews also consisted of 10 online business executives whose business has been affected by hackers. There were also 15 online security experts who have taken part in the process protecting e-commerce businesses. The experts also gave their thoughts on the current security challenges and possible solutions.

3.2.2 Secondary data

Books and journals: The study used several books and journals which had information related to security issues within the e-commerce sector.

There were specific inclusion and exclusion criteria adopted in the study. The inclusion criteria consisted of:

i. Peer-reviewed literature
ii. Literature that is not more than 7 years.
iii. Company websites

On the other hand, the exclusion criteria for the research study consisted of:

i. Non-peer reviewed journals
ii. Personal reviews and editorials

The databases that were used by the study consisted of several journal sites such as the Journal of Business Ethics and International Journal of Advanced Research in Computer and Communication Engineering.

Online data from websites: The study used online platforms that contained information on the modern security risks that face the e-commerce industry. The choice for the online platforms was based on the accessibility of most recent data on the security issues within the sector. The online platforms contained recent emerging security threats and discussions by professionals on the possible solutions to the rising challenges.

3.3 Ethical issues in the research

While conducting the research, the study considered several ethical issues which are essential for the completion of a successful study. The ethical issues are discussed below:

Informed consent: the study ensured that before collecting data from the respondents, there was a clear acceptance from the respondents to participate in the study. The study had to make early formal requests to the respondents and request for their participation in the study. The respondents who declined to participate in the study were not included. The study also assured that the respondents that the information that they provided would only be used for the purpose of the research only.

Respect for confidentiality and anonymity:
The study ensured that privacy is paramount. In fact, the study did not collect personal information of the respondents such as names, religious affiliations or age. The collection of data was done within an environment that made the respondents feel secure and confident.

Respect for privacy: The analysis took into account the privacy of the respondents. While formulating the interview questions and the questionnaires, the study made sure that there was no direct question that would interfere with the privacy of the respondent.

Professionalism: The study also observed the highest level of professionalism. Specifically, the study adhered to the codes of ethics in research.

3.1 Research limitations and assumptions

The study relied on secondary data, from online sources which were the subject of manipulation and change. The study also found it hard to obtain primary data from the respondents. Further, due to increased competition most of the e-commerce entities did reveal their security details for the sake of their customers. Lastly, the e-commerce companies did not provide information on the possible security solutions to the e-commerce security lapses since they did not want the security measures to cause public fear and compromise sales.

3.4 Study population

The population consisted of customers who had used the e-commerce sites to purchase goods or services. The table below summarizes the respondents.

Table 1: Research population

Category of respondents	**Number of respondents**
e-commerce executives	20
Online security experts	30
e-commerce Customers	50
Total	**100**

Based on table 1.0, the study will seek to obtain data from a total of 100 respondents drawn from different groups and stakeholders in the e-commerce industry.

4. RESEARCH ANALYSIS, DISCUSSIONS AND VALIDATION

The research analysis, discussion and validation section provided the various analyses that the study conducted based on the data that had been collected.

4.1 Privacy concerns within the e-commerce sector

The study wanted to establish the existence of security concerns within the e-commerce sector. Therefore, the research came up with a list of security issues within the e-commerce sector and asked the respondents their opinion on the major security threat to the e-commerce market. The table below gives the analysis of the research findings.

Table 2: privacy concerns

Privacy concern	Respondents	Percentage (%)
Misuse of personal data	80	80%
Physical security threat	12	12%
Exposure of company data	18	18%
Total	**100**	**100%**

Based on the figure, the study found out that most of the respondents cited loss of personal data as one of the biggest security threats within the e-commerce industry. Most of the respondents believed that in a number of cases the information that is given by the customer ends up being misused. The findings attributed the loss of information to information theft either within or outside the e-commerce companies. The research findings were in agreement with the works of Das Udo & Bagchi (2017) who argued that most online based customers feared giving out their personal data since they feared that such information would be misused and lead to their data privacy breach.

The research findings also revealed that 18% of the respondents believed that e-commerce company itself faced a threat to its privacy as a result of its exposure to third parties. The results may show that the respondents believed that the e-commerce business could also face the possibility of hacks and misuse of its data. The research findings also showed that 12% of the respondents believed the biggest privacy issue within the e-commerce industry was an exposer of persons to physical security threats. The respondents believed that people could use the commerce sites to gain information about the personal details of people. These respondents, therefore, believed that the incident would cause a personal security breach to the affected persons. The findings were similar to the works of Gai, Qiu, Sun & Zhao (2016) who believed that the e-commerce companies also faced similar security threats dues to possible data breaches from external sources.

4.2 Causes of security threats in the e-commerce industry.

The study also sought to know the major security threats that were associated with operating an e-commerce business, both for the customers and the business. The study aims to examine the belief of respondents on how the causes such as hacking, internal online security compromise and weak security protocol. The table given below shows a summary of the different findings.

Table 3: causes of security threats in the e-commerce

Cause	Respondents	Percentage (%)
Hacking	45	45%
Internal data breaches	15	15%
Weak security protocol	40	40%
Total	**100**	**100%**

Based on the result obtained in table 3.0, the study found out that majority of the respondents believed that the major cause of security threat to the e-commerce business was hacking. 45% of the respondents believed that hackers used advanced technological methods to gain unauthorized entry on the e-commerce database and gain access to crucial customer and company data. The respondents also believed that the hackers used such data for personal gains, leading to the company losing customers. The research findings were similar to those of Galanxhi-Janaqi & Fui-Hoon Nah (2014) who stated that the major security threat within the e-commerce sector was caused by hacking activities which were promoted by malicious individuals. The findings f Gai, Qiu, Sun & Zhao (2016) were also relevant since the author found out that most companies had complained that they were facing numerous hack attempts which increased their zeal to enhance online security.

However, 40% of the total respondents also believed that weak internal security portal was responsible for the breach on e-commerce security. The respondents attributed the breaches to the failure of the e-commerce establishment to institute stringent security policies and measures which would help to improve overall reliability and security. The works of Spiekermann, Grossklags & Berendt (2011) were also in agreement with the research findings. The study noted that some of the online-based companies failed due to the poor internal security procedures aimed at reducing security breaches. Only a few of the employee believed that internal data and security breaches were responsible for causing the problems to the e-commerce sector. The 15% of the respondents believed that the employees working for the e-commerce companies conspired to gain entry into the system and cause different forms of breaches and security threats both t the customers and to the entity. The research outcome was also supported by Gai, Qiu, Sun & Zhao (2016) who noted that some of the employees within the e-commerce companies conspired and helped to increase incidences of data breaches.

4.3 The measures aimed at curbing rising e-commerce security threats.

The study also sought the opinion of the respondents on whether they believed that there were adequate measures to improve and increase e-commerce security. The study categorized the security agencies responsible for enhancing online security int two sections. The table below gives a summary of the research findings.

Table 4: are there measures for curbing security threats?

Measures		**Respondents**	**%**
Industrial	Adequate	40	40%
	Inadequate	60	60%
Company-based	Adequate	65	65%
	Adequate	35	35%

Based on the above responses, the study discovered that most of the respondents believed that the e-commerce companies had positively responded to handling e-commerce shortcomings as compared to the measures taken by the industry players and regulatory bodies. Out of all the respondents, 60% believed that the industrial e-commerce stakeholders and policymakers had not adequately put measures that could help to curb the rising problem of security threats. The studies who gave the above opinion shared an ideology with the research findings of Gai, Qiu, Sun & Zhao (2016). The studies noted that e-commerce industrial players were committed to increasing security surveillance and making more policies that were aimed at developing the e-commerce sector. Only 40% of the respondents had faith in the policymakers and believed that they had the capacity to effectively handle the issue within the available constraints.

On the other hand, 65% of the respondents believed that the individual e-commerce companies had been responsible for creating security measures study that help in curbing the security challenges that exist online. The respondents attributed the increase in security surveillance to the security systems that the businesses were using as a back-up to their other security processes. Gai, Qiu, Sun & Zhao (2016) also gave views which were similar to the research outcome. The studies mentioned that different companies were installing newer security software and enhancing their security capabilities in readiness to handle the emerging security threats within the industry.

4.4 Security measures for curbing e-commerce security threats.

The study also wanted to establish from the respondents the security measures which they deemed most appropriate in handling and managing the challenging e-commerce security threat. The study came up with specific security apparatus that most of the players within the e-commerce sector were using. The respondents were asked to determine the measures that they considered most appropriate.

Table 5: security measures in e-commerce

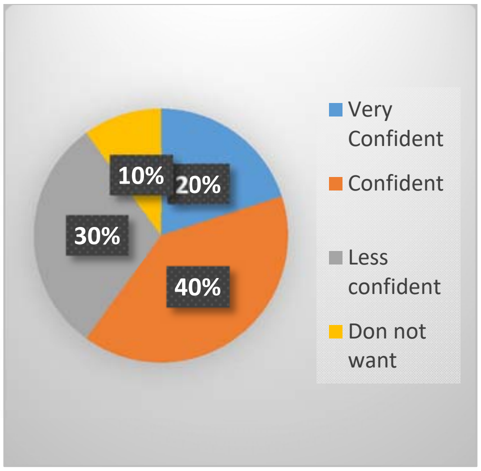
Security measure	**Respondents**	**Percentage**
Security software	50	50%
Security policies	15	15%
Customer sensitization	25	45%
Physical security	10	10%
Total		**100%**

Based on the above research findings, it is clear that most respondents believed that the best solution to the security issues within the e-commerce space was the use of security software. The 50% of the respondents believed that by e-commerce businesses installing adequate security systems, they were at a better position to overcome the security challenges such as online hacks and improve on the integrity and reliability of online-based businesses. 45% of the respondents believed that sensitizing the customer on the threats of security within the online space was important in creating a secure e-commerce environment. The findings were consistent with the works of Spiekermann, Grossklags & Berendt (2011) who believed that the biggest way of reducing e-commerce security threats was by having updated security software installed within the business systems. On the other hand, 15% of the respondents believed that instituting adequate and stringent security policies would help to overcome the rising e-commerce security challenges. The finding closely related to the works of (Gai, Qiu, Sun & Zhao, 2016). Gai, Qiu, Sun & Zhao (2016) stated that new policies and security protocol were an important way of eliminating the current security breaches and improving the performance of online businesses. Only 10% of the respondents believed that having physical security systems would be a solution suitable for solving online security threats within the online business space.

4.5 Customer confidence in the e-commerce system

The study also sought to find out the current level of customer confidence in the use of e-commerce systems for their daily purchase needs. The respondents gave a varying opinion which is summarized in the diagram shown below:

Figure 2.0: Customer confidence in e-commerce platforms



The above research findings revealed different factors regarding customer confidence in the e-commerce platforms. From the data, 40% of the total customers reported that they were confident that they would continue to make purchases and carry on online-based buying. The majority were optimistic, even though they appreciated the dangers of online purchases due to potential security threats. The findings were consistent with the works of Motti & Caine (2015) who mentioned that despite the knowledge of online risks in the e-commerce market, the customers still carried out buying and selling on these platforms.

The study also showed that only 20% of the total respondents had absolute assurance that the e-commerce platforms would provide them with value for their transactions. The respondents were certain that e-commerce was safe for their use. Therefore, the group expressed their interest in using the platform.

30% of the respondents expressed less confidence in the e-commerce business based on the security threats that were experienced within the sector. The group believed that though there was higher risk involved, they would still undertake specific transactions or purchases from the e-commerce websites while taking much caution. However, 10% of the respondents did not have any confidence in the security of the e-e-commerce transactions. The above group of respondents believed that the platforms posed very high risks they would not comfortably use them. The research findings compared to the works of Gai, Qiu, Sun & Zhao (2016) which acknowledged that there were many customers who were shying away from using online purchase platforms. Gai, Qiu, Sun & Zhao (2016) noted that the customers feared that their own security was at risk and that they would risk losing much of their data to unknown persons and hackers.

5. DIFFERENCE FROM PAST RESEARCH

The research findings revealed several outcomes which were not consistent with the earlier assertions and conclusions by different authors. A comparative analysis between the past between the research findings and the review of past literature revealed the differences.

First, the research findings revealed that customer sensitization on security approaches within the e-commerce platform was one of the biggest ways that would be used to improve online security. In fact, the research found out that 45% of the respondents believed that the sensitization process was able to successfully help in reducing e-commerce security breaches. However, Vakeel, Das Udo & Bagchi (2017) mentioned that the most important some of the most important security management platforms available for the e-commerce sector included software solutions and policy guidelines. In fact, the author did not even appreciate that sensitization was one of the measures. Similar opinions were also shared by Das Udo & Bagchi (2017) who also failed to acknowledge the use of security sensitization approaches in the management of e-commerce security threats.

Additionally, the findings from the data also showed that the exposure of the company data and information was a major security threat. The findings revealed that 18% of the respondents acknowledged that when data belonging to the e-commerce companies were exposed, there was a higher risk of a security breach. However, the findings were not supported by Spiekermann, Grossklags and Berendt (2011). The authors, however, mentioned that the operation of the e-commerce companies is based on public advertising on its online platforms. The author also noted that the above requirement was only limited to the marketing on the products and services. The findings of Niranjanamurthy & Chahar (2013) also provided a different viewpoint of the research outcome. The study argued that almost of online-based companies seek to have a policy of non-revelation of their internal data. Above all, the security of e-commerce companies is paramount. Therefore, the authors alluded that there are no cases of such companies exposing their data for public scrutiny. Instead, they seek to protect such data as they include sensitive information such as customer data. Therefore, the authors' thought was not in agreement with the research findings which blamed the availability of public data on the breach of internal company security.

6. CONCLUSION

In conclusion, the research found that there has been a steady growth and popularity of e-commerce business. The research established that increase in the digital economy have been the major driving force in the development of the e-commerce space. The study also noted that despite increased popularity of the e-commerce businesses, it faces major security threats.

The study reviewed different literatures which refuted while others agreed with the topic at hand. The literature review also discussed causes, trends and possible solutions to the rising security concerns in the online marketing. In exploring the research area, the study used different methodologies to analyze the primary data. The study, concluded that most of the customers and users of e-commerce platforms believe that the biggest security concern was the theft and manipulation of personal data y criminal for financial again. The research also established that hacking is the biggest threat to a secure e-commerce business platform. The study also found out that most of the stakeholders within the e-commerce sector believed that the company-based interventions were the best measures that would help in curbing the security threat, both to the customers and the business. There were a few findings which were also not consistent with the findings of another study. However, the differences were minimal and did not affect the overall findings.

Limitation of the study

The research provides a foundation upon which other studies would depend on in assessing security threats facing e-commerce businesses. The results of this research would be appreciated academically as well as throughout the globe. Additionally, the study is limited to e-commerce platform because it is the current and most used means of the trade in the near future. Also, this paper is limited to managers, users and online security experts who will find this information useful for predicting which systems will be acceptable to customers, diagnosing reasons why the system may not be fully acceptable to customers, and which corrective actions to take in increasing the acceptability of their systems. Besides, another limitation is that being a relatively new field, many organizations were not willing to disclose as much information as possible. Hence, majority of the information were limited to peer-reviewed articles.

7. RECOMMENDATIONS

In this knowledge and technological dependant world, e-commerce remains one of the vial mans of doing business. This paper suggests the following recommendations to: enhance the security of both shoppers and e-commerce companies.

1. Embrace HTTPS technologies: these technologies are increasingly being embraced e-commerce companies as effective online security. Earlier, online platforms used HTTPS specifically in payment areas as the most sensitive area. However, as time went by it became increasingly demanding to secure the whole site and not just one particular page. It became pertinent to include each page as a potential threat hence the need to protect client's data. Adopting HTTPS technologies implies that sites display a green secure text with a green lock around the URL area. The green lock goes an extra mile of easing the doubts of online shoppers who always look for a sign to assure them of a credible and secure site.

2. Choosing the right e-commerce platform: a larger percentage e-commerce shops use the Magento and Shopify which has been bedevilled by security issues. Key among the factors that shoppers and merchants look for in any online shopping is convenience, robust functionality, and security.

3. Use of security Plug-Ins: Online merchants are advised to pick the right Plug-Ins such as Wordfence security which is powered by Web application firewall. Tis particular Plug-In prevent online shopping sites from getting attacked and also gives e-commerce platforms real time view of the traffic including potential hacking attempts.

4. Keep admin panel secure: Hackers use various angle to penetrate e-commerce site. However, the most common they use is to penetrate through the admin panel. However, if well secured, admin panel has proved to be one of the effective ways of securing the e-commerce shop. What it takes is a strong password to secure the online shop. It is advisable to change the admin username as well as password on often basis.

REFERENCES:

[1] Akter S, Wamba SF. Big data analytics in E-commerce: a systematic review and agenda for future research. Electronic Markets. 2016 May 1;26(2):173-94.

[2] Aljifri HA, Pons A, Collins D. Global e-commerce: a framework for understanding and overcoming the trust barrier. Information Management & Computer Security. 2003 Aug 1;11(3):130-8.

[3] Bingi P, Mir A, Khamalah JN. The challenges facing global e-commerce. IS Management. 2000 Sep 1;17(4):1-9.

[4] Chatterjee S. Security and privacy issues in E-Commerce: A proposed guidelines to mitigate the risk. In2015 IEEE International Advance Computing Conference (IACC) 2015 Jun 12 (pp. 393-396). IEEE.

[5] Gai K, Qiu M, Sun X, Zhao H. Security and privacy issues: A survey on FinTech. InInternational Conference on Smart Computing and Communication 2016 Dec 17 (pp. 236-247). Springer, Cham.

[6] Galanxhi-Janaqi H, Fui-Hoon Nah F. U-commerce: emerging trends and research issues. Industrial Management & Data Systems. 2004 Dec 1;104(9):744-55.

[7] Hsu T. Why Rewards for Loyal Spenders Are 'a Honey Pot for Hackers' [Internet]. The New York Times. The New York Times; 2019 [cited 2019May22]. Available from: https://www.nytimes.com/2019/05/11/business/rewards-loyalty-program-fraud-security.html

[8] Kokolakis S. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. Computers & security. 2017 Jan 1; 64:122-34.

[9] Chou HL, Chen CH. Beyond identifying privacy issues in e-learning settings–Implications for instructional designers. Computers & Education. 2016 Dec 1; 103:124-33.

[10] Motti VG, Caine K. Users' privacy concerns about wearables. InInternational Conference on Financial Cryptography and Data Security 2015 Jan 26 (pp. 231-244). Springer, Berlin, Heidelberg.

[11] Niranjanamurthy M, Chahar D. The study of e-commerce security issues and solutions. International Journal of Advanced Research in Computer and Communication Engineering. 2013 Jul;2(7).

[12] Quinlan C, Babin B, Carr J, Griffin M. Business research methods. South Western Cengage; 2019.

[13] Spiekermann S, Grossklags J, Berendt B. E-privacy in 2nd generation E-commerce: privacy preferences versus actual behaviour. InProceedings of the 3rd ACM conference on Electronic Commerce 2001 Oct 14 (pp. 38-47). ACM.

[14] Stead BA, Gilbert J. Ethical issues in electronic commerce. Journal of Business Ethics. 2001 Nov 1;34(2):75-85.

[15] Vakeel KA, Das S, Udo GJ, Bagchi K. Do security and privacy policies in B2B and B2C e-commerce differ? A comparative study using content analysis. Behaviour & Information Technology. 2017 Apr 3;36(4):390-403.

APPENDIX

Appendix 1: Interview questions

For customers

I. Kindly mention why you opted to use e-Commerce options as a customer.

………………………………………………
………………………………………………
……………………………………..

II. What greatest fears make you feel skeptical about using e-commerce sites?

………………………………………………
………………………………………………
……………………………………..

III. Have you ever been affected by hackers?

………………………………………………
………………………………………………
……………………………………..

For business managers and security experts

IV. Kindly mention the security measures aimed at increasing e-commerce security awareness.

………………………………………………
………………………………………………
……………………………………..

V. Describe the different remedies that are available towards the promotion of security.

………………………………………………
………………………………………………
……………………………………

I. What policy changes can help to prevent further e-commerce fraudulence.

………………………………………………
………………………………………………
……………………………………

Appendix 2: Questionnaires

For customers

i. Have you ever been affected by the actions of hackers?

………………………………………………
………………………………………………
……………………………………

ii. Do you have faith in the security system that is used in the e-commerce market?

………………………………………………
………………………………………………
……………………………………

iii. What personal security measures guide your online transaction?

………………………………………………
………………………………………………
……………………………………

For business managers and security experts

iv. What are the best e-commerce security solutions?

………………………………………………
………………………………………………
……………………………………

v. What are the current security trends that promote e-commerce security and safer working environment?

………………………………………………
………………………………………………
……………………………………

vi. What do you think are effectiveness levels for the adopted sector measures within e-commerce?