

Network Security and Its Impact on Business Strategy: A Case Study on E-Commerce Site Daraz.Com

Vinaya Shakya¹, Jyotir Moy Chatterjee² & RN Thakur²

¹PG Scholar, College for Professional Studies, Kathmandu, Nepal

²Assistant Professor (IT), LBEF Campus, Kathmandu, Nepal

Abstract

With the growth of e-commerce and its acceptance, it is quite certain that it will be the future of shopping. However, there are a lot of security issue that has to be considered during online shopping and its procedures which can impact in such a way that both customers as well as companies could suffer such that they can never come up again. Therefore, this paper attempts to find out if people in Nepal have adopted online shopping or still prefer traditional shopping and also identify if people are conscious about e-commerce security on the basis of the leading e-commerce company daraz.com. However, the main aim of the paper is to determine if the security considerations and fear in e-commerce and trust of customers over the e-commerce system impact the business of a company.

In this paper, mixed research approach is applied i.e., the mixture of quantitative and qualitative research methodologies so that better and deeper insight can be obtained. Several previous papers like journals, conference papers, case studies, etc. were reviewed and also data collection is done through questionnaires distributed through online forms and few offline forms. Cronbach's alpha reliability testing is used for statistical reliability testing of the data collected through online and offline questionnaires. Further analysis of the data is done using Pearson's Chi-Square test by applying the test on certain variables and using the data analysis application "SPSS".

Keywords: Mixed research, data analysis, online shopping.

1 INTRODUCTION

E-commerce is the short form of Electronic Commerce which is in simple terms a modern way of performing commerce or business online with the intension of addressing the needs of customers, vendors and enterprises to deliver goods and services in short time accompanied with reduced cost. With the popularity and world wide web emergence, there has been a drastic boom in e-commerce and customers and companies have developed interest in this digital business. Hence, business strategy and operations now a days have changed in a way to adopt e-commerce as secondary source of business or many of the companies have considered online trading as primary too. (Fianyi, 2015) E-commerce can also be called as e-business is not only the center for buying and selling of goods and services but also incorporates producing demands for goods and services, providing customer service and sales service or facilitating business partners with communications. (Revathi C, 2015) With the emergence and adaptation of e-commerce by customers as well as business enterprises, there is, has been and will always be a concern regarding the e-commerce security i.e., how secure it is to perform transactions and operations through e-commerce.

1.1 Introduction to e-commerce security

One of the most e-commerce critical success factors is security. Without customers and enterprises being assured and confident regarding the security of e-commerce, e-commerce may not reach to where it intended to reach. E-commerce is seen simple and easy for everyone involving with it but with simplicity, there is complexity too as e-commerce security includes the personal information which may be extremely sensitive, confidence between the buyers and sellers and other entities like credit card, etc. If there is one thing that restricts customers and organizations, then it is security and without the restrictions several inappropriate and unwanted incidents may take place. Some web e-commerce companies that are indulged in payments (electronic transactions, PayPal, credit cards, online banking, debit cards or other mediums of online payment) have more complexity in terms of security like the consequences that have to be faced if any data loss or alteration takes place. E-

commerce needs a trustable infrastructure and a framework in order to perform successful and stable e-commerce. (Sibo Prasad Patro, 2016) In the present context, the e-commerce owners are considering on how to increase more customers and how to make clients feel assured about security when performing e-commerce through web applications or other mobile applications and on the other side, it is also important how the clients rate a web based commerce site or application and how can customers supposed to secure themselves as they are one of the most important parties in the online network.

The customer should be clear about the security policies and should trust the e-commerce site which is at the hands of e-commerce owners and how they have designed the security framework which performing e-commerce. Below are the most essential requirements to ensure trustable and safe electronic payments or transactions: (Ghayoumi, 2016)

- Confidentiality: Confidentiality incorporates a set of policies and rules (may be executed through agreements on confidentiality) that prevents and limits access or provides restriction on certain information that are shall not be visible to unauthorized users.
- Integrity: It means that the information shall not be altered over a network during its transmission. In order words, the information shouldn't be tampered so that the exact information remains same throughout its transmission.
- Availability: It is based on the principle that the information or details should be available whenever needed anywhere and wherever appropriate on the mentioned time frame.
- Authenticity: It is another mechanism of authenticating if the user is authorized one before providing people or users with the information requested or required.

1.2 Brief background on security in e-commerce systems

It is to agreement of most experts without effectiveness of security systems, e-commerce can't reach to the level of success it should meet. If customers don't feel that there is adequate security, they wouldn't be willing to share the personal details/information that are sensitive and needed for e-commerce transactions like the information of credit card numbers, contract of business, etc. The losses due to cybercrime reached to approximately US\$378 million as found by Computer Security Institute and FBI study in 2001. US\$700 million loss in e-tail sales was found by another study due to online fraud which compared to traditional retailer's fraud was 19 times higher. (Encyclopedia.com, 2021)

1.3 Ethical issues, challenges

E-commerce is a platform in which exchange of products and services is involved over the internet. Such kind of trading process, is done through online shopping websites through which retail sales directly to the customers can be made. Here many activities like third party business-to-business, customer-to-customer sales, business-to-customer selling and buying takes place which may involve collecting and using demographic data via social media or web contacts. For the e-commerce systems to be easy and effective, the system requires some other third-party applications or communities like online banking platform, mobile and internet connection, electronic data interchange, etc. (club, 2018)

This kind of electronic trading system has made business really easy but also has disadvantages aligned with the benefits. There might be umpteen number of threats regarding the information and network security to any organization in which transaction is involved. Also, it is not possible for the organizations to afford or apply all the assets which can be used to protect from such security threats and vulnerabilities. There can be several dangers to an e-commerce company such as a hacker, a spy, any faulty hardware or software, etc.

Below are some of the ethical security issues that affect e-commerce and there are always a number of ways or ever-changing new ways of attacking a computer network system due to which can result in consequences that an e-commerce company might not be able to bear or compensate.

- a) Information Theft: Information theft means that the attackers obtain the records belonging to an organization. The attackers do it with the help of eavesdropping, spoofing, using brute force technique using some kind of software program helping to guess passwords. There are

some vulnerabilities through which information theft can be done and some information theft examples are ATM spoofing, PIN capturing, credit card number theft, electronic cash, etc.

- b) IP spoofing: It refers to acting as if one has acquired the IP address of another. E-commerce enterprises have routers to track which packets are ingress from which IP address belonging to the sender, hence, this kind of techniques can be used by the attackers. There are also some applications which need login by clients and the valid users are organized by the IP address of the client but the attackers can in such cases can act like the valid users spoofing the IP address of the valid users and acting as the valid users being the unauthorized users. It is difficult to detect IP spoofing, hence the e-commerce security system should be developed with the ability of monitoring traffic on the interface of the routers in the internet checking the destination and source IP address of the clients.

1.4 Problem Statement

E-commerce is becoming a dominant field in trading now a days and has become the future of business in this global world where the usage of internet and smart devices is increasing day by day. As the accessibility to internet has increased and also people are becoming more and more familiar to smart devices, it seems that people have preferred e-commerce a lot. We can say that customers have adopted e-commerce as the e-commerce sales has been predicted to reach to \$4.5 trillion by 2021. (Loop54, 2019) Below are the problem statements of this research which have relationship to e-commerce security and what is the impact on business regarding the e-commerce security-commerce has made its immense growth lately in this digital world but with its success, it might not be secure for business sensitive data, information of customers. (Affia, 2018)

- Only if the customer is satisfied by buying from the e-commerce site, only then customer will trust the e-commerce site. (Dan J. Kim, n.d.)
- Somehow, people are aware of the vulnerabilities and security issues with e-commerce especially during e-commerce transactions. If customers don't feel secured and don't trust the e-commerce site regarding security, e-commerce can't be effective and will not reach to the level of success it should reach to.

1.5 Research Questions

There are several other research journals/papers regarding e-commerce security globally available, however, this research is based on the security of e-commerce and its impact on business in the context of Nepal. There are currently many companies that have started and/or already adopted e-commerce over traditional commerce like Daraz, SastoDeal, Nepbay, Socheko, Hamrobazar, Gajabko, Bhatbhateni Online Shopping, Smart Doko, etc. and among them Daraz is one of the best online shopping sites and also is the number one online shopping site in Nepal. This research is based on this leading e-commerce company i.e., Daraz. Following are the research questions included in this research:

- RQ1 As Nepal is a developing country and e-commerce has recently been evolving in Nepal, have customers here adopted e-commerce over traditional e-commerce?
- RQ2 Are customers aware of the e-commerce security and do customers in Nepal consider e-commerce security while performing e-commerce purchases?
- RQ3 Will e-commerce security in e-commerce trading impact on the business for the e-commerce companies in Nepal?

1.6 Aims

The research aims to enlighten on the security challenges and security issues in e-commerce which e-commerce companies or customers might face while using e-commerce for buying and selling goods and services.

1.7 Objectives

Whenever, a customer wants to purchase something online through some e-commerce companies/websites, the first thing needed to be done is to access the internet and there seems an

increase in the growth of e-commerce use. The objective of the study is to understand if security fear or issues while using e-commerce would impact on business or utilization of the e-commerce site and as a whole impact on the buy and sell of the particular e-commerce companies.

The specific objectives of the study are outlined below:

- To find out if majority of people here prefer traditional shopping or have adopted online shopping over traditional shopping.
- To identify if the people using e-commerce are conscious and aware about e-commerce security issues.
- To determine if the security considerations and fear in e-commerce and trust of customers over the e-commerce system impact the business of a company.

1.8 Scope and significance of research

The study is all about the security issues and vulnerabilities that can be faced during online shopping by customers and e-commerce enterprises. It is not only brief explanation on those issues but this study also covers the growth of e-commerce and the impact of e-commerce security on the business.

E-commerce is booming as an unavoidable form of business with the abundancy of internet and smart devices and the ease e-commerce provides is the main cause why e-commerce is being adopted by most of the customers and companies. Nowadays, people are busy in their own work and most of the people are really busy on their own, so, they have no or very less time for shopping in the traditional way. We have seen that even the big departmental stores like Bhat-bhateni Supermarket here in Kathmandu, Nepal has already started adopting online shopping in order to maintain its status in this competitive market. However, if the customers feel threatened by security issues or somehow have fear of doing online shopping due to some security circumstances, customers will hesitate in online shopping and the business will slowly go down. In such cases, the companies must gain the trust of customers and also change the business strategy. The beneficial areas of the research are listed below: The study can assist business entrepreneurs or also existing small e-commerce companies that are operating for security of customers and company too.

- It can be helpful for the customers too as they will have insight of the weakness and gain knowledge that the company, they are involved for e-commerce is implementing required security measures.
- With this research, what customers think about security and impact on business strategy will be somehow clear to the readers.

1.9 Limitations of the study

There is no such research or study without limitations and as other researches too, this study also has certain limitations which are outlined below:

- The sample size or the participant number couldn't be large in number due to the pandemic situation and only online survey forms could be used at such times.
- It could be more effective if the survey could be conducted from all over Nepal but the participants are mostly from Kathmandu, the capital city.
- In context of Nepal, e-commerce is still growing and it doesn't seem that people here have more concerns on security issues in e-commerce, rather it seems that they are concerned on the delivery time, quality vendors, and so on.
- There are lot of studies conducted on e-commerce security or their challenges and measures but very few studies seemed to have been conducted on this subject i.e. security and how it impacts business and its policies and all are from different countries/cities.
- Some people may not still have used online shopping or some may not have interest in e-commerce/online shopping.

2 LITERATURE REVIEW

Use of e-commerce is application in enterprises for various reasons like cost reduction, reaching to greater market and also boosting the relationship between buyers and sellers. With the new way of

commerce, there is increase in new risks and threats like network attacks, identity theft, etc. This paper enlightens on the classification of threat in categories like Denial of Service, unauthorized access as well as theft and fraud and their control measures. (Revathi C, 2015) With the threat classification and identification, this paper also provides the concept of risk management framework which can be used by the e-commerce enterprises to enhance their security. Different aspects of security like privacy, availability, non-repudiation, etc. are also discussed in this paper.

Without privacy and security, customers wouldn't want to shop or visit the site of e-commerce. Here, privacy means the assurance that personal data is not tampered and security means that the data is not accessible or can't be tampered by people with unauthorized access. Thus, this paper reviews the privacy and security from various perspectives like social psychological, technical, organizational and economic perceptions. This paper has briefly explained the terms integrity, non-repudiation, authenticity, confidentiality, privacy and availability. (Ghayoumi, 2016) Identifying the security and privacy issues and making effort to resolve those issues are the vital concerns for e-commerce companies at the moment as information is vulnerable.

E-commerce can take different forms like business-to-business, business-to-customer, customer-to-customer or customer-to-business which uses network of computers like online social media networks and internet. The technology change and business change is never constant and hence a coordinated algorithm matching the requirement is always needed and also technical solutions are needed for those changing environments. This paper discusses the overview of security in e-commerce, different steps that shall be followed for placing an order in the electronic commerce various security issues in e-commerce and also provides the online shopping guidelines for security. (Sibo Prasad Patro, 2016) The life cycle of e-commerce is also discussed briefly accompanied by some security tools in e-commerce like integrity, privacy, authenticity, non-repudiation, confidentiality.

Many people and companies have adopted e-commerce and e-services now, therefore, inadequate security measures can lead to great loss to customers as well as enterprises. This paper discusses on the security risk management on the basis of a threat-driven approach for an e-commerce system Web shop in the form of case study. The approach discussed here helps for security risk management procedure which are validated by experts and is documented in an easily understandable way so that the respective stakeholders involved in the e-commerce can implement them. Some security risk metrics are too defined in this paper. (Affia, 2018) It was found in this paper that the approach was useful in e-commerce system development cycle and introducing new requirements needed as well as enhancement in the old requirements in the phase of e-commerce development.

It is true that the internet and online shopping has made customers and enterprises easy for shopping but it is also true that it has also made the organizations and people vulnerable to outside attacks. The motivation of this paper is the need of automated systems level approach and also a more intuitive approach that can be used in determining overall security characteristics of an information security system. In this paper a security framework called EAS-SGR is used which is applicable for IT governance systems, and other enterprises in order to lower the vulnerabilities of cyber security. (Hajar Iguer, 2014) This paper also discusses the vital governance concepts like vision, mission, equity, accountability, transparency, accounting and corporate responsibility.

There are always limited resources in an enterprise in every sector so is for network security protection. This paper proposes the security plan for small and medium sized businesses which is under the comprehensive budget. It also provides with the top ten affordable and free tools applicable to organizations and also provides some important practices on factors like firewall, authorization, intrusion detection and monitoring, prevention, auditing, etc. (Margie S. Todd, 2013)

3 RESEARCH DESIGN AND METHODOLOGY

3.1 Introduction

This part of the research provides some overview on how the study has been systematically designed in order to obtain reliable as well as valid results that fulfills the aims and objectives of the

research. The main focus of this section is about what and how the data is collected, from whom the data is collected and how the collected data is analyzed which will be further elaborated in the sections below. Without the proper data collection, the results of the study wouldn't be reliable and effective. Similarly, research process is also an important part which will be discussed below with the research type too.

3.2 Research Strategy

There are several other papers regarding the topic of the dissertation but there are no abundant studies conducted in the e-commerce network security and its impact in business in the context of Nepal. As China has adopted e-commerce widely, a lot of papers are found to be related to the e-commerce security in China. The papers studied have explained briefly about the security issues and also have made an effort to provide some solutions to e-commerce issues so that the e-commerce can develop rapidly and customers of e-commerce have high security over e-commerce transaction. As mentioned earlier, in the context of Nepal, the proposed research is quite new, however, but it is true that some other similar research subject also exists already.

3.3 Research Method

The research method is the procedure which guide to collect and analyze data to dig out new information or to provide more understanding about a given topic. There are several types of research method which are used for collection of data which are discussed briefly below:

Qualitative research method

This research method is used to collect data related to emotions or behaviors and the meanings attached to them by individuals and also the data about lived experiences. It helps the researchers in better understanding the concepts, cultural phenomena and social interactions that are complex. Qualitative method can assist in exploring on why and how some cases have occurred, helps in describing actions and interpreting events.

Quantitative research method

It is the kind of method that helps to gather numerical data so that results can be generated on the basis of measurement, categorization, ranking through statistical analysis. Generalizations can be made with the help of finding patters or relationships. This type of research method is helpful in finding out to what extent, how often or how much.

Below table illustrates the techniques and tools that can be used in gathering data for research.

Table 1: Research techniques and tools (QuestionPro, 2021)

| Qualitative Techniques or tools | Quantitative techniques and tools |
|---|---|
| Interviews: Interviews might be structured, semi-structured or unstructured on the basis of session between the participant/s and researcher. | Surveys/questionnaires: It is used to ask same questions to a large group of participants which is used to measure opinions as the numerical data. |
| Focus groups: are number of participants discussing in group about a particular topic or bundle of questions. | Observation: It can be count of the times that a specific phenomenon takes place or translating the observational data into numbers by coding. (Streefkerk, 2019) |
| Observations: Site visit, or working in the context or role play. | Document screening: Word occurrence counting or sourcing from financial reports the numerical data. |
| Document analysis: It means interrogating the correspondence like emails, diaries, letters, etc. or reports. | Experiments: Laboratory hypothesis testing, field experiments, etc. |

3.4 Research Approach

In this study, mixed approach is used i.e., integration of both qualitative and quantitative research methodologies. A better and deeper insight can be gained with the help of combining and analyzing statistical data. Using mixed approach, we can gain holistic approach to a problem or study and more

insight to a problem. Mixed type of research methods has been accepted in the research designs recently besides choosing purely qualitative or purely quantitative methods in a research. The integration of both these methods as a mixed method helps a researcher in various research disciplines to answer research questions with a rigorous approach. (Aramo-Immonen, 2013)

3.5 Data collection method and tools for data collection

The method used in this research is mixed approach which means that several papers from previous researchers were reviewed, several case studies of different countries were reviewed and also several conference papers were reviewed. Apart from these kind of previous papers, online survey forms were created and a number of people were distributed with the online survey forms. The objective of this research is to identify if people or specifically let's say customers consider e-commerce security as a vital factor or not and will the security of e-commerce affect the business and eventually according to the customer's perception towards e-commerce, will there be an effect on business strategy.

The main benefit of the questionnaire survey will be that it would answer if people will or won't purchase goods and services for which they have to make online transactions through online companies or websites which don't consider security as a vital part or doesn't focus much on security of information.

3.6 Sample Selection

This research is done in order to find out if e-commerce security vulnerabilities or issues would affect the business and its strategies or not. For this purpose, the customers/people who use online shopping specially Daraz online shopping are required. The sample or the participants can be anyone i.e., there is no any age bar, there is no any profession bar, there is no any other filtration in the form of the participants. It is just that the participants genuinely use e-commerce sites and it is about finding if they consider about security in e-commerce and business is affected by their perception about security in e-commerce. Hence, the sample selection is based on the non-probability sampling technique.

The sample in this research is random but has relationship with the subject of the research. The main requirement of the participants and at the same time the assumption is that, the participants use e-commerce. The sample participants are normal people like working in the office or doing some kind of jobs, students and other professions who can use online shopping applications. Most of the respondents are from Kathmandu city.

3.7 Reliability and Validity

In this study, online survey forms have been used as the data collection method. It is known to us that the e-commerce has flourished in the world mostly in developing countries, however, in countries like Nepal, it is still developing and people still prefer traditional type of shopping and e-commerce is in developing phase. Thus, the online forms were distributed to the normal people mostly above age 20 who are working and can buy using e-commerce. The respondents are supposed to be aware of e-commerce security hence, respondents who are bit knowledgeable about online shopping and can give their own opinions have been chosen.

3.8 Analysis Plan

The analysis part is very important here and the researcher here has aimed to analyze the data collected through Microsoft forms from the respondents. Several questions/statements have been created in those online form on the basis of the objective of the research in order to get the answer of the research questions. For more broad way of analysis, the researcher has created certain number of research questions for a particular objective so that valid and proper results could be obtained and interpreting and analyzing those results would give the readers a lot of good insight on the matter.

4 DATA ANALYSIS AND FINDINGS OF RESEARCH

4.1 Reliability test analysis (Cronbach's Alpha Reliability Test)

Reliability testing is done in order to find the reliability of the questions prepared and distributed to

the participants and also to determine if the questions are measuring the similar and relevant variables. In this survey, the researcher is trying to determine that people have adopted or have preferred online shopping/e-commerce or not, they are conscious and consider the security in e-commerce or not and finally determine if the security issues in e-commerce sites impact the business and business strategy or not. The output produced by the reliability test gives insight on the quality of the questions asked as survey.

In this research Cronbach’s alpha reliability test is used in which the high value of alpha indicates that the items or variables are highly correlated with each other. The range of Cronbach alpha (α) can be 0 to 1 and the highly acceptable value is taken as 0.7 to 0.8 and above. (Emerson, 2019) The general rule is that the value of alpha 0.6 – 0.7 indicates that the reliability level is acceptable, however, 0.8 or greater is considered to be a very good level. If the value of α is above 0.95 then the reliability cannot be considered necessarily good as it may indicate redundancy. (Nadaf, 2021) Here, in this research, Cronbach’s Alpha testing has been done in SPSS and the first figure below (Figure 1) depicts the case processing summary while the second figure (Figure 2) depicts the reliability statistics. Here the coefficient value obtained is .657 and according to the George and Malley rule, the value is acceptable meaning that the questions asked in the survey are acceptable.

Case Processing Summary

| | | N | % |
|-------|-----------------------|-----|-------|
| Cases | Valid | 224 | 100.0 |
| | Excluded ^a | 0 | .0 |
| | Total | 224 | 100.0 |

a. Listwise deletion based on all variables in the procedure.

Figure 1: Case Processing Summary

Reliability Statistics

| Cronbach's Alpha | Cronbach's Alpha Based on Standardized Items | N of Items |
|------------------|--|------------|
| .657 | .688 | 30 |

Figure 2: Alpha value from Cronbach's reliability test

4.2 Know about e-commerce

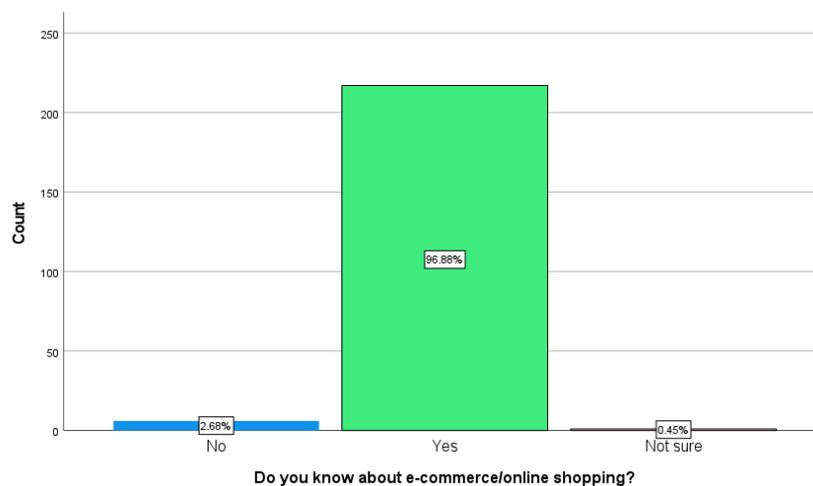


Figure 3: Customers that know about e-commerce

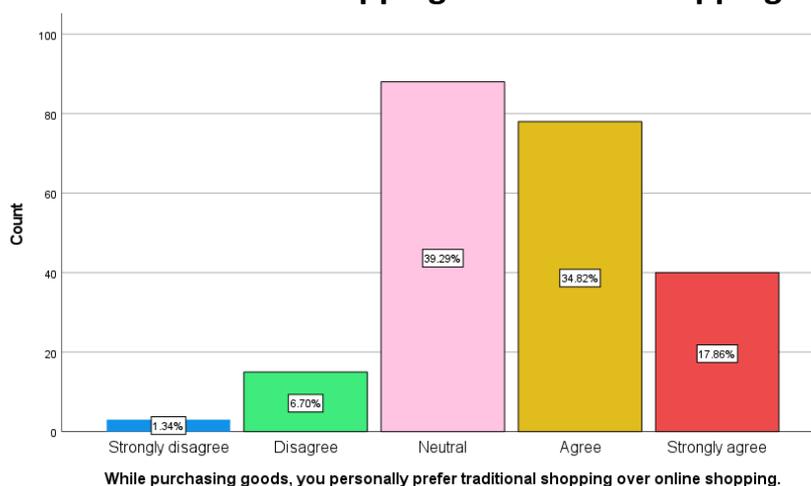
Do you know about e-commerce/online shopping?

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|-------|----------|-----------|---------|---------------|--------------------|
| Valid | No | 6 | 2.7 | 2.7 | 2.7 |
| | Yes | 217 | 96.9 | 96.9 | 99.6 |
| | Not sure | 1 | .4 | .4 | 100.0 |
| | Total | 224 | 100.0 | 100.0 | |

Figure 4: E-commerce concept tabular representation

Above question is about the concept of people about e-commerce and it is found that most of the people in Nepal know about e-commerce (96.88%) and only a few have no idea about it or not so certain about e-commerce.

4.3 Preference of traditional shopping over online shopping



While purchasing goods, you personally prefer traditional shopping over online shopping.

Figure 5: Preference of traditional shopping over online shopping

While purchasing goods, you personally prefer traditional shopping over online shopping.

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|-------|-------------------|-----------|---------|---------------|--------------------|
| Valid | Strongly disagree | 3 | 1.3 | 1.3 | 1.3 |
| | Disagree | 15 | 6.7 | 6.7 | 8.0 |
| | Neutral | 88 | 39.3 | 39.3 | 47.3 |
| | Agree | 78 | 34.8 | 34.8 | 82.1 |
| | Strongly agree | 40 | 17.9 | 17.9 | 100.0 |
| Total | | 224 | 100.0 | 100.0 | |

Figure 6: Preference of traditional shopping over online shopping tabular representation

Above section determines if people prefer online shopping or traditional shopping more and it can be said from the analysis that still more people prefer traditional shopping than online shopping. Most of the participants don't seem sure about the preference of online shopping or traditional shopping.

5 Discussion

5.1 Summary

The purpose of this research is to find out the opinion of people about e-commerce, security in e-commerce and the main purpose of the study is to find out the opinion of people on the impact of the e-commerce security issues in the e-commerce business. Also, another purpose is to identify if the business strategies shall be changed with the time and necessity in the days to come. The study was conducted in order to find what people think about the e-commerce security and its impact i.e. are people conscious about the security issues in e-commerce and will they be using the e-

commerce site/app if there is doubt in the security of the system. It is clear that if people are unwilling to use the application due to security issues then obviously the business of the company would degrade and the company must come up with new security as well as business strategies, otherwise the company will gradually vanish from this digital world where there is a lot of competition and the digital world is always growing. In the conclusion of this chapter, limitation of the research, future possible areas of the research and short summary of the research findings will be discussed.

5.2 Interpretation of findings

Having access to internet and smart devices, getting to choose a lot of e-commerce applications and sites and also having the chance to choose between a lot of goods and items in the specific e-commerce application is not enough for e-commerce. When we talk about e-commerce, it simply doesn't include buying and selling goods digitally and also includes monetary transactions, providing the information like personal, bank account number, entering passwords/PINs, entering e-sewa id and so on. Hence, such kind of interpretations about the opinions are discussed in the below section. Due to the pandemic situation while distribution stage of the survey questions, offline survey for large number of people couldn't be performed. There were only 10 offline surveys conducted and the survey questionnaires were distributed online to around 400 people. Therefore, the questionnaires were distributed to around 410 populations but the response gained was 224. A total of 214 samples were collected through online survey forms and 10 samples were collected from offline survey form. The offline survey form responses were also fed into the SPSS software for statistical analysis.

Table 2: Survey distribution and response number

| Survey type | Questionnaire distributed count | Responses received |
|----------------|---------------------------------|--------------------|
| Online survey | 390 | 214 |
| Offline survey | 15 | 10 |
| Total | 415 | 224 |

5.3 Concept of e-commerce and preference of online or traditional shopping

On the basis of the statistical analysis, from figure 7 it is clear that most of the people in Nepal know about e-commerce as 96.88% among the 224 samples knew about e-commerce analyzing the responses. A very few people are not aware about the digital shopping platform. Even if people know about e-commerce, it is not sure that the people will use e-commerce. From the analysis, figure 9, it can be seen that still most of the people prefer to shop in a traditional way i.e., the physical way than to do shopping online. It can also be concluded that most of the people have no opinion on preference to online or traditional shopping as the most respondents to this question have stayed neutral (39.29%) while responding.

5.4 Consciousness/awareness on e-commerce security

Through analysis of the data, it can be seen that most of the people are aware about the e-commerce security (Figure 13). In this research, most of the respondents are from age 20-30, this may be one of the reasons that most of them know about e-commerce security. There are very few people who have no idea about the security in e-commerce.

5.5 Impact of e-commerce security on business and business strategy

In this section, it will be determined if people will use or will be using the online commerce site if the application is secured to a trustful level and also the need of business strategy change as per the security necessities in the future. It is observed from the analysis (Figure 21) that still people are uncertain that they will use the same site once hacked or have had previous record of security breach but having claimed by the owners that the security has been improved. Around 38.39% people are not sure about using the site in the above-mentioned situation. However, it can be seen that almost 40.63 % of people are ready to use the sites if the owners ensure that they have changed

the security policies and have made their system secured. Some people (20.98%) completely disagree in using such site again in the future.

5.6 Research questions and findings of the survey

According to the results obtained from the survey and statistical analysis, the related answers/findings to the research questions are discussed below:

RQ1 As Nepal is a developing country and e-commerce has recently been evolving in Nepal, have customers here adopted e-commerce over traditional e-commerce?

Findings: The statistical analysis of the survey questions show that:

- Almost every respondent knows about e-commerce.
- However, even after knowing about e-commerce, people in Nepal still prefer traditional shopping over online shopping. Only a few numbers of people prefer online shopping than traditional one.

RQ2 Are customers aware of the e-commerce security and do customers in Nepal consider e-commerce security while performing e-commerce purchases?

Findings: The statistical analysis done for the above research question illustrates the following findings:

- It is quite impressive that most of the people know about e-commerce security and are somehow concerned on the security in e-commerce.
- Since many people know about the e-commerce security, it can be found that almost half of the people don't feel secured while providing information to the e-commerce systems like bank account details, entering transaction PINs, and other information.
- It is quite obvious from the analysis that people fear most when performing monetary transaction online like payment activities.

RQ3 Will e-commerce security in e-commerce trading impact on the business for the e-commerce companies in Nepal?

- It is observed that almost 40 percent of people are ready to use a site having previous record of security breach but claimed to have improved the security policies. Some people still don't want to use such sites ever again.
- Most of the people in Nepal are not sure if Daraz is completely secured; only some people believe Daraz to be completely secured.
- From statistical analysis, it can be observed that almost all the people seem to not use the sites that are doubtful in terms of security.

5.7 Finding from Chi-Square test

Chi-square test was performed for three cases and findings are as follows:

- There is significant relation between people being afraid of monetary transaction in e-commerce and how often will they be using the system as the alternative hypothesis is accepted (significance is $< .001$). This means if people fear monetary transaction will affect the use of online shopping.
- There is significant relation between business degradation and need of change of security policy. This means that if due to security issues if business is degrading, the e-commerce owners need to come up with new improved business strategy and security policies.

5.8 Conceptual Model for security in e-commerce (Anirban Sengupta, 2015)

Seeing the growth and adoption of e-commerce in this global world, it is clear that e-commerce is the future of commerce or trading. But with the high rate of adoption of digital commerce, the security issues are also high as attackers or hackers are everywhere just trying to find out the loophole and hack or manipulate the system. The main threat is when money is involved i.e., when payments are done. There are other threats too like information leakage which would be common in e-commerce. So, to make a good security system in e-commerce, there should be a good conceptual model.

Above figure (Figure 29), is the conceptual model that is proposed for e-commerce security. All the

e-commerce activities are either done through a website or a mobile application. Hence, security should be well maintained in the system so that the customers and owners don't fall victim to the attacks and the business doesn't lose its wealth and goodwill. As per the conceptual model, first of all, security requirements should be collected or specified. The requirements are not always same. For example, if the e-commerce is being implemented only through website, later it may be implemented through iOS and android apps too. In such cases the security requirements can change. Such requirement must be specified and documented well.

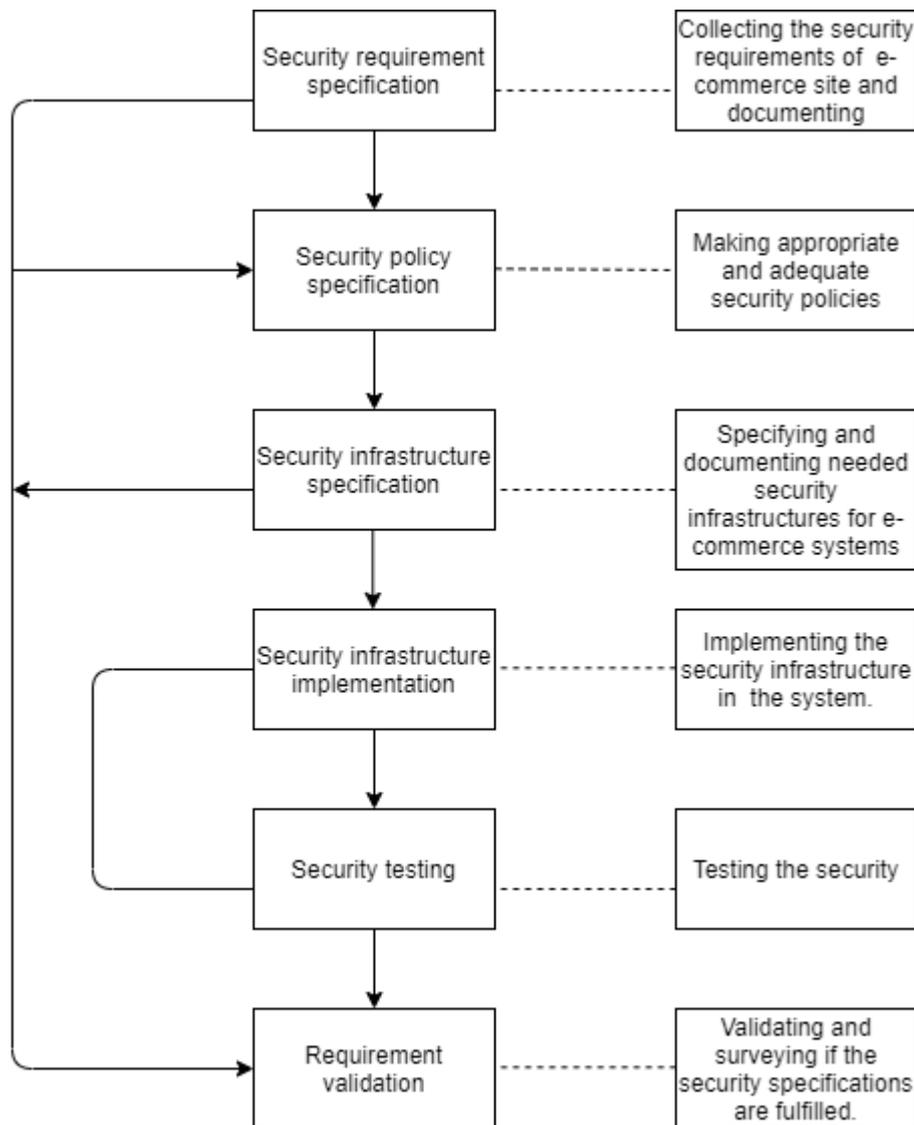


Figure 3 Conceptual model of e-commerce security

5.9 Validation of the proposed framework

The e-commerce security conceptual model proposed here were given to validate to two of the interview participants from Nepal Police and Vianet Communications Pvt. Ltd in Kathmandu, Nepal and the model has been validated by two engineers mentioned above. Good feedback for the proposed framework has been received and it can be concluded from the feedback that the conceptual model could be applicable and used in case of e-commerce security and this conceptual model can be useful for e-commerce companies existing or startups. The questionnaire for validation were addressed to Mr. Arun Kishor Sahani, System Engineer in Nepal Police Department and Mr. Tejendra Bahadur Gurung, Senior Network Engineer of Vianet Communications.

5.10 Limitations of the survey and findings

As everything in this world has limitations, this survey also has certain limitations in the survey itself and also in the findings even if this research was done following proper methods and procedures. The foremost limitation can be considered the sample size i.e., the sample size is limited with the number of only 224 participants. There could be more sample size but due to the Covid-19 pandemic situation, the sample size couldn't be as big as it could be. Also, among those participants most of the age group participating are n between 20 to 30 years of age.

6 Conclusion and Recommendation

6.1 Conclusion

With the rate of growth of e-commerce globally, it can be predicted that e-commerce will be the future of commerce. However, in the digital world, the advancement in technology accompanies with the security issues too which when not considered and planned well can result to a situation which can't be replenished. Therefore, for a successful e-commerce, the e-commerce companies must consider and plan for security and a good network security policy so as to survive in the competitive market.

As per the findings of the research, it can be derived that most of the people in Nepal know about e-commerce and also are aware about the security in e-commerce but still are using traditional shopping and very less online shopping. There are several reasons for doing so as the fear of performing online payments while using e-commerce.

6.2 Recommendation

In most of the scenarios in developing countries like Nepal, it can be seen that most of the companies are mostly focused on providing better options on goods and items and better service like delivery. However, one of the most important and unavoidable factors in e-commerce is its security. Using e-commerce can help a lot in business like it can cut the cost of physical stores or shops and many other associated infrastructures. The recommendation part is believed to be helpful for the readers, online shopping companies or entrepreneurs and even to Daraz itself. Some of the recommendations are listed below:

- Since it was observed from the analysis that still people prefer traditional shopping, if the e-commerce companies want to succeed, they have to come up with new policies and should ensure people that e-commerce is completely secured.
- The companies can use the online payment systems even if they might be quite costly than using their own payment systems as the third-party payment systems are more focused in monetary matters and would obviously be more secured.

With the focus on quality of products and services, the same level of focus on e-commerce security will prove a boon in the development of the e-commerce business. Even though this is a small study as the research contains small sample size, the researcher believes that the findings of this research will help the e-commerce owners, entrepreneurs who are thinking about starting the e-commerce business, the readers and Daraz itself.

6.3 Future work

This section contains some of the future work that can be adopted or done by the e-commerce companies in order to sustain in the competitive market.

- E-commerce companies or owners should not just focus on the quality of goods and services but equally security in e-commerce should also be focused. We have seen from the analysis that most people are aware of security in e-commerce, hence feeling of being secured while doing online shopping will be a driving factor of e-commerce success.
- One future work that e-commerce startup is that, people fear lot while doing monetary transactions in e-commerce, hence the startups can adopt the trusted third-party payment systems for online payment in the e-commerce.

References

Affia, A.-a. O., 2018. Security Risk Management of E-commerce Systems. *Thesis for: MSc*, pp. 2-72.

- Affia, A.-a. O., 2018. Security Risk Management of E-commerce Systems. *Security Risk Management of E-commerce Systems*, pp. 2-72.
- Aldrich, M., 2011. *The Michael Aldrich Archive*. [Online] Available at: http://www.aldricharchive.com/inventors_story.html [Accessed 21 January 2021].
- Alqahtani, F. H., 2017. *Developing an Information Security Policy: A Case Study Approach*. Bali, Indonesia, Elsevier B.V..
- Anirban Sengupta, C. M. M. B., 2015. e-Commerce security — A life cycle approach. *Sadhana*, 14 September, Volume 30, pp. 119-140.
- Aramo-Immonen, H., 2013. Mixed Methods Research Design. In: M. D. L. R. D. T. O. D. P. J. G. P. Rusu, ed. *Information Systems, E-learning, and Knowledge Management Research*. Mykonos, Greece: Springer-Verlag, pp. 32-43.
- Banach, Z., 2019. <https://www.netsparker.com/>. [Online] Available at: <https://www.netsparker.com/blog/web-security/session-hijacking/> [Accessed 3 January 2021].
- Carl S. Guynes, J. C. W. Y. A. W., 2011. E-Commerce/Network Security Considerations. *International Journal of Management & Information Systems (IJMIS)*, 15(2), pp. 1-7.
- Chen, X., 2017. *The application of information security technology in electronic commerce*. Chongqing, China, s.n.
- club, U. a., 2018. *UK assignment Club*. [Online] Available at: <https://www.assignmentclub.co.uk/blog/999-ethical-issues-in-e-commerce> [Accessed 28 January 2021].
- Craig A Horne, A. A. S. B. M., 2015. Organisational Information Security Strategy: Review, Discussion and Future Research. *Australasian Journal of Information Systems 21*, Volume 21.
- Dan J. Kim, D. L. F. H. R. R., 2009. TRUST AND SATISFACTION, TWO STEPPING STONES FOR SUCCESSFUL E-COMMERCE. *Information Systems Research*, 20(2), pp. 1-36.
- Dan J. Kim, D. L. F. R. R., n.d. TRUST AND SATISFACTION, TWO STEPPING STONES FOR SUCCESSFUL E-COMMERCE RELATIONSHIPS: A LONGITUDINAL EXPLORATION. *TRUST AND SATISFACTION, TWO STEPPING STONES FOR SUCCESSFUL E-COMMERCE RELATIONSHIPS: A LONGITUDINAL EXPLORATION*, pp. 1-36.
- Emerson, R. W., 2019. Cronbach's Alpha Explained. *Journal of Visual Impairment and Blindness*, 113(3), p. 1.
- Encyclopedia.com, 2021. *Encyclopedia.com*. [Online] Available at: <https://www.encyclopedia.com/books/educational-magazines/security-e-commerce-systems> [Accessed 3 January 2021].
- Fianyi, I. D., 2015. Curbing cyber-crime and Enhancing e-commerce security with Digital Forensics. *IJCSI International Journal of Computer Science Issues*, 12(6), pp. 78-85.
- Fianyi, I. D., 2015. Curbing cyber-crime and Enhancing e-commerce security with Digital Forensics. *IJCSI International Journal of Computer Science Issues*, 12(6), pp. 78-85.
- Ghayoumi, M., 2016. Review of Security and Privacy Issues in e-commerce. *Int'l Conf. e-Learning, e-Bus., EIS, and e-Gov. | EEE'16 |*, pp. 156-160.
- Haixiang Li, W. X., 2019. *Dimensions and Construction of E-commerce Network Security*. Xi'an, China, Institute of Electrical and Electronics Engineering, pp. 150-154.
- Hajar Iguer, H. M., 2014. *The Impact of Cyber Security Issues on Businesses and Governments: A Framework for Implementing a Cyber Security Plan*. Barcelona, Spain, Institute of Electrical and Electronics Engineers.
- Hamirani, E., 2020. *THE CHALLENGES FOR CYBER SECURITY IN E-COMMERCE*. Mumbai, s.n.
- Hu, J., 2017. *Research on Security Issues and Strategies of E-commerce*. Nanchang, China, s.n., pp. 570-574.

- Hu, L., 2019. E-commerce Trade Consumption Payment. *International Journal of Network Security Security and Privacy Based on Improved B2C Model*, 21(4), pp. 545-550.
- Isah, A. A., 2015. Concern for e-commerce security. *Global Journal of Computers & Technology*, 3(2), pp. 173-175.
- Ji, Q., 2018. *Study on Information Security Issues of E-Commerce*. Fuzhou City, Fujian Province, IOP Publishing Ltd.
- Jolita Greblikaite, D. P., 2014. ETHICAL ISSUES RELATED TO E-COMMERCE: CASE OF DISCOUNT E-SHOPPING SITE IN LITHUANIA. *European Integration Studies*, Issue 8, pp. 124-130.
- Kautish S, Thapliyal MP. Concept of Decision Support Systems in relation with Knowledge Management–Fundamentals, theories, frameworks and practices. *International Journal of Application or Innovation in Engineering & Management*. 2012;1(2):9.
- Kautish S, Thapliyal MP. Design of new architecture for model management systems using knowledge sharing concept. *International Journal of Computer Applications*. 2013 Jan 1;62(11).
- Kautish, S., Peng, S., & Obaid, A. J. (2021). *Computational Intelligence Techniques for Combating COVID-19 (EAI/Springer Innovations in Communication and Computing)* (1st ed. 2021 ed.). Springer.
- Kaur, H. and Kautish, S., (2016). "An Implementation of Wireless Sensor Network Using Voronoi _ PSO (Particle Swarm Optimization)", *International Journal for Research in Applied Science & Engineering Technology (IJRASET)*, Volume 4, Issue XI, November 2016, pp.361-368
- Kathryn Ormiston, M. E., 2006. *Denial-of-Service & Distributed Denial-of-Service on The Internet*. Balalaika Hotel, Sandton, South Africa, s.n.
- Kothari, B. L., 2007. *Research methodology : tools and techniques*. 18th edition ed. Jaipur, India: ABD Publishers.
- Kuldeep Kaur, D. A. P. P. K. K. K., 2015. E-Commerce Privacy and Security System. *Int. Journal of Engineering Research and Applications*, 5(5), pp. 63-74.
- Kumar, S. N., 2015. Review on Network Security and Cryptography. *International Transaction of Electrical and Computer Engineers System*, 3(1), pp. 1-11.
- Li, Y., 2016. *Research on the Network Security Management of Artwork E-commerce in New Media Context*. Yunnan Province, s.n.
- Loop54, 2019. *LOOP54*. [Online] Available at: <https://www.loop54.com/blog/top-5-security-threats-facing-e-commerce-today> [Accessed 7 2 2021].
- Mahdi Choshin, A. G., 2016. An investigation of the impact of effective factors on the success of e-commerce in small- and medium-sized companies. *Computers in Human Behaviour*, pp. 66-74.
- Margie S. Todd, S. (. M. R., 2013. *International Journal of Network Security & Its Applications (IJNSA). COMPLETE NETWORK SECURITY PROTECTION FOR SME'S WITHIN LIMITED RESOURCES*, 5(6), pp. 1-13.
- Ms. Palak Gupta, D. A. D., 2016. E-Commerce- Study of Privacy, Trust and Security from Consumer's Perspective. *International Journal of Computer Science and Mobile Computing*, 5(6), pp. 224-232.
- N. Kuruwitaarachchi, P. A. L. & S., 2019. A Systematic Review of Security in Electronic Commerce- Threats and Frameworks. *Global Journal of Computer Science and Technology: E-Network, Web & Security*, 19(1).
- Nadaf, D.-Z. A., 2021. *What is the acceptable range for Cronbach alpha test of reliability?*, s.l.: Reasearchgate.
- Nasrin ALISHIRVANI, B. M., 2016. Guaranteeing of trust and security in e-commerce by means of improved SET protocol. *Bulletin de la Société Royale des Sciences de Liège*, Volume 85, pp. 1136-1147.
- Reyana, A. and Kautish, S., 2021. Corona virus-related Disease Pandemic: A Review on Machine Learning Approaches and Treatment Trials on Diagnosed Population for Future Clinical Decision Support. *Current Medical Imaging*.
- Rani, S. and Kautish, S., 2018. Application of data mining techniques for prediction of diabetes-A review. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 3(3), pp.1996-2004.

Reyana, A., Krishnaprasath, V.T., Kautish, S., Panigrahi, R. and Shaik, M., 2020. Decision-making on the existence of soft exudates in diabetic retinopathy. *International Journal of Computer Applications in Technology*, 64(4), pp.375-381.

Rudra T., Kautish S. (2021) Impact of Covid-19 Infodemic on the Global Picture. In: Kautish S., Peng SL., Obaid A.J. (eds) *Computational Intelligence Techniques for Combating COVID-19*. EAI/Springer Innovations in Communication and Computing. Springer, Cham. https://doi.org/10.1007/978-3-030-68936-0_16

Srivastava, R., Kautish, S., & Tiwari, R. (2020). *Green Information and Communication Systems for a Sustainable Future (Green Engineering and Technology)* (1st ed.). CRC Press.

Patil, D. P., 2017. Study on E-Commerce Security Issues and Solutions. *International Journal of Computer Science and Mobile Computing*, 6(1), pp. 100-102

Wentao, C.H.U., Kuok-Tiung, L.E.E., Wei, L.U.O., Bhambri, P. and Kautish, S., 2021. Predicting the security threats of internet rumors and spread of false information based on sociological principle. *Computer Standards & Interfaces*, 73, p.103454.