J. Management and Humanity Research
Vol. 6, 2021, 19-45
ISSN: 2582-7766 *(online)*
Published on 11 October 2021
www.researchmathsci.org
DOI: http://dx.doi.org/10.22457/jmhr.v06a02132

Journal of
Management and Humanity Research

Determinants of Cybercrime and its Impact on e-Commerce Development in Bangladesh

Farjana Yeasmin [*] **and** ***Xianfeng Wu***

School of Economics and Management
Chongqing University of Posts and Telecommunications
Chongqing 400065, China.
[*]Corresponding author. Email: farjanapain@gmail.com

Received 9 September 2021; accepted 10 October 2021

Abstract. The research study aims to delve into the various external factors in the socio-cultural and political domain of Bangladesh that encourage cybercrime. These factors play a major role in shaping the psyche and perspective of offenders. The paper applies the method of survey and systematic review. The survey is conducted using the method of stratified sampling for having the best idea about the trends and perspectives of the indigenous population of Bangladesh. The systematic review in context is conducted by application of the grounded theory approach of qualitative research method. Constant comparative method with the three levels of coding procedure is used for zeroing in on the theoretical perspective regarding the answers to the research questions of this study. The intricate process in context is used for identifying the reasons leading to acts of cybercrime. Moreover, the intertwined relationship between cybercrime and the domain of e-commerce in Bangladesh gets explored. The various ways in which the domain of e-commerce is exploited by the offenders for victimizing companies or consumers is scrutinized. The thesis explores the manner in which e-commerce is being detrimentally affected by the encompassing challenges. The findings and analysis lead to the identification of key ways in which the domain of e-commerce can thrive and flourish in Bangladesh. The aspects of management, trust, awareness, and technology are explored in detail. Apart from this, other factors that are associated with the performance of e-commerce companies are also scrutinized in the course of the study. The recommendations made in the study can pave the way for successful business management of e-commerce companies and stronger economy in Bangladesh.

Keywords: Cybercrimes, e-commerce development, awareness of cybercrime, technological security solution, trust on ecommerce, cyber security management

1. Introduction

A developing country such as Bangladesh is bound to be under constant threat due to cybercrime due to its fragile technological and IT structure and lack of knowledge and knowhow for the same. Therefore, it can be ascertained that the biggest challenge being faced by e-commerce management in Bangladesh as well as around the world revolve around their promulgation and promotion. This is because research studies reveal that

customers are less likely to use e-commerce facilities and refuse the performance of online exchanges and transactions due to fear for their personal data and breach of privacy. Absence of trust is another reason for refusal of the same (Rashad Yazdanifard, Noor Al-Huda Edres, (2011). The management of e-commerce companies fail to develop trust and confidence in the consumers, which develops problems for companies and its development.

Such organizations are also under a constant challenge to battle cybercrime considering their lack of knowledge and awareness of cyber culture and cyber security. Moreover, the lack of available manpower for implementing counters-measures and develop cyber security technology adds to the issue (Malik, 2018). Often management face problems to tackle such problems due to lack of manpower or authority in their hand. Such problems contribute to increasing cybercrime and weak management in the e-commerce companies.

Moreover, since e-commerce companies are providing a greater amount of access to systems as well as individuals not directly under their control, they must ensure that they have integrated a cyber-defense developed by their management. This is a major challenge since cyber attackers are constantly growing and finding new ways of attacking and hacking systems and organizations. Another challenge for such ecommerce companies include avoiding under informed behavior and establishing holistic strategies of defense.

2. Theoretical background

2.1. Fraud triangle

In context of ascertaining the determinants of cybercrime, one should delve deep into the theoretical notion of fraud triangle. Fraud triangle can be described as a concept that explicates the causes behind committing fraudulent activities at any workplace. The theoretical concept consists of as many as three distinct elements that can be held responsible for the fraudulent activities. The three distinct elements are: Pressure, Opportunity, and Rationalization.

According to the notion of fraud triangle, a person engages in committing the fraud when the encompassing conditions for committing the fraudulent act are quite favorable to the individual. So, it is noteworthy that the fraudulent act is not a random thing in any way.

Pressure can be comprehended to be a motivation for a person who commits a fraud. The individual might be under the influence of personal financial onus or any other kind of pressure that prompts the fraudulent act. If the individual is unable to solve the pressure through legal and rational means, then the person might opt for illegal or irrational ways for addressing the problem. A person can be under the pressure of financial burden, maintenance of his lifestyle, and so on. When there is no apparent means of achieving one’s work goals or personal goals treading on the path of honesty, the person might resort to the use of dishonestly and illegality to fulfill the needs (Thakur, n.d.).

When a person is under pressure, he would look for the right opportunity to commit the fraudulent act. A person might abuse his own position, or use his knowledge to execute the fraud. In the domain of technology, committing fraudulent acts become

somewhat easier for people as they do not need to be physically present in front of the victim in any way for committing the act.

The last stage of the concept of fraud triangle is known as rationalization. At this stage, the person who is defrauding others endeavors to justify the fraudulent act in any acceptable way. It should be noted that most people who commit such frauds so not perceive themselves to be criminals. Instead, such people explicate the situation of the act and rationalize their position (Thakur, n.d.).

So, one can understand how the contextual theoretical concept of fraud triangle explores the motivations and needs of the criminals who engage in committing cybercrime. Fraud triangle sheds light on the psychological aspects that precede the act of cybercrime. It is important to understand the psyche and perspective of the criminals to delve deeper into the determinants that lead to such criminal acts on the internet.

2.2. Organized criminal groups

There is apprehension that organized crime groups might also be involved in cybercrime in various developing nations of the world. For comprehending operations of organized criminal groups, one should consider them akin to rational economic players who have an aim of maximization of profit. The profit of such organized criminal groups depends on the capacity of emulating market mechanisms. The said emulation might need formulating strategic alliances and making proper decisions about capital investment. Moreover, it might also involve identification of areas of new growth or adopting new systems. The organized criminal groups engage in considering certain factors while taking any decision about geographical location of the fraudulent activities (Monsma et al., 2013).

The organized criminal groups are specifically influenced to take location decision on the basis of the strength of that place's rule of law. Any individual's decision to take part in any kind of criminal activity is related to the probability of being caught by the law enforcing authorities and convicted for the illegal act. So, an individual's inclination toward crime can be enhanced due to laxity or shortcoming in the rule of law. In case of a country like Bangladesh, the weak rule of law in context of cybercrime and permissive regulations create a fertile ambiance for such criminal activities by individuals. One should note that in an economic domain like that of Bangladesh, the level of readiness of regulatory institutions to curb cybercrime is not at par with the regulatory authorities in developed nations like the United States or United Kingdom.

In fact, the scenario is not unique to the country of Bangladesh. Many other developing nations have the same problem. Many Asian and African countries were late in adopting the latest developments in technology. These countries were late in integrating such technology in their administrative functions as well. Over the years, many developing economies of the world have taken measures to enact law for dealing with cybercrime within their territories. However, such laws lack proper enforcement. The developing economies lack enforcement mechanisms of such laws. So, one can comprehend that the lack of strong mechanism of implementing law against cybercrime is one of the primary determinants that encourage such criminal activities (Al-Dosari, 2020). In context of Bangladesh, one can comprehend the fact that the country does not have a strong legislation that could curb cybercrime effectively. Further exploration of

the legislations related to such acts of criminality can create a better notion about the status quo of law enforcement in Bangladesh.

2.3. Bangladesh and law against cybercrime

With the evolution of digital economy across the entire world, the urgency of ensuring digital security has enhanced by a substantial degree. Globalization has further enhanced the speed of this evolution of digital economy. Under the circumstance, various governments are left to face complicated cyber-security threats. Such threats have the capacity to substantially damage a country's infrastructure and economic growth. The scenario is most complicated for countries in Asia where expansion of internet has heightened in the midst of internet revolution. The countries in this region are inclined toward leveraging the various benefits of the nouveau digital economy. These countries want to preserve their national security at the same time in this post-internet globe. Hence, many countries in Asia have adopted policies that can be described as protectionist in characteristic. It should be remembered in context of this discussion that Bangladesh's neighbors have developed strong legislations for dealing with the threat of cybercrime within their sovereign territories. India has also developed separate police stations for investigating cases of cybercrimes within its territory. Moreover, many policies that are adopted by certain nations of the region are not totally aligned with international parameters. One can comprehend that such environments that do not align themselves with international standards of protection and stringent action become the best possible places for engaging in cybercrimes. The individuals engaging in such criminal endeavors see the environments as comparatively easier for such actions.

One should take into reckoning the fact that Bangladesh goes on to lead the entire globe in share of mobile malware infection. Other counties in the Indian sub-continent like Nepal and Sri Lanka have also experienced a significant rise in instances of cyber-security threats or attacks. The trend makes it conspicuous that this region is seen as a safer place for committing such crimes. The government of Bangladesh has recognized the threat posed by cybercriminals in the country. The recognition of the encompassing threat in the era of digital economy and digitization has led to enactment of legislation in the country that aims to curb the contextual problem. The Digital Security Act, 2018, has come into existence in Bangladesh for dealing with the threat of cybercrimes. The act aims to address the heightened concerns about digital security. However, it should be noted that the legislation is location within this larger Information Technology regulatory ecosystem (Singh, 2020).

2.4. Education about technology

Some years back Bangladesh went on to recognize the massive scope of development in the sector of Information Technology. The massive growth of the neighboring nations like India, Sri Lanka, Singapore, Malaysia, and Singapore prompted the government of Bangladesh to heighten its efforts of educating the youth with technological knowledge. Various academic programs went on to be adopted by the public educational institutions and the private educational institutions to disseminate knowledge of technology and computers among thousands of youngsters. Various recommendations of the JAG commission report went on to be implemented by the government across the entire nation of Bangladesh.

It is the primary aim of Bangladesh government to emerge as one of the key software exporting nations in the region within a short span of time. The utmost efforts of the educational system to imbibe technological knowledge among the students are meant to fulfill the contextual aim of the government. The educational institutions have significantly enhanced the number of students who can pursue such academic degrees. More students are getting enrolled in Computer Science programs across Bangladesh over the last few years. Various educational institutions have set up proper educational infrastructure for enriching the students with substantial knowledge in the domain of study.

However, it is imperative to reckon that proportional enhancement in employment opportunities should be there in the national economy. The students who are getting educated in the domain of knowledge would immediately seek proper employment after they complete their academic program in colleges or universities. There should be ample scope for such students in the domain of work. The economic condition of the nation might become an occlusion in the path of success for such educated youth if they do not find proper employment in the country.

One can understand that these educated individuals can possibly get lured by the prospects of earning easy money through cybercrime. These individuals are properly educated in the field of work, and they have the scope of employing their skills for malpractices. The acts of criminality in the cyber world require using technological knowledge on the part of all the offenders. Bangladesh government has recognized the need for developing its human capital by disseminating knowledge of technology through academic programs. However, the government should also have a vision and mission of using the contextual human capital in constructive manner. Channelizing the youth properly would lead to economic development of the nation. The educated youth should have ample opportunities of finding good employment. These efforts by the government can work as deterrents to cybercrime in Bangladesh.

3. Research hypotheses

3.1. Hypotheses

Hypothesis 1: There are certain external socio-economic factors that function as positive catalyst to the growth of cybercrimes across Bangladesh in the contemporary era.

While the literature survey has already identified certain key aspects that have the potential to play a pivotal role in ascertaining the scope of executing cybercrimes, there is need to further test the validity of this hypothesis. The hypothesis' correctness can lead to further exploration of the extent of impact exuded by such socio-economic factors across Bangladesh. The specific causes that affect the domain of criminality in Bangladesh can involve dynamics that are left unexplored in a generalized scrutiny. Testing this hypothesis is a primary requirement of the research study. The research study ought to involve the best possible methodology of research that can help in advancing toward the deciphering the latent aspects.

Hypothesis 2: The acts of cybercrime in Bangladesh can detrimentally affect the domain of e-commerce by waning sales and discouraging further addition of businesses across the field.

The second hypothesis of this research study postulates the notion that the commission of cybercrimes in Bangladesh can affect the e-commerce businesses in a

substantial manner. The hypothesis uses the commission of cybercrimes as an independent variable, while the business of e-commerce is the dependent variable in this context. The literature review of this research study has already shed light on the manner in which cybercrimes can complicate business in any country. In context of Bangladesh, the scenario becomes all the more complicated owing to certain factors. It is imperative to check this hypothesis on the basis of further data and interpretation. The accuracy of this hypothesis is closely intertwined with the soul of the research topic of this study. Its level of accuracy would provide strength to the holistic argument presented in the study. Moreover, it would pave the way for finding interventions.

Hypothesis 3: The application of certain key interventional methods can substantially lessen the scope of commission of cybercrimes in the domain of e-commerce in Bangladesh, thereby catapulting the performance of businesses and transaction between consumers and companies.

The third hypothesis of this research study postulates the notion that there are various ways in which the threat of cybercrimes in Bangladesh's e-commerce business can be mitigated. As such, the interventional methods are the independent variables on which the variable of e-commerce business' performance is dependent. The contextual study aims to identify the methods of intervention that can be initiated by the companies or businesses across Bangladesh for safeguarding themselves from cybercriminals. The correct methodology of research can pave the way for zeroing in on the most effective interventional acts in businesses. The interventions can strengthen the relationship between the companies and the consumers. Moreover, these interventions can also encourage the potential consumers to engage in e-commerce devoid of any apprehensions about safety and security on such platforms.

3.2. Conceptual basis for comprehension and analysis

It is the purpose of a theoretical framework of a research study to shed light on the conceptual basis for comprehension and analysis. The framework explores the design of ways in which the intertwined relationships among variables can be explored. A theoretical framework should pave the way for the best research methodology that can help in identification of the certain aspects.

New research data needs to be interpreted as well as coded for subsequent usage. New problems that have no previously ascertained solutions should be strategically solved. The solutions to the identified research problem should be properly evaluated. The most important facts / information should be distinguished from other data. Old / existing data or information should be given new meaning and new interpretation. Significant new issues can be identified and the comprehension of such issues should be maximized. People from the professional domain should be provided with a frame of reference that can help in their profession. Further research can be guided and informed for improvement of professional practice.

For the fulfillment of the above-mentioned purposes the contextual research work would use the grounded theory approach of qualitative research method to conduct a systematic review. The subsequent sections of the chapter would discuss the intricacies of the method of research. The next sections also discuss in detail about the modus operandi of grounded theory approach and survey that are applied in the case of this research study.

4. Research design and findings

4.1 Sample Description

The survey was conducted on 120 respondents from Bangladesh. The questionnaire was shared online. The respondents sent the questionnaire back with their replies. The subsequent analysis of the information collected via this survey has shed light on intricacies of the research area. The present research work aims to identify the determinants of cybercrime. Also, the effects of cybercrime on Bangladesh's e-commerce need to be ascertained. When it comes to the question of survey, the respondents were chosen from the general public. So, it can be presupposed that none of the respondents are experts in the field of technology. It was the primary aim of the survey to gauge the perspective and notion of the general public regarding cybercrime and threats in the domain of e-commerce. The findings could be associated with the identified aspects from the systematic review of the scholarly sources that is conducted using the constant comparative method of grounded theory approach.

Among the 120 respondents, 60 people were males, while the rest were females. The respondents were further stratified on the basis of age. The sample was created on the basis of three age groups: 18-30 years, 31-40 years, 41 and above. The contextual stratifications were made to ascertain the holistic picture of the larger population of Bangladesh. Half the respondents were chosen from the city of Dhaka, the capital of Bangladesh. The rest of the respondents were from certain suburban areas of the country. This distinction was made to ensure that the survey represented both the urban and suburban masses. It is imperative to have an inclusive mindset toward people of the suburbs as they also engage in e-commerce transactions. The questionnaire that was used for the survey is attached in the appendix section of the research work. The findings and analysis are discussed in detail in the subsequent sections for treading toward a concrete theoretical model of comprehension.

4.2. Statistical description

The respondents were asked if they have a substantial idea about cybercrime. 82 per cent of the respondents opined that they have a good idea about cybercrime. When they were asked if they have heard about certain terms like malware, spyware, key-logger, etc. only 37 percent people responded with a positive answer. These two initial questions of the survey clearly expose how maximum people in Bangladesh have little understanding of the intricate aspects of cybercrime. It is shocking to note that most of the people think that they have a good idea about cybercrime. This gap between belief of having knowledge and reality of lacking comprehension further complicates the scenario in the country. It is understandable that the lack of proper understanding helps cybercriminals in executing their fraudulent activities in the domain of e-commerce.

The respondents were further asked if they had trust in all the e-commerce platforms of Bangladesh. However, just 68 per cent of the total respondents opined that they trust the e-commerce platforms in the country. A large section of the respondents opined that there are trust issues when it comes to the question of e-commerce platforms of Bangladesh. 32 per cent of the respondents' opinion reflects the larger issue of lack of trust in e-commerce business in Bangladesh. The finding needs to be attributed utmost significance as it reflects the larger perspective of people living in the country. If there is

lack of trust among potential consumers across the society, the entire domain of e-commerce would be detrimentally affected in the times ahead.

The respondents were then asked if they know anyone personally who has faced fraudulent activity while engaging in e-commerce. 18 per cent of the respondents opined that they are personally aware of people who have become victims of e-commerce fraud in the past. In goes beyond saying that the findings shed light on the complicated scenario in Bangladesh where incidents of cybercrime have enhanced significantly. Directly knowing people who have become victims of such cybercrimes creates a negative impression about the entire domain of business in context. The status quo ought to have a negative effect on business, if not controlled properly.

The respondents were also asked if they feel that there should be stronger laws for curbing cybercrime in Bangladesh. 78 per cent of the total number of respondents of this survey said that Bangladesh needs stronger laws to deal with the issue of cybercrime in the country. The significantly high number of respondents in favor of stronger laws shows that most people feel that the present legislations need alteration. There is scope of bringing further developments to satiate the needs of rule of law in Bangladesh. It is comprehensible that the domain of cybercrimes is transforming itself rapidly. The criminals who engage in such activities update themselves with the latest technology. So, the laws should also be periodically updated to curb the illegal activities of these criminals.

The respondents were asked if they feel entirely safe while sharing their banking details at the time of shopping online. 65 per cent of the total respondents of this survey said that they feel safe while sharing their banking details online during e-commerce. The figure shows that a lot needs to be done for reposing people's faith on the e-commerce platforms of Bangladesh. People would refrain from buying things online, if there are concerns about their safety. Online payments would be avoided by the consumers. In such a scenario, cases of tax evasions can increase significantly in the domain of e-commerce. The exchequer of the government of Bangladesh would also be negatively affected in such a scenario.

Finally, the respondents of the survey were asked if there is need of conducting awareness campaigns across Bangladesh for heightening the knowledge of people about cybercrimes. 88 per cent of the respondents said that it would be a good idea to start awareness campaigns in Bangladesh educating the civilians about the risks posed by cybercrimes today. So, one can understand that majority of people want planned campaigns regarding the contextual issue. It would prove to be helpful in controlling cases of frauds. People with proper awareness would refrain from engaging in dubious transactions. It is the prerogative of the government and major e-commerce companies to come forward for heightening people's awareness about the matter.

The questions of the survey have endeavored to gauge certain aspects associated with cybercrime and e-commerce in Bangladesh. The perspective of people about the issues can help the research study in gauging the intricate dynamics at play in the socio-economic domain of Bangladesh in the contemporary times. The survey clearly indicates that there is need to heighten people's awareness about cyber threats in Bangladesh. Both the government and the e-commerce companies should do their best to raise people's awareness about the matter. Prevention by the companies and the consumers can be a major step toward minimizing cases of cybercrimes in the domain of e-commerce.

4.3. Hollow diffusion as a determinant of cybercrime in Bangladesh

One should gauge the conceptual perspective of 'hollow diffusion' of the internet across Bangladesh. Comprehending the scenario of 'hollow diffusion' of the internet can pave the way for delving deeper into the dynamics of cybercrime and e-commerce in Bangladesh. It goes beyond saying that the e-commerce technology that is used by various firms in the country of Bangladesh is characterized by quite weak defense mechanism. It is the prerogative of the companies engaging in e-commerce to adopt highest possible parameters of safety and security in business.

The fundamental notion behind the concept of 'hollow diffusion' is quite simple. It is understandable that many nations are adopting e-commerce in developing nations of the world. Bangladesh is identified as a country with low average income. Under the circumstance, the country has to make all efforts to strength its economy. E-commerce is seen as a viable means to supplement the country's economy. However, the companies that engage in e-commerce in such an environment are not inclined toward spending on human resources and technological advancements. Such expenses can lead to lesser profit margins for the companies. So, the fundamental requirements for e-commerce are generally satiated by the companies in such environments. Such companies also undermine expenditure for various other basic ingredients that are required for long-term success. In spite of engaging in e-commerce with utmost interest, such companies can be comprehended to lack real depth of adopting the internet (Kshetri, 2010).

This lack of expertise or resource creates a major impediment for growth of the business as well as the consumers of the company. 'Hollow diffusion' might occur due to lack of experience and skills. The companies that engage in e-commerce might feel it is not necessary to hone to skills of the employees regarding the use of technological platforms. Providing training for the existing employees of a company might not be cost-effective. In addition to this, employing new individuals to work on technological aspects might also be avoided by such a company. In such a scenario, the company would obviously remain less equipped in technological prowess while conducting e-commerce. The company would only function with fundamental aspects of e-commerce being satiated. The safety and security of the platform would remain at stake.

'Hollow diffusion' is also applicable in case of consumers in Bangladesh. As mentioned earlier, Bangladesh is on the path of achieving economic betterment using its resources and human capital. However, a lot needs to be done to empower the entire population. The literacy level of the country is not at par with developed nations or other developing nations of the region. Under the circumstance, it is quite difficult for the government or other bodies to catapult people's awareness about the best way to use e-commerce platforms. So, the consumers or users also remain less accustomed to the encompassing threats. They are exposed to the malice and manipulation of cybercriminals who use this opportunity for their own benefit.

So, one can understand that the issue of lack of experience and skills of the businesses and the consumers in the domain of e-commerce has created a positive scenario for fraudulent activities on the internet. Cybercriminals who have ample knowledge about the intricate aspects of e-commerce can bypass the security measures of companies and manipulate the consumers. 'Hollow diffusion' is caused in the country of Bangladesh owing to the sudden growth of technological devices and dissemination of the internet. The holistic scenario of education and awareness are not favorable for skilled

use of technology. People who have lesser exposure to technological knowledge and education would only develop fundamental skills to operate e-commerce platforms. They would be able to execute fundamental activities, while remaining ignorant of security issues on the internet.

Apart from this, 'hollow diffusion' can also happen due to technological aspects. A business or an individual might fail to use available security products or practices properly. In case of organizations, the scenario can get complicated when they integrate internet technologies before taking into consideration the efforts and costs required for maintaining the systems. If the company fails to reckon the need of the costs and efforts, it would obviously lead to substantially negative externality. In case of consumers in Bangladesh, the access to internet is mostly via cell phones. Many people do not understand the basic concepts of privacy and security while using the internet. Thus, usage of the internet is often conducted without firewalls or anti-virus / anti-malware / anti-spyware software installed on the technological devices. The scenario heightens the vulnerability of the consumers. Cybercriminals take advantage of the situation and engage in malicious activities using the models of e-commerce.

So, it is evident that 'hollow diffusion' is one of the primary aspects that problematize the domain of e-commerce in Bangladesh. The scenario of 'hollow diffusion' goes on to impact Bangladesh and other similar socio-economic environments across the world. Such a mode of diffusion of the internet and e-commerce can occur at a rapid pace across a community or society. However, it is difficult to educate the masses about the encompassing threats and security issues at such a pace. Hence, it is imperative to take into reckoning the need to spread awareness about the issues. Heightened awareness about security issues is a necessary requirement for diffusion of the internet and e-commerce in any socio-economic environment. The pace of diffusion of the internet cannot be slowed down owing to various factors. The rapid pace of diffusion is necessary for fulfilling the aim of digitization. Moreover, rapid digitization and diffusion of the internet can enable Bangladesh to come at par with other neighboring nations of the Indian sub-continent.

4.4. Trust in e-commerce sector

One cannot deny that the sector of e-commerce has seen substantial growth over the last few years. However, potential impediments that can thwart the development of this sector should be recognized. Challenges like unavailability of high-speed internet, net neutrality, logistical issues, and quality assurance of products can pose hindrance to the growth of this sector. The chances of foreign players dominating the domestic market also poses risk to indigenous start-ups in Bangladesh. The shortcomings in transportation system also functions as an obstacle for e-commerce trade's expansion across Bangladesh. There are certain challenges in the sector of logistics as well. Under the circumstance, a large portion of e-commerce trade occurs within the capital and a few other regions. The infrastructural problems and inability of accessing remote locations impedes e-commerce. One can imagine how the detrimental effect of cybercrime can further complicate the scenario. In spite of the previously mentioned obstacles, the e-commerce companies are endeavoring to expand their trade. But, cybercriminals can simply break the relationship of trust between the companies and their consumers. Fraudulent acts in the domain of e-commerce can make people deter from online shopping in the times ahead. The advent of

mobile payment gateways has eased the process of payment during online shopping. A large section of the consumers opt for online payments prior to the delivery of their ordered products.

Lack of trust in the payment system would surely have a negative impact on the growth of the e-commerce sector in Bangladesh. Most customers would opt for cash-on-delivery method of payment, if they become apprehensive about their banking data being stolen or goods not being delivered. The previous sections of the research study have already shed light on the manner in which cybercriminals can misuse the payment gateway for stealing sensitive data of the consumers. The previous discussions have also highlighted the manner in which cybercriminals create fake e-commerce platforms for executing fraud. In such fraudulent platforms, the consumers pay for the chosen product that they wish to obtain. But, the product never reaches the consumers. Thus, they lose their money due to the online payment for the perceived delivery of the chosen products.

The contextual scenario has the possibility of discouraging the general public from opting for online payment or using digital wallet while buying things online. Owing to the apprehension of being defrauded, many customers can opt for cash-on-delivery means of payment for the products that they buy online from various e-commerce platforms. However, while cash-on-delivery mode of payment can lead to considerable safety and security of the consumers, it has certain negative effects for the economy of Bangladesh. COD paves the way for the chances of tax evasion. The mode of payment also leads to substantial lack of transparency in monetary transactions (Saban et al., 2002).

So, it is significant to recognize the ill-effects of lack of trust in the domain of e-commerce. The consumers would only be more inclined toward opting for COD means of payment if they do not trust the platforms or the payment systems. The findings of the survey conducted during the course of this research study shed light on the lack of trust that characterizes consumer behavior. The absence of safe and reliable payment system in case of e-commerce creates the contextual problem. The banking system of Bangladesh should take immediate cognizance of the matter. The needed changes and developments should be made for facilitating safe and secure payment gateways. The focus should be on winning back the trust of the general public.

The responsibility of winning back people's trust does not solely lie on the shoulders of the government. The companies that engage in e-commerce should give the required efforts to create an ambiance of utmost safety and security for the consumers. The previous section of the research study has discussed about the lack of resources on the part of the businesses when it comes to the question of technological advancements and security. Such shortcomings should be addressed with heightened importance. The companies should have up-to-date technological systems so that the back-end operation of the e-commerce platforms has no flaw or scope of security breach. On the other hand, the companies in context should also develop their manpower so that the employees have ample technological knowledge to safeguard the operations from cyber threats. Human capital has a substantial role to pay in mitigating the threat of cybercrime in e-commerce.

One should also reckon the fact that the number of debit and credit card users in Bangladesh is lower in comparison to other developing or developed nations. Under the circumstance, many customers are unable to engage in online payments. The mentioned aspect can further complicate the situation, if not handled properly. If the ambiance of apprehension of cybercrime prevails, when new consumers would obtain debit or credit

cards, they might refrain from online transactions. Such a scenario would lead to heightened tax evasions and lack of transparency. So, the government should ensure that the e-wallet system is developed properly. The e-wallet system can effectively undermine the problem in context to certain extent. One should reckon that bKash has come to partner with various e-commerce ventures in Bangladesh. If banks of the country engage in such partnerships, it would be beneficial for e-commerce. Moreover, it can mitigate the threat of online frauds to a substantial degree.

The e-commerce sector in Bangladesh is still in the process of emergence. The industry is on the path of gaining steady pace of growth. The level of competitiveness in this sector is also increasing with time. E-commerce can boost Bangladesh's economy, if the challenges to the sector are addressed effectively. Being a developing nation, Bangladesh should utilize the opportunity for growth with utmost impetus. There are many local e-commerce businesses that are in the regional market from the start of the industry. Such companies should be supported and given protection. The government should take the necessary steps so that such companies can thrive in the contemporary scenario.

In addition to the local companies, foreign investments should also be welcomed in the e-commerce sector. Foreign investments would not come to Bangladesh if security threats and cybercrime continue to thwart the growth of e-commerce. The authorities should ensure that the payment procedures of various e-commerce platforms are more secure. Heightened security would win the trust of the general public. Also, the foreign companies would be encouraged to enter the market. The trust of people and foreign investments can also be won by arranging for high-speed and low cost internet connections in the extensive rural region of Bangladesh.

The trust of the consumers can also be won by focusing on consumers' rights. The government should scrutinize the role of regulatory authority in the e-commerce sector. Such a regulatory authority can play an active role in protecting the customers from frauds by taking the required steps. Nurturing people's trust in e-commerce can help in realizing the true potential of the sector in Bangladesh. Within the next decade, e-commerce can emerge as the most powerful industry across the nation. E-commerce can also contribute substantially to Bangladesh's GDP in the times ahead. Recognizing the real potential of e-commerce sector, the government needs to come forward and support the sector to corroborate its initiative of creating Digital Bangladesh.

In the subsequent section, the closely associated relationship between an e-commerce company's management and the element of trust would be explored. The actions of the management have key roles to play in shaping the notion of the consumers or potential consumers. So, the management should consider actions that would catapult the trust and nurture the relationship between the company and its consumers.

4.5. Strategies to be adopted by management as interventions

The companies engaging in e-commerce should understand that the aspects of safety and security in the domain of e-commerce are directly related to the image and position of the businesses. The management of every business engaging in e-commerce should play a proactive role in mitigating the threats. The growth of a business is not just ascertained in term of the company's sales. The growth can also be ascertained in terms of the intricacy of managing the business. In case of e-commerce business, the management should have

the mindset to reach a level where it can ascertain and set up specialized responsibilities and functions.

Table 1: Steps to be taken by management

Measures	***Requirements***
1. Marketing	PPC or SEO
2. Technology	Help of experts, Leveraging social media proof, etc.
3. Positive Reviews	Urging customers for positive reviews, subsequent display of the same
4. Efficient Admin Panel	Using helpful UI, all-inclusive admin panel
5. Checkout Process	Enable ease of customers during checkout
6. Customer Support	Having human representatives, using chat-bots

It is significant to note in the context of this discussion the different legs that characterize the foundation of any e-commerce business. Since the domain of e-commerce in Bangladesh is characterized by utmost competition, all legs of the business need to be strong. Apart from ensuring proper production of goods, the management of an e-commerce business should pay utmost importance to marketing. In a scenario where cybercrime threatens the credibility and influence of e-commerce, marketing can be an effective and necessary tool to mitigate the apprehensions among the potential consumers. A business can adopt certain approaches for marketing about itself. The management has the scope of opting for PPC or pay-per-click ad. Such a form of marketing would require focusing on PPC spends. The potential consumers would come to notice the details about the e-commerce platforms as the surf the internet. Higher visibility and consistency of advertisement would portray the business as a credible one to the potential consumers. Apart from PPC advertisements, a company's management can focus on SEO or search engine optimization for reaching out to the potential buyers. The company can, thus, focus on building links. SEO would pave the way for higher visibility of the e-commerce platform on the internet. Such a practice would create a positive perception about the company among the potential consumers.

It should be reckoned that the fraudulent sites or platforms would not engage in extensive advertisement on the internet. Such extensive advertisement about a fraudulent platform for e-commerce can gather significant attention from the law enforcers. Subsequently, the individuals running such platforms might come under scrutiny of the law enforcing agency. While cybercriminals can engage in some amount of online canvassing for gaining the attention of potential buyers, they would generally refrain from consistent advertisements or marketing.

So, it is best for the management of any e-commerce company aiming to conduct proper business to engage in consistent marketing activities. Such consistency in marketing would also build the image of the company among the consumers. Building the image of the e-commerce company would make people believe in the propriety of the services or products provided by the business. With time, the image of the company

would attract more customers to buy products or seek services from the e-commerce platform.

Apart from this, technology is one of the principal aspects of any e-commerce business. So, the management of any e-commerce business should ensure that the company remains on top of technology under any circumstance. The management should take the help of experts while making the decisions about domain name, hosting, and the software of shopping cart. Moreover, utmost importance should be given to the implementation of security measures. The management should understand that there is no scope of any breach of data. Any sort of breach of privacy would lead to a crisis situation for the company. A situation of crisis would harm the overall image of the business. In an ambiance where substantial apprehension already prevails about the propriety of services provided by e-commerce platforms, such a situation can be harmful for the future prospects of such a business. The company's management should constantly evaluate various new technologies which get introduced. After gauging the usage and effectiveness of new technologies, the management should optimize the e-commerce platform with latest updates and security measures.

The management of the e-commerce companies should engage in leveraging social proof. It should be reckoned that display of reviews from other customers who are satisfied with the service can substantially impact the visitors of the e-commerce platform. The visitors would trust the e-commerce platform with ease on reading positive reviews from past customers. Such reviews can talk about the impressive experience of customer service or product quality. The consumers can also review about the timely arrival of their ordered products or any other positive experience of shopping from the e-commerce platform. These reviews effectively serve as proof of the credibility and worthiness of the e-commerce business. Such reviews can be described as approval from individuals who have interacted with the company. The social proof tells other potential customers about the quality and reliability of the products / services offered by the e-commerce business. So, the management should aim to encourage its customers to provide positive reviews about the company's products or services. These reviews should be properly displayed on the site or other platform that is visited by shoppers.

It is imperative for the management to have a well-organized and intuitive admin panel for running a successful e-commerce business. It goes beyond saying that an e-commerce business would have a lot of tasks that cannot be completed without the effectiveness of the admin panel. An effective admin panel would allow the manager of the store of company to access all details and manage all the orders. Moreover, the admin panel would also enable the control over details of payments, shipping, and inventory. Having all the required data in a singular dashboard can help the management focus on the intricacies of the business with considerable ease. Also, such a situation would enable the management to focus on issues of security and safety as other tasks would be executed in an organized manner.

One should reckon that managers of online stores spend a lot of time on various mundane tasks. They have to spend time in even filling out various sorts of forms. Such workload can be substantially lessened by having a properly connected backend for the business. The management can opt to have an effective admin panel by using a helpful UI admin panel. Such an admin panel should be able to handle and manage the modus operandi of the business. The management can substantially reduce the handling time of

orders in this manner. Moreover, it would also enhance the timeliness of deliveries. If the overall operations of the e-commerce business are conducted smoothly, the management would get the scope of scrutinizing further scope of development or advancement. If the other operations of the business are perfect, the management would obviously want to heighten the image of the company. Under such a circumstance, the focus would shift to enhancing the safety and security of the technological aspects.

The management of any e-commerce platform should comprehend the utmost significance of the checkout process for the consumers. The checkout process should be characterized by ease of use and credible indicators. The management should take all the required measures to streamline the e-commerce platform's checkout process. The platform should ideally refrain from asking for any kind of extra or unnecessary information. Such a process would heighten the trust and appeal of the e-commerce platform. In addition to this, the management should plan to add a progress bar during the checkout process that can help the customers.

Also, various payment options can be offered by the company. A number of payment options would allow the customers to pay for the chosen products as per their convenience. Moreover, various kinds of payment methods would enhance the trustworthiness of the company. The management of the e-commerce platforms should endeavor to accommodate as many payment options as possible. It should be noted in this context that fraudulent portals or sites would want to obtain money from the potential consumers at the time of checkout. They might not allow COD on the platform. However, a credible platform can have both the prepaid and post-delivery payment options. The options can make the consumers have more trust. The consumers can opt for prepaid orders under such a circumstance, feeling confident about the transaction and platform.

All through the process of checkout, the e-commerce platform should display ample trust signals to the consumers. The management of any e-commerce platform should always remember that the consumers are supposed to provide certain sensitive information to the e-commerce company for shopping. Hence, such consumers would require the utmost assurance from the company regarding the safety and security of the sensitive data that is shared. The management can decide to display trust badges during the checkout process. In this manner, the e-commerce platform can encourage the customers to provide their debit or credit card details and purchase the chosen items (Khurana, 2019).

The management of any company should consider the scope of provide proper customer support on the e-commerce platform. Customer support can prove to be a principal brand differentiator. In an ambiance where e-commerce is being threatened by cybercrime, providing proper customer support can have many benefits for the e-commerce companies. In case of e-commerce platforms, the consumers have the scope of making a purchase beyond the regular business hours. A consumer can even buy a product during holidays. So, it is best for any company to have 24/7 customer support. Having a 24/7 customer support would also enhance the credibility of an e-commerce platform. Such a feature would place it on a different platform from fraudulent sites that are functional in the same business environment.

Now, one might be apprehensive about the cost-effectiveness of the measure as a company would need to hire additional representatives for the purpose who would work in different shifts. However, the management of a company can opt for the cost-effective

technological alternative of having a conversational chat-bot that can satiate the needs of the customers during non-conventional hours of the day or during holidays. The algorithms of such a chat-bot can streamline the decision-making procedure of the consumers when they are engaged in shopping on the e-commerce platform (Khurana, 2019).

Nonetheless, the management should understand that the mentioned strategy would only work if the company uses it correctly. In spite of the fact that chat-bots have become very popular in the contemporary times, the company should not solely depend on it for customer support on the e-commerce platform. The chat-bot should be implemented carefully. Also, the management should keenly monitor the feedback of the audience or consumers. The management should comprehend that chat-bots are not sophisticated enough to address complicated queries. Such chat-bots cannot engage in critical thinking in any way. So, it is imperative to have customer support representatives who can address critical aspects of customer service on the e-commerce platform. These chat-bots can be used for improving customer service of an e-commerce business and boost the credibility of the platform. Thus, the negative perception of the potential consumers can be substantially neutralized using this mechanism.

The principal roles that such chat-bots can play should be reckoned by the company's management. Such chat-bots can help the platform's visitors in finding the right products. As such, the bots can save the time of shoppers as they surf through the website or platform. Moreover, such bots can identify the interests and preferences of the visitors. They can make recommendations about products or services. One of the most effective uses of chat-bots is the handling of transactions on the e-commerce platform. It is already conspicuous that the customers can be negatively impacted if the checkout process is complicated. The potential consumers can abandon the shopping cart if the find the process of checkout complicated or untrustworthy in any way. The management of a company should consider the fact that transactional chat-bots have the capacity to speed up the process. Such chat-bots can accept payments and allow the consumers to execute transactions without getting them redirected to various pages. While such a modus operandi would minimize the complications of payment, it would also enhance the credibility and trustworthiness of an e-commerce platform.

So, a chat-bot can surely be a helpful addition to a company's strategy of customer support. It can work in unison with human representatives to catapult the trustworthiness of the company. It can be a positive addition to an impressive e-commerce management plan. The online store can run without much hassle owing to such a strategy.

4.6. Required security measures

In addition to the mentioned managerial aspects, certain security measures should be adopted by all e-commerce companies for minimizing or eradicating the possibility of cybercrime. The specific requirements that should be satiated are represented in the table.

Table 2: Steps to be taken for Security of E-commerce platforms

Steps	***Comments***
Promoting strong password usage	Urgent, does not require extra expense
Using HTTPS	Very urgent, requires expense
Choosing a secure platform for e-commerce	Very urgent, requires expense
Refraining from storing sensitive user data	Urgent, does not require extra expense
Employing personal website monitor	Urgent, requires expense
Maintenance of a security-focused perspective	Urgent

It should be reckoned that passwords are facing competition from contemporary technologies like MFA (multifactor authentication) and facial recognition. Nonetheless, passwords remain the standard access key for a large number of software. One needs to use passwords for all the services or websites that are logged onto. Under the circumstance, using one password for accessing more than one service might seem to be quite convenient. However, this approach is problematic and unsafe. If hackers are able to access reused passwords or usernames, they can use the data for other services. Such a scenario can lead to widespread fraudulent acts.

One needs to note that even if the e-commerce platform or site has strong security, the customers can prove to the weakest link. Humans are often found to have weak credential hygiene. As such, there remains a high possibility that the same credentials would get used at a number of sites. Also, there remains a high possibility of one of security of one of those sites being breached. People can use a number of password managers that allow them not to remember a number of passwords for various services and websites. However, when it comes to the question of managing e-commerce websites, the managers should use complex passwords and 2FA (two-factor authentication) from customers and users. The contextual practice can ensure that customers / users do not rehash certain potentially compromised login credentials. Moreover, the practice makes sure that the real users are requesting to access the platform. If the management of an e-commerce company is truly inclined toward managing the authentication technology of the organization in a holistic manner, then it should utilize the efficacy of identity management systems. Such an identity management system can properly manage the contextual function across several software and services.

If an e-commerce company wants to use passwords, the company should use the format of the password having a certain minimum number of characters. The password should also use symbols and numbers mandatorily. The management should also ponder about forcing the consumers to change the passwords on a regular basis. Thus, having stronger passwords on the e-commerce website can potentially thwart cybercriminals from breaching the privacy and security of the platform using their technological skills.

Usage of HTTPS is of the most significant aspects of enhancing security of an e-commerce website. Hypertext Transfer Protocol Secure can be described as the protocol for securing communications that are executed over the virtual world of the internet. Using HTTPS is surely one of the best ways in which the management can secure the e-commerce website from any fraudulent activity. The use of HTTPS is designated by the icon of closed green lock on the address bar of the browser. Such a website is deemed to

be authentic and safe owing to the certification. The certification makes it clear that the contextual website truly is what it claims to be. It is not any counterfeit website that is placed on the virtual world for defrauding consumers. Although such counterfeit websites can engage in accessing sensitive data of the consumers in fraudulent manner, certified sites are totally safe.

For the purpose of enabling HTTPS, businesses need to have SSL (Secure Socket Layer) certificate from the competent authority. The receipt of this mentioned certificate is just the first step. After this, the layer should be implemented properly in the e-commerce solution. One should take into reckoning the fact that using HTTPS has various advantages apart from the enhancement of trustworthiness and security. The management of e-commerce companies should comprehend that search engines like Google provide better search ranking to HTTPS sites. As such, these sites have higher number of visitors. On the other hand, the contextual search engine goes on to label unencrypted sites as “not secure.” Such sites come across to be unsafe to the visitors. So, it is not hard to comprehend that using HTTPS can potentially aid the entire business of an e-commerce company by ensuring security and attracting more customers on the portal. It goes beyond saying that a number of online shoppers can avoid using an e-commerce website that might be insecure or lacks HTTPS designation (Enigbokan, & Ajayi, 2017).

Nonetheless, the management of e-commerce companies should reckon that it is quite challenging for existing sites without such certification to add the contextual feature. Such a situation might arise if the feature was not built in during the creation of the platform. The businesses that are in the process of planning their online shopping sites from scratch can plan to design the platform with HTTPS designation. Existing e-commerce businesses in Bangladesh should understand that it is best for them to initiate migration to HTTPS certified platforms for sales and services (Sevilla, 2019).

It is imperative for the management of an e-commerce company to opt for a secure platform for e-commerce. It should be noted that e-commerce platforms get picked by the consumers for their convenience, products, and functionality. However, security features should be attributed utmost importance for development of such platforms. The management of an e-commerce company should search for well-known e-commerce solutions. Such e-commerce solutions should be able to provide SSL certificates, payment gateways with encryption, and substantial authentication protocols.

The e-commerce companies in Bangladesh should engage in exploring the utility of cloud-based security platforms. Such security platforms have made security easily accessible to smaller companies. These tools can provide benefits of stronger automaton to an e-commerce company. A company can be help by the positives of machine learning via such platforms. So, a company can explore any cloud-based security platform with in-built intelligence. The management of an e-commerce company should focus on the aspect of long-term viability. Moreover, the management should consider that security patches and updates are added by such security platforms for ensuring long-term security to any company. Under such a circumstance, the e-commerce company can expect to remain entirely safe from hackers or fraudsters owing to the heightened security provided by the security platform. The management should envisage the future requirements of the company and take such constructive steps for sustenance and expansion of the company (Sevilla, 2019).

No e-commerce company should engage in storing the users' sensitive data. Not storing sensitive user data can substantially enhance the safety of the platform. The privacy and personal data of the company's customers have omnipotent significant. A consumer would only wish to engage in transaction with an e-commerce company if one feels that such sensitive data is entirely safe. In case of the domain of e-commerce in Bangladesh, a consumer would obviously be more critical in approach regarding such an issue. The status quo of cybercrime in the contextual domain comprehensibly makes people apprehensive while using e-commerce platforms.

However, such companies require the data of the customers for improving the product offerings and communications. Such data also helps the companies in ensuring return purchases. The management should reckon that cyber-attacks, hacking, or phishing target the contextual user data that might be saved by a company. So, it is essential for the company to collect only that information that can be useful for fulfilling the process of transaction between the company and the consumer. As such, e-commerce businesses need to avoid the inclination toward collecting more data about its customers than the minimum necessary details. Such a practice would ensure that sensitive data is not left vulnerable in any way. Hackers or other cybercriminals would not be able to misuse any data under such a circumstance.

So, personal and financial information of the consumers should be safeguarded to curb cybercrimes in e-commerce. The contextual rule should apply in cases of credit card information of the consumers. The e-commerce company does not require storing credit card details on its online server. If no sensitive data is saved on the server of an e-commerce company, hackers and cybercriminals cannot steal any sensitive detail. The management of the company should ensure that a safe storage repository is used for storing any data online. Such a repository should adhere to the best practices of safety and security. The repository should have regular audits, strong access controls, and encryption of data (Rahman, 2017).

Apart from this, the management of an e-commerce company should engage in employing its personal website monitor. Most of the hosting services of e-commerce websites have a sort of monitoring tool that is helpful for the customers. However, the management of such a company should explore the scope of using monitoring tools of third-party website. The management should explore such options as they can provide better management features. Such features can make the e-commerce website more reliable and secure for everyone.

The e-commerce website can run with heightened smoothness as the management can use its dashboard and engage in health monitoring of application. Moreover, the management can also use the feature of performance benchmarking. The management can effectively monitor the features from any place utilizing the option of mobile clients provided by such tools. So, the company should always explore the possibility of using advanced features. Code-level analysis of root cause and audit trial for modifications of features are actions that the management can explore for zeroing in on security issues in a timely manner. Such practices can keep the platform of business and data much more secure (Dod, n.d.).

Lastly, the management of any e-commerce platform should be driven by a security-focused perspective. One should understand that e-commerce security cannot be maintained by a one-time investment in any way. Hacking methodologies and threats to

security have the capacity to evolve at a fast pace. So, the management should have proper awareness about cyber security and developments in nature of cybercrimes. The company should be driven by a focused mindset that aims to ensure holistic security of data without any lapses. Ensuring prevention is the best possible way ahead for any company when it comes to cyber security. If the security of any e-commerce company is compromised, it can be quite late for controlling the damage. The damage control measures are often unsuccessful in addressing the crisis situation effectively (Dod, n.d.).

The management should reckon the negative effect on customer experience in case of any security breach. The scenario might lead to wane in the company's business and credibility. In case of Bangladesh, the domain of e-commerce is already under ample threat from cybercriminals. Any instance of security breach can largely damage an e-commerce company's image and reputation across the entire country. Such a company might fail to regain its position in Bangladesh. Moreover, the actions required to rectify things after any security breach would incur heavy costs for the e-commerce company (7 important ecommerce website security measures you should have in place, n.d.).

So, it is comprehensible that all e-commerce businesses in Bangladesh should focus on security measures and authentication with maximum effort. The management of the e-commerce companies should endeavor the best to give paramount importance to customer experience. The companies should take all the necessary steps to mitigate the encompassing threats of cybercrime in Bangladesh. The managements of the e-commerce companies have the key to the ultimate success of such ventures. The people involved with the management should understand the latent issues and dynamics of e-commerce and cybercrime in Bangladesh. Thus, they can implement the best measures through new additions to the modus operandi of their companies. Budgetary considerations should be made by the managements of e-commerce companies for executing the steps. The discussed steps would enable the companies to recover their expenses within a short span of time. The loyalty of customers for such companies would lead to a long-term benefit.

4.7. Formation of a model

The findings of the research study have led to the formation of a model which can simplistically explain the ongoing dynamics in Bangladesh's e-commerce business in the midst of the looming threat of cybercrime. The principal elements of the proposed model can be identified including elements of positive catalysts, environment, act(s), and negative catalysts.

Positive catalysts can be described as the determinants of cybercrime in context of Bangladesh. In a developing nation like Bangladesh, the determinants that are identified in the previous sections of the study play a major role in channelizing an individual toward illegality. The encompassing socio-economic and cultural aspects that are identified as determinants of cybercrime encourage a person to resort to the path of wrongful acts. Being influenced by one or many of the determinants, a person who has ample knowledge about technology engages in such criminal activities. Cybercrime requires special skills on the part of the offenders. However, the psyche and perspective of such offenders can be identified to be akin to the ones who engage in other sorts of criminal activities. Thus, such people who engage in cybercrime are in search of the most beneficial environment for executing their fraudulent activities. In context of this study, the domain of e-commerce in Bangladesh provides a safe environment for the

cybercriminals. The domain of e-commerce in the contextual country is still in the process of growth. The growth rate of e-commerce and the associated aspects are not at par with the scenario in developed economies of the world. The ongoing process of development provides the cybercriminals with best scope of exploring avenues for executing frauds.

4.8. The balance of the model's elements and efforts representing the interconnection among elements

The environment in the contextual model can be defined as the domain of e-commerce business that is created by all the types of transactions between two parties. The various modes of transactions and business between the two parties are discussed in detail in the previous sections of the study. Depending on the dynamics, any person engaging in cybercrime in e-commerce identifies the best zone of the environment where fraudulent activities can be conducted without much hassle or risk. The criminals are often driven by the scope of success in the environment. They explore the loopholes of the environment that can actively facilitate their criminal acts.

The acts by such cybercriminals constitute one of the major elements of the model. The acts can potentially harm the financial security of civilians who use e-commerce websites or platforms for shopping. Moreover, companies can also be defrauded by certain cybercriminals. The acts can take a number of forms as per the plan and convenience of the criminals. It is imperative for the victims to identify the acts. The patterns used by the criminals in context should be identified by the law enforcers as well. The acts have the scope of defrauding many victims at a time. As such, acts of cybercrime in the domain of e-commerce can grow at an exponential rate. The act of crime might not be identified immediately. If the identification process takes substantial time, it would obviously become more challenging to catch the criminals. The offenders are highly trained in technological work. They are properly equipped to remove any electronic evidence of their criminal acts.

4.9. Model representing the impact of catalysts on e-commerce in Bangladesh

Hence, it is important to understand the potential of negative catalysts in the context of such cybercriminal acts in e-commerce business. Bangladesh's e-commerce companies and government should take immediate cognizance of the possible deterrents to cybercrime in the domain of e-commerce. The previous sections of the research study have discussed in detail the aspects that should be attributed utmost importance in combatting against cybercrimes in e-commerce. There are four principal deterrents that constitute the element of negative catalyst in the contextual model. These elements are awareness, trust, technology, and management. These aspects are most important in creating an ambiance where execution of cybercrime would become difficult.

So, it is imperative to enhance the influence of the negative catalysts in the domain. The enhancement of the negative catalysts is directly proportional to the fall in number of cases of cybercrimes in the domain of e-commerce. The aim of the government and e-commerce companies should be to strengthen the mentioned factors in the near future. The deterrents in context closely involve the consumers in Bangladesh. The consumers would be left vulnerable in case of less impact of negative catalysts in the domain. On the other hand, the enhancement of positive catalysts to cybercrime can lead to enhancement in such acts of criminality. So, the best possible scenario is to neutralize all the positive

catalysts to cybercrime in Bangladesh. If a systematic approach can eradicate the positive catalysts in the times ahead, it would be considerably easier to control cybercrime. Here, it is significant to note the intertwined relationship that exists within the contextual elements of the model. The simplistic representation via the model portrays the elements and their relationship with clarity. The direction of influence exerted by the represented elements on another element of the model also becomes conspicuous by referring to the relationships or causality.

5. Recommendations and conclusion

5.1. Conclusion

The research study has delved into the factors that determine acts of cybercrime. The focus of this research study is on Bangladesh. The determinants of cybercrime in context of the country are explored in detail. The research study has identified the psyche and perspective of cybercriminals using the theoretical perspective of fraud triangle. The existence and development of cybercrime in developing nations is explored to zero in on the specific determinants associated with Bangladesh's cybercrime. The actions and motivations of organized criminal groups are explicated for developing a clear perspective about the modus operandi adopted by cybercriminals across Bangladesh. What complicates the scenario of cybercrime in Bangladesh is the lack of stringent legislations that can deal with the issue of cybercrime. Cybercrime can evolve at a fast pace, and the country's legislations should have utmost efficacy in identifying and dealing with criminal activities on the internet. Bangladesh's need of coming up with stringent regulations should be recognized. The lack of legal provisions to punish cybercrime further functions as a major determinant of such activities.

Moreover, Bangladesh's population is not properly knowledgeable in the domain of cyber security and cybercrime. The country lags behind in general awareness about ways to mitigate such security threats. The lack of awareness among civilians encourages cybercriminals to engage in fraudulent acts as the victims do not have proper idea about identifying and avoiding such acts. In addition to this, the thousands of youth who are properly educated in technology are unable to find appealing employment opportunities after finishing their academic programs. The economic weakness of the nation pushes such youth to engage in illegal activities using their technological prowess. The youth in context are influenced by the scope of earning easy money by defrauding others on the internet. The mentioned factors function as the principal determinants of cybercrime in Bangladesh.

The research study has further explored the dynamics of the e-commerce sector. The specific issues related to e-commerce in Bangladesh were also discussed in detail. The challenges and opportunities that characterize the domain of e-commerce in Bangladesh were discussed. The discussion has engaged in delving deep into the manner in which e-commerce sector is affected by the encompassing threat of cybercrime. The incidents of cybercrime and the apprehension of being victimized by such criminal acts have significantly occluded the growth and development of e-commerce sector in the country.

The subsequent development of a model simplistically portrays the intertwined relationships among various key factors associated with cybercrimes in Bangladesh and the domain of e-commerce. The model is developed for the purpose of representing the intricate findings of the research study in a fundamental form. The fundamental

representation indicates the manner in which cybercrimes can be controlled in Bangladesh. Moreover, the counteractive measures for undermining the risk of cybercrimes in the domain of e-commerce are represented. Treading on the path of executing the counteractive strategy would bring a positive development in the domain. The e-commerce businesses in Bangladesh would be able to flourish, in spite of the encompassing challenges. The customers would also be safeguarded effectively owing to the mentioned practices.

5.2. Recommendations into policy suggestions

In view of the findings and analysis of the intricate aspects associated with cybercrime and e-commerce in Bangladesh, certain steps are necessary to mitigate the problems. It goes beyond saying that having legislation for Consumer Protection is one of the most important aspects that should be addressed in the future. In context of Bangladesh's e-commerce business, building the trust of consumers is truly important. The status quo of cybercrime in the domain of e-commerce has created apprehensions among the potential consumers. If such apprehensions continue to develop in the minds of potential consumers across Bangladesh, the entire domain of e-commerce might get detrimentally impacted over the course of time.

The authorities should think about exploring the possibility of developing a mechanism of holding fund in the 'E-Payment' section of the bank account of the merchant. This development can bring heightened transparency or clarity in financial transactions that occur online. Apart from this, consumers should use their true identification so that they can complete the transaction online. The steps should be implemented by regulations ascertained by the government. It is the responsibility of the government of Bangladesh to search for ways in which frauds in e-commerce can be neutralized.

It is significant to ensure the privacy of the communication by the consumer. Moreover, the visit information and preferences of the consumers should also be kept safe. The financial and personal data of the consumers should be maintained by the merchant with utmost effectiveness. A conspicuous definition should be developed about the form of intention / promise and communication between the consumer and the merchant that would be seen as a valid service agreement. The government should shed light on the contextual aspect. The existing lacuna should be neutralized with immediacy. The government and other authorities should ensure that the violation of the service agreement can lead to substantial legal consequences in the nation's justice system.

Having strong legislations can work as deterrents to cybercrime in the domain of e-commerce. In addition to having strong legislations, it is significant to have effective regulatory authorities and law enforcing agencies across the entire nation. After establishing stronger legislations, the executive bodies of Bangladesh should be properly trained and encouraged to cognize the incidents of fraud or other cybercrimes on the internet. The cognizance and subsequent action of the law enforcers should be at par with their activeness in other cases of illegality. The enforcers of law should understand the primary importance to taking immediate steps against any incident of cybercrime. Cybercrime has the scope of monumental enhancement across the entire nation, if the law enforcers show any kind of shortcoming in dealing with the scenario.

Bangladesh should understand the need to establish policy that propagates community consciousness with utmost speed and efficacy. The consciousness of the community can bring a sea of change in the domain of e-commerce and the looming threat of cybercrime. It is comprehensible that the socio-economic dynamics differ from one nation to another. As such, various expectations from the consumers and the businesses should be in congruity to the existing standards. The research study has already shed light on the lack of awareness among general consumers about the threats of cybercrime while engaging in e-commerce transactions or buying.

Effective awareness campaigns can be undertaken by the government of Bangladesh through dissemination of public service announcements. The various mediums of mass communication can be used for spreading awareness. Television, radio, newspapers, and billboards are examples of popular traditional mediums of mass communication. The mentioned mediums can be used by the government to spread the messages about consumer protection and safety issues during e-commerce dealings. People would surely come across such messages if they are disseminated properly in the said platforms. Subsequently, they would become more aware and informed about the intricacies associated with e-commerce. Their heightened awareness and knowledge would help to curb cybercrime in e-commerce dealings.

Apart from this, the government and other regulatory bodies need to ascertain the code of conduct for the companies engaging in e-commerce and the consumers. No form of communication conducted via the digital platforms should violate traditional business and social etiquette in the domain of e-commerce business across Bangladesh. The two parties in the deal should always aim to uphold the propriety of practice. For heightening the trust of the general public, the mechanism of dispute resolution should be conspicuous to all the stakeholders.

The government of Bangladesh should consider the scope of establishing cyber police stations in the districts of the nation. Moreover, the personnel who would work in those police stations should know how to handle the cases of cybercrime with utmost effectiveness. The mechanism of reporting incidents of cybercrime should be made easier. If the process of reporting crimes is made easier, more people who are defrauded by cybercriminals would be able to come forward and report their problems. The government should ponder about the scope of allowing civilians to report such crimes on an official application or website that is regulated by the law enforcing agency in context. Also, it is necessary to empower the judiciary to deal with such cases of cybercrime in a timely manner. Considering the number of pending cases in the judicial system of Bangladesh, the government should think about setting up cyber courts across the country. Such cyber courts should deal exclusively with such cases of cybercrime. In such a scenario, the criminals who engage in offenses related to e-commerce can be brought to justice after due investigation by the law enforcers. The trail would be conducted in a speedy manner in such courts. The consumers or victims of such cybercrime would also become more inclined toward reporting further incidents if they witness the heightened effectiveness of the country's judiciary in the contextual matter. The punishments for cybercrime should be sufficiently harsh. Harsh punishments can surely work as deterrents of crime. If the legislations make way for stringent actions on the offenders, many such criminals might opt to refrain from such acts. They would apprehend strict actions by the law enforcing authorities against them.

The public service announcements should also warn about the stringent rules and regulations related to propriety of action on the domain of e-commerce. The public messages would heighten the apprehension of the cybercriminals about the risks of committing such criminal acts. Their awareness about the strict procedure of law and the subsequent punishment for their crimes can make them abstain from such acts in the future. In such a scenario, the problem would get mitigated to a certain degree across Bangladesh.

So, it is comprehensible that unison of legislation, regulations, law enforcement, judicial trial, and awareness can pave the way for a better environment for the businesses and the general public engaging in e-commerce. The government and other agencies should reckon the fact that the cyber world is evolving at a rapid pace. Hence, it is imperative to revise the legislations on a periodic basis taking into context the changes in the cybercrime and modus operandi of cybercrime. The government should set up an expert committee that would review the existing laws. The committee should engage in ascertaining the required changes in the law after an interval of every six months or a year.

It is already clear that most operations in the domain of e-commerce involve a number of digital activities. In addition to the digital activities, certain conventional processes of business are also followed in such deals on the internet. The legislations should ensure that the parties to the deal or transaction are in compliance with the e-commerce regulations. It is understandable that e-commerce paves the way for easy access to the market or the consumers. However, certain regulations should be imposed eventually for all the new entrants into the domain of e-commerce. Such regulations should be meant to authenticate and identify the bodies. Moreover, such regulations should also make the process of monitoring and taxation easier than before. It should be primary aim of the government and law enforcing agencies to bring every action by a business or a consumer within the boundaries of legality and accountability.

The government should also consider the scope of introducing insurance policies. The formulation of such insurance policies would be aimed at protecting the consumers and the businesses from fraudulent incidents and larger accidents. If such insurance policies are introduced, both the consumers and the businesses would gain substantial confidence. Such a scenario would work as a positive catalyst to the development of e-commerce across Bangladesh. Rapid development of e-commerce would have a positive effect on the overall economy of the nation.

5.3. Limitation

It is significant to comprehend the limitation of this research study so that the research findings can be placed in context. Understanding the limitations is also important to interpret the validity of this research work. It would also help in ascertaining the level of credibility of the research work's conclusions. In context of this research work on determinants of cybercrime and its impact on e-commerce development in Bangladesh, the research design has used systematic review as well as survey method to find and interpret data. One can opine that the sample size chosen for the research work functions as a limitation of the study. There is always scope of heightening the number of respondents for further delving into the psyche and perspective of people. However, time constraints or other barriers generally impede the process of involving more respondents

in the sample of a research work. In addition to the sample size chosen for this study, one can also identify the lack of previous research studies on the contextual topic to be a limitation. While ample work is there to determine the determinants of cybercrime in general, the context of Bangladesh has not faced much exploration in the past. Nonetheless, the research work has proceeded with utmost commitment and accuracy, in spite of the encompassing challenges that are identified as the study's limitations.

REFERENCES

1. Madhuri Thakur, Fraud Triangle. [Online] (n.d.). Available: https://www.wallstreetmojo.com/fraud-triangle/
2. E. Monsma, V. Buskens, M. Soudijn, and P. Nieuwbeerta, Partners in Cybercrime. In Hsu D. & Marinucci D. (Eds.), *Advances in Cyber Security: Technology, Operations, and Experiences* (pp. 146-170) (2013). NEW YORK: Fordham University Press.
3. Khalifa Nasser K A. Al-Dosari, Cybercrime: theoretical determinants, criminal policies, prevention & control mechanisms, *International Journal of Technology and Systems, 5* (1) (2020) 34-63.
4. Vijayant Singh, Bangladesh: Introduction to digital security laws in Bangladesh. [Online] (2020). Available: https://www.mondaq.com/security/880248/introduction-to-digital-security-laws-in-bangladesh
5. N. Kshetri, Diffusion and effects of cybercrime in developing economies, *Third World Quarterly, 31*(7) (2010) 1057 – 1079.
6. K. Saban, E. McGivern, and J. Saykiewicz, A critical look at the impact of cybercrime on consumer internet behavior, *Journal of Marketing Theory and Practice*, 10(2) (2002) 29-37.
7. Ajeet Khurana, The secret to effectively managing an ecommerce business, [Online] (2019). Available: https://www.thebalancesmb.com/the-secret-to-effectively-managing-an-ecommerce-business-1141726.
8. O. Enigbokan and N. Ajayi, Managing cybercrimes through the implementation of security measures, *Journal of Information Warfare*, 16(1) (2017) 112-129.
9. Gadjo Sevilla, How to secure your e-commerce website: 6 basic steps, [Online] (2019). Available: https://www.pcmag.com/news/how-to-secure-your-e-commerce-website-6-basic-steps
10. Md. Raziur Rahman, Prevention of cyber crimes in Bangladesh, *Society & Change*, 11 (4) (2017) 7-18.
11. Ronald Dod, 10 ways to improve your ecommerce store's security, [Online] (n.d.). Available: https://www.chetu.com/blogs/retail/10-ways-to-improve-ecommerce-security.php
12. 7 important ecommerce website security measures you should have in place, [Online] (n.d.). Available: https://www.infisecure.com/blogs/ecommerce-website-security-measures.
13. J. Bandler, Cybercrime and fraud prevention for your home, office, and clients, *GPSolo*, 34(5) (2017) 58-61.
14. J. Bellasio, E. Silfversten, E. Leverett, A. Knack, F. Quimbre, E. Blondes, . . . G. Paoli, (Rep.), RAND Corporation. (2020).

15. BG. Glaser and AL Strauss, *The Discovery of Grounded Theory: Strategies for Qualitative Research*. New York: Aldine De Gruyter (1967).
16. B. Glaser, The constant comparative method of qualitative analysis, *Social Problems*, 12(4) (1965) 436-445.
17. M. Hathaway, Falling prey to cybercrime: implications for business and the economy, In Nye J. & Scowcroft B. (Authors) & Burns N. & Price J. (Eds.), *Securing Cyberspace: A New Domain for National Security* (2012) pp. 145-158. Aspen Institute.
18. J. Heyink and T. Tymstra, The function of qualitative research, *Social Indicators Research*, 29(3) (1993) 291-305.
19. International telecommunications union, global cybersecurity index & cyberwellness profiles, 2015. [Online] (2015). Available: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf.
20. Introduction to digital security laws in Nepal, Sri Lanka, and Bangladesh, [Online] (2019, Aug.). Available: https://www.ikigailaw.com/introduction-to-digital-security-laws-in-nepal-sri-lanka-andbangladesh/?utm_source=Mondaq&utm_medium= syndication &utm_campaign=LinkedIn-integration#acceptLicense
21. Z. Jamil, Global fight against cybercrime: undoing the paralysis. *Georgetown Journal of International Affairs*, (2012) 109-120.
22. Sunera Saba Khan, E-commerce in Bangladesh: Where are we headed? [Online] (2020). Available: https://thefinancialexpress.com.bd/views/views/e-commerce-in-bangladesh-where-are-we-headed-1578666791
23. J. Lusthaus, *Cybercrime in Southeast Asia: Combating a global threat locally* (pp. 08-10, Rep.) (2020). Australian Strategic Policy Institute.
24. A. Peters and A. Jordan, (Rep.). Third Way. (2019).
25. S. Reeves, M. Albert, A. Kuper, and B. Hodges, Qualitative research: why use theories in qualitative research? *BMJ: British Medical Journal*, 337(7670) (2008) 631-634.
26. K. Saban, E. McGivern and J. Saykiewicz, A critical look at the impact of cybercrime on consumer internet behavior, *Journal of Marketing Theory and Practice*, 10(2) (2002) 29-37.
27. Vijayant Singh, Bangladesh: Introduction to digital security laws in Bangladesh. [Online] (2020). Available: https://www.mondaq.com/security/880248/introduction-to-digital-security-laws-in-bangladesh
28. A. Strauss and J. Corbin, *Basics of Qualitative Research: Grounded Theory Procedures and Techniques*. Newbury Park, CA: Sage Publications (1990).
29. World Economic Forum, The Global Information Technology Report 2016. [Online] (2016). Available: http://www3.weforum.org/docs/GITR2016/WEF_GITR_Full_Report.pdf.