

E-Commerce and Cyber Vulnerabilities in Bangladesh: A Policy Paper

Muhammad Tanbirul Islam^{*1}, Md. Fokhrul Islam², Juairiya Sawda²

^{1,2,3}(Dhaka University, Nilkhet Rd, Dhaka 1000, Bangladesh)

*tanbirul@txstate.edu

Received: 2022-October-22

Rev. Req: 2022-November-10

Accepted: 2022-December-16



10.59683/ijls.v1i3.24

How to cite this paper: Islam, M. T., Islam, Md. F., & Sawda, J. (2022). E-commerce and Cyber Vulnerabilities in Bangladesh: A Policy Paper. *International Journal of Law and Society (IJLS)*, 1(3), 186-203. <https://doi.org/10.59683/ijls.v1i3.24>

This is an Open Access article distributed under the terms of the Creative Commons Attribution 4.0 International license (<https://creativecommons.org/licenses/by/4.0/>)

ABSTRACT: *The e-commerce growth scenario is forging a new dynamism in business and does not offer time-bound, cost-effective and hassle-free buying and selling. Following the changing approach, security management in e-commerce (cyber security) is now a focus. This research is a qualitative research that uses a case study method to analyze risks and vulnerabilities in the field. People in Bangladesh are primarily unaware of the risks related to using computing and digital devices and online platforms. This article articulates the risk factors associated with the growing reliance on digital technologies and devices. Then, some policy guidelines are prescribed for the national level and individual level, including leading social campaigns, new chapters in the school curriculum, advancing technological aptitudes of law enforcers, strengthening security systems in e-commerce, embanking sites, bringing frauds to justice, initiating law to define cybercrimes, fortifying institutional management of cyber securities.*

Skenario pertumbuhan e-niaga menempa dinamika baru dalam bisnis dan tidak menawarkan pembelian dan penjualan yang terikat waktu, hemat biaya, dan bebas kerumitan. Mengikuti pendekatan yang berubah, manajemen keamanan dalam e-commerce (cyber security) kini menjadi fokus. Penelitian ini merupakan penelitian kualitatif yang menggunakan metode studi kasus untuk menganalisis risiko dan kerentanan di lapangan. Orang-orang di Bangladesh sebagian besar tidak menyadari risiko yang terkait dengan penggunaan komputasi dan perangkat digital serta platform online. Artikel ini mengartikulasikan faktor risiko yang terkait dengan meningkatnya ketergantungan pada teknologi dan perangkat digital. Kemudian, beberapa pedoman kebijakan ditentukan untuk tingkat nasional dan tingkat individu, termasuk memimpin kampanye sosial, bab baru dalam kurikulum sekolah, memajukan kemampuan teknologi penegak hukum, memperkuat sistem keamanan dalam e-commerce, situs tanggul, membawa penipuan ke pengadilan, memprakarsai undang-undang untuk

mendefinisikan kejahatan dunia maya, memperkuat manajemen kelembagaan sekuritas dunia maya.

Keywords: *Cyber Vulnerabilities, E-commerce, Cyber Security.*

I. INTRODUCTION

As computing devices and communication technologies were developed and become more cost-efficient, online shopping or exchanging products or services over the internet is becoming more common. It has much room for growth. E-commerce is growing due to its accessibility, similar to the user-friendly benefits. Online retailers are no longer bound by conventional store hours. From small businesses to major corporations, e-commerce creates new windows of business opportunity. Today, many businesses choose to host their operations on the internet to enter a new market that they could not easily reach through their sales force or advertisement campaigns.

However, when e-commerce is overgrowing, cyber security risks or cybercrime become visible in the e-commerce area. The potential for failure or damage to an organization's information or communications systems is known as cyber danger or cyber security risk. Any company may be exposed to cyber risk from within the organization (internal risk) or third parties (external risk). Internal and external threats may be deliberate or accidental. The ever-increasing information and communication technology advancement has resulted in cybercrime (ICT). The attackers primarily target organizations' confidential data or personal details. According to the 2019 Global Risk Perception Survey, cyber risk was ranked as a top 5 priority by 79% of global organizations (Reagan, 2022). The growth of cyber risk is in large part tied to the increasing use of technology as a driver. Strategic initiatives such as outsourcing, use of third-party vendors, cloud migration, mobile technologies, and remote access are used to drive growth and improve efficiency but also increase cyber risk exposure. Cyber risk has evolved from a technology issue to an organizational problem.

With the growing digitalization of marketing practices and targeted marketing, it has been increasingly important to have additional rules and legislation to protect people's privacy and security. India and Pakistan, for example, have passed legislation in this regard. Therefore, the case in Bangladesh is much more severe as most users need to be made aware of their privacy and security. So, manipulation, falling into a trap, or getting hacked have been common. Bangladesh recently experienced a massive and organized cyber assault. At least 147 public and private organizations, including banks and non-bank financial institutions (NBFIs), were targeted, revealing their complete vulnerabilities (S. Rahman, 2021). Following the growing cybercrime scenario, Bangladesh Government established the Digital security act law 2018. The government has formed special bureaus to investigate, prevent cybercrimes, and execute the necessary measures to protect citizens' data.

In the era of digitalization, to keep pace with the modern world, there is no room to look back to alternative devices or technologies in any segment, including commerce and business. Therefore, in such a situation, people can use technology by adopting necessary

precautions and security measures. This research mainly dealt with the vulnerabilities of the general people in using technology, while indicating how people are falling into the trap of cybercriminals.

II. METHOD

The study is qualitative research that applies the case study method for analyzing the risks and vulnerabilities on the ground. The cases were mainly collected from secondary sources of information, including official and unofficial documents and complaints filed by the victims. As the study is significantly unique, it has found very few similar researches dealing with the problem. Because of that, it mainly relied on the new story, government reports, and police reports for information. Therefore, it has analyzed the existing policy measures by the government and law enforcement agencies to figure out the loopholes and step up with new recommendations. Here, it follows the policy review approach based on analyzing key indicators like Effectiveness, Equity, Acceptability, Feasibility, and Unintended consequences (Cassar et al., 2022; Chandia et al., 2022).

III. RESULT AND DISCUSSION

Conceptual Understanding: E-commerce

Electronic commerce is a relatively new concept that crept into the business vocabulary during the 1970s. E-commerce is frequently used to refer to the online sale of real goods, but it can also refer to any economic transaction that is made possible by the internet. The history of eCommerce begins with the first-ever online sale: on August 11, 1994, a man sold a CD by the band Sting to his friends through his website Net Market, an American retail platform. This is the first example of a consumer purchasing a product from a business through the World Wide Web or “eCommerce” as we commonly know it today. Since then, eCommerce has progressed to make it easier to find and buy things through online shops and marketplaces. Independent freelancers, small enterprises, and large organizations have benefited from e-commerce, allowing them to offer their products and services on a larger scale than traditional offline shopping.

In terms of customer dealings and business operations, some business models are going through, like Business to Consumer (B2C), Business to Business (B2B), Consumer to Consumer (C2C), and Consumer to Business (C2B), etc.

How Does E-Commerce Function?

Although the business (Buy and sell in exchange for money) proceeds are the same, there are some significant differences between e-commerce and traditional offline business. In the e-commerce process, several steps are followed to complete the process indicated in figure 01.

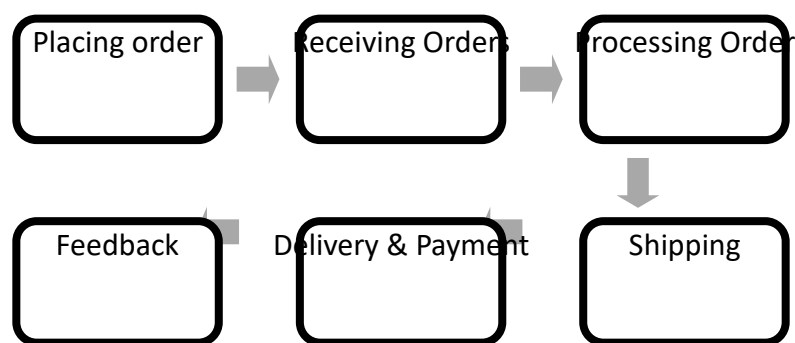


Figure 1. Cycle of Ecommerce

Figure 1 illustrates from the beginning of e-commerce, from placing orders to the delivery and feedback process. After receiving the order the vendor starts the process of preparing particular products and services. And then, shipment and delivery with payment complete the particular cycle. In the end, feedback and evaluation offer the customers control over the quality of products and services.

Emerging Cyber Threats in Ecommerce

A threat can be anything that can intentionally or accidentally exploit the vulnerability and obtain damage or destroy an asset. In other words, a threat is what an organization is defending itself against. Cyber threats are constantly evolving, and organizations must take steps to protect themselves against black market hackers, state-sponsored cybercriminals, and other nefarious individuals and groups. The most effective way to protect against cyber-attacks is by implementing a layered approach to cyber security reviewing your current cybersecurity measures regularly and adapting them as needed (Imperva, 2022).

The demand for online services is expanding significantly more than ever before. However, the ultimate goal of providing impartial security and handiness seems to be a difficult challenge due to the abundant conspicuous actors in a group known as "Cyber-Crime". Acknowledged, "Cyber-Crime" is an unlawful act that involves a computer and a network. Cybercrime is being measured as a grave threat to all spheres of the economic development of a country. Remarkably, monetary gain is still one of the pivotal driving factors behind the lion's share of cybercrime actions and there is a rare chance of this altering in the upcoming days.

Boccio & Leal, (2022) define cybercrime as the offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as the Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS)". The Oxford Dictionary defined the term cybercrime as "Criminal activities carried out using computers or the Internet.

In the last few decades, we have observed an increasing scenario of cybercrime all over the world, which mainly hampered the growth of infant industries like E-commerce. Confronting the vibrant nature of cyber threats, which are newly grown, always shakes the security management of this industry. Transaction transshipment, online marketplace,

everything is vulnerable due to insufficient cyber security measures. The problem is much worse in developing and third-world countries, where people are new to technology but have yet to be introduced to threats emanating from that.

Malign Actors of Originating Cybercrimes

Cyber threat is now a real threat, originating from various sources, including state actors, individuals, or groups from across the world. Usually, malign actors target national and international infrastructure institutions and communication portals to destabilize the order and create panic. Sometimes, as an eventual cause, economic growth, currency flow, and other factors related to the production process are hampered. The growing extent of reliance on the cyber world has been the real target to punish or pressure opponents. Nowadays, even the state mechanism is accused of sponsoring cyber threats to another country for a specific purpose. For example, Iran, Israel, North Korea, and others are accused of sponsoring such crimes. Sometimes, a well-structured crowd of hackers aims to intrude into computing systems for financial advantage. As a way of their weapons, these crowds use phishing, spam, spyware, and malware for extortion, theft of private information, and online scams. However, individual hackers aim at institutions by using a variety of attack methods.

They are generally inspired by individual hidden profits, vengeance, monetary gain, etc. Hackers frequently create new hazards to move forward with their criminal skills and ameliorate their private reputation in the hacker neighbourhood. In addition to that, the employee who has access to data and systems of the company sometimes misuses and pinches data or destroys computing systems for commercial or private gain.

Global Incidence of Cyberattacks

Big Basket, an Indian food e-commerce site, may have experienced a data breach that leaked the individual data of over two crore consumers. The data breach was found on October 30, 2020, during Cybele's normal dark web monitoring operation, according to the cyber intelligence group (Anmol, 2020).

In India, three out of every four small and medium-sized businesses (SMBs) had such a cyber event in the previous year, including 85 per cent losing user information to malicious actors and a noticeable impact on business. Cyber-attacks cost two-thirds (62%) of Indian SMBs more than 3.5 crores over the last year. Each of those surveyed estimated the cost to be in the extent of Rs. 7 crores (Bureau, 2021).

More than 100,000 payment card details were exposed due to a data breach announced by a Japanese e-commerce business. Customers of two of Acro's four beauty product websites were impacted as a consequence of the exploitation of a vulnerability in a third-party payment processing provider, according to a data breach alert.

The Bridge Chronicle reports that in the previous three years, a hacking organization has got into at least 570 e-commerce businesses across 55 countries, including India, exposing data to over 184,000 stolen credit cards and earning over \$7 million (Rs 52 crore) from the sale of compromised payment cards (Vuukle, 2020).

Global cybercrime expenses are expected to increase by 15% each year over the next five years, reaching USD 10.5 trillion annually by 2025, up from USD 3 trillion in 2015. This is the largest transfer of economic wealth in history, it jeopardizes incentives for innovation and investment, it is tenfold more excellent than the damage caused by natural catastrophes in a year, and it will be more profitable than the worldwide trade in all major illicit narcotics combined (Azmoodeh & Dehghantanha, 2022; Curtis & Oxburgh, 2022; Morgan, 2018).

Cyber Threats

Table 1. Categories of Cyber Threats

Cyber Threats Category	Threats
Social Engineering Threats	Baiting, Pretexting, Phishing, Vishing, Smishing, Piggybacking, and Tailgating.
Supply Chain Attacks	Invaders are searching for a non-secure network set of rules, server communications, and coding methods and utilize them to cooperate, construct and revise procedures, change resource code, and conceal malicious content.
Malware Threat	Viruses, worms, Trojans, spyware, and ransomware.
Supply chain Threats	Concession of form devices, the concession of the signing of the code, spiteful code sent as the updates programmed to hardware or firmware apparatuses, and spiteful code preinstalled on corporal instruments.
DoS Threats	HTTP flood DDoS, SYN flood DDoS, UDP flood DDoS, ICMP flood, and NTP amplification.
Injection Threats	SQL injection, Code injection, OS command injection, LDAP injection, XML external, attack. Injection Entities, Cross-site scripting.

Table 1 indicates that there are a number of threats that cause insecurity to cyber users. However, some threats, or cyber-crimes mostly applied to e-commerce, are given below.

Card Testing Fraud: Card fraud is when somebody gets access to credit card numbers that were taken in an illegitimate way. It is a well-known approach used to cheat eCommerce businesses. *Friendly Fraud:* Friendly fraud is identical to charge-back fraud. When a customer buys a product or deal virtually, the merchant demands a charge-back from the disbursement workstation, demanding the transaction was invalid. The financial institutes or banks refund the contract amount to the consumers. *The Fraud of Refund:* While somebody utilizes a credit card that was lifted to create an acquisition on an e-commerce website, this is described as repayment fraud. They then ask for a refund due to an unintended overpayment. On the surface, the scams seem to be building a valid assertion. However, they are trying to make money. *The Fraud of Account Takeover:* This happens if somebody acquires entrance into a client's account on an E-Commerce site. It involves many issues, including identity theft, price victims, and our seller status. Customers who believe their information is vulnerable to websites or E-Commerce sites are less likely to sign out. *Interception Fraud:* It occurs when swindlers place orders on an

e-commerce website where the billing address along with the delivery address goes to the data related to a credit card that was taken away. When the request of order is to be found, they aim to catch the box up and seize the items for their own purpose. They may do it in many ways.

Triangulation Fraud: When a buyer makes a legitimate purchase on a third-party marketplace (such as Amazon or Sears.com), the merchandise they get is purchased fraudulently from another retailer's website. This behaviour is detrimental to all types of enterprises. Customers are frequently unaware of this. *Supply Chain Attacks*: Software supply chain attacks are particularly ruthless because the requests being cooperated by attackers are contracted and qualified by truthful merchants. In the attack of many software supply chains, the software trader is unconscious and its usages or appries are contaminated. Spiteful code runs with the identical faith and freedoms as the conceded submission. Here are different types of supply chain attacks on form devices, the concession of the signing of the code, spiteful code sent as the updates programmed to hardware or firmware apparatuses, and spiteful code preinstalled on corporal instruments. *Malware Attack*: Malware is taken from the short form of "malicious software". The different types of malware that are frequently used are viruses, worms, trojans, spyware, and ransomware. *Social Engineering Attack*: It engages swindling users by giving an access point for malware. The sufferer gives sensitive data or unintentionally mounts malware on their gadget since the invader pretences as a genuine actor. Here are some other types of social engineering attacks: Baiting, Pretexting, Phishing, Vishing, Smishing, Piggybacking, and Tailgating (Chowdhury et al., 2022; N. Islam et al., 2019).

Man-in-the-Middle: It engages by interrupting the contact between two points whose are terminal points, for instance, a user and an application. The invader may snoop on the contact, pinch insightful information, and take off each party participating in the contact. For example, the MitM attacks include the spying of WI-FI, the stealing of Email, the hoaxing of DNS, the bluffing of IP, as well as the bluffing of HTTPS. *The Attack of Denial-of-Service (DoS)*: It overworks the system of objectives with a large amount of circulation, obstructing the method's capacity to task generally. An assault engaging numerous gadgets is acknowledged as a distributed denial-of-service (DDoS) attack. DoS spasm systems contain: HTTP deluge DDoS, SYN flood DDoS, UDP flood DDoS, ICMP flood, and NTP amplification. *The Attack of Injection*: Injection spasms abuse a helpless diversity to straightforwardly place spiteful inputs into the program of online submission. Flourishing acts of violence can uncover subtle data, implement a DoS, or cooperate with the whole method. Injection attacks include SQL injection, Code injection, OS command injection, LDAP injection, XML external attacks, injection Entities, and Cross-site scripting. *Phishing and spear-phishing*: Lance phishing is an electronic mail or electrical transportation cheat aiming at a sole individual, corporation, or association. Cybercriminals can expect to set up malware on a targeted user's machine along with thieving data for wicked purposes.

Spoofing: If somebody or else somewhat has faith in being unusual in an active effort to increase our self-assurance of us, lifting cash, taking information, acquiring right of entry to methods of us, otherwise stretch, malware is known as spoofing. Spoofing has many kinds, such as Spoofing of URL, Spoofing of Emails, P spoofing, spoofing concerned with a Text message, spoofing created from GPS, Spoofing of Extensions, Spoofing related to

Caller ID, Spoofing related to face, and many more. *Ransomware*: It is a modified form of malware that encrypts our data and demands a ransom, which is typically paid in Bitcoin, to decrypt it. *Website defacement*: It is an attack in which a malevolent group of people intrude into a website and then change text or writing given on the E-commerce site by means of their individual influenced communications or messages. The mails or posts may suggest a politically aware or spiritual text, vulgarity, or new inapt text, which might humiliate the owners of the E-commerce site. On the other hand, it is observed that a particular group of covetous hackers has lacerated the E-commerce site. The usual reasons for occurrences that are related to the defacement of E-commerce sites comprise illegal right of entry, SQL instillation, Scripting of Cross-site (XSS), Hijacking of DNS, and infection of malware.

E-commerce in Bangladesh

E-Commerce is now a more modern gadget that is attracting people all over the world, including in Bangladesh. Bangladesh has had a very positive outcome regarding its thriving e-commerce industry and the general people's participation in it. People have fully recognized the effectiveness of digital transactions and internet buying. Due to people's increased usage of internet shopping since the pandemic, there has been a significant shift in purchasing habits. Additionally, the e-commerce sector has gotten a boost from the expanding mobile financial services (MFS) market, which has made it easier for customers to make online purchases.

In 2012, the local e-commerce market in Bangladesh started to develop into a genuine ecosystem. Expanded internet access and the Bangladesh Bank's subsequent validation plus the endorsement of a virtual disbursement, made this possible. Some banks initially refused to support the online payment gateway technology. The growth of e-commerce has been facilitated by better internet connections and a rise in the number of individuals with access to the internet during the previously limited ages.

The E-commerce business growth has been aided by better internet connections and a rise in the number of individuals with access to the internet during the past few years. In 2016, 50 million dollars was consumed in the E-commerce market of Bangladesh. \$10 million of that total came from FDI. In the year 2017, the retail market generated BDT 1335.71 billion. On the other hand, the B2C market for E-commerce business was 110 – 115 million dollars (BDT 9.0 billion). According to the estimates of the E-Commerce Association of Bangladesh, the market reach of E-commerce companies increased to Tk 17.0 billion in 2017 from Tk 4.0 billion in 2016 (e-CAB). In 2021, it was worth Tk 70 billion.

According to the 2017 study by the E-Cab (E-Commerce Association of Bangladesh), smartphone and data connections in Bangladesh have 99 per cent geographic coverage. As of May 2021, the Bangladesh Telecommunication Regulatory Commission (BTRC) estimates that there are 117.3 million internet users nationwide, of whom only 9.8 million utilize broadband connections, and the remainder use mobile internet (Khan, 2020).

Payment Gateway in Bangladesh (Complete)

Some companies in Bangladesh nowadays offer payment gateway services, which allow customers to pay with convenience methods like online banking, debit card, credit card, mobile banking, etc., The payment gateway also allows using local currency to buy a particular product priced with international currency. Recently, many educational institutions are using such payment systems to facilitate the payment of academic fees and others. Mostly, the problem usually occurs in e-commerce where customers used to have a variety of payment choices, which the sellers could not afford for a single shop. But now, it has been solved by this payment login service, which lets people with debit and credit or mobile banking from different companies in a unique process. Some payment gateway service providers in Bangladesh are SSLCOMMERZ, Portwallet, Aamarpay, Shurjapay, Paddle, etc. (LYAMENKOV, 2022; Olanrewaju et al., 2017).

E-commerce Potentials in Bangladesh

E-commerce states the exchange of merchandise, products, services, and facilities involving businesses and customers through an electronic network. In Cisco, it is seen as Business-to-Business or B2-B E-commerce. In Amazon, we can observe business-to-consumer or B2C e-commerce. eBay, is seen as consumer-to-consumer or C2C e-commerce, and business-to-government e-commerce is the four broad categories that makeup e-commerce (B2G).

E-commerce trade includes a mix of various types of skills and technologies, for instance, email (Electronic mail), EDI (Electronic Data Interchange), as well as Electronic Fund Transfer (EFT). In the case of Electronic Data Interchange (EDI), trading partners must come to an agreement. A common way to exchange company data is using EDI. Other EDI methods include faxing and emailing. Small, medium and large businesses in Bangladesh have used e-business platforms.

Bangladesh is also using other e-commerce mediums for improving the e-commerce sector, like other developing and developed countries. In today's E-commerce business environment, Facebook Commerce (F-Commerce) and Mobile Commerce (M-Commerce) are quite prevalent.

The conventional e-commerce industry added an incredible additional Tk 1,000 crore to the total amount of business transactions conducted in the last year by the f-commerce sector. Currently, there are two thousand e-commerce websites and fifty thousand Facebook-based businesses that ship close to thirty thousand items daily. Currently, Dhaka, Chattogram, and Gazipur are responsible for eighty per cent among online deals (A. S. Islam et al., 2022).

M-commerce has also grown tremendously in Bangladesh. Many private companies have introduced smartphone applications for online shopping, including retail giants like Agora, Meena, Bazaar, Swapno, and electronics and gadget retailers. Customers in Bangladesh are already becoming accustomed to mobile purchases. Along with Amazon, eBay, and Alibaba, which are shortly to open, the international payment gateway PayPal, Xoom, has just been implemented in the nation and provides a new dimension to e-commerce (Fong & Hui, 2014; Kiselicki et al., 2022).

Ecommerce Related Government Regulation

Bangladesh passed the (ICT) Act of 2006 to promote information technology development and ease eCommerce. The 2013 amendment to the Act added provisions for persons who conduct cybercrimes to face jail time and/or penalties. The implementation of this act has significantly impacted Bangladeshi businesses and consumers of mobile and online commerce.

The Ministry of Commerce's adoption of the Digital Commerce Operation Guidelines 2021 (Guideline) is undoubtedly a significant step toward successful operational governance of Bangladesh's "e-commerce" industry, but it is equally important that the guidelines be properly put into practice (Hossain, 2021). A few operational procedures, including purchase, delivery, payment, refund, complaint management, etc., have been briefly covered in this guidance. These procedures are related to a number of legal issues.

Stories of Cyber Incidents

Deep Discount is Another Way of Fraud in E-commerce Business

Uneven competition plays a pivotal role in creating the net of fraud in e-commerce in Bangladesh by offering deep discounts. The story about discount fraud came out on February 1 2022 in a leading English Daily, The Daily Star. The Bangladesh Commission for Competition (BCC) paraded a case against the famous E-commerce hub Alesha Mart, a related E-commerce enterprise, for making uneven competition within the market by providing prejudiced money off. The case was filed, which follows the Act for Competition of 2012, which conditions that no commercialism will be able to misuse its leading situation. The commission had lodged an objection against the well-founded e-commerce organization on its individual in month of November. Conferring to the court case, Alesha Mart traded motorcycles whose brand name is Bajaj Pulsar that have a hundred and fifty solid capability engines at a worth that was thirty-five per cent less than the value in June 2021 (M. Rahman, 2021; Sameh, 2021).

Scams Shattered the E-Commerce Growth

The story concerning the downswing of the e-commerce business of Bangladesh given by the central bank, came out on December 28, 2021. A Bangladesh Bank report on e-commerce transactions through the formal channel showed that the transactions declined to Tk 743 crore in October 2021, reaching the highest amount of Tk 1277.4 crore in June 2021. The transactions in October were 41.53 per cent or Tk 534.4 less than the transactions in June. In Feb 2020, the transactions through the e-commerce platform were Tk 247.1 crore. Zeeshan Kingshuk Huq, co-founder and chief officer of e-commerce platform Sindabad.com, aforesaid that customers' confidence within the e-commerce sector was deterred due to the non-payment of the customers' cash by a variety of e-commerce platforms that oversubscribed the product on substantial discount against advance payments and didn't either deliver the product or to allow the cash back. Zeeshan conjointly believes that the restoration or retention of customers' confidence would rely upon the performance of platforms. Due to scams, this business is declining in its revenue on a large scale.

FB Page is a New Trap for Online Shoppers

Nowadays, it has been apparent that online marketing has additionally become standard through varied pages or groups on Facebook. Many folks have started online businesses by opening pages on their own initiative. However, the question is regarding how reliable sites are! The story is going to reflect the net of cybercrime through the FB page (Daily Sun, 2020). The complaint was from a student of Jahangirnagar University. While scrolling through his newsfeed on Facebook, he suddenly saw an advert for an associated e-commerce website. He ordered the shirt off his selection worth TK 1,100. As per their terms, he paid money through BKash, a leading mobile banking company. Three days later, the ordered products fell upon his address. Therefore, after opening the packet, he found that the shirt that he had ordered wasn't there. Moreover, a low-quality dress was delivered. However, some other similar experiences that occurred with many e-commerce customers have been widespread.

E-Orange is an Example Ponzi Scheme

In the previous record of the structures of the Ponzi, no instance of evenhanded fairness is found. We observe simply a consequence: only the household of cards approaches banging down, the instigator is hauled off to prison, and then the sufferers are the ones swung out to dry.

On March 15 2022, a news story became the buzzword that reflected the Ponzi scheme. Take E-orange as an illustration. More than 5,573 cases were lodged related to the fake business of the e-commerce hub with the DNCRP (Board of controllers of state customer human rights security). Nevertheless, with a single penny visibility, merely thirty-three objections might be predisposed of until now. The volume of cash in excess of which the objections were funnelled is a large quantity. The escrow accounts have been receiving a huge amount of payment money since July 1 of the last year, according to an instruction of the Central Bank of Bangladesh, as well as guessing authorization from the sellers relating to the supply of the manufactured goods, in agreement with the Ministry of Information of Bangladesh. Escrow is a third agent usage, which clutches a property or else deposits beforehand they are transmitted. The third agent grips the assets or cash until the individual agent has accomplished their inscribed contract requirement. On the other hand, although the e-orange owner and the COO (Chief Operating Officer) went to prison for more than Tk eleven thousand crore complaints as well as squashed bank accounts, that didn't bring any solution for the customers and investors. Thus, a number of incidents and risks grow concerned among people demotivating them mainly to involve in e-commerce-related business (CIRT Team, 2021).

Analysis of the Incidents

Causal Factors

The E-commerce sector in Bangladesh has been growing up rapidly for the last couple of years, welcoming a large number of new customers and sellers. Covid19 outbreak and strict lockdown forced people to stay inside rather than out with friends, family, and colleagues. In an eventual cause, people swiftly took the option of E-commerce. Besides covid 19 restrictions, people now figured out that the cost of time, travelling, and hassles

are not beneficial for them to go shopping. Rather making orders by staying home is comfortable and affordable. Therefore, nowadays, the quality of e-commerce services and products is improving day by day. Renowned business outlets, super shops, and shopping malls opened their new chapter of operating business in E-commerce, which helps significantly to turn back the trust of the customers. Mobile banking and the facilitation of card service terms and conditions by different private and government banks are also considered blessings for eCommerce. In addition to that, a supportive mindset from the government is also a major source of motivation for the growing e-commerce sector in Bangladesh.

Although online business in Bangladesh is amplified, however recent fraudulence of customers has always posed new challenges. Most particularly, newcomers in eCommerce, including small shop owners or homemade producers, are not aware of cyber security knowledge. Even many fully rely on a third person for opening up the account, doing promotions, and managing payment gateways. Consequently, the privacy and security of their business accounts are already at stake. Most of them even know nothing about the immediate steps to meet security threats if they get notifications.

The youth, who are new to eCommerce, mostly jumped up to social media tools to open their shops. But there are some issues like spamming, phishing, email, scam, and spy apps, which can be used by malicious actors to get crucial security information. In addition to that, the e-payment system in our country is not also developed as effectively as needed to grow successful e-commerce. So, fraudulent poor customer servicing, mismanagement, loopholes in apps, and many other vulnerabilities are found in our research that indicate the riskiest area of the eCommerce industry. Recently, the Bangladesh bank scam is the premier example of how the banking system in this country has grown through. Even until now, Bangladesh Bank has failed to make mobile banking, e-banking, and card service provider banking organizations accountable for fraudulence, mismanagement, and poor-quality services. Even the government has no such specific regulation to deal with the problems immediately. The last couple of years ago, the government introduced a digital security act in the orient of acting as a watchdog of security for online users. However, it is accused that the analysts are not getting properly utilized but rather being abused to tackle the dissent.

Law enforcement agencies have also taken the necessary steps to train their staff to deal with cyber security threats, including sending them abroad for higher education, hiring experts from outside, buying sophisticated technologies, and creating new units named cyber-crime in the police force. Therefore, it is not sufficient as crimes get increase rapidly in different forms and natures. And even law enforcement agencies cannot do anything until the users are not aware enough of their safety. Even many government organizations don't even have a cyber specialist and always rely on third-party services. In such a situation, the government requires a very concrete and coordinated step by utilizing its resources and manpower to deliver proper training and guidelines.

Steps Ahead

Table 2. Recommended Policy Steps

Key areas	Steps
Raising Public Awareness	<ul style="list-style-type: none"> ✓ Including a chapter in Textbooks ✓ Workshops, Seminars, Training ✓ Obligating a course completion before issuing a license ✓ Nationwide Campaign (Social Media Campaign, Physical Mobilization)
Framing Regulations and Acts	
Enhancing the Capacity of Law Enforcement Agencies	<ul style="list-style-type: none"> ✓ Training ✓ Buying Sophisticated Tools ✓ Hiring Specialists for Temporary Basis
Research and Fund Allocation	<ul style="list-style-type: none"> ✓ Special Research Cell ✓ Assess the extent of threats ✓ Priority in the University Research ✓ Identify the Variant and nature of threats ✓ Fellowships, Scholarships, and Grants ✓ Upgrade the Technology ✓ Technology Festivals ✓ Better adaptation of the methods ✓ Idea Contest ✓ SWOT Analysis
The comprehensive plan and better coordination	<ul style="list-style-type: none"> ✓ Collaborating and cooperating with NGOs and Others to deal with the issues
Other Threats to Ecommerce	<ul style="list-style-type: none"> ✓ Strict E-commerce regulation and consumer rights preservation acts ✓ Low-Quality Products and Fraudulences ✓ Special cell for monitoring ✓ Arbitrary in Pricing ✓ Facilitating the submission of complaints and prompt steps ✓ Bringing E-commerce under a particular umbrella of the organization

Source: Based on documents and story analysis

Raising Public Awareness

In 2022, it will be crucial to be aware of and take precautions against cyber threats, which are a developing issue that affects both enterprises and individuals. Cyber security knowledge is more essential than ever as digital technology advances and permeates most facets of peoples' personal and professional lives. Everyone increasingly uses Internet-connected PCs, laptops, and other gadgets to complete numerous jobs. Since the commencement of Covid, 19, students in school have become increasingly reliant on the internet. Consequently, by integrating terminology related to cyber security in textbooks, the public might first become informed.

Businesses and banks are beginning to consider hosting seminars and workshops on cybersecurity issues to raise awareness. For instance, UCB Bank started a workshop on cyber security. The countrywide campaign is significantly boosting public awareness of cyber security. A deal to start a cyber-security campaign for kids and teens was struck by the United Nations Development Programme (UNDP) and the government of Bangladesh's ICT Division (TBS Report, 2022).

Framing Regulations and Acts

Except for the traditional Information and Communication Technology (ICT) Act of 2006 and the Digital Security Act (DSA), of 2018, Bangladesh does not have any laws governing cyber security. The current legal system is unable to address the threats that have emerged as a result of the ultra-advancements in surveillance technology during the past ten years.

The government of Bangladesh aims to create a cyber-security strategy. The Digital Bangladesh initiative's four pillars Digital Government, Human Resource Development, IT Industry Promotion, and Connectivity & Infrastructure are supported by the Bangladesh Cybersecurity Strategy 2021–2025 (Gordienko, 2022; Molla, 2022).

Enhancing the Capacity of Law Enforcement Agencies

The government of Bangladesh requires cyber security training. A cyber range is a simulation platform used to teach and evaluate cyber security professionals, educate students about cyber security, and test processes and technology in a real-world setting that mimics assaults, scenarios, and networks.

Ctfd.io is an open-source solution that may be altered to suit the demands of any institution or organization. For those interested in cybersecurity and those who work in the sector, as well as those who view cybersecurity as an advanced subject in the field of computer science, it can be a great learning tool (Bangladesh e-Government Computer Incident Response Team, n.d.). Numerous online forums have been developed to practice and discuss relevant problem sets, and they have greatly increased the opportunity for networking with like-minded individuals.

Research and Fund Allocation

Cyber threats are nowadays becoming an epidemic in nature, and to an extent, that was not thought of in previous days. There is no such universal nature of threats. Every day, the nature and variants have changed. Even it varies from person to person, city to city, and context to context. For example, in the village area of Bangladesh, people do have adequate knowledge of cyber security threats. They are very vulnerable and can be pulled into risk by simple spam links or hacks. Therefore, in city areas, people use different kinds of apps and services where they are required to provide their information. Those apps also have access to their handsets and other information. So, in city areas, the threats are somewhat different from rural areas.

The traps being used always vary from person to person. So, rigorous and nonstop research is needed to assess and understand the variants of the threats and the reasons behind them. In addition to that, nowadays wide use of different apps also hampers the

customer's security. So, systematic and technical analysis is required to check and identify the malicious apps which fail to confirm users' security. However, methodological advancement and technological gradation also require advanced research. In doing so, government and Non-government actors should come forward and allocate research grants in different ways to accomplish the desired research objectives. There should be a special cell of research for this particular purpose to confirm the betterment and up gradation of the technology and methods. Therefore, law enforcement agencies and other institutions should also collaborate with the universities in research and innovation to deal with the threats.

Collaborating and Cooperating with NGOs and others to deal with the Issues

To improve online safety, The Bangladeshi government began collaborating with various NGOs and others to handle cyber concerns. At the moment, one of the top global agenda items is cooperation in the sphere of cyber security. On July 14 and 15, 2022, the Bay of Bengal Initiative for Multi-Sectoral Technical and Economic Cooperation (BIMSTEC) convened the first-ever meeting of its skilled assemblage on cyber safety collaboration in New Delhi. For the region's BIMSTEC nations, this is a new area of endeavour. Cyber Safety Coordinator of India, Lt. General Rajesh Pant, presided over this face-to-face government-to-government gathering, which included representatives from South-East Asian countries.

Here are seven policies that are recommended by the CPD (Centre for Policy Dialogue) to protect the E-commerce of Bangladesh.

Firstly, the present law and rules ought to be amended, and people are required to be enforced properly and take action against dishonest e-commerce organizations.

Secondly, the institutional capability of the relevant organizations and departments like the Ministry of Commerce, People's Republic of Bangladesh Bank, Board of National Consumers' Right Protection, Monetary Intelligence Unit, and Competition Commission ought to be increased through sufficient and experienced human resources and the adoption of technology.

Thirdly, coordination among the varied establishments as well as the Ministry of Commerce, People's Republic of Bangladesh Bank, law-imposing bodies, and alternative relevant organizations ought to be enlarged, and therefore the role of those bodies must be clearly outlined.

Fourthly, monetary intelligence ought to collect regular knowledge on E-commerce and share those with relevant bodies and conjointly with the public daily to extend the answerability of those businesses and build customers' attention to the activities of E-commerce businesses.

Fifthly, awareness among e-commerce customers ought to be enlarged, so they behave responsibly and don't fall prey to such traps of dishonest e-commerce organizations.

Sixthly, non-public associations like the e-Commerce Association of Bangladesh (e-CAB) have the job of gathering data on recent businesses before registering, as their property,

and permitting members of the companies to observe the operations of those businesses.

Seventhly, the govt. Ought to solve the matter, however, through the legal framework of the corporate Act and not by investing public cash in these dishonest firms.

IV. CONCLUSION

Security is always the prime focus of every system from its origin to evolution. Here, the new growing eCommerce sees an outnumbered youths involved with their new ideas, entrepreneurship, and businesses. The government must manage the flow of a growing number of e-commerce while maintaining its security. Therefore, it is now realized that after experiencing several cyber fraud incidents, the people who are the main actors lack security knowledge and risk. At the same time, the government shows also inactivity in response to those incidents indicating the government's unpreparedness and inexperience to problems. Therefore, this article explains the risks that occurred in those e-commerce sectors while indicating their' causal factors. By analyzing the problems and scenarios, the article also made some policy prescriptions for employing at individual and government levels, including engaging and educating people on cyber threats, vulnerabilities, and causal factors. At the same time, it recommends the government prepare for technological advancement, training, and approaches to dealing with the challenges of this techno-advanced future world.

V. REFERENCES

- [1] Anmol. (2020). *BigBasket Suffers Massive Data Breach; Over 2 Crore Users' Personal Details Leaked*. Beebom. <https://beebom.com/bigbasket-suffers-massive-data-breach/>
- [2] Azmoodeh, A., & Dehghantanha, A. (2022). *Deep Fake Detection, Deterrence and Response: Challenges and Opportunities*. <https://doi.org/10.48550/arXiv.2211.14667>
- [3] Boccio, C., & Leal, W. (2022). Does Socializing in the Virtual World Impact Victimization in the Real World? *Journal of Interpersonal Violence*, 38(3–4), 088626052211099. <https://doi.org/10.1177/08862605221109922>
- [4] Bureau, O. (2021). *Cyber-attacks in the past year cost 62% SMBs in India over ₹3.5 crore: Report*. Businessline. <https://www.thehindubusinessline.com/info-tech/cyber-attacks-in-the-past-year-cost-62-smbs-in-india-over-35-crore-report/article36689903.ece>
- [5] Cassar, M., Cutajar, J., & Thake, A. M. (2022). The Role of Public Policy in Promoting Gender Equality in Malta: A Diachronic Approach. *International Journal of Social Sciences Perspectives*, 12(1), 41–59. <https://doi.org/10.33094/ijssp.v12i1.734>
- [6] Chandia, K., Iqbal, M., & Bahadur, W. (2022). An analysis of the linkages among fiscal vulnerability, financial stress and macroeconomic policies: an econometric study. *Fulbright Review of Economics and Policy*, 2(1). <https://doi.org/10.1108/FREP-06->

[2021-0036](#)

- [7] Chowdhury, M., Bappi, M., Imtiaz, M., Hoque, S., Islam, S., & Haque, M. (2022). The Transition of E-Commerce Industry in Bangladesh: Added Concerns & Ways of Recovery. *International Journal of Economics and Finance*, 14(7), 18. <https://doi.org/10.5539/ijef.v14n7p18>
- [8] CIRT Team. (2021). *CTFd.io: An interactive learning tool for Cybersecurity*. BGD E-GOV CIRT. <https://www.cirt.gov.bd/ctfd-io-an-interactive-learning-tool/>
- [9] Curtis, J., & Oxburgh, G. (2022). Understanding cybercrime in 'real world' policing and law enforcement. *The Police Journal: Theory, Practice and Principles*, 96(1), 0032258X2211075. <https://doi.org/10.1177/0032258X221107584>
- [10] Daily Sun. (2020). *Online fraud: An obstacle to digital Bangladesh*. Daily-Sun.Com. <https://www.daily-sun.com/post/494473/Online-fraud:-An-obstacle-to-digital-Bangladesh>
- [11] Fong, A., & Hui, S. (2014). From E-Commerce to M-Commerce. In *Multimedia Engineering: A Practical Guide for Internet Implementation* (pp. 249–262). <https://doi.org/10.1002/9780470030851.ch8>
- [12] Gordienko, D. (2022). Trade and Economic Cooperation of China with the Countries of the World and Russia in the 14th Five-year Plan (2021-2025). *Problemy Dalnego Vostoka*, 56. <https://doi.org/10.31857/S013128120021449-4>
- [13] Hossain, A. (2021). *OP-ED: Concerns about e-commerce regulations in Bangladesh*. Dhaka Tribune. <https://archive.dhakatribune.com/business/2021/08/10/op-ed-concerns-about-e-commerce-regulations-in-bangladesh>
- [14] Imperva. (2022). *Cybersecurity Threats: What are Cybersecurity Threats?* Imperva.Com. <https://www.imperva.com/learn/application-security/cyber-security-threats/>
- [15] Islam, A. S., Ahmed, S., & Khan, R. (2022). A Review on E-Commerce System in Bangladesh: An Empirical Study. *ICCA 2022: 2nd International Conference on Computing Advancements*, 269–276. <https://doi.org/10.1145/3542954.3542994>
- [16] Islam, N., Sakib, T., Chiran, M., Elahee, R., Bushra, F., Mir, & Hossain, M. (2019, December 18). Success Factors of Online Commodity Business in Bangladesh. *International Conference on "Global Business, Economics, Finance & Social Sciences (ICGBEFSS-19)At: Malayisa*.
- [17] Khan, S. S. (2020). *E-commerce in Bangladesh: Where are we headed?* Financial Express. <https://thefinancialexpress.com.bd/views/views/e-commerce-in-bangladesh-where-are-we-headed-1578666791>
- [18] Kiselicki, M., Kirovska, Z., Anastasovski, M., & Jovevski, D. (2022, October 23). Security Aspects Of Digital Transactions E-Commerce And M- Commerce Implementations. *XXXVII International Conference "The Power Of Knowledge" At: Perea, Greece*.
- [19] LYAMENKOV, A. (2022). Settlement risk in international economic transactions. *Finance and Credit*, 28(8), 1831–1851. <https://doi.org/10.24891/fc.28.8.1831>
- [20] Molla, M. B. (2022). *Meeting on Bangladesh Cybersecurity Strategy 2021-2025 Responsibility Matrix*. BGD E-GOV CIRT | Bangladesh e-Government Computer Incident Response Team. <https://www.cirt.gov.bd/meeting-on-bangladesh-cybersecurity-strategy-2021-2025-responsibility-matrix/>
- [21] Morgan, S. (2018). *Cybercrime To Cost The World \$10.5 Trillion Annually By 2025*.

- Cybercrime Magazine. <https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/>
- [22] Olanrewaju, R., Khan, B., Mattoo, M., Anwar, F., Nordin, A., & Mir, R. (2017). Securing electronic transactions via payment gateways - a systematic review. *International Journal of Internet Technology and Secured Transactions*, 7(3), 245. <https://doi.org/10.1504/IJITST.2017.089781>
- [23] Rahman, M. (2021). *The Protection of Consumer Rights in E-commerce (B2C): A Critical Analysis of the Laws in Bangladesh* [University of Dhaka]. <https://doi.org/10.13140/RG.2.2.17637.68323>
- [24] Rahman, S. (2021). 240 govt entities, banks come under cyber-attacks. Financial Express. 240 govt entities, banks come under cyber-attacks
- [25] Reagan, T. (2022). 2019 Global Cyber Risk Perception Survey. Marshmclennan. <https://www.marshmclennan.com/insights/publications/2019/sep/global-cyber-risk-perception-survey-report-2019.html#:~:text=79%25 of respondents ranked cyber>
- [26] Sameh, M. S. (2021). The Emergence of E-commerce in Bangladesh And Its Growth. *International Journal Of Science and Business*, 5(10), 30–40. <https://doi.org/10.5281/zenodo.5542943>
- [27] TBS Report. (2022). UCB organizes workshop on “4th Industrial Revolution and Digital Upskilling.” The Business Standard. <https://www.tbsnews.net/economy/banking/ucb-organizes-workshop-4th-industrial-revolution-and-digital-upskilling-473834>
- [28] Vuukle. (2020). Hackers break into 570 e-commerce stores, generate over \$7 million in 3 years. Tribune India News Service. <https://www.tribuneindia.com/news/science-technology/hackers-break-into-570-e-commerce-stores-generate-over-7-million-in-3-years-110150>