frontiers | Frontiers in Psychology

TYPE Conceptual Analysis
PUBLISHED 19 October 2022
DOI 10.3389/fpsyg.2022.927398

Cyber security threats: A never-ending challenge for e-commerce

Xiang Liu[1], Sayed Fayaz Ahmad[2], Muhammad Khalid Anser[3,4], Jingying Ke[5]*, Muhammad Irshad[6], Jabbar Ul-Haq[7] and Shujaat Abbas[8]

[1]School of Economics and Management, Fuzhou University of International Studies and Trade, Fuzhou, China, [2]Department of Engineering Management, Institute of Business Management, Karachi, Pakistan, [3]Faculty of Business and Management Sciences, Superior University, Lahore, Pakistan, [4]School of Public Administration, Xi'an University of Architecture and Technology, Xi'an, China, [5]School of Business, Xiamen Institute of Technology, Xiamen, China, [6]Department of Management Sciences, University of Gwadar, Gwadar, Pakistan, [7]Department of Economics, University of Sargodha, Sargodha, Pakistan, [8]Graduate School of Economics and Management, Ural Federal University, Yekaterinburg, Russia

Check for updates

OPEN ACCESS

EDITED BY
Umair Akram,
RMIT University, Vietnam

REVIEWED BY
Roberto Cerchione,
University of Naples Parthenope, Italy
Abdallah Qusef,
Princess Sumaya University
for Technology, Jordan

*CORRESPONDENCE
Jingying Ke
kejingying@xit.edu.cn

SPECIALTY SECTION
This article was submitted to Organizational Psychology, a section of the journal Frontiers in Psychology

RECEIVED 27 April 2022
ACCEPTED 20 July 2022
PUBLISHED 19 October 2022

CITATION
Liu X, Ahmad SF, Anser MK, Ke J, Irshad M, Ul-Haq J and Abbas S (2022) Cyber security threats: A never-ending challenge for e-commerce. *Front. Psychol.* 13:927398. doi: 10.3389/fpsyg.2022.927398

COPYRIGHT
© 2022 Liu, Ahmad, Anser, Ke, Irshad, Ul-Haq and Abbas. This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY). The use, distribution or reproduction in other forums is permitted, provided the original author(s) and the copyright owner(s) are credited and that the original publication in this journal is cited, in accordance with accepted academic practice. No use, distribution or reproduction is permitted which does not comply with these terms.

This study explores the challenge of cyber security threats that e-commerce technology and business are facing. Technology applications for e-commerce are attracting attention from both academia and industry. It has made what was not possible before for the business community and consumers. But it did not come all alone but has brought some challenges, and cyber security challenge is one of them. Cyber security concerns have many forms, but this study focuses on social engineering, denial of services, malware, and attacks on personal data. Firms worldwide spend a lot on addressing cybersecurity issues, which grow each year. However, it seems complicated to overcome the challenge because the attackers continuously search for new vulnerabilities in humans, organizations, and technology. This paper is based on the conceptual analysis of social engineering, denial of services, malware, and attacks on personal data. We argue that implementing modern technology for e-commerce and cybersecurity issues is a never-ending game of cat and mouse. To reduce risks, reliable technology is needed, training of employees and consumer is necessary for using the technology, and a strong policy and regulation is needed at the firm and governmental level.

KEYWORDS

cyber security, e-commerce, social engineering, denial of services, malware and attacks on personal data

Introduction

Technology contributes a lot to our daily life. One of the significant contributions of technology is its applications to the way of doing business (Wang et al., 2022). It has shifted the traditional methods of doing business to the next level. New technologies influence the quality and cost of products and services and business means (Thomson et al., 2022). Business means exchanging something for something; to be more specific, it refers to selling and buying products or services in exchange for money (Burton, 2007).

As discussed earlier, the way of doing business has changed due to the application of technology; the business activity involving using or applying electronic technology is known as e-commerce or e-business (Reynolds, 2000). In e-commerce, activities are completed online through the internet. Primarily, e-commerce uses a website, but other technologies such as email, etc., can also be used. Three main parts of e-commerce are the electronic market, online retailing, and online auctions. A customer can buy a product or service distantly by using the application or technology offering the product (Khurana, 2019). E-commerce is still evolving with the development of new technology and its applications and has attracted researchers from various areas like business and technology to enhance the process and make it more beneficial and profitable. But these developments have also brought some challenges to the industry (Jennifer, 2022). One of the challenges is "the cyber security concern" in e-commerce (Mishra et al., 2022) which is one of the most critical and common concerns it faces.

E-commerce business entities and customers are always the targets of cybercriminals and cyber-attacks (D'Adamo et al., 2021). According to a report, 83% of the United States retailers are vulnerable and could easily be attacked (Security Magazine, 2020). Attackers usually attack customers' private data, which is the most valuable asset in e-commerce. They can either steal the data from the database of online stores, malware, ransomware, and e-skimming. They can also attack in the form of distributed denial of services (DDoS) or Pishing (Bigcommerce, 2022). This is clear that with the advent of business with the help of technology like e-business and e-commerce, opportunities are reaching us more rabidly but not in the absence of issues like cyber security, etc. Like the e-commerce organizations, cybercriminals are also constantly enhancing their technology and skills to find vulnerabilities in the existing system of e-commerce and take advantage of them (Jang-Jaccard and Nepal, 2014). Therefore, this is necessary to explore technology's pros and cons and address the issues.

It is necessary to highlight here that using advanced technology for addressing the issues of cybersecurity is expensive and most of the e-commerce organizations cannot afford. Many organizations often ignore this control on cybersecurity threats due to its huge costs but they also ignore the returns which may gain the organizations in the longer term (Koomey, 2012). Without a doubt it is true that invest in technology ensures security to al large extant yet it is difficult for smaller and new organization to adopt (Dobrowolska, 2020).

Problem statement

Even though technology provides tremendous opportunities for the business sector, the challenges accompanying these opportunities cannot be ignored. One of the challenges is in the form of a cyber security threat, the intensity of which is increasing day by day.

Objectives

The research aims to explore the concerns about cyber security threats in e-commerce with a focus on social engineering, denial of services, Malware, and Attacks on Personal Data and provide a managerial solution.

Research questions

i. What are the concerns about the cybersecurity threats in e-commerce?
ii. How cybersecurity threats can be addressed and minimized?

This conceptual analysis aims to contribute to understanding cybersecurity in e-commerce. Many of today's researchers focus on technology's support in business and ignore the challenges technology is bringing to the company. This work highlights cybersecurity as one of the most critical issues related to technology used in industry (e-commerce). It is focused on some cybersecurity issues, e.g., social engineering, denial of services, malware, and attacks on personal data. Although the scope of cybersecurity is huge, we only discuss some most common types of security breaches. We base this analysis on multiple data sources like books, journal articles, magazines articles, newspapers, blogs, etc. to answer the research questions.

Theoritical background

Cyber-attack theory

The cyber-attack theory (CAT) believes that information is the central part of any cyber-attack and states that the success of cyber-attacks depends on the information owned by the attackers at the time of the attack and the information modified or gained during the attack (Zhuang et al., 2015). Each system has configuration information that plays a significant role in a cyber-attack. And it is necessary for a cyber-attacker to have this information. This information includes the information about the system, i.e., configuration information, the system data, etc. CAT describes any system or device to be targeted by the set of information parameters, which the attackers want to gain or modify. Furthermore, the attackers have also information about likewise systems, technical skills, etc. which is helpful in conducting such attacks (Zhuang et al., 2015).

Information security theory

The *information security theory* (IST) states that "Information security is a conscious or subconscious process in which people and organizations attempt to create sustainably viable resources, from information" (Horne et al., 2016). According to the objectives of information, individuals and organizations protect information from risks and threats by applying suitable control measures. Keeping the information protected according to the need of organization and individual make the information sustainable resources. To be more specific, Information security focuses on the protection of information, suitable for the type and sensitivity of the information and its strategic use for the organization (Horne et al., 2016).

System theory

The system-theoretic process analysis is an approach that takes the interaction of each component of a system into account to make a system safer and more secure (Thomas, 2016). It is developed by Leveson to find out hazardous states and unsafe control actions which cause accidents or system losses. In addition, it also generates comprehensive safety requirements to stop the happening of known hazardous scenarios (Leveson, 2004). It integrates factors like software, hardware, human, organizational and safety, etc. for the identification of potential threats and risks (Leveson, 2004).

Causal analysis based on system theory

The causal analysis based on system theory theory states that in order to minimize the risks of accidents and losses, the causes must be identified and analyzed at each component of the system. The objective of this theory is to maximize the learning from incidents and accidents. Although there are some critics of this theory and they believe that it produces too much information to be managed. Yet, it is very helpful in identifying the root cause of any incidents, and the expenditures made in finding those causes or root causes save time and money in the long run (Henderson, 2013).

The above theories show that there are some important factors that must be understood to establish a safe system. For example, the CAT and IST focus on the information and say that in order to make an incident-free system the information must be kept out of the reach of the attackers. Without enough information and knowledge, the attackers are either unable to enter the system or unable to harm a lot. The system theory focuses on the safety measures to be taken at each component of the system, to make the system more secure and protected, and out of the reach of attackers. Even then if an accident occurs, the case analysis theory emphasizes the lesson learned and digging into the root cause of the accident, to plan for the future. Our framework is based upon these theories which is given at the end of discussion section.

Literature review

E-commerce

E-commerce is an enormously growing field that came into being due to the advancement and convergence of technology and the internet, where people do many activities related to commerce. In other words, e-commerce refers to the selling and buying of products online. It involves an online money transfer in exchange for completing the business activity. E-commerce uses digital means to develop and perform different actions and transactions among organizations or groups or between

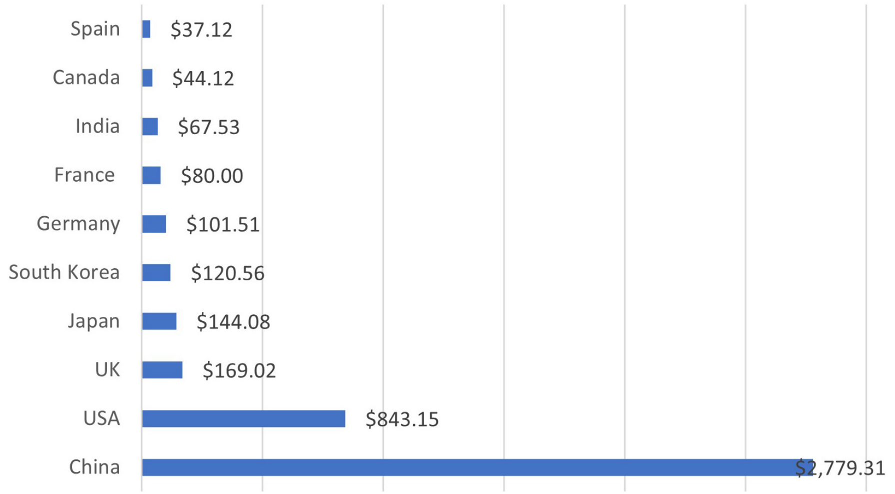

FIGURE 1
E-commerce sale by country (OBERO, 2022a).

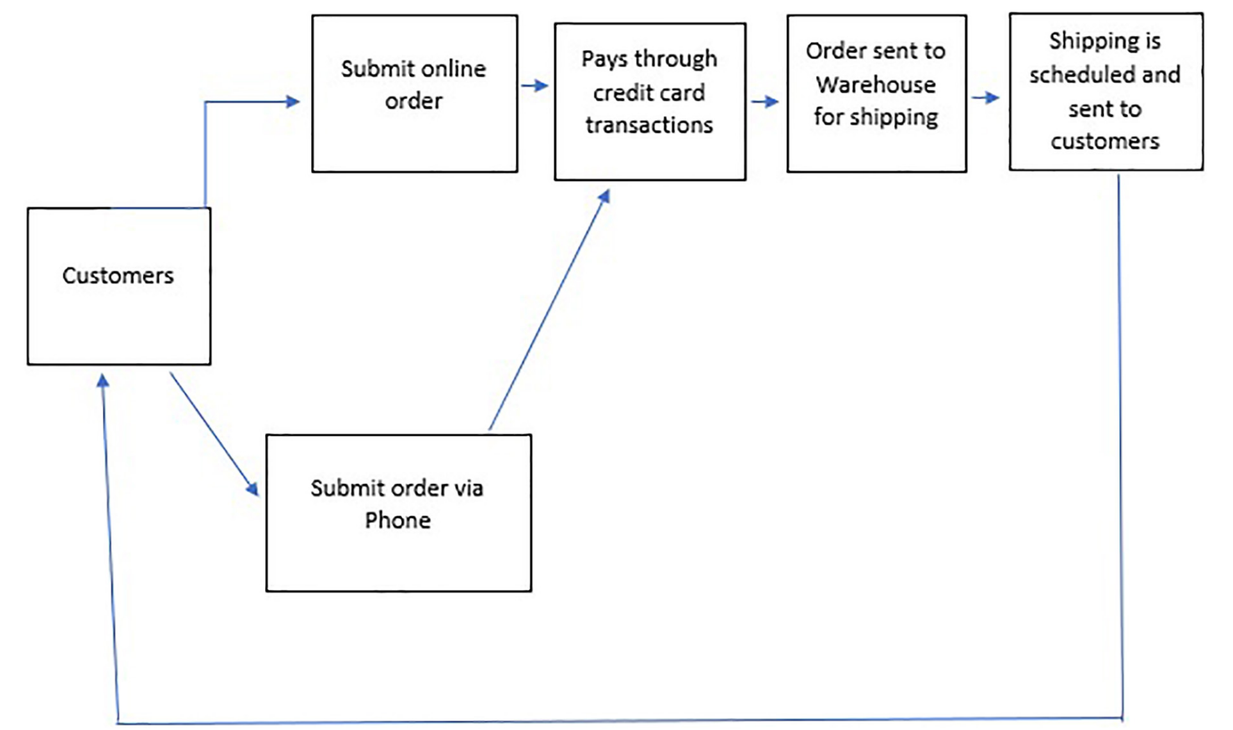
Submit online order
Pays through credit card transactions
Order sent to Warehouse for shipping
Shipping is scheduled and sent to customers
Customers
Submit order via Phone

FIGURE 2
E-commerce workflow diagram (Smart Draw, 2022).

a firm and a customer. According to a study, there are more than 12 million – 24 million e-commerce websites across the globe (Gennaro, 2022). **Figure 1** shows the country-wise e-commerce sale in 2021 (OBERO, 2022a).

In e-commerce, the business process of buying and selling is completed with the help of the internet. The significant e-commerce activities include a selection of a specific product, money transfer, and data exchange (Ahmadian, 2021). Other activities include marketing through the internet, online management systems, and automatic systems for data collection. E-commerce is helping businesses by enlarging their market scope and size; and reducing operating costs and barriers (Lorette, 2022). The research shows that it positively impacts the economy (Anvari and Norouzi, 2016). In e-commerce, a customer buys directly from the online store using mobile applications and websites. Communication can take place through chatbots, live chat, or voice assistants. The **Figure 2** (Smart Draw, 2022) below summarizes the framework of the e-commerce business process from a customer.

The world is shifting from in-store to online shopping, and big companies like Alibaba, Amazon, etc., are leading the transition. Due to this shift, technological advancements are being made to further online business processes (Hooks et al., 2022). E-commerce provides an ease for customers to buy something and has also proved itself one of the powerful agents for business transformation (Li X. et al., 2022; Thomson et al., 2022). The market value of e-commerce in 2021 is given in the following **Figure 3**. It shows that Amazon has the largest share, with a value of 1,634 Billion USD (OBERO, 2022b).

Due to the rapid growth, the firms upgraded their networks, operations, etc., to provide better services to suppliers and customers. E-commerce technology made yesterday's impossible goals for business firms possible by providing them with many opportunities to find and capture new markets and attract customers beyond boundaries (Snihur et al., 2021; Giorgi et al., 2022). Although doing e-commerce has many advantages for business firms and customers, it is impossible without a sophisticated approach to security (Dupont, 2012).

There are four main market sections where e-commerce operates. These sections are Business to Business, where the sale of products is between businesses; Business to Consumer, which involves sales between businesses and consumers; Consumer to Consumer, which allows sale between individuals, and Consumer to Business, where individuals sell to businesses (Shopify, 2022).

It is important to note that in 2020, the e-commerce sales were 4.28 Trillion USD and are expected to reach 5.4 Trillion USD. The e-commerce share was only about 469.2 billion USD in the United States in 2021. The **Figure 4** below shows e-commerce statistics from 2014 to 2024 (Statista, 2022).

The trends and statistics show that e-commerce is a growing field of doing business and is not limited to some specific areas. It

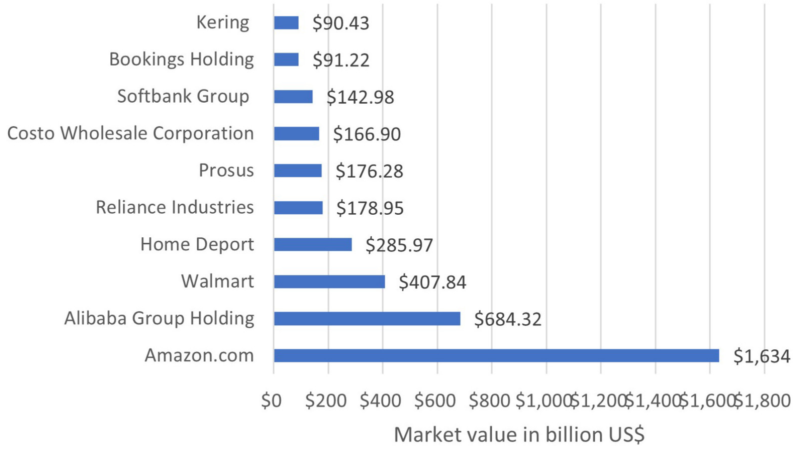

FIGURE 3
Top e-commerce companies by market value (OBERO, 2022b).

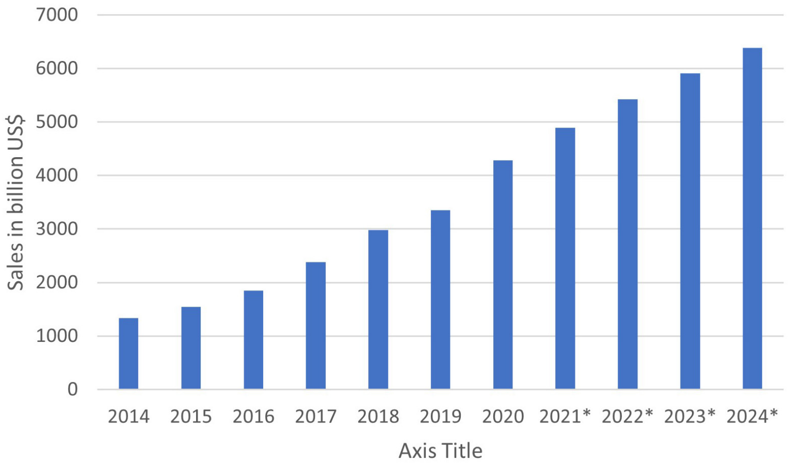

FIGURE 4
E-commerce sales worldwide (Statista, 2022).

is typical for where internet and technology are available across the globe. For example, an industry like tourism is also adopting technology and changing its traditional business. Now sale and purchase of tickets, hotel reservations, etc., can be made with the help of the internet and the relevant technology. The market size of the global online travel agent sector is about 432 Billion USD, the online travel booking platform industry worldwide is about 517 Billion USD and the revenue share of online sales in the global travel and tourism is about 65%.

Therefore, e-commerce technology and firms must be capable of doing business without difficulty and provide their customer with the best possible experience. But as said earlier, as technology is involved between the purchasers and buyers, the activity completes remotely after sharing the required information. E-commerce invites many threats, and cyber security is the most common and severe in them.

Cyber security

One of the most significant challenges e-commerce faces from the beginning is cyber security threats (Kianpour et al., 2021). Cyber security protects computer systems from information disclosure, misdirection, damage, or theft of electronic data, software, or hardware (Schatz et al., 2017). In e-commerce, it is all about electronic security related to e-commerce activity. Business firms continuously invest in technologies to prevent cyber threats, but cyber actors obtain access to business systems and data. The landscape of cybersecurity issues is evolving as cyber actors are searching for new vulnerabilities through different means. On one hand, malicious actors are enhancing their skills and on the other, they are adopting advanced technologies and techniques to target various organizations

(Wirth, 2017). Almost all organizations using internet or computer connectivity, including healthcare, financial firms, transportation, government, and manufacturing industries, are targeted continuously (Strategic Technologies Program, 2022). During the Covid-19 pandemic, the number of attacks were increased by 600% due to the increase in the number of users and dependency on technology. The cost of cybercrime was 3 Trillion USD in 2015, estimated to be 6 trillion USD in 2021 (Morgan, 2017). It is estimated that by 2025, the cost will be 10.5 Billion USD for businesses which is more than the economy of any country after the United States and China (Expert, 2021). This shows how cybersecurity is essential in the current digital and technological era for businesses and organizations, especially those involved in e-commerce (Team, 2022).

It is essential to understand why cybersecurity breaches occur. There are three main reasons for cybersecurity-related issues;

Humans are listed as a significant source of CS by the United States and the United Kingdom (Dykstra, 2017). According to a study, humans are more vulnerable to cause a security breach than technology, i.e., 86, and 63%, respectively, (Metalidou et al., 2014). Another study shows that 80% of cyber-attacks occur due to human-enabled errors (Saeed et al., 2013). Human technology interactions invite security risks, and firms continuously struggle to prevent and mitigate human behavioral-based threats to information security (Nobles, 2015). To obtain a competitive advantage and capture a significant share in the market, business firms adopt and invest in advanced information systems, which often leads to an increase in human mistakes when using the technology. Customers and employees are the weakest link in risk and security management (Alavi et al., 2016). With each passing day, the CS threats are increasing, and firms are continuously adopting and leveraging new technologies to prevent them (Neely, 2017). In addition to inducing the latest technologies to counter the threats, it is also necessary to minimize the behavioral risk associated with humans by adequately training and enhancing their understanding of their interactions with the organization's information systems (Metalidou et al., 2014). As much as human factors are involved in the concerns related to cybersecurity, most organizations have failed to invest in humans to address the issue (Alavi et al., 2016). It is clear that humans cause cybersecurity threats, as a customer may share their information or data incorrectly, with the wrong person, or to a vulnerable information system. Humans as an employee of the business organization may not be able to use the technology properly and may invite severe cybersecurity threats for both the organization and customer. Last but not the least, the employee may use the information (consumer and organizational) for their personal gain. In all form, human poses a serious threat and it is a big challenge for e-commerce to address.

Technology: In addition to the human factor associated with cyber threats, the second potential threat is the technology itself. Cybercriminals are taking advantage of vulnerabilities induced by the technology, hyper-connected systems, human-enabled errors, and organizations not prepared to prevent or counter such attacks. The most common cyber threats noted in 2021 are phishing, social engineering, credential theft, and compromised or stolen devices with 57, 30, and 33%, respectively, (Team, 2022). Other common threats are spyware, ransomware, trojans, etc. (kaspersky, 2022). A study shows that "-about 81% of breaches resulted from weak or stolen passwords, 62% of breaches stemmed from hacking, 51% of breaches involved malware, and 43% of breaches were social engineering attacks" (Verizon, 2017). One of the most significant sources of cybersecurity issues is the hyper-connectivity of technology in the modern era and the dependency of business and commerce on these hyper-connected systems (Abdel Hakeem et al., 2022). It refers to the networked societies or technologies with each other and the various ways of communication like email, instant messaging, etc. In the context of e-business or e-commerce, it is about the connectivity of an organization's information system having enormous records with the outside world. This connectivity makes it vulnerable to cybercriminals who take advantage of it.

Non-preparedness: Another reason for cybersecurity threats is non-preparedness (Pusey and Sadera, 2011). Many organizations are unprepared for cyberattacks (Abdelhamid et al., 2019). Either they lack advanced protocols and tools to prevent counter-cyberattacks (Zwilling et al., 2022), or do not respond well (Akpan et al., 2022). Due to their un-preparedness, the attackers take advantage of the opportunity.

The severity of non-preparedness in cybersecurity threats in the modern electronic era is evident from the statistics that only in 2021, 21.8 Billion USD was poured into cybersecurity compared to 5.1 Billion USD in 2017, 5.9 Billion USD in 2018, 8.3 Billion USD in 2019, and 8.9 Billion USD in 2020. In addition, if we look at the data, the last quarter of 2021 witnessed the highest amount of 7.8 Billion USD investment in cybersecurity as shown in **Figure 5** (Metinko, 2022).

Figure 5 above shows that the investment in cybersecurity is increasing yearly with rapid growth in 2021. It is also evident from the **Figure 6** that in each coming quarter, the amount for cybersecurity funding increased with a sudden high increase in the last quarter of 2021 from 3.9 Billion USD in the first quarter, 5.3 Billion USD in the second quarter, 4.8 Billion USD in the third quarter and 7.8 Billion USD in the fourth one (Metinko, 2022). To summarize the discussion, the challenge of the cybersecurity landscape is getting worse, and the actors are becoming more experienced and acquiring

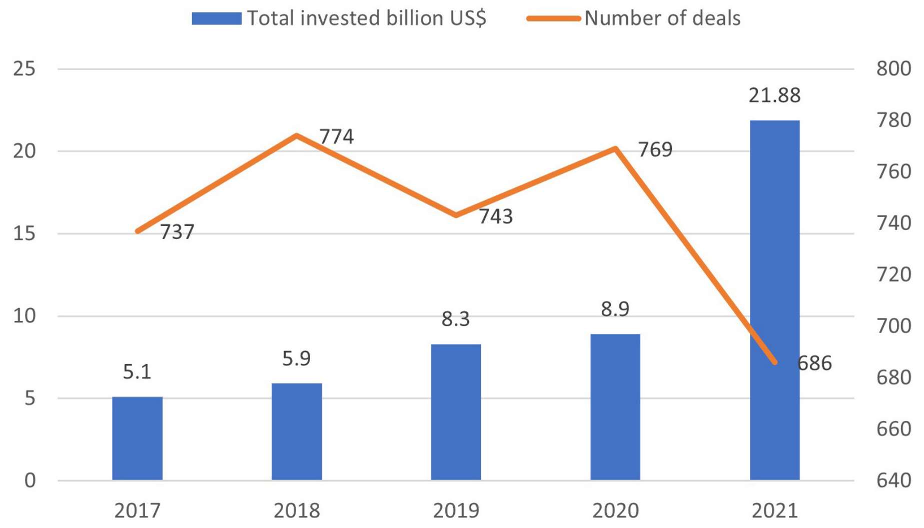

FIGURE 5
Investment in cybersecurity (Metinko, 2022).

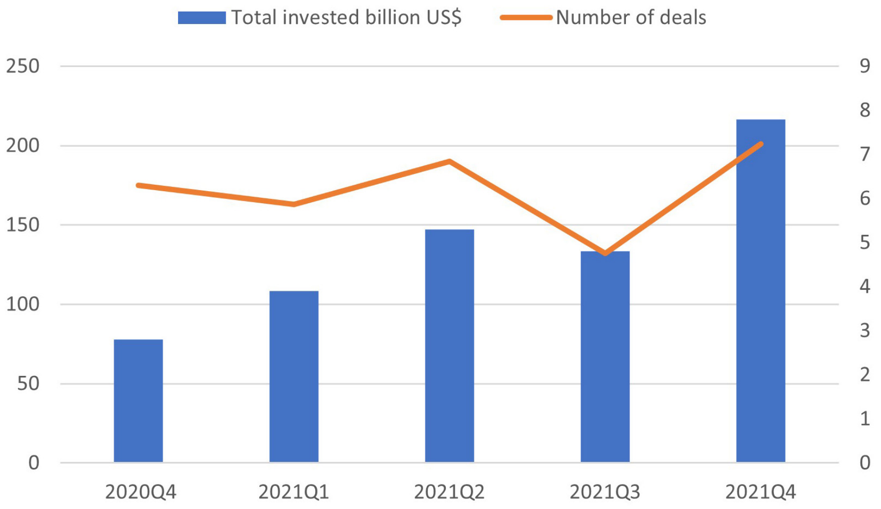

FIGURE 6
Investment in cybersecurity quarterluy (Metinko, 2022).

more sophisticated ways for attacks. This not only increased the number of data breaches, etc. but also threatened the e-commerce organization.

Social engineering

Social Engineering is the most common type of scam, that cybercriminals use (Nick Galov, 2022). It is any activity that influences a person's behavior for taking an action that is not necessarily in their interest (Social-engineer, 2022). It is the psychological manipulation of compelling customers to perform various tasks, activities, etc., and to expose or reveal their confidential information. It may be one step trick or maybe of many steps, but the purpose remains the same, to collect conditional details or to get access to the system (Anderson, 2008). The simplest example of social engineering is the "forget password" option which, after clicking, may direct the user to a malicious link and grant access to the attackers to the user account or system.

Similarly, the original user will no more able to access the invoice (Purplesec, 2022). The target of social engineering may be a firm's top executives or a student. In other words, anyone can be a target of social engineering attackers (Sanders, 2022). The severity of social engineering can be seen from the statistics that about 98% of cyber-attacks come from this threat (Purplesec, 2022). The most common techniques used in malicious social engineering are:

Phishing: Where the attacker sends emails showing that it is coming from a reputable source and ask for information. Through this process, the criminal gathers personal data and uses it accordingly (Phishing, 2022). Phishing websites are 75 times more than malware, and about 70% of the companies worldwide were a victim in 2020 (Galov, 2022). Only in 2020, business losses were $1.8 billion due to it (Purplesec, 2022).

Vishing: Where the attacker uses a telephone call to attempt or to encourage an action. The purpose is to gather data and obtain valuable information necessary for a firm or individual to compromise (Olson, 2018). Only in 2021, there was a 554% increase in the volume of vishing attacks, which is about 27% of the overall response-based threats. It can be seen from these statistics that it will further increase in the future (LaCour, 2022).

Impersonalization: The attacker presents itself as another person or firm and gets socialized to obtain and gather information or access to a firm, system, etc. (Easydmarc, 2021). Between 2020 and 202, there was a 131% increase in personalization, costing 1.8 Billion USD to the targeted enterprises (Securitymagazine, 2022).

Smishing: Where the attacker is sending messages on the phone to influence the immediate actions of a victim, like direction to visit a malicious website, downloading something, etc. (Hughes, 2021). It is reported that smishing scams only rose by about 328% in 2020.

In e-commerce, when a customer enters a website or page, the attackers socialize and get the data after making a trustful relationship and then use the information or data for personal use. It is not necessarily that the victim must be a new one, but maybe anyone, regardless of his experience, education, and position, might be on target.

Attack on customer personal data

Targeting personal data is also one of the significant challenges e-commerce is facing. As the world is getting more digitized, the amount of data (firm's data and customer data) shared, stored, and saved on systems and online; is also increasing daily to a tremendous huge volume (Zende, 2022). Similarly, access and utilization of the data and network are also growing. This increases the risk of cybercrime in the form of an attack for retrieving confidential data and also decreases the trust of customers and firms in each other (Hussien et al., 2022). In e-commerce, the customer must share their private information with the organization, making it capable of knowing and recording much information about the customers (Vasupula et al., 2022). For example, home address, phone number, bank card number, date of birth, etc. The online store or company may also record your purchasing history and compare it with your buying details.

There are two main types of attacks on personal data:

1. The online store or organization can use the customer personal information without consent.
2. The data can be attacked and used by cyber attackers, who do not belong to the online firm but from outside and want to steal data.

Only in 2019, around 15 billion data records were compromised (Security Magazine, 2020). It means that concern regarding the attacks on customer personal data is the number one challenge for e-commerce. The customers and e-commerce companies need to understand the risks associated with customer data and the cost of the breach (Varga, 2021). It is a fact that we are living in an information age and information is the most precious asset of this era. Based on the information, organizations design their strategies, plan their products and services, and invest. Also, sharing information with someone or some organization needs a significant trust from the party sharing its information and doing so for a purpose. It is the organization's responsibility to keep the information safe and protected from illegal use to maintain the customer's trust and use it in a competitive strategic manner. Suppose the attackers successfully steal the customer information. In that case, it will hurt the customer's trust and the organization will be no more able to behave in a competitive strategic manner in the market.

Distributed denial of service attacks

It is a type of cyber-attack in which the criminal tries to make the service or system unavailable to the users by disrupting the services through different means (Ncsc, 2022). The most common denial of the service attack method is sending a flood of requests to overload the system and prevent legitimate submissions. Most traffic flooding comes from more than one source, and it is difficult to stop the attack (Fortinet, 2022). In a DDoS attack, the attackers continuously send requests from many authorities to get the web resource down. In e-commerce, for example, they flood the online store, etc., with massive traffic and make the customers unable to purchase something (Anshari et al., 2022). This leads to the disability of the online firm for hours or even for several days. And if the attack is in peak season, it is more annoying and severe; it may cost a considerable amount in the form of customer and income loss (Dahiya and Gupta, 2020).

The primary purpose is to make service delivery impossible by thwarting online firm or store access. It can be of many forms and depends upon the purpose of the attackers and the nature of the e-commerce firm or store (Mishra et al., 2022). There are three main types of DDoS attacks (Fruhlinger, 2022):

1. *Volume-based:* The attackers use considerable traffic to make a resource (server or a website) unavailable (Fruhlinger, 2022).
2. *Network layer:* The attackers use many data packets to target the network infrastructures (Gargar, 2021).
3. *Application layer:* Here, the attackers use maliciously crafted requests to flood the applications and make them unavailable to genuine customers (Gargar, 2021).

It is one of the most significant cybersecurity issues of e-commerce, where the criminals make the e-commerce source or resource unavailable or unreachable to the customers. Availability of service is an essential part of attracting users. For example, if a service is available and its quality is better than that of competitors, people will get automatically drawn to it. In other words, if a service is unavailable, it will not attract people and if the quality is not good, again, the people will opt for a better service. In both cases, there is a loss. Therefore, e-commerce organizations must make sure that their service is available with better quality than competitors. Their system must have the capability to detect DDoS attacks and responds promptly.

Malware (malicious software)

Malware is any software that could infect computers, and cybercriminals use it to insert it on target websites (CYBER EDU, 2021). The primary purpose is to obtain personal data like passwords, account details, money stealing, or blocking the system owner from using it (Lutkevich, 2021). Usually, this way, the user gets misled and is redirected to another website or page. Malware attacks are widespread attacks that execute illegal activities on the victim's system. It may be ransomware, control of the device, or spyware (Rapid7, 2022). Malware is designed to interrupt or malfunction a server, computer, or computer network. After gaining unauthorized access to the system, it breaks security and privacy and obtains private information (Brewer, 2016). Common types of malware are worms, viruses, trojans, ransomware, horses, spyware, rogue software, scareware, adware, etc. It is challenging to address all types of threats with the same strategy because each type needs its defense strategy like antivirus, firewalls, algorithms, etc. (Xiao et al., 2020). It is a severe problem for e-commerce (Kim et al., 2018). The number of attacks through malware is a serious threat to e-commerce as the number of attacks is increasing yearly by a significant proportion. There were 670,000,000 malware variants in 2017, almost double the number in 2016 (Xiao et al., 2020).

The development and application of modern technology have a lot of advantages for the business sectors but also bring threats in the form of malware. The number of incidents and threats increases yearly as the technology develops and its applications enter new boundaries. It is necessary for the e-commerce organizations that the technology they are using must have the capabilities to detect malicious software and prevent them from entering their system. Again, it can target the organization and its customers; both need to know about it and use secure technology and service.

Discussion

In the contemporary era, technology is everywhere, in education (Ahmad et al., 2021), assisting in academics and administration tasks (Ahmad et al., 2022) to business (Ibrahim et al., 2014), from marketing to industry (Sayed et al., 2020), from health to space sciences, etc. Trade and commerce are tremendously influenced by digital technologies, which changed the business mood from traditional/conventional to electronic (den Hond and Moser, 2022). Due to technology, not only did the business sector find new opportunities but also expanded beyond geographical limits. Technology enabled the sustainability of e-commerce in the recent Covid-19 pandemic, and enormous growth was witnessed (Stalmachova et al., 2021). But some concerns need to be explored for sustainable and successful e-commerce using technology. The most common among them is cybersecurity threats. E-commerce sites are always targeted for cybercrimes in the form of cyberattacks. Cybercriminals or attackers target e-commerce firms through different means for different purposes. They aim to steal private data like personal information, account details, or financial data and compromise the system not to work correctly. Usually, e-commerce firms of all sizes are on target. The most common cyberattacks are Pishing, denial of service, social engineering, malware, direct access attacks, reverse engineering, spoofing, etc.

The word of e-commerce stands for electronic commerce or the commerce done with the help of electronic technology, the application of technology is increasing daily in e-commerce (Rahman, 2014). Firms are also adopting/implementing technologies without any delay to reach customers and capture market share (Kramer, 2022). There is never-ending competition among the firms in almost all sectors (Wall, 2022). Now each product is available online, from books to medicine, from ticket booking to hotel booking, etc. Also, the customers are looking for their comforts and need fulfillment from buying through trustworthy means (Joyce, 2022). E-commerce is the platform that provides products and services according to the customer's needs. In an e-commerce environment, the customer can explore the market with the help of a few clicks and quickly find out the difference in product quality, price, and delivery time and compare with the other service providers in the market. So this makes a win-win situation for the customers. But searching different websites/pages and clicking various links are not free from the threats. Sometimes it becomes difficult to differentiate between the actual website and the one aimed at cybercrimes. Sharing information like name, address, account details, phone numbers, etc., may reach the wrong place or person through these websites. Not only the criminals who steal customer information through social engineering, phishing, malware, etc. the same can also attack the e-commerce organization in the same manner (Li and Liu, 2021). Competitors may also pose a severe cybersecurity threat by hacking access to an e-commerce website, DDoS, etc. They may also attack to stole customer information and the selling records of an organization. Such records are the backbone of strategic planning and mean a lot to the e-commerce organization (Hepfer and Powell, 2020).

To address the issue of cybersecurity threats, e-commerce organizations are investing a lot to get rid of it (Team, 2022). The statistics show that the investment to address the issue is increasing each year, but the number of attacks is also growing. It means that the problem can't be resolved without advanced technology. One reason for this is that new people are getting inclined to avail e-commerce and are more vulnerable than the old user. Hackers, attackers, or cybercriminals are also enhancing their skills and searching for vulnerabilities in the technology, etc. It is a fact that there are many other cybersecurity threats besides social Engineering, denial of services, malware and attacks on personal data were discussed in this study. Based on the review, it is evident that cyber-attacks negatively impact businesses in two ways.

1. The cost of a data breach.
2. Losing the customer trust.

As discussed earlier, e-commerce business firms are continuously investing to address cybersecurity concerns, which are increasing yearly (Vinoth et al., 2022). The governments are also making laws and policies regarding this issue (Luo and Choi, 2022). Still, criminals are also finding new methods to target a customer or firm as technology develops. Similarly, firms support implementing innovative and trustful technologies and tools on their websites to remain competitive and maintain the trust of their customers (Gull et al., 2022). On the other hand, researchers are also continuously enhancing the technology, e.g., work has been done to improve the effect of false alarm detection and then more accurately identify real alarms (Li S. et al., 2022), and various tools were proposed for phishing detection (Gupta et al., 2021). Also, researchers are developing new methods and frameworks to find out the vulnerabilities (Cvitić et al., 2021). Work has been done to develop a botnet defense system to exterminate malicious botnets and make the technology usage more secure (Pan et al., 2021). But on the other hand, the attackers are searching for vulnerabilities, and the never-ending game of mouse and cat continues. Block chain technology is another option for e-commerce trust and security (Centobelli et al., 2021a) and digitalization (Cerchione et al., 2022). It may also shape the future of decentralized technologies also (Centobelli et al., 2021b).

We divide the cyber security concerns in e-commerce at three different levels and proposed the following framework as shown in **Figure 7**.

1. *Human:* Cyber security issues occur due to humans (employees, attackers, and consumers) either lacking the proper knowledge and skills to use the e-commerce technology or not following the protocols related to Cyber security (Zhuang et al., 2015). And if they are attackers, then they know more about the technology, organization, and the users of the technology, i.e., they possess more information. Employees and customers, who are using a particular e-commerce technology must have sufficient knowledge, skills, and information to use the technology properly and to complete a business transaction successfully (Al-Ghamdi, 2021). They also need to have information about the technology and organization and must know the vulnerabilities in both. With the help of information, cybersecurity threats could be minimized as the employees and customers will always be alert where there is some vulnerability. And to a greater extent, they are well aware of the attackers, and what and how they attempt (Zwilling et al., 2022).
2. *Organization:* At the organizational level, security concerns occur due to inadequate rules, regulations, and policies to implement the security protocols and use the systems according to the law. If cybersecurity is not the theme of an e-commerce organization's strategy, it is impossible to address it. Organizations need to invest in training, enhancing security controls and measures, and must continuously be searched for the vulnerabilities and their possible solution at the management level (Roumani et al., 2015). If it ignores the need for something that should be done to address cybersecurity threats, they may become a cause of potential damage in the future (Guembe et al., 2022). Organizations should adopt new procedures and policies to overcome the cybersecurity threats as per market demand, organizational need, and attackers' skills and knowledge.
3. *Technology:* E-commerce organization often does not invest much to implement a suitable and safe technology, due to which cybersecurity risks increase (Guembe et al., 2022). It is necessary for e-commerce organizations to invest significantly in hiring new and more secured technology (Dobrowolska, 2020). Maybe it is expensive but more beneficial in the longer term (Koomey, 2012).

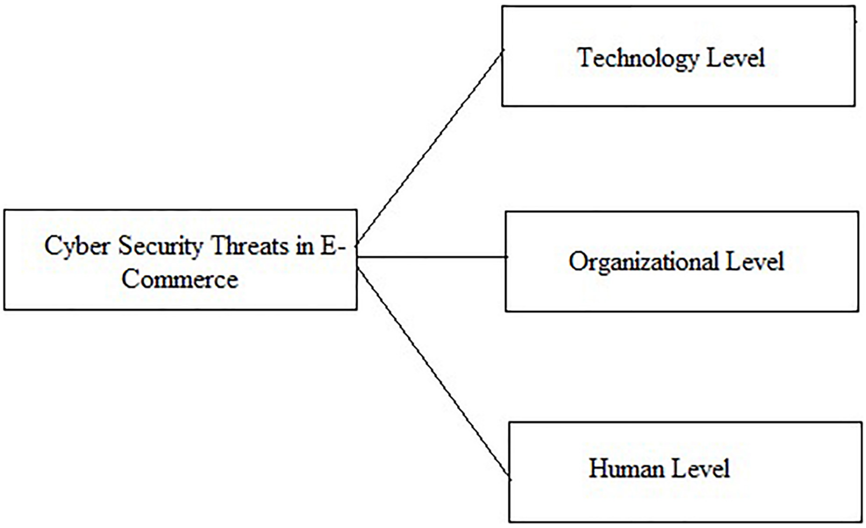

FIGURE 7
Conceptual framework for cybersecurity in e-commerce.

Conclusion

The name of e-commerce is attractive and the need of the modern-day business market, but it is facing the challenge of cyber security threats. Although firms continuously invest a lot to address the issue, it is not easy. Personal and organizational data are often the target of cyber-attacks. Without a doubt, technology offers new ways of doing business and provides many additional benefits, but cyber security concerns will always be there. Investing and enhancing the security of e-commerce is substantially essential for getting a competitive advantage and for the success of e-commerce business (Hepfer, 2021). No one can afford the price of customers' trust; they lose because of the exposition of their data. Strong monitoring protocols must be followed before any mishap on both organizational and customer ends. For example, strong passwords and being cautious about clicking and downloading something. Taking advance precautions and investing in a secure version of the technology in e-commerce is the need of the day.

We conclude that no matter how much the employees and consumers are trained and skilled to do e-commerce, how much the e-commerce firm implements and focuses on the implementation of cyber security protocols and policies; and how much-advanced technology is used for conducting the e-commerce business activities; the challenge of cyber security threats will always be there like a sword to hurt the business and no one knows when.

Recommendation

With each passing day, the involvement of technology is increasing with a surprising speed in doing business, i.e., in e-commerce. And to be honest, we cannot escape from its applications or ignore its benefits. But the technological transformation in the form of e-commerce has the foremost challenge of cyber security threats. No matter in e-commerce, the technology we are using today, no matter how trained we are to use a particular technology, and no matter what precaution measures we take, the cybersecurity concerns will always be there for various reasons. We put the following four questions before e-commerce organizations to be answered for sustainable and less risky business activities.

1. Is your organization always ahead and aware of cybersecurity concerns and of advanced practices to address them?
2. Do the technology you are using or implementing for doing an e-commerce business enough secured to face cyber-attacks?
3. What was the impact of any cyber-attack on this technology when it was targeted somewhere or in this organization?
4. Do you have an effective and efficient policy or protocols regarding using technology or doing activities to minimize or overcome cyber threats, etc.?
5. Are you prepared for starting or continuing e-commerce without cyber security threats? Are you ready to handle such situations?

Implication/contribution

Theoretical contribution

This conceptual analysis analyzes the cybersecurity threats in e-commerce. It explores that cybersecurity is a potential threat to e-commerce and must attract more attention than the present, according to the statistics analyzed (Furner, 2004).

Managerial implications/contribution

The study has the following implications for managers.

1. Without a doubt, modern technology is the need of the day and its applications in business is an irrevocable fact. Managers should take full advantage of modern technology and implement it to capture a larger market and business expansion volume. But they should also be aware of the cyber security threats coming with using and implementing new technology. They should select the appropriate technology to ensure cyber security and train their emplyees how to use it and respond in an unwanted situation.
2. The challenges come with technology, and often, the organization's employees have less understanding of the new technology. This study highlights the importance of employees' knowledge about technology usage and managers should provide proper training to the employees to minimize the risks coming from cybersecurity threats.
3. In short, managers can use this work to choose a secured technology for their e-commerce operations and continuously invest in addressing emerging cybersecurity threats.

Future work

1. Many other factors related to cyber security were not studied in this study due to its limited scope, and they can be explored in future studies.
2. Addressing the questions as recommended above are also significant areas for future work.
3. Quantitative analysis of this study to make it more generalized.
4. Research on block chain technology in e-commerce can be done in future to make it more trustworthy (Centobelli et al., 2021a).
5. Similar research can be done on knowledge management in e-commerce to address the contemporary challenges (Castagna et al., 2020).
6. Research can also be done on the social, economic and environmental issues and impact of cybersecurity and e-commerce.

Limitation

The scope of cyber security and e-commerce is comprehensive, and this work is limited to its scope as a perspective work. Explorative, qualitative, and quantitative research with a much broader scope is needed to discover other sides of this study.

Author contributions

SFA and SA contributed to conceptualization, writing – original draft, and methodology. XL contributed to supervision. JK contributed to formal analysis. MA contributed to variable construction. MI contributed to funding acquisition. MI and JU-H contributed to data handling. All authors have read and agreed to the published version of the manuscript.

Acknowledgments

We acknowledge the role of our teachers, supervisors, and friends, who supported us throughout the journey.

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

References

Abdel Hakeem, S. A., Hussein, H. H., and Kim, H. (2022). Security requirements and challenges of 6G technologies and applications. *Sensors* 22:1969. doi: 10.3390/s22051969

Abdelhamid, M., Kisekka, V., and Samonas, S. (2019). Mitigating e-services avoidance: the role of government cybersecurity preparedness. *Inform. Comput. Secur.* 27, 26–46. doi: 10.1108/ICS-02-2018-0024

Ahmad, S. F., Alam, M. M., Rahmat, M. K., Mubarik, M. S., and Hyder, S. I. (2022). Academic and administrative role of artificial intelligence in education. *Sustainability* 14:1101. doi: 10.3390/su14031101

Ahmad, S. F., Rahmat, M. K., Mubarik, M. S., Alam, M. M., and Hyder, S. I. (2021). Artificial intelligence and its role in education. *Sustainability* 13:12902. doi: 10.3390/su132212902

Ahmadian, S. (2021). Review of e-commerce service delivery models. *Arman Process J.* 2, 14–20.

Akpan, F., Bendiab, G., Shiaeles, S., Karamperidis, S., and Michaloliakos, M. (2022). Cybersecurity challenges in the maritime sector. *Network* 2, 123–138. doi: 10.3390/network2010009

Alavi, R., Islam, S., and Mouratidis, H. (2016). An information security risk-driven investment model for analysing human factors. *Inform. Comput. Secur.* 24, 205–227. doi: 10.1108/ICS-01-2016-0006

Al-Ghamdi, M. I. (2021). Effects of knowledge of cyber security on prevention of attacks. *Mater. Today Proc.* doi: 10.1016/j.matpr.2021.04.098

Anderson, R. J. (2008). "A guide to building dependable distributed systems," in *Security engineering*, 2nd Edn, (Hoboken, NJ: Wiley).

Anshari, M., Almunawar, M. N., and Al-Mudimigh, A. (2022). "Digital marketplace as a new frontier of electronic commerce," in *Handbook of research on big data, green growth, and technology disruption in asian companies and societies*, (Hershey: IGI Global), 122–137. doi: 10.4018/978-1-7998-8524-5.ch007

Anvari, R. D., and Norouzi, D. (2016). The Impact of E-commerce and R&D on economic development in some selected countries. *Proc. Soc. Behav. Sci.* 229, 354–362. doi: 10.1016/j.sbspro.2016.07.146

Bigcommerce (2022). *What you need to know about securing your ecommerce site against cyber threats*. Available online at: https://www.bigcommerce.com/articles/ecommerce/ecommerce-website-security/ (accessed April 10, 2022).

Brewer, R. (2016). Ransomware attacks: Detection, prevention and cure. *Netw. Secur.* 2016, 5–9. doi: 10.1016/S1353-4858(16)30086-1

Burton, W. (2007). *Burton's legal thesaurus*, 4 Edn. New York, NY: McGraw-Hill Education.

Castagna, F., Centobelli, P., Cerchione, R., Esposito, E., Oropallo, E., and Passaro, R. (2020). Customer knowledge management in SMEs facing digital transformation. *Sustainability* 12:3899. doi: 10.3390/su12093899

Centobelli, P., Cerchione, R., Esposito, E., and Oropallo, E. (2021a). Surfing blockchain wave, or drowning? Shaping the future of distributed ledgers and decentralized technologies. *Technol. Forecast. Soc. Change* 165:120463. doi: 10.1016/j.techfore.2020.120463

Centobelli, P., Cerchione, R., Vecchio, P., Del, Oropallo, E., and Secundo, G. (2021b). Blockchain technology for bridging trust, traceability and transparency in circular supply chain. *Inform. Manag.* 103508. doi: 10.1016/j.im.2021.103508

Cerchione, R., Centobelli, P., Riccio, E., Abbate, S., and Oropallo, E. (2022). Blockchain's coming to hospital to digitalize healthcare services: Designing a distributed electronic health record ecosystem. *Technovation.* 102480. doi: 10.1016/j.technovation.2022.102480

Cvitić, I., Peraković, D., Periša, M., and Gupta, B. (2021). Ensemble machine learning approach for classification of IoT devices in smart home. *Intl. J. Mach. Learn. Cybern.* 12, 3179–3202. doi: 10.1007/s13042-020-01241-0

CYBER EDU (2021). *What is Malware? ForcePoint.* Available online at: https://www.forcepoint.com/cyber-edu/malware (accessed March 20, 2022).

D'Adamo, I., González-Sánchez, R., Medina-Salgado, M. S., and Settembre-Blundo, D. (2021). E-Commerce calls for cyber-security and sustainability: How european citizens look for a trusted online environment. *Sustainability* 13:6752. doi: 10.3390/su13126752

Dahiya, A., and Gupta, B. B. (2020). An economic incentive-based risk transfer approach for defending against DDoS attacks. *Intl. J. E-Serv. Mob. Appl.* 12, 60–84. doi: 10.4018/IJESMA.2020070104

den Hond, F., and Moser, C. (2022). Useful servant or dangerous master? Technology in business and society debates. *Bus. Soc.* 1–30. doi: 10.1177/00076503211068029

Dobrowolska, K. (2020). *Modern technology implementation: Costs and benefits*. Availble online at: https://archdesk.com/blog/modern-technology-implementation-costs-and-benefits/ (accessed February 2, 2022).

Dupont, B. (2012). *The cyber security environment to 2022: Trends, drivers and implications*. Available online at: https://ssrn.com/abstract=2208548 (accessed February 20, 2022).

Dykstra, J. (2017). *Cyber issues related to social and behavioral sciences for national security. National Security Agency. White Paper.* Availble online at: https://sites.nationalacademies.org/cs/groups/dbassesite/documents/webpage/dbasse_177250.pdf (accessed January 2, 2022)

Easydmarc. (2021). *Impersonation. easydmarc.com*. Available online at: https://easydmarc.com/blog/what-is-an-impersonation-attack (accessed March 20, 2022).

Expert, S. (2021). *Cybersecurity, cyberlaw, cybercrime to cost over $10 Trillion by 2025.* Available online at: https://securityboulevard.com/2021/03/cybercrime-to-cost-over-10-trillion-by-2025/ (accessed March 20, 2022).

Fortinet (2022). *Distributed Denial-of-Service (DDoS) attacks meaning and prevention*. Available online at: https://www.fortinet.com/ (accessed March 20, 2022).

Fruhlinger, J. (2022). *DDoS attacks: Definition, examples, and techniques.* Available online at: https://www.csoonline.com/article/3648530/ddos-attacks-definition-examples-and-techniques.html (accessed March 24, 2022).

Furner, J. (2004). Conceptual Analysis: A method for understanding information as evidence, and evidence as information. *Arch. Sci.* 4, 233–265. doi: 10.1007/s10502-005-2594-8

Galov, N. (2022). *17+ sinister social engineering statistics for 2022.* Available online at: https://webtribunal.net/blog/social-engineering-statistics/#gref (accessed March 20, 2022).

Gargar, D. (2021). *Do network layer and application layer DDoS differ*. Available online at: https://vaporvm.com/do-network-layer-and-application-layer-ddos-attacks-differ (accessed March 20, 2022).

Gennaro, L. (2022). *68 Useful ecommerce statistics you must know in 2022.* Available online at: https://wpforms.com/ecommerce-statistics/ (accessed April 1, 2022).

Giorgi, G., Ariza-Montes, A., Mucci, N., and Leal-Rodríguez, A. L. (2022). The dark side and the light side of technology-related stress and stress related to workplace innovations: From artificial intelligence to business transformations. *Intl. J. Environ. Res. Public Health* 19:1248. doi: 10.3390/ijerph19031248

Guembe, B., Azeta, A., Misra, S., Osamor, V. C., Fernandez-Sanz, L., and Pospelova, V. (2022). The emerging threat of ai-driven cyber attacks: A Review. *Appl. Artif. Intell.* 1–34. doi: 10.1080/08839514.2022.2037254

Gull, H., Saeed, S., Iqbal, S. Z., Bamarouf, Y. A., Alqahtani, M. A., Alabbad, D. A., et al. (2022). An empirical study of mobile commerce and customers security perception in Saudi Arabia. *Electronics* 11:293. doi: 10.3390/electronics11030293

Gupta, B. B., Yadav, K., Razzak, I., Psannis, K., Castiglione, A., and Chang, X. (2021). A novel approach for phishing URLs detection using lexical based machine learning in a real-time environment. *Comput. Commun.* 175, 47–57. doi: 10.1016/j.comcom.2021.04.023

Henderson, J. P. (2013). *Causal analysis based on system theory/CAST Handbook.pdf.* Available online at: https://github.com/joelparkerhenderson/causal-analysis-based-on-system-theory/blob/main/CAST_Handbook.pdf (accessed April 15, 2022).

Hepfer, M. (2021). *Gaining competitive advantage from cybersecurity*. Available online at: https://istari-global.com/insights/perspectives/gaining-competitive-advantage-from-cybersecurity/ (accessed April 2, 2022).

Hepfer, M., and Powell, T. C. (2020). *Make cybersecurity a strategic asset.* Cambridge, MA: MIT Sloan Management Review.

Hooks, D., Davis, Z., Agrawal, V., and Li, Z. (2022). Exploring factors influencing technology adoption rate at the macro level: A predictive model. *Technol. Soc.* 68:101826. doi: 10.1016/j.techsoc.2021.101826

Horne, C. A., Ahmad, A., and Maynard, S. B. (2016). "A Theory on information security," in *proceedings of the Australasian Conference on Information Systems.* Wollongong, NSW.

Hughes, M. (2021). *What is smishing? How text messaging scams work and why a 'skeptical pause' can save you*. Available online at: https://auth0.com/blog/what-is-smishing/ (accessed March 2, 2022).

Hussien, F. T. A., Rahma, A. M. S., and Wahab, H. B. A. (2022). Design and implement a new secure prototype structure of e-commerce system. *Intl. J. Electrical Comput. Eng.* 12, 2088–8708.

Ibrahim, M., Shahid, M. K., and Ahmed, S. F. (2014). The Impact of Telecom Services Characteristics on Consumer for Use in Pakistan. *Adv. Econ. Bus.* 2, 172–179. doi: 10.13189/aeb.2014.020403

Jang-Jaccard, J., and Nepal, S. (2014). A survey of emerging threats in cybersecurity. *J. Comput. Syst. Sci.* 80, 973–993. doi: 10.1016/j.jcss.2014.02.005

Jennifer. (2022). *Top E-commerce challenges facing SMBs. business news daily*. Availble online at: https://www.businessnewsdaily.com/6028-small-ecommerce-challenges.html (accessed March 23, 2022).

Joyce, S. (2022). *Four steps to gaining consumer trust in your tech. PWC*. Available online at: https://www.pwc.com/us/en/tech-effect/cybersecurity/trusted-tech.html (accessed April 11, 2022).

kaspersky (2022). *What are the different types of malware? Resource-Center*. Availble online at: https://www.kaspersky.com/resource-center/threats/types-of-malware (accessed April 9, 2022).

Khurana, A. (2019). *"Did You Know That There Are 4 Types Of Ecommerce?". The Balance Small Business*. New York, NY: Dotdash.

Kianpour, M., Kowalski, S. J., and Øverby, H. (2021). Systematically understanding cybersecurity economics: A Survey. *Sustainability* 13:13677. doi: 10.3390/su132413677

Kim, J.-Y., Bu, S.-J., and Cho, S.-B. (2018). Zero-day malware detection using transferred generative adversarial networks based on deep autoencoders. *Inform. Sci.* 461, 83–102. doi: 10.1016/j.ins.2018.04.092

Koomey, J. (2012). *The benefits of information technology outweigh the costs*. New York, NY: The New York Times.

Kramer, L. (2022). *What strategies do companies employ to increase market share?*. Available online at: https://www.investopedia.com/ask/answers/031815/what-strategies-do-companies-employ-increase-market-share.asp (accessed April 20, 2022).

LaCour, J. (2022). *Vishing volume increases 554% in 2021*. Availble online at: https://www.phishlabs.com/blog/vishing-volume-increases-554-in-2021 (accessed March 27, 2022).

Leveson, N. (2004). A new accident model for engineering safer systems. *Saf. Sci.* 42, 237–270. doi: 10.1016/S0925-7535(03)00047-X

Li, S., Qin, D., Wu, X., Li, J., Li, B., and Han, W. (2022). False alert detection based on deep learning and machine learning. *Int. J. Semant. Web Inf. Syst.* 18, 1–21. doi: 10.4018/IJSWIS.297035

Li, X., Voorneveld, M., and de Koster, R. (2022). Business transformation in an age of turbulence–lessons learned from COVID-19. *Technol. Forecast. Soc. Change* 176:121452. doi: 10.1016/j.techfore.2021.121452

Li, Y., and Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Rep.* 7, 8176–8186. doi: 10.1016/j.egyr.2021.08.126

Lorette, K. (2022). *How ecommerce can reduce business transaction costs. Small business*. Available online at: https://smallbusiness.chron.com/adobe-creative-cloud-grow-business-13771091.html (accessed April 13, 2022).

Luo, S., and Choi, T. (2022). E-commerce supply chains with considerations of cyber-security: Should governments play a role? *Prod. Oper. Manage.* 31, 2107–2126. doi: 10.1111/poms.13666

Lutkevich, B. (2021). *Network security. Techtarget*. Available online at: https://www.techtarget.com/searchsecurity/definition/malware (accessed March 20, 2022).

Metalidou, E., Marinagi, C., Trivellas, P., Eberhagen, N., Skourlas, C., and Giannakopoulos, G. (2014). The human factor of information security: Unintentional damage perspective. *Procedia Soc. Behav. Sci.* 147, 424–428. doi: 10.1016/j.sbspro.2014.07.133

Metinko, C. (2022). *Cybersecurity venture funding surpasses $20B in 2021, fourth quarter smashes record*. Available online at: https://news.crunchbase.com/news/cybersecurity-venture-funding-2021-record/ (accessed April 2, 2022).

Mishra, A., Alzoubi, Y. I., Gill, A. Q., and Anwar, M. J. (2022). Cybersecurity enterprises policies: A comparative study. *Sensors* 22:538. doi: 10.3390/s22020538

Morgan, S. (2017). *Cybercrime report, editor-in-chief cybersecurity ventures cybercrime damages will cost the world $6 trillion annually by 2021*. Available online at: https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/ (accessed March 2, 2022).

NCSC (2022). *Denial of service (DoS) guidance*. Available online at: Www.Ncsc.Gov.Uk. https://www.ncsc.gov.uk/collection/denial-service-dos-guidance-collection/understanding-denial-of-service-attacks (accessed April 5, 2022).

Neely, L. S. I. (2017). *Threat landscape survey: Users on the front line*. Available online at: https://www.sans.org/reading-room/whitepapers/threats/2017-threat-landscape-survey-users-front-line (accessed February 2, 2022).

Nobles, C. (2015). *Exploring pilots' experiences of integrating technologically advanced aircraft within general aviation: A case study*. Available online at: http://search.proquest.com.ezproxy.libproxy.db.erau.edu/docview/1658234326?accountid=27203 (accessed March 7, 2022).

OBERO (2022a). *E-commerce Sales By Country*. Available online at: https://www.oberlo.com/ (accessed April 20, 2022).

OBERO (2022b). *Top ecommerce companies. Statistics*. Available online at: https://www.oberlo.com/ (accessed April 20, 2022).

Olson, E. (2018). *When answering the phone exposes you to fraud*. New York, NY: The New York Times, 0362–4331.

Pan, X., Yamaguchi, S., and Kageyama, T. (2021). "Machine-learning-based white-hat worm launcher adaptable to large-scale IoT network," in *Proceedinds of the 2021 IEEE 10th Global Conference on Consumer Electronics* (Kyoto), 283–286. doi: 10.1109/GCCE53005.2021.9621895

Phishing (2022). *What is phishing*. Available online at: https://www.phishing.org/what-is-phishing (accessed April 20, 2022).

PURPLESEC (2022). *Social engineering. Purplesec.Us*. Available online at: https://purplesec.us/resources/cyber-security-statistics/ (accessed April 2, 2022).

Pusey, P., and Sadera, W. A. (2011). Cyberethics, cybersafety, and cybersecurity. *J. Digit. Learn. Teach. Educ.* 28, 82–85. doi: 10.1080/21532974.2011.10784684

Rahman, S. (2014). *Introduction to E-commerce technology in business*. Available online at: https://www.grin.com/document/280494 (accessed March 11, 2022).

RAPID7 (2022). *Malware attacks: Definition and best practices. Rapid7*. Available online at: https://www.rapid7.com/fundamentals/malware-attacks (accessed March 21, 2022).

Reynolds, J. (2000). eCommerce: a critical review. *Int. J. Retail Distrib. Manage.* 28, 417–444. doi: 10.1108/09590550010349253

Roumani, M. A., Chun Che, Fung, and Choejey, P. (2015). "Assessing economic impact due to cyber attacks with system dynamics approach," in *Proccedings of the 2015 12th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology* (Hua Hin: ECTI-CON), 1–6. doi: 10.1109/ECTICon.2015.7207084

Saeed, S., Saman, A., and Norafida, I. (2013). Main human factors affecting information system security. *Interdiscip. J. Contemp. Res. Bus.* 5, 329–354.

Sanders, A. (2022). What is social engineering and why is it such a threat in 2022? Available online at: https://www.safetydetectives.com/blog/what-is-social-engineering-and-why-is-it-so-dangerous/ (accessed March 21, 2022).

Sayed, A. F., Shahid, M. K., and Ahmad, S. F. (2020). "Adoption of mobile payment application and its impact on business," in *Impact of mobile payment applications and transfers on business* (Hershey, PA: IGI-Global), 253–269. doi: 10.4018/978-1-7998-2398-8.ch012

Schatz, D., Bashroush, R., and Wall, J. (2017). Towards a more representative definition of cyber security. *J. Digit. Forensics Secur. Law* 12, 1558–7215. doi: 10.15394/jdfsl.2017.1476

Security Magazine (2020). *83% of top 30 US retailers have online vulnerabilities, posing cybersecurity threats*. Available online at: https://www.securitymagazine.com/ (accessed April 1, 2022).

Securitymagazine (2022). *Executive impersonation attacks increased substantially between Q1 2020 and Q1 2021*. Available online at: https://www.securitymagazine.com/articles/95206-executive-impersonation-attacks-increased-substantially-between-q1-2020-and-q1-2021 (accessed April 1, 2022).

Shopify (2022). *Ecommerce. Encyclopedia/what-is-ecommerce*. Available online at: https://www.shopify.com/ (accessed April 1, 2022).

Smart Draw (2022). *E-commerce workflow diagram*. Available online at: https://www.smartdraw.com/ (accessed March 2, 2022).

Snihur, Y., Lamine, W., and Wright, M. (2021). Educating engineers to develop new business models: Exploiting entrepreneurial opportunities in technology-based firms. *Technol. Forecast. Soc. Change* 164:119518. doi: 10.1016/j.techfore.2018.11.011

Social-engineer (2022). *Social engineering defined*". Available online at: https://www.social-engineer.org/framework/general-discussion/social-engineering-defined/ (accessed March 20, 2022).

Stalmachova, K., Chinoracky, R., and Strenitzerova, M. (2021). Changes in business models caused by digital transformation and the COVID-19 pandemic and possibilities of their measurement—case study. *Sustainability* 14:127. doi: 10.3390/su14010127

Statista (2022). *Retail e-commerce sales worldwide from 2014 to 2024*. Available online at: https://www.statista.com/statistics/379046/worldwide-retail-e-commerce-sales (accessed April 20, 2022).

Strategic Technologies Program (2022). *Significant cyber incidents*. Available online at: https://www.csis.org/ (accessed April 2, 2022).

Team, E. (2022). *Must-know cyber attack statistics and trends, business advice & research*. Available online at: https://www.embroker.com/blog/cyber-attack-statistics (accessed March 27, 2022).

Thomas, J. (2016). *Systems theoretic process-analysis STPA*. Availble online at: http://psas.scripts.mit.edu/home/wp-content/uploads/2016/01/

Thomson, L., Kamalaldin, A., Sjödin, D., and Parida, V. (2022). A maturity framework for autonomous solutions in manufacturing firms: The interplay of technology, ecosystem, and business model. *Int. Entrep. Manage. J.* 18, 125–152. doi: 10.1007/s11365-020-00717-3

Varga, G. (2021). *Understanding data privacy*. Available online at: https://cybersecuritymagazine.com/why-should-data-privacy-be-a-top-priority-for-companies/ (accessed April 20, 2022).

Vasupula, N., Munnangi, V., and Daggubati, S. (2022). "Modern privacy risks and protection strategies in data analytics," in *Soft computing and signal processing* (Singapore: Springer), 81–89. doi: 10.1007/978-981-16-1249-7_9

Verizon (2017). *Data breach investigations report*, 10th Edn. Available online at: http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017 (accessed February 20, 2022).

Vinoth, S., Vemula, H. L., Haralayya, B., Mamgain, P., Hasan, M. F., and Naved, M. (2022). Application of cloud computing in banking and e-commerce and related security threats. *Mater. Today Proc.* 51, 2172–2175. doi: 10.1016/j.matpr.2021.11.121

Wall, W. P. (2022). *Global competitiveness*. Singapore: Springer Nature. doi: 10.1007/978-981-16-7755-7

Wang, Z., Li, M., Lu, J., and Cheng, X. (2022). Business innovation based on artificial intelligence and blockchain technology. *Inf. Process. Manage.* 59:102759. doi: 10.1016/j.ipm.2021.102759

Wirth, A. (2017). The economics of cybersecurity. *Biomed. Instrum. Technol.* 51, 52–59. doi: 10.2345/0899-8205-51.s6.52

Xiao, F., Sun, Y., Du, D., Li, X., and Luo, M. (2020). A novel malware classification method based on crucial behavior. *Math. Probl. Eng.* 2020, 1–12. doi: 10.1155/2020/6804290

Zende, S. (2022). Digitalization in india prospect and challenges. *Int. J. Entrep. Technopreneur (INJETECH)* 2, 29–37.

Zhuang, R., Bardas, A. G., DeLoach, S. A., and Ou, X. (2015). "A theory of cyber attacks," in *Proceedings of the second ACM workshop on moving target defense* (New York, NY: Association for Computing Machinery), 11–20. doi: 10.1145/2808475.2808478

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł, Cetin, F., and Basim, H. N. (2022). Cyber security awareness, knowledge and behavior: A comparative study. *J. Comput. Inf. Syst.* 62, 82–97. doi: 10.1080/08874417.2020.1712269