Austin Journal of Forensic Science and Criminology

Open Access

Austin Publishing Group

Review Article

Information and Cyber Security in Digitally Transformed E-Commerce Landscapes in 21st Century: An Overview

Murtala Ismail Adakawa*
Department of User Studies, University Library, Bayero University, Nigeria

***Corresponding author:** **Murtala Ismail Adakawa**
Department of User Studies, University Library, Bayero University, Kano, Nigeria.
Email: murtala@lisc.uni-mysore.ac.in

Received: March 09, 2023
Accepted: April 27, 2023
Published: May 04, 2023

Abstract

The current paper aims at reviewing information security and cybersecurity in digitally transformed e-commerce landscapes. COVID-19 pandemic has led to the disruption of technology and met several businesses unprepared to take off technological transformation consequently, jeopardized many clients into untold hardships and loss. The lockdown period has changed the way people transact their businesses from physical to online mood. More recently, India has been placed on 8th position in terms of e-commerce. This requires protection of network and Apps used in communicating and transacting businesses. Students of commerce and other related programs should be encouraged to take interest in this regard for the continued development and progress of the country in particular and world in general. Governments, organizations, and societies need to security budgetary allocations for tackling the issues of cybersecurity squarely. Several issues have been discussed to justify the claim raised in the paper.

Keywords: Information Security; Cybersecurity; Digital Transformation; COVID-19 Pandemic; Cyberthreat

Introduction

As the situation of COVID-19 pandemic intensifies, so do the new challenges emerge [1]. This is true, as most of the hard-hit sectors during the pandemic were airlines, leisure, hospitality, restaurants, etc. to the extent the pandemic been described as the biggest threat to global economy and financial markets [1]. The COVID-19 pandemic and the resultant restriction of movement brought about disruption to global trade, supply chains, labor markets, slackened consumption, and investment, and dwindled economic activity [2]. Interestingly, there is recognition that, the online world is transforming in almost the same proportion the offline world does [3]. At the onset of the COVID-19 pandemic, there was a decline in the adverting rate in China from 7% to 3.9% in 2020 and the expenditure of e-commerce on advertising grew by 17.7% and on social media rose to 22.2%. This was due to the change of consumer behavior as they resorted to online purchase accounting for 14% spending online [3]. The study reported that, consumers avoided physical stores and in mid-March 2020, 50% of Chinese and 31% of Italian are using e-commerce. This agrees with similar pattern of high e-commerce usage in US where 74.6% of internet users avoided physical stores and embracing e-commerce [3]. While this transformation has assisted many areas, there is always a room for consequences. This is to say that, COVID-19 has characterized cyberbehavior of bad cybercriminals based on their tendency to use the civility of the situation, fear, vulnerability of clients, and structure of the uncertainty to dupe cyberweak audience [4].

The COVID-19 pandemic has caused a stir on how businesses run and change the way employees communicate by forcing rapidly digitalized business models into function thereby laying a new foundation for growth, working environments, reaching clients, and managing employees through digital channels [5]. This opens up a way for increased cybersecurity attacks and laying a sound base requiring cybersecurity services [5] like never before. This translates the fact that, there has never been a time when businesses recognized the indispensable need for using technology for foundational identity security than during the pandemic [6]. To support this claim, as noted by [7], as the COVID-19 continued to affect global health, social, economic, political, etc. systems, so does the threat of cyberattack prey on digital space due to reliance on the digital tools. This is the case,

Citation: Adakawa MI. Information and Cyber security in Digitally Transformed E-Commerce Landscapes in 21st Century: an Overview. Austin J Forensic Sci Criminol. 2023; 10(1): 1092.

as the identity security determines success of business transaction absence of which signifies heightened unexpected risk management [6]. This is to suggest that, there are many indicators that convey the rationales why things go the way they do, which include overdependence on digital infrastructure, which promotes the cost of failure, cybercrimes continuity to exploit fear and uncertainty, and the number of hours spent online could lead to riskier behavior [7]. To concur with this finding, Health Sector Cybersecurity Coordination Center [8] noted that, in order to increase the scope of the spectrum of cyberattacks, cybercriminals exploit their targets in a variety of industries including but not limited to finance, healthcare, pharmaceutical, government, consulting, manufacturing, education, technology. This is to the extent of shifting their focus from attacking individuals, small businesses, to major corporations, governments, and critical infrastructure that respond to the pandemic [8].

To begin with, COVID-19 pandemic has caused restriction of movement and compelled individuals to stay at home. There is an observed rapid digital transformation where digital solutions ensured continual socio-economic activities remotely despite physical distancing imposition [9]. The main reason for imposing lockdown by governments and NGOs upon citizens was *inter alia* to slacken the rapid spread of the virus within community and across the globe. This restriction rendered most of the outdoor activities into indoor practices a consequence of giving rise to highly increased relations between man and machines, which pose cybersecurity threats [10]. Stay at home order came at a time when it was needed the most but brought with it many challenges that encompassed cyberattacks on businesses, government, vaccine development code, to mention but a few [11]. Prior to the eruption of COVID-19 pandemic, in 2019, in US alone, there was a shortage of 500,000 cybersecurity professionals and the gap is even wider in the post-pandemic era exemplified by high demand of these professionals in healthcare, insurance, business making cybersecurity engineers, risk management analysts, etc. as essential staff for assessing infrastructure viability and security [5]. Notably, this threat stemmed from the fact that, many companies concentrated on granting access to customers neglecting to consider the implications of giving access to whom, which resulted in a myriad unsecure access to technology [6]. For instance, in the domain of healthcare alone, cyberattacks increased by 150% disrupting the customer trust through impersonating staff links via Zoom, Google Meet, etc. This caused the blockage of 18 million COVID-19 related malware and emails every day in the second quarter of 2020 [11]. Similarly, in a period of four months from January to April, 2020, there were about 907,000 spam messages, 737 incidents related to malware, 48,000 malicious URLs related to COVID-19 pandemic [12]. A breach on data has economic consequences. For example, in health sector, it accounts for loss of $6.45 million, financial $5.86 million, energy $5.6 million, industrial $5.20, pharma $5.20, technology $5.05 among others [7]. Prior to the eruption of the pandemic, [13] opined that, the global spend on IT security was $120 billion in 2017 thereby hinting the need for cybersecurity issues to be addressed holistically since they behave in the same way as pathogens. That is why many programs and interventions have been put in place to reduce such cyberattacks on e-commerce. Examples of such programs include neural network [4], ICT Policy institutionalized by UN through the United Nations, United Nations Conference on Trade and Development (UNCTAD) laden with responsibility of drafting policy-oriented analytical work [9], to mention but a few.

However, in spite of the programs and interventions to bring the cyberthreats to the barest minimum, the problems of cybersecurity are still prevalent. The consequences of not addressing these problems resulted in embarrassment on the company, individual thereby resulting in significant financial impairment leading to psychosocial problems [10], among others. This calls for other studies from a suitable perspective. Unless the problem of cybersecurity is addressed from information security, the problem will continue to prevail. Even though studies about cybersecurity in e-commerce have focused on using pragmatic approaches to study cybersecurity, unless the problem is looked at from how much organization has planned for security budget, the problem of cybersecurity will continue. Some of the contemporary key theorists that discussed issues of the information security are [14]. These scholars stated that, *Information security is a process where people and organisations attempt to create sustainably-viable resources, from information".* Information security depends on how much organizations spend on security budget and organization's ability to match controls with threats [14].

Statement of the Problem

From the onset, it has to be acknowledged that, globalization and IT have remarkably changed the way business are conducted by organizations through the integration and implementation of IT system [15]. Among the facilitators of e-commerce are internet, payment gateway, analytics, social media, autonomous vehicles (like AI), etc. [15]. COVID-19 pandemic has brought with it many challenges for various human endeavors including e-commerce. Many enterprises were waiting for the right time to digitize their businesses but taken aback by the sudden eruption of the pandemic without proper planning to prepare well for the uptake of the technological transformation. This disruption caused many bad elements of the society to use the weakest points of cyber-behavior of many customers to have unauthorized access to their information [10]. Realizing the inefficiency of the system to tackle all the nagging problems at once resulted in many companies to invite other corporate bodies to conduct researches on the breach of their customer information database [12]. Unfortunately, it takes days, weeks, or even months to recognize a cybersecurity threat a consequence of requesting to look at the problem of the cybersecurity issues from useful perspective. This research is an attempt to add no matter how little contribution to the body of knowledge for raising awareness on cybersecurity among enterprises and business corporations.

Significance of this Review

It is hoped that, at the end of reading this piece of information, audience will appreciate the significance of this research especially considering the following facts

a) Higher number of cyberattacks is cosmopolitan

b) Increased frequency of businesses requiring cybersecurity is alarmingly growing

c) Increased security needs for certain industries [5]

d) 1.8 million cybersecurity jobs will remain unfilled across the globe [16]

In order to achieve the objectives of this study, the paper tries to provide an overview according to the following subheadings

1. Understanding Information Security and Cybersecurity in e-Commerce: Why They Matter?

2. Information Security Theory and e-Commerce

3. Conclusion

Understanding Information Security and Cybersecurity in e-Commerce: Why They Matter?

E-commerce is dynamic, fluid in its actual form, scope, and definition. Its fluidity might have originated from the fact that, the kind of definitions it received varies with time. For instance, Colecchia, (n.d) observed that, e-commerce has a wide range of definitions that spin around business, research, policymakers, statisticians. To this end, e-commerce refers to the business activities (encompassing communication and transaction) conducted electronically that comprise ordering, invoicing, payment, marketing, advertising, and communicating (Colecchia, n.d). In other words, e-commerce means any kind of transactions relating to commercial activities that have to do with processing and transmitting digitized data or those that occur over open, non-proprietary networks or those that involve production, marketing, distribution, sales of services over e-means (Colecchia, n.d). This is to imply different types of e-commerce, which include B2B, B2C, C2C, C2B, among others [15]. This implies that, e-commerce is a complex domain characterized by a many seeming disjointed components that give rise to collective whole. At each level of analysis, a slight breach of trust can result in the total collapse of the entire business. This is to show how impact it is to make the e-commerce structure intact, compact, and focused to avoid any challenges. Unfortunately, many threats are confronting the integrity, confidentiality, availability, and implementation of e-commerce from different angles. In other words, the threats are evolving, transforming, and no slackening in their pace, which challenge the organizational and network security.

From another perspective, it is available in the literature that, in 2008, the internet connected 541.7 million computers in more than 250 countries across the globe [17]. Similarly, research showed that, in richer countries, more than 2/3rd of the population are online and in developing countries, even though lower but it is alarmingly increasing [18]. To be precise, in 2017/2018, China has 765 million (50%) users online followed by India 391 million (26%), United States 245 million, Brazil 126 million, Japan 116 million, Russia had 109 million users [18]. In terms of rising of social media platforms, as of 2019, Facebook had 2.38 billion users, YouTube had 1.9 billion, WhatsApp had 1.33 billion, WeChat had 1 billion, Instagram had 1 billion, TickTok had 500 million, among others [18]. This report revealed that, the current generation regardless of age, gender, etc. uses internet, smartphone/mobile phone, social media, for communicating, which form the basis of transacting business.

Relevance of information has gone far that its circumference and neighborhood has to be protected from unauthorized or unauthenticated third party infringement. Many organizations engage in a number of ways of top-bottom, broader to specific, etc. methods to ensure the integrity, confidentiality, and availability of information at all cost. Reading [19] paper carefully will reveal a rather complication or even impossibility to encounter in defining the word security. From its inception, security is very important as regard international relations with respect to the safety and security of states and citizens for their survival. The implication of this simple account of the security gives rise to various perceptions about what entails it. To begin with, security in this sense capitalizes on the foreign policy of large economies. From the realist perspective, state receives maximum reference as an object of security. From liberal angle, security ensues when there is cooperation to solve global problems. Stemming from critical security studies, constructivist position believes that security is subjective [19]. Combing the two words yields a rather different definition. That is, information security, which is a major issue for businesses and their clients, refers to the protection of information and its assets thereby preserving its confidentiality, integrity, and [10]. In order to ensure maximum protection of information, from 1997-2001, America had to spent $2.5 trillion on IT. Briefly, the main reason for protecting personal information from infringement are due to operational value, individual value, value to others, and value to the society [10]. There is a marked difference between information security and cybersecurity as information a subset of cybersecurity and concerns with network and app code [20].

Due to the eruption of COVID-19 pandemic, about 80% of professionals have witnessed a remarkable change in their daily routines. That, almost half of the professionals have transitioned from performing their traditional roles to IT-related tasks, which include *inter alia* troubleshooting computer, networking problems, installing Virtual Private Networks (VPNs), manning helpdesks, to mention but a few [5]. In other words, because of this transitioning to work remotely, many organizations are experiencing an increased infringement of their services [5]. This Implies the need to tighten information security measures in organizations to contain existing and prosperous threats. The fact that pandemics will continue to occur, organizations stand a chance to experience several technological disruptions since different pandemic gives rise to different cybersecurity issues and the quest for focusing on information/cybersecurity.

The pattern of e-commerce in the world is best explained and described by one of the most influential textbooks on e-commerce written by Morgan. Morgan's Global E-Commerce Trends Report portrays the most 37 countries that are well automated to conduct e-commerce. The report began by mentioning America specifically Brazil. In Brazil, the market despite at early stage of development, e-commerce grows and has a unique online shopping that draws local and foreign buyers highly domiciled in Argentina's Mercado Livre, domestic site Americanas and U.S. giant Amazon [21]. Lovers' Day followed by Black Friday, which cumulatively generate huge amount of money for Brazilian economy totalling around $1.5 billion in 2020. "*App-friendly Brazilians have demonstrated a preference for shopping via mobile devices and paying with cards and cash*" [21]. Similarly, in Canada with 91% penetration of internet and smartphone, with quality of life, its market reached projected to reach $7.9 million in sales against the $6.9 million in 2020 [21]. In Canada, the preferable means of e-commerce payment route is card and PayPal [21]. This is to indicate that, developed countries are adopting cashless policies to transact business over network.

To support the above presupposition, Morgan noted that, "*India's massive population represent huge e-commerce growth potential, particularly for international brands that have mastered mobile commerce*" where Digital Wallets form significant platforms for e-commerce payment method in the country [21]. In other words, any internet giant willing to invest, India e-commerce has potential of meeting its needs and requirements. This sets her as the 8th largest e-commerce in the world

to the extent every 4 out of 10 citizens shop online with many platforms carrying out this assignment predominantly Amazon.in, Bigbasket, and Grofers serving 1.4 billion population with Google investing $10 billion [21]. This follows from the policy government has taken to prevent a single platform from dominating all sectors thereby giving equal opportunities to innovative minds to invent new ideas thereby creating open access source that will enhance intellectual hybridization [21]. These studies so far have shown the relevance and necessity to promote information security infrastructure to guard against illegal access into the databank of organizations.

Information Security Theory and e-Commerce

Fundamentally, information science or rather library science and business studies have something in common: customer (business)/user (information science) and commodity exchanged (money/information respectively). In addition, among the many relations between these two domains, customer/user and money/information brought about a strong pillar upon which library/information science pivots. In effect, many business models form the fundamental theories or practices in librarianship thereby raising the same questions asked in the two domain-specific environments: how to satisfy customer/users' needs. To begin with, study by [22] is one of the many researches that demonstrated a number of cyberthreats that occurred during the pandemic. Notably, among the institutions that experienced such a disastrous attack are financial services, healthcare system, governments, among others [22]. This is to the extent that many theories are formulated to augment this the duality of infringing organizational data by unauthorized access and guarding the data intact for the safety and security of information especially during Electronic Data Interchange (EDI).

As noted above, COVID-19 has sped up the evolution, growth, and development of e-commerce from various angles including new firms, customers, products, access to product at the convenience of their homes, and continuity of operations of firms despite restriction of movement [23]. The e-commerce landscape is dynamic in terms of its scope across countries and include purchase of luxury to necessary commodities to a large number of customers, which permanent these changes to a long-term [24]. In spite of this dynamism, there still exists digital divide among individuals and regulations put in place play a vital role in creating barriers of sales or delivery calling for a revised policy [24]. In response to this, UN, (2022) has reported some regional governments to initiate economic recovery by implementing adoption of new digital channels, business models, and modified consumption habits to the extent 36.6% of firms in Georgia, 40% in the Republic of Moldova, 24% in North Macedonia and 18% in Albania. The report further highlighted that, the dominat areas where challenges occur are mainly ICT infrastructure and services, trade facilitation and logistics, legal and regulatory framework, electronic payment system, skills development, and gender gap [2].

Among the notable researches done in this area is that of [14]. The basic premise of the theory is that, "*Information security is a process where people and organisations attempt to create sustainably-viable resources, from information".* To state the theory in a more general form, every organization depending on its goals, tries to "*apply suitable controls to protect information from threats, according to the goals of the organisation, which results in sustainable resources*" [14].

From the above, it is clear that, the basic constructs of the theory are; information, threat, control, resources, and goals.

Information: Is an amorphous entity that can be printed on paper, stored on computers, either sent by post or electronically, shown on videos or articulated in discussion. The information can be sensitive or non-sensitive. Sensitive information classified as protected, confidential, secret or top secret [14].

Control: Is a mixture of physical, technical, and operational security controls in an organization with a sole aim of protecting or reducing the risk of information due to the exposure or vulnerability arising from the threat [14]

Threats: Integrity, confidentiality, and availability of organizational information experience threats in a number of ways either unauthorized access, changing of information, or destruction of protective infrastructure

Resources: Are the units of production, which form the basic units of analysis. These include capital equipment, skills of employment, patents, brand names, finance [14]

Information Security Theory in e-Commerce in India

India ranked 8th position in terms of e-commerce [21] and always strives to move forward in an increasing, competitive, and competent direction. Maintaining an eighth position in an e-mediated commerce is not an easy task and should be approached with all hands on deck for a fruitful and reproducible future. This suggests that, no matter how little a contribution is, stakeholders concerned have to look inwardly and logically to associate the relationships existing among the variables of importance for the protection of information. Looking at this phenomenon from the perspective of humans as subjects in an objective world will provide a clue why governments or owners of businesses should be committed to the protection of organizational wealth. In other words, sacrifice that has to do with provision of infrastructure and financial commitment in this regard is very vital. To begin with, OECD, (2020*) highlighted that, COVID-19 pandemic has deepened the digital divide among individuals and communities and governments at various levels are employing several means to make ends meet especially with respect to digital technologies and communications infrastructure and digital strategies to narrow the flaring gaps. According to OECD, (2020*), digital policy integrated framework on growth and wellbeing should encompass market openness, access, use, innovation, jobs, societies, and trust. Even though budget is mentioned, however, security budget that serves as an engine upon which this policy pivots remains overshadowed. To bring to the table and limelight of the stakeholders, maximum supply of security budget means protection of businesses, policies, individuals, information systems, to mention but a few.

E-commerce as a sale or purchase of goods, services, and exchange of information based on communication [25] is confronted with many risks. Risk, which is not an uncertainty, but involves probability or threat of damage, injury, liability, vulnerability, or any other negative occurrence [25]. Thus, e-commerce risk management deals with identification, assessment, and prioritization of risks by following economic and coordinated use of resources to reduce its impacts [25]. According to [26], there are four levels to distinguish risk/threats in an organization: technical, individual, business, societal risks. Through vulnerability management, organizations can process and use technologies to identify, assess, and remediate the threat [26]. In short, risk management process encompasses definition of scope (i.e. understanding the organizational background, evalu-

ate previous management activities, develop structure for the countermeasure), risk assessment, risk treatment, monitoring and reviewing, risk communication, and risk acceptance [26].

For firms, whether governmental or non-governmental, to function effectively and efficiently, they need proficient supply of finances to back any of the risk management process. At all different levels of analysis, each category of the risk management process requires financial inputs to function effectively. In this respect, security budget is instrumentally and critically imperative for the successful protection or otherwise of any given organization. As captured by [27] citing Nemertes Research as an example, he cited eight key points that challenge security administration in a given organization. The people problem (staffing, skills and knowledge), process latency (process latency and budget allocated on wrong basis), and the technology problem (shortage of tooling, shortage of analytics and filtering, and lack of automation and integration) [27]. Most often than not, one of the most observed failure to meet with the security budget is the issue of compliance budget where employees fail to comply with security policies despite efforts being made by many organizations to change or influence security behaviour [28]. This came up because of the actual and perceived cost and benefits of compliance and organizational security behavior [28].

Drawing from risk management policies, important areas that slip the sight of most researchers on security are data archival policies, asset owners, talent management, personnel resources. To begin with, it has become a commonplace nowadays to hear about cyberattacks that cause problems to the privacy and of millions of online users or cyberwar that expose many societies to unending dangers [29]. For instance, in 2013, in US, Target Corporation referenced by [29] noted that there were 40 million customers whose information on credit and debit cards were stolen. Similarly, in 2015, there was a data breach of 79 million insurance customers' personal information [29]. Furthermore, in 2018, in Russia, Fultonhistory.com with more 44 million pages had crashed [29]. This implies the importance of archival information on net. To concur with this presupposition, [29] cited Society of American Archivists (AAS) who noted the intense and serious vulnerability of born-digital materials agreeing that, it is an emerging topic that "*warrants more investigation*". This implies the importance born-digital or digitized information has on the web and the seriousness in protecting its integrity. Maximum advantage should be given to the single elements highlighted above to guard against unauthorized access to personal, or organizational or societal information.

Conclusion

The 21st century has witnessed a remarkable disruption in many aspects of the contemporary society ranging from health, economic, social, environmental, to cybersecurity, to mention but a little. COVDI-19 has challenged every facet of human endeavor in a diverse manner. It has caused a pause on the way businesses are run and enforced digitization process whether organization has prepared or not. Restriction of movement was one of the few things that necessitated employing other avenues that ensure embracing technology. Many cyberattacks are ubiquitous on the web that called for concentrating on threats organizations are experiencing. India has attained 8th position in e-commerce globally and has to put more efforts on security budgets to guard against intrusion by unauthorized individuals

References

1. Öven H, Hicintuka M. COVID-19: How does it affect international e-commerce firms? A qualitative case study about how the Covid-19 situation affects e-commerce firms and how they respond to it. A bachelor thesis submitted to the Department of International Business, Linnaeus University, Sweden. 2020.
2. United Nations. COVID-19 impact on e-commerce- Post-pandemic COVID-19 Economic Recovery: Harnessing E-commerce for the UNECE Transition Economies. 2022.
3. Al-maaitah TA, Majali T, Alsoud M, Almaaitah DA. The impact of COVID-19 on the electronic commerce users behavior. Journal of Contemporary Issues in Business and Government. 2021; 27: 784-793.
4. Tawalbeh L, Muheidat F, Tawalbeh M, Quwaider M, Saldamli G. Predicting and preventing cyber attacks during COVID-19 time using data analysis and proposed secure IoT layered model. 2020 Fourth International Conference on Multimedia Computing, Networking and Applications (MCNA). Predicting and Preventing Cyber Attacks During COVID-19 Time Using Data Analysis and Proposed Secure Iot layered Model. 2020.
5. Deppa, Ouellette M. The impact of COVID-19 on the cybersecurity sector. 2020.
6. Security. Cybersecurity doorways left ajar in the race to remote work. Cybersecurity doorways left ajar in the race to remote work | 2020-11-20 | Security Magazine. 2020.
7. World Economic Forum. Why cybersecurity matters more than ever during the coronavirus pandemic. Coronavirus pandemic: why cybersecurity matters | World Economic Forum. 2020.
8. Health Sector Cybersecurity Coordination Center (HC3, 2020). COVID-19 threats. 2020.
9. United Nations. COVID-19 and e-commerce: A global review. 2021.
10. Adakawa MI, Alhassan ZM, Auyo MA. Now and future of libraries: The necessity to equip librarians with cybersecurity skills. Management of library and information centers in the era of global insecurity: A festschrift in honor of Prof. M.I. Ajibero.Al-Dhahri S, Al-Sarti M, Abdul Aziz A. 2017. Information security management system. International Journal of Computer Applications. 2020; 158: 29-33.
11. Kabir KM. Digital transformation and cybersecurity during COVID-19. Digital Transformation And Cybersecurity During Covid-19. 2020.
12. INTERPOL. INTERPOL report shows alarming rate of cyberattacks during COVID-19. INTERPOL report shows alarming rate of cyberattacks during COVID-19. 2020.
13. Gandhi G. Complexity in cybersecurity. 2014.
14. Horne CA, Ahmad A, Maynard SB. A theory on information security. 2016.
15. Jain V, Malviya B, Arya S. An overview of electronic commerce (e-commerce). Journal of Contemporary Issues in Business and Government. 2021; 27: 665-670.
16. Adakawa MI. Libraries, cybersecurity, and webinars: review. Journal of Information Studies & Technology. 2022; 2.
17. Pesante L. Introduction to information security. Introduction to Information Security. 2008.
18. Roser M, Ritchie H, Ortiz-Ospina E. Internet- Interactive charts on internet. Internet - Our World in Data. 2020.

19. Degaut M. What is security?. 2015.

20. Roohparvar R. What is information security? Definitions, principles, and policies. What is information security? Definition, principles, and policies - Cyber Security Solutions, Compliance, and Consulting Services - IT Security. 2020.

21. Morgan JP. Local and cross-border: Insights global e-commerce trends report. Global e-commerce trends report. 2020.

22. Chigada J, Madzinga R. Cyberattacks and threats during COVID-19: A systematic literature review. South African Journal of Information Management. 2021; 23: a1277.

23. OECD. E-commerce in the times of COVID-19. Tackling coronavirus (COVID-19): Contributing to a global effort. 2020.

24. OECD. Digital transformation in the age of COVID-19: Building resilience and bridging divides. Digital Economy Outlook 2020 Supplement, OECD, Paris, 2020.

25. Quyet CB, Cuong HC. E-commerce risk management: Analyzing the case Vietnam Airlines incident. Open Science Journal. 2017; 2.

26. Nastase F, Nastase P. Risk management for e-business. Revista Informatica Economică. 2007; 3: 56-59.

27. Burke J. 8 challenges every security operations center faces. 2022.

28. Beautement A, Sasse MA, Wonham M. The compliance budget: Managing security behaviour in organizations. 2014.

29. Donaldson R, Bell L. Security, archivists, and digital collections. Journal of Archival Organization. 2019; 1-19.