International Journal of Scientific Engineering and Science
Volume 8, Issue 1, pp. 102-107, 2024. ISSN (Online): 2456-7361

Addressing the Threat of Security Breach in the E-Business Process

Bilquis Ferdousi[1], Jamal Bari[2]
[1]School of Information Security and Applied Computing, Eastern Michigan University, Ypsilanti, Michigan, USA
[2]School of Engineering, Eastern Michigan University, Ypsilanti, Michigan, USA

Abstract*—This article explores the issues of protecting consumers' public and private information in e-business. With advancement of innovative digital technology, the exponential growth of e-business has become almost ubiquitous throughout the world. However, cybersecurity has been one of the major concerns since the increasing consumption of online business. The weaknesses that create threat to cybersecurity in online transactions negatively impact both the consumers and the merchants in online business. The purpose of this paper is to explain the possible cybersecurity risks associated with e-business, why the cybersecurity risks matter, and how they can be mitigated. This paper outlined some of the strategies to ensure cybersecurity in online business protecting consumers' privacy and data security. The paper provided ways to protect e-business consumers from these flaws in ensuring cybersecurity are worth worrying about. This study may help e-business organizations to mitigate damages when all else fails in cybercrime. Thus, the result of this study may also help cyber security and cybercrime professionals in implementing consumers' privacy and cybersecurity procedures and practices.*

Keywords— *E-commerce, cybersecurity, data protection, policy*.

I. INTRODUCTION

Technology is increasingly advancing at a faster pace than anything else in the world today. With this rapid advancement businesses organizations are marketing to consumers, selling their products and services in new approaches, and generating online businesses. As online businesses flourish through technology, people in general are increasing their technology consumption with the increased use of mobile devices and social media platforms. The ever-enhanced advanced technologies are contributing in people's online businesses around the world. They are buying products and getting services after reviewing and paying online. People are using a wide range of digital tools and platforms to purchase products and services.

Cybersecurity has been one of the major concerns since the increasing use of the internet for online business. Maintaining the integrity and confidentiality of consumers' data allows to establish trust between consumers and business organizations. Developing trust is important because it assures integrity of the information in online business. Ensuring cybersecurity of information is a very important issue that should not be taken lightly. When the integrity or privacy of consumers has been lost it can result in not only financial loss but reputational loss as well.

With the growing use of online business, there is a greater amount of data that is being shared. Therefore, improving cybersecurity is a priority for all business organizations. The assurance of cybersecurity consists of eight elements: cybersecurity threats, security policy, management support, budget for security, hardware, software, employees, and more secured information. Each of these elements rely on each other in order to result in a more secure information system [1].

The increasing phenomenon of global e-commerce together with the advances in online data collection technologies and online marketing techniques have created potential threats to consumers' privacy and cybersecurity [2]. E-business is now universal. Whether it be buying and selling or providing and receiving services online business are becoming ubiquitous in society. E-business poses unprecedented problems in security that were not present before. The types of digital transactions include digital wallets, credit card terminals, cryptocurrency, and general e-business. However, it's a serious concern how consumers' personal and financial information is being used, shared, and protected in e-business. The lack of security can hinder the successful process of e-business [3].

Using the fast-growing technology both private companies and public authorities collect and use people's personal data on an unprecedented scale in order to pursue their business and services [4]. The personal data refers to any information relating to a natural person, who is identified or identifiable, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. The personal data breach defined as breach of data security that led to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed [4]. In this context, the purpose of this paper is to find the possible cybersecurity risks associated with online transactions in e-business, why the security risks matter, and how they can be mitigated.

II. EXPONENTIAL GROUTH OF E-BUSINESS

Electronic business, otherwise known as e-business, is any trade activity in which purchase, orders, and payments are made through an online environment which includes banking and financial services provided via the Internet. E-business takes advantage of innovative information technologies. E-businesses are growing throughout the world at a significant rate, making it easier to buy and sell products in different countries. Many businesses organizations use e-commerce so that they can stay open 24 hours and seven days a week,

International Journal of Scientific Engineering and Science
Volume 8, Issue 1, pp. 102-107, 2024. ISSN (Online): 2456-7361

making it easy to run around the clock without any increased overheads. There are four main categories of e-business: Business to business (B2B), business to consumer (B2C), consumer to business (C2B), and consumer to consumer (C2C). In business-to-business, it involves business organizations doing online business with each other. For example, manufacturers selling to distributors or wholesalers doing business with retailers. The business to customer (B2C) applies to any business that sells its products or services directly to customers online. Customer to business (C2B) is the one that any customer who sells a product or service to a business online. Lastly customer to customer (C2C) applies to customers offering goods and services to each other online. For example, an e-auction where customers are buying from and selling to each other.

In a U.S. Department of Commerce report it was estimated that the U.S. retail e-business sales for the third quarter of 2023 would be total $271.7 billion, an increase of 0.9% (±0.4%) from the second quarter of 2023. The third quarter 2023 e-business estimate increased 7.8% (±1.2%) from the third quarter of 2022 while total retail sales increased 2.0% (±0.4%) in the same period. E-business sales in the third quarter of 2023 accounted for 14.9% of total sales [5].

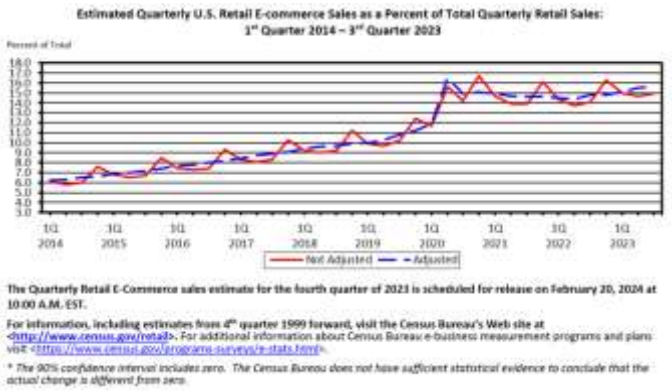

Fig. 1. Estimated retail e-commerce sales from 1st quarter 2014 to 3rd quarter 2023. Source: [5]

A survey by Pew Research Center conducted in 2016 found that roughly 80% of adults in the USA shop online. About 79% of them use any type of digital devices, 51% use cell phones, and 15% use social media for online shopping [6]. Another survey conducted by Pew Research Center in 2022 found that while 57% of adults in the USA use PayPal, 38% have used Venmo, 36% use Zelle, and 26% have ever used Cash app. In total, 76% of them have ever used at least one of these four payment sites or apps. It was found that the use of digital platforms for online shopping varies based on age groups. The adults under 50 have adopted these tools at higher rates. Especially, a significant age gap found in using Venmo. About 57% of 18- to 29-year-olds use Venmo, compared to 49% of 30 to 49, 28% of 50-64 and only 15% of 65 and older age group use Venmo [7]. In addition, depending on their age groups, people's use of digital devices for online shopping varies too. In particular, adults under 50 in the USA use mobile phones for their online business. Around 91% of 18- to 49-year-olds in the USA buy online using a smartphone, compared with 69% of 50 to 64, and 48% of 65 and older age groups. About 32% of these adults use smartphones to buy online at least once a week, while 21% use desktop or laptops, and 7% use tablets for online shopping [8].

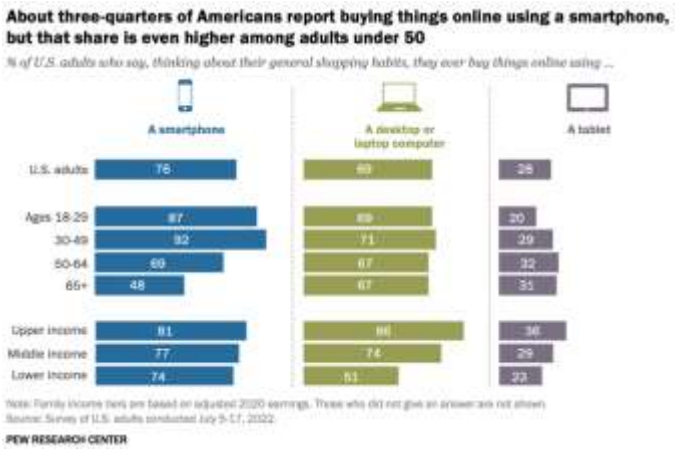

Fig. 2. Using digital devices in online business among different demographic groups. Source: [3]

III. Threats to Cyber Security In E-Business

The increased advancement and reliance on digital devices and computer networks have expanded the cyberattacks globally. This threat to cyber security is not limited in businesses, organizations, and governments. The common people are also victims of cyberattacks on a regular basis in this digital society. While increasingly popular, online innovation isn't without the threats of cyber-attacks and cybercrimes.

Globalization, exponential growth of e-commerce, use of social media, cloud computing, big data, created concern of consumers' privacy and data protection. A special report anticipated that with online business the global cybercrime costs will grow by 15% per year over the next five years, reaching $10.5 trillion annually by 2025, up from $3 trillion in 2015 [9]. Data breaches are very self-explanatory in how the impact of the lost data affects businesses. The data lost, which can range from Social Security Numbers to usernames and passwords, to intellectual property, ends up in the hands of people all around the world.

In online business consumers are making electronic transactions using debit cards, credit cards, PayPal, Venmo, e-checks, etc. Nowadays even social media platforms are being used for online businesses. The use of social media platforms for online businesses is gradually increasing as these platforms become part of people's everyday life [10]. However, the concern for threat to data security and privacy also increased accordingly. This concern is not limited to the financial transactions in the buying products only, but also in services such as keeping electronic health records, personnel records, service records, financial records, academic records, etc. [11].

In the past, significant cybercrimes included online scamming and phishing. Current attacks are more advanced with the capability of disrupting critical operations and infrastructure of technology [12]. More recent cybercrimes include criminal computer activities with the traditional

criminal aspects, such as fraud, theft, blackmail through ransomware attacks, social engineering, etc. Privacy and data security issues are part of a larger cyber security concern in online business. Protection of privacy and data have become a perplexing and fast cyber security challenge during this time of cutting-edge technology.

A. Consumers' Privacy and Data Security

As online business has become prevalent with the advancement of digital technology, the threat to consumers' privacy and data security also increased exponentially. The issues of data security and privacy are a concern for both consumers and business alike. The concern is more serious especially in the business to consumer (B2C) type online business model, where direct financial transactions with regular consumers processes completely online without any human interaction. Therefore, especially in the B2C type online business model consumers need a robust sense of assurance of their data security and privacy when conducting financial transactions completely online [13].

Since e-business is strictly done online, cybersecurity is an essential part of any business transaction that takes place over the internet. Businesses organizations and consumers would lose faith in e-business if data security is compromised and not protected. Therefore, e-businesses must provide the essential requirements for the safety and protection of consumers' personal identifiable information. For that purpose, e-businesses use the secure socket protocol (SSL) to meet the security requirements, authentication, encryption, integrity, non-repudiation to protect its customers and enable businesses to transact instantly. This may take away all of the apprehension and fears consumers may have when making transactions to buy product or pay their bills online.

Still Consumers are afraid of how their information, which they want to keep private and secure, is being used and shared by the business organizations. Consumers have the right to protect their privacy and business organizations have responsibility to ensure that. A study showed that about 45% of consumers, especially older consumers, have very low trust or no trust at all in business organizations. They do not believe that the business organizations they are dealing with are using their digital data securely or protecting their privacy the way it should be [14].

Also, the weakest link to the cybersecurity chain is the human because a significant number of people, who are using online business are not properly aware of the threat to their privacy and data security. They do not know how to handle the security risks of taking proper precautions to protect themselves. There are people who have concerns about cybersecurity, but they do not make much effort to learn about how to protect their privacy and data; thus, it is difficult to ensure good online behavior among consumers.

Privacy: Privacy, an important part of cyber security, is concerned with authentication and proper handling of data with a person's consent, notice, and related regulatory obligation [15]. Privacy is a crucial factor in online businesses as consumers share their personal and financial information with expectation that their sensitive information will be kept confidential. In online business consumers are concerned with business organizations' marketing practices that may breach privacy and data security [16]. Privacy in online refers to the protection of personally identifiable information (PII), popularly known as *personal data*, which is a vital factor in the scope of any law on data security and privacy [17].

Data security: While Privacy is defined as the control over one's own personal data [18], the threat to data security is the attempted unauthorized access to the data. Data security is the most important factor in online business where data security refers to protection of consumers' financial and personal information from unauthorized access.

Consumers have serious concern about the protection of their financial and personal information during the online business transactions. If online businesses organizations handle the consumers' data negligently or leak their information purposefully that may cause ethical concerns among online consumers [16].

B. Consumers' Trust in E-Business

The success in online business significantly depends on ensuring consumers' trust that is significantly impacted by their data security and privacy. Trust in a business influences consumers taking risk in financial transactions sharing their sensitive information adopting new technology [18]. The transparency in data processing by business organizations is vital to gain trust from the consumers who expect security of their data and privacy is guaranteed [15]. Therefore, ensuring data security and privacy is an essential requirement for any efficient and effective online payment transaction activities [19]. Study shows that about 92% consumers believe that it is business institutions' responsibility to protect their personal sensitive information [20].

The development of trust among consumers not only affects their intentions buy products or services, but also directly affects profitability and lifetime value of a business very positively [21].

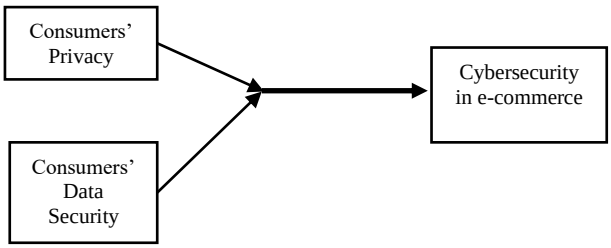

Fig. 3. Consumers' trust in cyber security in online business impacted by privacy and data security.

However, there is a significant lack of trust among online business consumers who have serious concerns in conducting online transactions providing their financial and personal information. If online businesses organizations handle their consumers' data negligently or leak their information purposefully that may cause ethical concerns among online consumers breaking their trust in online business organizations [16].

To protect consumers' data and privacy, the business institutions must ensure a completely secure system. But the

business systems, even with advanced technology, are facing more and more challenges to provide consumers with privacy and data security. Research findings show that the breaches of consumers' data are also caused as a result of lack of complete measurement from online business institutions. In this context, it is important that there is legislative action to ensure people's privacy and data security.

IV. Lagislations To Protect Consumers' Privacy And Data Security

Consumers' privacy and data security challenges are becoming a serious issue in online business that must be addressed as an increasing number of people are now conducting business online. Along with the increase of online business, the threat to online users' privacy and data security has grown steadily. In this context, it is very important to find the measures that can protect users' privacy and data security in online business.

Government agencies that regulate consumers' privacy and data security exist at the federal and state levels. The laws at the federal and state levels are written from different perspectives but often overlap in requirements. Therefore, as much as these regulations might differ, there are also common concepts in federal and state level laws. There are a number of laws and regulations that focus on protecting people's privacy and personal data. Some of the federal and state level regulations to protect consumes privacy and data security are discussed below.

A. Federal Legislations to Protect Data and Privacy

Consumer Data Privacy and Security Act of 2020: The act aimed to establish a clear federal standard for consumers' data and privacy protection, strengthening the existing laws that govern consumers' personal data. The act creates uniform standards and regulations for businesses that collect, process, and use consumers' personally identifiable information [22].

Children's Online Privacy Protection Act (COPPA): This children's online privacy protection legislation was enacted by congress in 1998. To protect children's safety and privacy on the Internet, this act limits the collection of personally identifiable information from children under 13 without their parents' consent. Issued in November 1999 and effective since April 2000 by Federal Trade Commission, COPPA (16 CFR Part 312) requires websites to post a complete privacy policy, notify parents directly about their information collection practices, and get verifiable parental consent before collecting personal information from children or sharing their information with others [23]. COPPA further revised and updated in 2013 to include:

1) Details website operator must include in a privacy policy,
2) When and how to seek verifiable consent from a parent or guardian,
3) What responsibilities an operator has to protect children's privacy and safety online including restrictions on the marketing to those under 13,
4) Children under 13 can legally give out personally identifiable information with their parents' permission [24].

Gramm-Leach-Bliley Act: This act requires the financial organizations safeguarding and protecting their consumers' data. The act allows reducing all possible fines and reputational damages caused by sharing or leaking of sensitive financial data. This act ensures the implementation of consumers' privacy disclosures annually [15].

B. State legislations to Protect Data and Privacy

There are some state-level data breach laws and data breach notification laws with lists of data that are covered by the statutory requirements. Different states such as California and New York have enacted consumers' privacy, data security, cyber security, and data breach notification laws. While more legislative actions are needed, these legislations currently protect state consumers' data and privacy on some levels.

California Consumer Privacy Act of 2018: According to the California Consumer Privacy Act of 2018 (CCPA), "A consumer shall have the right to request that a business that collects a consumer's personal information disclose to that consumer the categories and specific pieces of personal information the business has collected." This legislative act aims to further protect the privacy rights of the consumers in California by giving them an effective way to control their personally identifiable information. The legislation includes the right of people in California to refuse accessing and selling their personal information, to equal service and price, and to even exercise their privacy rights.

CCPA secures privacy rights for consumers in California including: 1) consumers' right to know about their personal information businesses organizations collect, and use and share, 2) consumers' right to delete personal information collected from them (with some exceptions), 3) consumers' right to opt-out of the sale of their personal information, and 4) non-discrimination for exercising their CCPA rights [25]. Most recently in November 2020, the California Privacy Rights Act (CPRA) became effective.

New York Privacy Act of 2021: New York state Senate Bill S6701 enacted this act requiring businesses to disclose their methods of de-identifying consumers' personally identifiable information, to place special safeguards around data sharing, and to allow consumers obtaining the names of all entities with whom their information is shared.

Furthermore, the act requires business organizations to clearly notify consumers of how their data is being used, processed, and shared with third parties. This law allows consumers to 1) access and obtain a copy of their data in a commonly used electronic format, with the ability to transfer it between services, 2) correct or delete inaccurate data, and 3) challenge certain automated decisions. This act seeks to help the consumers in New York to exercise more control over their personal data as it requires businesses organizations to be responsible, thoughtful, and accountable of their consumers' sensitive personal and financial information [26].

V. Cybersecurity Policy And Practices

The online business has exponentially grown in recent decades, especially with the advancement of digital technology and tools. However, the serious threat to

International Journal of Scientific Engineering and Science
Volume 8, Issue 1, pp. 102-107, 2024. ISSN (Online): 2456-7361

consumers' privacy and data security has also become a serious challenge. Research shows that people are increasingly buying and selling products as well as receiving and providing service in business-to-consumer (B2C) online business models. To protect consumers' privacy and data security, legislative measures have been taken at the federal and state level in the USA.

The concepts of cyber security and cyber law are now intertwined [27]. However, there are more measures that need to be taken to protect people's privacy and data security. Privacy and data security policies address consumers' data security and privacy issues. These policies are mainly from online business organizations' perspective that require them to act properly to protect their customers' privacy and data security. But the stated policies are not always matching organizations practice. These differences between practice and policies reflect in the consumers' data security and privacy that can have a very serious impact on consumers' life. The consumers in B2C online business models take the risk of threat to their data security and privacy in varying levels while making financial transactions [28].

A. NIST Special Publication (SP) 800-53

NIST, an agency of the U.S. Department of Commerce, developed cybersecurity standards and guidelines in its Special Publication 800-53. This publication recommended security controls for federal information systems. The recommendations include 18 areas addressing managerial, operational, and technical controls. Business organizations often rely on these recommendations to develop their own internal cybersecurity management programs. Two important measures to ensure cybersecurity in e-commerce are access control to information systems and awareness and training [29].

Access Control to Information Systems: Only authorized users, processes acting on behalf of authorized users, relevant devices and systems, and the transactions and functions that authorized users are permitted to exercise, should have access to the data. One of the important strategies in access control in e-commerce is multifactor authentication as shown in figure 4.

The multifactor authentication for access in e-business systems can help to reduce fraudulent purchases online, show customers that business organization is committed to the cybersecurity, protecting their e-business systems, providing greater security awareness, avoiding system-administrator-account takeover through phishing, and implementing the solutions [30].

Awareness and Training: To ensure business organizations and consumers are aware of the cybersecurity risks associated with e-commerce process. Also, provide proper training to ensure cybersecurity.

B. Payment Card Industry Data Security Standard

The Payment Card Industry Data Security Standard (PCI DSS) is a global information security standard that describes what procedures organizations require to follow to protect consumers' credit card information. The PCI DSS applies to all organization that stores, processes, or exchanges their credit cardholder consumers' information. The PCI DSS has six control objectives that need to be included in the cybersecurity policies in any organization [31]. These control objectives are:

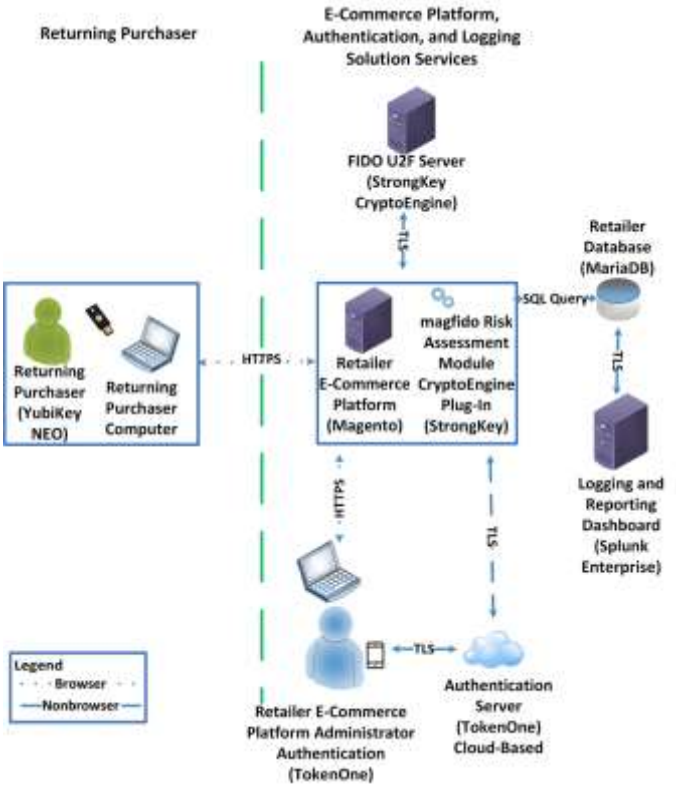

Fig. 4. Multifactor authentication for e-commerce. Source: [30].

Build and maintain secure network: The systems networks should have specific firewall, password, and other security layer controls.

Protect cardholders' data: Specify how the cardholders' data will be stored, protected, and encrypted.

Maintain vulnerability management program: Specify how the systems and applications security including required use of antivirus software will be maintained.

Implement strong access control measures: Specify how to restrict the access to cardholders' data.

Regular monitoring and testing networks: Require monitoring access to cardholders' information and periodic penetration testing of the network.

Maintain security policy: Requires updated information security policies reflecting the PCI DSS requirements. Also, require cybersecurity awareness programs among management and consumers.

VI. CONCLUSION

Finally, if online business platforms lack unified highly efficient secure management systems, and there are no sufficiently effective legal and statutory supervision and sanctions for data breach in online business, the consumers' privacy and data security issues affect sustainable development of online business [32]. With an increasing

number of people around the world are now buying products and getting services online using different platforms, reliable infrastructures, and platforms for financial transactions online is crucial. Also, to ensure consumers' privacy and data security a business organization must let its consumers know how their personal information will be protected.

REFERENCES

[1] Smith, A. D. "E-security issues and policy development in an information-sharing and networked environment", *Aslib Proceedings, 56*(5), 272-285, 2004.

[2] G. L. White, F. A. M. Mediavilla and J. R. Shah, "Information Privacy: Implementation and Perception of Laws and Corporate Policies by CEOs and Managers," *International Journal of Information Security and Privacy (IJISP), IGI Global, 5*(1), pp. 50-66, January, 2011.

[3] Kuruwitaarachchi, N., Abeygunawardena, P.K.W., Rupasingha, L., and Udara, S.W.I. "A systematic review of security in electronic commerce - threats and frameworks", *Global Journal of Computer Science and Technology: E-Network, Web & Security, 19*(1), 2019.

[4] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016. *Official Journal of the European Union.* https://op.europa.eu/en/publication-detail/-/publication/3e485e15-11bd-11e6-ba9a-01aa75ed71a1

[5] U.S. Department of Commerce, 2023.U.S. Census Bureau News. Quarterly Retail E-Commerce Sales 3rd Quarter 2023.

[6] A. Smith and M. Anderson, "Online shopping and E-commerce", Pew Research Center. 2016. Retrieved from: https://www.pewresearch.org/internet/2016/12/19/online-shopping-and-e-commerce/

[7] M. Anderson, "Payment apps like Venmo and Cash App bring convenience – and security concerns – to some users", *Pew Research Center,* 2022. Retrieved from: https://www.pewresearch.org/fact-tank/2022/09/08/payment-apps-like-venmo-and-cash-app-bring-convenience-and-security-concerns-to-some-users/

[8] M. Faverio, and M. Anderson, "For shopping, phones are common and influencers have become a factor – especially for young adults", *Pew Research Center,* 2022. Retrieved from: https://www.pewresearch.org/fact-tank/2022/11/21/for-shopping-phones-are-common-and-influencers-have-become-a-factor-especially-for-young adults/?utm_source=Pew+Research+Center&utm_campaign=f1bcdcb1d6-Weekly_2022_11_26&utm_medium=email&utm_term=0_-f1bcdcb1d6-%5BLIST_EMAIL_ID%5D

[9] S. Morgan, "2021 Report: Cyberwarfare in the C-Suite", *Cybercrime Facts and Statistics, Cybersecurity Ventures,* Intrusion, Inc. January 21, 2021. Retrieved from: https://cybersecurityventures.com/wp-content/uploads/2021/01/Cyberwarfare-2021-Report.pdf.

[10] I. Akman, and A. Mishra, "Factors influencing consumer intention in social commerce adoption", *Information Technology & People,* vol. 30 no. 2, pp.356-370, 2017. Retrieved from: https://doi.org/10.1108/ITP-01-2016-0006

[11] S. Khan, "Cyber Security Issues and Challenges in E-Commerce", *SSRN Electronic Journal,* January 2019. DOI:10.2139/ssrn.3323741

[12] P. K. Pattnaik, and I. Mishra, "Cybercrimes in India and related laws," *Psychology and Education,* 57(9), pp. 757-760, 2020.

[13] M. I. Alharbi, S, Zyngier, and C. Hodkinson, *Journal of Enterprise Information Management, 26*(6), pp. 702-718, 2013.

[14] S. Higginbotham, "Data Privacy Will Be the Achilles Heel of the Internet of Things," Fortune.com. Fortune, 06 July 2015. Web. 19 April, 2017. Retrieved from: http://fortune.com/2015/07/06/consumer-data-privacy/.

[15] M. M. Nair and A. K. Tyagi, "Privacy: History, Statistics, Policy, Laws, Preservation and Threat Analysis," *Journal of Information Assurance and Security*. ISSN 1554-1010 Vol. 16, pp. 024-034, 2021. © MIR Labs, www.mirlabs.net/jias/index.html

[16] Y. B. Limbu, M. Wolf, and D. L. Lunsford, "Consumers' perceptions of online ethics and its effects on satisfaction and loyalty," *Journal of Research in Interactive Marketing,* 5(1), pp. 71-89, 2011. Emerald Group Publishing Limited, 2040-7122. DOI: 10.1108/17505931111121534

[17] W. G. Voss and K. A. Houser, "Personal Data and the GDPR: Providing a Competitive Advantage for U.S. Companies," *American Business Law Journal*, 56(2), pp. 287-344, Summer 2019.

[18] Martin, K, "The penalty for privacy violations: How privacy violations impact trust online," *Journal of Business Research, 82,* pp. 103-116, 2018.

[19] P. Gupta, and A. Dubey, "E-commerce- study of privacy, trust and security from consumer's perspective," *IJCSMC,* 5(6), pp. 224-232, 2016.

[20] A. Muneer, S. Razzaq, and Z. Farooq, "Data privacy issues and possible solutions in E-commerce," *J Account Mark,* 7, 294, 2018. DOI: 10.4172/2168-9601.1000294.

[21] C. Flavián, and M. Guinalíu, "Consumer trust, perceived security and privacy policy: Three basic elements of loyalty to a web site", Industrial Management & Data Systems, 106(5), pp. 601-620, 2006.

[22] Congress.gov., "S.3456 - Consumer Data Privacy and Security Act of 2020", 2020. Retrieved from: https://www.congress.gov/bill/116th-congress/senate-bill/3456/text

[23] Federal Trade Commission. "Protecting Children's Privacy Under COPPA: A Survey on Compliance," April 2002. Retrieved from: https://www.ftc.gov/sites/default/files/documents/rules/children%E2%80%99s-online-privacy-protection-rule-coppa/coppasurvey

[24] National Credit Union Administration, "Children's Online Privacy Protection Act," 2021. Retrieved from: ncua.gov/regulation-supervision/manuals-guides/federal-consumer-financial-protection-guide/compliance-management/deposit-regulations/childrens-online-privacy-protection-act

[25] R. Bonita, "California Consumer Privacy Act (CCPA)," State of California Department of Justice, Office of the Attorney General, 2018. Retrieved from: https://oag.ca.gov/privacy/ccpa

[26] NCSL. "2019 Consumer Data Privacy Legislation", National Congress of State Legislature, 1/3/2020. Retrieved from: https://www.ncsl.org/research/telecommunications-and-information-technology/consumer-data-privacy.aspx

[27] U. Pathak, "Cyber security and cyber laws in India: Focus areas and issue areas," The Clarion- International Multidisciplinary Journal, vol. 6, no. 1, pp. 51-56, 2017. https://doi.org/10.5958/2277-937x.2017.00008.9

[28] K. A. Vakeel, S. Das, G. J. Udo, and K. Bagchi, "Do security and privacy policies in B2B and B2C e-commerce differ? A comparative study using content analysis," *Behaviour & Information Technology*, vol. 36, no. 4, 390–403, 2017. Retrieved from: http://dx.doi.org/10.1080/0144929X.2016.1236837

[29] Joint Task Force, Security and privacy controls for information systems and organizations, NIST Special Publication 800-53 Revision 5, National Institute of Standards and Technology, U.S. Department of Commerce, 2020. https://doi.org/10.6028/NIST.SP.800-53r5

[30] W. Newhouse, B. Johnson, S. Kinling, J. Kuruvilla, and B. Mulugeta Kenneth Sandlin Multifactor Authentication for E-Commerce Risk-Based, FIDO Universal Second Factor Implementations for Purchasers, *NIST SPECIAL PUBLICATION 1800-17,* U.S. Department of Commerce, 2019. https://doi.org/10.6028/NIST.SP.1800-17

[31] M. E. Whitman and H. J. Mattord. "Management of Information Security", 6th Edition, Cengage Learning Publishers.

[32] Q. Ji, "Study on information security issues of E-Commerce," IOP Conf. Series: Materials Science and Engineering, 452, 2018, 032050. IOP Publishing, doi:10.1088/1757-899X/452/3/032050.