International Journal of Human Research and Social Science Studies

ISSN(p): 3050-547X, ISSN(e): 3050-5488

Volume 02 Issue 11 November, 2025

DOI: https://doi.org/10.55677/ijhrsss/13-2025-Vol02I11

Page No : 859-867

The Impact of Cybersecurity on E-Commerce Activities: Case Studies of Ebay And Tokopedia

Tran Thi Ngoc My

University of Economics and Business- Vietnam National University

ABSTRACT: E-commerce is rapidly expanding worldwide; however, the growing threat of cyberattacks has increasingly impacted the trust of both consumers and businesses operating or trading on these platforms. This study employs qualitative case studies and comparative analysis approach to examine the impact of cybersecurity on the operations of eBay and Tokopedia. In addition, surveys and questionnaires were conducted to assess the cybersecurity factors affecting Vietnam's e-commerce sector.

Corresponding Author:
Tran Thi Ngoc My

KEYWORDS:
Cybersecurity, E-commerce, Cyberattacks, eBay, Tokopedia, Vietnam.

1. INTRODUCTION

E-commerce has experienced rapid growth, particularly in the aftermath of the COVID-19 pandemic, as the demand for online payment systems has significantly increased. According to Demand Sage (2023), approximately 2.64 billion individuals worldwide engaged in online shopping by the end of 2023 [7]. In comparison, the global population was estimated at around 8 billion during the same period (United States Census Bureau, 2023). This indicates that nearly one-third of the world's population participated in online purchasing activities. However, these several potential risks, among which cybersecurity has emerged as a major concern in recent years. In 2023, Indian cybersecurity expert Mr. Pabitra Kumar Sahoo [23] stated that 32% of global cyberattacks targeted e-commerce companies, and the majority of these firms lacked adequate cybersecurity solutions. According to Fortinet [9], in 2023, approximately 40% of enterprises were forced to lay off employees or replace senior executives due to security system incidents. Additionally, 35% of companies had to temporarily suspend operations to address the consequences, while 67% suffered financial losses ranging from 1 to 10 million USD per cyberattack incident.

In 2014 and 2020, two major e-commerce enterprises, eBay and Tokopedia, suffered significant losses due to cybersecurity breaches. These incidents not only affected their business operations but also damaged the corporate reputation that had been built over the years. Analyzing these two typical cases helps to clearly illustrate the impact of cybersecurity on e-commerce activities, as both represent large-scale cyberattacks with serious consequences. Such analysis provides valuable lessons for enterprises in general, and for Vietnamese e-commerce businesses in particular. Firstly, eBay, a U.S.-based company from a market with a high level of cybersecurity awareness, offers important insights. Despite having implemented multiple cybersecurity protection measures, the company still faced major challenges during its operations. The 2014 cyberattack on eBay compromised the global user system, leading to the leakage of personal information from numerous accounts. Secondly, Tokopedia, an Indonesian enterprise whose national context is comparable to that of Vietnam—where cybersecurity awareness remains relatively low compared to many developed countries—also suffered a major breach. The 2020 attack on Tokopedia resulted in user data being sold on online forums, causing widespread alarm within the Indonesian online community. The cases of eBay and Tokopedia provide highly practical reference points and offer useful implications for Vietnamese e-commerce enterprises in improving and strengthening their cybersecurity systems.

2. LITERATURE REVIEW

The impact of cybersecurity has been widely examined across various sectors. Nguyen Phi Hung et al. [21] identified 15 cybersecurity risks within Vietnam's financial and banking systems, among which malware infection and system vulnerabilities were found to cause the most severe consequences. Similarly, Aya Aljaradat et al. [4] evaluated the impact of cybersecurity on the adoption of digital payments and reached three key conclusions: first, digital payment service providers that do not invest in cybersecurity measures will face users' reluctance to use their services due to fears of personal information leakage, which negatively affects their profitability; second, providing customers with information about cybersecurity issues encourages a higher adoption rate of digital payment systems; and third, law enforcement agencies play a crucial role in addressing cybercrime-related issues.

Jiehui Huang et al.[14] examined how cybersecurity assurance strategies influence investors' judgments and decisions. The study found that the growing complexity of IT systems and the rise of IoT devices have expanded the cybersecurity "attack surface." To address data breaches and investor concerns, the U.S. Securities and Exchange Commission (SEC) now requires firms to regularly disclose their cybersecurity policies and management expertise. These disclosures help investors make more informed valuations based on a company's cybersecurity risk management and incident history. In addition, Julian Jang-Jaccard et al. [16] examined the growing risks of cybersecurity threats in cyberspace, noting that the rise of online shopping and users' increasing comfort in sharing personal information, such as credit card numbers and delivery addresses, have further exacerbated cybersecurity vulnerabilities.

Regarding the impact of cybersecurity on e-commerce activities, in 2022, Alok Mishra et al. [1] examined cybersecurity regulations across seven countries— the U.S., EU, Canada, Australia, China, India, and Malaysia—identifying 14 sectors vulnerable to cyber risks. In e-commerce, they found that while users value convenience, online platforms are prime targets for cybercriminals seeking to steal data and profit. Houssam Saleh et al. [10] reported that cybercrime causes e-commerce firms to lose billions annually and damages their reputation, as security breaches erode customer trust in data protection and transaction reliability. Similarly, Sireesha et al. [6]found that technical vulnerabilities lead to customer loss, reduced revenue, and reputational decline. Shweta et al. [25] highlighted that data breaches diminish customer confidence, cut sales by about 5%, and may even trigger legal consequences for affected companies.

Regarding studies on cybersecurity in e-commerce activities at eBay and Tokopedia, Nwosu Amarachukwu Grace [22] analyzed essential security services to protect systems from potential risks, using eBay's 2014 data breach as a case study. The study highlighted that "humans are often the weakest link," as the breach stemmed from stolen employee credentials. Jeane Neeltje Saly [17] examined Tokopedia's 2020 data leak, where personal information of 91 million users was exposed and sold on the illegal *Empires Market*. Austin Bowler et al. [3] investigated eBay's 2014 cyberattack, identifying system vulnerabilities and its impacts—stock decline, revenue loss, and diminished customer trust in online transactions.

3. THEORETICAL FRAMEWORK

According to the NCCS, a non-governmental organization (NGO) in the United Kingdom, *"Cybersecurity helps individuals and organizations reduce the cyberattacks. Its core function is to defend the digital services and devices we rely on from online threats, which includes safeguarding the vast amounts of data and personal information stored locally or in the cloud"*. In Vietnam, based on Clause 1, Article 2 of the 2018 Cybersecurity Law, it defines *"cybersecurity as the assurance that activities in cyberspace do not harm national security, social order and safety, or the lawful rights and interests of agencies, organizations, and individuals. Cybersecurity protection means preventing, detecting, stopping, and handling acts that violate cybersecurity."*

Shahriari et al. (2017) defined e-commerce as including activities such as electronic payments, supply chain management, Internet marketing, online transactions, EDI, inventory management, and automated data collection [23]. According to Clause 1, Article 3 of Decree No. 52/2013/NĐ-CP, *e-commerce activities involve conducting part or all of commercial processes through electronic means connected to the Internet or other open networks.*

Sireesha (2017) highlighted the importance of cybersecurity in e-commerce, defining it as the use of technological measures to protect systems, networks, and data from attacks or unauthorized access. Besides technology, compliance with cybersecurity laws is vital to prevent cybercrime [6]. According to Article 72 of Decree No. 52/2013/NĐ-CP, e-commerce security requires organizations to safeguard users' personal data, prevent unauthorized access or misuse, and provide mechanisms to handle consumer complaints related to data breaches.

Considering the factors of cybersecurity that influence e-commerce activities, four key factors can be identified. The first is advanced security systems**,** which safeguard customer data and information on e-commerce platforms through modern technological solutions such as firewalls**,** intrusion detection systems (IDS), and intrusion prevention systems (IPS)**.** The second factor is training and raising cybersecurity awareness among individuals**.** Enhancing users' and employees' understanding of cybersecurity helps minimize human errors and reduces vulnerabilities within e-commerce operations. The third factor is cybersecurity regulations and laws, which play a crucial role in establishing standards for protecting personal information and data in e-commerce activities. Finally, incident response and security system recovery plans are essential. Organizations with clear response strategies and transparent incident reporting can maintain customer trust even when cybersecurity breaches occur.

Cybersecurity has a dual impact on e-commerce activities. On the positive side, a strong security system protects customer accounts and data, as well as the business secrets of e-commerce companies. Effective data protection also helps build and strengthen customer trust. Implementing cybersecurity measures reduces financial risks, prevents fraud and data breaches, ensures regulatory compliance, and strengthens the brand competitiveness of e-commerce businesses. Moreover, strong cybersecurity enhances brand competitiveness for e-commerce businesses. On the negative side, cybersecurity incidents can disrupt business operations and customer experience, damage corporate reputation and customer trust, and lead to high costs for investment and recovery.

4. RESEARCH METHOD

4.1. Qualitative Method: Case Studies

This study analyzes two major cybersecurity incidents—Tokopedia (2020) and eBay (2014)—to clarify the impact of cybersecurity on e-commerce operations, as both cases are large-scale and caused severe consequences. Tokopedia, a leading platform in Indonesia, offers practical relevance since the country's level of cybersecurity awareness is comparable to that of Vietnam. Meanwhile, eBay, as a global corporation, demonstrates that even large enterprises are not immune to risks without proper security measures. Examining these incidents, which occurred at different times, also allows for an analysis of how companies' responses to cyberattacks have evolved, providing valuable lessons and recommendations for Vietnam's e-commerce sector.

4.2. Comparative Method.

The research evaluates and compares the dual impacts of the two cyberattacks on eBay (2014) and Tokopedia (2020). Regarding negative impacts, the study compares the time each company took to handle and restore their systems, the extent of customer trust damage, and the losses in revenue and profit. In terms of positive impacts, the study examines variables such as increased cybersecurity awareness and the enactment of related laws and regulations that became effective after the incidents.

4.3. Survey and Data Collection

The study developed a research questionnaire to survey and collect data on cybersecurity factors affecting e-commerce activities. The surveyed factors include cybersecurity regulations and laws, employee and user awareness, incident response plans, and cybersecurity systems. These four factors were selected because they represent the core aspects of ensuring cybersecurity in e-commerce activities. Legal regulations provide a protective framework, user and employee awareness influence safe usage behavior, incident response plans help minimize damage when breaches occur, and cybersecurity systems serve as the technical foundation for protecting data and transactions. The effective coordination of these elements contributes to maintaining trust and stability in the digital commerce environment.

5. RESULTS

5.1. The Impact of Cybersecurity on E-Commerce Activities: Case Studies of eBay and Tokopedia

5.1.1. The Impact of Cybersecurity on E-Commerce Activities: A Case Study of eBay

- *Cybersecurity in eBay's E-Commerce Activities: The 2014 System Breach Incident*

Although the e-commerce company eBay had implemented cybersecurity measures, it was still severely affected by a major system breach in 2014. Specifically:

(1) eBay's security and intrusion detection systems failed to provide timely alerts. Employee login credentials were compromised around late February 2014, allowing attackers to gain access to the company's user database. However, eBay only detected the issue after noticing unusual activities from several employee accounts approximately two weeks before the public disclosure of the breach.

(2) The issue of employee training and cybersecurity awareness at eBay proved ineffective. The root cause of the incident was a phishing attack, in which hackers deceived eBay employees into revealing sensitive login credentials, which were then used to infiltrate the company's systems.

(3) The enforcement of regulations imposing penalties on cybercriminals and companies with security lapses was still unclear. In 2014, cybersecurity regulations outlining implementation principles and penalty cases in both Europe and the United States had not yet come into effect.

(4) eBay's incident response plan was criticized for being slow. The company's first public statement about the breach was posted on its less-visited corporate website, eBayinc.com. It was only a day later that eBay issued another notice on its main website, providing minimal details about the incident and simply instructing users to reset their passwords.

- *The impact of cybersecurity on eBay's e-commerce activities*

a. Negative impacts

(1) Disruption of e-commerce activities

Due to the cyberattack, eBay's online shopping platform became completely inaccessible for 26 hours, halting all buying and selling activities of both individuals and businesses. This caused major disruptions, especially during the peak summer shopping season when online demand was high. Buyers were unable to search for products, place orders, or track shipments, resulting in a poor user experience. Sellers, on the other hand, faced difficulties updating prices and inventory, while order processing and delivery were delayed. Moreover, the downtime caused sellers to lose significant sales opportunities, particularly during major shopping events, leading to decreased revenue. This cyberattack also impacted online payments, as payment transactions were delayed or failed, preventing buyers from completing their purchases. On top of that, eBay spent a significant amount of time and resources to remediate the consequences. The incident response and recovery process lasted up to 12 weeks, and it took at least two years to implement campaigns and programs aimed at restoring customer trust.

(2) Impact on customer trust and eBay's reputation.

According to Mateusz Brogowicz (2014), a customer survey revealed that 62% of respondents rated their experience as *"Poor"*,

indicating that most users felt the service was severely disrupted. Meanwhile, 27% rated it as *"Average"*, suggesting that some could still access the site but experienced difficulties or slow performance. Only 1% rated their experience as *"Good"*, meaning a small group was minimally affected or had a more stable experience [18].

(3) Impact on eBay's revenue and stock performance.

In the second quarter of 2014, eBay's revenue reached USD 2.17 billion, but following the cyberattack, it declined by approximately 0.92% in the third quarter, down to USD 2.15 billion. The downward trend continued over the next three quarters in 2015, with revenues dropping to USD 2.06 billion in Q1/2015 and USD 2.1 billion in both Q2 and Q3/2015. (Source: Statista.com). The cybersecurity incident also affected eBay's stock price. The immediate impact was a sharp decline of up to 20% in the company's share value on the afternoon following the public announcement of the breach [3].

(4) Impact on post-incident recovery costs.

According to Steve Roberts [27], the total cost eBay incurred to address the aftermath of the cyberattack across all affected markets was estimated at USD 300 million**.** This amount covered expenses related to upgrading security systems, hiring cybersecurity experts, investigating the cause of the breach, restoring brand reputation, and implementing communication strategies to regain customer trust.

b**.** Positive impacts

(1) Promoting the enactment of data protection regulations.

The cyberattack on the global e-commerce giant eBay prompted regulators to implement more robust data protection laws. In the European Union, the General Data Protection Regulation (GDPR) was introduced in 2016 and took effect in 2018, becoming one of the world's most comprehensive data protection frameworks. It applies to 30 countries, including the all EU member states and three European Economic Area (EEA) countries—Norway, Iceland, and Liechtenstein. In the United States, the California Consumer Privacy Act (CCPA) was passed in 2018, establishing strict data protection requirements similar to those under the GDPR.

(2) Impact on information security awareness:

For e-commerce enterprises: After the attack, eBay enhanced its customer data encryption and introduced new policies to restrict employee access to sensitive information, minimizing intrusion risks. The company also provided detailed user guidelines on its website to help customers recognize and avoid phishing attempts.

For individual users and businesses using e-commerce platforms: Although customer trust initially declined, the incident ultimately raised awareness of personal data protection.

The growing awareness of cybersecurity's importance is also reflected in the Global Cybersecurity Index (GCI) published by the International Telecommunication Union (ITU), which measures national commitment to cybersecurity. In 2018, the United States—where eBay's headquarters is located—ranked second globally with a score of 0.926, just behind the United Kingdom (0.931) [11]. By 2020, the United States rose to first place worldwide in this index [12].

- *The impact of cybersecurity on Tokopedia's e-commerce activities*

a. Negative impacts

(1) Disruption of e-commerce activities

This cyberattack impacted on user experience. Consequently, the transaction processing system experienced delays as Tokopedia implemented additional security measures. Some users encountered errors when logging in, searching for products, or making payments. Moreover, buyers lost trust and turned to other e-commerce platforms, which in turn negatively affected sellers who were unable to generate sales. Moreover, the cyberattack impacted on payments and financial transactions. Customers became more cautious about linking their bank accounts or e-wallets to Tokopedia. In addition, several transactions were delayed due to the implementation of enhanced security verification procedures. Finally, the company spent a significant amount of time and resources on remediation efforts. It took the company at least six months to fully address and resolve the consequences of the incident.

(2) Impact on consumer's trust and corporation's reputation

The lack of transparency in disclosing the investigation results caused many users to lose confidence in the platform. The Indonesian consumer community formally filed a lawsuit against Tokopedia, demanding that the company be held accountable and provide compensation for damages. However, the lawsuit quickly encountered legal obstacles when the Central Jakarta District Court dismissed the case on the grounds that it lacked jurisdiction. The absence of clear punitive measures has raised public concerns that digital platforms in Indonesia may not be fully held liable in the event of major data breaches.

(3) Impact on profit

According to data reported by *The Wall Street Journal*, during the 2019–2020 period, Tokopedia recorded a significant improvement in business performance, with losses falling sharply from USD -101.75 million to USD -24.56 million. However, this positive trend did not last long, as in 2021, Tokopedia reported a loss of USD -115.77 million, considerably higher than the previous year.

b. Positive impacts

(1) Enactment of Indonesia's Personal Data Protection Law in 2022. The cyberattack on Tokopedia was one of the large-scale

incidents that had a severe impact on the Indonesian market. Consequently, the 2020 incident contributed to the Indonesian government's enactment of the Personal Data Protection Law in September 2022, aiming to establish a robust legal framework for safeguarding privacy and personal data amid the rapid growth of the digital economy.

(2) Raising awareness of the importance of cybersecurity. The 2020 Tokopedia cyberattack helped raise cybersecurity awareness in Indonesia. According to the GCI 2020 [12], the country ranked 24th out of 194, improving 24 positions compared to 2019. The government strengthened data protection regulations, enhanced international cooperation, and bolstered information security. Businesses also upgraded their security measures by implementing multi-factor authentication and stronger data encryption.

5.1.3. Compare the impacts of cybersecurity on e-commerce operations between eBay and Tokopedia.

In terms of similarities, when cyberattacks occur, the negative impacts generally affect e-commerce activities such as buying and selling on the platform, customer trust, corporate reputation, revenue, and profits. On the positive side, cybersecurity incidents clearly help e-commerce companies recognize the importance of implementing enhanced security measures and improving professional expertise in cybersecurity. More importantly, governments and regulatory authorities evaluate the situation and introduce stricter laws and regulations to prevent hackers from exploiting vulnerabilities to attack businesses.

Regarding the differences in the impact of cybersecurity on the e-commerce operations of eBay and Tokopedia, specifically:

- Negative impacts

(1) Disruption of e-commerce activities

For eBay: The company spent 12 weeks addressing technical issues and at least 2 years implementing campaigns and programs to restore customer trust.

For Tokopedia: The company took at least 6 months to fully remediate the consequences, including upgrading security measures and restoring customer trust.

Assessment: eBay's recovery took longer than Tokopedia's.

(2) Consumers' trust and corporation's reputation

For eBay: eBay received lower customer ratings on the platform following the cybersecurity incident. The company also had to address lawsuits related to violations of general data protection regulations, indicating that customer trust in eBay was significantly affected.

For Tokopedia: Tokopedia was sued by a group of users in Indonesia for allegedly failing to adequately protect personal data. The lawsuit demanded compensation for damages due to the risk of fraud and identity theft.

Assessment: eBay, as a global platform with customers from multiple countries, faces a potential loss of trust on a much larger scale than Tokopedia.

(3) Loss of profits

For eBay: As eBay handles a massive volume of transactions globally, the cyberattack had a severe impact on its revenue and profits.

For Tokopedia: Profits from the Indonesian market were affected following the attack.

Assessment: eBay operates in international markets, so its profits were impacted more significantly than Tokopedia's.

- Positive impacts

(1) Improvement of cybersecurity-related laws and regulations

For eBay: The cybersecurity incident at eBay accelerated the need for regulations ensuring security and privacy. International regulations such as GDPR (Europe) and CCPA (U.S.) were subsequently enacted and implemented.

For Tokopedia: The cyberattack on Tokopedia also contributed to the Indonesian government enacting cybersecurity laws and applying them in practice.

Assessment: eBay faced greater pressure to comply with stringent security regulations from governments and international regulatory bodies due to its global operations. Tokopedia, operating solely in Indonesia, only needed to comply with cybersecurity laws and regulations within the country.

(2) Raising cybersecurity awareness

For eBay: In 2020, the global cybersecurity index (GCI) for the U.S., where eBay is headquartered, ranked 1st in the world [12].

For Tokopedia: In 2020, Indonesia's global cybersecurity index ranked 24th in the world [12].

Assessment: Although Indonesia's GCI had entered the top 25 globally by 2020, it still ranked more than 20 positions behind the U.S. and European Union countries.

5.2. The Impact of Cybersecurity on E-Commerce Activities in Vietnam

5.2.1. Cybersecurity Factors Affecting E-Commerce Activities in Vietnam

The study conducted a survey of both individuals and businesses to evaluate four key factors influencing e-commerce activities: cybersecurity regulations/laws**,** awareness among employees and users**,** incident response planning, and enterprise cybersecurity systems. The objective was to assess how these factors impact the development and operation of e-commerce in Vietnam.

Survey period: From December 1, 2024, to February 1, 2025.

Survey method: The research utilized data collected through pre-designed questionnaires distributed via Google Forms and in-person surveys.

Survey sample: A total of 300 questionnaires were distributed; after verification, 278 valid responses were obtained, including 32 from businesses and 246 from individuals.

The survey results indicated that the majority of respondents were individual users of e-commerce platforms, accounting for 88.5%, while business respondents represented only 11.5% of the total sample.

Table 1. Descriptive Statistics of Individuals and Businesses Participating in the Survey

Respondent type	Frequency	Percentage (%)
Businesses	32	11.5%
Individuals	246	88.5%
Total	**278**	**100%**

Source: Author's survey, 2025

Based on the analysis of 278 responses (including both individuals and businesses), the findings revealed that among the examined factors, cybersecurity regulations and laws had the greatest impact on e-commerce activities, with 60% of respondents rating their influence as high. The second most influential factor was advanced security systems and access management, with 50% of respondents assessing it as having a strong impact on e-commerce operations.

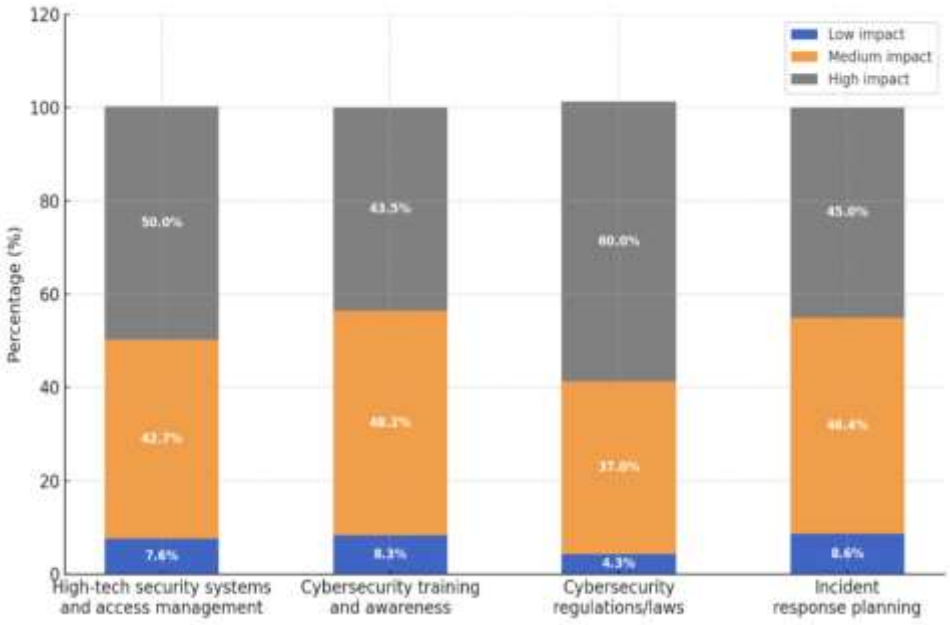

Figure 1. Survey results assessing the impact level of four cybersecurity factors on e-commerce activities according to three scales.

Source: Author's survey, 2025

5.2.2. The impact of Cybersecurity on E-Commerce Activities: A Case Study of Shopee in Vietnam

- *Cybersecurity in Shopee's E-Commerce Activitiesin Vietnam*

Shopee entered the Vietnamese market in August 2016 and quickly became one of the leading e-commerce platforms. Despite implementing various security measures, the platform has still been exploited by cybercriminals who took advantage of its vulnerabilities to commit illegal acts.

On April 1, 2024, the Phu Tho Provincial Police prosecuted four individuals who exploited a seller authentication vulnerability on Shopee to commit fraud. The group created fake online stores and recruited people through social networks to place proxy orders. They then sent empty or worthless packages. Once the orders were delivered, they appropriated money, commissions, and discount codes from Shopee [28].

- *The impact of Cybersecurity on E-Commerce Activities: A Case Study of Shopee in Vietnam*

a. Negative impacts

First, the incident involving the fraudulent appropriation of discount codes on Shopee has caused significant financial losses to the e-commerce platform. According to VTV.vn [28], in an interview with the investigating authorities, within just the first four months of 2024, the perpetrators earned about 600 million VND from this scheme.

Second, the incident could seriously damage Shopee's reputation, as it undermines users' trust in the platform's security and reliability.

Third, the incident has affected both genuine sellers and real buyers on the e-commerce platform.

For genuine sellers: The fake stores created by the perpetrators offered extremely low prices, creating unfair competition for legitimate sellers. This fraudulent activity increased costs and reduced revenue for real sellers on Shopee, negatively impacting their business operations.

For buyers: They often received products that did not match the descriptions and had no real value, yet were unable to request refunds.

b. Positvie impacts

First, improving Shopee's security systems and policies. To open a store on Shopee, sellers must go through verification steps regarding both their identity and the quality of their products. Other measures to enhance buyer confidence in online shopping have also been gradually implemented by the company. According to an interview with Shopee's Communications Director, the company has launched the "Shopee Co-Inspection" program, which allows customers to check the appearance of goods before accepting delivery. In addition, through the "Safe Shopping" initiative, Shopee has partnered with the Vietnam E-Commerce Association to implement practical measures aimed at reducing consumer concerns when shopping online.

Second, raising awareness about cybersecurity. The incident has attracted public and governmental attention, thereby increasing vigilance and awareness of online fraud schemes. For Shopee as a business, it is necessary to review and strengthen its cybersecurity policies to prevent similar risks in the future. For consumers, when shopping online, they should carefully read store reviews, compare products with similar ones on other e-commerce platforms before purchasing, and thoroughly check product details before accepting delivery.

5.3. Proposed Solutions for Vietnamese E-Commerce Businesses

After major cyberattacks targeting eBay (2014) and Tokopedia (2020), Vietnamese e-commerce businesses need to draw important lessons and implement stricter security measures. Below are several solutions to enhance cybersecurity, protect customer data, and maintain user trust:

Firstly, strengthening advanced security systems and access management is crucial. Enhanced measures help detect suspicious activities early and prevent data breaches. Implementing continuous monitoring and abnormal behavior analysis provides early warnings of cyber threats. The eBay and Tokopedia incidents show that such systems could have prevented prolonged undetected intrusions. In Vietnam, many businesses still rely on basic security solutions without proactive monitoring, making them vulnerable to attacks. SMEs, in particular, face financial and human resource limitations, creating major gaps in cyber defense. Adopting emerging technologies like AI and applying proper data encryption can further enhance system security and minimize damage from potential breaches. Measures like data encryption are also crucial. In the cyberattacks on eBay and Tokopedia, the encryption of password and financial data prevented hackers from immediately decrypting and exploiting the information, thereby reducing the potential for greater damage.

Secondly, businesses should strengthen cybersecurity awareness among both employees and users. Employees play a vital role in security, so companies should invest in training, organize simulated attack exercises, and promote good practices such as using strong passwords and following security protocols. At the same time, user education is equally important, as many Vietnamese customers remain vulnerable to scams like fake payment pages or malicious apps. Therefore, companies should regularly share security tips and alerts through websites, emails, and other channels alongside internal training programs.

Thirdly, e-commerce businesses must comply with and stay updated on cybersecurity laws and regulations. As authorities tighten data protection requirements, companies need to proactively ensure compliance to avoid penalties and protect their reputation. In Vietnam, this is increasingly vital as legal frameworks become stricter. Businesses should adopt lawful data management processes, use data anonymization to safeguard user information, and maintain transparency in data collection and storage. In case of a breach, they must report incidents promptly to prevent loss of customer trust, as seen in the eBay and Tokopedia cases.

Fourth, businesses need to develop a cybersecurity incident response plan to minimize negative impacts. An important lesson from the eBay and Tokopedia cases is how to handle crisis communication. First, transparency is crucial when disclosing incidents to the media. eBay was criticized for delaying its announcement, while Tokopedia responded faster but with insufficient details. Therefore, companies should provide timely notifications with clear information on the impact and guidance for protecting accounts. Second, businesses must cooperate closely with authorities. Immediately after detecting an incident, they should work with cybersecurity agencies and security experts to investigate the cause and implement remediation measures. Finally, companies should run customer reassurance campaigns. This can include special offers or guarantees, such as refunds for losses due to security breaches, to retain customer trust.

6. CONCLUSION

The study has achieved its research objectives, helping to clarify the impacts of cybersecurity on e-commerce operations. At the same time, it proposes a set of solutions to help Vietnamese e-commerce businesses improve security systems, raise internal

awareness, provide security information to users, and develop incident response plans to minimize damage in case of a security breach.

First**,** the study identified theoretical issues related to cybersecurity in e-commerce.

Second**,** it assessed the impact of cybersecurity on e-commerce by examining two notable cyberattacks on eBay and Tokopedia. The study analyzed four key cybersecurity factors affecting e-commerce operations: advanced security systems and access management, cybersecurity training and awareness, cybersecurity laws and regulations, and incident response planning. From this, it evaluated the negative impacts of the two cyberattacks on eBay and Tokopedia.

Third**,** the research conducted surveys and collected data to evaluate how these four factors influence e-commerce in Vietnam. The survey lasted two months and received responses from individuals and businesses using or operating on e-commerce platforms. The study also analyzed a cybersecurity fraud case involving Shopee in Vietnam to assess its impact on the company.

Finally, the study proposed solutions for Vietnamese e-commerce businesses to optimize their systems, enhance security, and strengthen training, thereby minimizing the negative impacts of cyberattacks.

In conclusion, cybersecurity plays a crucial role in the development and sustainability of e-commerce operations. The cases of cyberattacks on eBay (2014) and Tokopedia (2020) show that security vulnerabilities not only affect user data but also negatively impact reputation, customer trust, and overall business performance.

REFERENCES

1. Alok Mishra, 2022. *Attributes impacting cybersecurity policy development: An evidence from seven nations. Computers and Security*, Volume 120.
2. Aniket Signh and Poornima Tapas, 2023. *Research methodology- Cyber security awareness*. Symbiosis Institute of Business Management, Pune.
3. Austin Bowler, 2024. *Case project: The attack on eBay.* Brigham Young University – Idaho.
4. Aya Aljaradat, 2024. *Modelling cybersecurity impacts on digital payment adoption: A game theoretic approach*. Journal of Economic Criminology, Volume 5.
5. Badriya, 2015. *An Analysis of eBay's Communication response to the hacking crisis and the impact on users'trust and behavioural intentions*. International Journal of Arts & Sciences, CD-ROM. ISSN: 1944-6934: 08(07):161–199.
6. CH.Sireesha, V.Sowjanya, K.Venkataramana, 2017.*Cyber security in E-commerce*, International Journal of Scientific and Engineering Research Volume 8, Issue 5.
7. Daniel Ruby, 2024. *Ecommerce Statistics: Global Data*. Demand Sage, Boston.
8. Egger, F.N, 2000. *Towards a model of trust for e-commerce system design*. Center for User- System Interaction, Eindhoven University of Technology, Einhoven.
9. Fortinet, 2023. Ransomware statistics and ransomware trends. Sunnyvale.
10. Houssam Saleh, Amira Rezk, Sherif Barakat, 2017. *The impact of cyber crime on e-commerce*. International Journal of Intelligent Computing and Information Science, Volume 17, No.3.
11. International Telecommunication Union, 2018. *Global cybersecurity index 2018*. Geneva
12. International Telecommunication Union, 2020. *Global cybersecurity index 2020*. Geneva.
13. International Telecommunication Union, 2024. *Global cybersecurity index 2024*. Geneva
14. Jiehui Huang, Uday Murthy, 2024. *The impact of cybersecurity risk management strategy disclosure on investors' judgments and decisions*. International Journal of Accounting Information Systems, Volume 54.
15. Jonathan Juin Yang Pan and Chun Che Fung, 2009. *Malware's impact on e-business and m-commerce: they mean business!*. The 8th International Conference on e-Business, Bangkok, Thailand, October 28th-30th, 2009.
16. Julian Jang-Jaccard, 2014. *A survey of emerging threats in cybersecurity*. Journal of Computers and System Sciences, Volume 80, Issue 5, Pages 973-993.
17. Julius Perkasa, Jeane Neltje Saly, 2022. *Legal Liability of Marketplace Companies Against Leaking of User Data Due to Third Party Breaking According to Law Number 8 of 1999 Concerning Consumer Protection (Case Example: Tokopedia User Data Leaking in 2020*). Advances in Social Science, Education and Humanities Research, volume 655.
18. Mateusz Brodowicz, 2024. *Cyber Attack on eBay company: The summer of 2014 Report.* University of Houston.
19. Mukherjee, A., & Nath, P, 2007. *Role of Electronic Trust in Online Retailing: A Re-Examination of the Commitment-Trust Theory*. European Journal of Marketing, 41, 1173-1202.
20. Ni Made AynIntan, 2021. *The influence of customer experience, ease of use, and trust on repurchase intention (Case study of Tokopedia Consumers in Denpasar)*. American Journal of Humanities and Social Sciences Research, Volume 5, Issue 2, Pages 378-383.
21. Nguyen Phi Hung et al., 2024, *Assessing cybersecurity risks and prioritizing top strategies In Vietnam's finance and banking system using strategic decision-making models-based neutrosophic sets and Z number* , Research Center of Applied Sciences, Faculty of Business, FPT University.

22. Nwosu Amarachukwu Grace, 2024. *A cyber security case study on eBay data breach*.
23. Pabitra Kumar Sahoo, 2023. *Top 10 latest security threats in E-commerce and their solutions.*
24. Ruchi Gupta, 2024. Cyber threats in e-commerce: *Trends and mitigation strategies,*Vol.1, Issue 3, Journal of Advanced Management studies.
25. Shweta, Vikas Deep, Naveen Garg, 2017. *Cyber threats and its impact on e-commerce sites. International Journal of control theory and applications*, Volume 10, Number 15.
26. Shahzrad Shahriari, Mohammadreza Shahriari, 2017. *Perspective and prospect of E-commerce and M-commerce*, Vol 5, Issue 3, International Journal of Research in Management and Social Science.
27. Steve Roberts, 2018. *Learning lessons from data breaches. Network Security, Volume 2018, Issue 11, Pages 8-11.*
28. VTV, 2024. *Khởi tố hàng loạt đối tượng chiếm đoạt mã giảm giá trên Shopee.*