Contents lists available at GrowingScience

International Journal of Data and Network Science

homepage: www.GrowingScience.com/ijds

Investigating of the role of cybercrime and e-brand trust on purchase interest of e-commerce platforms

Mohammad Fadil Imran[a*] and Hendra Gunawan[a]

[a]*Sekolah Tinggi Ilmu Kepolisian, Jakarta, Indonesia*

CHRONICLE

Article history:
Received: July 11, 2024
Received in revised format: August 2, 2024
Accepted: August 8, 2024
Available online: August 8, 2024

Keywords:
Cybercrime
e-brand trust
Purchase intention
e-commerce platform
SEM-PLS

ABSTRACT

In this digital era, the use of the Internet in business transactions through e-commerce platforms has created many conveniences, the development of Internet technology has given rise to crimes called cyber crime or crimes through the Internet network. The purpose of this study is to investigate the relationship between cybercrime and purchase intention on e-commerce platforms, and the relationship between e-brand trust and purchase intention on e-commerce platforms. This research method is a quantitative method to analyze the relationship between variables, research data was obtained by distributing online questionnaires through social media platforms, and questionnaires containing statement items were designed using a Likert scale of 1 to 5. The respondents of this study were 535 consumers who had shopped online on e-commerce platforms determined by the simple random sampling method. Data analysis used the PLS Partial least squares SEM (PLS-SEM) technique. In the study, the outer model which is called the measurement model has a meaning between indicators connected by other variables. The measurement model of convergent validity, discriminant, and reliability was used. The standard loading factor value in the concurrent validity test must be > 0.7 or greater than the established criteria. The same applies to the discriminant validity test, which uses a larger value for the loading factor. The construct reliability test uses Cronbach's alpha and the composite reliability value. The hypothesis testing uses partial least square (PLS) which is the inner model test result, namely the R-square output, path coefficient, or t-statistic. The convincing t-statistic result > 1.96 is that Ha is accepted and Ho is rejected. If the probability number (p-value) <0.005 is included, then Ha is accepted. If the p-value is <0.05 (or 5%), the t-statistic is > 1.96, and the beta coefficient is positive, then Ha can also be accepted. The results of the analysis show that cybercrime has a positive effect on consumer purchasing intentions on e-commerce platforms and e-brand trust hurts consumer purchasing intentions on e-commerce platforms.

1. Introduction

The rapid development of human reason creates and requires computer network technology. The Internet is a commercial community activity that is the largest and fastest-growing part that has crossed the boundaries of a country. Through the internet network, we can find out what is happening right now in other parts of the world. With the internet world also called cyberspace, almost everything can be done. The positive side of this virtual world certainly forms the trend of world technology development with all forms of human creativity. However, negative impacts cannot be avoided, for example in the form of pornography that is rampant on the Internet media (Zahari et al., 2019). The development of Internet technology has given rise to crimes called cyber crimes or crimes through the Internet network. The emergence of several cases of cybercrime in Indonesia is a phenomenon, such as credit card theft, hacking of various sites, tapping other people's data transmissions (for example email), and data manipulation

* Corresponding author.
E-mail address mfadilimran@stik-ptik.ac.id (M. F. Imran)

ISSN 2561-8156 (Online) - ISSN 2561-8148 (Print)

doi: 10.5267/j.ijdns.2024.8.010

by preparing unwanted commands for computer programmers. The various actions above can be subject to criminal acts, both formal and material crimes. Formal crimes because they involve someone's actions accessing other people's computer data without permission, while material crimes are those actions that have caused losses to others. The development of the era has led to the development of technology and information. With technology, everything can be obtained instantly. This can be seen from the many applications that provide various needs so that everyone does not need to go somewhere, but rather just buy online (Mujtaba, 2024).

The pattern of business activities and trade industries has undergone many changes, this is influenced by the rapid development in the fields of communication technology, media and informatics. One of the technological advances that is currently widely used by people, organizations and companies around the world is the Internet. This phenomenon is certainly a business opportunity for several parties who then seize the opportunity by selling via the Internet until an online store is created as part of e-commerce. E-commerce can generally be interpreted as a concept regarding the process of buying, selling or exchanging either in the form of products, services, or information with computer network media including the Internet (Sabillon et al., 2016).

The advancement of information and communication technology is currently growing rapidly, where information is very easily spread using information technology and the internet. In this era of information technology, the development of internet users themselves has increased every year. Internet users in Indonesia, every year increase, continuously. In 2023, internet users in Indonesia will only reach 98 million people. In cyberspace, almost everything can be done. The positive side of this cyberspace forms a trend in the development of world technology with all forms of human creativity. In addition, the presence of the internet today makes it easier for someone to access or obtain information, and interact with each other on social media or social networks without having to meet face to face. However, various problems arise due to the misuse of this information technology (Kaakinen et al., 2018). On the other hand, the use of the internet which is almost uncontrolled causes various crimes in cyberspace, the number of online crimes aka cybercrime has become a new trend in many countries today, including Indonesia. cybercrime as a crime in the computer field can generally be interpreted as the illegal use of computers. The emergence of cybercrime cases in Indonesia is a phenomenon, such as cases of credit card theft or carding, hacking of various sites, tapping of other people's data transmissions, and data manipulation by preparing unwanted commands for computer programmers (Leukfeldt & Holt, 2022). Cybercrime in the future will shift to social networks with the increasing number of social network users such as Facebook, Twitter and so on.

Today, the role of information technology is increasingly important, for the interests of individuals, businesses, and governments. With the existence of information technology, especially the internet, the world seems to be borderless, there are no more barriers of space and time in interacting with anyone, and anywhere (Basuchoudhary & Searle, 2019). Consumers can buy products from other countries via the Internet, make transactions in seconds, search for information using search engines, or provide public services using various e-government applications. In the economic sector, electronic systems are developed as infrastructure for smooth electronic trade. On the other hand, information technology opens up opportunities for new forms of crime that are more sophisticated than conventional crimes. To overcome this, it is not enough to approach it through the conventional legal system, considering that its activities are no longer limited by the territory of a country, in the sense that access can easily be done from any part of the world. Negative impacts in the form of losses can occur both to the perpetrators of the transaction and to other people, who have never been in contact at all, for example in the theft of credit card funds through shopping on the internet.

All the various advances in smartphone technology that can access the virtual world quickly, have slowly but surely changed the behavior of both individuals and our society in general today. The development of information and communication technology has also caused world relations to become limitless and caused significant social, economic and cultural changes in society to take place so quickly (Khoiriah et al., 2024). In addition, the development of today's information and technology flow is a double-edged sword, because, in addition to providing good/positive contributions to society, it also has negative impacts on the other side. Negative impacts can arise when errors occur caused by computer devices that will result in major losses for users or interested parties. These deliberate errors lead to misuse of computers so they have the potential to use computer and internet media to commit various crimes. Various crimes that use computer and internet technology as their media have recently shown significant numbers, both in terms of quantity and quality (Khiong, 2022). Various types of crimes range from light to the most severe. Indonesia can get 42,000 cyber attacks per day. This tends to undermine the security of companies and countries, as well as hinder individual development considering the mobility of internet usage which tends to increase from day to day. In connection with the increasingly rapid flow of globalization, currently, people tend to no longer keep their money in their wallets (Kshetri, 2013). The rapid advancement of technology, especially in urban areas, has made physical money very rarely used. The advancement of banking technology has changed every aspect of our lives to the point that most people are more afraid of not being connected to the internet than losing their wallets. In addition to the positive impact in terms of ease of online transactions, technological advances also hurt cybercrime such as data theft.

In addition to the various positive impacts in terms of ease of online transactions, technological advances also have a dangerous negative impact. The benefits of ease of transactions offered make the circulation of money in cyberspace even greater. The increasing circulation of money has also caused crime patterns to slowly change from conventional crimes such as pickpocketing, and snatching, to thuggery, to cybercrime such as data hacking, and carding, to online fraud (Mulyandi & Tjandra, 2022). Cybercrime, also known as cybercrime, is a form of crime that occurs in cyberspace via computers, mobile devices, and the internet. The perpetrators of this cybercrime are generally 'smart people' who understand how algorithms and computer programming are run. Through certain algorithms, perpetrators can easily analyze, find loopholes, and ultimately break into our devices. When the perpetrators have mastered the device, the perpetrators can freely steal our data and use it for their gain. In Indonesia itself, cybercrime cases have been rampant, especially during the pandemic. The ease of digital transactions coupled with the turmoil in the world economy due to the pandemic has led to the emergence of online lending platforms. Several cases of cybercrime related to online loans have finally emerged, namely, the rampant theft of data in the form of ID cards to be misused for online loans. Several people admitted that they were suddenly called by unknown people asking for debts that they had never borrowed (Khoiriah et al., 2024).

The development of technology and information has brought many changes in the business world. One form of change that has occurred in the business world is the use of Internet media as a new transaction system known as electronic transactions. In general, e-commerce can be defined as business activities involving consumers, manufacturers, service providers, and intermediary traders, using computer networks (computer networks), namely the Internet (Akinbowale et al., 2020). E-commerce is a business activity involving consumers, manufacturing industries, service providers, and business actors using Internet networks. In the business sector, the use of technology can improve performance. Currently, companies compete with the structural transformation of their internal foundations by developing e-business strategies. This is because e-commerce creates practical business transactions without using paper and without direct meetings. E-commerce brings changes to business actors who have been managing their businesses in the real world, and then developing these businesses into the virtual world. This change can be seen from the number of "online shops" on internet sites. In this system, business actors advertise products sold on the internet, and consumers who are interested in the product can then contact the business actor concerned to make a sales agreement, including regarding the method of shipping goods and the method of payment made. E-commerce uses an electronic payment system, namely through electronic fund transfer (EFT) (Hasbullah, 2022). Transactions in this business also have a fast moving quickly nature which gives rise to various transactions that do not require direct meetings between sellers and buyers. Buyers simply use facilities in the form of applications available via cell phones or the internet/website. Agreements between business actors and consumers made through e-commerce benefit many parties, so it is not surprising why agreements through e-commerce are in great demand amid a pandemic like today. For consumers, e-commerce can change the way they buy the desired goods/services (Adejumo & Oyeniyi, 2024). Meanwhile, for business actors, agreements through e-commerce can simplify the marketing process of goods/services. Although the use of the Internet in business transactions always promises many conveniences, this does not mean that e-commerce is a system that is free from problems, especially for countries that have not regulated e-commerce.

There are risks for consumers when conducting e-commerce transactions. First, consumers are faced with conditions of uncertainty due to not being able to directly assess the quality of products sold on internet sites. Second, business actors and consumers do not meet face-to-face, which results in a lack of communication. E-commerce is a high-risk transaction because the laws and regulations governing these transactions are still very limited (Cao et al., 2024). In practice, there have been many problems that have harmed consumers as a result of the use of the internet media in online buying and selling transactions. The problem that often occurs is that the goods ordered and the goods that arrive do not match, meaning that there are deficiencies in terms of colour, type and quality of materials, even worse, the goods ordered are not sent by the business actor so that in responding to this, Indonesia has had a legal, namely Law Number 8 of 1999 concerning Consumer Protection. Fraud in online buying and selling activities is one of the cybercrimes and of course, it will be difficult to catch the perpetrators. First, handling the problem of cybercrime is still hampered by the problem of space. Cyberspace is a world without borders so the police need a long time to uncover the perpetrators of online buying and selling activities because of the unclear identity of the perpetrators who are often falsified. Second, in terms of collecting evidence it will be difficult considering that this legal event occurred in an electronic system, in collecting evidence an easy way that can be attempted is to look for clues that indicate there has been malicious intent in the form of unauthorized access, fake identity during registration, location of the device, and gadgets used to commit the crime (Julianti et al., 2024). This can be realized by seeing and listening to witness statements in court, electronic letters or printouts of data, or also from the defendant's statement in court. Third, cybercrime perpetrators are difficult to identify due to the strong network between fellow cybercrime perpetrators. Fourth, the facilities and infrastructure in the cybercrime unit in Indonesia is currently not optimal so the law enforcement process is hampered. Realizing a clue from the evidence found in cybercrime will be difficult if it is only based on witness statements, letters, and defendant statements, although this is still possible to apply.

2. Literature review and hypothesis development

2.1 Cybercrime

Cybercrime is a crime that utilizes computer technology and internet networks to hack, steal, fraud, spread viruses, and other digital crimes (Cascavilla et al., 2021). Cybercrime itself is included in the form of crime that utilizes internet technology, one type of crime is fraud in online businesses on the internet. This fraud is rampant because of the consumerist nature of society, coupled with the ease of facilities and infrastructure in accessing it. The types of cybercrime themselves include Carding, a form of abuse in cyberspace when the perpetrator can shop using the victim's number and credit card. Hacking, hacking activities or breaking into someone else's computer network system for a specific purpose (Elisanti et al., 2024). Phishing is in the form of stealing someone's data. In most cases of fraud such as those that occur on social media, for example, this group of crimes is included in Computer Related Fraud or fraud that is deliberately carried out for personal gain so that it harms others. For example, the spread of incorrect or inappropriate information, so that later there will be a party who is harmed by the information. Meanwhile, based on the type of activity, cybercrime is a crime committed by entering/infiltrating a computer network system illegally, without permission or without the knowledge of the owner of the computer network system that is entered (Behl et al., 2019). Usually, the perpetrators of the crime (hackers) do it to sabotage or steal important and confidential information. However, some do it just because they feel challenged to try their skills in penetrating a system that has a high level of protection. It is a crime to enter data or information into the internet about something that is not true, unethical, and can be considered unlawful or disturbing public order (Brands & Van Doorn,2022). For example, the loading of fake news or slander that will destroy the dignity or self-esteem of other parties, things related to pornography or the loading of information that is a state secret, agitation and propaganda to fight the legitimate government, and so on. It is a crime to falsify data on important documents stored as scriptless documents via the Internet.

Cybercrime is a crime that uses the internet network to conduct espionage activities against other parties, by entering the target party's computer network system. This crime is usually aimed at business rivals whose important documents or data are stored in a computerized system. This crime is committed by creating interference, damage or destruction of data, computer programs or computer network systems connected to the internet (Bekkers et al., 2023). Usually, this crime is committed by infiltrating a logic bomb, computer virus or a certain program, so that data, computer programs or computer network systems cannot be used, do not run properly, or run as desired by the perpetrator. This crime is aimed at Intellectual Property Rights owned by other parties on the internet. An example is the illegal imitation of the appearance of a web page on a site belonging to someone else, broadcasting information on the internet that turns out to be someone else's trade secret, and so on. This crime is aimed at someone's information which is very private and confidential. This crime is usually aimed at a person's personal information stored on a personal data form stored on a computer, which if known by others can harm the victim materially or immaterially, such as credit card numbers, ATM PINs, hidden disabilities or diseases and so on. Crimes using computer technology are carried out to damage the security system of a computer system and usually carry out theft, and anarchic actions once they gain access. Usually, we often misinterpret between a hacker and a cracker where the hacker himself is identical to negative actions, whereas a hacker is a person who likes to program and believes that information is something very valuable and some are public and confidential. Carding is a crime using computer technology to make transactions using someone else's credit card so that it can harm the person both materially and non-materially.

2.2 e-brand trust

Trust is the willingness to make oneself sensitive to actions taken by a trusted party based on belief. Trust has shown a profound impact on individual behavior. Including the e-payment payment system must make customers believe in the services and products offered, otherwise if customer trust does not exist, consumers will automatically not use the provision of e-commerce and e-payment in online business. Customer trust is not obtained just like that, but the process and efforts given can later provide customer trust in the service products and goods that will be offered (Gill et al., 2021). To gain high trust from customers, the right and brilliant strategy is needed so that customer trust can be obtained and maintained in the future. After trust exists on both sides and then communication and coordination can be applied to carry out transactions without any fear of fraud. With high trust, in making transactions, a sense of security will be felt and the possibility of the same transaction will occur again. Brand trust is the hope or high possibility that the brand will result in positive results for consumers. Brand trust is the willingness of the average consumer to rely on the consumer's ability to perform brand functions. brand trust is the existence of high expectations or possibilities that the brand will result in positive outcomes for consumers (Hanaysha, 2022). brand trust is a brand that successfully creates an impressive brand experience in consumers that is sustainable in the long term, based on the integrity, honesty and politeness of the brand. Based on several definitions above, it can be concluded that brand trust is the willingness and willingness of individuals as consumers to trust a brand to produce positive results based on experience or integrity, honesty and politeness of the brand. brand trust components are based on subjective consumer assessments or are based on several perceptions, namely: Consumer perception of the benefits that can be provided by the product/brand. Consumer perception of brand reputation, consumer perception of the similarity of their interests with the seller and their perception of the extent to which consumers can control the seller and perception.

Brand trust is the customer's trust in a brand or company. Customers have confidence that the company or band can solve their problems. The company or brand is also considered worthy of customer respect, which provides added value (Ibrahim, 2016). According to the Edelman Trust Barometer Special Report, brand trust is the second most important reason, after price, why consumers and businesses buy products. Buyers look for companies that can deliver on brand promises. Brand trust is the result of consistently positive experiences and good interactions between brands and consumers over some time. Brand trust involves elements such as Consistent product quality, Brand integrity, Transparency, Commitment to values relevant to consumers, and Ability to meet expectations and promises given trust plays an important role in influencing consumer behavior. Consumers who trust a brand are more likely to choose products from that brand than other brands that are less well-known or less trusted. This can certainly generate competitive advantages for the brand. In addition, customer trust also helps maintain and expand market share, as well as build long-term relationships (Karine, 2021). So it's no wonder that brand trust is one of the important foundations in the relationship between consumers and brands or companies. This reflects the belief and loyalty developed by consumers towards the brand's ability to meet expectations and deliver the promised value consistently. Furthermore, brand trust can turn into brand loyalty when consumers are confident with your product. This makes consumers not hesitate to recommend the product to family, friends, and colleagues. Conversely, losing trust can hurt brand image and can result in decreased sales and ongoing reputational losses. Therefore, maintaining and strengthening brand trust should be a primary focus for every brand that wants to build lasting relationships with consumers. Trust is a very important factor in converting buyers or consumers into first-time customers. Consumers who believe in a brand tend to entrust their problems to that brand (Lien et al., 2015). Consumer trust in a brand will have an impact on the loyalty of consumer attitudes or behavior towards a brand. Brand trust is a feeling of security that consumers have as a result of their interactions with a brand based on the perception that the brand is reliable and responsible for the interests and safety of consumers. In addition, brand trust is the expectation of the reliability of the brand's good intentions.

2.3 Purchase interest

Purchase interest is part of purchasing behavior, which will then form loyalty in consumers. In addition, customers who commit are generally more receptive to the expansion of new products offered by the company. The suitability of the performance of the products and services offered with what consumers expect will provide satisfaction and will result in consumer repurchase interest in the future. Repurchase interest is a consumer attitude in terms of taking the initiative to buy the same product for the second time or even beyond (Mishra et al., 2022). Repurchase interest is a repurchase activity carried out by a consumer who has a high level of satisfaction when the consumer has tried to adopt the product and gets a positive response to a trust from the product and the consumer will intend to revisit or consume the company's products again. From the opinions above, repurchase interest can be concluded as a consumer behavior that has felt the quality of the product, and the quality of service then the consumer feels satisfaction, then loyalty will arise in the consumer, then the consumer will intend to make a repurchase. Factors that influence purchase interest are related to feelings and emotions, if someone feels happy and satisfied in buying goods or services, it will strengthen consumer purchase interest (Nasution et al., 2018). In addition to feelings and emotions, other factors that influence consumer interest are the desire to buy, buying interest based on experience in choosing and buying and using a product, buying interest is influenced by a person's emotions who want and need goods or services that can be based on personal experiences that come from within or outside, for example, the experiences of others who have used the product. Consumer buying interest is influenced by culture, social, personal and psychology. These factors are factors that drive consumer interest in carrying out the decision-making process in deciding whether or not to buy a product or service. Buying interest is influenced by a person's desire to make a purchase, choose the right product for their needs, experience in using the product, and the desire to own the product.

Purchase intention is often used to analyze consumer behavior. Before making a purchase, consumers will collect information about the product based on personal experience and information from their environment. After the information is collected, consumers will start to research the product, evaluate it and make a purchase decision after comparing products and considering them. Intention is generally referred to as a fully planned purchase. Consumers will be more willing to invest time and energy in shopping and buying. Consumers form preferences for brands in the choice set. Consumers also form an intention to buy the most preferred brand. A purchase decision is an individual's thought to evaluate various product options and make a choice from many options. Purchase decision as an individual's problem-solving activity and then choose the most appropriate alternative action after going through the decision-making stages (Riek et al., 2015). The purchase decision is a psychological process that buyers go through starting from the stage of observing the product. If it interests consumers, they continue to the interest stage to learn more about the product's features, and if the interest is strong, they continue to have a desire because they need the product.

2.4 E-Commerce

The development of information technology has changed many aspects including changes in the financial sector, many people today want things that are usually done to be practical including payment methods. The term online payment is now commonly known as e-commerce, which is a payment system for services or goods purchased via the Internet. Even the term e-commerce is not only done in online purchases in offline purchases, many stores already provide online payment systems (e-payment in their stores (Ratnasari et al., 2021). The definition of e-commerce itself is the transfer of electronic payment values from the payer to the recipient of payment through the e-commerce mechanism. In the implementation of transactions using e-payments, security and trust issues are important to consider considering that sellers and buyers do not meet face to face, especially in the online shopping process. Unlike offline shopping, sellers and buyers can meet directly to transact and it is difficult to commit fraud, security and trust are not important factors. The benefits obtained by online store business actors are making the sales process easier, more efficient, without errors, and on time (Rughiniș et al., 2024). The benefits obtained by E-Commerce Management or companies are getting increased income, and customer loyalty. E-commerce (electronic commerce) is a buying and selling transaction that is carried out online using electronic media. In the world of trade, e-commerce brings many changes, the changes in question are now the buying and selling process is no longer like in the days of conventional stores, namely face-to-face meetings (Saban et al., 2002). Sellers and buyers now only need to do it online. The presence of e-commerce makes transactions more efficient and faster. Especially with the integration of various payment systems with the presence of API (Application Programming Interface) technology. An example is through a virtual account or e-wallet. Changes in the era have made e-commerce facilities not only via telephone and television but now more using the internet. It should be underlined that some people misunderstand the marketplace with e-commerce. The marketplace is one model of e-commerce. Another form of e-commerce can be a website or online store application (Smith, 2004).

2.5 Relationship between cybercrime and consumer purchase intention

Cybercrime business transactions raise concerns for consumers because cybercrime activities affect consumer purchase intention to shop in e-commerce. Fear of cybercrime affects consumers to transact or buy on digital platforms (Shareef et al., 2019).The results of the study show that most consumers are afraid and worried about making purchases in cyberspace which affects consumer behavior in purchasing to transact on digital platforms. Perceptions of cybercrime affect consumers to transact online. Research related to the threat of cybercrime has been widely conducted, for example, research by Hartati and Muhammad through descriptive qualitative methods to analyze the impact of cybercrime in Indonesia and regulations with very high intercorrelation research (Strzelecki & Rizun, 2022). The study found that the need to handle cybercrime in e-commerce must be done collectively by customers and e-commerce companies, The latest study by Subandi et al on improving security in simple network time protocol (SNTP) to detect cybercrime in network activity found that it was necessary to migrate Sophos software to Trend Micro, From several previous studies, this study is relatively new where research related to cybercrime threats in Indonesia was conducted by selecting national and international publications that were analyzed based on a systematic review (Sarkar & Shukla, 2023). Based on the study above, the hypothesis is formulated:

H$_1$: *Cybercrime has a positive effect on consumer purchasing intentions.*

2.6 The relationship between e-brand trust and consumer purchasing intentions

Brand trust has a very significant influence on businesses or brands in various aspects. Here are some of the main benefits of brand trust for businesses or brands., consumers who have strong trust in a brand tend to be more loyal customers (Sarkar & Shukla, 2023). They will choose products from that brand again without excessive consideration. Customers may remain loyal even though there are alternatives available. Brand trust can increase sales conversions because consumers who trust will be more likely to buy products from that brand. Consumers will feel confident that the product will meet their expectations (Sharma & Annaboina, 2024). When customers know, like, and trust a brand, they are often willing to pay more for it. When a brand name becomes a premium product, companies can charge higher prices. This will certainly result in increased revenue and greater profits. Strong Reputation: Consistent and positive trust from consumers can build a good brand reputation. A good reputation can help a brand survive in the long run and even become a valuable asset in a crisis. Consumers who trust a brand are more likely to recommend it to others. Word of mouth has a big impact on the purchasing decision process, and this can help brands attract more potential customers. Consumers who have brand trust tend to be less sensitive to price changes (Sahin et al., 2011). They are more willing to accept price increases if they are confident that the product they are getting is still of high quality. Brands with strong brand trust can have a significant competitive advantage. Consumers tend to choose brands they trust over competing brands that have not built the same level of trust. The same is true when a crisis or challenging situation occurs for a brand or company (Wahab et al., 2023). Brands that have strong customer trust are more likely to recover and overcome negative impacts. Consumers who trust a brand are more likely to give the benefit of the doubt rather than switch to another brand. Based on the study above, the following hypothesis is formulated:

H$_2$: *e-brand trust has a positive effect on consumer purchasing intentions.*

3. Method

This research method is a quantitative method to analyze the relationship between variables, research data was obtained by distributing online questionnaires through social media platforms, and questionnaires containing statement items were designed using a scale of 1 to 5. The respondents of this study were 535 consumers who had shopped online on e-commerce platforms, as determined by the simple random sampling method. Data analysis used the PLS technique. Partial least squares SEM (PLS-SEM) is a non-parametric method that does not make assumptions about distribution and can be evaluated by small samples. In the study, the outer model, which is called the measurement model, has a meaning between indicators connected by other variables. The measurement model of convergent validity, discriminant validity, and reliability is used. The standard loading factor value in the concurrent validity test must be> 0.7 or greater than the established criteria. The same applies to the discriminant validity test, which uses a larger value for the loading factor. The construct reliability test uses Cronbach's alpha and the composite reliability value. Meanwhile, the design multicollinearity test can be used by the variance inflation factor and tolerance value. In the internal model assessment technique R-square, SRMR (Standardized Root Mean Square Residual) is considered appropriate to understand the requirements between models. In addition, there is an effect size used to check the impact of exogenous latent variables by the R-square of endogenous latent variables. While F-Square is used to check the level of risk of measurement. The hypothesis testing uses partial least squares (PLS) which is the result of the inner model test, namely the R-square output, path coefficient, or t-statistic. The convincing t-statistic result> 1.96 is that Ha is accepted and Ho is rejected. If the probability number (p-value) <0.005 is included, then Ha is accepted. If the p-value is <0.05 (or 5%), t-statistic> 1.96, and the beta coefficient is positive, then Ha can also be accepted. The research hypothesis model is shown in Fig. 1 as follows:

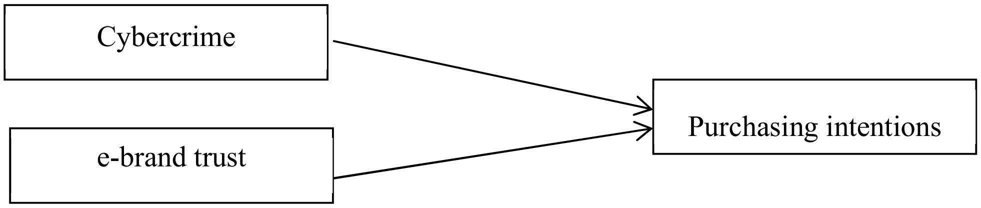

Fig. 1. Research Model

4. Result and discussion

4.1 Partial Least Square (PLS) Analysis

In this study, this study uses the Partial Least Square (PLS) analysis method. This analysis method has several advantages over several other analysis methods. One of them is that the use of this test method can use samples that have relatively small quantities and can apply all types of data scales. This analysis method has three stages. Among others, namely the measurement model (outer model), structural model (inner model), and hypothesis testing.

4.2 Validity Test

The validity test is used to measure whether the data collected is valid data or not. This test aims to assess whether the instrument measures the intended construct or variable accurately and reliably. The validity test model in this study was measured using convergent validity and discriminant validity tests.

4.3 Convergent validity

Convergent validity is the level to which the results of measuring a concept show a positive correlation with the results of measuring other concepts that theoretically should be positively correlated. Convergent validity testing is carried out by looking at the loading factor value (correlation between item scores/component scores and construct scores) and the average variance extracted (AVE) value. To assess convergent validity, the loading factor value must exceed 0.7 intolerance to 0.5 and the average variance extracted (AVE) value must be more than 0.5. The following is a picture of the measurement model (Outer Model) used to measure the loading factor value of the PLS program in this study:

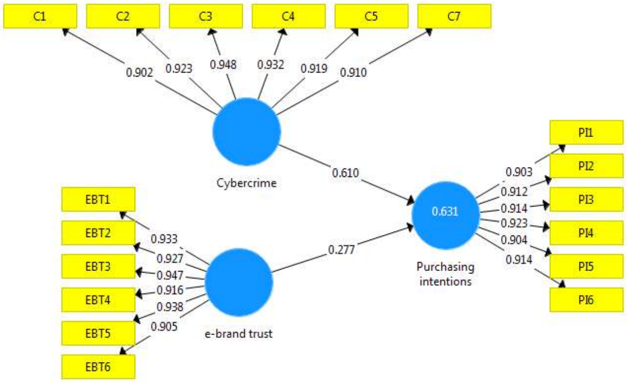

Fig. 3. Convergent validity

Discriminant validity proving that each underlying concept has differences from other variables. To test the second level of discriminant validity, AVE (Average Variance Extracted) is used as the method for each construct and latent variable. It is said to be good if the square root of AVE in several constructs is higher than the correlation between latent constructs of discriminant validity, and the AVE of all latent constructs must be >0.5.

Table 1
Discriminant Validity

Variable	AVE
Cybercrime	0.645
e-brand trust	0.687
Purchase Interest	0.634

The AVE shows that all variables are more than 0.5. So that all variables and indicators of this study meet discriminant validity and have good values in each compilation of data measurements. Reliability testing is a statistical test used to measure the extent to which a measurement instrument can produce consistent and reliable results. The testing method in this study was measured using Cronbach alpha and composite reliability. a. Cronbanch Alpha Evaluates the lowest value of the reliability of each variable. Cronbach Alpha is said to be good if its value is >0.6 (the construct is declared reliable) for explanatory research and >0.7 for confirmatory.

Table 2
Discriminant Validity

Variable	Composite Reliability	Cronbach alpha
Cybercrime	0.823	0.814
e-brand trust	0.854	0.843
Purchase Interest	0.826	0.8123

The Cronbach Alpha above shows that the entire table data is reliable, which is 0.7 (the construct is said to have high reliability). The results of the table show that the entire Composite Reliability variable has a value of >0.7, so it meets the reliability requirements. It is concluded that all variables meet the requirements for obtaining research data that shows internal consistency or can be relied on. All data has a large value in its reliability. Structural Model (Inner Model) After passing the validity and reliability tests, the next test can be carried out, namely the structural model. This evaluation model is to estimate whether there is a cause and effect in the relationship of latent variables (cannot be evaluated directly), in the form of testing the relationship of latent constructs carried out by bootstrapping on PLS as below:

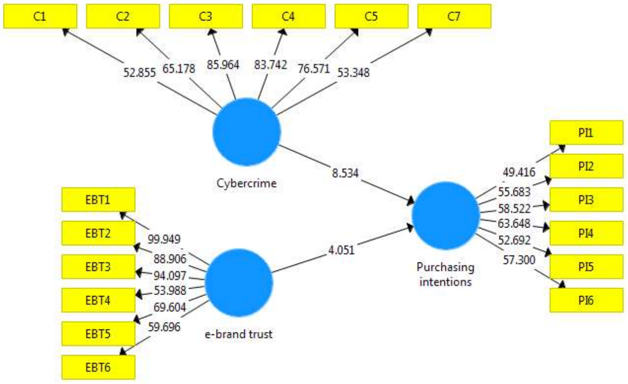

Fig. 3. Hypothesis Testing

4.4 Hypothesis Testing

To see the level of significance in each research variable concerned. Seen through the T-Statistic value of the exogenous latent variable path coefficient on the endogenous latent variable (comparing the t table). In testing through T-statistics, you must first know whether the hypothesis you have has a direction or not. This research hypothesis is tested using the bootstrapping procedure on sample data, obtained from the structural model data that was tested previously. This hypothesis test must meet three criteria, the first is through the original sample value to complete the regression equation, by knowing the direction of the hypothesis being tested, namely if the original sample is positive, it means that the direction of the research is positive, and vice versa. The second is to look at the T-Statistic value to test the significant influence of the relationship between variables obtained from the previous test. The third is to look at the P-value value to compare whether the value is below the significance standard. The way to accept the development of the hypothesis in this study is that the P-value value must reach <0.05.

Table 3
Hypothesis testing

Hypothesis	T value	P value	Result
Cybercrime → Purchase interest	8.534>1,96	0.000 <0.050	Supported
e-brand trust → Purchase interest	4.051>1,96	0.000<0.050	Supported

4.5 Relationship of Cybercrime to Consumer Purchase Intention

From the table above, it can be seen that the original sample on the path coefficient of the company value test results by company size has a positive direction coefficient of 0.288, and the P-value value is less than 0.05 ranging from 0.007. Showing only two criteria according to the provisions (variables are interrelated and the value is positive), so it is concluded that hypothesis 1 is accepted. Threats are any form of action or effort by certain individuals or groups that can threaten the safety of one or another group. Threats to the security of users' data in e-commerce are in the form of digital crimes or attacks that threaten the security, privacy, and crime of users. The main threat to the security system in e-commerce that is seen will have a devastating effect not only on business actors but also on consumers, this threat also affects the security of personal data of e-commerce users because the more or more dangerous the threat, the more the security of the user's data is threatened. Threats have a major influence on the security of personal data in e-commerce. This is because e-commerce is a form of online trading, where customers make transactions by providing personal information such as name, address, telephone number, credit card number, and so on. If this information falls into the wrong hands, e-commerce users can suffer financial losses and even their identities can be stolen and misused by irresponsible parties (Sharma & Annaboina, 2024). Most people have concerns when they shop and transact online on e-commerce. This shows that the security factor of user data privacy is still vulnerable to the threat of crime or cybercrime that attacks e-commerce users, both sellers and buyers, which causes losses due to misuse of personal information or personal data. The Impact of Risk on the security of personal data on e-commerce users. The threat of cybercrime that occurs on the personal data of e-commerce users is certainly detrimental to both users and companies. No action occurs without risk. In the context of personal data security in e-commerce, the risk is related to the possibility of damage or loss of customer personal data, as well as the potential negative impact on the company such as bad reputation, legal sanctions, or loss of customers (Strzelecki & Rizun, 2022). The author hypothesizes that this risk also affects the security of the personal data of e-commerce users. Risks can impact the security of e-commerce users' data because, in e-commerce transactions, users provide personal information such as name, address, telephone number, and credit card number or other financial information. Risks that arise in the security of e-commerce users' data can cause data security breaches that can harm users and companies that provide e-commerce services (Wahab et al., 2023).

System vulnerabilities in e-commerce infrastructure can be a loophole for cybercriminals to access customer data, therefore this paper discusses security strategies against threats to the personal data of e-commerce users. The author has a hypothesis that this security strategy affects the security of the personal data of e-commerce users. Security strategies greatly affect the security of personal data of e-commerce users. This is because the right security strategy can help protect the personal data of users which are of course private from security threats (Akinbowale et al., 2020). The better the strategy used; the less cybercrime will occur on the personal data of users. The security strategy implemented by e-commerce is very important in maintaining the security of the personal data of e-commerce users. the online shop has used the OTP (One-time password) security strategy when consumers want to log into their accounts as a form of protection for user Personal Data (Akinbowale et al., 2020). This security strategy is used to further maintain the security of user personal data. By implementing the right security strategy, e-commerce owners can ensure that customer personal data and other important information are protected from cyberattacks (Behl et al., 2019). However, not only the party or owner of the e-commerce company must have a good security strategy, from the user side must also have a strategy on how to keep their data safe. Because if the security strategy is bad, the level of vulnerability of personal data security to cyberattacks will increase.

4.6 Relationship between brand trust and consumer purchase intention

From the table above, it can be seen that the original sample on the path coefficient of the company value test results by company size has a positive direction coefficient of 0.288, and the P-value value is less than 0.05 ranging from 0.007. Showing only two criteria according to the provisions (variables are interrelated and the value is positive), so it is concluded that hypothesis 1 is accepted. Trust, lifestyle and satisfaction have a partial effect on repurchase intention while handling of service failure has no effect. Meanwhile, handling of service failure and trust have an effect on repurchase intention through consumer satisfaction, brand trust is the willingness and risk of someone to rely on a brand because someone expects positive results from the brand (Cao et al., 2024). Brand trust has a major impact on consumer satisfaction. Because when consumers trust a brand, they are happy and repeat purchases. brand trust has a significant and dominant effect on consumer satisfaction. their brand trust has a relevant positive effect on satisfaction. Trust related to a brand is the willingness to trust a brand by consumers in the hope of providing results that. Being able to provide the satisfaction desired by consumers is one way to increase consumer loyalty so that consumers will not switch to other brands. consumer trust in brands towards consumer loyalty is closely related to each other (Cascavilla et al., 2021). Product quality towards consumer loyalty Product quality is a product and service that goes hand in hand with consumer desires where the advantages of the product that can be sold are by consumer expectations Based on the opinion of the influence of product quality on loyalty. the better the product quality, the greater the influence on the level of consumer loyalty. Brand trust in consumer loyalty through consumer satisfaction (Elisanti et al., 2024). Consumer trust in a brand is the consumer's assumption of the trustworthiness of a particular brand accompanied by the consumer's desire to trust or rely on a particular brand. If the expected expectations are in accordance, consumers will increasingly trust and get satisfaction from the brand. argue that some interventions on consumer satisfaction can increase the direct impact of consumer trust in a brand on consumer loyalty. Relationship between Variables Brand trust is the focus of attention by almost all retailers and business people in Indonesia, this is because the better the customer's understanding of brand trust, the easier the strategy to win competition in the business world. Brand trust is built because of the hope that other parties will act according to the needs and buying interests of consumers. Brand trust is important for online shop organizers or E-Commerce in Indonesia because customers will spread their trust to other potential customers, in addition, brand trust can increase buying interest in a company. Brand trust (brand trust or customer trust) is a feeling of security that consumers have as a result of their interaction with a brand, which is based on the perception that the brand is reliable and responsible for the interests and safety of consumers. So in the end, trust comes from consumer expectations that the brand's promise will be fulfilled (Gill et al., 2021). When consumer trust is lost, it will be difficult for companies to rekindle buying interest. Customer trust in a brand affects purchasing interest because consumers have a more cautious attitude towards the brand. Trust is a form of attitude that shows feelings of liking and persisting in using a product or brand. Trust will arise from the minds of consumers if the product purchased can provide the benefits or value desired by consumers in a product. Sales promotion also has a very important role because the results obtained are carried out so that prospective consumers are interested in purchasing the products or services offered. After several factors that can stimulate brand trust and sales promotion, it will then lead to final decisions such as online buying interest

5. Discussion

Based on the previous explanation regarding the forms of online fraud, it is only right that the public, both buyers and sellers, take several preventive measures. The first preventive measure is that buyers and sellers must first ensure the identity of the seller and buyer. Second, buyers prioritize the Cash on the Delivery (COD) system (Hasbullah, 2022). This COD system is a payment method that can be done directly after the order from the courier is received by the buyer. However, if COD is not possible, buyers are advised to always ask for a receipt for the shipping service so that they can check the goods ordered. Third, buyers should not be easily tempted to buy cheap goods because the goods could be used or counterfeit goods. Then, sellers are expected to always ensure account mutations when buyers send proof of transfer to avoid that the proof of transfer sent is fake. If prevention has been carried out but online fraud still occurs, then what the victim can do is immediately contact the call centre for the electronic money application provided by E-Commerce such as Shopee Pay, Ovo, or others to cancel the payment. In addition, you can contact the relevant mobile banking (m-banking) so that you can ask the bank to block the account and immediately visit the bank outlet to get further solutions. Then, also report it to the authorities to complete the report and further investigation. Although Indonesia does not yet have a "cyberlaw" that specifically targets the interests of victims, Indonesia still needs legal action using existing laws such as legislation, jurisprudence and international conventions that have been ratified to protect the interests of cyberspace residents in Indonesia. Various efforts can be taken to resolve Internet crimes, both preemptively, preventively, and repressively. Preemptive efforts can be carried out by ratifying international cybercrime agreements into the legal system in Indonesia. The Council of Europe Agreement is one form of international agreement, and some of its covenants have been ratified into the legal system in Indonesia. Preventive cybercrime prevention can be carried out by developing security and increasing energy for computer features, capabilities and discipline in using these features in cyberspace. These activities can be in the form of actions that can be carried out individually, nationally, or globally. Meanwhile, repressive cybercrime countermeasures can be implemented by ensnaring the perpetrators of criminal acts to be handled by the law. The law determines the interests of victims by providing restitution, compensation, or assistance which is the responsibility of the perpetrator with the State as the provider.

Information technology opens up opportunities for new forms of crime (cybercrime) that are more sophisticated than conventional crimes to prevent it is not enough to just take a conventional legal system approach considering that activities are no longer limited by a country's territory. Therefore, negative impacts in the form of losses can occur both to the perpetrators of the transaction and other people who have never been in contact, for example, theft of credit card funds through shopping on the internet. For many people who do business/trade online (Facebook, Twitter) if there is a case of fraud, the first step is to report it to law enforcement officers accompanied by initial evidence in the form of electronic data or information and printouts. If the problem is followed up by law enforcement officers, then law enforcement officers trace the electronic source of the perpetrator's internet address based on the IP address log stored on the homepage web processing server used as a means for the perpetrator to commit fraud.

Repurchase is a real action that shows the consumer's intention to involve customers in future transactions with the seller. Repurchase or repurchase is illustrated as a concrete activity where customers buy or reuse a product. When customers buy an item, they can buy it again in the future. This indicates that customers repeatedly use products or services that have similar sales. There is a strong relationship between brand trust and repurchase intention (Rughiniș et al., 2024). In other words, if consumers have trusted a brand, they are more likely to repurchase the product in the future. Thus, even though consumers trust a brand, it does not directly affect their decision to repurchase the product in the future. The study revealed that customer satisfaction has a significant and positive effect on repurchase intention. This finding suggests that consumers who are satisfied with a brand are more likely to have a positive experience with the product or service in the future (Rughiniș et al., 2024). The study found that satisfaction is positively related to repurchase intention. In addition, the significant effect of brand trust on repurchase intention underscores the importance of building trust in long-term relationships with consumers. Trust in a brand makes consumers more likely to remain loyal and repurchase products from the same brand. This confirms that marketing strategies must include efforts to build and maintain consumer trust through transparent and consistent communication.

6. Managerial Implications

The use of e-commerce carries threats and risks to the security of users' data. E-commerce users need to take appropriate precautions to protect their data. The greater the threat to the data processing system, the greater the risk of a breach of personal data security for e-commerce users. The better and more appropriate the security strategy used, the more secure the user's data will be. Based on the results of the literature review analysis, it can be concluded that threats, risks, and security strategies influence the security of personal data for e-commerce users. Threats are possible because the more numerous or dangerous the threats are, the more vulnerable and threatened the security of the user's data. Meanwhile, the risks that arise in the security of e-commerce users' data can cause data security breaches that can harm users in financial or non-financial forms. The right security strategy can greatly affect the protection of personal data so that the security of the user's data is well maintained.

Judging from the data processing and discussion above, there is potential that can be maximized and utilized from these variables, namely brand trust and sales promotion to increase online buying interest in e-commerce. To increase purchasing interest, e-commerce parties can maximize services and continue to provide various sales promotions in the form of cashback, free shipping, cashback, and vouchers, etc. to consumers so that they trust the brand when they know that e-commerce creates a safe, enjoyable, and practical shopping experience. This can increase the intensity of consumer purchasing interest in e-commerce if they routinely hold sales promotions. E-commerce parties must also drive and follow up on consumer complaints properly and listen to consumer desires so that the relationship between e-commerce and consumers can be maintained so that e-commerce brands can be trusted by consumers. Therefore, this can be considered and carried out by the company to optimize existing opportunities to increase company profits.

7. Conclusion

The results of the analysis show that cybercrime has a positive effect on consumer purchasing intentions on e-commerce platforms and e-brand trust hurts consumer purchasing intentions on e-commerce platforms. Thus, social media users are expected to be careful and maintain ethics in social media so that there is no misuse or violation of cybercrime law or in other words using social media intelligently. In addition, every internet and social media user must make efforts that can be done to prevent cybercrime, namely protecting computers from viruses, maintaining privacy, maintaining account security, avoiding hoaxes, and always being up to date with information or reviewing the truth of social media content, and spreading positive information. Social media is one of the places that is very easy to misuse for the spread of cybercrime. Where many cases of cybercrime occur on several social media such as Facebook, Instagram and Twitter. In general, perpetrators of cybercrime on social media, whether intentional or unintentional, will be charged with Law Number 11 of 2008 concerning Information and Electronic Transactions (UU ITE). Every internet and social media user must make efforts to prevent cybercrime, including protecting computers from viruses, maintaining privacy, securing accounts, avoiding hoaxes, always being up to date with information, spreading positive information, and considering ethics in social media. With this research, it is hoped that the Indonesian people will be more aware of fraudulent actions carried out by cybercrime, the impact of which can be detrimental to many people. By continuing to follow developments in this digital era, we will not be trapped in criminal acts. The government is also expected to be more assertive in following up on cybercrimes who commit fraudulent transactions in e-commerce applications. In its development, electronic commerce transactions must be made with regulations or regulations as a legal umbrella that can be a reference for the community. In carrying out electronic commerce transactions, there is often a lot of unrest in the community, especially public trust in producers (sellers) of goods via the Internet. Sometimes what has been purchased by consumers does not match what is seen via the internet (online shop), and can be said to be fraudulent. This is one example of a crime that occurs on the internet in electronic commerce transactions. Therefore, here the role of the Government is very much needed in regulating and creating regulations or rules and laws that can make producers more deterred and afraid of committing a crime in electronic transactions.

References

Akinbowale, O. E., Klingelhöfer, H. E., & Zerihun, M. F. (2020). Analysis of cyber-crime effects on the banking sector using the balanced score card: a survey of literature. *Journal of Financial Crime, 27*(3), 945-958.

Adejumo, A. D., & Oyeniyi, K. O. (2024). Cybercrime and its Effect on Nation Identity Image: Pragmatic Evidence from Nigeria. *Pakistan Journal of Multidisciplinary Innovation, 3*(1), 29-40.

Behl, A., Pal, A., & Tiwari, C. (2019). Analysis of effect of perceived cybercrime risk on mobile app payments. *International Journal of Public Sector Performance Management, 5*(3-4), 415-432.

Brands, J., & Van Doorn, J. (2022). The measurement, intensity and determinants of fear of cybercrime: A systematic review. *Computers in Human Behavior, 127*, 107082.

Bekkers, L., van't Hoff-De Goede, S., Misana-ter Huurne, E., van Houten, Y., Spithoven, R., & Leukfeldt, E. R. (2023). Protecting your business against ransomware attacks? Explaining the motivations of entrepreneurs to take future protective measures against cybercrimes using an extended protection motivation theory model. *Computers & Security, 127,* 103099.

Basuchoudhary, A., & Searle, N. (2019). Snatched secrets: Cybercrime and trade secrets modelling a firm's decision to report a theft of trade secrets. *Computers & Security, 87*, 101591.

Cao, D. M., Sayed, M. A., Islam, M. T., Mia, M. T., Ayon, E. H., Ghosh, B. P., ... & Raihan, A. (2024). Advanced cybercrime detection: A comprehensive study on supervised and unsupervised machine learning approaches using real-world datasets. *Journal of Computer Science and Technology Studies, 6*(1), 40-48.

Cascavilla, G., Tamburri, D. A., & Van Den Heuvel, W. J. (2021). Cybercrime threat intelligence: A systematic multi-vocal literature review. *Computers & Security, 105*, 102258.

Elisanti, E., Khaerudin, A., Junaidi, A., Putri, H. A. A., & Muhtarom, M. (2024). Analysis of Cybercrime Potential in E-Commerce Buying and Selling Transactions. *AL-MANHAJ: Jurnal Hukum dan Pranata Sosial Islam, 6*(1), 163-180.

Gill, A. A., Ali, M. H., Aslam, M., & Amjad, M. H. (2021). A Model to Analyze the Mobile e-banking Application Quality Factors Impact on Consumers'e-Loyalty: Mediating Role of e-Satisfaction. *iRASD Journal of Management, 3*(2), 137-145.

Hasbullah, M. A. (2022). Identifying the Effects of Cybercrime on Business Laws: Implications for Businesses and Consumers. *International Journal of Cyber Criminology, 16*(2), 119-130.

Ibrahim, S. (2016). Social and contextual taxonomy of cybercrime: Socioeconomic theory of Nigerian cybercriminals. *International Journal of Law, Crime and Justice, 47*, 44-57.

Julianti, H., Ainaya, S., Azzahra, T., & Andriany, D. (2024). Cyber Crime Communication Patterns Impulsive Purchase Behavior of NCT 127" The Unity Jakarta" Concert Tickets on X (Twitter). *Indonesian Journal of Advanced Research, 3*(7), 987-1004.

Khoiriah, Z., Harahap, M. I., & Yanti, N. (2024). Cybersecurity Impact of Cybercrime in Strengthening Trust In BSI Kc Rantau Prapat. *Kontigensi: Jurnal Ilmiah Manajemen, 12*(1), 320-331.

Kshetri, N. (2013). Cybercrime and cyber-security issues associated with China: some economic and institutional considerations. *Electronic Commerce Research, 13*, 41-69.

Kaakinen, M., Keipi, T., Räsänen, P., & Oksanen, A. (2018). Cybercrime victimization and subjective well-being: An examination of the buffering effect hypothesis among adolescents and young adults. *Cyberpsychology, Behavior, and Social Networking, 21*(2), 129-137.

Khiong, K. (2022). Impact and Challenges of Digital Marketing in Healthcare Industries during Digital Era and Covid-19 Pandemic. *Journal of Industrial Engineering & Management Research, 3*(5), 112-118. https://doi.org/10.7777/jiemar.v3i5.408

Karine, H. A. J. I. (2021). E-commerce development in rural and remote areas of BRICS countries. *Journal of Integrative Agriculture, 20*(4), 979-997.

Leukfeldt, E. R., & Holt, T. J. (2022). Cybercrime on the menu? Examining cafeteria-style offending among financially motivated cybercriminals. *Computers in Human Behavior, 126*, 106979.

Lien, C. H., Wen, M. J., Huang, L. C., & Wu, K. L. (2015). Online hotel booking: The effects of brand image, price, trust and value on purchase intentions. *Asia Pacific Management Review, 20*(4), 210-218.

Mujtaba, B. G. (2024). Cybercrimes and safety policies to protect data and organizations. *Journal of Crime and Criminal Behavior, 4*(1), 91-112.\

Mulyandi, M. R., & Tjandra, R. H. (2022). The Influence of Product Quality and Brand Image on repurchase Intention of Halal Cosmetic Products in e-Commerce. *Journal of Industrial Engineering & Management Research, 4*(1), 41- 52. https://doi.org/10.7777/jiemar.v4i1.438

Mishra, A., Alzoubi, Y. I., Anwar, M. J., & Gill, A. Q. (2022). Attributes impacting cybersecurity policy development: An evidence from seven nations. *Computers & Security, 120,* 102820.

Nasution, M. D. T. P., Rossanty, Y., Siahaan, A. P. U., & Aryza, S. (2018). The phenomenon of cyber-crime and fraud victimization in online shop. *International Journal of Civil Engineering Technology, 9*(6), 1583-1592.

Riek, M., Bohme, R., & Moore, T. (2015). Measuring the influence of perceived cybercrime risk on online service avoidance. *IEEE Transactions on Dependable and Secure Computing, 13*(2), 261-273.

Ratnasari, I., Siregar, S., & Maulana, A. (2021). How to build consumer trust towards E-satisfaction in e-commerce sites in the covid-19 pandemic time?. *International Journal of Data and Network Science, 5*(2), 127-134.

Rughiniş, R., Bran, E., Stăiculescu, A. R., & Radovici, A. (2024). From cybercrime to digital balance: How human development shapes digital risk cultures. *Information, 15*(1), 50.

Saban, K. A., McGivern, E., & Saykiewicz, J. N. (2002). A critical look at the impact of cybercrime on consumer internet behavior. *Journal of Marketing Theory and Practice, 10*(2), 29-37.

Smith, A. D. (2004). Cybercriminal impacts on online business and consumer confidence. *Online Information Review, 28*(3), 224-234.

Shareef, M. A., Dwivedi, Y. K., Kumar, V., Davies, G., Rana, N., & Baabdullah, A. (2019). Purchase intention in an electronic commerce environment: A trade-off between controlling measures and operational performance. *Information Technology & People, 32*(6), 1345-1375.

Strzelecki, A., & Rizun, M. (2022). Consumers' change in trust and security after a personal data breach in online shopping. *Sustainability, 14*(10), 5866.

Sarkar, G., & Shukla, S. K. (2023). Behavioral analysis of cybercrime: Paving the way for effective policing strategies. *Journal of Economic Criminology, 100034*, 34-45

Sabillon, R., Cano, J. J., & Serra-Ruiz, J. (2016). Cybercrime and cybercriminals: A comprehensive study. *International Journal of Computer Networks and Communications Security, 4*(6).

Sharma, N., & Annaboina, K. (2024). Analytical Study On Prevention And Detection Of Financial Cybercrime And Frauds Using Transaction Pattern Generation Tool. *Journal of Scientific Research and Technology*, 9-31.

Sahin, A., Zehir, C., & Kitapçı, H. (2011). The effects of brand experiences, trust and satisfaction on building brand loyalty; an empirical research on global brands. *Procedia-Social and Behavioral Sciences, 24,* 1288-1301.

Wahab, F., Khan, I., Hussain, T., & Amir, A. (2023). An investigation of cyber attack impact on consumers' intention to purchase online. *Decision Analytics Journal, 8,* 100297.

Zahari, A. I., Bilu, R., & Said, J. (2019). The role of familiarity, trust and awareness towards online fraud. *Journal of Research and Opinion, 6*(9), 2470-2480.