Cybersecurity Impact of Cybercrime in Strengthening Trust In BSI Kc Rantau Prapat

[1]Zulfa Khoiriah, [2]M. Ikhsan Harahap, [3]Nursantri Yanti
Universitas Islam Negeri Sumatera Utara, Medan, Indonesia
Email:Zulfakhoiriah19@gmail.com

DOI: https://doi.org/10.56457/jimk.v12i1.559

Received: June 12, 2024	Accepted: June 20, 2024	Published: June 30, 2024

ABSTRACT

The study aims to analyze the impact of cybercrime security in increasing customer confidence in bsi kc prapat region. This research uses a quantitative method with a case study approach. Data collected through questionnaires A new study was conducted to test the impact of cybercrime security on customer confidence, involving customers of Bank Syariah Indonesia (BSI) in the Prapat Region. This analysis is used to determine the extent to which data measurements provide comparable or no different results when measured again on the same subject, revealing the reliability or consistency of the measuring instrument (questionnaire). If the Cronbach alpha value is at least 0.06 and the R value is greater than 0.60, the research instrument is considered more reliable, which means that the data collection tool has a higher level of trust. If the test is carried out using the Crobach alpha method, the calculated r will be displayed in the following table as the alpha value. Research results show that cybercrime security has a positive and significant impact on customer confidence, suggesting that customers have more confidence in banks that are able to secure their data from cyber crime threats. In conclusion, cybercrime security plays an important role in building andining customer confidence in the Shariah financial industry. Banks need to continue to improve their security infrastructure and respond quickly to security incidents to ensure customer confidence remains awake. Reliability testing is the process of testing the data obtained, such as questionnaire results.

Keywords: Cybercrime Security, Customer Confidence. Bank Syariah Indonesia (BSI)

INTRODUCTION

The Islamic finance industry, including BSI, faces increasingly complex security threats in the current digital era. Hacking is the biggest threat, which can destroy public trust in banks and expose customer data. BSI has recently faced many technical and security issues. One of the most well-known incidents was a BSI error that occurred at the end of May 2023 and had an impact on the bank's daily operations. Additionally, hacking allegations emerged, raising concerns about the security of customer data and information. According to reports circulating in the media, this incident made customers worried and distrustful of the security of their data at the bank. They also feel uncomfortable and have difficulty making transactions. This incident raises serious questions about BSI's technical and security readiness to face contemporary challenges as well as the impact on customer trust. According to Maulana & Fitriana (2023), superior service is usually used by companies operating in the service industry, especially banking companies, to gain a competitive advantage . Wahlers stated that appropriate and effective plans for service quality are an important component that influences competitive advantage. Service quality is a measure of product quality in bank services. Parasuraman et al. defines service quality as the service received by customers in accordance with customer expectations for quality (Hotdiana et al., 2023). Technological developments are currently increasing in Indonesia, and have even become a means to assist several human activities. People often assume that today's internet technology can meet their needs more efficiently. Currently, information technology is very important for people's lives, and almost all operations in the banking sector use this technology. Currently, we know a lot about various types of banking transactions in the banking world, such as deposits, withdrawals, transfers and clearing, and many more that are carried out by bank customers (Nawawi, 2024). With advances in communications and information technology, the types of attacks that will occur in cyberspace are becoming increasingly complex. The terms hacker and cracker were first known, referring to people who have special abilities or activities to enter computer systems. Advances in technology today are always associated with efforts to digitize various things. Digitalization changes digital information media into analog, changing all kinds of information into bits or binary digits so that they can be changed or changed. Digitalization aims not only to provide the widest possible access to the public, but also to preserve archives and make them accessible for research, documentation and publication (Sabda et al., 2023). Cybercrime, or cybercrime, emerged as a result of the existence of the internet.Cybercrime itself is a type of crime that involves the use of information technology without borders (Sabda et al., 2023). According to Widodo (2009), Cyber Crime includes all forms of activities related to the activities of a person, group of people, or legal entity that uses computers as a means of to commit a crime or as an object of a crime. On the other hand, Wahid & Labib (2005) say that Cyber Crime includes all kinds of computer network users who aim to commit crimes or crimes with high technology by abusing the convenience. Even though internet banking is easy to use, there are risks that accompany it. For example, there are many violations related to personal data via the internet and bank customers face financial risks due to the actions of criminals known as cybercrime, who utilize sophisticated information technology and computers for money laundering purposes. Therefore, there are many crimes that take people's personal data , which can cause casualties (Haditya, 2020).

Apart from that, there are many negative consequences that arise when we use the internet banking system that cannot be avoided. Along with the development of Internet technology that can make everything easier, many crimes known as Cyber Crime have also emerged. In Indonesia, many cases such as credit card theft, banking fraud and hacking have emerged (Haditya, 2020). PT Bank Syariah Indonesia Tbk (BSI) was recently hit by a cyber attack. 1.5 terabytes of data containing nine databases containing the personal information of more than 15 million BSI customers and employees was allegedly leaked. This data includes name, address, document information, card number, telephone number, and transactions. Those responsible for hacking BSI data are the LockBit 3.0 ransomware hacking group. A screenshot of the site posted on Twitter on Saturday (13/5/2023) shows that the group has been attacking BSI since last Monday (8/5). Additionally, they stated that all BSI services had been terminated as a result of the attack.Arofah et al. (2000) Some time ago, PT Bank Syariah Indonesia (Bank BSI) was one of the state-owned banks which was very disturbing to the Indonesian people. The cyber attack paralyzed BSI Bank's banking system for approximately one week, making it impossible for customers to access and carry out financial transactions through mobile banking services, branch offices and BSI Bank ATMs. A press release issued by BSI Bank on May 8 2023 stated that On that date, Bank BSI is carrying out system maintenance to improve services, and will soon return to normal operations. BSI Bank distributed the release via the BSI Bank Instagram account, @banksyariahindonesia. Gunawan Arief Hartoyo, General Secretary of BSI, said, "BSI is committed to continuing to improve services to customers, and is of course very grateful for the trust that customers have given to Bank Syariah Indonesia." This is quoted from coverage page 6. Currently, BSI is carrying out system maintenance, which will make it temporarily inaccessible as part of service improvements. We apologize, but customers may not be able to use BSI services for a while. We also maintain the security of customer funds, so all customers must be alert and wary of fraud claiming to be Bank Syariah Indonesia (Afifah, 2023). With increasing levels of competition, every bank must strive to increase its competitiveness. This is because the profits obtained by a bank from existing products are very sensitive and easily surpassed by other competing banks. If banks want to grow rapidly, they must have human resources who are capable of performing well. Improving the quality of human resources is demonstrated through increasing employee performance, using sophisticated technology, improving systems, procedures, and others.According to Fitriani (2019), every bank must be able to work together with clients to provide high quality services. With the quality of service that customers expect, customers will make the decision to buy this product again or make them feel confident. Trade thinks about customer trust. This depends on the level of fulfillment of the expected benefits of the product or service, as well as the level of consistency between actual results and expectations. If customers expect a certain level of service, and it turns out they receive better service than they expected and continue to use the product or service, then the customer can be considered trusting. Likewise, if customers expect a certain level of service, and it turns out they feel that the service they receive is in line with their expectations, then the customer can be considered trusting. Fitriani (2019) Trust in sharia banking customers also includes belief in profit sharing, which means that both parties The parties will share profits in accordance with the agreed agreement. Profit sharing also requires that capital owners work together with the business for the benefit of both parties and society as a whole. In addition, obedience to religious commands and a deep understanding of Islamic sharia principles show that clients are interested in happiness that is ukhrawi (afterlife). Wahyuni (2015) This research was written by Lutfi Maulana and Nadia Fitriana in 2023 in an article entitled "Impact analysis "The BSI Error Incident and Alleged Hacking of Bank Syariah Indonesia (BSI) affected the trust and loyalty of Bank Syariah Indonesia (BSI) customers in Subang Regency." The level of trust (47.6%) and customer loyalty (35.6%) were significantly influenced by the event, according to key findings from the determinants test. Customer confidence was significantly affected by the incident, which highlights concerns about the security of banking services. One can question BSI's credibility as a sharia financial institution if there is no trust. To maintain customer loyalty, events are also important. A decline in trust can lead to a decline in loyalty, impacting the relationship between clients and financial institutions in the long term. This research provides an in-depth look at the consequences caused by security incidents, and emphasizes how important proactive response and recovery methods are to restoring customer trust. Financial institutions must take concrete action to restore customer trust and maintain the integrity and security of banking services.

Trade thinks about customer trust. This depends on the level of fulfillment of the expected benefits of the product or service, as well as the level of consistency between actual results and expectations. If customers expect a certain level of service, and it turns out they receive better service than they expected and continue to use the product or service, then the customer can be considered trusting. Likewise, if customers expect a certain level of service, and it turns out they feel that the service they receive is in line with their expectations, then the customer can be considered trusting. Fitriani (2019) Trust in sharia banking customers also includes belief in profit sharing, which means that both parties The parties will share profits in accordance with the agreed agreement. Profit sharing also requires that capital owners work together with the business for the benefit of both parties and society as a whole. In addition, obedience to religious commands and a deep understanding of Islamic sharia principles show that clients are interested in happiness that is ukhrawi (afterlife). Wahyuni (2015) This research was written by Lutfi Maulana and Nadia Fitriana in 2023 in an article entitled "Impact analysis "The BSI Error Incident and Alleged Hacking of Bank Syariah Indonesia (BSI) affected the trust and loyalty of Bank Syariah Indonesia (BSI) customers in Subang Regency." The level of trust (47.6%) and customer loyalty (35.6%) were significantly influenced by the event, according to key findings from the determinants test. Customer

confidence was significantly affected by the incident, which highlights concerns about the security of banking services. One can question BSI's credibility as a sharia financial institution if there is no trust. To maintain customer loyalty, events are also important. A decline in trust can lead to a decline in loyalty, impacting the relationship between clients and financial institutions in the long term. This research provides an in-depth look at the consequences caused by security incidents, and emphasizes how important proactive response and recovery methods are to restoring customer trust. Financial institutions must take concrete action to restore customer trust and maintain the integrity and security of banking services.Trade thinks about customer trust. This depends on the level of fulfillment of the expected benefits of the product or service, as well as the level of consistency between actual results and expectations. If customers expect a certain level of service, and it turns out they receive better service than they expected and continue to use the product or service, then the customer can be considered trusting. Likewise, if customers expect a certain level of service, and it turns out they feel that the service they receive is in line with their expectations, then the customer can be considered trusting. Fitriani (2019) Trust in sharia banking customers also includes belief in profit sharing, which means that both parties The parties will share profits in accordance with the agreed agreement. Profit sharing also requires that capital owners work together with the business for the benefit of both parties and society as a whole. In addition, obedience to religious commands and a deep understanding of Islamic sharia principles show that clients are interested in happiness that is ukhrawi (afterlife). Wahyuni (2015) This research was written by Lutfi Maulana and Nadia Fitriana in 2023 in an article entitled "Impact analysis "The BSI Error Incident and Alleged Hacking of Bank Syariah Indonesia (BSI) affected the trust and loyalty of Bank Syariah Indonesia (BSI) customers in Subang Regency." The level of trust (47.6%) and customer loyalty (35.6%) were significantly influenced by the event, according to key findings from the determinants test. Customer confidence was significantly affected by the incident, which highlights concerns about the security of banking services. One can question BSI's credibility as a sharia financial institution if there is no trust. To maintain customer loyalty, events are also important. A decline in trust can lead to a decline in loyalty, impacting the relationship between clients and financial institutions in the long term. This research provides an in-depth look at the consequences caused by security incidents, and emphasizes how important proactive response and recovery methods are to restoring customer trust. Financial institutions must take concrete action to restore customer trust and maintain the integrity and security of banking services.then the customer can be considered to trust. Fitriani (2019) The trust of sharia banking customers also includes belief in profit sharing, which means that both parties will share profits in accordance with the agreed agreement. Profit sharing also requires that capital owners work together with the business for the benefit of both parties and society as a whole. In addition, obedience to religious commands and a deep understanding of Islamic sharia principles show that clients are interested in happiness that is ukhrawi (afterlife). Wahyuni (2015) This research was written by Lutfi Maulana and Nadia Fitriana in 2023 in an article entitled "Impact analysis "The BSI Error Incident and Alleged Hacking of Bank Syariah Indonesia (BSI) affected the trust and loyalty of Bank Syariah Indonesia (BSI) customers in Subang Regency." The level of trust (47.6%) and customer loyalty (35.6%) were significantly influenced by the event, according to key findings from the determinants test. Customer confidence was significantly affected by the incident, which highlights concerns about the security of banking services. One can question BSI's credibility as a sharia financial institution if there is no trust. To maintain customer loyalty, events are also important. A decline in trust can lead to a decline in loyalty, impacting the relationship between clients and financial institutions in the long term. This research provides an in-depth look at the consequences caused by security incidents, and emphasizes how important proactive response and recovery methods are to restoring customer trust. Financial institutions must take concrete action to restore customer trust and maintain the integrity and security of banking services.then the customer can be considered to trust. Fitriani (2019) The trust of sharia banking customers also includes confidence in profit sharing, which means that both parties will share profits in accordance with the agreed agreement. Profit sharing also requires that capital owners work together with the business for the benefit of both parties and society as a whole. In addition, obedience to religious commands and a deep understanding of Islamic sharia principles show that clients are interested in happiness that is ukhrawi (afterlife). Wahyuni (2015) This research was written by Lutfi Maulana and Nadia Fitriana in 2023 in an article entitled "Impact analysis "The BSI Error Incident and Alleged Hacking of Bank Syariah Indonesia (BSI) affected the trust and loyalty of Bank Syariah Indonesia (BSI) customers in Subang Regency." The level of trust (47.6%) and customer loyalty (35.6%) were significantly influenced by the event, according to key findings from the determinants test. Customer confidence was significantly affected by the incident, which highlights concerns about the security of banking services. One can question BSI's credibility as a sharia financial institution if there is no trust. To maintain customer loyalty, events are also important. A decline in trust can lead to a decline in loyalty, impacting the relationship between clients and financial institutions in the long term. This research provides an in-depth look at the consequences caused by security incidents, and emphasizes how important proactive response and recovery methods are to restoring customer trust. Financial institutions must take concrete action to restore customer trust and maintain the integrity and security of banking services.One can question BSI's credibility as a sharia financial institution if there is no trust. To maintain customer loyalty, events are also important. A decline in trust can lead to a decline in loyalty, impacting the relationship between clients and financial institutions in the long term. This research provides an in-depth look at the consequences caused by security incidents, and emphasizes how important proactive response and recovery methods are to restoring customer trust. Financial institutions must take concrete action to restore customer trust and maintain the integrity and security of banking services.One can question BSI's credibility as a sharia financial institution if there is no trust. To maintain customer loyalty, events are also important. A decline in trust can lead to a decline in loyalty, impacting the relationship between clients and financial institutions in the long term. This research provides an in-depth look at the consequences caused by security incidents, and emphasizes how important proactive response and recovery methods are to restoring customer trust. Financial institutions must take concrete action to restore customer trust and maintain the integrity and security of banking services.

Andyan Pradipta Utama and Tri Ratna Murti wrote an article entitled "Customer Satisfaction as a Mediator of the Influence of Trust on Customer Loyalty". The purpose of this research is to find out how customer satisfaction influences trust in customer loyalty. This research involved 342 people who were customers of various commercial banks in Jakarta. In this research, the instruments used are the customer satisfaction scale, trust scale, and customer loyalty scale. This research was carried out using path analysis and processed using the JASP program version 12.2. The research results show the indirect effect of trust on customer loyalty on customer satisfaction, with a coefficient of0.377 and p <0.05. Thus, it can be concluded that trust influences customer loyalty through satisfaction. Customer trust will increase customer satisfaction, which in turn will increase customer loyalty. Juliandi Fitri (2021) conducted research with the title "the influence of internet banking and cyber crime on customer trust in sharia banking (study at the independent sharia bank tapak sir)." This study aims to identify the following factors: the influence of internet banking on Bank Syariah Mandiri customer trust; the influence of cybercrime on Bank Syariah Mandiri customer trust; and the influence of the combination of internet banking and cybercrime on Bank Syariah Mandiri customer trust. In the field research process, quantitative methods are used. Three things were found: (1) internet banking elements had a positive and significant impact on customer trust; (2) elements of cyber crime have a negative and significant impact on customer trust; and (3) internet banking customer trust and cyber crime as a whole have a positive and negative impact on customer trust. Dewa Ayu Pargita Apsari (2021) wrote an article entitled "The Influence of Internet Banking Use and Customer Data Protection on Cyber Crime in Denpasar City". The aim of this research is to find out how the use of internet banking and the protection of customer data used by internet banking facilities affects cybercrime in the Denpasar area. This research collects data by distributing online questionnaires to a population consisting of internet banking facility users in the Denpasar area, in total 72 people. To obtain accurate data to produce conclusions that are in accordance with the actual situation, valid, consistent and appropriate tools are needed to convey research results. Where the Cronbach alpha correlation is used to evaluate the validity of this research instrument. Multiple linear analysis was used. Faturrahman Haditya's thesis was entitled "The Influence of Cyber Crime on Customer Loyalty of Users of E-Banking Products (Case Study of Customers in the Yogyakarta Region". The aim of this research is to determine whether cyber violations can influence customer loyalty towards the bank they use. To ascertain the relationship between cyber crime and customer loyalty, multiple linear analysis was used. The initial data used came from questionnaires distributed to one hundred respondents via the internet. The results of the research showed that the knowledge variable had a positive and significant impact on the loyalty variable, with t count > t table (4.282 < 1.661), while the experience variable has a negative and significant impact on the loyalty variable.The study written by Abil Yossa Indah Mauliza was entitled "The influence of data protection and cybersecurity on the level of customer trust in using fintech among the people of Surabaya". This research aims to identify data protection and accountability for the level of public trust in Fintech. This research uses quantitative research using the SPSS program. Primary data for this research was obtained by distributing questionnaires online to respondents via Google Forms, using purposive sampling techniques. The research results show that the level of fintech trust is strongly influenced by data protection and cyber security. Therefore, people's beliefs about whether or not to use fintech in everyday life are strengthened by data and cyber security. Based on the description above, researchers want to conduct research on Bank Syariah Indonesia (BSI) customers to find out how they know about possible criminal acts. will happen or how it will impact them when they use the modern technological features provided by the bank to access banking activities independently. Therefore, researchers are interested in conducting research with the title "the influence of cyber crime security in increasing customer trust in BSI KC Rantau Prapat". The aim of this research is to find out how cyber crime security observations influence customer trust in the Rantau Prapat area (case study of Indonesian sharia bank customers in Rantau Prapat).The aim of this research is to find out how cyber crime security observations influence customer trust in the Rantau Prapat area (case study of Indonesian sharia bank customers in Rantau Prapat).The aim of this research is to find out how cyber crime security observations influence customer trust in the Rantau Prapat area (case study of Indonesian sharia bank customers in Rantau Prapat).

METHOD

This quantitative research aims to examine the effect of security on consumer trust through consumer trust. In this research, two variables are involved: the security variable as the independent variable and the trust variable as the dependent variable. According to Sugiyono (2018; 13), quantitative data is a research method based on positivism (concrete data). This data consists of numbers that will be measured using statistics to test the problem being studied. This research uses non-probability sampling and accidental sampling. This research involved 100 customers who worked at Indonesian sharia banks in the Prapat area. Data was obtained through questionnaires distributed online using Google Forms and then analyzed using SPSS 26. Validity and reliability tests were used to test the data collected. Then the classical assumption test is carried out, which includes normality, multicollinearity and heteroscedasticity tests. Next, the hypothesis was tested using simple linear regression analysis to carry out the t test and coefficient of determination.

RESULTS AND DISCUSSION

A significant test is carried out to determine the level of validity by contrasting the estimated r value with the table r value. Under these conditions, the degrees of freedom (df) are equal to nk, where k is the number of constructs and n is the number of samples. If the calculated r, which is the total correlation of the corrected collection of question items for each question item, is greater than the table r and the r value is positive, then the question item is said to be valid. To get r table 0, the size of df in this case can be calculated as 100-1 or df = 99 with alpha 0.05.

Table 1. Validity Test Results

Variable	Question Item	Total Correlation	R table	Information
Security (X1)	X1.1	0.816	0.1191	Valid
	X1.2	0.801	0.1191	Valid
	X1.3	0.836	0.1191	Valid
Trust (Y)	Y.1	0.602	0.1191	Valid
	Y.2	0.854	0.1191	Valid
	Y.3	0.798	0.1191	Valid
	Y.4	0.809	0.1191	Valid
	Y.5	0.564	0.1191	Valid

Each question item has a positive calculated r> from r table (0.1191), as seen in the table above. As a result, the questionnaire was considered valid.

Reliability Test

Reliability tests were carried out to assess the consistency and reliability of respondents' answers to form questions. The test results will show whether the learning tool can be trusted based on the level of precision and stability of the measuring tool.

criteria used to evaluate how reliable a research instrument is. One of them is to carry out a comparison between table values and calculated values at a transparency level of 95 percent (5 percent significance). If the test is carried out using the Cronbachl's Alpha method, the Alpha value will be displayed in the following table:

Table 2. Reliability Test Results

Reliability Test	Reliability Coefficient	Cronbrach Alpha	Information
Security Variables	3 Question items	0.748	Reliable
Trust Variables	5 Question items	0.785	Reliable

As shown in the summary table above, each variable has a Cronbach Alpha above 0.60. Variables such as security and trust can be considered reliable.

Normality test:

This test is carried out to determine whether the dependent and independent variables in the regression model have a normal distribution. You can find out whether the data is normal by checking the spread of the data with a Normal PP plot. If the data distribution shows a straight line pattern on the graph, then the data is considered normal. If the Kolmogrov-Smirnov sig value is greater than 0.05, the normality test table is considered to be normally distributed. Test the normality of the following research:

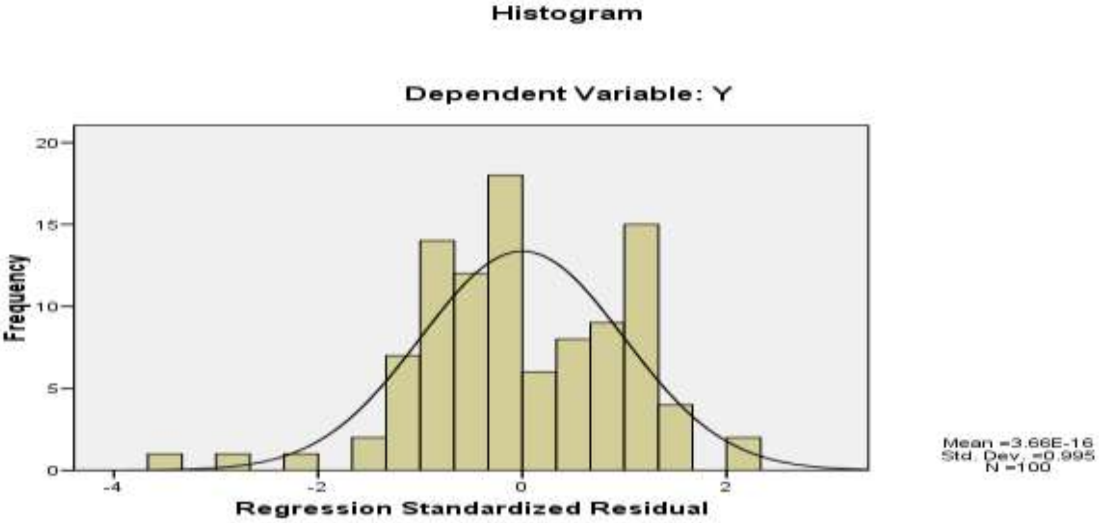
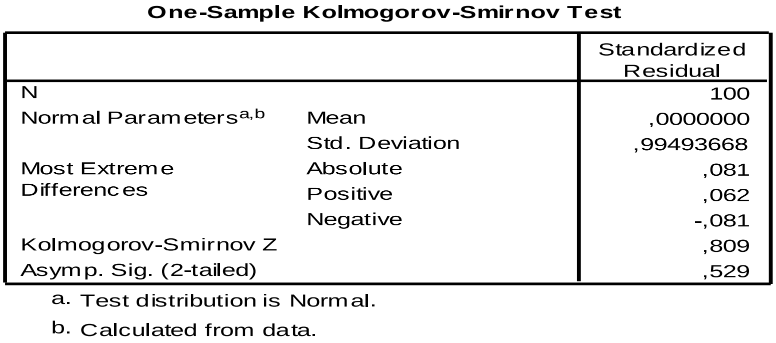


Figure 1. Normality Test Results

It can be concluded from graph1 above, which is used to test normality, that all variables are normally distributed because the histogram curve is parabolic and not a straight line.

Kolmogorov-Smirnov calculations are then used. If the asymptotic significance value of the variable data (2-tailed) is greater than 0.05, a normal distribution for the data can be concluded. Below are the results of the Kolmogrov-Smirnov calculations used by SPSS to determine the normality of all variables:

Table 3. Normality Test Results



One-Sample Kolmogorov-Smirnov Test

		Standardized Residual
N		100
Normal Parameters[a,b]	Mean	,0000000
	Std. Deviation	,99493668
Most Extreme Differences	Absolute	,081
	Positive	,062
	Negative	-,081
Kolmogorov-Smirnov Z		,809
Asymp. Sig. (2-tailed)		,529

a. Test distribution is Normal.

b. Calculated from data.

Judging from the results of the normality test for all variables using the Kolmogrov-Smirnov calculation above, it is 0.529 and greater than 0.05, it can be concluded that the variable data has a normal distribution.

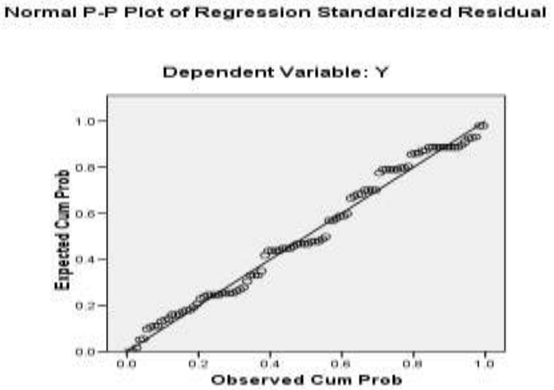


Figure 2. Normality Test Results

From Figure 2 above, it shows that Daa spreads around the diagonal line and follows the direction of the diagonal line, so the regression model meets the normality assumption.

Heteroscedeticity Test

TestHeteroscedeticity aims to test whether in the regression model there is inequality of variance. Heteroscedasticity is a situation where the variance of confounding errors is not constant for all values of the independent variable, where this test aims to test whether in the regression model there is inequality of variance in the residuals or one other observation. To detect it, look at the points spread above and below the number 0 on the Y axis on the Scatterplot graph. The results of the Heteroscedeticity statistical test obtained in this study are as follows:

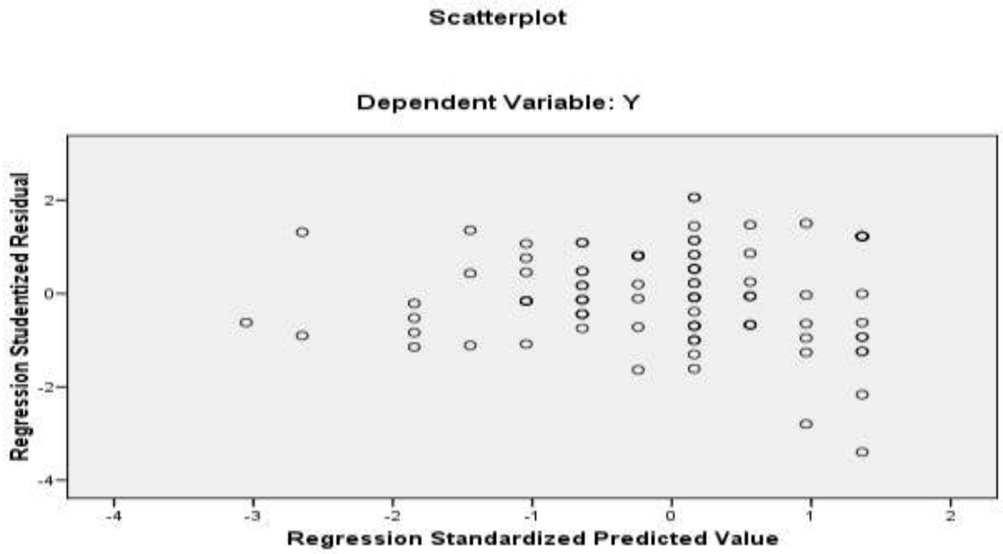
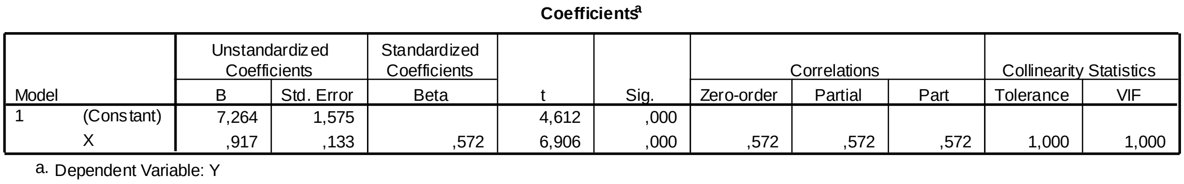


Figure 3 Heteroscedeticity test

Resultsheteroscedeticity testing shows that the dots do not form a clear pattern. As can be seen, the points spread above and below the number 0 (zero) at temperature Y. So it is concluded that heteroscedeticity does not occur in the regression model. In this way the assumptions of normality, multicollinearity and heteroscedeticity in the model can be fulfilled.

Simple Linear Regression Test.

Table 4. Simple Linear Regression Test Results.



Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	Correlations			Collinearity Statistics	
		B	Std. Error	Beta			Zero-order	Partial	Part	Tolerance	VIF
1	(Constant)	7,264	1,575		4,612	,000					
	X	,917	,133	,572	6,906	,000	,572	,572	,572	1,000	1,000

a. Dependent Variable: Y

From table 6 above, it can be seen that the results of the equation model for the variable Influence of Cyber Crime Security in Increasing Customer Trust in BSI KC Rantau Prapat are as follows:

Y = 7.264 + 0.917 (X) +ε

Based on the results of the equation obtained, the meaning and meaning of the Cyber Crime Security coefficient in increasing customer trust in BSI KC Rantau Prapat can be explained as follows:

1. The constant value (c) is 7,264, this means that if the Security variable is equal to zero then Customer Trust in BSI KC Rantau Prapat is equal to a value of 7,264 assuming other variables are constant.
2. Security (X) 0.917, this means that if the independent variable, namely Security, increases by 1%, it will increase Customer Trust in BSI KC Rantau Prapat by 0.917%.

Hypothesis testing

Statistical T Test

The t test aims to determine whether the independent variable or Security partially or individually has a significant effect on the dependent variable or Customer Trust in BSI KC Rantau Prapat (Y)

Table 5. Statistical T Test Results

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	Correlations			Collinearity Statistics	
		B	Std. Error	Beta			Zero-order	Partial	Part	Tolerance	VIF
1	(Constant)	7,264	1,575		4,612	,000					
	X	,917	,133	,572	6,906	,000	,572	,572	,572	1,000	1,000

a. Dependent Variable: Y

The formula for finding t-table =α: n – k – 1 = 0.05: 100 – 1– 1 = 0.05: 98

T –table = 1.65291

Security (X) has a calculated t value of 6.906. This value is greater than the t table (1.65291) with a t sig value (0.000) < 0.05. So the research hypothesis testing is that Ha is accepted and H0 is rejected. This explains that partially the features have a significant and positive effect on customer trust in BSI KC Rantau Prapat (Y)

R Square Test

Test coefficient of determination or R2 aims to know how much great ability variable independent/free (Security) explained variable dependent/bound (Trust) or to know large percentage bound variation which is explained on variable free.

Table 6. R Square Test Results

Model Summary[b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics					Durbin-Watson
					R Square Change	F Change	df1	df2	Sig. F Change	
1	,721[a]	,735	,896	3,29000	,327	47,693	1	98	,000	1,590

a. Predictors: (Constant), X

b. Dependent Variable: Y

The results of the coefficient of determination test provide meaning, that 73.5% of Cyber Crime Security in Increasing Customer Trust in BSI KC Rantau Prapat

DISCUSSION

The influence of cyber crime security in increasing customer trust in BSI KC Rantau Prapat.

ResultsStatistical testing shows that the calculated t value for the Security (X) variable is 6.906. This value is greater than the t table value determined at a significance level of 0.05 (in this case, the t table value is 1.65291). In addition, the significance value (t sig) is 0.000, which is much smaller than the specified significance level (0.05). In inferential statistics, if the significance value (p-value) is smaller than the specified significance level, then we reject the null hypothesis (H0) and accept the alternative hypothesis (Ha).

InIn this context, the null hypothesis (H0) states that there is no influence between security (X) and customer trust in BSI KC Rantau Prapat (Y), while the alternative hypothesis (Ha) states that there is an influence between these two variables.

With a significant t count (6.906) and a very low significance value (0.000), we can conclude that partially, security has a significant and positive influence on customer trust in BSI KC Rantau Prapat. This means that increasing the level of security will contribute positively to increasing customer trust in the institution.

Thus, these findings emphasize the importance of security factors in forming positive perceptions and customer trust in financial institutions such as BSI KC Rantau Prapat. This shows that investment and efforts in improving cyber crime security can have a positive impact in strengthening the relationship between financial institutions and their customers.

Cybercrime attacks on BSI KC Rantau Prapat can cause various significant problems. The following are some of the problems that arise, including the following:

1. Theft of Customer Data: Cybercrime attacks can result in the theft of customer data, including personal information, account numbers, and other sensitive financial information. This can threaten customer privacy and financial security.
2. Financial Loss: Cybercrime attacks can cause direct financial loss for BSI KC Rantau Prapat, both through theft of funds from customer accounts and costs to restore systems and infrastructure affected by the attack.
3. Service Disruption: Cybercrime attacks can disrupt banking services and operations of BSI KC Rantau Prapat, such as delays or failures in processing transactions, unavailability of online banking services, or disruption in ATM access.
4. Reputation Damage: Cybercrime attacks can damage the reputation of BSI KC Rantau Prapat in the eyes of customers, investors and the general public. This can reduce customer trust and loyalty, as well as hamper business growth and bank competitiveness.
5. Lawsuits and Regulators: If a cybercrime attack involves violations of regulations and laws, BSI KC Rantau Prapat may face legal action from affected customers, as well as investigations and sanctions from regulators such as the Financial Services Authority (OJK).
6. Operational Disruption: Cybercrime attacks can cause disruption in BSI KC Rantau Prapat's daily operations, including data loss, decreased productivity, and difficulty in providing expected services to customers.
7. Economic and Financial Losses: Cybercrime attacks can have far-reaching economic and financial impacts, both direct and indirect, including recovery costs, reduced revenue, and long-term reputational damage.

In the face of cybercrime attacks, BSI KC Rantau Prapat must take proactive steps to improve the security of their IT systems and infrastructure, as well as increase employee cyber security awareness and skills. This is important to protect customers, data and bank reputation.

Thus, this research has similarities with previous research entitled "The influence of data protection and cyber security on the level of trust in using fintech in Surabaya." This research aims to determine data protection and accountability for the level of public trust in using fintech. The results of this research conclude that Cyber security data protection significantly influences the level of trust in using fintech. Therefore, data protection and cyber security strengthen people's reasons for whether or not to use fintech in their daily activities. Meanwhile, the research being researched is entitled "The Influence of Cyber Crime Security in increase customer trust in BSI KC Rantau Prapat. The results of this research show that cyber crime security has a positive and significant influence on customer trust which shows that customers have more trust in banks that are able to secure their data from cyber crime threats. In conclusion, cyber crime security plays an important role in building and maintaining customer trust in the sharia financial industry. Banks need to continue to improve their security infrastructure and respond quickly to security incidents to ensure customer trust is maintained.

CONCLUSION

Based on the data analysis and sequence carried out in this research, namely "The Influence of Cyber Crime Security in Increasing Customer Trust in Bsi Kc Rantau Prapat" the following conclusions can be drawn: Judging from the results of the normality test for all variables using the Kolmogrov-Smirnov calculation above, it is 0.529 and above. greater than 0.05, it can be concluded that the variable data is normally distributed, Security (X) has a calculated t value of 6.906. This value is greater than the t table (1.65291) with a t sig value (0.000) < 0.05. So the research hypothesis testing is that Ha is accepted and H0 is rejected. This explains that partially the features have a significant and positive effect on customer trust in BSI KC Rantau Prapat (Y). The results of the coefficient of determination test provide meaning that 73.5% of Cyber Crime Security increases customer trust in BSI KC Rantau Prapat. In conclusion, cyber crime security plays an important role in building and maintaining customer trust in the Islamic finance industry. Banks need to continually improve their security infrastructure and respond quickly to security incidents to ensure customer trust is maintained.

REFERENCES

Afifah, D. (2023). Perlindungan Konsumen di Sektor Jasa Keuangan pada Kasus Serangan Siber Ransomware yang Menimpa Perbankan. JIIP - Jurnal Ilmiah Ilmu Pendidikan, 6(11), 9318–9323. https://doi.org/10.54371/jiip.v6i11.3176

Arofah, N. R., Sari, Y. P., Amaliyah, F., Reliabilitas, U., Normalitas, U., & Regresi, U. (2000). Pengaruh Penggunaan Internet Banking Terhadap Cyeber Crime di Wilayah Tegal (Studi Kasus Pada Nasabah PT. Bank Rakyat Indonesia (PERSERO), Tbk. Kantor Cabang Tegal). 1–5.

Fitriani, A. (2019). Kepercayaan Nasabah terhadap Bank Syariah (Studi Kasus BPRS Aman Syariah Sekampung). Skripsi, Institut Agama Islam Negeri (IAIN) Metro 2019, 3.

Haditya, F. (2020). Pengaruh Cyber Crime Terhadap Loyalitas Nasabah Pengguna Produk E-Banking (Studi Kasus Nasabah Bank Syariah di Indoneisa). 1–23.

Hotdiana, F., Indah, A., Nasution, L., Lathief, M., & Nasution, I. (2023). Pengaruh Pelayanan dan Produk Perbankan Syariah Terhadap Loyalitas Nasabah Dalam Mengambil Pendanaan dan Pembiayaan (Studi Kasus : Bank Syariah KC Padangsidimpuan). 9(02), 2442–2450.

Ilmiah, J., & Islam, E. (2022). Pengaruh Relationship Marketing , Comporate Image dan Syariah Compliance Terhadap Loyalitas Nasabah dengan Kepuasan Nasabah Sebagai Variabel Intervening Pada PT BSI KCP Gunung Tua. 8(03), 3423–3433.

Maulana, L., & Fitriana, N. (2023). Analisis dampak Insiden BSI Eror dan Dugaan Hacking Bank Syariah Indonesia (BSI) terhadap kepercayaan dan loyalitas nasabah Bank Syariah Indonesia di Kabupaten Subang. 7(3), 1755–1768.

Nawawi, Z. M. (2024). PENGARUH KUALITAS PELAYANAN DAN BRAND IMAGE PENGETAHUAN PRODUK SEBAGAI VARIABEL MODERASI. 7.

Sabda, P. F., Harahap, M. I., Syariah, J. A., Islam, U., & Sumatera, N. (2023). Jurnal Ilmu Komputer , Ekonomi dan Manajemen (JIKEM). 3(1), 1311–1346.

Wahyuni, E. (2015). Pengaruh Kepercayaan dan Kepuasan terhadap Loyalitas Nasabah Perbankan Syariah. Akmenika, 12(2), 683–688.