ASSES THE IMPACT OF CYBER CRIME MITIGATION STRATEGIES ON ISLAMIC BANKS IN BANDAR LAMPUNG CITY

Muhammad Varhisky Febriawan[1], Eogenie Lakilaki[2], Dwiki Ariefandri[3], Ryan Aditya Saputra[4], Panca Wijaya[5], Desta Manikam[6]

[1]Sharia banking, Faculty of Economics and business islam, Universitas Islam Negeri Raden Intan Lampung, Indonesia
[2,4]Accounting, Faculty of Economic, Universitas Sriwijaya, Indonesia
[3,5] Development Economics, Faculty of Economic, Universitas Sriwijaya, Indonesia
[6]Management, Faculty of Economic, Universitas Sriwijaya, Indonesia

febriawanvaris@gmail.com[1], eogenie09@gmail.com[2], dwikiariefandry@gmail.com[3], ryanaditya2502@gmail.com[4], pancawijaya09@gmail.com[5], manikamdesta4@gmail.com[6]

ABSTRAK

Kepercayaan nasabah terhadap perbankan syariah sangat penting. Pengelolaan teknologi di sektor perbankan dapat memainkan peran krusial dalam meningkatkan kepercayaan dan loyalitas nasabah. Tujuan dari penelitian ini adalah menguji dampak dari penanganan siber terhadap loyalitas nasabah, dengan kepercayaan sebagai variabel mediasi. Pengambilan sampel dilakukan dengan menggunakan metode Lemeshow, dengan jumlah responden sebanyak 96 orang. Analisis data dilakukan dengan metode SEM-PLS. Temuan penelitian menunjukkan bahwa penanganan siber memiliki pengaruh positif dan signifikan masing-masing terhadap loyalitas nasabah dan kepercayaan. Implikasi dari temuan ini menyoroti perlunya bank untuk memperkuat strategi keamanan siber guna mempertahankan loyalitas nasabah dan mengembangkan inovasi lain untuk meningkatkan kepercayaan, yang pada akhirnya akan berkontribusi pada loyalitas nasabah. Kesimpulannya, penanganan siber yang efektif dan peningkatan kepercayaan nasabah adalah kunci dalam mempertahankan dan meningkatkan loyalitas nasabah perbankan.
Kata Kunci: Kejahatan Siber, Loyalitas Nasabah, Bank Syariah, Kepercayaan

ABSTRACT

It is of the utmost importance to cultivate customer trust in Islamic banking. The effective management of technology in the banking sector has the potential to significantly influence customer trust and loyalty. The objective of this study is to investigate the influence of cyber security on customer loyalty, with trust as a mediating variable. The sampling was conducted using the Lemeshow method, with a total of 96 respondents. The data were analysed using the structural equation modelling with partial least squares (SEM-PLS) method. The research findings demonstrate that cyber-handling has a positive and significant influence on customer loyalty and trust, respectively. The implications of these findings emphasise the necessity for banks to reinforce their cybersecurity strategies in order to maintain customer loyalty and to develop further innovations with the objective of increasing trust, which will ultimately contribute to customer loyalty. In conclusion, effective cyber management and increased customer trust are pivotal in retaining and enhancing banking customer loyalty.
Keywords: Cyber Crime, Customer Loyalty, Islamic Bank, Trust.

INTRODUCTION

In the context of the national economy, the banking sector plays an essential role as a financial intermediary, which serves to link parties with surplus funds with parties in need of funds to support various economic activities (Rahayu et al., 2024). As an intermediary financial institution, banks play an important role in maintaining financial stability and promoting economic growth (Lakilaki et al., 2024). According to Ibrahim et al. (2021), the banking sector contributes significantly to maintaining the balance of financial circulation at the micro and macro levels. Therefore, maintaining the quality
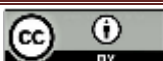
of banking services and products is crucial, as customer satisfaction directly affects the level of trust and increases the competitiveness of the banking industry in an increasingly competitive market.

In essence, Islamic banks diverge considerably from conventional banks, particularly with regard to their profit-making mechanisms (Anyndita et al., 2023). The aforementioned authors elucidated that in conventional banks, profits are generated through the implementation of interest rates, whereas Islamic banks prohibit interest and instead adopt a profit-sharing system as their primary financial instrument. Moreover, Mukti dan Suprayogi (2019) posit that, as financial institutions operating in accordance with Sharia principles, Islamic banks play a pivotal role in supporting the country's economic activities. They function as intermediary institutions that drive the economy in a fair and Sharia-compliant manner.

In addition to being oriented towards Islamic values, Islamic banking is also obliged to plan, organise, implement and manage quality systems to ensure that their services satisfy their customers (Kwarto & Angsito, 2018). Furthermore, Crystallography (2016) suggests that business actors should pay attention to issues that are considered important by consumers.

One of the key considerations for banking consumers is the level of customer trust in Islamic banking. This condition is reflected in the profit-sharing system, which is based on a fair agreement between the capital owner and the business manager. This collaboration offers advantages to both parties and also has a beneficial impact on society as a whole. Furthermore, customers' adherence to the principles of Islamic law and commitment to religious commandments demonstrates their orientation towards both worldly gains and the achievement of ukhrawi happiness as the ultimate goal (Kamilullah et al., 2018).

The role of customer trust in transactions that utilise technology is of paramount importance (Sandora, 2020). This is because users require assurance that the technology is reliable, including the guarantee of the security and privacy of their activities. The construction of trust is frequently impeded by considerable obstacles, including the potential for cybercrime, which can evoke surprise and apprehension among customers, thereby disrupting their perception of security in the context of technology use (Hasyim et al., 2022).

In a report released by CNBC, the Financial Services Authority (OJK) elucidated during the launching and media briefing of the OJK Banking Digital Transformation Blueprint (2021-2025) that cybercrime attacks have resulted in considerable financial losses. In 2022, the number of phishing attacks reached an all-time high, with the APWG reporting over 4.7 million incidents throughout the year, representing a 150% increase annually since 2019. In accordance with the Phishing Activity Trends report for the fourth quarter of 2022, Indonesian banks sustained financial losses amounting to IDR 246 billion as a consequence of cyber attacks that occurred between the first semester of 2020 and the first semester of 2021. During the same period, losses from other forms of cybercrime reached IDR 208 billion.

In their 2024 definition of cybercrime, Purwandari et al. (2024) describe criminal activity carried out by individuals, groups, or legal entities that utilise computers as the main means, with computers or computer networks as the target of the crime. The optimal alleviation of cybercrime in the banking domain can lead to an increase in customer satisfaction (Gomulya, 2023). Hidayat et al. (2023) additionally posited that the provision of superior quality services can enhance customer loyalty, given that the satisfaction of customers with products and services provides them with greater benefits. To this end, banks are engaged in ongoing efforts to enhance their systems, including through the adoption of integrated security measures that aim to bolster security, service quality, and product offerings (Kapitan et al., 2024). This initiative is designed to reinforce customer trust and loyalty. Moreover, in the context of mounting cybercrime threats, it is imperative for banks to closely monitor customer loyalty and trust in their banking services.

Sayid Qutb in Yasin et al. (2022) explained that the importance of Islamic Worldview principles in this problem lies in Islamic values such as trust (trust and responsibility), justice, ihsan (goodness), and maslahah (common welfare). Amanah in Islam requires banks to maintain customer privacy and security properly, especially in the face of cyber crime threats (Armasito & Musfirah, 2023). Yetno (2024) explains that when banks can effectively protect customer data, they demonstrate this responsibility, which strengthens customer trust in the bank. In the Islamic context, trust (tsiqah) is an important key in social and economic interactions, and this trust will be the link between the bank's success in dealing with cyber crime and customer
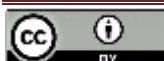
loyalty (Aprilya et al., 2024).

Furthermore, the Islamic worldview's conceptualisation of justice and ihsan serves to reinforce the interconnection between the handling of security and the demonstration of loyalty (Yetno, 2024). Banks that act in a fair and equitable manner, providing all customers with equal protection and striving to exceed expectations in their service, will tend to gain greater trust from customers (Pertiwi & Herianingrum, 2024). The principle of maslahah, which aims to achieve the common good, not only protects individuals from cyber crime but also maintains overall economic stability and security. In this way, customer trust, which is maintained through good security management, leads to a significant increase in customer loyalty.

In light of the aforementioned description, it is imperative to examine the impact of cybercrime on customer loyalty, with trust as a mediating variable.

METHODE

This research hypothesis is based on the findings of several previous studies. As Adestyan & Rapida (2022) have demonstrated, one of the factors affecting the loyalty of BSI Net Banking users is the level of customer loyalty, particularly in the context of security concerns. Despite the implementation of robust security measures, customers remain apprehensive about potential threats, including interference with bank servers, when utilising BSI Net Banking. These findings suggest that security plays a pivotal role in fostering customer loyalty. Consequently, H_1 postulates: that effectively addressing cyber crime will have a positive and significant impact on customer loyalty.

Subsequently, Savalas et al. (2018) delineate that information quality is defined as customer perceptions of the quality of product or service information on a website, whereas security is defined as the ability of online stores to control and maintain the security of transaction data. Trust is a cognitive component of psychological factors. Belief refers to the acceptance of a proposition as true or false based on evidence, advice, authority, experience, or intuition. The most important finding of this research is that security and trust have a positive effect on each other. Thus, H_2: The handling of cyber crime has a positive and significant effect on trust.

In their respective publications, Kamilullah et al. (2018) and Supertini et al. (2020) present a similar argument, namely that trust is a key determinant of customer loyalty. The relationship between customer trust and satisfaction with customer loyalty is positive and significant. Similarly, customer satisfaction has a positive and significant effect on customer loyalty. The findings of this study led to the formulation of the following hypothesis, H_3: The effect of trust on customer loyalty is positive and significant.

The fourth hypothesis is based on the findings of research conducted by Gultom et al. (2020), which states that the handling of cybercrime has a significant effect on customer trust and that this, in turn, affects customer loyalty. Therefore, it can be posited that H_4: that the handling of cybercrime has a positive and significant effect on customer loyalty through trust.

In this study, a quantitative approach is employed in reference to the aforementioned framework. The sampling method employed was the Lemeshow method, which involves determining the number of samples based on a large and tentative population (Somantri, 2021). This resulted in a sample size of 96 respondents, comprising 56 BSI customers and 40 Muamalat Bank customers. This study employs three variables: handling cyber crime (independent), customer loyalty (dependent), and trust (intervening).
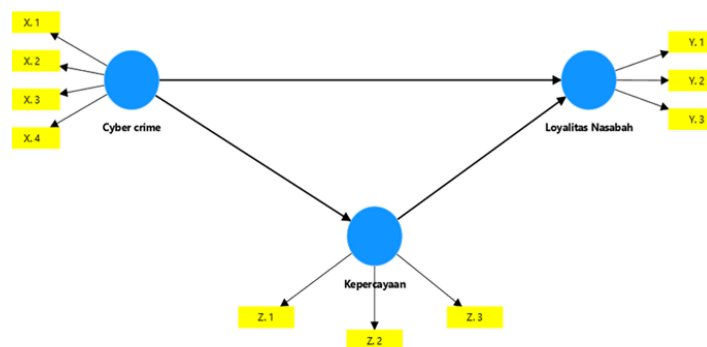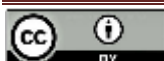

Figure 1. Research Model

The research data underwent several tests, including partial least squares SEM (PLS) analysis, outer model analysis (measurement model), inner model analysis (structural model), and hypothesis verification (Garson, 2016). The research model above is continued into an equation model as follows:

Tabel 1. Equation Model

Outer model For exogenous latent variable 1 (reflective)	Outer model For endogenous latent variable 1 (formative)	Outer model For endogenous latent variable 2 (reflective)	Inner Model
$X_{1.1} = \lambda X_{1.1} . X_1 + \delta_1$	$Y_{1.1} = \lambda Y_{1.1} . Y_1 + \delta_1$	$Y_{2.1} = \lambda Y_{2.1} . Y_2 + \delta_1$	$Y_1 = \gamma_1 X_1 + \zeta_1$
$X_{1.2} = \lambda X_{1.2} . X_1 + \delta_2$	$Y_{1.2} = \lambda Y_{1.2} . Y_1 + \delta_2$	$Y_{2.2} = \lambda Y_{2.2} . Y_2 + \delta_2$	$Y_1 = \beta_1 Y_1 + \gamma_1 X_1 + \zeta_2$
$X_{1.3} = \lambda X_{1.3} . X_1 + \delta_3$	$Y_{1.3} = \lambda Y_{1.3} . Y_1 + \delta_3$	$Y_{2.3} = \lambda Y_{2.3} . Y_2 + \delta_3$	
$X_{1.4} = \lambda X_{1.4} . X_1 + \delta_4$			

Source: Smart-PLS processed data (2024)

Description:
X_1 = Cyber crime exogenous latent variable
$Y_1(Z)$ = Endogenous and exogenous latent variables Trust
Y_2 = Endogenous latent variable Customer Loyalty
λX = Lamnda, factor loading of exogenous latent variables
λY = Lamnda, factor loading of endogenous latent variables
β = Gamma, the coefficient of influence of exogenous variables on endogenous
γ = Zeta, model error
ζ = Delta, measurement error on exogenous latent variables
δ = Epsilon, measurement error on latent variables endogen

Primary data was collected through a questionnaire with measurements shown in Table 2 below:

Tabel 2. Variable Measurement

Variable	Proxy	
Handling of *cyber crime* (Independent)	1.	Ascertain attack incidents from reliable source information
	2.	Efforts to minimise the attack from spreading
	3.	Post-attack incident services
Customer loyality (Dependent)	1.	Repeat, *i.e.* using the service repeatedly
	2.	Retention, which is the tendency to be loyal to a service
Trust (Intervening)	1.	Trust, the belief in one's performance.
	2.	Integrity, consistency between words and deeds
	3.	Kindness is a person's inner connection with intention.

Source: Some previous research (2024)

RESULTS AND DISCUSSION
Validity Test
The objective of the validity test is to ascertain the extent to which an instrument is capable of accurately measuring the concepts in **Convergent Validity Test**
question (Garson, 2016). In order to evaluate the model through a confirmatory lens, this study employs the Multi-Trait Multi-Method approach, with a focus on assessing both convergent and discriminant validity (Panca et al., 2017).
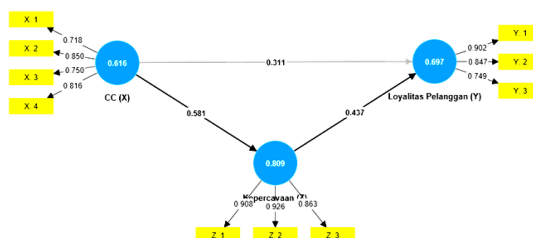

Figure 2. Outer Model Output of Convergent Validity Test
Source: Smart-PLS processed data (2024)

Tabel 3. Average Variace Extracted (AVE) of Convergent Validity Test

Indicators	*Average Variace Extracted (AVE)*
Handling of *cyber crime*	0.555
Customer loyality	0.809
Trust	0.597

Source: Smart-PLS processed data (2024)

The results of the convergent validity analysis, as illustrated in Figure 2, demonstrate that all indicators of each construct have a loading factor value exceeding 0.7. Additionally, as evidenced in Table 3, the AVE value is above 0.5, indicating that the instruments utilized in this study have fulfilled the requisite convergent validity criteria

.

Descrimant Validity Test

Tabel 4. Results of Cross Loading Descrimant Validity Test

Questions	HCC (X)	T (Z)	CL (Y)
HCC1	0.728	0.364	0.396
HCC2	0.824	0.544	0.514
HCC3	0.729	0.395	0.349
HCC4	0.795	0.491	0.510
T1	0.432	0.908	0.513
T2	0.598	0.927	0.587
T3	0.470	0.862	0.543
CL1	0.527	0.568	0.881
CL2	0.568	0.522	0.821
CL3	0.386	0.451	0.746

Source: Smart-PLS processed data (2024)

Reliability Test

The reliability of a construct can be reflected in the Cronbach alpha value and the composite reliability value. Cronbach alpha is employed to ascertain the lower limit of the reliability value of a construct, whereas composite reliability is utilised to determine the true reliability value of a construct (Garson, 2016).

Tabel 5. Composite Reliability and Cronbach Alpha Value

| Variable	*Cronbach's Alpha*	*Composite Reliability*
Handling of *cyber crime*	0.798	0.818
Customer loyality	0.772	0.808
Trust	0.882	0.894

Source: Smart-PLS processed data (2024)

Table 5 illustrates the Cronbach's Alpha value for the cybercrime handling variable, customer loyalty, and trust, which are 0.798, 0.772, and 0.882, respectively. Notably, these values align with a notable 0.60 consistency. This indicates that the consistency of responses across each construct is reliable. Subsequently, the Composite Reliability value for the variables of cybercrime handling, customer loyalty, and trust is 0.818, 0.808, and 0.894, respectively. This indicates that all variables have a Composite Reliability value exceeding 0.70. It can therefore be concluded that all constructs (variables) meet the requisite reliability criteria.

Inner Model or Structural Model Test

The objective of testing the inner model or structural model is to ascertain the relationship between the constructs of significant value and the R-Square of the research model. The structural model is evaluated using the R-Square for the dependent construct, a t-test, and the significance of the structural path parameter coefficients (Garson, 2016)
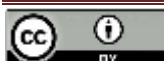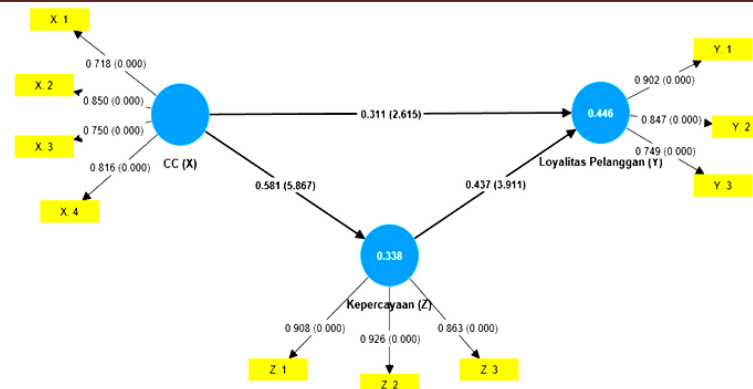
Figure 2. Inner Model Output or Structural Model from Bootstrapping Results
Source: Smart-PLS processed data (2024)

Tabel 6. R-Square Result

Variable	R-Square	R Square Adjusted
Customer loyality	0.475	0.464
Trust	0.317	0.310

Source: Smart-PLS processed data (2024)

So, based on the test results, several mathematical equations are obtained as shown in the table below:

Tabel 7. Equation Model

Outer model For exogenous latent variable 1 (reflective)	Outer model For endogenous latent variable 1 (formative)	Outer model For endogenous latent variable 2 (reflective)	Inner Model
$X_{1.1} = 0,718\ X1 + \delta_1$	$Y_{1.1} = 0,908\ Y1 + \delta_1$	$Y_{2.1} = 0,902\ Y2 + \delta_1$	$Y_1 = 0,010\ X_1 + \zeta_1$
$X_{1.2} = 0,850\ X2 + \delta_2$	$Y_{1.2} = 0,926\ Y1 + \delta_2$	$Y_{2.2} = 0,847\ Y2 + \delta_2$	$Y_2 = 0,010\ Y_1 + 0,010\ X1 + \zeta_2$
$X_{1.3} = 0,750\ X3 + \delta_3$	$Y_{1.3} = 0,863\ Y1 + \delta_3$	$Y_{2.3} = 0,749\ Y3 + \delta_3$	
$X_{1.4} = 0,816\ X4 + \delta_4$			

Source: Smart-PLS processed data (2024)

Table 6 indicates that the R-Square value for the Trust variable is approximately 0.317. These results indicate that customer loyalty has an R-Square value of 0.475, suggesting that the cyber crime handling and trust variables may be able to explain the customer loyalty variable by approximately 47.5%. It is possible that the .

remaining 52.5% is explained by other variables not included in the model. Further results for the cyber crime handling variable suggest that it may be able to explain the trust variable by 31.7%. It seems that the remaining 68.3% may be explained by other variables not hypothesised in the model
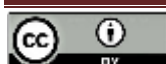
Hypothesis Test

Tabel 8. Path Coefficients Results

Hypothesis	Original Sample (O)	Sample Mean (M)	Standard Deviation (STDEV)	P Values
X →Y	0.384	0.369	0.111	0.001
X →Z	0.563	0.581	0.105	0.000
Z → Y	0.395	0.408	0.113	0.000
X → Z → Y	0.223	0.244	0.098	0.024

Source: Smart-PLS processed data (2024)

The handling of cyber crime on customer loyalty obtained a p value of 0.001 (<0.05) and an original sample value of 0.384. This means that handling cyber crime has a positive and significant

effect on customer loyalty. Therefore, the first hypothesis which states that handling of cyber crime has a positive and significant effect on customer loyalty is accepted. Handling of cyber

crime on trust obtained a p value of 0.000 (<0.05) and an original sample value of 0.563. This means that handling cyber crime has a positive and significant effect on trust. Therefore, the second hypothesis which states that handling of cyber crime has a positive and significant effect on trust is accepted. Trust on customer loyalty obtained a p value of 0.000 (<0.05) and an original sample value of 0.395. This means that trust has a positive and significant effect on customer loyalty. Therefore, the third hypothesis which states that Trust has a positive and significant effect on customer loyalty is accepted. The handling of cyber crime on customer loyalty through trust obtained a p value of 0.0024 (<0.05) and an original sample value of 0.223. This means that handling cyber crime has a positive and significant effect on customer loyalty through trust. Therefore, the fourth hypothesis which states that handling cyber crime (X) has a positive and significant effect on customer loyalty (Y) through trust (Z) is accepted.

Handling Of Cyber Crime On Customer Loyalty

In alignment with the findings of Adestyan & Rapida (2022), which revealed that the handling of cyber crime (security) has a significant effect on customer loyalty, this is substantiated by the Islamic perspective, which emphasises the necessity for the prevention and management of all forms of crime, including cyber crime, in order to safeguard relationships between individuals and society. This is crucial as any disruption to the order of life based on the values of justice and trust has the potential to have far-reaching consequences. In this context, customer loyalty can be defined as a form of commitment to a relationship based on trust, which represents a fundamental principle in Islamic economic transactions (*muamalah*). Ramdhani (2016) also voiced that when the aspects of confidentiality, integrity and availability are fulfilled, it can increase the level of customer loyalty.

From the perspective of the public good (*maslahah*), actions that prevent loss or insecurity (such as cybercrime) and support the common good, such as increasing loyalty through security protection, are aligned with the objective of achieving the welfare of the ummah. A similar sentiment was also expressed by Habibi & Liviani (2020). If cybercrime can be effectively addressed and security guaranteed, this will enhance customer loyalty, which in turn will yield benefits for individuals and society at large in financial transactions.

Handling Of Cyber Crime On Trust

The results of hypothesis testing conducted with the bootstrapping method show that the handling of cyber crime on trust. Savalas et al. (2018), Suprapto & Susanti (2019) and Adestyan & Rapida (2022) compactly state that the handling of cyber crime (security) has a significant effect on Trust.

In the context of the Islamic worldview, the results of this test confirm the importance of maintaining security and trust as part of trust (responsibility) in social relations, including in economic and digital transactions. Islam emphasises that trust is an important foundation in all aspects of life, especially in muamalah (social and business interactions). Effective handling of cybercrime leads to increased trust, which is the essence of business ethics in Islam, where every party should feel safe and secure in transactions, in line with the principles of fairness and honesty.

Protection from cybercrime and increased security create better conditions for society at large, which in turn improves general welfare (Kurniawan et al., 2022). Handling cybercrime with a positive impact on trust supports the creation of stronger and more sustainable business relationships, which in turn brings benefits to both customers and financial institutions.

Handling Of Trust On Customer Loyality

The findings of this study are consistent with those of previous studies, which similarly identified trust as a significant determinant of customer loyalty. This is in line with the findings of Kamilullah et al. (2018) and Supertini et al. (2020). It is reasonable to conclude that there is a causal relationship between trust and loyalty. When an individual trusts a service or product, they are more likely to become a loyal customer (Andesra, 2016). This lends further support to the theory that trust is a crucial factor in maintaining long-term relationships between consumers and service providers.

The Islamic worldview offers a conceptualisation of trust (*amanah*) as a principal tenet of social and economic life. The trust that is established between individuals and institutions reflects the values of honesty and integrity, which serve as the cornerstones of business interactions. The results of the study demonstrate that trust has a significant impact on loyalty, aligning with Islamic principles that emphasise the importance of maintaining harmonious and trusting
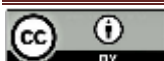
relationships in *muamalah* (economic transactions). Loyalty in this context is not merely a matter of customer attachment; it also signifies recognition of the honesty and reliability of the service provider.

From a *maslahah* perspective, increased trust that leads to loyalty contributes to the creation of benefits for all parties involved (Soediro & Meutia, 2018). Furqani (2019) also added that The sustainability of business relationships is contingent upon the establishment of trust, which in turn is dependent upon the existence of loyalty. The consequence of this is that the well-being of society is ultimately enhanced. This is because trust is a key factor in fostering loyalty, which in turn leads to the creation of benefits for all parties involved. In this context, trust confers benefits not only on individuals or institutions, but also on the wider economic system, which is rendered more stable and sustainable as a result. Loyalty that is based on trust helps to guarantee the sustainability of business relationships, which in turn contributes to the general well-being of society.

Handling Of Cyber Crime On Customer Loyalty Through Trust

In their publication, Gultom et al. (2020) posit that the handling of cybercrime (security) exerts a positive and significant influence on loyalty through the formation of trust. Once the threat of cybercrime has been successfully mitigated, customers will have greater confidence in the existing security system, which will encourage them to remain loyal to the institution. Trust serves as an intermediary that connects the handling of cyber crime with customer loyalty (Sondakh, 2018). In the absence of trust, customers will be unable to perceive the services provided as safe, and thus will be disinclined to continue using them. It is therefore reasonable to conclude that enhanced security measures against cybercrime will directly result in increased customer loyalty.

In Islamic thought, the handling of cyber crime is inextricably linked to the concepts of trust and moral responsibility, which must be upheld by all individuals and institutions. Islamic teachings posit that the safeguarding of security and the prevention of detrimental actions, such as cybercrime, is a moral obligation. When cyber crime is handled effectively, customer trust is likely to increase, as a sense of security and protection is afforded to them. This trust then serves to foster customer loyalty, in accordance with Islamic teachings that prioritise relationships based on justice, honesty and mutual trust.

Hasyim et al. (2022) hasyim views in terms of maslahah's eye, the effective handling of cyber crime provides benefits to all parties involved. By reducing the risks caused by cybercrime, people can transact more safely, thereby supporting sustainable business relationships and economic prosperity. The trust established through digital security brings benefits to customers and institutions, which in turn strengthens loyalty and economic sustainability.

CONCLUSION

The findings of the study, which was conducted on 96 customers of an Islamic bank in Bandar Lampung, indicate that the effective handling of cybercrime has a positive and significant impact on customer loyalty, both directly and indirectly. The effective handling of cyber crime incidents engenders a sense of security, reinforces customer trust, and fosters customer loyalty. Furthermore, trust functions as an intervening variable, reinforcing the relationship between the handling of cyber crime and customer loyalty. This serves to reinforce the importance of effectively managing cyber crime in order to maintain customer loyalty.

From the side of Worldview Islamic, effective management of cyber crime is an expression of trust and moral responsibility in protecting individual and collective rights. This is in alignment with the principle of justice in *muamalah*. Effective handling of cyber crime fosters a sense of security, enhances customer trust, and reinforces loyalty in alignment with Islamic teachings on sustainable, mutually beneficial relationships. From a *maslahah* perspective, this aspect of security confers widespread benefits by protecting customers from cybercrime, bolstering economic stability, and advancing prosperity.

REFERENCES

Adestyan, F. M., & Rapida, I. (2022). Pengaruh Keamanan, Kepuasan, Kemudahan dan Kepercayaan terhadap Loyalitas Pengguna BSI Net Banking di Bank Syariah Indonesia KCP Suropaticore Bandung. Jurnal Maps (Manajemen Perbankan Syariah, 6(1), 53–61.

Anyndita, R., Salsadila, P., & Djasuli, M. (2023). Analisis Perbandingan Kinerja Keuangan Perbankan Syariah Dengan Perbankan Konvensional. Jurnal Ekonomi Islam Al-Infaq, 2(2), 19–48.

https://doi.org/10.47233/jemb.v1i1.451

Aprilya, N. W., Amrullah, A., & Misbach, I. (2024). Analisis Penerapan Good Corporate Governance Perspective Sharia Pada Bank Syariah Indonesia. El-Iqthisadi Jurnal Hukum Ekonomi Syariah, 6(1), 62–78. https://doi.org/10.24252/el-iqthisady.vi.46705

Armasito, & Musfirah, D. (2023). Problematika Perlindungan Data Pribadi Dari Cyber Crime Di Era Ekonomi Digital Menurut Hukum Positif. Sharia and Law Proceeding (SL-Pro) The 2 Nd Raden Fatah International Conference On Sharia and Law Faculty (RAFAH-ICoShaL), 1(1), 2023.

Andesra, Y. (2016). Peran Kualitas Pelayanan Dalam Mebangun Kepercayaan Dan Loyalitas Nasabah Bank Syariah Mandiri Cabang Simpang Empat. Jurnal Apresiasi Ekonomi, 4(2), 139–150.

Anita, F., & Tanujaya, K. (2023). Pengaruh Kejahatan Siber Terhadap Kinerja Organisasi Dengan Moderasi Kesadaran Keamanan Informasi. Jurnal Ekuilnomi, 5(2), 266-275

Fernandes, Y. D., & Marlius, D. (2018). Peranan Customer Service Dalam Meningkatkan Pelayanan Kepada Nasabah Pada Pt. Bank Pembangunan Daerah Sumatera Barat Cabang Utama Padang. Akademi Keuangan Dan Perbankan Padang, 1–12.

Furqani, H. (2019). Teorisasi Ekonomi Islam. Ar-Raniry Press

Garson, G. D. (2016). Partial Least Squares: Regression & Structural Equation Models. In Statistical Associates Publishing. https://doi.org/10.1201/b16017-6

Gomulya, A. M. (2023). Efektivitas Peran Literasi Digital Dalam Pembangunan Ekonomi Digital, Studi Kasus Pada Korban Kejahatan Pinjaman Online Ilegal. Jurnal Kritis, 32(2), 117–136. https://doi.org/10.24246/kritis.v32i2p117-136

Gultom, D. K., Arif, M., & Muhammad Fahmi. (2020). Determinasi Kepuasan Pelanggan Terhadap Loyalitas Pelanggan Melalui Kepercayaan Dedek. MANEGGGIO: Jurnal Ilmiah Magister Manajemen, 3(2), 273–282.

Habibi, M. R., & Liviani, I. (2020). Kejahatan Teknologi Informasi (Cyber Crime) dan Penanggulangannya dalam Sistem Hukum Indonesia. Al-Qanun: Jurnal Pemikiran Dan Pembaharuan Hukum Islam, 23(2), 400–426.

Hidayat, F., Riono, B., Kristiana, A., & Dewi, I. (2023). Pengaruh Kualitas Pelayanan dan Inovasi Produk terhadapKepuasan Pelanggan untuk Meningkatkan Loyalitas Pelanggan. JECMER: Journal of Economic, Management and Entrepreneurship Research, 1(3), 214–231.

Ibrahim, R. A., Yaqin, C., & Simbolon, M. J. (2021). Optimalisasi Pengaturan Layanan Urun Dana (Crowdfunding) Berbasis Teknologi Informasi Sebagai Solusi Permodalan Usaha Mikro, Kecil, Dan Menengah Di Masa Pandemi Covid-19. Jurnal Lex Renaissan, 6(4), 732–751. https://doi.org/10.20885/jlr.vol6.iss4.art7

Kamilullah, J., Kusyanti, A., & Aryadita, H. (2018). Analisis Pengaruh Kepercayaan, Kepuasan, dan Reputasi Terhadap Loyalitas Konsumen Online Shop Dalam Pembelian Produk di Toko XYZ. Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer (J-PTIIK) Universitas Brawijaya, 2(7), 2660–2669.

Kapitan, Y., Suryana, K. D., & Herawati, K. M. (2024). Tantangan dan Prospek Implementasi E-Government Dalam Meningkatkan Kualitas Pelayanan Publik di Era Digital. Nusantara Hasana Journal, 4(4), 20–38.

Kurniawan, A. S., Widowati, R., & Handayani, S. D. (2022). Integration of the Theory of Reasoned Action (TRA) on Hotel Room Repurchase Intention using Online Hotel Room Booking Applications. Jurnal Manajemen Teori Dan Terapan | Journal of Theory and Applied Management, 15(1), 77–90. https://doi.org/10.20473/jmtt.v15i1.34935

Kwarto, F., & Angsito, M. (2018). Pengaruh Cyber Crime Terhadap Cyber Security Compliance Di Sektor Keuangan. Jurnal Akuntansi Bisnis, 11(2), 99–110. https://doi.org/10.30813/jab.v11i2.1382

Lakilaki, E., Soediro, A., & Akram Hassan, S. (2024). A Study of GRI on Financial Performance Phenomenon. AKRUAL: Jurnal Akuntansi, 15(2), 165–175. https://doi.org/10.26740/jaj.v15n2.p165-p175

Mukti, T. W., & Suprayogi, N. (2019). Apakah
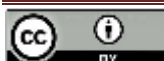
Bank Syariah Berbeda Dengan Bank Konvensional? (Kajian Fenomenologi). Jurnal Ekonomi Syariah Teori Dan Terapan, 6(6), 1137–1152. https://doi.org/10.20473/vol6iss20196pp 1137-1152

Panca, W. A., Jamin Ariana, I. N., & Arismayanti, N. K. (2017). Pengaruh Kualitas Pelayanan Terhadap Loyalitas Wisatawan dan Citra Hotel Melati di Kelurahan Seminyak Kabupaten Badung Bali. Jurnal Kepariwisataan Dan Hospitalitas, 1(1), 65–72.

Pertiwi, T. D., & Herianingrum, S. (2024). Menggali Konsep Maqashid Syariah: Perspektif Pemikiran Tokoh Islam. Jurnal Ilmiah Ekonomi Islam, 10(1), 807–820. https://doi.org/10.29040/jiei.v10i1.12386

Purwandari, M. D., Awaliah, A. U., Una, B. K., Yogi, H., Indonesia, U. I., Ekonomi, F., Sulawesi, U. T., Sosial, F. I., & Gorontalo, U. M. (2024). Phishing Case Disclosure Strategy: A Case Study in Indonesia. COST, 7(5), 3516–3533.

Rahayu, M., Fauzi, R., Fadilah, M. R., & Firmansyah, R. Y. (2024). Jasa-Jasa Bank dalam Kegiatan Perbankan : Sebuah Kajian Literatur. JISOSEPOL: Jurnal Ilmu Sosial Ekonomi Dan Politik, 2(2), 220–227.

Ramadhani, T., Budimansyah, B., & Sanjaya, Vi. F. (2021). Pengaruh Rating Dan Online Consumer Review Terhadap Minat Beli Dengan Kepercayaan Sebagai Pemediasi Pada Marketplaceshopee Dalam Persfektif Ekonomi Islam (Studi Pada Mahasiswa Universitas Islam Negeri Raden Intan Lampung). REVENUE: Jurnal Manajemen Bisnis Islam, 2(2), 143–162. https://doi.org/10.24042/revenue.v2i2.96 23

Ramdhani, N. (2016). Penyusunan Alat Pengukur Berbasis Theory of Planned Behavior. Buletin Psikologi, 19(2), 55–69.

Sandora, M. (2020). Pengaruh Kepercayaan Dan Kemudahan Terhadap Keputusan Pembelian Belanja Secara Online. Jurnal Eko Dan Bisnis, 11(3), 290–310. https://doi.org/10.36975/jeb.v11i3.288

Soediro, A., & Meutia, I. (2018). Maqasid Sharia As A Performance Framework For Islamic Financial Institutions. Jurnal Akuntansi Multiparadigma, 9(1), 70–86.

Shoffan Hasyim, I. et al. (2022). Analysis of Perceived Usefulness, Perceived Ease of Use, Trust, And Sharia Financial Literature on The Adoption of Sharia Fintech By MSMEs. Al-Kharaj : Jurnal Ekonomi, Keuangan & Bisnis Syariah, 5(3), 1218–1234. https://doi.org/10.47467/alkharaj.v5i3.15 72

Somantri, B. (2021). Kontribusi Etnosentrisme dan Gaya Hidup Terhadap Keputusan Pembelian Baju Batik Sebagai Identitas Diri. Jurnal Cakrawala, 75(17), 399–405.

Sondakh, C. (2018). Kualitas Layanan, Citra Merek dan Pengaruhnya Terhadap Kepuasan Nasabah dan Loyalitas Nasabah Tabungan (Studi Pada Nasabah Taplus BNI Cabang Manado). Jurnal Riset Bisnis Dan Manajemen, 3(1), 19–32. https://ejournal.unsrat.ac.id/index.php/jrb m/article/view/7525

Supertini, N. P. S., Telagawati, N. L. W. S., & Yulianthini, N. N. (2020). Pengaruh kepercayaan dan kepuasan pelanggan terhadap loyalitas pelanggan pada Pusaka Kebaya di Singaraja. Prospek: Jurnal Manajemen Dan Bisnis, 2(1), 61. https://doi.org/10.23887/pjmb.v2i1.2620 1

Suprapto, R., & Susanti, M. (2019). Pengaruh Pengetahuan Produk dan Kepercayaan terhadap Sikap Loyalitas Peserta BPJS Kesehatan Daerah Istimewa Yogyakarta. Buletin Bisnis & Manajemen, 02(01), 69.

Yasin, H., Jannah, S. P., Nadiaturrohmah, T., Izzatun, N., & Risma. (2022). Islamic World View. Tahdzib Al-Akhlaq : Jurnal Pendidikan Islam, 5(1), 1–678. https://doi.org/10.4324/9780203019139

Yetno, A. (2024). Tanggung Jawab Bank Dalam Menjaga Keamanan Dan Kerahasiaan Data Nasabah Perbankan Di Indonesia. Morality: Jurnal Ilmu Hukum, 10(1), 67–76.