Jurnal Ekonomi & Keuangan Islam
2025, 11(2), 179-195

Do cyberattacks and religiosity impact customers' loyalty? Study on Bank Syariah Indonesia

Noorfaiz Athallah Koeswandana[1], Mayang Yorindafitri Yulfiatmi [2]

[1]Department of Accounting, Faculty of Business and Economics, Universitas Islam Indonesia, Yogyakarta, Indonesia
[2]Department of Accounting, Faculty of Economy and Business, Universitas Gadjah Mada, Yogyakarta, Indonesia

Article Info

Article History
Received : 2024-12-17
Revised : 2025-04-16
Accepted : 2025-08-04
Published : 2025-08-06

Keywords:
Cyberattacks, Customer Satisfaction, Customer Loyalty, Protection Motivation Theory.

DOI:
10.20885/JEKI.vol11.iss2.art2

JEL Clasification:
G21, G41

Corresponding author:
Noorfaiz Athallah Koeswadana
Noorfaiz.koeswandana@uii.ac.id

Author's email:
mayangyorindafitriyulfiatmi3199@mail.ugm.ac.id

Paper type:
Research paper

Center for Islamic Economics Studies and Development, Faculty of Business and Economics, Universitas Islam Indonesia

Abstract

Purpose – This study aimed to investigate the impact of cyberattacks on customer loyalty and satisfaction in the context of Islamic banking, particularly focusing on recent cyberattacks on Bank Syariah Indonesia (BSI).

Methodology – Respondents were chosen using purposive sampling and analyzed using Partial Least Square - Structural Equation Modelling (PLS-SEM). 244 respondents participated in this study and were analyzed using SmartPLS 3.2.9 Software.

Findings – The results showed that perceived vulnerability and perceived risk negatively influence customer satisfaction, while religiosity positively influences customer satisfaction. Religiosity also has a positive, direct effect on customer loyalty. Surprisingly, perceived severity did not show any significant influence on customer satisfaction after the cyberattacks.

Implications –This study can be used by every bank in Indonesia to increase customer loyalty by minimizing the risk that customers might experience, especially in cybersecurity issues.

Originality – This study contributes to the literature on customer loyalty after cyberattacks. This study incorporates the religiosity variable in combination with Protection Motivation Theory. Religiosity is expected to have a positive influence on both loyalty and satisfaction, as the research object is Bank Syariah, Indonesia, which offers Islamic financial products. Most customers choose Islamic banks because of the alignment of financial products with Islamic principles (Wijaya et al., 2020).

Cite this article:
Koeswandana, N. A., & Yulfiatmi, M. Y. (2025). Do cyberattacks and religiosity impact customers' loyalty? Study on Bank Syariah Indonesia. *Jurnal Ekonomi & Keuangan Islam*, 11(2), 179-195. https://doi.org/10.20885/JEKI.vol11.iss2.art2

Introduction

As major players in the financial industry, banks face the greatest risk of cyberattacks because of their management of sensitive customer information and large financial assets. Data from Kost (2023) highlights that most banking cyberattacks aim to steal sensitive customer data. Common attack methods include malware, Distributed Denial of Service (DDoS) attacks, and Advanced Persistent Threats (APT). Cyberattacks, such as the 2016 Bangladesh Bank Heist, have caused significant financial losses worldwide, resulting in a $101 million loss (Maurer & Nelson, 2021), ransomware payments exceeding $1 billion in the United States (Cox, 2022), and a $10 million loss in Chile in 2018 (Zurkus, 2018). A recent cyberattack in May 2023 targeted Bank Syariah Indonesia

P ISSN 2088-9968 | E ISSN 2614-6908

(BSI). The attack, conducted by the hacker group LockBit, compromised 15 million customer records, including names, addresses, phone numbers, account details, legal documents, and passwords (Pandagle, 2023). Initially, BSI attributed system outages to maintenance, failing to inform customers about the breach. The hackers demanded $20 million, whereas the BSI offered $10 million. Negotiations failed, leading to the release of customer data from the Dark Web.

BSI is not the only Islamic bank targeted by cyber-attacks. In 2018, BankIslami in Pakistan suffered a $6 million loss, with over 8,000 credit card records stolen and sold online (Rewterz, 2018). Islamic banks in the Middle East, including those in Saudi Arabia and the United Arab Emirates, have also faced frequent cyberattacks. In 2017, over 3.6 trillion cyber incidents were reported in these regions (Yazbeck, 2019). These cases highlight that Islamic banks are prime targets for cybercriminals, necessitating enhanced security measures, such as using Artificial Intelligence (AI) and advocating for stronger cybersecurity laws.

Cyberattacks inevitably affect the customer satisfaction in the banking industry. Key factors influencing customer satisfaction include performance, privacy, and security issues (Khedmatgozar & Shahnazi, 2018). Among these, perceived security significantly affects customer trust (Hanafizadeh & Khedmatgozar, 2012). Trust can be evaluated from multiple dimensions, including transaction reliability, organizational integrity, information quality, and technological robustness (Qasaimeh et al., 2022). Addressing privacy and security concerns is essential for building customer trust, which in turn fosters loyalty (Al Batayneh et al., 2021; Qasaimeh et al., 2022). This study focuses on the impact of cyberattack on customer satisfaction, particularly in the context of Islamic banking. It also explores whether religiosity influences customer loyalty following cyberattacks. This study incorporates the religiosity variable in combination with Protection Motivation Theory. Religiosity is expected to have a positive influence on both loyalty and satisfaction, as the research object is Bank Syariah, Indonesia, which offers Islamic financial products. Most customers choose Islamic banks because of the alignment of financial products with Islamic principles (Wijaya et al., 2020). Previous research has primarily addressed the impact of cyberattacks on stock performance (Nisa & Cahyono, 2024) and IT risk-mitigation strategies (Fitriani et al., 2023). However, previous studies have limitations when discussing user perceptions after a cyberattack incident. Sebayang et al. (2024) conducted research focusing on customer perceptions, but it was based on the Technology Acceptance Model (TAM) and was not linked to cyberattack incidents. Bajwa et al. (2023) also conducted research to investigate the impact of cyberattack awareness on customer trust and commitment in the Pakistani banking sector. This study seeks to fill this gap by investigating how customers perceive severity, risk, and vulnerability after such incidents. This study also aims to fill the research gap in previous studies, which have not examined this issue in the context of Islamic banking in Indonesia. In this study, we have an objective to predict what factors influence loyalty and satisfaction in the context of customers of Bank Syariah Indonesia.

The study is organized into five sections: introduction, literature review, hypothesis development, research methodology, results, discussion, and conclusion. Theoretically, this study expands the literature on the relationship between customer loyalty and cyberattacks within Sharia-based organizations. Practically, it offers insights for Islamic banks such as BSI to understand the key drivers of customer loyalty after cyberattack. Furthermore, the findings can guide governments in formulating robust cybersecurity legislation to protect customers, thereby ensuring that digital trust is preserved in the financial sector.

Literature Review

Cyberattacks

Cyberattacks have become a critical issue in Islamic banking accounting, affecting financial reporting, risk management, and customer trust. In the case of BSI, recent cyberattacks have raised concerns about data security, financial disclosures, and internal control weaknesses, which are essential aspects of accounting and corporate governance. Such incidents can lead to financial misstatements, operational losses, and reputational damage, ultimately affecting customer satisfaction and loyalty. From an Islamic accounting perspective, cybersecurity breaches challenge the principles of trust (*amanah*) and transparency (shariah compliance), which are fundamental to ensuring accurate financial reporting and stakeholder confidence. Therefore, addressing cybersecurity risks in Islamic banking accounting is crucial for enhancing internal controls, regulatory compliance, and financial stability in the sector.

Cyberattacks include various types such as phishing attacks, malware, ransomware attacks, and data breaches. A data breach occurs when unauthorized parties access confidential information held by firms, causing financial and privacy harms to both employees and customers (Culnan & Williams, 2009). Failure to protect sensitive information damages a firm's reputation and negatively impacts customer relationships (Janakiraman et al., 2018; Perera et al., 2022). Cyberattacks and data breaches are categorized as service failures (Culnan & Williams, 2009), which are distinct from product failures. Product failures can be addressed through product guarantee procedures, which are typically resolved quickly (Chen & Jai, 2021). By contrast, service failures require more time for detection, assessment, and recovery, making the process significantly more complex (Malhotra & Malhotra, 2011). Service failure recovery involves communicating the issue, addressing customer concerns regarding vulnerability and severity, issuing apologies (Janakiraman et al., 2018), and offering compensation (Greve et al., 2020). Service failures can worsen when publicly announced, particularly to customers (Rasoulian et al. 2023). In such cases, firms must invest additional effort in rebuilding customer trust and restoring relationships (Choi et al., 2016). Thus, data breaches are categorized as service failures, which may further damage customer relationships.

Most previous studies have explored the organizational impact of data breaches, such as managerial responses (Herath & Rao, 2009) and market reactions (Rasoulian et al., 2023; Rosati et al., 2019). However, studies focusing on user perceptions remain limited. This study investigated the impact of cybersecurity breaches on user perceptions.

Protection Motivation Theory (PMT)

Protection Motivation Theory (PMT) explains the three components of a fear appeal, such as the severity level of danger occurring, the probability of the event occurring, and the protective response (Rogers, 1975). These components were interrelated and occurred sequentially. If an event is perceived as highly severe, protection motivation is likely to be triggered (Rogers 1975). Conversely, if an event is considered low in severity, protection motivation will not be activated. In contrast, if an event occurs and is considered to be of low severity, protection motivation will ll not appear. The PMT involves two cognitive mediation processes: threat appraisal and coping appraisal (Floyd et al., 2000). Threat appraisal assesses maladaptive behavior based on perceived severity and vulnerability. Once a threat is evaluated, coping appraisal evaluates the ability to manage danger through response efficacy or self-efficacy.

Previous studies have used PMT as the underlying framework to investigate cybersecurity awareness across various countries. For instance, Kiran et al. (2025) examined cybersecurity behavior in Pakistan using PMT and found that perceived severity significantly influenced threat appraisal. Similarly, Jamil et al. (2024) applied PMT to analyze microbusiness owners' security behavior in Australia, while Mukhopadhyay and Jain (2024) explored strategies to mitigate cyberattacks in the Australian insurance sector. Following these prior studies, this research also employs PMT to predict individual cybersecurity behavior, particularly by focusing on threat appraisal mechanisms, such as perceived severity and perceived vulnerability.

The PMT has been widely adopted in information security research (Prentince-Dunn & Rogers, 1986). Herath and Rao (2009) found that the PMT construct performs well in examining security behaviors. Thus, this study extends the application of PMT by investigating how these factors influence customer satisfaction in the context of cybersecurity threats in Islamic banking.

Hypothesis Development

Perceived vulnerability & perceived severity on customer satisfaction

User vulnerability refers to customers' likelihood of being exposed to a specific threat (Rogers, 1975), while severity reflects the extent to which a security breach impacts or threatens their financial and personal well-being (Chakraborty et al., 2016). Both factors play a crucial role in shaping customer perceptions of data security and privacy risks, particularly in the banking sector, where sensitive personal and financial information is stored and processed (Dang-Pham & Pittayachawan, 2015). When banks collect extensive customer data, the risks of unauthorized access, fraud, and misuse increase, making cybersecurity a critical concern. In the case of a severe cyberattack, customers may lose trust in the bank, blaming it for failing to uphold its responsibility for protecting confidential information.

In the context of Islamic banking, cybersecurity risks take on an additional dimension related to the Shariah principles of trust (*amanah*) and transparency (*mas'uliyyah*). According to Hill and Sharma (2020), vulnerability arises when customers feel exposed to cyber threats beyond their control, which can lead to stress, uncertainty, and dissatisfaction (Baker et al. 2005). This is particularly relevant for Islamic banks, which operate based on ethical financial principles and are expected to prioritize customer welfare. Rasoulian et al., (2017) emphasized that information security is a fundamental obligation of financial institutions, and failure to provide adequate protection can significantly reduce customer satisfaction and loyalty (Rasoulian et al., 2023). For Islamic banks, ensuring robust cybersecurity measures is not just a matter of compliance, but also aligns with Shariah values of integrity and customer protection, reinforcing consumer confidence and long-term trust in the institution. Based on this argument, we hypothesized the following:
H_1: Perceived Vulnerability has a negative effect on customer satisfaction

Each individual perceives the severity of a cyberattack differently (Chakraborty et al., 2016). Those with low cybersecurity awareness may be indifferent to the exposure of their personal information, whereas individuals with higher awareness may experience significant distress even if only basic data are compromised (Aivazpour et al., 2018). In the banking sector, particularly Islamic banking, where trust (*amanah*) is a core principle, perceptions of severity can directly influence customer satisfaction and loyalty. Greve et al. (2020) found that the severity of a breach significantly affects customer satisfaction because customers who experience greater financial or personal harm are more likely to lose trust in the institution. However, their study also highlighted that expressing remorse and offering compensation can help restore customer confidence and mitigate the negative effects of cyberattacks. For Islamic banks, addressing cybersecurity incidents transparently and ethically aligns with the Shariah principles of fairness and accountability, reinforcing consumer trust and long-term loyalty despite security challenges. Based on this argument, we hypothesize the following.
H_2: Perceived Severity has a negative effect on customer satisfaction

Perceived risk on customer satisfaction

Perceived risk can be defined as the trade-off between the expected output and potential loss associated with product or service usage (Featherman & Pavlou, 2003). Aivazpour et al. (2018) define perceived risk as a customer's assessment of the probability of experiencing a negative outcome. Previous studies have examined perceived risk in various contexts such as digital payment (Kirmani et al., 2022), online shopping (Chang et al., 2016), and e-banking (Mulia et al., 2020). These studies consistently use perceived risk to predict its influence on customer satisfaction. If customers receive outcomes different from what they expect, their satisfaction tends to decrease (Riefel, 2022). In the context of Islamic banking, Rohman et al. (2021) found that system reliability and security are key factors influencing customer satisfaction, as Islamic banks operate under the principles of *maqashid sharia,* particularly the protection of wealth. Based on these findings, we hypothesize the following:
H_3: Perceived risk has a negative effect on customer satisfaction.

Religiosity on satisfaction and loyalty

Terms such as "religiosity" and "religion" are sometimes used interchangeably to describe the same concept, reflecting the regard, adoration, and conviction that individuals hold for a divine being (Souiden and Rani 2015). Religiosity can be defined as a person's level of devotion and adherence to divine rules (Suhartanto et al. 2020). Souiden and Rani (2015) described religiosity as an individual's commitment to their religion and its teachings, including the behaviors and attitudes that demonstrate this commitment. Individuals with high religious knowledge and practice base their decisions and actions on religious principles (Abou-Youssef et al. 2015). Thus, religiosity can shape an individual's mindset and actions when multiple options are available (Yusfiarto et al. 2022).

Research has found that religiosity affects both satisfaction and loyalty. Yusfiarto et al. (2022) found that religiosity positively influences satisfaction, but has no direct effect on customer loyalty. Koeswandana and Sugino (2023) emphasized the importance of religiosity in shaping customer attitudes and behaviors toward financial products and services. Suhartanto et al. (2020) find that individuals with higher levels of religiosity are more loyal to Islamic banks. Sutarso (2022) also finds that religiosity affects the usage of Islamic products. Setiawan et al. (2019) and Soma et al. (2017) demonstrate that religiosity directly influences customer loyalty.

Religiosity plays a key role in shaping how customers feel and stay loyal to Islamic banks. Many people choose Islamic banking because it aligns with their faith-based values, such as avoiding *riba* (interest) and ensuring ethical financial practices. When an Islamic bank retains these principles, customers feel that their financial choices are not only beneficial but also spiritually meaningful, leading to greater satisfaction (Abror et al., 2022)**.** At the same time, religiosity creates a deeper sense of trust and commitment, making customers more likely to stick with their banks (Monoarfa et al., 2024), even when faced with challenges such as cyberattacks. Instead of immediately switching to another bank, religious customers may believe that Islamic banks operate with integrity and take responsibility to address security issues. Research has shown that people with strong religious beliefs tend to remain loyal to brands or institutions that reflect their values (Suhartanto et al., 2020), and this also applies to banking. In the case of cybersecurity concerns, religiosity can help ease fears and maintain trust, reducing the likelihood of customers leaving even after a breach. Based on these arguments, we hypothesized that:

H_4: Religiosity has a positive effect on customer satisfaction

H_5: Religiosity has a positive effect on customer loyalty.

Customer satisfaction on customer loyalty

Satisfaction is crucial for maintaining long-term customer loyalty (Anderson & Sullivan, 1993). Satisfaction arises from comparing expectations with actual experiences (Geyskens & Steenkamp, 2000). Highly satisfied customers tend to share positive information, whereas dissatisfied customers are more likely to share negative experiences (Aisyah, 2018). Ahmed et al. (2021) noted that maintaining trust and customer loyalty is an ongoing challenge in Islamic banks.

Research has shown that satisfaction positively affects loyalty. Sulaiman et al. (2021) find that loyalty is strongly influenced by customer satisfaction in the context of non-interest banks in Nigeria. Alnaser et al. (2018) discovered that satisfaction significantly affected customer loyalty in Malaysian Islamic banks. Based on these arguments, we hypothesize the following.

H_6: Customer satisfaction has a positive effect on customer loyalty.

Research Methods

Sample selection

Purposive sampling was used to select respondents based on several criteria: (a) Indonesian nationality, (b) Muslim, and (c) users of BSI during the cyberattack period. These criteria were chosen to align with this study's objective of investigating the determinants of customer loyalty among BSI users. The focus on Muslim respondents is due to the fact that the majority of BSI's customers are Muslim. In addition, selecting respondents who used BSI during the cyberattack period allowed us to assess both the severity and vulnerability experienced during this time. The questionnaire was designed using Google Forms and distributed via popular social media platforms such as WhatsApp and Instagram, which are widely used by potential respondents (Sunarmo & Majid, 2024). Following Hair et al. (2019), the minimum sample size should be five times the number of indicators. With 27 indicators in this study, the minimum sample size is 135. Our final sample consisted of 244 respondents, the majority of whom were female (63.25%), Gen Z (74.18%), and had at least a Bachelor's degree (67.26%).

Table 1. Respondents demographic

Constructs	Frequency	Percentage
Gender		
Male	89	36,75%
Female	155	63,25%
Age		
17-27	181	74,18%
28-43	57	23,36%
44-59	4	1,65%
>60	2	0,81%
Educational Level		
High School	7	2,87%
Bachelor	165	67.62%
Master	67	27,45%
Doctoral	5	2,06%

Source: Data processed by Authors

Variable measurement

This was a quantitative study using a survey method. The questionnaire uses five scales ranging from strongly disagree to strongly agree. Measurements for each variable were adopted and modified from several previous studies. Perceived severity and vulnerability were adopted from Chen and Jai (2019). Religiosity is adopted from Rahim et al. (2016) and Utomo et al. (2020). Perceived risk and customer satisfaction were adopted from Riefel (2023) and Chakraboty et al., (2016). Customer loyalty adopted from (Zeithaml, 1988).

Data analysis

This study used the Partial Least Square - Structural Equation Modelling (PLS-SEM) method and used SmartPLS 3.0 software. We follow Koeswandana and Sugino (2023) to follow the statistical steps of the PLS-SEM method. We chose PLS-SEM instead of another method such as covariance-bt Based – Structural Equation Modelling (CB-SEM), because we think PLS-SEM is more suitable for predicting the determinants of customer loyalty and satisfaction. According to Dash and Paul, (2021), CB-SEM is more suitable for confirming or testing this theory. In this study, we have an objective to predict what factors influence loyalty and satisfaction. According to Hair et al. (2017), SEM requires both measurement and structural models. The measurement model tests validity and reliability, while the structural model tests the proposed hypothesis. Moreover, this study also uses the PLSpredict approach, with a focus on customer loyalty as the main target. This study also conducted a robustness test using nonlinearity criteria based on Sarstedt et al. (2020).

Results

Measurement model

The first step of the measurement model was to test the outer loading of each instrument. According to Hair et al. (2019), the value of the outer loading is perfect if greater than 0,7. Even though the perfect value is greater than 0,7 Hair et al. (2019) still allow to use of the outer loadings if the value is between 0,5 and 0,7. Based on this theory, we eliminated only the indicators that had outer loading values lower than 0,5. The items to be dropped are PV1, PV2, PV3, and PV7. Table 2 presents the results of both the validity and reliability tests after dropping the items that did d not meet the criteria. Table 2 also presents the values of Cronbach's alpha (CA), composite reliability (CR), and Average Variance Extracted (AVE). The minimum value needed to be fulfilled for CA and CR is 0,7 while for AVE is 0,5 (Hair et al., 2019). Our results show that all the variables fulfill these requirements.

Table 2. Measurement Model

Indicator	Loadings Factor
Perceived Severity	CA:0,764 CR:0,857 AVE:0,670 rho_A: 1,036
PS1: I believe cyberattack is a serious problem that will invade my privacy	0,702
PS2: It is a serious issue if my personal information is compromised by a cyberattack	0,794
PS3: I believe that identity theft caused by cyberattacks is a serious problem	0,941
Perceived Vulnerability	CA:0,748 CR:0,858 AVE:0,676 rho_A: 0,821
PV4: Cyberattack news makes me feel exposed	0,602
PV5: Cyberattack news makes me feel threatened	0,916
PV6: Cyberattack news makes me feel vulnerable	0,910
Perceived Risk	CA:0,842 CR:0,904 AVE:0,760 rho_A: 0,949
PR1: If a service company where I store my data faced a cyber incident, it would be a serious problem for me	0,537
PR2: Customers' information stored by BSI is not safe	0,707
PR3: Customers are vulnerable if BSI faces incidents of cyberattacks	0,940
Religiosity	CA:0,884 CR:0,900 AVE:0,512 rho_A: 0.918
R1: I believe Allah who determines destiny	0,517
R2: I believe and feel comfortable with my religion	0,701
R3: I always fulfill my obligation to Allah	0,641
R4: I always avoided haram earnings	0,650
R5: I understand about the halal concept	0,634
R6: I allocated my time to religious activity	0,820
R7: Religion influences all of my decision	0,733
R8: I spent my time to study about my religion	0,739
R9: Religion is very important because it can answer all of life's problems.	0,738
R10: I contribute financially to my religion.	0,701
Customer Satisfaction	CA:0,914 CR:0,946 AVE:0,853 rho_A: 0,917
CS1: I will recommend my friend and my colleagues to use BSI	0,921
CS2: I will recommend BSI because it is a safe place to save our data	0,916
CS3: Based on my experience, I will recommend BSI	0,935
Customer Loyalty	CA:0,962 CR:0,971 AVE: 0,869 rho_A: 0,965
CL1: After the cyberattack occurs, I will say positive things about BSI	0,898
CL2: After a cyberattack occurs, I will recommend BSI to the other	0,963
CL3: After a cyberattack occurs, I will encourage my friends and colleagues to use BSI	0.949
CL4: After a cyberattack occurs, I consider BSI as the first option to save money	0,929
CL5: After a cyberattack occurs, I will keep using BSI in the future.	0,922

Source: Data processed by Authors

After testing and eliminating the outer loading that did not meet the criteria, the next step was to conduct discriminant validity, such as the Fornell-Larcker and Heterotrait-Monotrait (HTMT). Fornell Larcker must show that the value of correlation for each variable must be greater than that for other variables (Fornell & Larcker, 1981). While the minimum value of HTMT is 0,9 (Henseler et al., 2015). Our study fulfills all these requirements, as shown in Tables 3 and 4.

Table 3. Fornell Larcker

Variables	Loyalty	Religiosity	Risk	Satisfaction	Severity	Vulnerability
Loyalty	0,932					
Religiosity	0,493	0,691				
Risk	-0,090	0,108	0,747			
Satisfaction	0,700	0,544	-0,090	0,924		
Severity	-0,181	-0,462	0,003	-0,267	0,818	
Vulnerability	-0,202	-0,352	0,037	-0,289	0,519	0,822

Source: Data processed by Authors

The Fornell-Larcker table shows that the correlation of each variable is greater than the correlation between the other variables. For example, the value of the correlation between loyalty and loyalty is 0,932 and greater than any other variable's correlation such as religiosity, risk, satisfaction, severity, and vulnerability. This means that there was no multicollinearity problem in this model.

Table 4. HTMT

Variables	Loyalty	Religiosity	Risk	Satisfaction	Severity	Vulnerability
Loyalty						
Religiosity	0,456					
Risk	0,103	0,206				
Satisfaction	0,743	0,541	0,084			
Severity	0,178	0,558	0,170	0,277		
Vulnerability	0,229	0,406	0,110	0,342	0,649	

Source: Data processed by Authors

According to Henseler et al. (2015), the maximum value of HTMT is 0,9. Table 4 shows that all the HTMT values meet the criteria, which is lower than 0,9. This result indicated that the model had discriminant validity.

Structural model

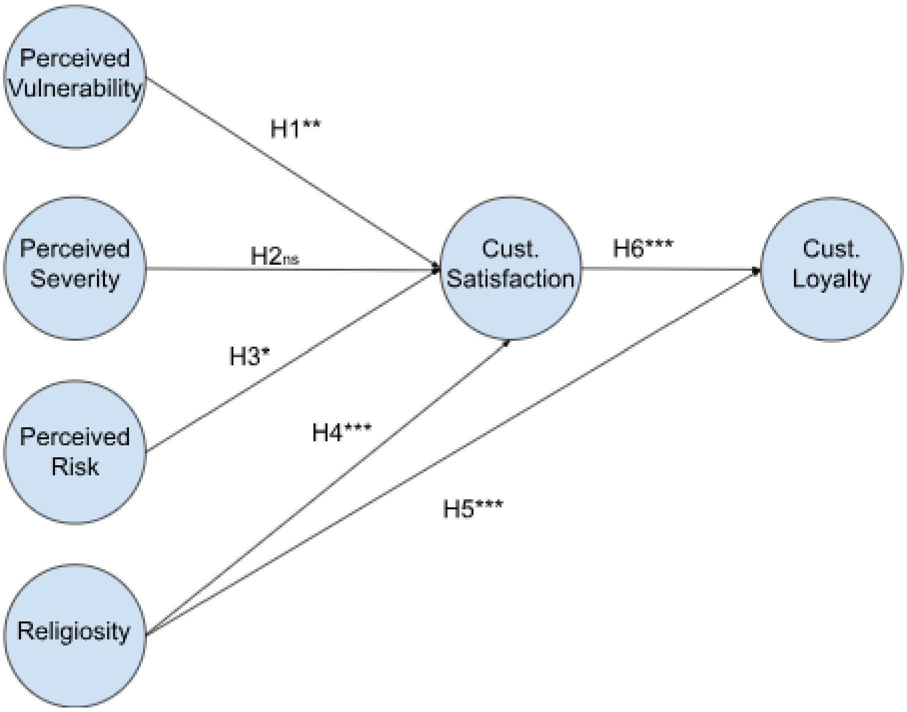

Figure 1. Hypothesis result
Source: Authors (2025)

The result shows that the value of R^2 for customer loyalty is 0,504 and that R^2 for customer satisfaction is 0,317. This means that 50,4% of customer loyalty is explained by customer satisfaction and religiosity, and the other 49,6% is explained by other variables. In addition, for customer satisfaction, 31,7% was explained by perceived vulnerability, perceived severity, and perceived risk, and the other 68,3% was explained by other variables. Hair et al. (2017) stated that if $R^2 >0{,}5$ it means the study is substantial, whereas if $R^2 >0{,}25$ is moderate. Figure 1 presents the results of the hypothesis testing, indicating that H1, H3, H4, H5, and H6 are supported. H4, H5, and H6 are positively significant at 0,01 level. H1 and H3 were negatively significant at 0,05 and 0,1 levels. H2 is unsupported because its p-value is greater > 0,1. For a better explanation, we provide details of the hypothesis testing in Table 7.

Table 5. Effect size and multicollinearity

Construct Relationship	f^2	VIF
SAT → CL	0.540	1,420
PV → SAT	0,014	1,405
PS → SAT	0,002	1,559
PR → SAT	0,030	1,019
R → SAT	0,326	1,322
R → CL	0,036	1,420

Source: Data processed by authors

Cohen's f^2 was used to identify the influence of each variable on the model. According to Hair et al. (2017), Cohen's f^2 is categorized as large if it is 0,35 or higher, medium if it is 0,15, and low if the value is 0,02. Table 5 shows that f^2 is between 0,002 – 0,540. According to Hair et al. (2017), the threshold for the variance inflation factor (VIF) was lower than 5. Our results show that VIF fulfills the VIF threshold.

Table 6. PLS predict output

Construct	PLS-SEM			LM		
	RMSE	MAE	Q^2	RMSE	MAE	Q^2
CL1	1,004	0,857	0,139	0,923	0,772	0,273
CL2	1,036	0,864	0,178	0,936	0,785	0,328
CL3	0,974	0,829	0,232	0,922	0,773	0,312
CL4	1,010	0,837	0,236	0,931	0,788	0,350
CL5	0,934	0,765	0,208	0,934	0,766	0,208

Source: Data processed by authors

We also performed predictive relevance using Stone–Geisser's Q^2. It can be used as a reference to predict the relevance between the independent and dependent variables (Hair et al., 2017). The minimum threshold is 0. In this study, the results of Q^2 fulfilled the threshold (> 0). This indicates that our model has predictive relevance and that the observed values have been properly reconstructed. Table 6 presents the results.

Table 7. Hypothesis testing

Hypothesis	Original sample	P-Value	Decision
H1: PV – SAT	-0,116	0,033**	Supported
H2: PS – SAT	0,042	0,301	Not supported
H3: PR – SAT	-0,144	0,079*	Supported
H4: R + SAT	0,583	0,000***	Supported
H5: R + LOY	0,518	0,000***	Supported
H6: SAT + LOY	0,614	0,000***	Supported

Source: Data processed by authors

Robustness test

We also conducted a robustness test to ensure that the model is robust. For the robustness test, we use the nonlinearity criteria recommended by Sarstedt et al. (2020). According to Hair et al. (2019), when the relationship between two constructs is nonlinear, the size effect depends not only on the exogenous construct but also on its value. Moreover, this study added quadratic effects to the model. The result of the quadratic effects can be seen in Table 8, which indicates that there is no significant relationship between those variables in terms of the robustness test. This insignificant result can be explained by evidence of the robustness of the linear effects (Sarstedt et al., 2020).

Table 8. Robustness test

Hypothesis	P-Value
H1: PV – SAT	0,073
H2: PS – SAT	0,541
H3: PR – SAT	0,224
H4: R + SAT	0,000
H5: R + LOY	0,000
H6: SAT + LOY	0,000
Quadratic Effect 1 (H1)	0,108
Quadratic Effect 2 (H2)	0,300
Quadratic Effect 3 (H3)	0,555
Quadratic Effect 4 (H4)	0,106
Quadratic Effect 5 (H5)	0,147
Quadratic Effect 6 (H6)	0,150

Source: Data processed by Authors

Discussion

The results indicate that perceived severity does not significantly influence customer satisfaction after cyberattacks. This suggests that Islamic bank customers assess security incidents differently. They may prioritize other factors, such as trust in the institution, ethical responsibility, and service recovery efforts. Given that an Islamic bank is built on the principle of transparency and responsibility, customers may expect banks to take corrective action rather than immediately lose trust by being dissatisfied. Future studies could explore additional factors to gain a better understanding of how Islamic banks' customers respond to cyberattacks.

Our unsupported hypothesis was based on the premise that the information users provide to banks is critical; therefore, a cyberattack on these banks would be perceived as more severe. However, in this study, perceived severity was not found to have a significant relationship with customer satisfaction, suggesting a low level of technology security awareness among the respondents. We believe that in Indonesia, awareness of technological security remains relatively low. This argument is supported by a study conducted by Amin et al. (2021), who found that technology awareness and privacy concerns are still low in Indonesian society. Insufficient knowledge of technology leads to underestimation of the potential impact of cyberattacks (Aivazpour, 2018). Several factors may contribute to this lack of awareness, including limited exposure to serious cyber threats and a cultural tendency to prioritize convenience over security (Ernita et al., 2022).

Our results indicate that perceived vulnerability and perceived risk have a negative effect on customer satisfaction following cyberattacks on BSI. This suggests that a higher level of perceived vulnerability and risk leads to a lower level of customer satisfaction after a cyberattack. When customers feel vulnerable to cyberattacks and believe that they have little control over their personal information, they can create negative emotions and stress (Baker et al., 2005), leading to dissatisfaction. Similarly, when customers perceive technology to be risky, their satisfaction decreases. This finding is consistent with Protection Motivation Theory (PMT), which posits that threat appraisal, such as perceived vulnerability, is used to assess maladaptive behavior. Maladaptive behaviors such as cyberattacks violate social norms (Oostdam et al., 2019). Cyberattacks can be categorized as maladaptive because they violate social norms. Therefore, our results support the PMT hypothesis that perceived vulnerability is a key factor in the evaluation of cyberattacks.

Our study also revealed that customer satisfaction positively influences customer loyalty after BSI cyberattacks, indicating that greater customer satisfaction results in greater customer loyalty. Satisfaction occurs when a customer's actual experience meets or exceeds expectations (Geyskens and Steenkamp 2000). When banks provide reliable services, quick responses, and strong security, customers feel satisfied and are more likely to remain loyal while sharing positive experiences with others. Word of mouth can enhance a bank's reputation and attract new customers (Aisyah, 2018). This finding aligns with those of previous research (Alnaser et al., 2018; Amin, 2016; Sulaiman et al., 2021). For instance, Sulaiman et al. (2021) demonstrated that in the context of non-interest banks in Nigeria, customer loyalty is strongly affected by satisfaction. Alnaser et al. (2018) found that satisfaction positively influences customer loyalty in Malaysian Islamic banks, whereas Amin (2016) showed that e-customer satisfaction significantly affects customer loyalty.

Religiosity also positively affects customer satisfaction and loyalty after BSI. This result is consistent with that of several previous studies (Setiawan et al., 2019; Soma et al., 2017; Yusfiarto et al., 2022). A higher level of religiosity leads to higher levels of customer satisfaction and loyalty even after a cyberattack on BSI. This finding is logical, as customers with high religiosity tend to have a more positive and stable outlook on life, value tolerance, and forgiveness and are committed to Islamic values (Dinh et al., 2022). These qualities help them overcome the negative impacts of cyberattacks and remain loyal to BSI. Furthermore, as BSI is the largest Islamic bank in Indonesia, people with high religiosity are more likely to remain loyal to BSI due to the lack of alternative Islamic banking options in the country.

This study contributes to the literature by expanding our understanding of how cyberattacks affect customer satisfaction and loyalty in Islamic banking. Previous studies have primarily focused on stock performance (Nisa & Cahyono, 2024) and IT risk mitigation strategies (Fitriani et al., 2023), which integrate Protection Motivation Theory (PMT) with religiosity to explore customer perceptions after a cyberattack. By incorporating perceived severity, risk, and vulnerability, this study introduced a new framework for assessing customer trust and loyalty in the wake of cybersecurity breaches. Additionally, this research extends the application of PMT to the financial sector, particularly in the context of Islamic banking, where religiosity is anticipated to significantly influence customer reactions to security breaches.

For Islamic banking practitioners, this study highlights the urgent need to strengthen cybersecurity infrastructure through advanced technologies, such as Artificial Intelligence (AI), machine learning, and blockchain, to enhance data protection. Banks should also implement transparent crisis communication strategies to maintain customer trust after cyber incidents. These findings emphasize the importance of cybersecurity awareness programs for customers, as lower awareness can lead to greater vulnerabilities. Additionally, regulators should consider enhancing cybersecurity legislation to align with international standards, ensuring that Islamic banks are well protected against evolving cyber threats. By addressing these issues, Islamic banks such as Bank Syariah Indonesia (BSI) can improve customer satisfaction, strengthen loyalty, and sustain long-term trust in their financial services.

Conclusion

This study investigated the impact of cyberattacks on customer loyalty and satisfaction in Islamic banking, focusing on recent cyberattacks on Bank Syariah, Indonesia (BSI). The findings indicate that perceived vulnerability and perceived risk negatively influence customer satisfaction, whereas religiosity has a positive impact on both customer satisfaction and loyalty. Interestingly, perceived severity did not significantly affect customer satisfaction after cyberattack. These results highlight the importance of religiosity in shaping customer responses to cybersecurity threats in Islamic banking, where trust (amanah) and ethical compliance (shariah compliance) play crucial roles in maintaining customer relationships. Customers who value Islamic financial principles tend to remain loyal as long as banks uphold their ethical values, integrity, and transparency. From a practical perspective, this study offers valuable insights for banks in Indonesia, particularly Islamic banks, to enhance customer loyalty by minimizing cybersecurity risks and reinforcing their commitments to ethical banking practices. These findings contribute to the literature on customer loyalty in the context of cyberattacks and support previous research by Yusfiarto et al. (2022), Rasoulian (2023), and Riefel (2023), while contradicting Greve et al. (2020) regarding the role of perceived severity. In conclusion, this study shows that maintaining security, transparency, and ethical responsibility is essential for Islamic banks to sustain customer trust and loyalty even in the face of cybersecurity threats.

Islamic Banking practitioners should focus on customer data security to enhance their satisfaction and loyalty. For regulators, to the best of our knowledge, Indonesian law about cybercrime is not as good as that of other developed countries such as the United States of America or several countries in the Middle East. Our study has some limitations. This result might not be generalizable to other countries, especially developed ones. According to Amin et al. (2021), technology security awareness in Indonesian society is still low. Meanwhile, Aviazpour (2018) stated that lower technology security awareness leads to lower severity levels during cyberattacks. With the rise of digital banking, examining the role of financial technology (fintech) in enhancing cybersecurity in Islamic banking is essential. Future studies could also analyze customers' perceptions of security measures and their willingness to adapt to stricter cybersecurity protocols. Furthermore, case studies on cybersecurity breaches in Islamic banking can offer deeper insights into vulnerabilities and preventive strategies.

Author contributions

Conceptualization: Noorfaiz Athallah Koeswandana, Mayang Yorindafitri Yulfiatmi
Data curation: Mayang Yorindafitri Yulfiatmi
Formal analysis: Noorfaiz Athallah Koeswandana, Mayang Yorindafitri Yulfiatmi
Investigation: Noorfaiz Athallah Koeswandana, Mayang Yorindafitri Yulfiatmi
Methodology: Noorfaiz Athallah Koeswandana
Project administration: Noorfaiz Athallah Koeswandana
Supervision: Noorfaiz Athallah Koeswandana
Validation: Mayang Yorindafitri Yulfiatmi
Visualization: Noorfaiz Athallah Koeswandana
Writing – original draft: Noorfaiz Athallah Koeswandana, Mayang Yorindafitri Yulfiatmi
Writing – review & editing: Noorfaiz Athallah Koeswandana

References

Abou-Youssef, M. M. H., Kortam, W., Abou-Aish, E., & El-Bassiouny, N. (2015). Effects of religiosity on consumer attitudes toward Islamic banking in Egypt. *International Journal of Bank Marketing, 33*(6), 786–807. https://doi.org/10.1108/IJBM-02-2015-0024

Abror, A., Patrisia, D., Engriani, Y., Idris, I., & Dastgir, S. (2022). Islamic bank trust: The roles of religiosity, perceived value and satisfaction. *Asia Pacific Journal of Marketing and Logistics, 34*(2), 368–384. https://doi.org/10.1108/APJML-10-2020-0715

Ahmed, R. R., Streimikiene, D., Channar, Z. A., Soomro, R. H., & Streimikis, J. (2021). E-banking customer satisfaction and loyalty: Evidence from serial mediation through modified E-S-QUAL model and second-order PLS-SEM. *Engineering Economics, 32*(5), 407–421. https://doi.org/10.5755/J01.EE.32.5.28997

Aisyah, M. (2018). Islamic bank service quality and its impact on Indonesian customers' satisfaction and loyalty. *Al-Iqtishad: Jurnal Ilmu Ekonomi Syariah, 10*(2), 367-388. https://doi.org/10.15408/aiq.v10i2.7135

Aivazpour, Z., Valecha, R., & Chakraborty, R. (2018). The impact of data breach severity on post-breach online shopping intention. *International Conference on Information Systems 2018 (ICIS 2018)*, 1–9.

https://web.archive.org/web/20210815032258id_/https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1218&context=icis2018

Al Batayneh, A. A., Qasaimeh, M., & Al-Qassas, R. S. (2021). A scoring system for information security governance framework using deep learning algorithms: A case study on the banking sector. *Journal of Data and Information Quality, 13*(2), Artikel 14. https://doi.org/10.1145/3418172

Alnaser, F. M. I., Ghani, M. A., & Rahi, S. (2018). Service quality in Islamic banks: The role of PAKSERV model, customer satisfaction and customer loyalty. *Accounting, 4*(2), 63–72. https://doi.org/10.5267/j.ac.2017.8.001

Amin, M. (2016). Internet banking service quality and its implication on e-customer satisfaction and e-customer loyalty. *International Journal of Bank Marketing, 34*(3), 280–306. https://doi.org/10.1108/IJBM-10-2014-0139

Amin, M., Tasmil, Herman, Bahrawi, Alam, N., Dhahir, D. F., & Hadiyat, Y. D. (2021). Security and privacy awareness of smartphone users in Indonesia. *Journal of Physics: Conference Series, 1882*(1), Artikel 012134. https://doi.org/10.1088/1742-6596/1882/1/012134

Anderson, E. W., & Sullivan, M. W. (1993). The antecedents and consequences of customer satisfaction for firms. *Marketing Science, 12*(2), 125–143. https://doi.org/10.1287/mksc.12.2.125

Bajwa, I. A., Ahmad, S., Mahmud, M., & Bajwa, F. A. (2023). The impact of cyberattacks awareness on customers' trust and commitment: An empirical evidence from the Pakistani banking sector. *Information and Computer Security, 31*(5), 635–654. https://doi.org/10.1108/ICS-11-2022-0179

Baker, S. M., Gentry, J. W., & Rittenburg, T. L. (2005). Building understanding of the domain of consumer vulnerability. *Journal of Macromarketing, 25*(2), 128–139. https://doi.org/10.1177/0276146705280622

Chakraborty, R., Lee, J., Bagchi-Sen, S., Upadhyaya, S., & Raghav Rao, H. (2016). Online shopping intention in the context of data breach in online retail stores: An examination of older and younger adults. *Decision Support Systems, 83*, 47–56. https://doi.org/10.1016/j.dss.2015.12.007

Chang, S. H., Chih, W. H., Liou, D. K., & Yang, Y. T. (2016). The mediation of cognitive attitude for online shopping. *Information Technology and People, 29*(3), 618–646. https://doi.org/10.1108/ITP-08-2014-0172

Chen, H. S., & Jai, T. M. (2021). Trust fall: Data breach perceptions from loyalty and non-loyalty customers. *Service Industries Journal, 41*(13-14), 947–963. https://doi.org/10.1080/02642069.2019.1603296

Choi, B. C. F., Kim, S. S., & Jiang, Z. (Jack). (2016). Influence of firm's recovery endeavors upon privacy breach on online customer behavior. *Journal of Management Information Systems, 33*(3), 904–933. https://doi.org/10.1080/07421222.2015.1138375

Cox, C. (2022, 1 November). *U.S. banks processed roughly $1.2 billion in ransomware payments in 2021, according to federal report*. CNBC. https://www.cnbc.com/2022/11/01/us-banks-process-roughly-1point2-billion-in-ransomware-payments-in-2021.html

Culnan, M. J., & Williams, C. C. (2009). How ethics can enhance organizational privacy: Lessons from the ChoicePoint and TJX data breaches. *MIS Quarterly, 33*(4), 673–687. https://doi.org/10.2307/20650322

Dang-Pham, D., & Pittayachawan, S. (2015). Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university: A protection motivation theory approach. *Computers and Security, 48*, 281–297. https://doi.org/10.1016/j.cose.2014.11.002

Dash, G., & Paul, J. (2021). CB-SEM vs PLS-SEM methods for research in social sciences and technology forecasting. *Technological Forecasting and Social Change, 173*, Article 121092. https://doi.org/10.1016/j.techfore.2021.121092

Dinh, H. P., Van Nguyen, P., Trinh, T. V. A., & Nguyen, M. H. (2022). Roles of religiosity in enhancing life satisfaction, ethical judgements and consumer loyalty. *Cogent Business and Management, 9*(1), Article 2010482. https://doi.org/10.1080/23311975.2021.2010482

Ernita, H., Ruldeviyani, Y., Nurul Maftuhah, D., & Mulyadi, R. (2022). Strategy to improve employee security awareness at information technology directorate bank XYZ. *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi), 6*(4), 577–584. https://doi.org/10.29207/resti.v6i4.4170

Featherman, M. S., & Pavlou, P. A. (2003). Predicting E-services adoption: A perceived risk facets perspective. *International Journal of Human-Computer Studies, 59*(4), 451–474. https://doi.org/10.1016/S1071-5819(03)00111-3

Fitriani, R., Subagiyo, R., & Asiyah, B. N. (2023). Mitigating IT risk of bank syariah Indonesia: A study of cyber attack on May 8, 2023. *Al-Amwal: Jurnal Ekonomi dan Perbankan Syari'ah, 15*(1), 86–99. https://doi.org/10.24235/amwal.v15i1.14124

Floyd, D. L., Prentince-Dunn, S., & Rogers, R. W. (2000). A meta-analysis of research on protection motivation theory. *Journal of Applied Social Psychology, 30*(2), 407–429. https://doi.org/10.1111/j.1559-1816.2000.tb02323.x

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research, 18*(1), 39–50. https://doi.org/10.2307/3151312

Geyskens, I., & Steenkamp, J. B. E. M. (2000). Economic and social satisfaction: Measurement and relevance to marketing channel relationships. *Journal of Retailing, 76*(1), 11–32. https://doi.org/10.1016/S0022-4359(99)00021-4

Greve, M., Masuch, K., & Trang, S. (2020). The more, the better? compensation and remorse as data breach recovery actions - An experimental scenario-based investigation. *Proceedings of the 15th International Conference on Business Information Systems 2020.* https://doi.org/10.30844/wi_2020_l2

Hair, J. F., Hult, G. T. M., Ringle, C., & Sarstedt, M. (2017). *A primer on partial least squares structural equation modeling (PLS-SEM)* (2nd ed.). Sage Publications. https://eli.johogo.com/Class/CCU/SEM/_A%20Primer%20on%20Partial%20Least%20Squares%20Structural%20Equation%20Modeling_Hair.pdf

Hair Jr, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2019). *Multivariat data analysis* (8th ed.). Annabel Ainscow. Cengage learning EMEA. https://eli.johogo.com/Class/CCU/SEM/_Multivariate%20Data%20Analysis_Hair.pdf

Hanafizadeh, P., & Khedmatgozar, H. R. (2012). The mediating role of the dimensions of the perceived risk in the effect of customers' awareness on the adoption of internet banking in Iran. *Electronic Commerce Research, 12*(2), 151–175. https://doi.org/10.1007/s10660-012-9090-z

Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science, 43*(1), 115–135. https://doi.org/10.1007/s11747-014-0403-8

Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems, 47*(2), 154–165. https://doi.org/10.1016/j.dss.2009.02.005

Hill, R. P., & Sharma, E. (2020). Consumer vulnerability. *Journal of Consumer Psychology, 30*(3), 551–570. https://doi.org/10.1002/jcpy.1161

Jamil, H., Zia, T., Nayeem, T., Whitty, M. T., & D'Alessandro, S. (2024). Human-centric cyber security: Applying protection motivation theory to analyse micro business owners' security behaviours. *Information and Computer Security, 33*(1), 49–76. https://doi.org/10.1108/ICS-10-2023-0176

Janakiraman, R., Lim, J. H., & Rishika, R. (2018). The effect of a data breach announcement on customer behavior: Evidence from a multichannel retailer. *Journal of Marketing, 82*(2), 85–105. https://doi.org/10.1509/jm.16.0124

Khedmatgozar, H. R., & Shahnazi, A. (2018). The role of dimensions of perceived risk in adoption of corporate internet banking by customers in Iran. *Electronic Commerce Research, 18*(2), 389–412. https://doi.org/10.1007/s10660-017-9253-z

Kiran, U., Khan, N. F., Murtaza, H., Farooq, A., & Pirkkalainen, H. (2025). Explanatory and predictive modeling of cybersecurity behaviors using protection motivation theory. *Computers and Security, 149*, Artikel 104204. https://doi.org/10.1016/j.cose.2024.104204

Kirmani, M. D., Haque, M. A., Sadiq, M. A., & Hasan, F. (2022). Cashless preferences during the Covid-19 pandemic: Investigating user intentions to continue UPI-based payment systems in India. *Journal of Science and Technology Policy Management*. https://doi.org/10.1108/JSTPM-08-2021-0127

Koeswandana, N. A., & Sugino, F. A. (2023). Intention to use cryptocurrency: Social and religious perspective. *Jurnal Ekonomi & Keuangan Islam, 9*(1), 91–103. https://doi.org/10.20885/jeki.vol9.iss1.art7

Kost, E. (2023, 27 April). *10 Biggest data breach*. UpGuard. https://www.upguard.com/blog/biggest-data-breaches-financial-services

Malhotra, A., & Malhotra, C. (2011). Evaluating customer information breaches as service failures: An event study approach. *Journal of Service Research, 14*(1), 44–59. https://doi.org/10.1177/1094670510383409

Maurer, T., & Nelson, A. (2021). The global cyber threat. *Finance & Development, 58*(1), 24–27. https://www.imf.org/external/pubs/ft/fandd/2021/03/pdf/global-cyber-threat-to-financial-systems-maurer.pdf

Monoarfa, H., Al Adawiyah, R. A., Prananta, W., Sadat, A. M., & Vakhroh, D. A. (2024). Switching intention of conventional bank customers to Sharia bank based on push-pull-mooring theory. *Journal of Islamic Marketing, 15*(8), 2104–2121. https://doi.org/10.1108/JIMA-08-2022-0220

Mukhopadhyay, A., & Jain, S. (2024). A framework for cyber-risk insurance against ransomware: A mixed-method approach. *International Journal of Information Management, 74*, Article 102724. https://doi.org/10.1016/j.ijinfomgt.2023.102724

Mulia, D., Usman, H., & Parwanto, N. B. (2020). The role of customer intimacy in increasing Islamic bank customer loyalty in using e-banking and m-banking. *Journal of Islamic Marketing, 12*(6), 1097–1123. https://doi.org/10.1108/JIMA-09-2019-0190

Nisa, Z. F., & Cahyono, Y. T. (2024). The effect of cyber attacks on stock performance bank syariah Indonesia. *ICBE, 2*, 359–368. https://journal.uii.ac.id/inCAF/article/view/32669/16210

Oostdam, R. J., Koerhuis, M. J. C., & Fukkink, R. G. (2019). Maladaptive behavior in relation to the basic psychological needs of students in secondary education. *European Journal of Psychology of Education, 34*(3), 601–619. https://doi.org/10.1007/s10212-018-0397-6

Pandagle, V. (2023, 20 Mei). *LockBit demands $20m for 1.5TB of data from Bank Syariah Indonesia cyber attack*. The Cyber Express. https://thecyberexpress.com/lockbit-bank-syariah-indonesia-cyber-attack/#google_vignette

Perera, S., Jin, X., Maurushat, A., & Opoku, D. G. J. (2022). Factors affecting reputational damage to organisations due to cyberattacks. *Informatics, 9*(1), Article 24. https://doi.org/10.3390/informatics9010024

Prentince-Dunn, S., & Rogers, R. W. (1986). Protection motivation theory and preventive health: Beyond the health belief model. *Health Education Research, 1*(3), 153–161. https://doi.org/10.1093/her/1.3.153

Qasaimeh, M., Halemah, N. A., Rawashdeh, R., Al-Qassas, R. S., & Qusef, A. (2022). Systematic review of e-commerce security issues and customer satisfaction impact. *Proceedings - 2022 International Conference on Engineering and MIS, ICEMIS 2022*, 1–8. https://doi.org/10.1109/ICEMIS56295.2022.9914393

Rahim, S. H. A., Rashid, R. A., & Hamed, A. B. (2016). Islamic financial literacy and its determinants among university students: An exploratory factor analysis. *International Journal of Economics and Financial Issues, 6*(7Special Issue), 32–35. https://www.econjournals.com/index.php/ijefi/article/view/3572

Rasoulian, S., Grégoire, Y., Legoux, R., & Sénécal, S. (2017). Service crisis recovery and firm performance: Insights from information breach announcements. *Journal of the Academy of Marketing Science, 45*(6), 789–806. https://doi.org/10.1007/s11747-017-0543-8

Rasoulian, S., Grégoire, Y., Legoux, R., & Sénécal, S. (2023). The Effects of Service Crises and Recovery Resources on Market Reactions: An Event Study Analysis on Data Breach Announcements. *Journal of Service Research, 26*(1), 44–63. https://doi.org/10.1177/10946705211036944

Rewterz. (2018, 20 Oktober). *BankIslami hit by Cyber Attack, $6 Million Stolen.* https://www.rewterz.com/articles/bankislami-hit-by-cyber-attack-6-million-stolen

Riefel, M. T. (2022). *A quantitative study on the impact of data breaches on customer satisfaction* (Master's thesis). Purdue University

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology, 91*(1), 93–114. https://doi.org/10.1080/00223980.1975.9915803

Rohman, P. S., Fianto, B. A., Ali Shah, S. A., Kayani, U. N., Suprayogi, N., & Supriani, I. (2021). A review on literature of Islamic microfinance from 2010-2020: Lesson for practitioners and future directions. *Heliyon, 7*(12), Article e08549. https://doi.org/10.1016/j.heliyon.2021.e08549

Rosati, P., Deeney, P., Cummins, M., van der Werff, L., & Lynn, T. (2019). Social media and stock price reaction to data breach announcements: Evidence from US listed companies. *Research in International Business and Finance, 47*, 458–469. https://doi.org/10.1016/j.ribaf.2018.09.007

Sarstedt, M., Ringle, C. M., Cheah, J. H., Ting, H., Moisescu, O. I., & Radomir, L. (2020). Structural model robustness checks in PLS-SEM. *Tourism Economics, 26*(4), 531–554. https://doi.org/10.1177/1354816618823921

Sebayang, T. E., Hakim, D. B., Bakhtiar, T., & Indrawan, D. (2024). The investigation of preference attributes of Indonesian mobile banking users to develop a strategy for mobile banking adoption. *Journal of Risk and Financial Management, 17*(3), Artikel 109. https://doi.org/10.3390/jrfm17030109

Setiawan, F., Idris, I., & Abror, A. (2019). The relationship between religiosity, service quality, customer satisfaction and customer loyalty. *Advances in Economics, Business and Management Research, 64*, 517–525. https://doi.org/10.2991/piceeba2-18.2019.31

Soma, A. M., Primiana, I., Wiryono, S. K., & Febrian, E. (2017). Religiosity and Islamic banking product decision: Survey on employees of PT Telekomunikasi Indonesia. *Etikonomi, 16*(1), 25–42. https://doi.org/10.15408/etk.v16i1.4379

Souiden, N., & Rani, M. (2015). Consumer attitudes and purchase intentions toward Islamic banks: The influence of religiosity. *International Journal of Bank Marketing, 33*(2), 143–161. https://doi.org/10.1108/IJBM-10-2013-0115

Suhartanto, D., Marwansyah, M., Muflih, M., Najib, M. F., & Faturohman, I. (2020). Loyalty formation toward halal food: Integrating the quality–loyalty model and the religiosity–loyalty model. *British Food Journal, 122*(1), 48–59. https://doi.org/10.1108/BFJ-03-2019-0188

Sulaiman, S. M., Muhammad, M. A., Muhammad, A. D., & Sabiu, T. T. (2021). Mediating role of customer satisfaction between service quality and customer loyalty with non-interest bank in Nigeria. *International Journal of Islamic Economics and Finance (IJIEF), 4*(1), 1–30. https://doi.org/10.18196/ijief.v4i1.10424

Sunarmo, S., & Majid, R. (2024). The role of knowledge and trust in explaining intention of performing waqf in agricultural sector. *International Journal of Islamic Economics and Finance (IJIEF), 7*(1), 411–432. https://doi.org/10.18196/ijief.v7i1.17003

Sutarso, Y. (2022). The role of Islamic religiosity on the relationship between risk, trust, and intention to use digital payments during the Covid-19 Pandemic. *International Journal of Islamic Economics and Finance (IJIEF), 5*(2), 177–200. https://doi.org/10.18196/ijief.v5i2.13990

Utomo, S. B., Sekaryuni, R., Widarjono, A., Tohirin, A., & Sudarsono, H. (2020). Promoting Islamic financial ecosystem to improve halal industry performance in Indonesia: a demand and supply analysis. *Journal of Islamic Marketing, 12*(5), 992–1011. https://doi.org/10.1108/JIMA-12-2019-0259

Wijaya, I. F., Hakim, A. R., Saputro, N., & Mulyadi, M. (2020). Religiosity level and saving decisions in Baitul Maal wat Tamwil: the case of Indonesia. *Journal of Islamic Marketing, 11*(6), 1465–1483. https://doi.org/10.1108/JIMA-09-2018-0160

Yazbeck, F. (2019, 13 November). *Cyber security on Islamic banking*. Temenos. https://www.temenos.com/news/2019/11/13/cyber-security-islamic-banking/

Yusfiarto, R., Nugraha, S. S., Pambudi, D. S., & Pambekti, G. T. (2022). Islamic banking and loyalty: service quality, intimacy or religious driven? *Studies in Business and Economics, 17*(2), 300–318. https://doi.org/10.2478/sbe-2022-0040

Zeithaml, V. A. (1988). Consumer perceptions of price, quality, and value: A means-end model and synthesis of evidence. *Journal of Marketing, 52*(3), 2–22. https://doi.org/10.2307/1251446

Zurkus, K. (2018, 14 Juni). *Bank of Chile suffers $10m loss*. Infosecurity Magazine. https://www.infosecurity-magazine.com/news/bank-of-chile-suffers-10m-loss/