Resiliensi
Jurnal Ekonomi dan Keuangan Syariah
Yayasan Paramarta Akademika Indonesia

Dampak Serangan Siber Terhadap Kepercayaan Nasabah dan Minat Beralih Bank (Switching Intention) Pada Bank Syariah Indonesia Pasca-Insiden 2023

ABSTRACT *- This study aims to analyze the impact of cyberattacks on customer trust and the intention to switch banks (switching intention) at Bank Syariah Indonesia following the 2023 ransomware incident. A descriptive qualitative approach utilizing a literature review method was employed. Research data were gathered from various scientific articles, national and international journals, and official documents concerning cybersecurity, customer trust, and customer switching behavior in Islamic banking. Data analysis was conducted through stages of data presentation, data reduction, and conclusion drawing. The findings indicate that the cyberattack increased perceived security risk and diminished consumer trust in Bank Syariah Indonesia's digital services. This decline in trust fostered a switching intention—a tendency among customers to consider moving to other banks perceived to have superior security systems. However, mass customer migration did not occur due to mitigating factors such as loyalty to Islamic banking principles, high switching costs, and customer attachment to the financial services they were already using. Therefore, strengthening digital resilience, enhancing information system security, and maintaining transparent crisis communication are strategic measures for preserving customer trust and ensuring the sustainability of the Islamic banking industry in the digital era..*

ABSTRAK -. Kajian ini bertujuan dalam menganalisis pengaruh serangan siber terhadap kepercayaan nasabah dan minat beralih bank (Switching Intention) pada Bank Syariah Indonesia pasca-insiden ransomeware tahun 2023. Kajian ini memakai pendekatan kualitatif deskriptif dengan metode studi pustaka (Library Research). Data penelitian didapati dari beberapa artikel ilmiah, jurnal nasional dan internasional, serta dokumen resmi yang kaitannya dengan keamanan siber, kepercayaan nasabah, dan perilaku perpindahan nasabah pada perbankan syariah. Analisis data dijalankan dalam tahapan penyajian data, reduksi data, serta penarikan kesimpulan. Hasil kajian menyebutkan yakni serangan siber meningkatkan persepsi Risiko keamanan (Perceived Security Risk) dan menurunkan Tingkat kepercayaan konsumen terhadap layanan digital Bank Syariah Indonesia. Penurunan kepercayaan tersebut mendorong munculnya Switching Intention, yaitu kecenderungan nasabah untuk mempertimbangkan perpindahan ke bank lain yang dianggap memiliki system keamanan yang lebih baik. Namun, perpindahan nasabah secara massal tidak terjadi karena adanya faktor penahan berupa loyalitas terhadap prinsip perbankan syariah, tingginya biaya perpindahan (Switching Costs), serta ketertarikan nasabah terhadap layanan keuangan yang telah digunakan. Oleh karena itu, penguatan ketahanan digital (Digital Resilience), peningkatan keamanan system informasi, dan transparansi komunikasi krisis menjadi langkah strategis dalam menjaga kepercayaan nasabah dan keberlanjutan industri perbankan syariah di era digital. .

Author
[1] **Salwa Kamila Yanissa**
[2] **Andini Duarti**,
[3] **Siti Nur Variza**,
[4] **Shella Rahmayani**
[1,2,3,4] Program Studi Manajemen, Fakultas Ekonomi, Universitas Al-Azhar Medan, Indonesia

*[1]***Corresponding email:**
salwakmila2609@gmail.com

Article History
Submitted: 14 Juli 2026
Revised: 20 Juli 2026
Accepted: 23 Juli 2026
Published: 23 Juli 2026

Keywords
Serangan Siber;
Kepercayaan Nasabah;
Beralih Bank;
Switching Intention;
Bank Syariah Indonesia.

PENDAHULUAN

Perkembangan teknologi informasi serta komunikasi telah mendesak transformasi digital pada sektor perbankan. Perbankan digital memberikan berbagai kemudahan kepada masyarakat melalui layanan Mobile Banking, Internet Banking dan transaksi elektronik yang biasanya diakses dimana saja serta kapan saja. Digitalisasi tersebut meningkatkan efesiensi operasional dan kualitas pelayanan kepada nasabah. Namun, dibalik berbagai manfaat tersebut, perkembangan teknologi juga menaikkan resiko terwujudnya kejahatan siber (cybercrime) yang mengancam keamanan data dan stabilitas operasional perbankan

Sektor perbankan termasuk salah satu sektor yang rentan terhadap serangan siber karena menyimpan data pribadi dan informasi keuangan nasabah dalam jumlah besar. Berbagai model serangan siber mencakup malware, phishing, ransomware, dan kebocoran data (data breach), akan mengakibatkan kerugian finansial ataupun nonfinansial bagi bank dan nasabah. Selain mengganggu operasional, serangan siber juga dapat menurunkan kepercayaan masyarakat terhadap sistem keamanan dan layanan digital yang disediakan oleh perbankan.

Pada tangal 8 Mei 2023, Bank Syariah Indonesia (BSI) terjadi kendala fasilitas digital yang diduga diakibatkan oleh kemunculan ransomware yang dijalankan oleh kelompok peretas LockBit 3.0. Gangguan ini mengakbiatkan layanan mobile banking, ATM, serta berbagai transaksi perbankan tidak mampu diakses dalam beberapa hari. Kondisi tersebut mengakibatkan kepanikan di kalangan nasabah dan memunculkan kekhawatiran terhadap keamanan data pribadi serta dana yang disimpan di bank. Di satu sisi, transformasi digital diharapkan mampu memperbaiki kualitas pelayanan perbankan, tetapi di sisi lain justru menaikkan kerawanan terhadap ancaman siber yang dapat menurunkan tingkat kepercayaan masyarakat. Kondisi inilah yang menunjukkan adanya gap fenomena, yaitu perbedaan antara harapan terciptanya layanan perbankan digital yang aman dengan kenyataan terjadinya gangguan layanan dan ancaman terhadap keamanan data konsumen.

Bank Syariah Indonesia termasuk bank syariah terluas di Indonesia yang memiliki peran strategis dalam perkembangan industri keuangan syariah nasional. Sebagai lembaga yang beroperasi berdasarkan prinsip syariah, kepercayaan (trust) menjadi modal utama dalam menjaga loyalitas nasabah. Penurunan kepercayaan akibat insiden keamanan digital berpotensi menimbulkan switching intention, yaitu keinginan nasabah untuk berpindah ke bank lain yang dianggap lebih aman dan mampu memberikan perlindungan data yang lebih baik. Apabila kondisi tersebut tidak segera diatasi, umumnya akan berdampak pada reputasi, loyalitas nasabah, dan keberlanjutan industri perbankan syariah di Indonesia.

Penelitian mengenai keamanan siber, kepercayaan nasabah, dan perilaku perpindahan nasabah pada sektor perbankan telah banyak dilakukan. Beberapa penelitian terdahulu lebih banyak membahas pengaruh keamanan layanan digital terhadap loyalitas nasabah, persepsi resiko terhadap kepercayaan nasabah, serta faktor-faktor yang memengaruhi switching intention pada perbankan secara umum. Namun, kajian yang secara khusus mengkaji hubungan antara serangan siber, kepercayaan nasabah, dan switching intention pada perbankan syariah, khususnya pasca-insiden serangan ransomware Bank Syariah Indonesia tahun 2023, umumnya relatif terbatas. Keadaan

tersebut memaparkan terdapat research gap, yaitu masih minimnya kajian mengintegrasikan ketiga variabel tersebut dalam konteks perbankan syariah di indonesia.

Berdasarkan fenomena dan kesenjangan penelitian tersebut, penelitian ini menjadi penting dilakukan karena memberikan gambaran mengenai dampak serangan siber terhadap tingkat kepercayaan nasabah dan minat beralih bank (switching intention) pada Bank Syariah Indonesia pasca-insiden tahun 2023. Selain memberikan kontribusi terhadap pengembangan literatur mengenai ketahanan digital (digital resilience) pada perbankan syariah, hasil penelitian ini juga diharapkan dapat menjadi bahan evaluasi bagi Bank Syariah Indonesia, regulator, dan industri perbankan dalam menyusun strategi penguatan keamanan siber serta menjaga kepercayaan dan loyalitas nasabah di era digital.

METODOLOGI

Kajian ini menjalankan pendekatan kualitatif dengan metode studi pustaka (library research). Studi pustaka dilakukan melalui penelusuran literatur yang relevan pada database Scopus, ScienceDirect, Google Scholar, Garuda serta Crosref memakai kata kunci cyberattack, customer trust, switching intention, digital resilience, islamic banking, dan Bank Syariah Indonesia. Literatur yang digunakan merupakan artikel ilmiah, prosiding, laporan resmi OJK, Bank Indonesia, BSSN, dan publikasi akademik yang diterbitkan periode 2018-2025.

Seleksi literatur dilakukan menggunakan kriteria inklusi yaitu: (1) membahas keamanan siber pada sektor perbankan; (2) mengkaji kepercayaan nasabah atau switching intention; (3) dipublikasikan pada jurnal ilmiah bereputasi; dan (4) memiliki keterkaitan dengan industri perbankan syariah. Literatur yang tidak relevan atau tidak mempunyai informasi empiris di eliminasi.

Analisis data dijalankan memakai model analisis interaktif Miles serta Huberman yang berisi penyajian data, reduksi data, serta penarikan kesimpulan sehingga didapati sintesis mengenai hubungan antara serengan siber, kepercayaan nasabah, dan switching intention, pada Bank Syariah Indonesia pasca-insiden tahun 2023

Teori utama yang melandasi kajian ini ialah Theory of Planned Behavior (TPB) yang disebutkan Ajzen (1991). Kajian ini menyebutkan yakni persepsi individu terhadap suatu kondisi akan memengaruhi niat berprilaku. Dalam konteks penelitian ini, serangan siber meningkatkan perceived security risk, menurunkan customer trust, dan akhirnya mendorong switching intention. Penelitian ini juga didukung teori Perceived Risk dan Customer Trust yang menjelaskan bahwa meningkatnya persepsi risiko keamanan akan menurunkan kepercayaan nasabah sehingga meningkatkan kecenderungan berpindah bank.

HASIL DAN PEMBAHASAN

Pengaruh Serangan Siber Terhadap Persepsi Risiko Keamanan Nasabah

Insiden *ransomware* yang melanda Bank Syariah Indonesia (BSI) di Mei 2023 meningkatkan persepsi risiko keamanan *(perceived security risk)* di kalangan nasabah. Gangguan pada layanan *mobile banking,* ATM, dan transaksi digital menyebabkan munculnya kekhawatiran mengenai keamanan data pribadi dan dana yang tersimpan di bank.

Menurut Rahman Prabawani dan Nugraha (2024), persepsi risiko yang tinggi akibat serangan siber berpengaruh negatif terhadap kenyamanan dan kepercayaan nasabah ketika menjalankan layanan perbankan digital. Makin tinggi risiko yang dijalani, maka makin rendah tingkat keyakinan nasabah terhadap keamanan layanan digital yang disediakan bank. Sejalan dengan penelitian tersebut, Rustan, Haanurat dan Nurlina (2026) menemukan bahwa ancaman *cybercrime* memiliki pengaruh signifikan terhadap persepsi keamanan serta tingkat kepercayaan konsumen pada Bank Syariah Indonesia.

Berdasarkan kajian tersebut, penulis berpendapat bahwa insiden BSI tahun 2023 tidak hanya menimbulkan masalah teknis berupa gangguan operasional, tetapi juga menimbulkan dampak psikologis bagi nasabah. Dalam industri perbankan, persepsi keamanan merupakan faktor utama yang memengaruhi keputusan nasabah dalam menggunakan layanan digital. Ketika nasabah merasa bahwa data dan dananya tidak terlindungi dengan baik, makan kepercayaan terhadap bank akan menurun dan berpotensi memengaruhi loyalitas mereka.

Dengan demikian, serangan siber pada BSI menyebutkan yakni keberhasilan transformasi digital tidak sekedar ditetapakan oleh inovasi teknologi, namun juga oleh kemampuan bank dalam menciptakan serta mempertahankan rasa aman di kalangan nasabah.

Pengaruh Serangan Siber Terhadap Kepercayaan Nasabah

Kepercayaan *(customer trust)* merupakan aset tidak berwujud yang sangat penting dalam industri perbankan, terutama pada perbankan syariah yang menjunjung tinggi prinsip amanah, transparansi, dan perlindungan terhadap nasabah.

Menurut Maulana dan Fitriana (2023), gangguan sistem dan dugaan peretasan pada Bank Syariah Indonesia menyebabkan sebagian nasabah mengalami penurunan kepercayaan terhadap layanan digital bank. Kondisi tersebut dipicu oleh ketidakpastian mengenai keamanan data pribadi dan terganggunya aktivitas transaksi keuangan

Kajian Rahman et al. (2024) juga menujukkan yakni persepsi risiko keamanan memiliki pengaruh negatif terhadap kepercayaan dan loyalitas nasabah pasca-serangan siber. Sementara itu, Koeswandana dan Yulfiatmi (2025) menyatakan bahwa kepercayaan merupakan faktor penting yang menentukan loyalitas konsumen ketika memakai layanan perbankan syariah.

Penulis menilai bahwa penurunan kepercayaan pasca-serangan siber merupakan konsekuensi yang wajar karena nasabah menempatkan keamanan sebagai kebutuhan utama dalam melakukan transaksi keuangan. Dalam konteks perbankan syariah, dampak tersebut dapat menjadi lebih serius karena kepercayaan tidak sekedar berkaitan dengan aspek teknis pelayanan, tetapi juga hubungannnya dengan nilai amanah yang menjadi dasar operasional bank syariah. Oleh karena itu, insiden BSI menjadi pelajaran penting bahwa ketahanan digital *(digital resilience)* harus dipandang sebagai bagian integral dari upaya menjaga kepercayaan dan reputasi perbankan syariah.

Pengaruh Penurunan Kepercayaan Terhadap Switching Intention

Switching intention merupakan kecenderungan nasabah untuk mempertimbangkan perpindahan ke bank lain akibat ketidakpastian terhadap layanan yang diterima. Menurut HS, Khasnah, dan Sutrisno (2022), kepercayaan pelanggan

berpengaruh signifikan terhadap *switching intention*. Semakin rendah tingkat kepercayaan nasabah, maka semakin tinggi kecenderungan mereka utuk mencari alternatif bank lain.

Penelitian Jannah dan Widodo (2018) juga menunjukkan bahwa persepsi negatif terhadap layanan perbankan dapat meningkatkan niat berpindah nasabah. Selain itu, Sari dan Aji (2022) menemukan bahwa ketidaknyamanan akibat perubahan layanan dan gangguan sistem mendorong nasabah untuk mempertimbangkan penggunaaan layanan perbankan lain.

Dalam jangka panjang, kondisi tersebut dapat berdampak pada penurunan daya saing dan reputasi perbankan syariah apabila tidak diantisipasi melalui penguatan keamanan siber dan peningkatan kualitas pelayanan.

Faktor Penahan (Mooring Factors) Terhadap Switching intention

Meskipun serangan siber meningkatkan *switching intention,* tidak seluruh nasabah melakukan perpindahan secara nyata. Menurut Koeswandana dan Yufiatmi (2025), religuisitas dan loyalitas terhadap prinsip perbankan syariah memiliki peran penting dalam mempertahankan hubungan antara nasabah dan Bank Syariah Indonesia meskipun terjadi serangan siber.

Selain itu, Hafiz, Muslihun, dan Sanurdi (2025) menyatakan bahwa keterikatan terhadap produk, jaringan layanan, dan sistem teknologi yang telah digunakan menjadi faktor yang menghambat perpindahan nasabah ke bank lain. Penelitian HS et al. (2022) juga menunjukkan bahwa loyalitas pelanggan dapat memediasi hubungan antara kepercayaan dan *switching intention.*

Penulis menilai bahwa faktor religuisitas dan loyalitas merupakan karakteristik unik pada perbankan syariah yang membedakannya dari perbankan konvensional. Banyak nasabah BSI tetap bertahan bukan semata-mata karena pertimbangan ekonomi, tetapi juga karena adanya keyakinan terhadap prinsip-prinsip syariah yang diterapkan. Hal tersebut menujukkan bahwa loyalitas nasabah pada perbankan syariah tidak sekedar diwujudkan melalui kualitas layanan, namun juga melalui kesesuaian nilai dan keyakinan dianut oleh nasabah.

Implikasi Terhadap Ketahanan Digital (digital Resilience)

Menurut Nadia, Susanty, Muda, Soemitra, dan Yusrizal (2025), ketahanan digital serta kualitas layanan mempunyai pengaruh signifikan terhadap *switching intention* nasabah. Semakin baik kemampuan bank dalam mengelola risiko digital dan memulihkan layanan pasca-insiden, maka makin rendah kecenderungan konsumen dalam beralih ke bank lain. Selain itu, Aisyah, Sesunan, dan Wicaksono (2025) menyatakan bahwa pemulihan kepercayaan pasca-serangan siber memerlukan penguatan sistem keamanan informasi, komunikasi krisis yang transparan, serta peningkatan kualitas layanan digital secara berkelanjutan.

Berdasarkan hasil penelitian tersebut, penulis berpendapat bahwa insiden BSI tahun 2023 menjadi momentum bagi indsutri perbankan syariah untuk melakukan evaluasi menyeluruh terhadap sistem keamanan siber yang dimiliki. Ketahanan digital tidak hanya berarti kemampuan mencegah serangan siber, tetapi juga kemapuan bank

dalam merespons, memulihkan, dan membangun kembali kepercayaan nasabah setelah isniden terjadi.

Dengan demikian, investasi keamanan siber, peningkatan kompetensi sumber daya manusia, penyusunan *disaster recovery plan,* serta edukasi keamanan digital kepada nasabah merupakan langkah strategis yang harus dilakukan oleh Bank Syariah Indonesia guna menjaga keberlanjutan layanan digital dan mempertahankan kepercayaan masyarakat terhadap industri perbankan syariah di zaman digital.

Tabel 1: Rangkuman Hasil Kajian Terdahulu

Peneliti	Tahun	Variabel yang Diteliti	Hasil Kajian
Maulana dan Fitriana	2023	Gangguan Sistem BSI dan Loyalitas Nasabah	Gangguan layanan BSI menurunkan tingkat kepercayaan dan loyalitas sebagaian nasabah.
Rahman, Prabawani, dan Nugraha	2024	*Perceived Risk, Customer Trust,* dan *Customer Loyality*	Persepsi resiko keamanan berpengaruh negatif terhadap kepercayaan dan loyalitas nasabah.
Koeswandana dan Yufiatmi	2025	Cyberattack, Religiosity, dan *Customer Loyality*	Religuisitas dan kepercayaan berperan dalam mempertahankan loyalitas nasabah pasca-serangan siber.
Nadia et al.	2025	*Digital Resilience* dan *Switching Intention*	Ketahanan digital yang baik dapat menurunkan kecenderungan nasabah untuk berpindah bank.
Rustan, Haanurat, dan Nurlina	2026	*Cybercrime* dan *Customer Trust*	Ancaman siber menurunkan persepsi keamanan dan tingkat kepercayaan nasabah.
HS, Khasanah,dan Sutrisno	2022	*Customer Trust, Customer Loyalty, Switching Intention*	Kepercayaan nasabah berpengaruh negative terhadap switching intention dan positif terhadap loyalitas nasabah.
Sari dan Aji	2022	*Switching Intention pada Nasabah BSI*	Ketidaknyamanan layanan dan perubahan system meningkatkan niat berpindah nasabah.

Sumber: Jurnal Penelitian Terdahulu

Transformasi digital telah menjadikan layanan perbankan semakin bergantung pada teknologi informasi, namun pada saat yang sama meningkatkan eksposur terhadap ancaman siber. Insiden gangguan layanan Bank Syariah Indonesia (BSI) pada Mei 2023, yang secara luas dikaitkan dengan serangan ransomware, menjadi salah satu peristiwa paling signifikan dalam sejarah perbankan syariah Indonesia. Gangguan tersebut mengakibatkan terhentinya berbagai layanan digital, termasuk mobile banking, ATM, dan transaksi elektronik, sehingga menimbulkan kekhawatiran mengenai keamanan sistem informasi dan perlindungan data nasabah.

Dalam perspektif pemasaran jasa keuangan, kepercayaan (customer trust) merupakan fondasi utama hubungan jangka panjang antara bank dan nasabah. Kepercayaan dibangun melalui persepsi bahwa bank mampu menjaga keamanan dana, kerahasiaan informasi, serta menyediakan layanan yang andal dan berkesinambungan. Ketika terjadi serangan siber yang mengganggu operasional bank, persepsi terhadap keamanan dan reliabilitas layanan akan menurun sehingga berpotensi mengurangi tingkat kepercayaan nasabah. Penelitian mengenai insiden BSI menunjukkan bahwa gangguan layanan dan dugaan kebocoran data berdampak nyata terhadap tingkat kepercayaan dan loyalitas nasabah, meskipun besarnya pengaruh berbeda pada setiap kelompok responden.

Penurunan kepercayaan tersebut selanjutnya dapat memunculkan switching intention, yaitu kecenderungan nasabah untuk memindahkan dana atau menggunakan layanan bank lain yang dianggap lebih aman dan lebih stabil. Dalam teori perilaku konsumen, switching intention dipengaruhi oleh persepsi risiko (perceived risk), kepuasan layanan, reputasi perusahaan, serta tingkat kepercayaan terhadap penyedia jasa. Pada sektor perbankan digital, persepsi risiko keamanan informasi menjadi salah satu determinan utama keputusan nasabah untuk tetap menggunakan atau meninggalkan suatu bank.

Pada kasus BSI pasca-insiden 2023, tidak seluruh nasabah langsung berpindah ke bank lain. Beberapa penelitian menunjukkan bahwa loyalitas nasabah tetap dipertahankan oleh faktor religiusitas, komitmen terhadap layanan perbankan syariah, serta keyakinan bahwa bank mampu melakukan pemulihan sistem keamanan secara bertahap. Dengan demikian, hubungan antara serangan siber dan switching intention tidak selalu bersifat langsung, tetapi dimediasi oleh tingkat kepercayaan, persepsi risiko, kepuasan layanan, dan nilai-nilai religius yang dimiliki nasabah.

Dari perspektif Technology Acceptance Model (TAM), insiden siber menyebabkan perubahan persepsi terhadap kemudahan penggunaan (perceived ease of use), kebermanfaatan layanan (perceived usefulness), serta tingkat keamanan sistem digital. Penelitian terbaru menunjukkan bahwa kepercayaan menjadi faktor utama yang mendorong keberlanjutan penggunaan aplikasi BSI Mobile setelah insiden siber. Semakin tinggi tingkat kepercayaan yang berhasil dipulihkan, semakin besar pula kemungkinan nasabah tetap menggunakan layanan digital meskipun sebelumnya mengalami gangguan. Sebaliknya, apabila proses pemulihan tidak mampu mengembalikan rasa aman, kecenderungan untuk beralih ke bank lain akan meningkat.

Dalam perspektif ekonomi Islam, kepercayaan merupakan manifestasi dari prinsip amanah, shiddiq, dan maslahah. Bank syariah tidak hanya berkewajiban menjaga keamanan dana nasabah, tetapi juga melindungi informasi pribadi sebagai bagian dari

hifz al-mal (perlindungan harta) dan hifz al-'irdh (perlindungan kehormatan dan privasi). Kegagalan menjaga keamanan sistem informasi dapat dipandang sebagai pelanggaran terhadap prinsip amanah apabila tidak diikuti dengan langkah mitigasi, transparansi, dan pemulihan yang memadai. Oleh karena itu, penguatan keamanan siber merupakan bagian dari implementasi maqashid syariah dalam tata kelola perbankan modern.

Untuk memulihkan kepercayaan dan menekan switching intention, bank syariah perlu menerapkan strategi yang komprehensif. Strategi tersebut meliputi penguatan infrastruktur keamanan siber, penerapan autentikasi multifaktor, peningkatan sistem deteksi ancaman berbasis Artificial Intelligence, transparansi komunikasi kepada nasabah selama proses pemulihan, edukasi mengenai keamanan transaksi digital, serta audit keamanan informasi secara berkala. Selain itu, penguatan manajemen risiko digital yang selaras dengan prinsip syariah akan meningkatkan keyakinan masyarakat bahwa bank mampu melindungi dana dan data nasabah secara profesional.

Secara konseptual, hubungan antarvariabel dalam penelitian ini dapat dijelaskan bahwa serangan siber berpengaruh negatif terhadap kepercayaan nasabah, sedangkan kepercayaan nasabah berpengaruh negatif terhadap switching intention. Dengan demikian, semakin besar dampak serangan siber terhadap penurunan kepercayaan, semakin tinggi kecenderungan nasabah untuk mempertimbangkan perpindahan ke bank lain. Sebaliknya, keberhasilan bank dalam memulihkan kepercayaan melalui peningkatan keamanan, kualitas layanan, dan komunikasi krisis yang efektif akan menurunkan minat nasabah untuk beralih serta memperkuat loyalitas jangka panjang.

KESIMPULAN

Penelitian menunjukkan bahwa serangan siber pada Bank Syariah Indonesia pasca-insiden tahun 2023 tidak hanya mengganggu operasional perbankan, tetapi juga meningkatkan persepsi risiko keamanan, menurunkan kepercayaan nasabah, serta mendorong munculnya switching intention. Meskipun demikian, perpindahan nasabah tidak terjadi secara masif karena dipengaruhi oleh loyalitas terhadap prinsip perbankan syariah, biaya perpindahan, dan keterikatan terhadap layanan yang telah digunakan. Penelitian ini menegaskan bahwa penguatan keamanan siber, ketahanan digital, dan komunikasi krisis yang transparan merupakan strategi penting dalam mempertahankan kepercayaan, loyalitas, serta keberlanjutan industri perbankan syariah di era digital.

REFERENSI

Aisyah, M., Sesunan, Y. S., & Wicaksono, A. T. S. (2025). Customers' trust in Islamic banking post-cyberattack leads to digital service breakdowns in Indonesia. Sustainable Futures, 10, 101530. https://doi.org/10.1016/j.sftr.2025.101530

Apaua, R., & Lallie, H. S. (2022). Measuring user perceived security of mobile banking applications. arXiv. https://doi.org/10.48550/arXiv.2201.03052

Hadratullah, H., & Hidayati, R. (2025). The influence of innovation, network, and technology on customer switching to Bank Syariah Indonesia. Indonesian Journal of Islamic Economics and Finance, 4(2). https://doi.org/10.37680/ijief.v4i2.5793

Hafiz, M., Muslihun, M., & Sanurdi, S. (2025). The influence of product innovation, branch network, and information technology systems on switching behavior of customers from conventional banks to Bank Syariah Indonesia: A case study in Selong District. Jurnal Pendidikan IPS, 15(2). https://doi.org/10.37630/jpi.v15i2.3057

HS, M. S. R., Khasanah, M., & Sutrisno, S. (2022). Linking sharia bank corporate image and customer trust with customer switching intention: The mediating role of customer loyalty. Journal of Islamic Economic and Business Research, 2(2), 89–104. https://doi.org/10.18196/jiebr.v2i2.81

Jannah, A. M., & Widodo, A. (2018). Pengaruh persepsi Bank Syariah di Indonesia terhadap customer switching intention dengan customer satisfaction sebagai mediator. Jurnal Sekretaris dan Administrasi Bisnis, 2(1), 57–66. https://doi.org/10.31104/jsab.v2i1.27

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). https://doi.org/10.20885/JEKI.vol11.iss2.art2

Maulana, L., & Fitriana, N. (2023). Analisis dampak insiden BSI eror dan dugaan hacking Bank Syariah Indonesia (BSI) terhadap kepercayaan dan loyalitas nasabah Bank Syariah Indonesia di Kabupaten Subang. Rayah Al-Islam, 7(3), 1755–1768. https://doi.org/10.37274/rais.v7i3.899

Nadia, N., Susanty, W., Muda, I., Soemitra, A., & Yusrizal, Y. (2025). The influence of digital resilience and service quality on switching intention of Bank Syariah Indonesia customers in Aceh with subjective norm as a mediating variable. MALIA: Journal of Islamic Banking and Finance, 16(2). https://doi.org/10.35891/ml.v16i2.6284

Rahman, B. S., Prabawani, B., & Nugraha, H. S. (2024). Analysis of the effect of perceived risk, service quality and customer trust toward customer loyalty after a cyber attack (Study in Bank Sharia Indonesia). Jurnal Ilmu Administrasi Bisnis, 13(4), 1092–1101. https://doi.org/10.14710/jiab.2024.44725

Salsabila, D., Mainata, D., & Noni, Y. (2024). Pengaruh merger tiga bank syariah menjadi PT Bank Syariah Indonesia terhadap switching behavior nasabah. Indonesian Scientific Journal of Islamic Finance, 2(1). https://doi.org/10.21093/inasjif.v2i1.7283

Sari, B. F. N. E., & Aji, H. M. (2022). Niat berpindah nasabah yang termigrasi paksa ke Bank Syariah Indonesia. Jurnal Manajerial, 10(1), 1–15. https://doi.org/10.30587/jurnalmanajerial.v10i1.4546

Rustan, S., Haanurat, I., & Nurlina, N. (2026). Cybercrime and customer trust in digital banking services: Evidence from Bank Syariah Indonesia. Jurnal Ekonomi dan Bisnis, 5(1), 42–51. https://doi.org/10.57151/jeko.v5i1.1079

Aisyah, M., Sesunan, Y. S., & Wicaksono, A. T. S. (2025). Trust, perceived risk, and continuance intention in Islamic mobile banking after cyberattacks in Indonesia. Sustainable Futures, 10, 101530. https://doi.org/10.1016/j.sftr.2025.101530