Maliki Interdisciplinary Journal (MIJ) eISSN: 3024-8140
Volume 3, Issue Desember, 2025 pp. 2014-2017 http://urj.uin-malang.ac.id/index.php/mij/index

Mengelola risiko layanan digital: kasus gangguan m-banking pada BSI

Najwa Ishma Shofiranti
Program Studi Perbankan Syariah, Universitas Islam Negeri Maulana Malik Ibrahim Malang
Email: najwaishfa@gmail.com

Kata Kunci:
digitalisasi perbankan, risiko siber, ransomware, manajemen risiko, Bank Syariah Indonesia.

Keywords:
banking digitalization, cyber risk, ransomware, risk management, Bank Syariah Indonesia.

A B S T R A K
Transformasi digital dalam sektor perbankan telah membawa kemudahan dan efisiensi layanan bagi nasabah, namun juga memunculkan tantangan baru berupa risiko siber yang semakin kompleks. Artikel ini membahas kasus gangguan layanan digital yang dialami Bank Syariah Indonesia (BSI) pada Mei 2023 sebagai contoh nyata rentannya sistem perbankan terhadap serangan ransomware. Gangguan tersebut berdampak luas, tidak hanya secara teknis, tetapi juga terhadap reputasi dan kepatuhan terhadap regulasi perlindungan data pribadi. Melalui pendekatan deskriptif-kualitatif berbasis studi literatur, artikel ini mengidentifikasi berbagai jenis risiko digital serta merumuskan strategi pengelolaan risiko yang mencakup penguatan keamanan sistem, kesiapan tanggap darurat, komunikasi krisis, diversifikasi saluran layanan, dan peningkatan literasi digital. Kolaborasi antara bank, regulator, dan otoritas keamanan siber juga ditekankan sebagai langkah penting untuk memperkuat ketahanan sistem keuangan nasional di era digital yang terus berkembang.

A B S T R A C T
Digital transformation in the banking sector has brought convenience and efficiency of services to customers, but has also given rise to new challenges in the form of increasingly complex cyber risks. This article discusses the case of a digital service disruption experienced by Bank Syariah Indonesia (BSI) in May 2023 as a real example of the vulnerability of the banking system to ransomware attacks. The disruption had a wide impact, not only technically, but also on reputation and compliance with personal data protection regulations. Through a descriptive-qualitative approach based on literature studies, this article identifies various types of digital risks and formulates risk management strategies that include strengthening system security, emergency response readiness, crisis communication, diversification of service channels, and increasing digital literacy. Collaboration between banks, regulators, and cybersecurity authorities is also emphasized as an important step to strengthen the resilience of the national financial system in the ever-evolving digital era.

Pendahuluan

Pada era industri 4.0, digitalisasi telah menjadi elemen kunci dalam perubahan besar-besaran pada layanan keuangan, termasuk dalam dunia perbankan. Lembaga perbankan kini tidak lagi terbatas pada pelayanan tradisional melalui kantor cabang, melainkan telah mengadopsi berbagai platform digital seperti mobile banking, internet banking, dan layanan pembayaran berbasis aplikasi. Perubahan ini ditujukan untuk meningkatkan efisiensi operasional, memperluas akses layanan, serta memberikan kemudahan dan kecepatan bagi nasabah dalam melakukan transaksi keuangan. Namun, seiring dengan meningkatnya ketergantungan pada teknologi digital, berbagai risiko

baru pun ikut muncul yang berpotensi mengganggu kelancaran operasional serta menurunkan tingkat kepercayaan publik terhadap institusi perbankan.

Salah satu peristiwa yang menarik perhatian publik adalah terganggunya layanan digital Bank Syariah Indonesia (BSI) pada Mei 2023. Gangguan ini berlangsung selama beberapa hari, menyebabkan nasabah tidak dapat mengakses berbagai layanan vital seperti mobile banking, mesin ATM, hingga transaksi digital lainnya. Dampaknya sangat terasa, terutama karena layanan keuangan kini menjadi bagian penting dari aktivitas masyarakat yang serba digital (SETIAWAN & MUGIYATI, 2023). Walaupun BSI telah menyampaikan permintaan maaf dan mengambil langkah-langkah pemulihan, kejadian tersebut tetap menimbulkan kekhawatiran mengenai seberapa tangguh sistem digital perbankan Indonesia dalam menghadapi serangan siber yang semakin canggih.

Gangguan ini diduga kuat dipicu oleh serangan ransomware, yakni jenis serangan siber yang mengenkripsi data penting dan menuntut tebusan agar data tersebut dapat dipulihkan. Dampak dari serangan semacam ini tidak hanya terbatas pada kerusakan teknis, tetapi juga menyentuh aspek reputasi lembaga dan kemungkinan pelanggaran terhadap aturan perlindungan data pribadi (JANNAH, 2024). Dalam hal ini, insiden yang dialami BSI menjadi contoh nyata akan urgensi pengelolaan risiko digital yang menyeluruh. Memperkuat sistem teknologi saja tidak cukup; kesiapan organisasi dalam merespons kejadian, membangun komunikasi yang terbuka dengan masyarakat, serta memastikan kepatuhan terhadap regulasi juga sangat krusial. Melihat skala dan konsekuensi dari insiden ini, muncul pertanyaan penting, seperti sejauh mana kesiapan bank khususnya bank syariah dalam menghadapi risiko digital yang terus berkembang? Apa langkah strategis yang dapat diterapkan untuk menjaga kepercayaan nasabah dan memastikan kelangsungan layanan? Artikel ini akan membahas secara komprehensif berbagai jenis risiko yang mengancam layanan digital perbankan, serta strategi pengelolaan yang efektif untuk menghadapi tantangan tersebut di era digital saat ini.

Pembahasan

Transformasi digital dalam sektor perbankan membawa manfaat besar, namun juga diiringi dengan berbagai risiko yang kompleks. Kejadian terganggunya layanan Bank Syariah Indonesia (BSI) menjadi contoh nyata bahwa sistem perbankan digital sangat rentan terhadap ancaman yang bersifat teknis maupun non-teknis. Insiden tersebut bukan hanya menghambat akses nasabah terhadap layanan penting, tetapi juga memicu kekhawatiran mengenai seberapa siap bank dalam menghadapi tantangan dunia siber yang terus berkembang. Gangguan ini menunjukkan bahwa risiko dalam layanan digital tidak hanya bersifat operasional akibat kegagalan sistem internal, tetapi juga mencakup risiko serangan eksternal seperti ransomware, yang dapat melumpuhkan layanan dan mengancam keamanan data (AZHARA, 2024).

Selain risiko teknis, ada pula risiko reputasi yang sangat berdampak pada citra bank di mata publik. Ketika layanan terganggu dalam waktu lama dan komunikasi tidak dikelola secara efektif, kepercayaan nasabah akan menurun, bahkan bisa berdampak pada loyalitas jangka panjang. Di sisi lain, lembaga perbankan juga menghadapi tekanan regulatif, terutama terkait dengan perlindungan data nasabah sebagaimana diatur

dalam regulasi nasional seperti Undang-Undang Perlindungan Data Pribadi. Kegagalan dalam memenuhi kewajiban hukum ini dapat menimbulkan sanksi dan memperparah kerugian institusi (MAULANA & FITRIANA, 2024). Oleh karena itu, pendekatan yang komprehensif sangat diperlukan dalam mengelola risiko digital. Tidak cukup hanya memperkuat infrastruktur teknologi, tetapi perlu juga adanya sistem pengawasan yang berkelanjutan, penggunaan perangkat lunak keamanan yang canggih, dan audit keamanan secara berkala. Selain itu, kesiapan organisasi dalam menghadapi situasi darurat menjadi hal yang sangat krusial. Setiap institusi keuangan harus memiliki rencana tanggap darurat yang dapat dijalankan segera saat terjadi insiden, serta memiliki tim yang mampu menangani krisis dengan cepat dan tepat (SYAHRIR ET AL., 2023).

Di tengah insiden seperti yang dialami BSI, kemampuan dalam membangun komunikasi yang terbuka dan empatik kepada nasabah sangat menentukan keberhasilan pemulihan kepercayaan. Penjelasan yang transparan mengenai penyebab gangguan, langkah perbaikan yang dilakukan, serta kepedulian terhadap dampak yang dirasakan oleh nasabah menjadi bagian penting dalam manajemen krisis. Komunikasi yang baik mampu meredam keresahan dan menunjukkan bahwa bank memiliki komitmen untuk bertanggung jawab dan terus memperbaiki diri. Lebih jauh lagi, bank perlu membangun ekosistem layanan yang tidak hanya bergantung pada satu platform digital. Diversifikasi saluran layanan seperti penguatan call center, ketersediaan aplikasi alternatif, atau dukungan layanan berbasis web menjadi strategi untuk menjamin kelangsungan akses nasabah saat gangguan terjadi. Di samping itu, peningkatan literasi digital, baik untuk karyawan maupun nasabah, menjadi modal penting dalam menciptakan ekosistem perbankan digital yang aman. Kolaborasi antara bank, regulator, dan lembaga keamanan siber juga menjadi langkah strategis dalam menciptakan sistem yang lebih tangguh dan adaptif terhadap ancaman digital yang terus berkembang (LARASSATI & FAUZI, 2022). Kejadian yang menimpa BSI memberikan pelajaran penting, tidak hanya bagi bank syariah, tetapi juga bagi seluruh sektor perbankan nasional. Di tengah upaya digitalisasi yang semakin masif, bank harus memprioritaskan perlindungan terhadap nasabah dan menjaga integritas sistem. Pengelolaan risiko digital harus dilakukan secara menyeluruh, tidak hanya dari sisi teknis, tetapi juga dari sisi etika pelayanan, regulasi, dan kepercayaan publik sebagai pilar utama keberlangsungan industri perbankan di era digital.

Kesimpulan dan Saran

Peristiwa gangguan layanan digital yang menimpa Bank Syariah Indonesia pada Mei 2023 mengungkapkan bahwa digitalisasi dalam sektor perbankan, meskipun memberikan berbagai kemudahan, tetap menyimpan risiko besar yang tidak boleh diabaikan. Gangguan ini tidak hanya mengganggu aktivitas keuangan nasabah, tetapi juga menimbulkan keraguan terhadap ketahanan sistem digital dan kesiapan institusi dalam menghadapi ancaman siber. Serangan seperti ransomware dapat berdampak luas, mulai dari terganggunya operasional, ancaman hukum terkait data pribadi, hingga kerusakan reputasi lembaga. Oleh karena itu, pengelolaan risiko digital perlu dilakukan secara menyeluruh, tidak hanya berfokus pada infrastruktur teknologi, tetapi juga

mencakup kesiapan organisasi dalam merespons insiden, membangun komunikasi yang transparan, dan menjaga kepercayaan nasabah. Untuk menjawab tantangan ini, bank perlu memperkuat sistem keamanan informasi, menyiapkan prosedur tanggap darurat, memperluas saluran layanan agar tidak bergantung pada satu platform, serta meningkatkan literasi digital baik bagi internal karyawan maupun nasabah. Selain itu, sinergi antara lembaga keuangan, regulator, dan otoritas keamanan siber sangat penting untuk memastikan sistem keuangan tetap aman, berkelanjutan, dan adaptif terhadap dinamika risiko di era digital.

Daftar Pustaka

Azhara, R. (2024). Pengaruh Persepsi Risiko, Persepsi Keamanan, dan User Experience Terhadap Loyalitas Nasabah Menggunakan Aplikasi BSI Mobile. 3.

Jannah, N. M. (2024). Pengaruh Serangan Siber dan Kualitas Pelayanan Terhadap Loyalitas Nasabah (Studi Kasus Bank Syariah Indonesia).

Larassati, N., & Fauzi, A. (2022). Strategi Meningkatkan Kualitas Layanan Melalui Digitalisasi Perbankan di BSI Trade Center Kota Kediri. Jurnal At-Tamwil: Kajian Ekonomi Syariah, 4(2), 202–217. https://doi.org/10.33367/at.v4i2.1473

Maulana, L., & Fitriana, N. (2024). 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

Setiawan, J. A., & Mugiyati, M. (2023). Peluang dan Tantangan Bank Syariah di Indonesia Dalam Mempertahankan Eksistensi di Era Digital. Al-Kharaj : Jurnal Ekonomi, Keuangan & Bisnis Syariah, 6(1), 834–845. https://doi.org/10.47467/alkharaj.v6i1.2396

Syahrir, D. K., Ickhsanto Wahyudi, Santi Susanti, Darwant, D., & Ibnu Qizam. (2023). Manajemen Risiko Perbankan Syariah. AKUA: Jurnal Akuntansi dan Keuangan, 2(1), 58–64. https://doi.org/10.54259/akua.v2i1.1382