JKAM Jurnal Kajian Akademik Multidisiplin
Yayasan Paramarta Akademika Indonesia
P-ISSN XXXX, E-ISSN XXXX

Manajemen Risiko Siber dan Strategi Pemulihan Citra Bank Syariah Indonesia: Pasca-Insiden Gangguan Layanan Digital Perbankan Syariah

ABSTRACT *- This study aims to analyze the implementation of cyber risk management and image restoration strategies conducted by Bank Syariah Indonesia (BSI) following a major digital banking service outage. This research employs a descriptive qualitative method based on literature study and secondary document analysis. The primary theoretical frameworks utilized include the Situational Crisis Communication Theory (SCCT) by W. Timothy Coombs and the Image Restoration Theory by William L. Benoit. The results demonstrate that rebuilding customer trust and image recovery were achieved through the integration of four main pillars: (1) responsive crisis communication via mass and social media; (2) activation of the Business Continuity Plan (BCP) utilizing frontline staff to mitigate customer panic on the ground; (3) fundamental technical fixes, including building a new server, consolidating a single gateway, strengthening encryption, and implementing double authentication; and (4) operational compensation through weekend banking services and a gift-reward deposit incentive program. The implications of this study emphasize the necessity of integrating technical corrective action with transparent crisis communication to maintain customer loyalty and ensure the liquidity stability of Islamic banks following a cyber crisis.*

ABSTRAK –Penelitian ini bertujuan untuk menganalisis penerapan manajemen risiko siber dan strategi pemulihan citra (image restoration strategy) yang dilakukan oleh Bank Syariah Indonesia (BSI) pasca-insiden gangguan layanan digital perbankan. Metode penelitian yang digunakan adalah kualitatif deskriptif berbasis studi literatur dan analisis dokumen sekunder. Kerangka teori utama yang digunakan meliputi Situational Crisis Communication Theory (SCCT) oleh W. Timothy Coombs dan Image Restoration Theory oleh William L. Benoit. Hasil penelitian menunjukkan bahwa pemulihan kepercayaan dan citra nasabah dicapai melalui kombinasi empat pilar utama, yaitu: (1) komunikasi krisis responsif melalui media massa dan media sosial; (2) pengaktifan Business Continuity Plan (BCP) berbasis peran pegawai frontline untuk meredakan kepanikan nasabah di lapangan; (3) perbaikan teknis fundamental meliputi pembangunan server baru, konsolidasi single gateway, penguatan enkripsi, dan double authentication; serta (4) kompensasi operasional melalui weekend banking dan program insentif deposito berhadiah. Implikasi dari penelitian ini menegaskan pentingnya integrasi antara tindakan korektif teknis (corrective action) dan komunikasi krisis yang transparan dalam menjaga loyalitas nasabah serta stabilitas likuiditas bank syariah pasca-krisis siber.

Author
[1] **Cindy Aulia Sari**, Universitas Al-Azhar Medan, Indonesia
[2] **Nabila Nuha**, Universitas Al-Azhar Medan, Indonesia
[3] **Gita Jumayni**, Universitas Al-Azhar Medan, Indonesia
[4] **Ummi Kalsum**, Universitas Al-Azhar Medan, Indonesia

*[*1]Corresponding email:* Cindyauliasari09@gmail.com

Article History
Submitted: 09 Agustus 2026
Revised: 10 Agustus 2026
Accepted: 21 September 2026
Published: 21 September 2026

Keywords
Manajemen Risiko Siber; Pemulihan Citra Bank Syariah; Layanan Digital

PENDAHULUAN

Pesatnya perkembangan teknologi informasi dan komunikasi telah mentransformasi lanskap industri keuangan global, termasuk pada sektor perbankan syariah. Digitalisasi perbankan syariah melalui inovasi seperti mobile banking, internet banking, dan ekosistem transaksi syariah digital kini bukan lagi sekadar pelengkap, melainkan kebutuhan utama untuk meningkatkan efisiensi operasional dan kenyamanan nasabah. Namun, ketergantungan yang kian tinggi terhadap infrastruktur Teknologi Informasi dan Komunikasi (TIK) secara bersamaan memperluas permukaan serangan (attack surface) dan meningkatkan risiko siber (cyber risk).

Dalam konteks perbankan syariah, risiko siber tidak hanya berdampak pada kerugian finansial atau teknis semata, tetapi juga mengancam pilar utama operasionalnya, yaitu kepercayaan (trust) dan prinsip amanah. Ketika insiden gangguan layanan digital seperti serangan ransomware, kebocoran data, atau downtime sistem dalam skala besar terjadi, dampak psikologis dan persepsi risiko di kalangan nasabah berpotensi memicu krisis reputasi yang masif. Mengingat bisnis perbankan berbasis pada kepercayaan, gangguan layanan digital yang menghambat akses transaksi nasabah dapat mengikis loyalitas dan memicu migrasi dana.

Oleh karena itu, institusi perbankan syariah dituntut tidak hanya memiliki ketahanan teknis melalui mitigasi risiko siber yang proaktif, tetapi juga strategi pemulihan citra bank syariah indonesia. Penelitian ini berfokus untuk mengeksplorasi secara mendalam bagaimana manajemen risiko siber dijalankan dan bagaimana strategi pemulihan citra bank syariah indonesia dirumuskan serta diimplementasikan pasca-terjadinya insiden gangguan layanan digital.

Perkembangan digitalisasi perbankan syariah membawa kemudahan dalam pelayanan dan efisiensi operasional, namun juga memunculkan tantangan baru berupa risiko cyber dan perlindungan data pribadi. Risiko ini mencakup potensi serangan malware, pishing, ransomware, dan kebocoran data nasabah. Dalam konteks syariah, keamanan data merupakan bagian dari prinsip keadilan dan amanah yang wajib dijaga dalam setiap aktivitas muamalah.

Manajemen Risiko Siber

Manajemen risiko siber dalam konteks perbankan syariah merupakan sebuah pendekatan terstruktur untuk mengidentifikasi, mengukur, memitigasi, dan mengendalikan ancaman teknologi guna menjaga integritas operasional dan keamanan data nasabah. Implementasi tata kelola teknologi yang tangguh menjadi suatu keharusan karena insiden kebocoran data maupun kelumpuhan sistem dapat berimplikasi langsung pada reputasi lembaga keuangan. Bagi perbankan syariah, pengelolaan risiko siber tidak hanya berfokus pada keandalan infrastruktur IT, tetapi juga berlandaskan pada prinsip kepatuhan syariah (sharia compliance) yang mengedepankan nilai-nilai amanah, transparansi, dan perlindungan terhadap hak-hak nasabah

Pemulihan Citra Bank Syariah

Menurut Sutisna, citra adalah total persepsi terhadap suatu objek yang terbentuk melalui pengolahan informasi dari berbagai sumber setiap waktu. Sedangkan menurut Alma, citra didefinisikan sebagai kesan yang diperoleh sesuai dengan pengetahuan

dan pengalaman seseorang terhadap suatu hal. Selanjutnya, Rhenald Kasali mendefinisikan citra sebagai kesan yang muncul akibat pemahaman terhadap suatu kenyataan. Dengan berlandaskan pada pandangan-pandangan tersebut, citra mencerminkan kesan suatu objek terhadap objek lain yang terbentukmelalui pengolahan informasi dari berbagai sumber terpercaya setiap waktu (Purba & Ibrahim, 2017).

Perbankan Syariah

Perbankan Syariah adalah lembaga keuangan yang operasional, produk, dan tata kelolanya diselenggarakan berdasarkan prinsip-prinsip syariah Islam, yakni aturan hukum Islam yang bersumber dari Al-Qur'an, Hadis, dan ikhtiar ijtihad para ulama (Uzlah & Setiawan, 2024).

Pendekatan kualitatif dipilih karena mampu menggali persepsi, pengalaman, serta dinamika respons strategis dari pihak manajemen bank dan nasabah dalam menghadapi situasi krisis pasca-gangguan layanan. Melalui pengumpulan data sekunder, studi literatur, serta analisis dokumen tepercaya, penelitian ini bertujuan merumuskan kerangka pemulihan reputasi dan manajemen risiko siber yang efektif bagi keberlanjutan perbankan syariah di Indonesia.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif deskriptif. Metode kualitatif dipilih karena mampu memberikan pemahaman mendalam mengenai dinamika, persepsi, serta respons strategis manajemen dan nasabah terkait krisis siber. Data diperoleh melalui studi kepustakaan (literature review) dan analisis dokumen/konten sekunder dari publikasi ilmiah, laporan resmi insiden, laporan tahunan (annual report), serta kebijakan terkait perbankan syariah. Analisis data dilakukan secara interaktif dengan tahapan reduksi data, penyajian data, dan penarikan kesimpulan secara obyektif.

HASIL DAN PEMBAHASAN

Strategi Manajemen Risiko Siber pada Perbankan Syariah Pasca-Insiden

Transformasi digital dan integrasi dengan ekosistem financial technology (fintech) telah memperluas cakupan operasional perbankan syariah di Indonesia. Namun, seiring meningkatnya aksesibilitas dan efisiensi, risiko serangan siber seperti ransomware, kebocoran data (data breach), phishing, dan manipulasi sistem juga meningkat secara signifikan. Mengingat perbankan syariah berlandaskan pada azas kepercayaan (amanah) dan kepatuhan syariah (sharia compliance), dampak insiden siber tidak hanya terbatas pada kerugian finansial, melainkan juga risiko reputasi dan krisis kepercayaan publik.

Implementasi manajemen risiko siber pada institusi perbankan syariah memerlukan penataan ulang kerangka kerja keamanan TIK yang tidak hanya mengandalkan resiliensi teknologi, tetapi juga menyelaraskan nilai kepatuhan syariah (Shariah compliance). Penguatan infrastruktur dilakukan secara bertahap melalui pembaruan sistem enkripsi, arsitektur zero-trust, serta autentikasi bertingkat untuk menjaga integritas data nasabah. Penanganan ancaman siber yang terstruktur menjadi faktor kunci untuk meminimalkan dampak gangguan operasional dan mencegah kerugian finansial yang lebih besar (Razikin & Soewito, 2022).

Berdasarkan hasil analisis kualitatif terhadap dokumen kebijakan, laporan insiden, dan literatur terkait, manajemen risiko siber pada perbankan syariah membutuhkan pendekatan terpadu yang tidak hanya bertumpu pada ketahanan teknis (technical resilience), melainkan juga keselarasan dengan tata kelola syariah (Shariah governance).

1. Mitigasi Proaktif dan Penguatan Infrastruktur TIK

Penguatan infrastruktur keamanan sistem merupakan lini pertahanan utama (first line of defense). Dalam ekosistem perbankan digital syariah, langkah-langkah mitigasi teknis yang ditemukan meliputi:

a. Enkripsi Data dan Autentikasi Ganda (Multi-Factor Authentication / MFA): Perlindungan data pribadi dan transaksi nasabah untuk menjaga kerahasiaan (confidentiality) sesuai dengan amanah pengelolaan dana.
b. Uji Penetrasi (Penetration Testing) dan Audit Keamanan Berkala: Evaluasi rutin terhadap potensi celah keamanan (vulnerabilities) pada sistem perbankan seluler (mobile banking) dan core banking.

2. Business Continuity Plan (BCP) dan Disaster Recovery Plan (DRP)

Keberhasilan penanganan saat insiden terjadi sangat ditentukan oleh kesiapan skenario BCP dan DRP. Institusi perbankan syariah yang adaptif menerapkan:

a. Sistem Cadangan Data (Data Redundancy & Backup): Pemulihan operasional yang cepat guna meminimalkan durasi downtime layanan digital.
b. Isolasi Sistem (Containment): Tindakan cepat melokalisasi area yang terindikasi terkena gangguan/serangan siber agar tidak meluas ke infrastruktur transaksi kritikal lainnya.

Pasca-terjadinya insiden siber, perbankan syariah dituntut untuk tidak hanya memulihkan ketersediaan sistem operasional secara teknis, tetapi juga melakukan audit menyeluruh, keterbukaan informasi yang bertanggung jawab (transparency/tabayyun), ganti rugi yang adil ('adl), serta penguatan sistem deteksi dini guna mencegah kejadian berulang.

Berikut adalah tabel ringkasan komprehensif mengenai strategi penanganan dan manajemen risiko siber pada perbankan syariah pasca-terjadinya insiden siber:

Tabel 1: Matriks Strategi Manajemen Risiko Siber Pasca-Insiden

Pilar Strategi	Langkah Tindakan Pasca-Insiden	Implementasi Teknis & Operasional	Integrasi Prinsip Syariah	Target/Output
1. Penanganan Krisis & Isolasi Dampak (Containment)	• Pemutusan akses jaringan terdampak. • Aktivasi Business Continuity Plan (BCP) & DRC.	Restorasi data melalui immutable backup, verifikasi keabsahan data saldo/transaksi nasabah,	Hifz al-Mal Perlindungan harta dan aset nasabah dari kerusakan lebih luas.	Minimasi potensi kerugian finansial & data nasabah.

		serta pengujian ulang sistem sebelum go-live.		
2. Investigasi Forensik & Root Cause Analysis	• Digital Forensics & Incident Response (DFIR). • Penelusuran log audit sistem. • Identifikasi celah keamanan (vulnerability).	Penyampaian notifikasi insiden resmi sesuai regulasi OJK, pembukaan kanal pengaduan khusus, serta mekanisme ganti rugi atas kelalaian teknis.	Tabayyun Klarifikasi dan pembuktian fakta secara cermat dan objektif.	Laporan analisis akar masalah & penutupan celah keamanan.
3. Pemulihan Sistem & Integritas Data (Recovery)	• Pemulihan data dari cadangan terenkripsi. • Sanitasi dan validasi integritas data. • Penetration testing pasca-pemulihan	Restorasi data melalui immutable backup, verifikasi keabsahan data saldo/transaksi nasabah, serta pengujian ulang sistem sebelum go-live	Amanah Pemulihan kerahasiaan & keutuhan titipan data/dana nasabah.	Sistem kembali beroperasi normal dengan tingkat keamanan teruji.
4. Komunikasi Transparan & Perlindungan Konsumen	• Pelaporan formal ke OJK & Bank Indonesia. • Pengumuman transparan kepada publik/nasabah. • Penyediaan Helpdesk & ganti rugi adil.	Penyampaian notifikasi insiden resmi sesuai regulasi OJK, pembukaan kanal pengaduan khusus, serta mekanisme ganti rugi atas	'Adl & Siddiq Keadilan dalam penyelesaian serta kejujuran informasi.	Mempertahankan kepercayaan nasabah & reputasi bank.

		kelalaian teknis		
5. Transformasi Budaya & Peningkatan SDM	• Pelatihan ulang (re-training) SDM. • Evaluasi etika & kesadaran siber pegawai. • Simulasi phishing & insiden berkala.	Peningkatan literasi keamanan digital pegawai, edukasi anti social engineering, serta internalisasi etika menjaga rahasia bank	Itqan Profesionalisme & ketelitian dalam menjalankan kewajiban.	Terbentuknya cybersecurity culture yang adaptif & tangguh.
6. Audit Tata Kelola & Penyempurnaan Regulasi	• Evaluasi kebijakan Manajemen Risiko IT. • Pengetatan SLA & standar API Fintech. • Integrasi Early Warning System (EWS).	Pembaruan regulasi internal, penerapan zero trust architecture, audit berkala vendor/fintech mitra, serta adopsi monitoring AI/Machine Learning	Syuura Musyawarah & kolaborasi lintas pemangku kepentingan.	Resiliensi sibel berkesinambungan dan terintegrasi.

Sumber : Diolah dari Aisyah, S. N., Wulandari, F., Tursina, & Hendra K, J. (2026). Optimalisasi Manajemen Risiko Siber Pada Perbankan Syariah di Indonesia dalam Menghadapi Era Fintech. JEBMAK, Vol. 5, No. 2, hlm. 331–344; diolah bersama regulasi OJK & standar ISO/IEC 27001.

Strategi Manajemen Risiko Siber Pasca-Insiden

Transisi Paradigma: Dari Reaktif Menuju Proaktif dan Preventif Berkelanjutan

Salah satu poin krusial pasca-insiden siber adalah perubahan paradigma tata kelola perbankan syariah. Jika sebelum terjadinya insiden manajemen risiko cenderung bersifat reaktif (merespons setelah dampak terjadi), maka pasca-insiden perbankan syariah diwajibkan membangun pendekatan yang berkesinambungan, proaktif, dan preventif. Hal ini disebabkan oleh karakteristik ancaman siber di era fintech yang bergerak sangat cepat, anonim, serta berdampak sistemik. Pemulihan tidak boleh berhenti pada penambalan bug teknis semata, tetapi harus mencakup penguatan Early Warning System (EWS) berbasis AI yang mampu memantau anomali transaksi secara real-time.

Integrasi Nilai Syariah dalam Penanganan Pasca-Insiden

Keunggulan dan keunikan perbankan syariah terletak pada landasan etika moralitas dan hukum Islam dalam setiap operasionalnya:

- Amanah (Accountability & Integrity): Bank memegang tanggung jawab moral dan legal atas penyimpanan data serta harta nasabah. Ketika terjadi kebocoran data, pemulihan sistem harus dilakukan dengan standar keamanan tertinggi sebagai bentuk pemenuhan janji amanah.
- 'Adl (Justice & Fair Compensation): Apabila kerugian nasabah timbul akibat kelalaian sistem keamanan bank, maka sesuai prinsip keadilan, bank syariah harus memberikan penyelesaian dan ganti rugi yang adil tanpa memberatkan nasabah.
- Tabayyun (Verification & Transparency): Dalam menyampaikan kronologi insiden, bank harus mengedepankan verifikasi data yang akurat serta keterbukaan informasi kepada publik dan regulator (OJK/BI), menghindarkan diri dari manipulasi informasi.

Penguatan Kemitraan Fintech dan Standar Keamanan Pihak Ketiga

Pasca-insiden, perbankan syariah harus mengevaluasi secara ketat seluruh keterhubungan Application Programming Interface (API) dengan mitra financial technology. Keterhubungan sistem dengan pihak ketiga sering kali menjadi pintu masuk (entry point) serangan siber jika mitra fintech memiliki tingkat keamanan yang lebih rendah. Bank syariah perlu menyusun standar keamanan bersama, menerapkan arsitektur Zero Trust, serta melakukan tes penetrasi (penetration test) berkala terhadap infrastruktur integrasi fintech.

Peningkatan Kapasitas SDM dan Pembentukan Budaya Keamanan (Cybersecurity Culture)

Faktor manusia (human element) sering kali menjadi mata rantai terlemah dalam pertahanan siber. Pasca insiden, perbankan syariah perlu merevolusi budaya organisasi dengan menanamkan kesadaran siber di seluruh tingkatan jabatan, mulai dari staf operasional hingga Dewan Pengawas Syariah (DPS) dan Direksi. Program edukasi yang berkelanjutan, simulasi ancaman rekayasa sosial (social engineering), serta pelatihan penanganan krisis siber harus menjadi bagian integral dari KPI pegawai.

Sinergi Regulasi dan Kolaborasi Ekosistem Keuangan Digital

Optimalisasi manajemen risiko siber memerlukan kolaborasi erat antara perbankan syariah, Otoritas Jasa Keuangan (OJK), Bank Indonesia (BI), Badan Siber dan Sandi Negara (BSSN), serta asosiasi industri. Pasca-insiden, pertukaran informasi intelijen ancaman (threat intelligence sharing) antarlembaga menjadi kunci utama untuk mengantisipasi pola serangan baru. Dengan kepatuhan terhadap regulasi OJK terkait Manajemen Risiko Teknologi Informasi dan penerapan kerangka kerja keamanan berstandar internasional, perbankan syariah dapat membangun ketahanan digital (cyber resilience) yang kokoh dan berdaya saing tinggi.

Strategi Pemulihan Citra Bank Syariah Indonesia Pasca-Insiden

Sebagai respons terhadap insiden yang merugikan citra perusahaan, Bank Syariah Indonesia (BSI) telah mengambil langkah-langkah strategis untuk memulihkan citra mereka dan mengatasi krisis yang terjadi. Dalam upaya ini, BSI telah merancang

serangkaian kebijakan sebagai strategi untuk mengembalikan kepercayaan masyarakat serta nasabah melalui beberapa cara, yaitu:

Tabel 2: Matriks Strategi Manajemen Risiko Siber Pasca-Insiden

Pilar Strategi	Tujuan Operasional	Bentuk Realisasi di Lapangan
Manajemen Krisis (BCP)	Meredakan kepanikan nasabah dan menahan potensi rush money.	Pembagian peran terstruktur pada frontline staff, marketing, dan branch manager di kantor cabang.
Infrastruktur TI	Memperbaiki kerentanan sistem dan mencegah terulangnya insiden.	Migrasi ke server terintegrasi baru, single gateway, enkripsi terpusat, dan double authentication (OTP).
Insentif Finansial	Mempertahankan likuiditas deposito dan meningkatkan retensi nasabah.	Peluncuran Program Pesta Hadiah deposito berjangka dan kampanye edukasi keuangan.
Kompensasi Layanan	Menyeimbangkan kendala transaksi yang tertunda akibat krisis.	Penyediaan operasional cabang pada hari Sabtu dan Minggu (Weekend Banking).

Sumber : Diolah dari Maulana & Nasrulloh (2024), "Analisis Strategi Pemulihan Citra Bank Syariah Indonesia Pasca Dugaan Serangan Siber", EKSISBANK, Vol. 8 No. 1, hal. 83–86.

Memperlihatkan bahwa pemulihan citra perbankan pasca-insiden siber memerlukan koordinasi yang solid antara perbaikan teknologi internal dan pelayanan langsung di lapangan. Langkah BSI yang tidak hanya memperbaiki server dan enkripsi data, tetapi juga menghadirkan insentif deposito serta layanan weekend banking, terbukti menjadi stimulus positif dalam meredakan kekhawatiran nasabah secara bertahap.

Implementasi Teori SCCT dan Teori Pemulihan Citra Benoit

Dari beberapa strategi, kebijakan, serta respon BSI di atas, dapat diketahui bahwa dalam beberapa aspek yang berkaitan dengan upaya Bank Syariah Indonesia (BSI) dalam mengelola krisis dan memulihkan citra, terdapat beberapa relevansi dengan metode SCCT serta teori pemulihan citra yang diusung oleh William L. Benoit.

Dalam perspektif SCCT, BSI memanfaatkan variasi strategi respon untuk mengelola atribusi kesalahan dan mengarahkan opini publik di media sosial. Sementara itu, teori pemulihan citra Benoit mengidentifikasi penggunaan tindakan korektif, pengakuan kesalahan, kompensasi, dan penguatan citra positif, yaitu:

Tabel 3: Matriks Relevansi Teoretis SCCT (Coombs) dan Image Restoration (Benoit)

Tindakan Operasional Pasca-Insiden	Relevansi SCCT (Coombs)	Relevansi Teori Benoit
Pernyataan Resmi & Press Release	Deny Strategy (alasan maintenance) & Diminish Strategy (permohonan maaf).	ortification (permohonan maaf tulus) & Minimization (mengurangi kepanikan).
Pengaktifan BCP Berbasis Pegawai	Bolstering Strategy (menunjukkan kualitas dan kesiapan tim internal).	Reducing Offensiveness (mengurangi dampak gangguan layanan langsung).
Program Pesta Hadiah Deposito	Bolstering Strategy (membangun ikatan positif via insentif).	Reducing Offensiveness via Bolstering & Minimization (menutup persepsi negatif).
Pembangunan Server Terintegrasi Baru	Bolstering Strategy (penegasan komitmen peningkatan mutu sistem).	Corrective Action (memperbaiki akar kelemahan infrastruktur lama).
Konsolidasi Single Gateway	Bolstering Strategy (peningkatan kapabilitas pemantauan jaringan).	Corrective Action (menutup celah eksternal serangan siber).
Pembaruan Kebijakan Enkripsi Data	Bolstering Strategy (penegasan jaminan integritas data).	Corrective Action (langkah konkret mengamankan kerahasiaan data).
Penerapan Double Authentication (OTP)	Bolstering Strategy (peningkatan standar keamanan digital).	Corrective Action (mitigasi risiko akses tanpa otorisasi).
Penyediaan Layanan Weekend Banking	Bolstering Strategy (menunjukkan dedikasi tinggi layanan nasabah).	Compensation (pemberian ganti rugi atas ketidaknyamanan transaksi).

Sumber : Diolah dari Maulana & Nasrulloh (2024), "Analisis Strategi Pemulihan Citra Bank Syariah Indonesia Pasca Dugaan Serangan Siber", EKSISBANK, Vol. 8 No. 1, hal. 87–88.

Menunjukkan bahwa tindakan korektif (Corrective Action) menjadi elemen paling dominan dalam strategi BSI pasca-krisis siber. Menurut teori Benoit, janji dan tindakan nyata untuk memperbaiki masalah teknis (seperti migrasi server, single gateway, dan double authentication) merupakan strategi pemulihan yang paling efektif untuk memulihkan reputasi organisasi yang ternoda. Selain itu, strategi Mortification dan Compensation terbukti menutupi impresi negatif dengan memberikan kenyamanan transaksi susulan bagi nasabah.

Dengan menerapkan strategi komunikasi dan pemulihan citra ini, BSI berupaya keras untuk memperbaiki citra mereka dan memulihkan kepercayaan nasabah setelah insiden yang merugikan. Dalam konteks teori pemulihan citra William L. Benoit, langkah-langkah yang diambil oleh BSI mencerminkan upaya untuk memperkuat citra

positif mereka melalui berbagai strategi komunikasi dan tindakan nyata yang ditujukan kepada nasabah.

Tantangan pada Strategi Pemulihan Citra BSI

Tantangan dari Sisi Internal BSI; Salah satu tantangan yang dihadapi oleh BSI adalah kurangnya sistem penilaian untuk mengukur pemahaman, dukungan, dan persetujuan nasabah terhadap kebijakan serta langkah-langkah penanggulangan dalam situasi krisis. BSI juga menghadapi keterbatasan dalam memberikan tanggapan yang memadai terhadap pertanyaan dan komentar nasabah di akun resmi mereka. Namun, hal tersebut merupakan bagian dari strategi BSI untuk menghindari kepanikan berlebih sembari berupaya memahami penyebab kesalahan sistem dan langkah-langkah untuk memulihkannya.

Tantangan dalam Memulihkan Kepercayaan Nasabah; Bank Syariah Indonesia (BSI) telah mengambil langkah-langkah strategis untuk memulihkan citra mereka pasca dugaan serangan siber. Meskipun demikian, membangun kembali kepercayaan nasabah menjadi tantangan yang nyata. Beberapa nasabah mungkin tetap skeptis meskipun BSI telah memberikan penjelasan dan mengambil langkah-langkah pemulihan. Selama masa penelitian, diketahui bahwa komunikasi selama periode awal insiden yang disebabkan oleh serangan siber masih menjadi masalah. Pihak BSI hanya memberi penjelasan singkat bahwa BSI sedang melakukan maintenance tanpa adanya penjelasan lebih lanjut. Di sisi lain, nasabah pasti mengharapkan komunikasi yang lebih baik dan respons yang lebih cepat dari BSI dalam menghadapi situasi krisis serta perbaikan layanan dan pengambilan keputusan yang lebih baik lagi dari BSI.

KESIMPULAN

Penelitian ini menyimpulkan bahwa pemulihan citra dan ketahanan Bank Syariah Indonesia (BSI) pasca-insiden gangguan layanan digital dicapai melalui integrasi antara ketahanan teknis TIK dan penerapan nilai-nilai tata kelola syariah (Shariah governance). Mengacu pada kerangka Situational Crisis Communication Theory (SCCT) dan Image Restoration Theory oleh Benoit, keberhasilan BSI dalam meredakan kepanikan publik serta menahan potensi rush money bertumpu pada empat pilar utama, yaitu komunikasi krisis yang responsif, pengaktifan Business Continuity Plan (BCP) operasional di tingkat cabang, perbaikan teknis fundamental (corrective action), serta pemberian kompensasi dan insentif finansial kepada nasabah. Integrasi prinsip syariah seperti amanah, 'adl, tabayyun, dan itqan terbukti menjadi pilar krusial dalam menjaga kepercayaan serta stabilitas likuiditas bank pasca-krisis siber. Langkah perbaikan teknis fundamental (corrective action) menjadi elemen paling dominan dan efektif dalam memulihkan reputasi BSI. Hal ini direalisasikan melalui pembangunan server terintegrasi baru, konsolidasi single gateway, penguatan enkripsi data terpusat, serta penerapan double authentication (OTP) untuk menutup celah keamanan eksternal. Tindakan teknis tersebut dikombinasikan dengan strategi kompensasi dan penguatan citra (bolstering), seperti penyediaan layanan weekend banking serta program Pesta Hadiah deposito berhadiah, yang terbukti mampu menutupi persepsi negatif dan memberikan stimulus positif bagi retensi nasabah.

Meskipun strategi pemulihan terbukti berjalan secara bertahap, penelitian ini menemukan beberapa tantangan utama pada aspek komunikasi dan respon awal krisis. Keterbatasan BSI dalam memberikan penjelasan mendetail di periode awal insiden—

yang cenderung hanya menyampaikan alasan maintenance—serta kurangnya tanggapan memadai di media sosial sempat memicu skeptisisme dan kepanikan nasabah. Selain itu, belum tersedianya sistem penilaian terukur untuk mengevaluasi tingkat pemahaman dan dukungan nasabah secara real-time menjadi celah dalam manajemen krisis yang dijalankan.

Berdasarkan temuan tersebut, disarankan bagi manajemen perbankan syariah untuk memperketat protokol komunikasi krisis agar lebih transparan, akurat, dan cepat pada tahap awal insiden guna mencegah spekulasi publik. Pihak bank juga perlu membangun sistem pemantauan sentimen dan evaluasi nasabah yang terukur, menerapkan arsitektur Zero Trust serta pengawasan ketat terhadap integrasi API dengan mitra fintech, dan merevolusi budaya organisasi melalui pelatihan kesadaran siber (cybersecurity culture) yang berkelanjutan bagi seluruh lini pegawai.

REFERENSI

Abdussamad, Z. (2021). Buku Metode Penelitian Kualitatif. Makassar: Syakir Media Press.

Adwiyah Hasibuan, R. (2023). Peranan Webform BSI Dalam Kemudahan Transaksi Online Di Bank Syariah Indonesia (BSI) KCP Medan Setia Budi. Trending: Jurnal Ekonomi, Akuntansi Dan Manajemen, 1(2), 95–107.

Aisah, S., & Kurniawan, R. (2023). Exploring Bank Syariah Indonesia and It's Customers Perceptions of Cyber Attacks. At-Taradhi: Jurnal Studi Ekonomi, 14(2), 117–132.

Ansori, A. (2016). Digitalisasi Ekonomi Syariah. Islamiconomic: Jurnal Ekonomi Islam, 7(1), 1–18.

Ayuning Tyas, L., & Purwanti, K. (2020). Pengaruh Adopsi E-Banking Dan Pengendalian Internal Terhadap Kinerja Keuangan Perbankan Syariah Di Indonesia. JIFA: Journal of Islamic Finance and Accounting, 3(2), 134–151.

Azhar, F. (2023). Analisis Strategi Komunikasi Bank Syariah Indonesia (BSI) dalam Penanganan Krisis Serangan Siber Perbankan. KLC: Kemenkeu Learning Center.

Blaney, J. R., Alwine, L., Benoit, W. L., Blosenhauer, J. D., Caldiero, C., Chewning, L. V., Cos, G. C., DiSanza, J., Gribas, J., Haigh, M. M., Halford, J., Lachlan, K., Legge, N. J., Montague, R. R., Omilion-Hodges, L. M., Sante, J. C., Spence, P. R., & Worrell, T. R. (2015). Putting Image Repair to the Test: Applications of Image Restoration. Lanham: Lexington Books.

Fitriani, R., Subagiyo, R., & Nur Asiyah, B. (2023). Mitigating IT Risk of Bank Syariah Indonesia: A Study of Cyber Attack on May 8, 2023. Al-Amwal: Jurnal Kajian Ekonomi Dan Perbankan Syariah, 15(1), 86–100.

Harahap, I. (2016). Peranan Perbankan Syariah dalam Upaya Peningkatan Kesejahteraan Masyarakat. At-Tijarah: Jurnal Ilmu Manajemen Dan Bisnis Islam, 2(1), 112–126.

Lengkong, S. L., Sondakh, M., & Londa, J. W. (2017). Strategi Public Relations dalam Pemulihan Citra Perusahaan (Studi Kasus Rumah Makan Kawan Baru Megamas Manado). Acta Diurna Komunikasi, 6(1), 1–11.

Maulana, B. R., & Nasrulloh, N. (2024). Analisis Strategi Pemulihan Citra Bank Syariah Indonesia Pasca Dugaan Serangan Siber. EKSISBANK: Ekonomi Syariah Dan Bisnis Perbankan, 8(1), 76–91. https://doi.org/10.37726/ee.v8i1.1123

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: Jurnal Ilmu Islam, 7(3), 1755–1768.

Maulana, N., Laurens, T., Faiz, H. A., & Patrianti, T. (2024). Manajemen Krisis PT. BSI Tbk Pasca Peretasan Data Nasabah. INNOVATIVE: Journal Of Social Science Research, 4(1), 8244–8258.

Muhammad, R. A., & Adawiyah, S. E. (2024). Manajemen Krisis Bank Syariah Indonesia Dalam Membentuk Citra Positif. TUTURAN: Jurnal Ilmu Komunikasi, Sosial Dan Humaniora, 2(2), 13–23.

Mulki, S. S., & Kurniadi, O. (2021). Strategi Komunikasi Krisis pada Masa Adaptasi Kebiasaan Baru di Bank Bukopin KCP Cianjur. JRPR: Jurnal Riset Public Relations, 1(1), 71–78.

Nasrulloh, N., Adiba, E. M., & Diar, T. R. (2022). Keengganan UMKM di Sekitar Wisata Religi dalam Mengambil Pembiayaan Bank Syariah: Sebuah Studi di Madura. Jurnal Ekonomi Syariah Teori Dan Terapan, 9(1), 34–46.

Nasrulloh, N., Adiba, E. M., & Efendi, M. N. (2023). Pengembangan Potensi Pariwisata Halal Pesisir Bangkalan Madura: Identifikasi Peranan Bank Syariah. Muslim Heritage: Jurnal Dialog Islam Dan Realitas, 8(1), 79–102.

Nurjanah, R. S. (2022). Wawancara Tentang Analisis Minat Mahasiswa Menggunakan Tabungan BSI. Mahasiswa Prodi Perbankan Syariah STIESIP.

Purba, R. P., & Ibrahim, M. (2017). Pengaruh Citra Perusahaan terhadap Loyalitas Pelanggan (Studi Kasus PT. Bintang Utara Perwakilan Dolok Sanggul). JOM: Jurnal Online Mahasiswa, 4(1), 1–13.

Putri, D. F., & Sari, W. R. (2023). Analisis Perlindungan Nasabah BSI terhadap Kebocoran Data dalam Menggunakan Digital Banking. JIEM: Jurnal Ilmiah Ekonomi Dan Manajemen, 1(4), 173–181.

Solikhawati, A., & Samsuri, A. (2023). Evaluasi Bank Syariah Indonesia Pasca Serangan Siber: Pergerakan Saham dan Kinerja. JIEI: Jurnal Ilmiah Ekonomi Islam, 9(3), 4201–4208.

Suharto, M. A., & Apriyani, M. N. (2021). Konsep Cyber Attack, Cyber Crime, Dan Cyber Warfare Dalam Aspek Hukum Internasional. Risalah Hukum, 17(2), 98–107.

Tambunan, N., Fitri Wulandari, A., Pangesti, A. N., Anggraini, A., Tunnaja, S., Dewi Gita, A., & Rusmarhadi, I. (2023). Berita Utama Tentang Error Service di Bank Syariah Indonesia (BSI). Community Development Journal: Jurnal Pengabdian Masyarakat, 4(2), 5096–5098.