EKSYA : Jurnal Ilmiah Ekonomi Syariah
Volume 3, Number 2, Januari 2026, Page 47 - 60
jurnal.iaih.ac.id/index.php/EKSYA
ISSN 3110-5424

ANALISIS KEGAGALAN MITIGASI RISIKO OPERASIONAL PADA BANK SYARIAH INDONESIA: STUDI KASUS SERANGAN RANSOMWARE LOCKBIT DAN IMPLIKASINYA TERHADAP KEAMANAN DATA NASABAH

Kaleksanan Ilham Hakqi Massani[1]
Institut Agama Islam Hasanuddin Pare
kaleksananihm@gmail.com

Ahmad Very Fadli[2]
Institut Agama Islam Hasanuddin Pare
ahmadveryfadli@gmail.com

Abstrak

Transformasi digital perbankan syariah menghadirkan tantangan keamanan siber yang serius, sebagaimana dibuktikan oleh insiden kelumpuhan layanan PT Bank Syariah Indonesia Tbk (BSI) akibat serangan *ransomware LockBit* pada Mei 2023. Penelitian ini bertujuan untuk menganalisis faktor penyebab kegagalan mitigasi risiko operasional pada kasus tersebut serta mengevaluasi dampaknya terhadap keamanan data nasabah. Menggunakan metode kualitatif studi kasus dengan teknik analisis akar masalah (*root cause analysis*) pada data sekunder, penelitian ini membedah kronologi insiden dan respons manajemen berdasarkan teori manajemen risiko perbankan syariah. Temuan utama menunjukkan bahwa kegagalan mitigasi disebabkan oleh lemahnya sistem deteksi dini (*early warning system*) dan ketidaksiapan protokol pemulihan bencana (*disaster recovery plan*), yang diperburuk oleh komunikasi krisis yang kurang transparan. Kebocoran 1,5 *Terabyte* data nasabah mengindikasikan pelanggaran terhadap prinsip kehati-hatian (*prudential banking*) dan amanah dalam menjaga privasi konsumen. Penelitian ini menyimpulkan bahwa insiden BSI bukan sekadar gangguan teknis, melainkan kegagalan tata kelola risiko operasional yang fundamental. Implikasi praktis dari studi ini menekankan urgensi transformasi arsitektur keamanan siber dari reaktif menjadi proaktif, serta penguatan regulasi perlindungan data untuk memulihkan kepercayaan publik terhadap ekosistem perbankan syariah di Indonesia.

Kata Kunci : Bank Syariah Indonesia, Keamanan Data Nasabah, Manajemen Risiko Operasional, Perbankan Syariah, Serangan Siber LockBit.

Abstract

The digital transformation of Islamic banking presents serious cybersecurity challenges, as evidenced by the service paralysis incident at PT Bank Syariah Indonesia Tbk (BSI) due to the LockBit ransomware attack in May 2023. This study aims to analyze the factors contributing to the failure of operational risk mitigation in this case and evaluate its impact on customer data security. Employing a qualitative case study method with root cause analysis on secondary data, this research examines the incident chronology and management response based on Islamic banking risk management theories. The main findings indicate that the mitigation failure was caused by a weak early warning system and the unpreparedness of the disaster recovery plan, exacerbated by a lack of transparency in crisis communication. The leakage of 1.5 Terabytes of customer data

indicates a violation of prudential banking principles and amanah (trustworthiness) in safeguarding consumer privacy. This study concludes that the BSI incident was not merely a technical disruption, but a fundamental failure of operational risk governance. The practical implications of this study emphasize the urgency of transforming cybersecurity architecture from reactive to proactive, alongside strengthening data protection regulations to restore public trust in Indonesia's Islamic banking ecosystem.
Keywords : *Bank Syariah Indonesia, Customer Data Security, Operational Risk Management, Islamic Banking, LockBit Cyber Attack.*

A. PENDAHULUAN

Transformasi digital dalam industri perbankan syariah bukan lagi sekadar pilihan, melainkan kebutuhan mendesak untuk mempertahankan daya saing dan efisiensi operasional. Integrasi teknologi memungkinkan bank syariah memperluas jangkauan layanan dan meningkatkan pengalaman nasabah. Namun, percepatan digitalisasi ini membawa konsekuensi inheren berupa peningkatan eksposur risiko operasional, khususnya ancaman siber. Bekti Widyaningsih, Ashlihah, dan Tolib Ibnu Afan menekankan bahwa dalam era digital yang terus berkembang, bank syariah menghadapi tantangan baru dalam menghadirkan layanan yang aman dan andal, di mana manajemen risiko memegang peran krusial untuk memastikan ketahanan institusi.[1] Kegagalan dalam memitigasi risiko ini tidak hanya berdampak pada kerugian finansial, tetapi juga reputasi dan kepercayaan yang menjadi fondasi utama perbankan syariah.

Fenomena risiko operasional akibat serangan siber menjadi sorotan publik ketika PT Bank Syariah Indonesia Tbk (BSI) mengalami gangguan layanan total pada 8 Mei 2023. Insiden ini disebabkan oleh serangan *ransomware* dari kelompok peretas *LockBit*, yang melumpuhkan akses nasabah terhadap layanan *mobile banking* dan ATM selama beberapa hari.[2] Lebih dari sekadar gangguan teknis, insiden ini bereskalasi menjadi krisis keamanan data ketika LockBit mengklaim telah mencuri 1,5 *Terabyte* data internal, termasuk informasi sensitif 15 juta nasabah, dan mempublikasikannya di *dark web* setelah negosiasi tebusan gagal.[3] Kasus ini menjadi preseden buruk dalam sejarah perbankan

[1] Bekti Widyaningsih dkk., "Peran Manajemen Resiko dalam Meningkatkan Ketahanan Bank Syariah di Era Digital," 1459.
[2] Balqis Fallahnda, "Kronologi LockBit Diduga Curi Data Nasabah BSI & Update Terkini," Tirto.id, 17 Mei 2023."
[3] CHAERUNISA, "PENGARUH KEPUASAN NASABAH, KUALITAS LAYANAN, DAN KEPERCAYAAN NASABAH TERHADAP LOYALITAS NASABAH BANK SYARIAH INDONESIA PASCA SERANGAN SIBER," 1.

ISSN 3110-5424

syariah Indonesia, mengingat BSI adalah entitas hasil merger bank syariah terbesar yang seharusnya memiliki infrastruktur keamanan mumpuni.

Secara teoretis, manajemen risiko operasional dalam perbankan syariah memiliki dimensi yang unik karena harus mematuhi prinsip-prinsip syariah selain regulasi konvensional. Hoirul Anam mendefinisikan risiko operasional sebagai risiko kerugian yang diakibatkan oleh proses internal yang kurang memadai, kegagalan sistem, kesalahan manusia, atau kejadian eksternal.[4] Dalam konteks syariah, pengelolaan risiko ini berkaitan erat dengan prinsip amanah dalam menjaga harta (*hifz al-mal*) dan privasi nasabah. Hamdi Agustin, Armis, dan Hasrizal Hasan menambahkan bahwa konsep manajemen risiko bank syariah harus dibangun di atas fondasi akidah yang benar serta mentalitas pegawai yang mencerminkan sifat *shidiq*, *fathonah*, amanah, dan tabligh.[5] Oleh karena itu, kegagalan sistem keamanan IT di BSI bukan hanya masalah teknis, melainkan juga indikasi adanya celah dalam penerapan prinsip kehati-hatian (*prudential banking*) dan kepatuhan syariah.

Tinjauan literatur terdahulu menunjukkan bahwa diskursus mengenai serangan siber pada perbankan syariah telah banyak dibahas, namun mayoritas terpolarisasi pada tiga kelompok topik utama. Pertama, kelompok penelitian yang berfokus pada dampak pasca-insiden terhadap citra dan reputasi. Bagus Restu Maulana dan Nasrulloh, misalnya, menganalisis strategi pemulihan citra BSI menggunakan *Situational Crisis Communication Theory* (SCCT) untuk memperbaiki persepsi publik setelah krisis.[6] Kedua, kelompok yang menyoroti aspek kinerja keuangan dan pasar modal, sebagaimana dilakukan oleh Anisa Solikhawati dan Andriani Samsuri yang mengevaluasi fluktuasi harga saham BRIS dan kinerja keuangan pasca serangan siber.[7] Ketiga, kelompok yang membahas perlindungan hukum dan loyalitas nasabah. Diana Afifah meneliti perlindungan konsumen sektor jasa keuangan dalam kasus *ransomware* BSI berdasarkan

[4] Anam, "Manajemen Risiko Operasional Bank Syariah; Teori dan Manfaat," 16.
[5] Agustin dkk., "TEORI MANAJEMEN RESIKO BANK SYARIAH," 1.
[6] Maulana dan Nasrulloh, *Analisis Strategi Pemulihan Citra Bank Syariah Indonesia Pasca Dugaan Serangan Siber*, 76.
[7] Solikhawati dan Samsuri, "Evaluasi Bank Syariah Indonesia Pasca Serangan Siber," 4201.

ISSN 3110-5424

regulasi OJK,[8] sementara Putri Chaerunisa mengkaji pengaruh kepercayaan dan persepsi keamanan terhadap loyalitas nasabah pasca serangan.[9]

Meskipun penelitian-penelitian tersebut telah memberikan wawasan berharga mengenai dampak dan penanganan pasca-krisis, terdapat kesenjangan penelitian (*research gap*) yang signifikan. Belum ada penelitian yang secara spesifik dan mendalam membedah "mengapa" dan "bagaimana" mitigasi risiko operasional di BSI bisa gagal mencegah penetrasi *ransomware LockBit* sejak awal, ditinjau dari kerangka kerja manajemen risiko operasional syariah. Penelitian terdahulu lebih banyak memotret *aftermath* (kejadian setelahnya), namun kurang mengeksplorasi kausalitas kegagalan sistem pertahanan preventif dan deteksi dini yang seharusnya menjadi benteng utama. Selain itu, implikasi spesifik dari kegagalan mitigasi ini terhadap keamanan data nasabah dari perspektif teknis-operasional belum banyak diulas secara komprehensif.

Berdasarkan latar belakang tersebut, penelitian ini bertujuan untuk: (1) Menganalisis faktor-faktor penyebab kegagalan mitigasi risiko operasional pada BSI dalam kasus serangan *ransomware LockBit*; (2) Mengevaluasi dampak kegagalan tersebut terhadap keamanan data nasabah; dan (3) Merumuskan strategi penguatan mitigasi risiko siber yang sesuai dengan prinsip perbankan syariah. Kontribusi teoretis penelitian ini diharapkan dapat memperkaya literatur manajemen risiko operasional perbankan syariah, khususnya terkait ancaman siber (*cyber risk*). Secara praktis, penelitian ini memberikan rekomendasi bagi praktisi perbankan dan regulator dalam menyusun kerangka kerja keamanan siber yang lebih tangguh (*resilient*).

Kebaruan (*novelty*) penelitian ini terletak pada pendekatan analisis akar masalah (*root cause analysis*) terhadap kegagalan prosedur mitigasi risiko operasional BSI yang spesifik pada serangan *LockBit*, yang belum banyak disentuh oleh peneliti sebelumnya. Rumusan masalah yang diajukan adalah: Bagaimana mekanisme kegagalan mitigasi risiko operasional terjadi pada kasus serangan ransomware di BSI dan apa implikasinya

[8] Afifah, "Perlindungan Konsumen di Sektor Jasa Keuangan pada Kasus Serangan Siber Ransomware yang Menimpa Perbankan," 9318.
[9] CHAERUNISA, "PENGARUH KEPUASAN NASABAH, KUALITAS LAYANAN, DAN KEPERCAYAAN NASABAH TERHADAP LOYALITAS NASABAH BANK SYARIAH INDONESIA PASCA SERANGAN SIBER," 2.

ISSN 3110-5424

terhadap keamanan data nasabah? Dengan demikian, penelitian ini diharapkan mampu mengisi *gap* literatur dengan menyediakan evaluasi kritis terhadap keandalan sistem operasional bank syariah di tengah ancaman kejahatan siber yang semakin canggih.

B. METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif dengan desain studi kasus (*case study*). Pendekatan kualitatif dipilih karena penelitian ini bertujuan untuk memahami fenomena kegagalan mitigasi risiko secara mendalam, berfokus pada proses "bagaimana" dan "mengapa" serangan *ransomware LockBit* dapat melumpuhkan sistem operasional Bank Syariah Indonesia (BSI). Desain studi kasus digunakan untuk mengeksplorasi suatu kejadian spesifik (insiden siber Mei 2023) dalam konteks kehidupan nyata, di mana batas antara fenomena dan konteksnya tidak tampak dengan tegas.

Metode ini selaras dengan penelitian terdahulu yang dilakukan oleh Bagus Restu Maulana dan Nasrulloh, yang menggunakan pendekatan kualitatif deskriptif untuk membedah strategi pemulihan citra pasca krisis di BSI.[10] Dalam penelitian ini, penulis tidak melakukan intervensi terhadap objek yang diteliti, melainkan menginterpretasikan data sekunder berupa kronologi kejadian dan fakta-fakta yang telah terpublikasi untuk dianalisis menggunakan kerangka teori manajemen risiko perbankan syariah. Sumber data dalam penelitian ini terbagi menjadi dua kategori utama, yaitu:

1. Data Primer (Dokumenter)

   Berupa arsip berita kronologis kejadian serangan *ransomware LockBit* terhadap BSI yang diterbitkan oleh media massa terpercaya (Tirto.id), serta rilis publik mengenai pengumuman kelompok peretas LockBit terkait pencurian 1,5 Terabyte data nasabah.
2. Data Sekunder (Literatur)

   Berupa jurnal-jurnal ilmiah yang relevan dengan topik manajemen risiko operasional, keamanan siber, dan perlindungan data nasabah. Referensi kunci

[10] Maulana dan Nasrulloh, *Analisis Strategi Pemulihan Citra Bank Syariah Indonesia Pasca Dugaan Serangan Siber*, 80.

ISSN 3110-5424

mencakup teori manajemen risiko operasional dari Hoirul Anam[11], serta analisis dampak serangan siber dari Putri Chaerunisa.[12]

Teknik pengumpulan data dilakukan melalui Studi Dokumentasi. Penulis mengumpulkan, mengklasifikasikan, dan mempelajari dokumen-dokumen tertulis yang berkaitan dengan masalah penelitian. Langkah-langkah pengumpulan data adalah sebagai berikut:

1. Inventarisasi Kronologi

   Mencatat urutan waktu kejadian (*timeline*) serangan *LockBit* dari tanggal 8 Mei 2023 hingga 15 Mei 2023 berdasarkan laporan berita investigatif.
2. Penelusuran Literatur

   Mengumpulkan jurnal ilmiah yang membahas teori manajemen risiko syariah dan studi kasus BSI untuk dijadikan pisau analisis.
3. Triangulasi Sumber

   Membandingkan pernyataan manajemen BSI di media dengan klaim peretas *LockBit* untuk mendapatkan gambaran objektif mengenai kegagalan sistem.

Analisis data dilakukan menggunakan model Analisis Akar Masalah (*Root Cause Analysis*) yang diadaptasi ke dalam deskripsi kualitatif. Teknik ini bertujuan mencari penyebab mendasar dari suatu masalah. Prosedur analisis terdiri dari tiga tahap:

1. Reduksi Data

   Memilah informasi dari berita yang relevan dengan aspek "kegagalan operasional" dan membuang informasi yang tidak relevan.
2. Penyajian Data (*Data Display*)

   Menyusun fakta-fakta kegagalan sistem dan respons manajemen dalam bentuk narasi kronologis yang sistematis.
3. Penarikan Kesimpulan (*Verification*)

[11] Anam, "Manajemen Risiko Operasional Bank Syariah; Teori dan Manfaat," 19.
[12] CHAERUNISA, "PENGARUH KEPUASAN NASABAH, KUALITAS LAYANAN, DAN KEPERCAYAAN NASABAH TERHADAP LOYALITAS NASABAH BANK SYARIAH INDONESIA PASCA SERANGAN SIBER," 45.

ISSN 3110-5424

Menganalisis fakta tersebut menggunakan teori Bekti Widyaningsih tentang peran manajemen risiko di era digital,[13] untuk menyimpulkan letak kegagalan mitigasi BSI, apakah berada pada level SDM (people), proses (process), atau teknologi (technology).

Untuk memastikan validitas data, penelitian ini menggunakan teknik Triangulasi Sumber Data. Penulis membandingkan informasi dari berita (fakta lapangan) dengan teori yang terdapat dalam jurnal ilmiah (konsep ideal). Hal ini dilakukan untuk memastikan bahwa analisis kegagalan operasional yang dihasilkan tidak hanya bersifat opini subjektif, tetapi memiliki landasan teoritis yang dapat dipertanggungjawabkan secara akademik sesuai standar literasi perbankan syariah yang dikemukakan oleh Hamdi Agustin dkk.[14]

C. HASIL DAN PEMBAHASAN

1. Analisis Kegagalan Mitigasi Risiko Operasional

Temuan penelitian berdasarkan kronologi fakta menunjukkan bahwa insiden bermula pada 8 Mei 2023 ketika seluruh layanan kanal digital BSI (*Mobile Banking* dan ATM) mengalami kelumpuhan total (*downtime*). Manajemen BSI pada awalnya mengklaim insiden tersebut sebagai kegiatan "pemeliharaan sistem" (*maintenance*). Namun, klaim ini terbantahkan ketika kelompok peretas *LockBit* mempublikasikan bukti pencurian 1,5 Terabyte data internal BSI.[15]

Dalam perspektif teori manajemen risiko perbankan syariah, insiden ini mengonfirmasi adanya kegagalan fundamental pada "Proses Internal" dan "Sistem Teknologi". Hoirul Anam menjelaskan bahwa risiko operasional didefinisikan sebagai risiko kerugian yang diakibatkan oleh proses internal yang kurang memadai, kesalahan manusia, kegagalan sistem, atau adanya kejadian eksternal yang mempengaruhi operasional bank.[16] Kasus BSI menunjukkan

[13] Bekti Widyaningsih dkk., "Peran Manajemen Resiko dalam Meningkatkan Ketahanan Bank Syariah di Era Digital," 1462.
[14] Agustin dkk., "TEORI MANAJEMEN RESIKO BANK SYARIAH," 492.
[15] Balqis Fallahnda, "Kronologi LockBit Diduga Curi Data Nasabah BSI & Update Terkini," Tirto.id, 17 Mei 2023."
[16] Anam, "Manajemen Risiko Operasional Bank Syariah; Teori dan Manfaat," 16.

ISSN 3110-5424

bahwa sistem pertahanan siber (*cyber defense*) bank tidak mampu mendeteksi intrusi *malware* sejak dini. *LockBit* bahkan mengklaim telah berada di dalam jaringan BSI selama dua bulan sebelum melancarkan enkripsi, yang mengindikasikan lemahnya sistem pemantauan (*monitoring*) dan *Intrusion Detection System* (IDS).

Kegagalan ini bertentangan dengan prinsip *prudential banking* (kehati-hatian) yang menjadi syarat mutlak operasional bank syariah. Bekti Widyaningsih dkk. menegaskan bahwa di era digital, manajemen risiko bukan hanya pelengkap, melainkan fondasi ketahanan (*resilience*) institusi. Kegagalan teknologi di BSI membuktikan bahwa transformasi digital yang dilakukan belum diimbangi dengan mitigasi risiko yang setara, sehingga menciptakan celah kerentanan yang fatal.[17]

Secara kritis, penulis menilai bahwa respons awal manajemen yang menyebut "*maintenance*" alih-alih mengakui serangan siber mencerminkan ketidaksiapan protokol komunikasi krisis. Hal ini berpotensi melanggar prinsip *Shidiq* (jujur/benar) dalam manajemen syariah sebagaimana dikemukakan oleh Hamdi Agustin. Manajemen risiko syariah seharusnya dibangun di atas akidah yang benar dan sifat transparansi, bukan menutup-nutupi fakta yang justru memperburuk spekulasi publik.[18]

2. Implikasi Kebocoran Data Terhadap Keamanan Nasabah dan Aspek Legal

Temuan kedua menyoroti dampak serangan terhadap keamanan data nasabah. *LockBit* merilis sampel data yang mencakup informasi sensitif 15 juta nasabah, termasuk nama, nomor telepon, saldo rekening, hingga riwayat transaksi. Kebocoran ini menempatkan nasabah pada risiko tinggi tindak kejahatan lanjutan seperti *social engineering* dan penipuan digital.

Analisis hukum menunjukkan bahwa posisi BSI sangat lemah dalam aspek perlindungan konsumen. Diana Afifah dalam penelitiannya menyebutkan bahwa berdasarkan POJK Nomor 6/POJK.07/2022, Bank wajib menjaga kerahasiaan dan keamanan data konsumen. Serangan *ransomware* yang berujung pada data leak

[17] Bekti Widyaningsih dkk., "Peran Manajemen Resiko dalam Meningkatkan Ketahanan Bank Syariah di Era Digital," 1460.
[18] Agustin dkk., "TEORI MANAJEMEN RESIKO BANK SYARIAH," 488.

ISSN 3110-5424

dikategorikan sebagai kegagalan bank dalam menyediakan sistem elektronik yang andal.[19] Lebih lanjut, BSI juga berpotensi melanggar Undang-Undang Perlindungan Konsumen karena tidak memberikan informasi yang benar, jelas, dan jujur mengenai kondisi keamanan dana dan data nasabah pada saat insiden terjadi.

Implikasi dari kebocoran data ini secara langsung menggerus kepercayaan (*trust*) yang merupakan modal utama perbankan. Putri Chaerunisa menemukan bahwa persepsi keamanan memiliki pengaruh signifikan terhadap loyalitas nasabah. Ketika nasabah merasa datanya tidak aman, loyalitas mereka menurun drastis, yang terbukti dari banyaknya keluhan dan ancaman penarikan dana (*rush money*) di media sosial pasca insiden.[20] Dalam konteks syariah, kegagalan menjaga data nasabah adalah pelanggaran terhadap amanah. Bank syariah tidak hanya bertanggung jawab secara hukum positif, tetapi juga secara teologis untuk menjaga harta (*hifz al-mal*) dan privasi (*hifz al-ird*) nasabahnya.

3. Evaluasi Strategi Pemulihan dan Rekonstruksi Citra

Setelah mengakui adanya gangguan akibat serangan siber, BSI melakukan serangkaian langkah pemulihan sistem dan citra. Bagus Restu Maulana dan Nasrulloh menganalisis langkah ini menggunakan *Situational Crisis Communication Theory* (SCCT). Ditemukan bahwa BSI cenderung menggunakan strategi *diminish* (pengurangan dampak) dengan narasi bahwa "dana nasabah aman" untuk menenangkan kepanikan, namun kurang menekankan pada strategi *rebuild* (membangun ulang) berupa kompensasi yang jelas bagi nasabah yang dirugikan.[21]

Penelitian ini mengkritik bahwa pemulihan teknis saja tidak cukup tanpa diikuti pemulihan aspek *governance*. Anisa Solikhawati mencatat bahwa meskipun kinerja keuangan (seperti rasio BOPO dan ROA) BSI masih tercatat baik pasca serangan, namun pergerakan saham BRIS sempat mengalami fluktuasi

[19] Afifah, "Perlindungan Konsumen di Sektor Jasa Keuangan pada Kasus Serangan Siber Ransomware yang Menimpa Perbankan," 9320.
[20] CHAERUNISA, "PENGARUH KEPUASAN NASABAH, KUALITAS LAYANAN, DAN KEPERCAYAAN NASABAH TERHADAP LOYALITAS NASABAH BANK SYARIAH INDONESIA PASCA SERANGAN SIBER," 45.
[21] Maulana dan Nasrulloh, *Analisis Strategi Pemulihan Citra Bank Syariah Indonesia Pasca Dugaan Serangan Siber*, 82–83.

ISSN 3110-5424

negatif akibat efek kepanikan investor.[22] Hal ini menunjukkan bahwa risiko operasional (serangan siber) memiliki korelasi kuat dengan risiko reputasi dan risiko pasar.

Sebagai solusi perbaikan, Rita Dwi Nur Indah Sari menyarankan transformasi sistem keamanan dengan penggunaan teknologi baru yang lebih adaptif terhadap ancaman siber yang terus berevolusi.[23] Bank Syariah Indonesia perlu merevisi Arsitektur Keamanan Siber mereka dengan mengadopsi standar internasional seperti ISO 27001 secara substantif, bukan sekadar administratif, serta memperkuat *Human Firewall* (edukasi SDM) agar tidak menjadi pintu masuk serangan siber di masa depan.

D. KESIMPULAN DAN SARAN

KESIMPULAN

Berdasarkan analisis kualitatif terhadap kronologi dan fakta serangan *ransomware LockBit*, penelitian ini menyimpulkan bahwa insiden kelumpuhan layanan PT Bank Syariah Indonesia Tbk (BSI) pada Mei 2023 bukan sekadar gangguan teknis semata, melainkan manifestasi dari kegagalan fundamental dalam mitigasi risiko operasional. Kegagalan ini terletak pada ketidakmampuan sistem pertahanan siber bank dalam mendeteksi intrusi *malware* secara dini, yang mengindikasikan lemahnya pengawasan pada aspek "Proses Internal" dan "Sistem Teknologi" sebagaimana didefinisikan dalam teori risiko operasional Hoirul Anam.[24] Keterlambatan manajemen dalam mengakui serangan siber dan penggunaan narasi "pemeliharaan sistem" di awal krisis justru memperburuk ketidakpastian dan mencederai prinsip transparansi (*tabligh*) yang menjadi etika bisnis Islam.

Temuan selanjutnya menegaskan bahwa kegagalan mitigasi tersebut memiliki implikasi serius terhadap keamanan data nasabah dan aspek legalitas. Bocornya 1,5 *Terabyte* data yang mencakup informasi sensitif 15 juta nasabah membuktikan bahwa BSI belum sepenuhnya mampu menjalankan amanah perlindungan konsumen sesuai standar regulasi Otoritas Jasa Keuangan (OJK). Hal ini berdampak langsung pada

[22] Solikhawati dan Samsuri, "Evaluasi Bank Syariah Indonesia Pasca Serangan Siber," 4202.
[23] SARI, "PENGARUH TRANSFORMASI SISTEM KEAMANAN DAN PENGGUNAAN TEKNOLOGI BARU TERHADAP SERANGAN SIBER PADA DATA NASABAH," 1.
[24] Anam, "Manajemen Risiko Operasional Bank Syariah; Teori dan Manfaat," 16.

ISSN 3110-5424

penurunan tingkat kepercayaan nasabah (*trust*), di mana nasabah merasa hak privasi mereka terlanggar. Sebagaimana temuan Putri Chaerunisa, persepsi keamanan yang rendah pasca serangan siber berkorelasi negatif terhadap loyalitas nasabah, yang berpotensi memicu risiko reputasi jangka panjang.[25]

Terakhir, strategi pemulihan yang diterapkan BSI pasca insiden dinilai lebih berfokus pada stabilisasi layanan teknis dan kinerja keuangan, namun kurang optimal dalam memulihkan aspek psikologis nasabah. Meskipun kinerja saham dan rasio keuangan BSI terbukti tangguh (*resilient*) dan kembali stabil dalam jangka pendek seperti diungkapkan oleh Anisa Solikhawati,[26] namun langkah mitigasi krisis komunikasi yang diambil belum sepenuhnya mampu meyakinkan publik mengenai jaminan keamanan data di masa depan.

SARAN

Berdasarkan kesimpulan di atas, penulis merumuskan beberapa saran bagi praktisi perbankan dan peneliti selanjutnya:

1. Bagi Praktisi Perbankan Syariah

   Disarankan untuk melakukan transformasi arsitektur keamanan siber dari yang bersifat reaktif menjadi proaktif. BSI perlu mengadopsi teknologi keamanan terbaru yang adaptif terhadap ancaman *ransomware*, serta melakukan audit forensik IT secara berkala oleh pihak independen. Selain itu, penguatan "*Human Firewall*" melalui edukasi rutin kepada SDM internal mutlak diperlukan untuk menutup celah *human error*. Rita Dwi Nur Indah Sari menekankan bahwa transformasi sistem keamanan yang komprehensif adalah kunci untuk mencegah berulangnya serangan serupa.[27]
2. Bagi Regulator

[25] CHAERUNISA, "PENGARUH KEPUASAN NASABAH, KUALITAS LAYANAN, DAN KEPERCAYAAN NASABAH TERHADAP LOYALITAS NASABAH BANK SYARIAH INDONESIA PASCA SERANGAN SIBER," 45.
[26] Solikhawati dan Samsuri, "Evaluasi Bank Syariah Indonesia Pasca Serangan Siber," 4207.
[27] SARI, "PENGARUH TRANSFORMASI SISTEM KEAMANAN DAN PENGGUNAAN TEKNOLOGI BARU TERHADAP SERANGAN SIBER PADA DATA NASABAH," 2.

ISSN 3110-5424

Perlu adanya penegakan aturan yang lebih ketat terkait sanksi bagi lembaga jasa keuangan yang gagal menjaga data nasabah, guna memberikan efek jera dan mendorong kepatuhan terhadap UU Perlindungan Data Pribadi.

3. Bagi Peneliti Selanjutnya

Penelitian ini memiliki keterbatasan karena hanya berfokus pada analisis kualitatif dokumen berita dan literatur dalam kurun waktu singkat pasca kejadian. Peneliti selanjutnya disarankan untuk memperluas objek penelitian dengan menggunakan metode kuantitatif guna mengukur dampak finansial jangka panjang (misalnya: *migration rate* nasabah ke bank lain setahun setelah insiden) atau membandingkan strategi mitigasi siber antara Bank Umum Syariah (BUS) dengan Bank Umum Konvensional (BUK) untuk melihat efektivitas model manajemen risiko yang berbeda.

ISSN 3110-5424

Daftar Pustaka

Adiyes Putra, Popi, Agus, dan Saparuddin. "PENERAPAN MANAJEMEN RESIKO LIKUIDITAS PADA BANK SYARIAH." *Jurnal Tabarru': Islamic Banking and Finance* 6, no. 1 (2023): 81–91. https://doi.org/10.25299/jtb.2023.vol6(1).11649.

Afifah, Diana. "Perlindungan Konsumen di Sektor Jasa Keuangan pada Kasus Serangan Siber Ransomware yang Menimpa Perbankan." *JIIP - Jurnal Ilmiah Ilmu Pendidikan* 6, no. 11 (2023): 9318–23. https://doi.org/10.54371/jiip.v6i11.3176.

Agustin, Hamdi, Armis, dan Hasrizal Hasan. "TEORI MANAJEMEN RESIKO BANK SYARIAH." *Jurnal Tabarru': Islamic Banking and Finance* 5, no. 2 (2022): 551–64. https://doi.org/10.25299/jtb.2022.vol5(2).11251.

Anam, Hoirul. "Manajemen Risiko Operasional Bank Syariah; Teori dan Manfaat." *Jurnal At-Tamwil: Kajian Ekonomi Syariah* 5, no. 1 (2023): 16–31. https://doi.org/10.33367/at.v5i1.1476.

Balqis Fallahnda. "Kronologi LockBit Diduga Curi Data Nasabah BSI & Update Terkini," Tirto.id, 17 Mei 2023." *Tirto.id*, t.t. https://www.google.com/search?q=https://tirto.id/kronologi-lockbit-diduga-curi-data-nasabah-bsi-update-terkini-gHjS.

Bekti Widyaningsih, Ashlihah, dan Tolib Ibnu Afan. "Peran Manajemen Resiko dalam Meningkatkan Ketahanan Bank Syariah di Era Digital." *Jurnal Masharif Al-Syariah: Jurnal Ekonomi dan Perbankan Syariah* 9, no. 3 (2024). https://doi.org/10.30651/jms.v9i3.22933.

CHAERUNISA, PUTRI. "PENGARUH KEPUASAN NASABAH, KUALITAS LAYANAN, DAN KEPERCAYAAN NASABAH TERHADAP LOYALITAS NASABAH BANK SYARIAH INDONESIA PASCA SERANGAN SIBER." Skripsi, UNIVERSITAS ISLAM INDONESIA YOGYAKARTA, 2024.

ISSN 3110-5424

Fasa, Muhammad Iqbal. *MANAJEMEN RESIKO PERBANKAN SYARIAH DI INDONESIA*. 2016.

Hardinata, Michelle Jefelyn, Shanty Shanty, Yesica Yentelina Sitohang, Indah Anggun Rahma, Setiyo Utomo, dan Sofwan Rizko Ramadoni. "Sosialisasi Kebijakan Bank Digital: Perlindungan Hukum Terhadap Data Nasabah Dari Risiko Serangan Siber." *RENATA: Jurnal Pengabdian Masyarakat Kita Semua* 2, no. 2 (2024). https://doi.org/10.61124/1.renata.53.

Hidayat, Wahyu. "Implementasi Manajemen Resiko Syariah Dalam Koperasi Syariah." *Jurnal Asy-Syukriyyah* 20, no. 2 (2019): 30–50. https://doi.org/10.36769/asy.v20i2.80.

Iskandar, Iskandar, Amiur Nuruddin, dan Saparuddin Siregar. "[No title found]." *Al-Ulum* 17, no. 1 (2017). https://doi.org/10.30603/au.v17i1.25.

Maulana, Bagus Restu, dan Nasrulloh Nasrulloh. *Analisis Strategi Pemulihan Citra Bank Syariah Indonesia Pasca Dugaan Serangan Siber*. 8 (2024).

Parulian, Sahat, Devi Anassalifa Pratiwi, dan Meiliya Cahya Yustina. *Ancaman dan Solusi Serangan Siber di Indonesia*. t.t.

Restika, Restika, dan Era Sonita. "TANTANGAN KEAMANAN SIBER DALAM MANAJEMEN LIKUIDITAS BANK SYARIAH : MENJAGA STABILITAS KEUANGAN DI ERA DIGITAL." *Krigan: Journal of Management and Sharia Business* 1, no. 2 (2023): 25. https://doi.org/10.30983/krigan.v1i2.7929.

SARI, RITA DWI NUR INDAH. "PENGARUH TRANSFORMASI SISTEM KEAMANAN DAN PENGGUNAAN TEKNOLOGI BARU TERHADAP SERANGAN SIBER PADA DATA NASABAH." Skripsi, INSTITUT AGAMA ISLAM NEGERI CURUP, 2025.

Solikhawati, Anisa, dan Andriani Samsuri. "Evaluasi Bank Syariah Indonesia Pasca Serangan Siber: Pergerakan Saham dan Kinerja." *Jurnal Ilmiah Ekonomi Islam* 9, no. 3 (2023): 4201. https://doi.org/10.29040/jiei.v9i3.10309.

ISSN 3110-5424