Maliki Interdisciplinary Journal (MIJ) eISSN: 3024-8140
Volume 4, Issue February, 2026 pp. 211-218 http://urj.uin-malang.ac.id/index.php/mij/index

Penerapan manajemen risiko terhadap serangan siber: studi kasus bank syariah indonesia (BSI)

Azhar Zahira Ramadhan
Program Studi Perbankan Syariah, Universitas Islam Negeri Maulana Malik Ibrahim
e-mail: azharzahira15@gmail.com

Kata Kunci:
Inovasi, digital, perbankan syariah, manajemen risiko, serangan siber

Keywords:
Innovation, digital, islamic banking, *risk management*, cyberattack

A B S T R A K

Penelitian ini bertujuan untuk menganalisis penerapan manajemen risiko terhadap serangan siber yang dialami oleh Bank Syariah Indonesia (BSI) pada Mei 2023. Serangan ransomware LockBit 3.0 menyebabkan gangguan layanan besar, kebocoran data sensitif, serta menurunnya kepercayaan nasabah dan reputasi perusahaan. Penelitian menggunakan pendekatan kualitatif deskriptif dengan metode studi kasus. Hasil menunjukkan bahwa BSI menerapkan berbagai strategi mitigasi seperti penguatan infrastruktur teknologi, evaluasi kebijakan keamanan data, komunikasi krisis yang terbuka, dan pemberian kompensasi kepada nasabah terdampak. Penanganan yang dilakukan memperlihatkan peran penting manajemen risiko dalam menjaga stabilitas dan keberlanjutan operasional bank di era digital. Studi ini memberikan wawasan penting bagi lembaga keuangan lainnya dalam menghadapi ancaman serangan siber yang kian kompleks.

A B S T R A C T

This study aims to analyze the application of risk management in response to the cyberattack experienced by Bank Syariah Indonesia (BSI) in May 2023. The LockBit 3.0 ransomware attack caused major service disruptions, leakage of sensitive data, and a decline in public trust and corporate reputation. The research adopts a descriptive qualitative approach using a case study method. Results show that BSI implemented several mitigation strategies, including strengthening IT infrastructure, revising data security policies, transparent crisis communication, and compensating affected customers. These efforts highlight the crucial role of risk management in maintaining operational stability and business continuity in the digital era. This study provides valuable insights for other financial institutions to address increasingly complex cyber threats.

Pendahuluan

Transformasi digital kini menjadi fondasi penting dalam mendorong kemajuan di perbankan syariah secara global. Di tengah pesatnya perkembangan teknologi dalam kehidupan sehari-hari, bank syariah dituntut untuk terus berinovasi dan menyesuaikan diri dengan tuntutan layanan perbankan yang serba digital. Harapan nasabah terhadap layanan yang cepat, efisien, dan mudah diakses mendorong bank syariah untuk memanfaatkan teknologi digital dalam setiap aktivitas operasionalnya. Digitalisasi tidak hanya memberikan nilai tambah dalam meningkatkan kualitas layanan nasabah, tetapi juga membuka peluang bagi pengembangan layanan yang lebih luas dan inovatif. Transformasi digital dalam perbankan syariah dapat meningkatkan aksesibilitas layanan

keuangan bagi masyarakat, terutama di daerah yang sebelumnya kurang terjangkau oleh sistem keuangan (Aziz et al., 2025).

Digitalisasi dalam sektor perbankan tidak hanya membawa manfaat, tetapi juga menghadirkan tantangan baru, khususnya dalam hal keamanan siber. Ancaman seperti *ransomware*, *phising*, dan kebocoran data menjadi tantangan yang harus dihadapi oleh institusi keuangan, termasuk bank syariah. Serangan siber terhadap sektor perbankan meningkat secara drastis, dengan banyak institusi yang menjadi target utama (Widya et al., 2025). Meskipun transformasi digital membawa banyak manfaat, namun risiko yang muncul tetap perlu diperhatikan dan dikelola dengan tepat. Keamanan siber menjadi isu yang sangat penting, mengingat data nasabah yang sensitif dan transaksi keuangan yang dilakukan secara *online* (Akbar, 2023).

Serangan siber tidak hanya menimbulkan dampak teknis, tetapi juga berimplikasi pada menurunnya tingkat kepercayaan masyarakat terhadap lembaga keuangan. Reputasi bank yang menjadi korban dapat mengalami penurunan, yang selanjutnya berdampak negatif terhadap kinerja finansial dan nilai sahamnya. Insiden semacam ini berpotensi menyebabkan penurunan yang tajam pada harga saham serta mendorong nasabah untuk berpindah ke lembaga keuangan lain yang dianggap lebih aman (Rezki, 2023). Oleh karena itu, bank syariah perlu memberikan perhatian tidak hanya pada digitalisasi, tetapi juga pada penguatan sistem keamanan siber demi menjaga perlindungan data nasabah dan mempertahankan citra perusahaan.

Seperti yang terjadi pada tahun 2023, serangan siber terhadap Bank Syariah Indonesia (BSI) menjadi fokus utama dalam pembahasan mengenai celah keamanan yang ada, tetapi juga menunjukkan dampak besar yang dapat ditimbulkan oleh serangan siber terhadap bank syariah di Indonesia. Serangan tersebut menyebabkan gangguan layanan yang signifikan dan menimbulkan kekhawatiran di kalangan nasabah, yang berpotensi mengurangi kepercayaan terhadap sistem perbankan syariah secara keseluruhan (Nurul Monika Larasati & Rayyan Firdaus, 2024). Dalam menghadapi tantangan ini, bank syariah perlu merancang strategi yang menyeluruh dalam mengelola risiko terkait keamanan siber. Langkah-langkah ini harus melibatkan penguatan infrastruktur teknologi, pelatihan bagi staf, serta peningkatan kesadaran nasabah mengenai pentingnya keamanan siber. Dengan begitu bank syariah dapat beroperasi secara aman dan efisien di tengah tantangan di era digital ini, serta menjaga kepercayaan nasabah dan reputasi perusahaan (Ardhianty & Semarang, 2025).

Keberhasilan transformasi digital tidak hanya ditentukan oleh penerapan teknologi, tetapi juga oleh kemampuan dalam mengelola risiko yang muncul akibat penggunaan teknologi tersebut. Oleh karena itu, penelitian ini bertujuan untuk menganalisis penerapan manajemen risiko terhadap serangan siber yang dialami oleh Bank Syariah Indonesia (BSI) serta mengkaji efektivitas strategi mitigasi risiko dan komunikasi krisis BSI dalam menjaga stabilitas dan kepercayaan nasabah. Pendekatan yang digunakan dalam penelitian ini ialah kualitatif deskriptif dengan studi kasus di BSI menjadi fokus utama. Selain itu, kajian literatur dan analisis data sekunder dari laporan media, publikasi akademik, serta laporan kinerja BSI akan dilakukan untuk mendukung analisis yang lebih mendalam. Dengan demikian, penelitian ini diharapkan dapat

memberikan wawasan berharga bagi bank syariah untuk menghadapi tantangan transformasi digital dan meningkatkan ketahanan terhadap ancaman siber.

Pembahasan

Serangan Siber Terhadap Bank Syariah Indonesia

Kronologi Serangan Ransomware Oleh LockBit 3.0

Pada tanggal 8 Mei 2023, Bank syariah Indonesia (BSI) mengalami gangguan serius akibat serangan siber yang dilakukan oleh kelompok *ransomware* LockBit 3.0 yang berhasil mengakses sistem internal bank. Serangan ini bermula dari email *phising* yang berhasil mengeksploitasi kerentanan pada salah satu akun karyawan BSI. Melalui akses tersebut peretas berhasil masuk ke sistem internal, mengenkripsi sistem, data penting dan meminta tebusan dalam bentuk *cryptocurrency*. Insiden ini berlangsung selama beberapa hari sebelum terdeteksi oleh tim keamanan siber internal. Awalnya, gangguan pada sistem layanan disangka sebagai bagian dari proses pemeliharaan rutin. Namun, seiring berjalannya waktu, diketahui bahwa gangguan tersebut disebabkan oleh serangan siber yang terencana. Tim IT BSI kemudian berupaya memulihkan sistem, namun prosesnya terkendala oleh kompleksitas serangan dan kurangnya kesiapan dalam menghadapi situasi semacam ini (Solikhawati & Samsuri, 2023).

Pada tanggal 13 Mei 2023, kelompok LockBit 3.0 menyatakan diri sebagai pihak yang melakukan serangan dan mengancam akan menyebarkan data nasabah jika tuntutan mereka tidak dipenuhi. Menurut Alfons Tanujaya, pakar keamanan siber, aksi ini dilakukan secara sistematis dan tersembunyi, dengan memanfaatkan momen libur lebaran untuk menghindari perhatian dari tim keamanan. Data yang dicuri diperkirakan mencapai 1,5 *terabyte* (TB), yang menunjukkan bahwa serangan ini bukan bersifat acak, melainkan telah dirancang dengan perencanaan matang dan tingkat kehati-hatian tinggi (Ghozali et al., 2024). Pada awalnya, BSI menyampaikan bahwa gangguan layanan yang terjadi disebabkan oleh pemeliharaan sistem. Namun, setelah dilakukan penelusuran lebih lanjut, pihak bank mengakui bahwa insiden tersebut merupakan akibat dari serangan siber, dan menyatakan telah melakukan koordinasi dengan Badan Siber dan Sandi Negara (BSSN), Otoritas Jasa Keuangan (OJK), serta Bank Indonesia (BI) dalam rangka investigasi dan upaya pemulihan sistem (Nugroho, 2023).

Kebocoran Data Nasabah Dan Reaksi Publik

Pada tanggal 16 Mei 2023, terungkap bahwa serangan tersebut telah mengakibatkan kebocoran data dalam skala besar, mencakup jutaan informasi pribadi milik nasabah dan karyawan BSI. Informasi yang bocor meliputi nama lengkap, alamat, nomor telepon, hingga rincian akun perbankan, yang sangat rentan untuk disalahgunakan. Insiden ini menuai respons negatif dari publik. Bayak nasabah menyuarakan hilangnya kepercayaan terhadap BSI akibat lemahnya perlindungan data

dan kurangnya transparansi dalam penanganan insiden tersebut. Media dan regulator juga memberikan sorotan tajam terhadap lambannya respons yang diberikan oleh pihak bank. Hal ini mendorong tekanan bagi BSI untuk memperkuat sistem keamanannya dan memberikan jaminan perlindungan data yang lebih baik dimasa mendatang (Zulfikar et al., 2024).

Dampak Serangan Terhadap Reputasi dan Kinerja Bank Syariah Indonesia

Pengaruh Terhadap Kepercayaan Publik dan Saham BRIS

Serangan siber ini sangat berdampak pada kepercayaan publik terhadap BSI. Banyak nasabah yang mempertimbangkan untuk memindahkan dana mereka ke bank lain, yang berpotensi mengurangi pangsa pasar BSI. Penurunan kepercayaan ini tidak hanya mempengaruhi nasabah perorangan, tetapi juga dapat berdampak pada hubungan BSI dengan mitra bisnis dan investor. Ketidakpastian yang ditimbulkan oleh serangan ini dapat menyebabkan investor ragu untuk berinvestasi lebih lanjut, yang pada akhirnya dapat mempengaruhi pertumbuhan dan ekspektasi bank di masa depan (Alfattah & Adawiyah, 2024).

Selain itu, reputasi BSI sebagai lembaga keuangan yang aman dan terpercaya juga terancam. Dalam industri perbankan, reputasi adalah aset yang sangat berharga. Ketika nasabah merasa bahwa data dan dana mereka tidak aman, mereka cenderung mencari alternatif lain. hal ini dapat menyebabkan penurunan jumlah nasabah dan pada akhirnya mempengaruhi pendapatan bank. Penurunan harga saham Bank Syariah Indonesia (BRIS) setlah serangan ini, mencerminkan reaksi pasar yang negatif terhadap insiden tersebut, yang menunjukkan bahwa investor sangat memperhatikan aspek keamanan siber dalam menilai kinerja bank (Putri et al., 2023).

Respons Pasar dan Media Serta Tekanan Politik dan Regulasi

Insiden ini mendapatkan perhatian luas dari media, yang banyak mengangkat berbagai analisis terkait kelemahan dalam sistem keamanan siber BSI. Isu mengenai kebocoran data serta terganggunya layanan menjadi fokus utama pemberitaan dan berpotensi memengaruhi persepsi publik terhadap reputasi bank. Merespons situasi tersebut, otoritas pengawas perbankan mulai melakukan audit terhadap kebijakan keamanan siber yang diterapkan oleh BSI, sehingga meningkatkan tekanan agar dilakukan perbaikan sistem secara menyeluruh. Kondisi ini turut menciptakan ketidakpastian di pasar, di mana para investor dan nasabah menantikan langkah-langkah strategis yang diambil oleh BSI untuk mengatasi krisis (B. R. Maulana & Nasrulloh, 2024).

Dalam situasi semacam ini, sangat penting bagi BSI untuk menjaga komunikasi yang transparan dengan publik dan para pemangku kepentingan. Komunikasi yang tepat dan terbuka dapat membantu meredam kekhawatiran serta memulihkan kepercayaan. Oleh karena itu, BSI perlu menyusun strategi komunikasi krisis yang terstruktur, mencakup pernyataan resmi serta pembaruan rutin terkait langkah-langkah

pemulihan yang dilakukan. Dengan pendekatan ini, BSI dapat menunjukkan komitmennya dalam memperkuat sistem keamanan serta menjaga perlindungan data nasabah (Hardeva, 2023).

Penerapan Manajemen Risiko di Bank Syariah Indonesia

Setelah mengalami serangan siber pada tanggal 8 Mei 2023, Bank Syariah Indonesia (BSI) menghadapi tantangan besar dalam mengelola risiko yang muncul akibat peristiwa tersebut. Penerapan manajemen risiko yang efektif menjadi sangat penting untuk memulihkan kepercayaan nasabah dan menjaga stabilitas operasional bank. Dalam hal ini, BSI telah menerapkan berbagai langkah strategis untuk memperkuat sistem pengelolaan risikonya.

Penguatan Infrastruktur dan Sistem Keamanan Siber

Setelah mengalami serangan siber pada Mei 2023, Bank Syariah Indonesia (BSI) segera melakukan berbagai langkah untuk memperkuat sistem keamanan digital dan manajemen risikonya. Salah satu langkah utama adalah dengan meningkatkan infrastruktur teknologi dan keamanan digital. Peningkatan ini diwujudkan dengan mengalokasikan dana di bidang teknologi hingga Rp 580 miliar, lebih dari dua kali lipat dibanding tahun sebelumnya. Dana ini digunakan untuk memperbarui sistem antivirus, memperkuat sistem pencadangan data (backup), serta melakukan pengujian keamanan oleh pihak ketiga yang independen. Hal ini menunjukkan bahwa BSI menyadari pentingnya menjaga keamanan digital secara berkelanjutan demi kelangsungan operasional jangka panjang (Hassandi et al., 2025). Selain itu, BSI juga melakukan perubahan dalam struktur manajemennya dengan menunjuk direktur baru yang fokus pada teknologi dan manajemen risiko. Langkah ini menunjukkan keseriusan BSI dalam meningkatkan pengawasan terhadap ancaman siber, serta memperbaiki tata kelola risiko secara menyeluruh, bukan hanya dari sisi teknologi saja (Sari et al., 2024).

Impelementasi strategi pemulihan dan komunikasi krisis

Dalam upaya pemulihan, BSI mengambil langkah pemulihan secara bertahap guna memastikan sistem kembali berjalan dengan aman sebelum dioperasikan sepenuhnya. Upaya ini diiringi dengan peningkatan keamanan teknologi informasi melalui penguatan sistem perlindungan data serta penerapan prosedur pemulihan bencana (disaster recovery) demi kelangsungan operasional. BSI juga menjalin kerja sama dengan berbagai lembaga seperti BSSN, OJK, dan Bank Indonesia untuk memperkuat koordinasi dan meningkatkan kepercayaan publik. Dalam aspek komunikasi krisis, BSI menyampaikan pernyataan resmi melalui media massa dan media sosial yang berisi permintaan maaf, penjelasan gangguan, serta jaminan keamanan dana dan data nasabah (Tannavaro & Wiraguna, 2025). Pendekatan yang digunakan mengacu pada *teori Situational Crisis Communication Theory* (SCCT), khususnya strategi *rebuild* yang

menekankan pentingnya tanggung jawab, empati, serta keterbukaan dalam menyampaikan proses pemulihan. Meskipun pada awalnya komunikasi dinilai lambat dan terlalu teknis, perbaikan yang dilakukan pada tahap berikutnya menunjukkan komitmen perusahaan dalam memulihkan kepercayaan nasabah. Sebagai bentuk tanggung jawab lebih lanjut, BSI juga memberikan kompensasi kepada nasabah yang terdampak, dengan nilai mencapai 20 juta euro atau sekitar 320 miliar rupiah, sebagai wujud tanggung jawab institusi (N. Maulana et al., 2024).

Evaluasi Dan Peyesuaian Kebijakan Keamanan Data

PT Bank Syariah Indonesia (BSI) segera melakukan investigasi internal untuk menelusuri akar masalah dan mengidentifikasi titik lemah dalam sistemnya. Salah satu fokus utama BSI adalah memperkuat kebijakan keamanan data melalui pembaruan regulasi internal serta peningkatan kapasitas deteksi dan respons terhadap ancaman digital. Dari hasil evaluasi ini, BSI kemudian merancang serangkaian penyesuaian kebijakan untuk memperkuat ketahanan digital mereka. Penyesuaian kebijakan yang dilakukan mencakup peningkatan sistem proteksi berlapis (multi-layered security), perbaikan prosedur pencadangan data (backup), dan peningkatan kemampuan pemulihan sistem pasca serangan siber. Selain memperkuat tata kelola internal, BSI juga meningkatkan literasi keamanan siber di kalangan nasabah sebagai upaya preventif terhadap potensi serangan lanjutan. Di sisi lain, perusahaan juga meningkatkan investasi di bidang teknologi informasi guna mengantisipasi ancaman yang semakin kompleks di era digital. Seluruh langkah ini mencerminkan komitmen jangka panjang BSI untuk menjaga keberlanjutan operasional sekaligus memperkuat ketahanan institusional terhadap gangguan siber di masa mendatang (Nabila et al., 2024).

Kesimpulan dan Saran

Serangan siber yang terjadi pada Bank Syariah Indonesia (BSI) tahun 2023 menunjukkan pentingnya kesiapan menghadapi risiko digital. Dampak dari serangan tersebut cukup besar, mulai dari gangguan layanan, kebocoran data nasabah, hingga menurunnya kepercayaan masyarakat. BSI merespons dengan memperkuat sistem keamanan, memperbaiki kebijakan internal, dan melakukan komunikasi terbuka kepada publik. Langkah-langkah ini menjadi bukti bahwa manajemen risiko yang baik sangat diperlukan dalam menjaga kepercayaan dan operasional bank di tengah tantangan digital. Untuk kedepannya disarankan BSI dan bank lainnya untuk rutin mengevaluasi keamanan sistem, memberikan pelatihan keamanan kepada karyawan, dan meningkatkan edukasi kepada nasabah. Selain itu, menjaga komunikasi yang jujur dan transparan saat terjadi gangguan akan jauh lebih dihargai oleh publik dibandingkan menutup-nutupi. Dengan begitu, bank bisa tetap dipercaya dan mampu menghadapi tantangan teknologi.

Daftar Pustaka

Akbar, M. R. (2023). Perkembangan yang Pesat dan Tantangan yang Dihadapi oleh Perbankan Digital di Indonesia. *Ecobankers: Journal of Economy and Banking*, *4*(2), 95–111.

Alfattah, M. R., & Adawiyah, S. El. (2024). *Manajemen Krisis Bank Syariah Indonesia Dalam Membentuk Citra Positif*. *2*(2).

Ardhianty, I. W., & Semarang, U. N. (2025). *Tantangan dan strategi perlindungan konsumen pada layanan perbankan di tengah kemajuan teknologi*. *2*(2), 151–162.

Aziz, A., Islami, N., Al-Habsy, A. R., Khoerunnisa, F., Pamungkas, J. D., Fadilah, M. F., & Suryani, R. (2025). Inovasi Produk Keuangan Syariah Dalam Persefektif Generasi Z: Studi Kasus Mahasiswa Ekonomi Syariah Iuqi. *Integrative Perspectives of Social and Science Journal*, *2*(01 Februari), 1340–1350.

Ghozali, M., Liana, N., Afra, C., Siregar, Z., & Hatta, M. (2024). Kejahatan Siber (Cyber Crime) dan Implikasi Hukumnya: Studi Kasus Peretasan Bank Syariah Indonesia (BSI). *Cendekia: Jurnal Hukum, Sosial Dan Humaniora*, *2*(4), 797–809.

Hardeva, H. (2023). *Analisis Respon Komunikasi Krisis Bank Syariah Indonesia di Kompas. com Terkait Serangan Ransomware*. UNIVERSITAS BAKRIE.

Hassandi, I., Yossinomita, & Pangestu, M. G. (2025). *Identifikasi Resiko Dalam Era Digital : Studi Kasus Resiko Teknologi Pada PT Bank Syariah Indonesia*. *5*, 996–1004.

Maulana, B. R., & Nasrulloh, N. (2024). Analisis Strategi Pemulihan Citra Bank Syariah Indonesia Pasca Dugaan Serangan Siber. *Ekonomi Syariah Dan Bisnis Perbankan*, *8*(1), 76–91.

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*, 8244–8258.

Nabila, F., Razief, I. B., & Amiludin. (2024). *Evaluasi terhadap kebocoran data dalam sistem perbankan di indonesia (studi kasus ransomware pada bank syariah indonesia)*. *7*(2), 295–310.

Nugroho, A. (2023, Mei 13). Geng Ransomware LockBit 3.0 Akhirnya Buka Suara: Kami Curi 1,5 TB Data Nasabah dan Karyawan BSI. Password Seluruh Layanan juga Dikuasai. Cyberthreat.id. Diakses pada 15 Mei 2025 di https://m.cyberthreat.id/read/15614/Geng-Ransomware-LockBit-30-Akhirnya-Buka-Suara-Kami-Curi-15-TB-Data-Nasabah-dan-Karyawan-BSI-Password-Seluruh-Layanan-juga-Dikuasai.

Nurul Monika Larasati, & Rayyan Firdaus. (2024). Analisis Bahaya Serangan Ransomeware Terhadap Layanan Perbankan. *Merkurius : Jurnal Riset Sistem Informasi Dan Teknik Informatika*, *2*(4), 102–109. https://doi.org/10.61132/merkurius.v2i4.151

Putri, D. F., Agama, I., Negeri, I., & Kediri, I. (2023). *Analisis Perlindungan Nasabah Bsi Terhadap Kebocoran Data Dalam Menggunakan Digital Banking*. *1*(4), 173–181.

Rezki, J. F. (2023). *Isu Keamanan Siber Perbankan Dan Potensi Bank Run*.

Sari, S. K., Anggryani, L., Hidayat, R., & Marzuki, S. N. (2024). *Tantangan Dan Solusi Dalam Pengawasan Risiko Di Perbankan Syariah Pada Era Cyber: Tinjauan Literatur Bank Syariah Indonesia*. *6*(1), 195–222. https://doi.org/10.1201/9781032622408-13

Solikhawati, A., & Samsuri, A. (2023). Evaluasi Bank Syariah Indonesia Pasca Serangan Siber: Pergerakan Saham dan Kinerja. *Jurnal Ilmiah Ekonomi Islam*, *9*(3), 4201. https://doi.org/10.29040/jiei.v9i3.10309

Tannavaro, D. M., & Wiraguna, S. A. (2025). *Strategi Komunikasi Humas Dalam Krisis Siber: Studi Kasus Bpjs Kesehatan Dan Bank Syariah Indonesia*. *7*(11), 1–23.

Widya, D., Simatangkir, E., Semarang, U. N., Semarang, U. N., Faliha, N. S., & Semarang, U. N. (2025). *Keamanan Siber Dalam Perbankan Serta Tantangan*. *2*(1), 33–42.

Zulfikar, F. R., Bintang, A., & Harley, M. (2024). *Analisis Hukum Dalam Kasus Serangan Siber Pada Bank Syariah Indonesia (BSI)*. *2*(4), 2022–2025.