Jurnal Ekonomi Bisnis, Manajemen dan Akuntansi (JEBMAK)
p–ISSN: 2964-8858 e-ISSN: 2963-3087
Vol. 5, No. 2, Juli 2026

Model Manajemen Risiko Siber Digital Banking: Studi Kasus Kualitatif Berbasis Perspektif Sosio-Teknis

Kelvinda Almathea[1], Adevia Indah Kusuma[2*]
[1] Program Studi Manajemen, Fakultas Ekonomi dan Bisnis, Universitas Terbuka, Tangerang Selatan, Indonesia
[2] Program Studi Kewirausahaan, Fakultas Ilmu Sosial dan Bisnis, Universitas Muhamamdiyah Bangka Belitung, Pangkal Pinang, Indonesia
[2] Program Studi Ilmu Manajemen, Fakultas Ekonomi, Universitas Sriwijaya, Palembang, Indonesia
Email: 048004585@ecampus.ut.ac.id, adevia.indahkusuma@unmuhbabel.ac.id

Abstrak

Transformasi digital di sektor perbankan Indonesia membawa peluang sekaligus ancaman keamanan siber yang semakin kompleks. Penelitian ini bertujuan untuk menganalisis bagaimana risiko keamanan siber memengaruhi adopsi digital banking serta mengevaluasi efektivitas strategi mitigasi yang diterapkan oleh lembaga perbankan. Menggunakan pendekatan kualitatif dengan desain studi kasus, penelitian ini berfokus pada insiden ransomware yang menimpa Bank Syariah Indonesia pada Mei 2023 yang mengakibatkan kebocoran 1,5 terabyte data lebih dari 15 juta nasabah. Data dikumpulkan melalui wawancara mendalam, studi dokumentasi, dan observasi berbasis kerangka perspektif sosio-teknis. Hasil penelitian mengidentifikasi lima tema utama: dominasi ancaman ransomware dan phishing, respons institusional melalui framework ISO 27001:2022, COBIT 2019, dan NIST CSF 2.0, penurunan kepercayaan konsumen sebagai hambatan adopsi, lemahnya peran regulasi OJK dalam pengawasan proaktif, serta pentingnya pendekatan holistik yang mengintegrasikan faktor manusia, teknologi, dan institusi. Penelitian ini menyimpulkan bahwa strategi mitigasi risiko siber yang efektif harus bersifat sosio-teknis, bukan sekadar teknis semata. Rekomendasi yang diberikan mencakup implementasi autentikasi multi-faktor, pelatihan kesadaran keamanan siber, dan pengembangan kerangka regulasi yang lebih adaptif.

Kata kunci: *Adopsi Layanan, Digital Banking, Keuangan Digital, Keamanan Informasi Perbankan, Manajemen Risiko Siber, Perspektif Sosio-Teknis.*

Abstract

Digital transformation in the Indonesian banking sector brings both opportunities and increasingly complex cybersecurity threats. This study aims to analyze how cybersecurity risks impact digital banking adoption and evaluate the effectiveness of mitigation strategies implemented by banking institutions. Using a qualitative approach with a case study design, this research focuses on the ransomware incident that hit Bank Syariah Indonesia in May 2023, which resulted in the leak of 1.5 terabytes of data belonging to more than 15 million customers. Data was collected through in-depth interviews, documentary studies, and observations based on a socio-technical perspective framework. The study identified five main themes: the dominance of ransomware and phishing threats, institutional responses through the ISO 27001:2022, COBIT 2019, and NIST CSF 2.0 frameworks, declining consumer trust as a barrier

Pengelolah	:	Sekolah Tinggi Ekonomi dan Bisnis Syariah (STEBIS) Indo Global Mandiri
Published by	:	Penerbit dan Percetakan CV. Picmotiv
Url	:	http://ejournal.lapad.id/index.php/jebmak/issue/view/1671

to adoption, the weak role of OJK regulations in proactive oversight, and the importance of a holistic approach that integrates human, technological, and institutional factors. This study concludes that effective cyber risk mitigation strategies must be socio-technical, not merely technical. Recommendations include implementing multi-factor authentication, cybersecurity awareness training, and developing a more adaptive regulatory framework.

Keywords: *Service Adoption, Digital Banking, Digital Finance, Banking Information Security, Cyber Risk Management, Socio-Technical Perspective.*

Pendahuluan

1.1. Latar Belakang

Transformasi digital di industri perbankan telah membawa revolusi dalam cara masyarakat mengakses layanan keuangan, dengan munculnya aplikasi mobile banking, internet banking, dan transaksi digital lainnya yang memudahkan nasabah untuk melakukan transfer, pembayaran, dan investasi secara *real-time*. Namun, kemajuan ini juga membawa risiko keamanan *cyber* yang semakin kompleks, seperti serangan *phishing* yang menipu pengguna untuk mengungkap informasi sensitif, *malware* yang menginfeksi sistem bank, *ransomware* yang memblokir akses data hingga tebusan dibayar, serta pelanggaran data yang mengakibatkan kebocoran informasi pribadi jutaan nasabah. Di Indonesia, risiko ini diperparah oleh tingginya tingkat digitalisasi tanpa disertai infrastruktur keamanan yang memadai, sebagaimana terlihat dari insiden serangan *cyber* pada Bank Syariah Indonesia pada Mei 2023, di mana kelompok *ransomware Lock Bit* berhasil membocorkan *1,5 terabyte* data, termasuk detail pribadi lebih dari 15 juta nasabah dan karyawan, yang menyebabkan penurunan saham bank hingga 4-6% dan erosi kepercayaan publik (Oftafiana et al., 2024). Selain itu, studi oleh Cele dan Kwenda menyoroti bahwa ancaman seperti *phishing* dan *malware* secara signifikan menghambat adopsi perbankan digital karena mengurangi kepercayaan konsumen, dengan contoh kasus perampokan Bangladesh Bank pada 2016 yang menunjukkan kerugian finansial miliaran dolar akibat kerentanan system (Cele & Kwenda, 2025). Penelitian ini muncul sebagai respons terhadap kebutuhan mendesak untuk memahami dinamika risiko *cyber* ini, dengan fokus pada bagaimana bank dapat mengelola risiko tersebut untuk mendorong adopsi digital banking yang aman. Melalui pendekatan kualitatif, penelitian ini akan menggali perspektif dari berbagai pemangku kepentingan,

termasuk regulator, bankir, dan nasabah, untuk memberikan rekomendasi yang holistik dalam membangun ekosistem perbankan digital yang lebih tangguh.

1.2 Perumusan Masalah

Berdasarkan uraian latar belakang di atas, yang menyoroti peningkatan ancaman keamanan *cyber* seperti *phishing, ransomware,* dan pelanggaran data di sektor perbankan digital Indonesia, serta dampaknya terhadap kepercayaan konsumen dan adopsi teknologi, peneliti dapat merumuskan masalah yang ada sebagai berikut:

1. Bagaimana risiko keamanan *cyber,* seperti serangan *phishing* dan *ransomware,* mempengaruhi tingkat adopsi digital banking di Indonesia, khususnya dalam konteks penurunan kepercayaan konsumen dan peningkatan persepsi risiko?
2. Apa saja strategi mitigasi risiko keamanan *cyber* yang efektif diterapkan oleh bank, berdasarkan analisis kasus insiden nyata seperti serangan pada Bank Syariah Indonesia, dan bagaimana strategi tersebut berkontribusi pada pemulihan reputasi dan peningkatan keamanan sistem?

1.3 Tujuan Penelitian

Tujuan dari penelitian ini adalah sebagai berikut:

1. Untuk mengidentifikasi dan menganalisis secara mendalam bagaimana risiko keamanan *cyber* mempengaruhi adopsi digital banking, melalui eksplorasi kasus-kasus spesifik yang melibatkan ancaman seperti phishing dan pelanggaran data, serta dampaknya terhadap perilaku konsumen. Tujuan ini mencakup pengumpulan data empiris dari survei nasabah, analisis laporan insiden dari bank, dan studi komparatif dengan negara lain untuk memahami pola umum, seperti peningkatan risiko selama pandemi COVID-19 yang mendorong transaksi online. Penelitian juga bertujuan untuk mengukur indikator kuantitatif seperti tingkat adopsi aplikasi mobile banking dan kualitatif seperti narasi konsumen tentang pengalaman serangan *cyber,* sehingga memberikan wawasan tentang dinamika risiko yang berkembang.
2. Untuk mengevaluasi strategi mitigasi risiko keamanan *cyber* yang telah diterapkan oleh bank, termasuk penerapan standar seperti ISO 27001 dan

Pengelolah	:	Sekolah Tinggi Ekonomi dan Bisnis Syariah (STEBIS) Indo Global Mandiri
Published by	:	Penerbit dan Percetakan CV. Picmotiv
Url	:	http://ejournal.lapad.id/index.php/jebmak/issue/view/1671

penggunaan teknologi *AI*, dengan fokus pada efektivitasnya dalam mencegah insiden berulang dan membangun kepercayaan jangka panjang di sektor perbankan digital. Tujuan ini melibatkan penilaian metrik seperti tingkat keberhasilan pencegahan serangan, biaya implementasi strategi, dan dampaknya pada indeks kepercayaan konsumen. Selain itu, penelitian akan mengintegrasikan analisis kasus studi mendalam terhadap bank yang berhasil memulihkan reputasi pasca-insiden, serta rekomendasi untuk adaptasi strategi berdasarkan tren teknologi seperti *blockchain* atau *zero-trust architecture*, guna memastikan keberlanjutan keamanan di era digitalisasi perbankan Indonesia.

1.4 Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan manfaat sebagai berikut:

1. Hasil penelitian ini dapat menambah kajian di bidang ilmu manajemen risiko dan keamanan informasi, khususnya melalui aplikasi teori risiko *cyber* pada sektor perbankan digital, dengan memberikan wawasan baru tentang dinamika ancaman dan respons adaptif. Manfaat ini mencakup kontribusi teoritis seperti pengembangan model risiko *cyber* yang disesuaikan dengan konteks Indonesia, termasuk integrasi teori perilaku konsumen dan analisis risiko sistemik, serta publikasi dalam jurnal internasional untuk memperluas pengetahuan global tentang keamanan digital di negara berkembang. Penelitian juga akan mendorong penelitian lanjutan, seperti simulasi serangan *cyber* atau *studi longitudinal* tentang evolusi ancaman.
2. Hasil penelitian ini dapat memberikan rekomendasi praktis bagi bank, regulator seperti Otoritas Jasa Keuangan (OJK), dan pemangku kepentingan lainnya untuk meningkatkan protokol keamanan, seperti implementasi autentikasi multi-faktor dan pelatihan karyawan, sehingga mendorong adopsi digital banking yang lebih aman dan berkelanjutan di Indonesia, serta mengurangi risiko kerugian finansial dan reputasi. Manfaat praktis ini meliputi panduan operasional untuk bank, seperti checklist audit keamanan tahunan, kampanye edukasi nasional untuk konsumen, dan kerangka regulasi yang lebih ketat untuk *fintech*. Selain itu, penelitian akan berkontribusi pada pengurangan kerugian ekonomi, seperti estimasi potensi penghematan miliaran rupiah dari

pencegahan serangan, serta peningkatan inklusi keuangan digital yang lebih aman, khususnya bagi masyarakat pedesaan yang rentan terhadap risiko *cyber.*(Munawarah, S.E. & Yusuf, 2022).

Metode Penelitian

2.1 Pendekatan dan Jenis Penelitian

Penelitian ini menggunakan pendekatan kualitatif dengan desain studi kasus. Pendekatan ini dipilih untuk menggali secara mendalam dinamika risiko siber di perbankan digital dari perspektif sosio-teknis, yaitu interaksi antara dimensi manusia, teknologi, dan institusi (AL-Dosari et al., 2024). Unit analisis utama adalah insiden *ransomware LockBit* yang menyerang Bank Syariah Indonesia (BSI) pada Mei 2023, mengakibatkan kebocoran 1,5 *terabyte* data lebih dari 15 juta nasabah (Oftafiana et al., 2024).

2.2 Subjek Penelitian

Informan dipilih menggunakan teknik purposive sampling berdasarkan keberagaman tingkat literasi digital, latar belakang pekerjaan, dan keterlibatan langsung dengan layanan digital banking BSI. Penelitian melibatkan tiga informan nasabah sebagaimana ditampilkan pada tabel berikut.

Tabel 1. Profil Nasabah

Kode	J.K.	Usia / Pekerjaan	Bank	Lama Pakai	Literasi Digital
N1	P	34 th / Guru SD	BSI & BCA	± 4 tahun	Menengah
N2	L	28 th / Karyawan IT	BSI, Mandiri	± 6 tahun	Tinggi
N3	P	52 th / Pedagang Online	BSI	± 2 tahun	Rendah

2.3 Teknik Pengumpulan Data

Data dikumpulkan melalui tiga teknik yang digunakan secara komplementer:

1. Wawancara Mendalam Semi-Terstruktur: dilakukan selama 45–75 menit per informan menggunakan panduan wawancara yang memuat 19 pertanyaan dalam 5 tema pengalaman penggunaan, persepsi risiko, dampak perilaku,

Pengelolah : Sekolah Tinggi Ekonomi dan Bisnis Syariah (STEBIS) Indo Global Mandiri
Published by : Penerbit dan Percetakan CV. Picmotiv
Url : http://ejournal.lapad.id/index.php/jebmak/issue/view/1671

evaluasi respons bank/OJK, dan rekomendasi dikembangkan berdasarkan kerangka ISO 27001:2022 (Ryanto & Tundjungsari, 2024), COBIT 2019 (Purnomo & Harwahyu, 2025), dan NIST CSF 2.0 (Adisardjono et al., 2026).

2. Studi Dokumentasi: telaah laporan insiden BSI, pemberitaan media, regulasi OJK, dan publikasi ilmiah untuk mengkontekstualisasikan data primer (Cele & Kwenda, 2025; Oftafiana et al., 2024)
3. Observasi Non-Partisipan: pengamatan antarmuka BSI Mobile untuk memverifikasi implementasi fitur keamanan yang disebutkan informan, seperti autentikasi multi-faktor dan notifikasi transaksi (Sari & Fitri, 2025).

2.4 Teknik Analisis Data

Analisis dilakukan menggunakan analisis tematik *(thematic analysis)* enam tahap: (1) transkripsi verbatim dalam 48 jam pasca wawancara; (2) familiarisasi data melalui pembacaan berulang; (3) *open coding* induktif-deduktif; (4) pengelompokan kode ke dalam tema; (5) *review* dan pendefinisian tema; serta (6) penyusunan narasi analitik. Sistem kode menggunakan hierarki tiga level: Tema (T) → Subtema (S) → Kode (K), menghasilkan lima tema utama yang mencerminkan dimensi sosio-teknis risiko siber. Analisis lintas kasus *(cross-case analysis)* juga dilakukan untuk membandingkan pola respons antara informan berliterasi berbeda (Hidayatun Muharromah et al., 2025; Kurniawan & Solihin, 2022).

2.5 Keabsahan Data

Keabsahan data dijamin melalui empat strategi: (1) triangulasi sumber membandingkan data dari N1, N2, dan N3 yang memiliki latar belakang berbeda; (2) triangulasi metode membandingkan hasil wawancara dengan temuan dokumentasi dan observasi; (3) member checking konfirmasi temuan sementara kepada informan sebelum laporan final disusun; dan (4) audit trail dokumentasi sistematis seluruh keputusan metodologis dalam jurnal reflektif peneliti (Rizal & Ardhian, 2023).

2.6 Etika Penelitian

Seluruh informan diberikan penjelasan lengkap dan menandatangani *informed cons*ent sebelum wawancara. Identitas informan dikodekan (N1, N2, N3)

dan data rekaman disimpan dalam sistem terenkripsi serta hanya dapat diakses oleh tim peneliti. Peneliti berkomitmen tidak mengungkap detail teknis yang dapat membahayakan keamanan sistem perbankan dalam pelaporan hasil (Febriyani & Wulandari, 2025; Widya et al., 2025).

Hasil dan Pembahasan

3.1 Gambaran Umum Informan Penelitian

Penelitian ini melibatkan tiga informan nasabah yang dipilih secara purposif berdasarkan perbedaan latar belakang literasi digital, jenis pekerjaan, dan tingkat keterlibatan dengan layanan digital banking BSI. Keragaman profil informan dirancang untuk memperoleh perspektif yang komprehensif sesuai kerangka sosio-teknis, yang memandang risiko siber sebagai produk interaksi antara faktor manusia, teknologi, dan institusi.

3.2 Hasil Penelitian: Lima Tema Utama

Analisis tematik terhadap transkripsi wawancara mendalam, studi dokumentasi laporan insiden BSI, dan observasi antarmuka digital banking menghasilkan lima tema utama yang mencerminkan kompleksitas risiko siber dari perspektif sosio-teknis. Kelima tema tersebut disajikan berikut ini beserta bukti kutipan dan analisisnya.

3.2.1 Tema 1: Dominasi Ancaman Ransomware dan Phishing

Seluruh informan secara konsisten mengidentifikasi dua jenis ancaman siber yang paling terasa dampaknya: serangan *ransomware* seperti yang menimpa BSI pada Mei 2023, dan serangan *phishing* berbasis rekayasa sosial melalui SMS atau telepon palsu. Temuan ini selaras dengan kajian sistematis (Cele & Kwenda, 2025) yang menempatkan phishing dan malware sebagai penghambat utama adopsi perbankan digital di berbagai negara berkembang.

Dari sisi teknis, N2 yang memiliki latar belakang IT menjelaskan mekanisme serangan dengan lebih rinci:

> *"Serangan LockBit yang menimpa BSI itu sebenarnya bukan hal baru di dunia keamanan siber. Yang bikin saya kaget justru betapa besar dampaknya 1,5 terabyte data itu sangat masif. Ini menunjukkan bahwa*

Pengelolah	:	Sekolah Tinggi Ekonomi dan Bisnis Syariah (STEBIS) Indo Global Mandiri
Published by	:	Penerbit dan Percetakan CV. Picmotiv
Url	:	http://ejournal.lapad.id/index.php/jebmak/issue/view/1671

> *sistem keamanan berlapis (defense in depth) BSI mungkin belum optimal. Kalau sistem mereka sudah menerapkan zero-trust architecture atau network segmentation yang baik, seharusnya serangan bisa diisolasi sebelum menyebar se-masif itu."* (N2)

Sementara itu, N1 dan N3 yang merupakan nasabah awam lebih merasakan dampak *phishing* dalam kehidupan sehari-hari:

> *"Yang paling sering saya khawatirkan itu SMS atau telepon penipuan yang pura-pura dari bank. Sudah tiga kali saya terima SMS yang isinya 'Rekening Anda akan diblokir, klik link ini.' Saya sudah tahu itu penipuan, tapi ibu-ibu lain di pengajian ada yang sampai kena."* (N1)

Temuan ini memperkuat argumentasi (Adisardjono et al., 2026) bahwa ancaman siber di perbankan bersifat multidimensi dan memerlukan integrasi kerangka COSO ERM dan NIST CSF 2.0 untuk penanganan yang komprehensif. Dominasi ancaman ransomware juga dikonfirmasi oleh (Soesanto et al., 2023) yang menyebutkan bahwa sektor keuangan merupakan target utama kelompok ransomware terorganisir di Asia Tenggara.

3.2.2 Tema 2: Penurunan Kepercayaan sebagai Hambatan Adopsi Digital Banking

Ketiga informan melaporkan mengalami penurunan kepercayaan yang signifikan pasca insiden BSI. Namun, secara paradoksal, tidak satu pun dari mereka yang akhirnya menutup rekening atau beralih sepenuhnya ke bank lain. Fenomena ini dapat disebut sebagai kepercayaan terpaksa *(forced trust)*, di mana nasabah mempertahankan hubungan dengan penyedia layanan bukan karena kepercayaan yang pulih, melainkan karena tingginya biaya perpindahan *(switching cost)*.

> *"Kepercayaan saya memang turun, tapi tidak sampai saya tutup rekening, karena memang tidak ada pilihan lain yang lebih praktis untuk rekening syariah."* (N1)
>
> *"Saya sempat tanya-tanya ke suami soal itu. Tapi akhirnya tidak jadi pindah, karena sudah banyak pelanggan yang tahu nomor rekening BSI saya dan repot kalau harus kasih tahu satu-satu."* (N3)

Temuan ini mengonfirmasi dan memperluas kajian (Rizal & Ardhian, 2023) tentang dampak serangan siber terhadap kepercayaan nasabah perbankan syariah.

(Sari & Fitri, 2025) juga menemukan bahwa persepsi risiko yang tinggi tidak selalu berkorelasi dengan niat berpindah, terutama pada segmen nasabah dengan ketergantungan institusional yang kuat. Dari perspektif manajemen reputasi, (Oftafiana et al., 2024) menegaskan bahwa pemulihan kepercayaan pasca-insiden memerlukan strategi komunikasi yang proaktif dan transparan aspek yang justru dinilai lemah oleh seluruh informan dalam penelitian ini.

3.2.3 Tema 3: Adaptasi Perilaku Berbasis Tingkat Literasi Digital

Salah satu temuan paling signifikan dalam penelitian ini adalah bahwa respons perilaku nasabah pasca insiden siber sangat dipengaruhi oleh tingkat literasi digital mereka. Hal ini menciptakan tiga pola adaptasi yang berbeda, sebagaimana dirangkum dalam tabel berikut:

Tabel 2. Hasil Penelitian Adaptaso Perilaku

Informan	Literasi Digital	Bentuk Adaptasi Perilaku	Sumber Informasi
N2	Tinggi (IT)	Aktifkan 2FA semua akun, gunakan password manager, cek breach via HaveIBeenPwned, matikan auto-login, pindahkan saldo, usulkan audit internal kantor	Pengetahuan profesional
N1	Menengah	Ganti PIN, pindahkan sebagian saldo ke BCA, pantau mutasi harian, pelajari tips keamanan dari YouTube	Media sosial & pengalaman sendiri
N3	Rendah	Konsultasi dengan anak, laporkan pesan mencurigakan ke anggota keluarga, tidak ada tindakan teknis mandiri	Anggota keluarga

Kesenjangan respons ini secara jelas menggambarkan bahwa strategi mitigasi risiko siber yang bersifat teknis semata seperti implementasi autentikasi multi-faktor

Pengelolah : Sekolah Tinggi Ekonomi dan Bisnis Syariah (STEBIS) Indo Global Mandiri
Published by : Penerbit dan Percetakan CV. Picmotiv
Url : http://ejournal.lapad.id/index.php/jebmak/issue/view/1671

atau enkripsi data tidak cukup bila tidak disertai upaya peningkatan literasi digital nasabah. Temuan ini memperkuat argumen (AL-Dosari et al., 2024) bahwa teknologi kecerdasan buatan dalam pertahanan siber harus diintegrasikan dengan program edukasi pengguna agar efektif. (Kurniawan & Solihin, 2022) juga menekankan bahwa penguatan manajemen risiko lembaga keuangan syariah harus mencakup dimensi sumber daya manusia, bukan hanya infrastruktur teknis.

3.2.4 Tema 4: Kegagalan Komunikasi Krisis dan Lemahnya Respons Institusional

Seluruh informan menilai respons komunikasi BSI pasca insiden sebagai lambat, tidak transparan, dan tidak memadai dari perspektif nasabah. Tidak satu pun informan yang menerima notifikasi resmi dari BSI, meskipun data pribadi mereka berpotensi telah dikompromikan.

> *"Saya tidak pernah mendapat SMS atau email resmi dari BSI yang menjelaskan apa yang sebenarnya terjadi dan apa langkah mereka untuk melindungi data saya. Informasi yang saya dapat justru dari berita di internet dan dari teman-teman. Kalau saya bandingkan waktu BCA pernah ada isu keamanan yang jauh lebih kecil, mereka cepat sekali kirim notifikasi dan penjelasan. BSI rasanya lambat dan kurang transparan."* (N1)

N2, dengan pemahamannya tentang standar keamanan informasi, memberikan analisis yang lebih terstruktur:

> *"Standar seperti ISO 27001 seharusnya mengharuskan incident response plan yang jelas, termasuk protokol komunikasi publik. Respons awal BSI menurut saya terlambat dan kurang transparan mereka mengakui adanya gangguan sekitar tiga hari setelah sistem mulai tidak bisa diakses. Dari sisi crisis communication, ini sangat buruk."* (N2)

Dari sisi regulasi, ketiga informan juga merasakan minimnya kehadiran OJK sebagai pengawas yang proaktif:

> *"Sebagai nasabah biasa, saya merasa ada yang kurang karena kejadian sebesar ini, data jutaan orang bocor, tapi tidak ada kabar*

bank dikenai sanksi berat atau diwajibkan memberi ganti rugi kepada nasabah." (N1)

Temuan ini sejalan dengan (Oftafiana et al., 2024) yang menyimpulkan bahwa manajemen risiko reputasi yang efektif mensyaratkan rencana komunikasi krisis yang terintegrasi dan diaktifkan secara cepat. (Ryanto & Tundjungsari, 2024) menegaskan bahwa implementasi ISO 27001:2022 yang komprehensif seharusnya mencakup klausul khusus tentang kewajiban notifikasi kepada pemangku kepentingan termasuk nasabah dalam tenggat waktu tertentu pasca insiden terdeteksi.

3.2.5 Tema 5: Kesenjangan Literasi Siber dan Kebutuhan Pendekatan Sosio-Teknis Holistik

Tema kelima merupakan sintesis dari keempat tema sebelumnya. Temuan menunjukkan bahwa akar dari hampir seluruh permasalahan yang teridentifikasi lambatnya respons bank, tingginya dampak insiden, minimnya perlindungan nasabah awam bermuara pada satu persoalan mendasar: belum terintegrasinya dimensi manusia, teknologi, dan institusi dalam ekosistem keamanan siber perbankan digital Indonesia.

N3 secara paling lugas mengungkapkan kebutuhan akan pendekatan yang berpusat pada pengguna:

"Yang paling saya butuhkan itu penjelasan yang mudah dimengerti. Waktu ada insiden itu, berita-beritanya pakai istilah-istilah yang tidak saya pahami. Kalau saja BSI kirim pesan singkat yang isinya: 'Ibu [nama], sistem kami sedang ada masalah keamanan. Uang Ibu aman. Mohon ganti PIN sekarang dengan cara ini...' itu sudah cukup bikin saya lebih tenang." (N3)

Pernyataan N3 ini secara implisit mencerminkan tiga dimensi sosio-teknis sekaligus: teknologi (sistem pesan otomatis), manusia (bahasa yang dapat dipahami nasabah awam), dan institusi (tanggung jawab bank untuk berkomunikasi proaktif). (Mulyana, 2025; Widya et al., 2025) mengonfirmasi bahwa tantangan keamanan siber perbankan di Indonesia tidak dapat diselesaikan hanya dengan investasi infrastruktur teknis, melainkan harus disertai pengembangan kapasitas sumber daya manusia dan reformasi kelembagaan secara simultan.

Pengelolah	:	Sekolah Tinggi Ekonomi dan Bisnis Syariah (STEBIS) Indo Global Mandiri
Published by	:	Penerbit dan Percetakan CV. Picmotiv
Url	:	http://ejournal.lapad.id/index.php/jebmak/issue/view/1671

3.3 Pembahasan

3.3.1 Menjawab Pertanyaan Penelitian Pertama

Pertanyaan penelitian pertama menanyakan bagaimana risiko keamanan siber memengaruhi adopsi digital banking di Indonesia. Temuan penelitian ini mengungkap bahwa pengaruh tersebut tidak bersifat linear risiko yang tinggi tidak selalu mengakibatkan penolakan terhadap teknologi *digital banking (dis-adoption).* Sebaliknya, yang terjadi adalah adopsi defensif: nasabah tetap menggunakan layanan digital banking, namun dengan perilaku yang lebih hati-hati, pola penggunaan yang lebih terbatas, dan kepercayaan yang mengalami erosi.

Mekanisme pengaruh ini dimediasi oleh dua faktor kunci. Pertama, tingkat literasi digital yang menentukan kapasitas nasabah untuk menerapkan tindakan protektif secara mandiri. Kedua, *switching cost* yang menciptakan ketergantungan struktural pada bank yang ada, bahkan ketika kepercayaan telah menurun. Hal ini memperluas model yang diusulkan oleh (Cele & Kwenda, 2025), di mana kepercayaan bukan hanya mediator tunggal, tetapi berinteraksi dengan variabel struktural seperti ketersediaan alternatif dan jaringan ketergantungan.

3.3.2 Menjawab Pertanyaan Penelitian Kedua

Pertanyaan penelitian kedua menanyakan strategi mitigasi risiko siber yang efektif. Berdasarkan triangulasi data wawancara, dokumentasi, dan observasi, penelitian ini mengidentifikasi gap kritis antara standar mitigasi yang tersedia (ISO 27001:2022, COBIT 2019, NIST CSF 2.0) dan implementasi aktualnya di lapangan, khususnya dalam hal:

1. *Incident Response*: Protokol respons insiden yang seharusnya mengharuskan notifikasi kepada pemangku kepentingan dalam 72 jam tidak dijalankan oleh BSI, sehingga melanggar ekspektasi minimum standar ISO 27001 (Ryanto & Tundjungsari, 2024).
2. Komunikasi Krisis: Tidak adanya saluran komunikasi langsung kepada nasabah menciptakan kekosongan informasi yang diisi oleh rumor dan informasi tidak terverifikasi di media sosial.

3. Perlindungan Regulatori: Ketidakhadiran OJK dalam memberikan panduan publik yang cepat dan mengenakan sanksi yang terukur memperlemah fungsi pengawasan sebagai jaring pengaman terakhir.
4. Edukasi Nasabah: Tidak adanya program edukasi berkelanjutan membuat nasabah dengan literasi rendah sepenuhnya tidak berdaya menghadapi ancaman siber, bahkan pasca insiden besar sekalipun.

Strategi mitigasi yang dievaluasi efektif berdasarkan temuan penelitian dan literatur mencakup: implementasi autentikasi multi-faktor wajib, sistem deteksi anomali berbasis AI (AL-Dosari et al., 2024), program kesadaran siber nasabah yang berkelanjutan, pengembangan protokol komunikasi krisis terstandar, serta penguatan regulasi OJK dengan mekanisme sanksi yang proporsional dan terukur.

3.3.3 Kontribusi Perspektif Sosio-Teknis

Kerangka perspektif sosio-teknis terbukti relevan dan produktif dalam menjelaskan kompleksitas fenomena yang diteliti. Temuan penelitian ini menunjukkan bahwa kegagalan manajemen risiko siber BSI bukan semata-mata kegagalan teknis (sistem keamanan yang tidak optimal), melainkan juga kegagalan pada dimensi manusia (komunikasi krisis yang buruk, literasi nasabah yang rendah) dan dimensi institusional (pengawasan OJK yang reaktif, tidak adanya regulasi notifikasi insiden yang tegas). Ketiga dimensi ini saling berinteraksi dan memperkuat dampak negatifnya, sehingga respons yang efektif harus bersifat simultan dan terintegrasi pada ketiga level tersebut.

Kesimpulan

4.1 Kesimpulan

Berdasarkan analisis tematik terhadap data wawancara mendalam dengan tiga informan nasabah digital banking, studi dokumentasi laporan insiden Bank Syariah Indonesia, dan observasi antarmuka layanan digital, penelitian ini menghasilkan tiga kesimpulan utama sebagai berikut.

4.1.1 Risiko Siber Menghasilkan Adopsi Defensif, Bukan Penolakan

Insiden *ransomware* BSI Mei 2023 yang mengakibatkan kebocoran 1,5 *terabyte* data lebih dari 15 juta nasabah terbukti secara signifikan menurunkan

Pengelolah : Sekolah Tinggi Ekonomi dan Bisnis Syariah (STEBIS) Indo Global Mandiri
Published by : Penerbit dan Percetakan CV. Picmotiv
Url : http://ejournal.lapad.id/index.php/jebmak/issue/view/1671

kepercayaan nasabah terhadap layanan *digital banking*. Namun, pengaruh ini tidak berujung pada penghentian penggunaan layanan *(dis-adoption)*, melainkan melahirkan fenomena adopsi defensive di mana nasabah tetap menggunakan digital banking dengan perilaku yang lebih protektif, pola penggunaan yang lebih terbatas, dan diversifikasi rekening ke bank lain sebagai cadangan. Fenomena ini dimediasi oleh tingginya *switching cost* yang bersifat struktural, mencakup ketergantungan jaringan nasabah dan ketiadaan alternatif bank syariah yang lebih terpercaya. Temuan ini memperluas model teoritis (Cele & Kwenda, 2025) tentang hubungan antara ancaman siber dan adopsi digital banking.

4.1.2 Literasi Digital Menentukan Kapasitas Respons Protektif Nasabah

Penelitian ini menemukan kesenjangan kapasitas respons yang sangat signifikan antara nasabah berliterasi tinggi dan nasabah berliterasi rendah dalam menghadapi ancaman siber. Nasabah dengan latar belakang IT mampu mengambil tindakan teknis yang komprehensif secara mandiri, sementara nasabah dengan literasi rendah sepenuhnya bergantung pada pendampingan pihak ketiga anggota keluarga atau komunitas. Kesenjangan ini mengonfirmasi bahwa strategi mitigasi risiko siber yang bersifat teknis semata tidak cukup efektif untuk melindungi seluruh segmen nasabah. Dimensi manusia dalam kerangka sosio-teknis mencakup literasi digital, kapasitas respons individu, dan akses terhadap informasi yang dapat dipahami harus menjadi komponen integral dari model manajemen risiko siber lembaga perbankan.

4.1.3 Kegagalan Dimensi Institusional Memperparah Dampak Insiden Siber

Respons institusional BSI pasca insiden dan pengawasan OJK selama dan setelah krisis dinilai tidak memadai oleh seluruh informan. Keterlambatan komunikasi, ketiadaan notifikasi resmi kepada nasabah, serta minimnya sanksi yang terasa bagi publik menciptakan kekosongan kepercayaan institusional yang memperparah dampak jangka panjang insiden. Temuan ini menegaskan bahwa implementasi standar keamanan informasi seperti ISO 27001:2022 dan COBIT 2019 harus disertai protokol komunikasi krisis yang teraktivasi dengan cepat dan regulasi OJK yang mewajibkan transparansi serta akuntabilitas institusional secara terukur.

4.2 Saran

Berdasarkan kesimpulan di atas, penelitian ini mengajukan saran kepada empat pihak yang memiliki peran kunci dalam ekosistem keamanan digital banking Indonesia.

4.2.1 Saran bagi Lembaga Perbankan (Khususnya BSI dan Bank Digital Lainnya)

1. Mengembangkan dan mengaktifkan protokol komunikasi krisis yang terintegrasi dengan standar ISO 27001:2022, yang mewajibkan notifikasi kepada seluruh nasabah terdampak dalam rentang waktu maksimal 24 jam setelah insiden terdeteksi, menggunakan bahasa yang sederhana dan dapat dipahami oleh semua segmen nasabah.
2. Mengimplementasikan sistem autentikasi multi-faktor (MFA) yang wajib untuk seluruh transaksi di atas nominal tertentu, disertai panduan visual yang ramah bagi nasabah lansia dan nasabah dengan literasi digital rendah.
3. Menerapkan arsitektur keamanan *zero-trust* dan segmentasi jaringan *(network segmentation)* untuk membatasi dampak lateral dari serangan *ransomware,* sebagaimana direkomendasikan oleh (Purnomo & Harwahyu, 2025) dalam kerangka COBIT 2019.
4. Menyelenggarakan program edukasi keamanan siber nasabah yang berkelanjutan melalui platform yang mudah diakses termasuk notifikasi dalam aplikasi, video pendek, dan *workshop* komunitas dengan materi yang disesuaikan berdasarkan segmen literasi digital nasabah.
5. Mendirikan unit respons insiden siber *(Computer Security Incident Response Team/CSIRT)* yang beroperasi 24/7 dan memiliki kewenangan untuk mengaktifkan protokol komunikasi publik secara independen dan cepat.

4.2.2 Saran bagi Otoritas Jasa Keuangan (OJK) dan Regulator

a. Menerbitkan regulasi yang secara eksplisit mewajibkan bank untuk melaporkan insiden siber signifikan kepada OJK dalam 6 jam dan kepada nasabah terdampak dalam 24 jam, dengan ancaman sanksi administratif yang tegas dan proporsional bagi yang melanggar.
b. Mengembangkan standar minimum keamanan siber perbankan digital yang mengintegrasikan dimensi teknis (ISO 27001:2022, NIST CSF 2.0), tata kelola

Pengelolah	:	Sekolah Tinggi Ekonomi dan Bisnis Syariah (STEBIS) Indo Global Mandiri
Published by	:	Penerbit dan Percetakan CV. Picmotiv
Url	:	http://ejournal.lapad.id/index.php/jebmak/issue/view/1671

(COBIT 2019, COSO ERM), dan perlindungan konsumen secara bersamaan, sebagaimana diusulkan (Adisardjono et al., 2026).

c. Mewajibkan bank dengan aset di atas ambang batas tertentu untuk menyampaikan laporan audit keamanan siber tahunan yang diverifikasi oleh auditor independen bersertifikasi.
d. Membentuk mekanisme kompensasi atau skema asuransi siber nasional yang memberikan perlindungan finansial kepada nasabah yang mengalami kerugian akibat kebocoran data yang bukan disebabkan kelalaian nasabah.
e. Melakukan kampanye edukasi literasi keuangan digital nasional yang mencakup modul keamanan siber khusus untuk masyarakat pedesaan dan segmen rentan lainnya, sesuai dengan mandat inklusi keuangan OJK.

4.2.3 Saran bagi Nasabah Digital Banking

a. Mengaktifkan fitur autentikasi dua faktor (2FA) dan notifikasi transaksi *real-time* pada seluruh akun digital banking yang dimiliki sebagai langkah perlindungan dasar yang paling efektif.
b. Menerapkan praktik keamanan digital dasar: tidak mengklik tautan dari SMS atau email yang tidak dikenal, tidak membagikan OTP atau PIN kepada siapa pun termasuk yang mengaku sebagai petugas bank, dan rutin memperbarui kata sandi secara berkala.
c. Mendiversifikasi penyimpanan dana di lebih dari satu rekening bank sebagai mitigasi risiko atas potensi gangguan layanan akibat insiden siber.
d. Memantau mutasi rekening secara rutin minimal tiga kali seminggu dan segera melaporkan transaksi yang tidak dikenal kepada bank melalui saluran resmi.

4.2.4 Saran bagi Penelitian Selanjutnya

a. Memperluas cakupan penelitian dengan melibatkan informan dari sisi bank (manajer keamanan informasi, tim CSIRT) dan regulator (pejabat OJK) untuk memperoleh gambaran sosio-teknis yang lebih lengkap dari ketiga dimensinya.
b. Melakukan studi komparatif antara bank yang telah mengalami insiden siber besar dengan bank yang belum, untuk mengidentifikasi faktor-faktor pembeda

dalam kesiapan dan ketahanan manajemen risiko siber.

c. Mengembangkan instrumen pengukuran kuantitatif berbasis temuan kualitatif penelitian ini khususnya variabel kepercayaan terpaksa *(forced trust)* dan adopsi defensif untuk diuji dalam skala sampel yang lebih besar.
d. Mengeksplorasi potensi implementasi teknologi *blockchain* dalam sistem keamanan data perbankan syariah Indonesia sebagai alternatif arsitektur yang lebih resilien terhadap serangan *ransomware,* sebagaimana disinggung dalam tujuan penelitian ini.
e. Melaksanakan studi longitudinal untuk memantau evolusi kepercayaan nasabah dan perilaku protektif mereka dalam jangka waktu tiga hingga lima tahun pasca insiden BSI 2023, guna memahami proses pemulihan kepercayaan institusional secara empiris.

Daftar Pustaka

Adisardjono, J. K., Nanlohy, D. S., Eka, A., & Serang, D. (2026). *Integrating Climate , Digital , and Cyber Risks into Traditional Banking Risk Types : A Conceptual IMRAD Framework Based on COSO ERM and NIST CSF 2 . 0*. *0*(0), 567–572. https://doi.org/10.47191/jefms/v9

AL-Dosari, K., Fetais, N., & Kucukvar, M. (2024). Artificial Intelligence and Cyber Defense System for Banking Industry: A Qualitative Study of AI Applications and Challenges. *Cybernetics and Systems*, *55*(2), 302–330. https://doi.org/10.1080/01969722.2022.2112539

Febriyani, W., & Wulandari, M. (2025). *Keamanan siber: melindungi data di dunia digital* | (V. Lusiana (ed.)). PT Penamuda Media.

Cele, N. N., & Kwenda, S. (2025). Do cybersecurity threats and risks have an impact on the adoption of digital banking? A systematic literature review. *Journal of Financial Crime*, *32*(1), 31–48. https://doi.org/10.1108/JFC-10-2023-0263

Hidayatun Muharromah, I., Irianto, G., & Djamhuri, A. (2025). Bibliometric Analysis Of Anticipating Digital Financial Report Fraud Using Vosviewer. *Jurnal Reviu Akuntansi Dan Keuangan*, *15*(1), 17–32. https://doi.org/10.22219/jrak.v15i1.37745

Kurniawan, F. A., & Solihin, K. (2022). Penguatan Manajemen Risiko Lembaga Keuangan Syariah Non-Bank dalam Menghadapi Ancaman Cyber Security. *JIOSE: Journal of Indonesian Sharia Economics*, *1*(1), 1–20. https://doi.org/10.35878/jiose.v1i1.360

Mulyana, S. L. (2025). *IMPLEMENTASI CYBER SECURITY DALAM SISTEM*. *2*(4), 276–289.

Munawarah, S.E., M. H. H., & Yusuf, M. S. . D. M. (2022). *Bank Digital Syariah Analisis Cyber Security Menurut Hukum Positif Di Indonesia Dan Hukum Ekonomi Syariah* (M. H. P. Komarudin, S.HI. (ed.)). PT. Borneo Development Project Anggota IKAPI: No. 005/KSL/2021.

Oftafiana, T., Subagiyo, R., Nur Asiyah, B., & Fauzan. (2024). Reputational Risk Management Strategies for Islamic Banking: Comparison of Bank Victoria Syariah and Bank Syariah Indonesia. *International Journal of Islamic Economics*, *6*(02), 105–118. https://doi.org/10.32332/ijie.v6i2.9417

Purnomo, R., & Harwahyu, R. (2025). *Risk Management Analysis in Digital Bank XYZ Using the COBIT 2019 Framework*. *5*(July), 1012–1018.

Rizal, I., & Ardhian, N. (2023). *Dampak serangan siber dan kebocoran data pada perbankan syariah terhadap tingkat kepercayaan nasabah*. *1*(3), 351–359.

Ryanto, K., & Tundjungsari, V. (2024). Standardization of Information Security Management in the Banking Sector using the ISO 27001:2022 Framework. *Journal La Multiapp*, *5*(4), 344–354. https://doi.org/10.37899/journallamultiapp.v5i4.1399

Sari, S. N., & Fitri, A. O. (2025). Inflasi : Jurnal Ekonomi , Manajemen dan Perbankan Analisis Persepsi Masyarakat Terhadap Keamanan Dan Risiko Cyber Crime Dalam Perbankan Digital Inflasi : Jurnal Ekonomi , Manajemen dan Perbankan. *Sari, Selvi Novita Fitri, Anggun Okta*, *2*, 77–83.

Soesanto, E., Romadhon, A., Mardika, B. D., & Setiawan, M. F. (2023). Analisis dan Peningkatan Keamanan Cyber. *SAMMAJIVA: Jurnal Penelitian Bisnis Dan Manajemen*, *1*(2), 172–191.

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.