Jurnal Manajemen Teknologi dan Sistem Informasi (JMS)
Volume 5, Nomor 1, Maret 2025
ISSN 2808-5450 (media cetak), ISSN 2808-5019 (media online)
Available Online at https: http://ejournal.unama.ac.id/index.php/jms
DOI https://10.33998/jms.v5i1

Identifikasi Resiko Dalam Era Digital: Studi Kasus Resiko Teknologi Pada PT Bank Syariah Indonesia

Irfan Hassandi[1*], Yossinomita[2], Mira Gustiana Pangestu[3]
[1,3] Fakultas Ilmu Manajemen Bisnis, Kewirausahaan, Universitas Dinamika Bangsa, Kota Jambi, Indonesia
[2] Fakultas Ilmu Manajemen dan Bisnis, Manajemen, Universitas Dinamika Bangsa, Kota Jambi, Indonesia
Email: [1*]irfanhassandi06@gmail.com, [2]yossinomita.saputra@gmail.com, [3] myraapangestu29@gmail.com
Email Penulis Korespondensi: irfanhassandi06@gmail.com

Submitted :
29 Oktober 2024

Revision :
09 Maret 2025

Accepted:
11 Maret 2025

Published:
28 Maret 2025

Abstrak−Pentingnya keamanan informasi dan keamanan *cyber* dalam konteks globalisasi dan transformasi digital, khususnya bagi perusahaan di sektor keuangan seperti bank. Studi kasus pada PT Bank Syariah Indonesia (BSI) mengidentifikasi, menganalisis, dan mengevaluasi risiko-risiko yang dihadapi, seperti serangan malware, phishing, dan insider threats. Analisis tersebut bertujuan untuk mengembangkan strategi mitigasi yang efektif dan berkelanjutan guna melindungi aset informasi dan kepentingan bisnis. Temuan studi ini memberikan wawasan penting bagi pemahaman praktik keamanan informasi dan *cyber* di sektor perbankan syariah, serta menjadi dasar untuk pengembangan kebijakan dan praktik terbaik dalam lingkungan bisnis yang semakin digital. Metode penelitian yang digunakan adalah deskriptif kualitatif dengan teknik pengumpulan data meliputi survei, observasi, wawancara, analisis dokumen, dan analisis data sekunder. Tantangan utama yang dihadapi termasuk perlunya perhatian khusus terhadap deteksi dan pencegahan serangan *cyber*, peningkatan kesadaran keamanan internal, perbaikan sistem deteksi intrusi, respons terhadap insiden, pelatihan keamanan karyawan, pembaruan kebijakan keamanan, dan kepatuhan terhadap standar industri dan regulasi pemerintah.

Kata Kunci: Identifikasi Resiko Bisnis, Informasi dan Keamanan *Cyber*, Kinerja Perusahaan

Abstract− The importance of information security and cyber security in the context of globalization and digital transformation, especially for companies in the financial sector such as banks. The case study at PT Bank Syariah Indonesia (BSI) identifies, analyzes, and evaluates the risks faced, such as malware attacks, phishing, and insider threats. The analysis aims to develop effective and sustainable mitigation strategies to protect information assets and business interests. The findings of this study provide important insights for understanding information and cyber security practices in the Islamic banking sector, as well as a basis for the development of policies and best practices in an increasingly digital business environment. The research method used is descriptive qualitative with data collection techniques including surveys, observations, interviews, document analysis, and secondary data analysis. Key challenges faced include the need for special attention to cyber attack detection and prevention, increased internal security awareness, improved intrusion detection systems, incident response, employee security training, security policy updates, and compliance with industry standards and government regulations.

Keywords: Business Risk Identification, Information and Cyber Security, Company Performance

1. PENDAHULUAN

Era globalisasi dan transformasi digital saat ini keamanan informasi dan keamanan *cyber* menjadi prioritas utama bagi perusahaan, terutama bagi institusi keuangan seperti bank [1] . PT Bank Syariah Indonesia (BSI), sebagai salah satu pimpinan dalam industri perbankan syariah di Indonesia, tidak terkecuali dari ancaman dan risiko yang berkaitan dengan keamanan informasi dan serangan *cyber* [2]. Sebagai bagian integral dari ekosistem keuangan, BSI menghadapi tantangan yang semakin kompleks dalam menjaga keamanan dan integritas data, serta melindungi kepentingan nasabah dan stakeholder lainnya. Peningkatan serangan siber dalam sektor keuangan menunjukkan pentingnya melindungi nasabah. Risiko keamanan seperti *phishing*, *malware*, dan gangguan layanan dapat menyebabkan kerugian bagi nasabah dan mengancam kepercayaan pada lembaga keuangan [3]. Analisis proteksi nasabah BSI mencakup pemahaman tentang kebijakan keamanan, tanggapan terhadap serangan siber, dan kebijakan perlindungan data nasabah [4].

Perbankan digital semakin diminati karena kemudahan dan efisiensi waktu yang ditawarkannya. Pentingnya perlindungan nasabah dalam penggunaan layanan perbankan digital muncul sebagai isu krusial mengingat adanya ancaman keamanan seperti pencurian identitas, penipuan, gangguan transaksi, dan serangan *malware* yang dapat mengganggu sistem keamanan perbankan digital dan mengancam kerahasiaan data pribadi. Oleh karena itu, menganalisis perlindungan nasabah Bank Syariah Indonesia (BSI) dalam menggunakan layanan perbankan digital bukanlah sekadar penting, melainkan sangat krusial. Digitalisasi dalam sektor keuangan meningkatkan risiko serangan siber hingga mencapai 86,70% [2]. IMF memperkirakan kerugian total tahunan yang dialami sektor jasa keuangan global akibat serangan siber mencapai USD100 miliar atau lebih dari Rp1.433 triliun. Indonesia sendiri menempati peringkat kelima dalam hal keamanan siber di kawasan Asia Tenggara [5].

Jurnal Manajemen Teknologi dan Sistem Informasi (JMS)
Volume 5, Nomor 1, Maret 2025
ISSN 2808-5450 (media cetak), ISSN 2808-5019 (media online)
Available Online at https: http://ejournal.unama.ac.id/index.php/jms
DOI https://10.33998/jms.v5i1

Menurut Widyaningsih, et al (2024), risiko bisnis adalah salah satu penentu penting dari struktur modal dan jumlah risiko yang melekat pada operasi perusahaan bahkan jika tidak menggunakan pembiayaan dengan utang [6]. Arifin, et al (2024) menjelaskan bahwa risiko bisnis adalah salah satu risiko aset perusahaan yang akan dihadapi jika perusahaan menggunakan utang yang terlalu tinggi akibat beban biaya pinjaman yang dilakukan perusahaan [7]. Risiko bisnis merupakan ketidakpastian dalam proyeksi perusahaan atas tingkat pengembalian atau laba yang akan datang [8]. Risiko bisnis adalah salah satu risiko yang akan dihadapi perusahaan ketika menjalankan kegiatan operasinya yaitu kemungkinan ketidakmampuan perusahaan untuk mendanai kegiatan operasional, perusahaan yang memiliki nilai risiko bisnis yang tinggi akan berakibat pada turunnya nilai perusahaan di mata investor [9].

Keamanan informasi adalah upaya untuk memastikan keberlangsungan bisnis dengan melindungi data dari berbagai ancaman, mengurangi risiko bisnis dan mengoptimalkan peluang bisnis. Menurut Widyaningsih, et al (2024), keamanan informasi adalah suatu bentuk perlindungan terhadap informasi dan unsur-unsur penting yang ada didalam seperti kerahasiaan, integritas dan ketersediaan tidak terkecuali sistem dan *hardware* untuk menyimpan dan mengirim informasi tersebut [6]. Menurut Affandi, et al (2015), salah satu standar keamanan siber internasional yang bisa digunakan sebagai acuan dalam manajemen kemanan digital adalah ISO 27002-2013 [10]. Keamanan informasi memiliki kontrol keamanan yang berguna untuk perlindungan dari berbagai macam ancaman dan memastikan keberlanjutan bisnis serta meminimalisir risiko dan meningkatkan investasi dan peluang bisnis. Berikut adalah klausal keamanan yang terdapat pada ISO 27002-2013:

Tabel 1. Klausa Keamanan Pada ISO 27002-2013

No. Klausal		Jumlah	
		Objek Kontrol	Kontrol
5	Kebijakan Keamanan Informasi	1	2
6	Organisasi Keamanan Informasi	2	7
7	Keamanan Sumber Daya Manusia	3	6
8	Manajemen Aset	3	10
9	Kontrol Akses	4	13
10	Kriptografi	1	2

Tabel 2. Penjelasan Klausal Keamanan Pada ISO 27002-2013

NO	NO. Klausul	Klausul Kontrol Keamanan	Penjelasan
1	5	Kebijakan Keamanan Informasi	Memberikan arahan kepada manajemen organisasi dan dukungan untuk keamanan informasi dalam hubungannya dengan persayaratan bisnis organisasi, hukum, dan aturan yang sedang berlaku
2	6	Organisasi Keamanan Informasi	Bagaimana mengelola keamanan informasi di dalam organisasi baik itu yang hubungan internal organisasi maupun terhadap pihak eksternal (pihak eksternal, vendor, dll)
3	7	Keamanan Sumber Daya Manusia	Memastikan bahwa karyawan dan kontraktor memahami tanggung jawab mereka dan sesuai untuk peran yang mereka pertimbangkan
4	8	Manajemen Aset	Untuk mengenali aset organisasi dan menerapkan tanggung jawab perlindungan yang sesuai dengan organisasi
5	9	Kontrol Akses	Untuk memastikan pengendalian dari setiap informasi
6	10	Kriptografi	Untuk memastikan penggunaan kriptografi secara tepat dan efektif dalam melindungi kerahasian, keaslian dan beutuhan sebuah informasi

Defence in Depth (DiD) adalah strategi keamanan siber yang menggunakan serangkaian lapisan pertahanan untuk menjaga keamanan data dan informasi yang penting. Jika satu lapisan pertahanan gagal, lapisan lainnya akan segera aktif untuk menghentikan serangan tersebut [11]. Pendekatan ini, yang didasarkan pada

Jurnal Manajemen Teknologi dan Sistem Informasi (JMS)
Volume 5, Nomor 1, Maret 2025
ISSN 2808-5450 (media cetak), ISSN 2808-5019 (media online)
Available Online at https: http://ejournal.unama.ac.id/index.php/jms
DOI https://10.33998/jms.v5i1

redundansi yang disengaja, meningkatkan keamanan sistem secara keseluruhan dan mengatasi berbagai jenis serangan yang mungkin terjadi. Konsep pertahanan dalam kedalaman ini sering diibaratkan sebagai pendekatan kastil, merujuk pada sistem pertahanan berlapis yang ditemui dalam kastil abad pertengahan.

Dari penjabaran diatas, penelitian ini bertujuan untuk melakukan analisis mendalam terhadap risiko bisnis yang berkaitan dengan keamanan informasi dan *cyber* pada Bank Syariah Indonesia (BSI). Pendekatan studi kasus yang digunakan pada penelitian ini memiliki fokus utama yaitu untuk mengidentifikasi, menganalisis, dan mengevaluasi berbagai jenis risiko yang dihadapi oleh BSI dalam ranah keamanan informasi dan *cyber*. Pemahaman yang mendalam terhadap risiko-risiko tersebut, diharapkan dapat dikembangkan strategi mitigasi yang efektif dan berkelanjutan untuk melindungi aset informasi dan kepentingan bisnis BSI. Studi kasus ini juga memberikan kontribusi penting bagi pemahaman umum tentang praktik keamanan informasi dan *cyber* di sektor perbankan syariah. Secara khusus, penelitian ini dapat memberikan wawasan yang berharga bagi institusi sejenis, serta menjadi landasan untuk pengembangan kebijakan dan praktik terbaik dalam menjaga keamanan informasi dan *cyber* di lingkungan bisnis yang serba digital.

2. METODOLOGI PENELITIAN

2.1 Objek Penelitian

Objek penelitian dalam studi ini adalah mencakup risiko-risiko terkait dengan kerahasiaan, integritas, dan ketersediaan informasi yang dimiliki oleh PT. Bank Syariah Indonesia (BSI). Ancaman-ancaman ini bisa berasal dari faktor internal maupun eksternal seperti kesalahan manusia, serangan siber atau kegagalan sistem.

2.2 Metode Pengumpulan Data

1. Studi Literatur

Menurut Nurjanah, et al (2021), studi literatur adalah pendekatan penelitian yang fokus pada peninjauan dan integrasi hasil-hasil penelitian yang relevan dan signifikan dalam upaya untuk memahami suatu fenomena, topik, atau isu tertentu [12].Studi literatur dilakukan untuk memperoleh informasi dan data yang berguna dalam penelitian. Data dan informasi diambil dari literatur-literatur yang berkaitan, berasal dari jurnal, buku, serta skripsi penelitian terdahulu.

2. Wawancara

Metodologi wawancara adalah pendekatan penelitian yang melibatkan interaksi langsung antara peneliti dan responden dengan tujuan untuk memperoleh informasi, pandangan, atau pengalaman dari perspektif responden [13]. Wawancara dilakukan kepada pengguna bank BSI dan kepala cabang untuk mengetahui kondisi perusahaan, aktivitas perusahaan, risiko yang muncul serta sumber risiko.

2.2 Alur Penelitian

Gambar 1. Alur Penelitian

Penelitian ini dimulai dengan melakukan identifikasi permasalahn yang akan dibahas pada penelitian ini yaitu identifikasi resiko digital dan kemanan siber pada Bank Syariah Indonesia (BSI). Setelah mengetahui permasalahan yang akan dibahas, langkah selanjutnya adalah melakukan studi literatur. Studi literatur berguna untuk memperkuat pengetahuan tentang teori yang digunakan dalam penelitian ini sehingga teori yang digunakan dapat relevan dengan masalah yang akan dibahas. Langkah selanjutnya adala menentukan metodologi penelitian. Metodologi penelitian bertujuan untuk mempermudah proses pencarian data dan proses pengolahan data pada suatu penelitian. Pada penelitian ini, metode penelitiannya adalah kualitatif yang menggunakan studi literatur dalam menganalisa permasalahan dan solusi yang ditawarkan. Langkah selanjutnya pada penelitian ini adalah membahas hasil dari temuan pada penelitian ini. Langkah terakhir yang dilakukan dalam penelitian ini memberikan kesimpulan atas penelitian ini serta memberikan saran kepada BSI tentang resiko digital yang dihadapi mereka.

Jurnal Manajemen Teknologi dan Sistem Informasi (JMS)
Volume 5, Nomor 1, Maret 2025
ISSN 2808-5450 (media cetak), ISSN 2808-5019 (media online)
Available Online at https: http://ejournal.unama.ac.id/index.php/jms
DOI https://10.33998/jms.v5i1

3. HASIL DAN PEMBAHASAN

3.1 Layanan Digital

Perkembangan teknologi digital saat ini semakin masif, salah satunya adalah di bidang perbankan. Perbankan digital terus berevolusi dan melahirkan berbagai inovasi guna menjawab kebutuhan dan memenuhi gaya hidup masyarakat yang kini telah bertransformasi ke dalam bentuk digital [14]. Layanan perbankan digital adalah sebuah kegiatan atau layanan perbankan yang sarananya menggunakan sistem elektronik atau digital melalui milik bank, milik calon nasabah, atau nasabah bank tersebut, yang semua prosesnya secara mandiri dan terotomasi [1].

Perbankan digital dapat membantu kebutuhan nasabah untuk dapat mengakses layanan perbankan termasuk pembuatan rekening dan registrasi (*onboarding*), melakukan pembayaran, transaksi *e-commerce*, mengajukan pinjaman, investasi, hingga pengelolaan keuangan secara mudah, cepat, dimanapun dan kapanpun. Keamanan selalu jadi prioritas tertinggi dalam penyediaan layanan perbankan digital. Kini, nomor pin bukan jadi pertahanan keamanan satu-satunya saat bertransaksi [15]. Terdapat *multi-factor authentication* yang menjamin keamanan rekening, misalnya hadirnya otentikasi biometrik, dan OTP (*one-time password*). Meski begitu, tantangan *cybersecurity* yang dihadapi perbankan digital juga ikut berevolusi, misalnya maraknya *social engineering* yang memanfaatkan ketidaktahuan dan keawaman masyarakat dengan literasi digital yang rendah. Karena itu, pertumbuhan perbankan digital juga perlu diikuti dengan edukasi dan usaha-usaha peningkatan literasi digital [16].

Digital banking merupakan transformasi perbankan yang mengadaptasi produk, proses, dan aktivitas perbankan ke ranah digital guna memberikan layanan kepada nasabah secara online. Ini telah mengubah cara interaksi pelanggan dengan layanan perbankan, meningkatkan kenyamanan dan aksesibilitas dengan layanan 24/7 melalui perangkat digital [17]. Perbankan digital memudahkan nasabah dalam transaksi keuangan dan membuka produk perbankan tanpa harus ke kantor cabang. Bank Syariah Indonesia (BSI) menawarkan beragam layanan digital, seperti Pembiayaan BSI OTO dan BSI Mobile, yang telah mencatat peningkatan penggunaan yang signifikan.

Bank Syariah Indonesia (BSI) menyediakan layanan perbankan digital yang memungkinkan pelanggan untuk mengakses layanan perbankan melalui berbagai perangkat digital seperti *smartphone*, tablet, atau komputer. Layanan digital ini mencakup beragam produk dan fitur, termasuk Pembiayaan BSI OTO, BSI *Smart Agent*, BSI *Mobile*, BSI Aisyah, Solusi Emas, BSI JadiBerkah id, BSI ATM CRM (*Cash Recycle Machine*), BSI *Merchant Business*, BSI API *Platform*, BSI *Cardless Withdrawal*, BSI *Payment Point*, BSI QRIS, Buka Rekening Online, BSI Net, Mitraguna Online, BSI *Debt Card*, BSI Debt OTP, Deposito *Mobile*, Griya Hasanah Online, dan E-mas BSI Mobile.

3.2 Resiko Bisnis dan Ancaman Keamanan

Umumnya, para pelanggan menghadapi berbagai risiko keamanan ketika menggunakan layanan perbankan digital, seperti risiko keamanan siber, phishing, malware, dan serangan *denial of service* (DoS). Risiko keamanan siber melibatkan ancaman dari pihak yang tidak bertanggung jawab yang berusaha untuk mengakses, merusak, atau mencuri data dan informasi penting dari sistem perbankan digital [18]. Namun, keberadaan layanan digital juga membawa risiko keamanan, seperti serangan siber, *phishing*, dan *malware*, yang dapat membahayakan data dan informasi nasabah. Gangguan pada layanan digital BSI pada Mei 2023 dan dugaan pencurian data menyoroti pentingnya peningkatan ketangguhan terhadap serangan siber dalam perbankan digital. BSI telah mengalokasikan dana besar untuk memperkuat keamanan data dan melakukan langkah preventif [19].

Pada 16 Mei 2023, Bank Syariah Indonesia (BSI) mengonfirmasi bahwa data nasabah dan dana tetap dalam keadaan aman meskipun terjadi gangguan pada layanan mereka. Otoritas Jasa Keuangan (OJK) mendorong BSI untuk memastikan layanan kembali normal setelah insiden tersebut, dan meminta seluruh lembaga keuangan di sektor perbankan untuk memperkuat ketahanan digital mereka [19]. Pada 18 Mei 2023, kelompok *ransomware LockBit* mengklaim telah mencuri 1,5 *terabyte* data dari BSI setelah negosiasi tebusan gagal. Ini menunjukkan bahwa BSI mengalami gangguan serius pada layanan digital mereka yang berdampak pada nasabah [19].

Selain banyaknya peluang untuk bisa menjadi perbankan digital untuk memenuhi kebutuhan masyarakat, ada juga tantangan yang menyertai. Tantangan tersebut dapat berasal dari internal maupun eksternal perbankan digital tersebut. Tantangan internal misalnya mengenai adanya perubahan kultur dan pola pikir dalam perusahaan. Secara internal, pemain perbankan digital harus menyiapkan infrastruktur IT dan sistem *cybersecurity* yang mumpuni. Selain itu, dari segi pengembangan fitur dan layanan keuangan juga harus mampu menjawab kebutuhan nasabah yang terus berubah. Sementara dari faktor eksternal, pengembangan layanan perbankan digital juga harus mempertimbangkan beragamnya tingkat literasi keuangan literasi digital, dan kemampuan adopsi digital dari target pasar [20].

Layanan *digital banking* merupakan suatu layanan terhadap nasabah untuk memperoleh suatu informasi, adanya komunikasi, dan melakukan transaksi perbankan secara digital yang mengoptimalkan dalam memanfaatkan data nasabah serta melayani nasabah secara cepat, praktis, dan mudah. Layanan *digital banking*, antara lain *internet banking*, *mobile banking*, dan *sms banking*. Media elektronik merupakan media yang paling

Volume 5, Nomor 1, Maret 2025
ISSN 2808-5450 (media cetak), ISSN 2808-5019 (media online)
Available Online at https: http://ejournal.unama.ac.id/index.php/jms
DOI https://10.33998/jms.v5i1

sering digunakan oleh nasabah. Adapun cara penggunaan dari produk dan layanan digital tersebut sangat mudah karena ditujukan untuk mempermudah nasabah saat melakukan pembayaran secara digital.

3.3 Perlindungan Hukum

Perlindungan hukum terhadap nasabah BSI didasarkan pada Undang-Undang Perlindungan Konsumen (UUPK), yang memberikan dasar bagi nasabah untuk mendapatkan kompensasi atas kerugian yang timbul akibat kebocoran data atau perbuatan melawan hukum oleh bank. Prinsip pertanggungjawaban mutlak dalam UUPK menuntut BSI untuk bertanggung jawab tanpa pembuktian kesalahan dalam kasus kebocoran data nasabah [21]. Jika dilihat dari fungsi dan perannya, bank syariah sebenarnya tidak berbeda dengan bank konvensional, yaitu sebagai lembaga intermediasi keuangan.

Maksudnya, bank syariah berfungsi menjembatani antara pihak yang kelebihan dana dan pihak yang memerlukan dana [21]. Baik bank syariah maupun bank konvensional, keduanya tunduk pada peraturan perbankan secara umum, seperti Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan (UU Perbankan) sebagaimana diubah dengan Undang-Undang Nomor 10 Tahun 1998 tentang Perubahan Atas Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan (UU 10/1998). Kedua lembaga ini juga sama-sama harus patuh terhadap regulasi yang dikeluarkan oleh Otoritas Jasa Keuangan tentang persyaratan permodalan, prinsip kehati-hatian, dan berbagai regulasi terkait dengan kesehatan perbankan [22].

3.4 Protokol Keamanan

Bank Syariah Indonesia (BSI) telah menerapkan serangkaian langkah keamanan untuk menjaga nasabahnya terlindungi. Ketika menghadapi serangan *ransomware*, perusahaan yang menjadi korban harus menghubungi penegak hukum, lembaga penanganan darurat serangan siber, atau perusahaan keamanan siber. BSI menggunakan berbagai teknologi keamanan, termasuk enkripsi data, otentikasi dua faktor, dan sistem keamanan lainnya. BSI telah mengalokasikan dana sebesar Rp 580 miliar untuk memperkuat digitalisasi dan keamanan data sebagai respons terhadap gangguan layanan dan isu kebocoran data yang terjadi sebelumnya [19]. BSI juga menekankan bahwa anggaran tersebut akan digunakan untuk meningkatkan keamanan data dan layanan perbankan. BSI mengambil langkah preventif dengan memperkuat sistem keamanan teknologi informasi untuk menghadapi potensi gangguan data, termasuk peningkatan proteksi dan ketahanan sistem. BSI berkoordinasi dengan pihak terkait seperti Badan Siber dan Sandi Negara (BSSN), Otoritas Jasa Keuangan (OJK), dan Bank Indonesia (BI) [23].

Melindungi data nasabah menjadi fokus utama, dengan BSI mengadopsi teknologi keamanan dan berkoordinasi dengan lembaga terkait, seperti OJK dan BSSN. Meskipun upaya-upaya ini penting, keberhasilan dalam mengamankan data nasabah juga memerlukan kepatuhan terhadap regulasi serta implementasi praktik terbaik yang terbukti efektif [24].

3.5 Pengelolaan Keamanan *Cyber*

BSI tentunya memiliki tanggung jawab untuk memberikan kompensasi kepada nasabah yang terkena dampak dari kesus kebocoran data yang terjadi. Pertanggungjawaban bisa berlandaskan sesuai dengan prinsip-prinsip pertanggungjawaban dalam UUPK. Perlindungan hukum dan kebijakan keamanan yang efektif adalah landasan penting bagi keberlanjutan dan kepercayaan nasabah dalam ekonomi digital [22]. Perkembangan digitalisasi di sektor perbankan telah meningkatkan risiko terhadap serangan siber bagi bank. Lonjakan serangan siber telah mendorong kebutuhan untuk meningkatkan ketahanan siber melalui penguatan keamanan siber. Upaya penguatan keamanan siber telah menghasilkan berbagai inisiatif di berbagai sektor industri, termasuk sektor perbankan, untuk mengatasi risiko siber oleh regulator di berbagai negara. Terutama, sektor keuangan, termasuk perbankan, menjadi target serangan siber paling tinggi baik secara global maupun di Indonesia [25].

Beberapa negara telah mengimplementasikan kebijakan khusus terkait keamanan siber, termasuk kebijakan terkait pengelolaan keamanan siber, penilaian risiko siber, pengujian kerentanan teknologi informasi, penilaian tingkat maturitas siber, dan pengujian keamanan siber . Keamanan siber sendiri adalah praktik untuk melindungi komputer, jaringan, perangkat lunak, dan data dari ancaman digital. Kategori ancaman digital yang sering muncul seperti virus, *malware*, peretasan, *phising*, dan serangan *ransomware*. Contoh beberapa kebijakan keamanan siber yang telah dilakukan di beberapa negara seperti India yang mulai menerapkan kebijakan kemanan siber nasional pada tahun 2013 yang bertujuan untuk meningkatkan keamanan dunia maya di India. Kebijakan kemanan siber di India ini meliputi melindungi infrastuktur dan informasi dunia maya dan memabangun kapasitas untuk mencegah dan menanggapi ancaman keamanan siber [26].

Menurut Alwi et al (2023), sistem pertahanan siber di bank-bank Indonesia dinilai kurang kuat, yang tampaknya menjadi masalah yang lebih luas dengan beberapa bank sebelumnya mengalami serangan siber, termasuk Bank Indonesia pada awal 2022 [1]. Penting bagi Bank Syariah Indonesia dan bank-bank lainnya di Indonesia untuk memperkuat sistem pertahanan digital mereka mengingat sektor keuangan, khususnya perbankan,

Volume 5, Nomor 1, Maret 2025
ISSN 2808-5450 (media cetak), ISSN 2808-5019 (media online)
Available Online at https: http://ejournal.unama.ac.id/index.php/jms
DOI https://10.33998/jms.v5i1

menjadi target serangan siber paling tinggi baik secara global maupun di Indonesia. Langkah-langkah yang perlu dipertimbangkan termasuk penerapan kebijakan terkait pengelolaan keamanan siber, penilaian risiko siber, pengujian kerentanan teknologi informasi, penilaian tingkat maturitas siber, dan pelaksanaan pengujian keamanan siber, sesuai dengan praktik terbaik yang telah terbukti di berbagai negara [27].

Meskipun peningkatan keamanan jaringan dan sistem melalui penerapan *firewall*, enkripsi data, dan pemantauan aktif dapat membantu mencegah serangan siber, tidak ada jaminan bahwa suatu sistem akan sepenuhnya aman dari serangan *ransomware*. Oleh karena itu, penting untuk mengimplementasikan mitigasi yang tepat dan melakukan persiapan yang baik. Praktik terbaik yang telah terbukti, seperti yang telah diimplementasikan di berbagai negara, seharusnya juga dipertimbangkan untuk diadopsi oleh bank syariah Indonesia guna memitigasi potensi ancaman dan kerentanan siber yang dapat mengancam keamanan digital mereka.

Untuk melawan serangan *ransomware* yang semakin berkembang, perusahaan memerlukan langkah-langkah keamanan siber yang tangguh. Menjawab tantangan ini, Helios Informatika Nusantara (HIN) menawarkan *Sangfor Cyber Command*, sebagai solusi *Network Detection and Response* (NDR) yang canggih dengan perlindungan komprehensif terhadap ancaman siber yang terus berkembang [16]. *Sangfor Cyber Command* adalah solusi yang menawarkan platform *Security Management* komprehensif untuk amankan bisnis dari berbagai ancaman siber. Menggunakan algoritma *Machine Learning* dan analitik *big data*, *Sangfor Cyber Command* dapat mengidentifikasi dan mencegah potensi serangan sebelum terjadi kerusakan yang dapat merugikan bisnis .

Kemampuan deteksi ancaman tingkat lanjut agar pengguna dapat mengidentifikasi dan merespons berbagai potensi ancaman keamanan secara *real-time*. Termasuk kemampuan blokir *ransomware*, *malware*, dan berbagai ancaman siber lainnya. Dapatkan visibilitas dan kontrol atas infrastruktur jaringan, termasuk monitoring trafik jaringan, kontrol akses ke sumber daya, dan mengelola kebijakan jaringan. Amankan aplikasi dan infrastruktur *cloud-based* dari berbagai ancaman yang secara spesifik menyasar *cloud*, misalnya pencurian data, pembajakan akun, dan ancaman internal [24].

Platform manajemen keamanan komprehensif untuk memudahkan pengelolaan dan monitoring seluruh infrastruktur IT hanya melalui satu konsol. *Sangfor Cyber Command* menyediakan berbagai fitur dan kemampuan untuk melindungi perusahaan dari berbagai ancaman dan serangan siber. Berikut ini beberapa fitur utama yang ditawarkan *Sangfor Cyber Command*. Dukungan teknologi algoritma AI dan *Machine Learning* tingkat lanjut untuk memberikan kecerdasan komprehensif saat mengidentifikasi potensi ancaman siber secara proaktif.

3.6 Pertanggung Jawaban Bank Syariah Indonesia

Tanggung jawab Bank Syariah Indonesia (BSI) terhadap kebocoran data nasabah diatur oleh prinsip-prinsip pertanggungjawaban dalam Undang-Undang Perlindungan Konsumen (UUPK). Prinsip-prinsip tersebut mencakup beberapa aspek yang penting [21]. Pertama, prinsip tanggung jawab berdasarkan unsur kesalahan, yang mengimplikasikan bahwa seseorang hanya diminta pertanggungjawabannya jika ada bukti kesalahannya. Ini sejalan dengan Pasal 1365 KUHPerdata yang menetapkan penggantian kerugian akibat tindakan melanggar hukum. Kedua, prinsip praduga untuk selalu bertanggung jawab menempatkan beban pembuktian pada tergugat, yang diasumsikan bertanggung jawab sampai dapat membuktikan tidak bersalah. Prinsip ini mendorong tanggung jawab atas setiap kerugian yang bersalah.

Ketiga, prinsip praduga untuk tidak selalu bertanggung jawab dibatasi pada transaksi konsumen dengan pembatasan yang masuk akal secara umum. Keempat, prinsip tanggung jawab mutlak atau strict liability menetapkan tanggung jawab tanpa mempertimbangkan unsur kesalahan, meskipun ada pengecualian seperti force majeure. Terakhir, prinsip tanggung jawab dengan pembatasan mengacu pada pembatasan tanggung jawab yang tidak merugikan konsumen dan harus sesuai dengan peraturan perundang-undangan yang jelas [25].

Dalam konteks BSI, UUPK menunjukkan bahwa BSI harus bertanggung jawab atas kebocoran data nasabah tanpa perlu pembuktian unsur kesalahan. UUPK juga mengatur bentuk ganti rugi terhadap perbuatan melawan hukum, seperti ganti rugi nominal, ganti rugi kompensasi, dan ganti rugi penghukuman. Pasal 47 ayat (1) Undang-Undang Nomor 21 Tahun 2008 tentang perbankan syariah menetapkan bahwa bank syariah harus menjamin kerahasiaan data nasabah, dengan tanggung jawab atas kerugian yang timbul jika terjadi kebocoran data, kecuali dapat membuktikan bahwa kebocoran tersebut bukan karena kesalahan bank syariah. Pasal 48 ayat (1) UU tersebut juga mengatur bahwa bank syariah wajib memberikan ganti rugi atas kerugian yang diderita nasabah akibat perbuatan melawan hukum yang dilakukan oleh bank syariah atau pegawainya. Dalam kasus kebocoran data nasabah BSI yang diduga dilakukan oleh *hacker*, prinsip-prinsip tersebut menunjukkan bahwa BSI harus memberikan ganti rugi kompensasi kepada nasabah yang terdampak [22].

Kasus ini menghasilkan kerugian pada nasabah, sehingga pihak bank wajib mengganti kerugian sesuai dengan aturan yang berlaku. Nasabah berhak untuk menuntut ganti rugi melalui jalur hukum yang sesuai dengan peraturan yang berlaku, dengan beban pembuktian terletak pada pihak nasabah yang bermasalah. Dengan pertumbuhan ekonomi digital yang pesat, perlindungan nasabah dalam pemanfaatan layanan digital banking menjadi esensial.

Volume 5, Nomor 1, Maret 2025
ISSN 2808-5450 (media cetak), ISSN 2808-5019 (media online)
Available Online at https: http://ejournal.unama.ac.id/index.php/jms
DOI https://10.33998/jms.v5i1

Implementasi perlindungan hukum serta kebijakan keamanan yang efektif akan menjadi landasan penting bagi keberlanjutan dan kepercayaan nasabah dalam era ekonomi digital. Oleh karena itu, untuk mencapai keberhasilan dalam era ekonomi digital, bank syariah wajib untuk lebih ketat dalam melindungi data dari nasabah atau konsumennya.

4. KESIMPULAN DAN SARAN

4.1 Kesimpulan

Dari penelitian ini didapati bahwa tantangan utama yang diidentifikasi adalah keberadaan ancaman serius seperti serangan *malware* dan *phishing* menunjukkan perlunya perhatian khusus terhadap deteksi dan pencegahan dan risiko *insider threats* menyoroti pentingnya meningkatkan kesadaran keamanan internal dan mengimplementasikan kontrol akses yang ketat. Untuk mengatasi tantangan tersebut, kontrol dan respons yang diperlukan adalah dengan melakukan perbaikan pada sistem deteksi intrusi dan respons terhadap insiden harus dilakukan untuk meminimalkan dampak serangan *cyber* dan melakukan pelatihan keamanan secara teratur harus diselenggarakan untuk meningkatkan kesadaran karyawan terhadap praktik keamanan yang baik. Aspek kebijakan dan kepatuhan yang dapat dilakukan dengan pembaharuan kebijakan keamanan secara berkala sesuai dengan perkembangan teknologi dan ancaman baru dan juga pentingnya mematuhi standar keamanan industri dan regulasi pemerintah untuk mengurangi risiko kepatuhan dan sanksi.

4.2 Saran

Beberapa saran yang dapat dilakukan oleh pihak Bank Syariah Indonesia dalam penanganan resiko teknologi adalah dengan penguatan infrastruktur TI seperti investasi dalam sistem keamanan yang lebih canggih dan *up-to-date* untuk mengatasi ancaman siber yang semakin kompleks. Peningkatan kesadaran keamanan juga dapat dilakukan seperti pelatihan rutin untuk semua karyawan tentang praktik keamanan informasi yang baik dan konsekuensi dari pelanggaran kebijakan. Peningkatan respons terhadap insiden seperti pembentukan tim respons terhadap insiden yang terlatih dengan baik untuk mengurangi waktu tanggap terhadap serangan *cyber*.

REFERENCES

[1] M. N. Alwi, F. Bahari, M. Turot, A. Nainggolan, and R. Semmawi, “Tantangan dan Peluang Perbankan Digital: Studi Kasus Inovasi Keuangan dan Transformasi Perbankan,” *Jurnal Cahaya Mandalika*, vol. 3, no. 2, pp. 2160–2177, 2023.

[2] E. R. M. Sembiring, N. Nurbaiti, and A. N. Daulay, “Pengaruh Ancaman Siber Ransomware dan Gangguan Sistem Layanan Mobile Banking Terhadap Kepercayaan Nasabah pada Bank BSI KCP Kisaran,” *JURNAL MANAJEMEN PENDIDIKAN DAN ILMU SOSIAL*, vol. 5, no. 4, pp. 880–887, 2024.

[3] D. Hendarsyah, “Keamanan Layanan Internet Banking Dalam Transaksi Perbankan,” *IQTISHADUNA: Jurnal Ilmiah Ekonomi Kita*, vol. 1, no. 1, pp. 12–33, 2012.

[4] D. Fatmala Putri and W. Ratna Sari, “ANALISIS PERLINDUNGAN NASABAH BSI TERHADAP KEBOCORAN DATA DALAM MENGGUNAKAN DIGITAL BANKING,” *Jurnal Ilmiah Ekonomi dan Manajemen*, vol. 1, no. 4, pp. 173–181, 2023, doi: 10.61722/jiem.v1i4.331.

[5] R. Hafidz, F. D. Setiawan, and F. Sinlae, “Keamanan Cybersecurity: Strategi Geometri Politik Dan Pembangunan Global Terkhusus Asia Tenggara,” *Nusantara Journal of Multidisciplinary Science*, vol. 1, no. 6, 2024.

[6] B. Widyaningsih and T. I. Afan, “Peran Manajemen Resiko dalam Meningkatkan Ketahanan Bank Syariah di Era Digital,” *Jurnal Masharif Al-Syariah: Jurnal Ekonomi dan Perbankan Syariah*, vol. 9, no. 3, 2024.

[7] M. A. Arifin, F. A. Azzahra, R. Hidayat, and M. Ikaningtyas, “Pengelolaan Risiko Bisnis Dalam Lingkungan Ekonomi Global yang Dinamis,” *IJM: Indonesian Journal of Multidisciplinary*, vol. 2, no. 3, 2024.

[8] I. Hassandi, M. Gustiana Pangestu, A. Septiawan Syaputra, T. Qur’aini, and A. Tri Agustin, “ANALISIS SWOT DALAM PENENTUAN STRATEGI BISNIS PADA UMKM AULIA SNACK JAMBI,” *Jurnal Ilmiah Manajemen dan Kewirausahaan (JUMANAGE)*, vol. 3, no. 2, 2024, [Online]. Available:

Volume 5, Nomor 1, Maret 2025
ISSN 2808-5450 (media cetak), ISSN 2808-5019 (media online)
Available Online at https: http://ejournal.unama.ac.id/index.php/jms
DOI https://10.33998/jms.v5i1

http://creativecommons.org/licenses/by/4.0/JUMANAGEhttps://ejournal.unama.ac.id/index.php/jumanage

[9] M. Kadar, I. Hassandi, I. Khoirunnisa, S. Handayani, and T. Adi Yonathan, "Analisis Resiko pada UMKM Pabrik Kerupuk Putri Bungsu di Kota Jambi," *Jurnal Ilmiah Manajemen dan Kewirausahaan (JUMANAGE)*, vol. 3, no. 2, p. 425, 2024, [Online]. Available: http://creativecommons.org/licenses/by/4.0/JUMANAGEhttps://ejournal.unama.ac.id/index.php/jumanage

[10] H. Afandi and A. Darmawan, "AUDIT KEMANAN INFORMASI MENGGUNAKAN ISO 27002 PADA DATA CENTER PT.GIGIPATRA MULTIMEDIA," *Jurnal TIM Darmajaya*, vol. 01, no. 02, pp. 175–191, 2015.

[11] S. Nurul, S. Anggrainy, and S. Aprelyani, "Faktor-Faktor Yang Mempengaruhi Keamanan Sistem Informasi: Keamanan Informasi, Teknologi Informasi Dan Network (Literature Review Sim)," *Jurnal Ekonomi Manajemen Sistem Informasi*, vol. 3, no. 5, pp. 564–573, 2022.

[12] N. E. Nurjanah and T. T. Mukarromah, "Pembelajaran berbasis media digital pada anak usia dini di era revolusi industri 4.0: Studi literatur," *Jurnal Ilmiah Potensia*, vol. 6, no. 1, 2021.

[13] Q. Fauziah, "Penerapan Metode Wawancara Narasumber Untuk Meningkatkan Kemampuan Menulis Teks Tanggapan," *Language: Jurnal Inovasi Pendidikan Bahasa dan Sastra*, vol. 3, no. 2, pp. 77–83, 2023.

[14] H. Shabri, "Transformasi digital industri perbankan syariah Indonesia," *El-Kahfi| Journal of Islamic Economics*, vol. 3, no. 2, pp. 228–234, 2022.

[15] shahnila F. Bayastura, S. Krisdina, and A. P. Widodo, "analisis tata kelola teknologi informasi menggunakan framework cobit 2019 pada pt. xyz," *JIKO (Jurnal Informatika dan Komputer)*, vol. 4, no. 1, pp. 68–75, 2021.

[16] F. M. Hutabarat and A. D. Manuputty, "Analisis Resiko Teknologi Informasi Aplikasi VCare PT Visionet Data Internasional Menggunakan ISO 31000," *Jurnal Bina Komputer*, vol. 2, no. 1, pp. 52–65, 2020.

[17] I. Hassandi, M. Haris Sapura, K. Puspa Kirana Lie, F. Ilmu Manajemen dan Bisnis, P. Studi Kewirausahaan, and U. Dinamika Bangsa, "Analisis Faktor Yang Berpengaruh Terhadap Kesadaran Pengguna Dalam Memakai Aplikasi E-Wallet Studi Kasus: Masyarakat Kota Jambi," *Jurnal Manajemen Teknologi dan Sistem Informasi (JMS)*, vol. 3, no. 1, 2023, [Online]. Available: http://ejournal.unama.ac.id/index.php/jms

[18] N. I. Putri, D. Widhiantoro, Z. Munawar, and H. Soerjono, "Penerapan Manajemen Resiko Pada Komputasi Awan," *TEMATIK*, vol. 9, no. 2, pp. 144–151, 2022.

[19] R. Binekasari, "Perkuat Keamanan Digital, BSI Gandakan Capex IT Jadi Rp580 M," https://www.cnbcindonesia.com/market/20230523065444-17-439619/perkuat-keamanan-digital-bsi-gandakan-capex-it-jadi-rp580-m.

[20] F. Novianto, "Evaluation of e-government information security using the defense in depth model," *Cyber Security dan Forensik Digital*, vol. 3, no. 1, pp. 14–19, 2020.

[21] M. O. Muhammad and L. D. Nugroho, "Perlindungan Hukum Terhadap Pengguna Aplikasi E-Commerce Yang Terdampak Kebocoran Data Pribadi," *Jurnal Pamator: Jurnal Ilmiah Universitas Trunojoyo*, vol. 14, no. 2, pp. 165–174, 2021.

[22] A. N. Rohman, "Urgensi Pengaturan Fintech Lending Syariah Di Indonesia: Analisis Perlindungan Hukum Bagi Pengguna Layanan," *Jurnal Legislasi Indonesia*, vol. 20, no. 1, p. 16, 2023.

[23] S. R. Buwono, L. Abubakar, and T. Handayani, "Kesiapan Perbankan Menuju Transformasi Digital Pasca Pandemi Covid-19 Melalui Financial Technology (Fintech)," *Jurnal Poros Hukum Padjadjaran*, vol. 3, no. 2, pp. 228–241, 2022.

[24] A. Mosteiro-Sanchez, M. Barcelo, J. Astorga, and A. Urbieta, "Securing IIoT using defence-in-depth: towards an end-to-end secure industry 4.0," *J Manuf Syst*, vol. 57, pp. 367–378, 2020.

Volume 5, Nomor 1, Maret 2025
ISSN 2808-5450 (media cetak), ISSN 2808-5019 (media online)
Available Online at https: http://ejournal.unama.ac.id/index.php/jms
DOI https://10.33998/jms.v5i1

[25] L. Abubakar and T. Handayani, "Penguatan regulasi Upaya percepatan transformasi digital perbankan di era ekonomi digital," *Masalah-Masalah Hukum*, vol. 51, no. 3, pp. 259–270, 2022.

[26] R. A. Rossdiana and T. R. Fahrisa, "STRATEGI CYBERSECURITY PEMERINTAH INDIA DARI PERSPEKTIF KAUTILYA," *Indonesian Journal of International Relations*, vol. 7, no. 1, pp. 140–164, Mar. 2023, doi: 10.32787/ijir.v7i1.408.

[27] Y. Ngamal and M. A. Perajaka, "Penerapan Model Manajemen Risiko Teknologi Digital Di Lembaga Perbankan Berkaca Pada Cetak Biru Transformasi Digital Perbankan Indonesia," *Jurnal Manajemen Risiko*, vol. 2, no. 2, pp. 59–74, 2022.