

CYBER CRIME SEBAGAI RISIKO SISTEMIK PADA BANK DIGITAL SYARIAH DI INDONESIA: ANALISIS PERSPEKTIF TEORI RISIKO ULRICH BECK

Hasanatul Munawarah¹, Masdar Hilmy², Desi Erawati³

^{1,3} Universitas Islam Negeri Palangkaraya

² Universitas Islam Negeri Sunan Ampel Surabaya

hasanatulmunawarah2510310051@uin-palangkaraya.ac.id¹, masdar.hilmy@uinsa.ac.id², desi.erawati@uin-palangkaraya.ac.id³

ARTICLE INFO

ABSTRACT

Article History

Published: 30 Aug 2026

Keywords:

Cyber Crime, Bank Digital Syariah, Risiko Sistemik, Ulrich Beck, Risk Society.



© Author(s) 2026
This work is licensed under a [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

Cyber Crime sebagai risiko sistemik dalam konteks bank digital syariah di Indonesia, dengan kerangka teori Risk Society dari Ulrich Beck. Perkembangan pesat teknologi digital membawa peluang sekaligus tantangan signifikan bagi sektor perbankan syariah, khususnya terkait keamanan siber. Penelitian ini mengkaji bagaimana risiko kejahatan siber, yang meliputi berbagai bentuk serangan digital, dapat mengancam stabilitas dan keberlanjutan bank digital syariah. Melalui pendekatan kualitatif dengan studi literatur dan analisis data sekunder, penelitian ini mengidentifikasi kerentanan sistemik yang muncul akibat digitalisasi perbankan, serta implikasinya terhadap perlindungan nasabah dan kepercayaan publik. Hasil penelitian menunjukkan bahwa bank digital syariah di Indonesia menghadapi risiko kejahatan siber yang kompleks dan multidimensional, yang memerlukan strategi mitigasi komprehensif. Penelitian ini juga mengusulkan rekomendasi kebijakan untuk meningkatkan keamanan siber, memperkuat regulasi, dan meningkatkan kesadaran masyarakat tentang risiko digital dalam ekosistem perbankan syariah.

Cybercrime as a systemic risk in the context of Islamic digital banks in Indonesia, using Ulrich Beck's Risk Society theoretical framework. The rapid development of digital technology brings significant opportunities and challenges to the Islamic banking sector, particularly regarding cybersecurity. This study examines how cybercrime risks, which include various forms of digital attacks, can threaten the stability and sustainability of Islamic digital banks. Through a qualitative approach with literature review and secondary data analysis, this study identifies systemic vulnerabilities arising from banking digitalization, as well as their implications for customer protection and public trust. The results show that Islamic digital banks in Indonesia face complex and multidimensional cybercrime risks, which require comprehensive mitigation strategies. This study also proposes policy recommendations to improve cybersecurity, strengthen regulations, and raise public awareness of digital risks in the Islamic banking ecosystem.

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi pada era digital telah membawa perubahan yang signifikan dalam berbagai sektor kehidupan, termasuk sektor keuangan dan perbankan.¹ Transformasi digital yang berlangsung secara masif telah mendorong lembaga keuangan untuk mengadopsi berbagai inovasi teknologi guna meningkatkan efisiensi operasional, memperluas akses layanan, dan memenuhi kebutuhan masyarakat yang semakin bergantung pada teknologi digital. Salah satu bentuk transformasi tersebut adalah munculnya bank digital yang menawarkan layanan perbankan tanpa batas ruang dan waktu melalui aplikasi berbasis internet.² Dalam konteks Indonesia, perkembangan bank digital tidak hanya terjadi pada perbankan konvensional, tetapi juga merambah sektor perbankan syariah yang dikenal sebagai bank digital syariah.

Bank digital syariah merupakan institusi perbankan yang mengintegrasikan prinsip-prinsip syariah dengan teknologi digital dalam penyelenggaraan layanan keuangannya. Kehadiran bank digital syariah menjadi solusi atas kebutuhan masyarakat modern yang menginginkan layanan keuangan yang cepat, efisien, transparan, dan tetap sesuai dengan prinsip-prinsip Islam.³ Berbagai layanan seperti pembukaan rekening secara daring, transaksi keuangan real-time, pembiayaan digital, hingga investasi syariah kini dapat dilakukan melalui perangkat digital tanpa harus mengunjungi kantor cabang. Kondisi ini menunjukkan bahwa digitalisasi telah menjadi faktor penting dalam meningkatkan daya saing industri perbankan syariah di Indonesia.

Namun demikian, kemajuan teknologi digital tidak hanya menghadirkan berbagai manfaat, tetapi juga memunculkan risiko-risiko baru yang semakin kompleks. Salah satu risiko yang paling menonjol adalah cyber crime atau kejahatan siber. Cyber crime merupakan tindakan kriminal yang memanfaatkan teknologi informasi, jaringan komputer, dan internet sebagai sarana maupun sasaran kejahatan. Bentuk-bentuk cyber crime meliputi pencurian identitas, peretasan sistem, malware, phishing, ransomware, pencurian data nasabah, manipulasi transaksi elektronik, hingga serangan terhadap infrastruktur teknologi informasi yang digunakan oleh lembaga keuangan.⁴ Dalam lingkungan bank digital syariah yang seluruh aktivitas layanannya sangat bergantung pada sistem digital, ancaman kejahatan siber menjadi salah satu risiko utama yang dapat mengganggu operasional dan keberlangsungan institusi.

¹ Otoritas Jasa Keuangan. (2024). *Roadmap Pengembangan dan Penguatan Perbankan Syariah Indonesia 2023–2027*. Jakarta: Otoritas Jasa Keuangan.

² Launa, L., & Mudjiyanto, B. (2022). Membincang Risiko dan Ketidakpastian (Sebuah Penjajakan Konseptual Studi Risiko Politik). *Jurnal Communitarian*, 3(2), 209–224.

³ Beik, I. S., & Yuniarti, V. S. (2022). *Ekonomi dan Keuangan Digital Syariah: Peluang, Tantangan, dan Regulasi*. Jakarta: Rajawali Pers.

⁴ Faridi, M. K. (2019). Kejahatan Siber dalam Bidang Perbankan. *Cyber Security dan Forensik Digital*, 1(2), 117–125.

Meningkatnya ancaman cyber crime terhadap sektor keuangan global menunjukkan bahwa digitalisasi selalu diikuti oleh munculnya kerentanan baru. Laporan berbagai lembaga keamanan siber menunjukkan bahwa industri perbankan merupakan salah satu sektor yang paling sering menjadi target serangan siber karena menyimpan data sensitif dan memiliki nilai ekonomi yang tinggi.⁵ Di Indonesia, kasus serangan ransomware terhadap Bank Syariah Indonesia (BSI) pada tahun 2023 menjadi salah satu contoh nyata bagaimana serangan siber dapat mengganggu layanan perbankan secara luas, menyebabkan kerugian finansial, menghambat operasional bisnis, serta menurunkan tingkat kepercayaan masyarakat terhadap sistem perbankan digital.⁶ Peristiwa tersebut sekaligus memperlihatkan bahwa ancaman siber tidak lagi bersifat individual, melainkan dapat berdampak sistemik terhadap keseluruhan ekosistem perbankan.

Cyber crime dalam bank digital syariah dapat dikategorikan sebagai risiko sistemik karena dampaknya tidak hanya dirasakan oleh satu institusi, tetapi berpotensi memengaruhi stabilitas industri keuangan secara keseluruhan.⁷ Ketika sebuah bank digital mengalami kebocoran data atau gangguan sistem akibat serangan siber, kepercayaan publik terhadap layanan digital dapat menurun. Penurunan kepercayaan ini berpotensi menimbulkan efek domino terhadap institusi lain yang memiliki karakteristik layanan serupa. Selain itu, keterhubungan sistem digital antarbank, penyedia layanan pembayaran, fintech, dan regulator semakin memperbesar kemungkinan terjadinya penyebaran risiko secara luas dalam ekosistem keuangan digital.

Kondisi tersebut menunjukkan bahwa cyber crime tidak dapat dipahami hanya sebagai persoalan teknis keamanan informasi semata. Cyber crime juga merupakan fenomena sosial yang berkaitan dengan modernisasi, globalisasi, dan ketergantungan masyarakat terhadap teknologi.⁸ Oleh karena itu, diperlukan pendekatan teoritis yang mampu menjelaskan hubungan antara perkembangan teknologi dan munculnya risiko-risiko baru dalam masyarakat modern. Salah satu teori yang relevan untuk menjelaskan fenomena ini adalah teori *Risk Society* yang dikemukakan oleh Ulrich Beck.

Menurut Beck, masyarakat modern telah mengalami pergeseran dari masyarakat industri menuju masyarakat risiko (*risk society*).⁹ Dalam masyarakat risiko, berbagai ancaman yang dihadapi manusia bukan lagi berasal dari alam, melainkan merupakan hasil dari perkembangan ilmu pengetahuan, teknologi, dan modernisasi itu sendiri. Risiko-risiko tersebut bersifat global, sulit diprediksi, serta

⁵ Kusvianti, P., Ashari, A. P. R., & Izzah, A. N. (2023). Pandangan Ulrich Beck tentang Risiko dan Ketidakpastian yang Dialami oleh Masyarakat Modern. *Jurnal Ilmiah Ecosystem*, 23(1), 22–32

⁶ Kholis, I. M. (2025). Perlindungan Data Pribadi dan Keamanan Siber di Sektor Perbankan: Studi Kritis atas Penerapan UU PDP dan UU ITE di Indonesia. *Staatsrecht Jurnal Hukum Kenegaraan dan Politik Islam*, 6(1), 1–20

⁷ Amrillah, M. U. (2020). Urgensi Pembentukan Undang-Undang Digital Banking Bagi Perbankan Syariah Di Indonesia. *Jurnal Lex Renaissance*, 5(4), 841–854.

⁸ Budianto, E. W. H., & Dewi, N. D. T. (2023). Pemetaan Penelitian Rasio Capital Adequacy Ratio (CAR) pada Perbankan Syariah dan Konvensional: Studi Bibliometrik VOSviewer dan Literature Review. *Journal of Accounting Finance Taxation and Auditing (JAFTA)*, 4(2), 162–176

⁹ Baidhowi, B. (2018). Sharia Banking Opportunities and Challenges in the Digital Era.

memiliki dampak yang melampaui batas geografis maupun institusional. Risiko yang muncul akibat perkembangan teknologi digital, termasuk cyber crime, merupakan contoh nyata dari risiko modern yang diciptakan oleh proses modernisasi. Dalam perspektif Beck, semakin maju teknologi yang digunakan masyarakat, semakin besar pula potensi munculnya risiko-risiko baru yang harus dikelola secara sistematis.¹⁰

Penerapan teori *Risk Society* dalam kajian bank digital syariah menjadi penting karena mampu memberikan pemahaman yang lebih komprehensif mengenai cyber crime sebagai risiko yang dihasilkan oleh modernisasi teknologi keuangan.¹¹ Teori ini menjelaskan bahwa risiko siber bukan sekadar ancaman teknis, melainkan bagian dari konsekuensi transformasi digital yang tidak dapat dihindari. Oleh karena itu, pengelolaan risiko siber tidak cukup dilakukan melalui penguatan teknologi keamanan semata, tetapi juga memerlukan kesiapan kelembagaan, peningkatan literasi digital, penguatan tata kelola risiko, serta regulasi yang adaptif terhadap perkembangan ancaman siber.¹²

Penelitian ini dilatarbelakangi oleh beberapa alasan penting. Pertama, meningkatnya intensitas dan kompleksitas serangan siber terhadap sektor perbankan digital di Indonesia. Kedua, besarnya potensi kerugian ekonomi, reputasi, dan sosial yang dapat ditimbulkan oleh kejahatan siber. Ketiga, pentingnya menjaga kepercayaan masyarakat terhadap bank digital syariah sebagai salah satu pilar pengembangan ekonomi syariah nasional. Keempat, masih terbatasnya kajian akademik yang menganalisis cyber crime dalam perbankan syariah menggunakan perspektif teori *Risk Society* Ulrich Beck.

Berdasarkan latar belakang tersebut, penelitian ini bertujuan untuk menganalisis cyber crime sebagai risiko sistemik dalam bank digital syariah di Indonesia dengan menggunakan perspektif teori *Risk Society* dari Ulrich Beck. Analisis ini diharapkan dapat memberikan pemahaman yang lebih mendalam mengenai karakteristik risiko siber dalam industri perbankan syariah, dampaknya terhadap stabilitas sistem keuangan, serta strategi mitigasi yang dapat diterapkan untuk memperkuat ketahanan dan keberlanjutan bank digital syariah di era transformasi digital. Hasil penelitian ini juga diharapkan dapat menjadi kontribusi akademik dalam pengembangan kajian ekonomi syariah dan manajemen risiko digital, sekaligus memberikan rekomendasi praktis bagi regulator, lembaga perbankan, dan pemangku kepentingan dalam menghadapi tantangan kejahatan siber di masa depan.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif dengan metode studi literatur dan analisis data sekunder. Pendekatan kualitatif dipilih untuk memberikan pemahaman mendalam tentang kompleksitas

¹⁰ Rasborg, K. (2019). *Ulrich Beck: En kritisk indføring i teorien om verdensrisikosamfundet*.

¹¹ Pratama, I. P. A. E. (2021). *Cyber Security: Teori dan Praktik Keamanan Siber*. Bandung: Informatika.

¹² Kristiyanto, S., & Widodo, S. (2020). Analisa Intermediasi Makroprudensial pada Bank Berdampak Sistemik di Indonesia. *JMD: Jurnal Riset Manajemen & Bisnis Dewantara*, 3(1), 1–14

Cyber Crime sebagai risiko sistemik dalam bank digital syariah. Studi literatur digunakan untuk mengumpulkan dan menganalisis informasi dari berbagai sumber, termasuk jurnal ilmiah, buku, laporan penelitian, peraturan perundang-undangan, dan berita media massa. Analisis data sekunder digunakan untuk mengkaji data dan informasi yang telah tersedia, seperti data statistik, laporan keuangan, dan laporan insiden keamanan siber.

Langkah-langkah penelitian meliputi: (1) Pengumpulan data: Pengumpulan data dilakukan melalui penelusuran literatur yang relevan, termasuk jurnal ilmiah, buku, laporan penelitian, peraturan perundang-undangan (UU ITE, UU PDP, POJK), dan berita media massa. Sumber-sumber data dipilih berdasarkan relevansi dengan topik penelitian dan kredibilitas. (2) Analisis data: Data yang terkumpul dianalisis secara kualitatif dengan menggunakan metode analisis isi (*content analysis*). Analisis isi digunakan untuk mengidentifikasi tema-tema kunci, pola, dan hubungan dalam data. Analisis dilakukan secara sistematis dan terstruktur untuk memastikan validitas dan reliabilitas hasil penelitian. (3) Sintesis dan interpretasi: Hasil analisis data disintesis dan diinterpretasikan untuk menjawab rumusan masalah penelitian. Interpretasi dilakukan dengan mengacu pada kerangka teoritis dan konsep-konsep kunci dalam teori *Risk Society*. (4) Penarikan kesimpulan dan rekomendasi: Berdasarkan hasil analisis dan interpretasi, kesimpulan penelitian ditarik dan rekomendasi kebijakan dirumuskan. Rekomendasi kebijakan dirancang untuk memberikan solusi praktis dan efektif untuk memitigasi risiko *Cyber Crime* dalam bank digital syariah.

Data yang dianalisis dalam penelitian ini meliputi: (1) Jenis-jenis *Cyber Crime* yang relevan dengan bank digital syariah. (2) Karakteristik bank digital syariah yang meningkatkan kerentanan terhadap *Cyber Crime*. (3) Dampak sistemik *Cyber Crime* pada perlindungan nasabah, regulasi, dan kepercayaan publik. (4) Regulasi terkait perbankan digital dan keamanan siber di Indonesia. (5) Studi kasus serangan siber terhadap bank digital syariah di Indonesia dan negara lain. (6) Laporan dari lembaga terkait, seperti OJK, Bank Indonesia, dan lembaga keamanan siber.

Teknik analisis data yang digunakan meliputi: (1) Analisis isi: digunakan untuk mengidentifikasi tema-tema kunci, pola, dan hubungan dalam data. (2) Analisis komparatif: digunakan untuk membandingkan regulasi dan praktik keamanan siber di berbagai negara. (3) Analisis SWOT: digunakan untuk mengidentifikasi kekuatan, kelemahan, peluang, dan ancaman terkait *Cyber Crime* dalam bank digital syariah. (4) Analisis kebijakan: digunakan untuk menganalisis efektivitas regulasi dan kebijakan yang ada dalam memitigasi risiko *Cyber Crime*.

HASIL DAN PEMBAHASAN

Analisis *Cyber Crime* Melalui Perspektif *Risk Society*

Hasil temuan penelitian ini Adalah Teori *Risk Society* dari Ulrich Beck memberikan kerangka kerja yang berguna untuk menganalisis dampak sistemik *Cyber Crime* pada bank digital syariah. Dalam

pandangan Beck, masyarakat modern menghadapi risiko yang dihasilkan oleh kemajuan teknologi dan industrialisasi. *Cyber Crime*, sebagai risiko yang dihasilkan oleh teknologi digital, menjadi pusat perhatian dalam masyarakat risiko. Berikut adalah beberapa aspek dari teori *Risk Society* yang relevan dengan analisis *Cyber Crime* dalam bank digital syariah:¹³ (1) Individualisasi: Dalam masyarakat risiko, individu semakin bertanggung jawab atas risiko yang mereka hadapi. Dalam konteks perbankan digital syariah, nasabah bertanggung jawab atas keamanan data dan transaksi mereka. Bank harus memberikan edukasi dan informasi yang memadai kepada nasabah tentang risiko *Cyber Crime* dan cara menghindarinya. (2) Refleksivitas: Masyarakat modern merefleksikan dan mengkaji kembali dampak dari kemajuan teknologi dan industrialisasi. Bank, regulator, dan masyarakat harus terus-menerus mengkaji risiko *Cyber Crime* dan mengembangkan strategi mitigasi yang efektif. (3) Kesadaran Risiko: Meningkatkan kesadaran masyarakat tentang risiko dan dampaknya. Bank harus meningkatkan kesadaran masyarakat tentang risiko *Cyber Crime* melalui berbagai program edukasi dan sosialisasi. (4) Institusionalisasi Risiko: Lembaga-lembaga sosial, seperti pemerintah dan perusahaan, berusaha untuk mengelola dan mengendalikan risiko. OJK dan Bank Indonesia harus mengembangkan regulasi dan kebijakan yang komprehensif untuk mengatasi risiko *Cyber Crime*. Bank harus mengimplementasikan sistem keamanan yang kuat dan mengelola risiko dengan efektif. (5) Globalisasi Risiko: Risiko menjadi bersifat global dan melintasi batas-batas negara. *Cyber Crime* dapat dilakukan dari mana saja di dunia dan dapat berdampak pada bank digital syariah di Indonesia. Perlu adanya kerjasama internasional untuk mengatasi *Cyber Crime*.¹⁴

Melalui perspektif *Risk Society*, *Cyber Crime* dalam bank digital syariah tidak hanya merupakan masalah teknis, tetapi juga masalah sosial, ekonomi, dan politik. *Cyber Crime* dapat mengancam stabilitas sistem keuangan, merusak kepercayaan publik, dan merugikan nasabah. Oleh karena itu, diperlukan pendekatan yang komprehensif untuk mitigasi, yang melibatkan berbagai pemangku kepentingan, termasuk bank, regulator, pemerintah, dan masyarakat.

Implikasi Risiko Sistemik *Cyber Crime*

Risiko sistemik *Cyber Crime* memiliki implikasi yang signifikan terhadap berbagai aspek dalam ekosistem perbankan digital syariah: (1) Perlindungan Nasabah: *Cyber Crime* dapat menyebabkan kerugian finansial, pencurian data pribadi, dan penyalahgunaan identitas nasabah. Bank harus mengambil langkah-langkah untuk melindungi data dan dana nasabah, termasuk implementasi sistem keamanan yang kuat, otentikasi ganda, dan enkripsi data. Perlindungan data pribadi menjadi sangat

¹³ Ika Atikah. (2023). Perlindungan Hukum Pelanggan Aset Kripto Transaksi Perdagangan Berjangka Komoditi Indonesia. *SALAM: Jurnal Sosial dan Budaya Syar'i*, 10(2), 343–358

¹⁴ Jange, B., Pendi, I., & Susilowati, E. M. (2024). Peran Teknologi Finansial (Fintech) dalam Transformasi Layanan Keuangan di Indonesia. *Indonesian Research Journal on Education*, 4(3), 4441–4456.

penting.^{15,16} (2) Stabilitas Sistem Keuangan: Serangan siber dapat mengganggu operasional bank, menyebabkan penarikan dana secara besar-besaran, dan merusak kepercayaan publik terhadap sistem keuangan. Hal ini dapat mengancam stabilitas sistem keuangan secara keseluruhan. Bank Indonesia dan OJK harus memantau risiko *Cyber Crime* secara ketat dan mengambil tindakan untuk mencegah dan mengatasi serangan siber. (3) Kepercayaan Publik: Serangan siber dapat merusak kepercayaan publik terhadap bank digital syariah. Kehilangan kepercayaan dapat menyebabkan penurunan jumlah nasabah dan volume transaksi. Bank harus membangun kepercayaan dengan memberikan layanan yang aman, transparan, dan bertanggung jawab. (4) Regulasi dan Pengawasan: Risiko *Cyber Crime* memerlukan regulasi dan pengawasan yang adaptif dan komprehensif. OJK harus terus memperbarui regulasi untuk mengatasi tantangan yang muncul dalam era digital. Pengawasan yang efektif sangat penting untuk memastikan kepatuhan bank terhadap regulasi keamanan siber.¹⁷ (5) Inovasi dan Pertumbuhan: *Cyber Crime* dapat menghambat inovasi dan pertumbuhan dalam sektor perbankan digital syariah. Bank mungkin enggan untuk meluncurkan produk dan layanan baru jika mereka merasa tidak aman. Oleh karena itu, keamanan siber harus menjadi prioritas utama untuk mendorong inovasi dan pertumbuhan.

Implikasi ini menunjukkan bahwa *Cyber Crime* merupakan ancaman serius yang memerlukan perhatian serius dari semua pemangku kepentingan dalam ekosistem perbankan digital syariah.

Rekomendasi Kebijakan

Untuk memitigasi risiko *Cyber Crime* dalam bank digital syariah, penelitian ini merekomendasikan beberapa kebijakan berikut: (1) Penguatan Regulasi dan Pengawasan: OJK harus terus memperbarui regulasi terkait keamanan siber dan perbankan digital. Regulasi harus mencakup standar keamanan minimum, kewajiban pelaporan insiden, dan mekanisme pengawasan yang efektif. OJK juga harus meningkatkan kapasitas pengawasan untuk memastikan kepatuhan bank terhadap regulasi.^{18,19} (2) Peningkatan Keamanan Siber: Bank harus menginvestasikan sumber daya yang cukup dalam teknologi keamanan siber, termasuk sistem deteksi intrusi, *firewall*, enkripsi data, dan otentikasi ganda. Bank juga harus melakukan pengujian keamanan secara berkala, seperti *penetration testing*,

¹⁵ Kholis, I. M. (2025). Perlindungan Data Pribadi dan Keamanan Siber di Sektor Perbankan: Studi Kritis atas Penerapan UU PDP dan UU ITE di Indonesia. *Staatsrecht Jurnal Hukum Kenegaraan dan Politik Islam*, 6(1), 1–20

¹⁶ Wardah Yuspin, Kelik Wardiono, Aditya Nurrahman, & Arief Budiono. (2023). Personal Data Protection Law in Digital Banking Governance in Indonesia. *Studia Iuridica Lublinensia*, 32(1), 99–130

¹⁷ Hasanah, N., Sayuti, M., & Lisnawati, L. (2024). Optimalisasi Regulasi Perbankan Syariah oleh Bank Indonesia dan Otoritas Jasa Keuangan dalam Akselerasi Transformasi Digital. *Jurnal Manajemen Terapan dan Keuangan*, 13(03), 512–525.

¹⁸ Hasanah, N., Sayuti, M., & Lisnawati, L. (2024). Optimalisasi Regulasi Perbankan Syariah oleh Bank Indonesia dan Otoritas Jasa Keuangan dalam Akselerasi Transformasi Digital. *Jurnal Manajemen Terapan dan Keuangan*, 13(03), 512–525.

¹⁹ Amrillah, M. U. (2020). Urgensi Pembentukan Undang-Undang Digital Banking Bagi Perbankan Syariah Di Indonesia. *Jurnal Lex Renaissance*, 5(4), 841–854

untuk mengidentifikasi kerentanan dan kelemahan dalam sistem mereka. Kerjasama dengan pihak ketiga spesialis keamanan siber juga penting. (3) Peningkatan Literasi dan Kesadaran Masyarakat: Bank dan regulator harus meningkatkan literasi dan kesadaran masyarakat tentang risiko *Cyber Crime*. Program edukasi dan sosialisasi harus dilakukan secara berkala untuk memberikan informasi tentang cara mengenali dan menghindari *phishing*, penipuan, dan serangan siber lainnya. (4) Kerjasama Antar Lembaga: Perlu adanya kerjasama yang erat antara bank, OJK, Bank Indonesia, lembaga penegak hukum, dan lembaga keamanan siber. Kerjasama ini diperlukan untuk berbagi informasi tentang ancaman siber, melakukan investigasi, dan mengambil tindakan yang diperlukan untuk mengatasi serangan siber.²⁰ (5) Pengembangan Standar Industri: Perlu adanya pengembangan standar industri untuk keamanan siber dalam perbankan digital syariah. Standar ini dapat membantu bank untuk mengimplementasikan praktik keamanan terbaik dan memastikan konsistensi dalam keamanan siber. (6) Implementasi *Cyber Insurance*: Bank dapat mempertimbangkan untuk mengimplementasikan *cyber insurance* untuk melindungi diri dari kerugian finansial akibat serangan siber. *Cyber insurance* dapat membantu bank untuk membayar biaya pemulihan, kerugian bisnis, dan biaya hukum yang terkait dengan serangan siber. (7) Pengembangan Kerangka Kerja Manajemen Risiko Siber: Bank harus mengembangkan kerangka kerja manajemen risiko siber yang komprehensif. Kerangka kerja ini harus mencakup identifikasi risiko, penilaian risiko, mitigasi risiko, dan pemantauan risiko. (8) Peningkatan Kesiapsiagaan dan Respon Insiden: Bank harus memiliki rencana tanggap darurat yang komprehensif untuk menghadapi serangan siber. Rencana ini harus mencakup prosedur untuk mengidentifikasi, merespons, dan memulihkan dari serangan siber. Latihan simulasi insiden keamanan siber harus dilakukan secara berkala.

Implementasi kebijakan-kebijakan ini akan membantu bank digital syariah untuk mengurangi risiko *Cyber Crime*, melindungi nasabah, menjaga stabilitas sistem keuangan, dan membangun kepercayaan publik.

KESIMPULAN

Penelitian ini telah menganalisis Cyber Crime sebagai risiko sistemik dalam bank digital syariah di Indonesia, dengan mengintegrasikan perspektif teori *Risk Society* dari Ulrich Beck. Temuan utamanya mengkonfirmasi bahwa Cyber Crime merupakan ancaman serius dan multidimensi terhadap stabilitas serta keinginan bank digital syariah. Kerentanan yang melekat pada bank digital syariah, yang timbul dari operasi sepenuhnya berani dan ketergantungan tinggi pada teknologi, membuat mereka rentan terhadap berbagai informasi modus kejahatan siber. Dari perspektif teori *Risk Society*, Cyber

²⁰ Kholis, I. M. (2025). Perlindungan Data Pribadi dan Keamanan Siber di Sektor Perbankan: Studi Kritis atas Penerapan UU PDP dan UU ITE di Indonesia. *Staatsrecht Jurnal Hukum Kenegaraan dan Politik Islam*, 6(1), 1–20

Crime dipandang sebagai risiko yang dihasilkan oleh modernisasi teknologi digital, bersifat sistemik dan global, yang menuntut kewaspadaan kolektif dan refleksi institusional.

Implikasi dari risiko sistemik Cyber Crime ini mencakup ancaman terhadap perlindungan nasabah, stabilitas sistem keuangan, dan kepercayaan masyarakat. Untuk mengatasi tantangan ini, penelitian ini menawarkan solusi strategi yang fokus pada penguatan ekosistem keamanan siber proaktif, termasuk investasi pada teknologi keamanan pertukaran dan kapabilitas respon kejadian yang teruji. Selain itu, kolaborasi yang erat antara regulator (OJK, Bank Indonesia) dengan industri perbankan syariah ditekankan untuk menyebarkan ancaman ancaman, mengembangkan standar keamanan bersama, dan memastikan penegakan peraturan yang adaptif.

Peningkatan literasi digital dan kesadaran finansial nasabah juga menjadi kunci, melalui program edukasi yang inovatif dan mudah diakses agar nasabah dapat melindungi diri dari modus penipuan siber. Bank digital syariah juga didorong untuk mengembangkan kerangka kerja manajemen risiko siber yang komprehensif, yang mengintegrasikan aspek teknis, dampak bisnis, dan kelangsungan operasional. Terakhir, pemanfaatan *asuransi cyber* dipertimbangkan sebagai mekanisme transfer risiko untuk melindungi dari kerugian finansial besar akibat insiden siber.

DAFTAR PUSTAKA

- Amrillah, M. U. (2020). Urgensi Pembentukan Undang-Undang Digital Banking Bagi Perbankan Syariah Di Indonesia. *Jurnal Lex Renaissance*, 5(4), 841–854. <https://doi.org/10.20885/jlr.vol5.iss4.art12>
- Baidhowi, B. (2018). Sharia Banking Opportunities and Challenges in the Digital Era. <https://doi.org/10.2991/icils-18.2018.30>
- Beik, I. S., & Yuniarti, V. S. (2022). *Ekonomi dan Keuangan Digital Syariah: Peluang, Tantangan, dan Regulasi*. Jakarta: Rajawali Pers.
- Budianto, E. W. H., & Dewi, N. D. T. (2023). Pemetaan Penelitian Rasio Capital Adequacy Ratio (CAR) pada Perbankan Syariah dan Konvensional: Studi Bibliometrik VOSviewer dan Literature Review. *Journal of Accounting Finance Taxation and Auditing (JAFTA)*, 4(2), 162–176. <https://doi.org/10.28932/jafta.v4i2.7650>
- Damkjær, S. (2006). Theory, culture and society. *Dansk Sociologi*, 10(1), 5–25. <https://doi.org/10.22439/dansoc.v10i1.669>
- Dewantara, R., & Sitorus, H. A. M. (2022). Re-Evaluasi Pendirian Bank Digital di Indonesia: Paradigma, Konsep dan Regulasi. *Veritas et Justitia*, 8(2), 226–252. <https://doi.org/10.25123/vej.v8i2.5433>
- Faridi, M. K. (2019). Kejahatan Siber dalam Bidang Perbankan. *Cyber Security dan Forensik Digital*, 1(2), 117–125. <https://doi.org/10.14421/csecurity.2018.1.2.1373>
- Fauzi, A., Widayati, E., Putri, T. A. P., Abiyyah, L. A., Sasmita, M., Maulana, R., Aulia, T., & Herdinov, A. (2023). Peranan Bank Indonesia dalam Mengatur dan Menjaga Kelancaran Sistem Pembayaran. *Jurnal Akuntansi dan Manajemen Bisnis*, 3(1), 1–12. <http://dx.doi.org/10.56127/jaman.v3i1.654>
- Fitrianto, B. (2025). Tinjauan Yuridis Tanggung Jawab Hukum Bank terhadap Kerugian Nasabah Akibat Kecerdasan Buatan (AI) dalam Pengambilan Keputusan Kredit. *Milthree Law Journal*, 2(1), 1–19. <https://doi.org/10.70565/mlj.v2i1.92>
- Hardyansah, R., & Darmawan, D. (2026). Mapping Digital Asset Regulatory Models and Their Implications for Islamic Financial Governance: A Comparative Study of Indonesia, the United Arab Emirates, and Turkey. *Jurnal Akta*, 13(1), 1–22. <https://doi.org/10.30659/akta.v13i1.51396>
- Hasanah, N., Sayuti, M., & Lisnawati, L. (2024). Optimalisasi Regulasi Perbankan Syariah oleh Bank Indonesia dan Otoritas Jasa Keuangan dalam Akselerasi Transformasi Digital. *Jurnal Manajemen Terapan dan Keuangan*, 13(03), 512–525. <https://doi.org/10.22437/jmk.v13i03.36621>
- Hidayat, M. S. (2023). Mengurai Potensi Ekonomi Syariah sebagai Solusi Krisis Keuangan Global: Kajian Mendalam melalui Studi Literatur. *ALAMIAH: Jurnal Muamalah dan Ekonomi Syariah*, 4(02), 223–242. <http://dx.doi.org/10.56406/jurnalalamiah.v4i02.220>
- Ika Atikah. (2023). Perlindungan Hukum Pelanggan Aset Kripto Transaksi Perdagangan Berjangka Komoditi Indonesia. *SALAM: Jurnal Sosial dan Budaya Syar'i*, 10(2), 343–358. <https://doi.org/10.15408/sjsbs.v10i2.31691>
- Jange, B., Pendi, I., & Susilowati, E. M. (2024). Peran Teknologi Finansial (Fintech) dalam Transformasi Layanan Keuangan di Indonesia. *Indonesian Research Journal on Education*, 4(3), 4441–4456. <https://doi.org/10.31004/irje.v4i3.1007>

- Kholis, I. M. (2025). Perlindungan Data Pribadi dan Keamanan Siber di Sektor Perbankan: Studi Kritis atas Penerapan UU PDP dan UU ITE di Indonesia. *Staatsrecht Jurnal Hukum Kenegaraan dan Politik Islam*, 6(1), 1–20. <https://doi.org/10.14421/t5sfe747>
- Kristiyanto, S., & Widodo, S. (2020). Analisa Intermediasi Makroprudensial pada Bank Berdampak Sistemik di Indonesia. *JMD: Jurnal Riset Manajemen & Bisnis Dewantara*, 3(1), 1–14. <https://doi.org/10.26533/jmd.v3i1.546>
- Kusvianti, P., Ashari, A. P. R., & Izzah, A. N. (2023). Pandangan Ulrich Beck tentang Risiko dan Ketidakpastian yang Dialami oleh Masyarakat Modern. *Jurnal Ilmiah Ecosystem*, 23(1), 22–32. <https://doi.org/10.35965/eco.v23i1.2495>
- Latifah, L., & Awad, A. (2023). Metode Pendidikan Karakter Di Pesantren Dalam Perspektif Pendidikan Agama Islam. *JIS: Journal Islamic Studies*, 1(3).
- Latifah, L., & Ngalimun, N. (2025). Teknologi Digital Sebagai Ruang Pertemuan Agama Dan Budaya Masyarakat Multikultural. *SINTESA: JURNAL SAINS & TEKNOLOGI*, 1(02), 51-64.
- Launa, L., & Mudjiyanto, B. (2022). Membincang Risiko dan Ketidakpastian (Sebuah Penjajakan Konseptual Studi Risiko Politik). *Jurnal Communitarian*, 3(2), 209–224. <https://doi.org/10.56985/jc.v3i2.180>
- Mauliza, A. Y. I., Machmudi, R. D. S., & Indrarini, R. (2022). Pengaruh Perlindungan Data dan Cyber Security terhadap Tingkat Kepercayaan Menggunakan Fintech Masyarakat di Surabaya. *SIBATIK Journal*, 1(11), 2397–2410. <http://dx.doi.org/10.54443/sibatik.v1i11.395>
- Ngalimun, H. (2017). Ilmu Komunikasi Sebuah Pengantar Praktis. *Banjarmasin: Pustaka Banua*.
- Ngalimun, N. (2022). Bahasa Indonesia Untuk Penulisan Karya Ilmiah. *EduCurio: Education Curiosity*, 1(1), 265-278.
- Otoritas Jasa Keuangan. (2024). *Roadmap Pengembangan dan Penguatan Perbankan Syariah Indonesia 2023–2027*. Jakarta: Otoritas Jasa Keuangan.
- Pratama, I. P. A. E. (2021). *Cyber Security: Teori dan Praktik Keamanan Siber*. Bandung: Informatika.
- Rahmawati, R., Imaduddin, M. A., Jufrin, & Muslimah. (2023). Hukum Perbankan Syariah di Indonesia: Optimalisasi Fungsi Berbasis Pengendalian Risiko pada Perbankan Syariah. *Wahana Islamika: Jurnal Studi Keislaman*, 9(2), 161–182. <https://doi.org/10.61136/zskcz305>
- Rasborg, K. (2019). *Ulrich Beck: En kritisk indføring i teorien om verdensrisikosamfundet*.
- Rohyati, R., Rokhmah, F. P. N., Syazeedah, H. N. U., Fitriyaningrum, R. I., Ramadhan, G., & Syahwildan, M. (2024). Tantangan dan Peluang Pasar Modal Indonesia dalam Meningkatkan Minat Investasi di Era Digital. *Kompeten: Jurnal Ilmiah Ekonomi dan Bisnis*, 3(1), 86–98. <http://dx.doi.org/10.57141/kompeten.v3i1.133>
- Saputri, M. E., Ningtias, I. C. K., & Holida, N. (2023). Ketidakpastian dan Risiko yang Dialami Masyarakat di Era Modernisasi. *Jurnal Insan Pendidikan dan Sosial Humaniora*, 1(2), 127–134. <http://dx.doi.org/10.59581/jipsoshum-widyakarya.v1i2.261>
- Ulya, N. U., & Musyarri, F. A. (2020). Reformulasi Pengaturan Mengenai Financial Technology dalam Hukum Positif di Indonesia. *Arena Hukum*, 13(3), 475–492. <https://doi.org/10.21776/ub.arenahukum.2020.01303.5>
- Universitas Muhammadiyah Sidoarjo, & Pebrianggara, A. (2023). *Design Thinking For Business*. Umsida Press eBooks. <https://doi.org/10.21070/2023/978-623-464-078-6>
- Wardah Yuspin, Kelik Wardiono, Aditya Nurrahman, & Arief Budiono. (2023). Personal Data Protection Law in Digital Banking Governance in Indonesia. *Studia Iuridica Lublinensia*, 32(1), 99–130. <https://doi.org/10.17951/sil.2023.32.1.99-130>.