HUMANITIS: Jurnal Humaniora, Sosial dan Bisnis
Vol. 1 No. 12 2024, hal. 692-700 e-ISSN: 2988-6287

TINJAUAN LITERATUR TENTANG ANCAMAN *CYBERCRIME* DAN IMPLEMENTASI KEAMANAN SIBER DI INDUSTRI PERBANKAN

Nasywa Shafa Azzahra[1], Aron Micael Tambunan[2], Najwa Nayra Aulia[3], Arista Binarsih[4], Tubagus Hedi Saepudin[5*]
[1,2,3,4]Teknik Industri, Fakultas Teknik, Universitas Bhayangkara Jakarta Raya, Indonesia
e-mail: [1]202210215085@mhs.ubharajaya.ac.id , [2]202210215090@mhs.ubharajaya.ac.id ,
[3]202210215170@mhs.ubharajaya.ac.id ,
[4]202210215049@mhs.ubharajaya.ac.id,[5]tubagus.hedi@dsn.ubharajaya.ac.id

ABSTRACT

Rapid technological development brings significant changes in social, economic and cultural aspects, but also increases the risk of the spread of viruses, piracy and software attacks. Cybercrime, as a cross-border crime, is a serious threat with far-reaching impacts, especially in the banking industry. This research reviews the literature regarding cybercrime threats and the implementation of cyber security in the banking sector, with a focus on threats such as Phishing, Malware, and data leaks that cause theft of sensitive information, financial losses, and reputational damage. Through a literature review of five journals, this research aims to identify the main threats of cybercrime, evaluate bank security measures, and recommend strategies for improving cyber security. Although the evaluation of cybersecurity policies faces obstacles, preventive measures have been taken. Increasing cyber security and cooperation between institutions is very important in facing the threat of cybercrime in the financial sector.
***Keywords**: Cybercrime, Banking Industry, Cybersecurity*

ABSTRAK

Perkembangan teknologi yang pesat membawa perubahan signifikan pada aspek sosial, ekonomi, dan budaya, tetapi juga meningkatkan risiko penyebaran virus, pembajakan, dan serangan perangkat lunak. *Cybercrime*, sebagai kejahatan lintas batas, menjadi ancaman serius dengan dampak luas, khususnya dalam industri perbankan. Penelitian ini meninjau literatur mengenai ancaman *cybercrime* dan implementasi keamanan siber di sektor perbankan, dengan fokus pada ancaman seperti Phishing, Malware, dan kebocoran data yang menyebabkan pencurian data sensitif, kerugian keuangan, dan penurunan reputasi. Melalui tinjauan pustaka terhadap lima jurnal, penelitian ini bertujuan mengidentifikasi ancaman utama *cybercrime*, mengevaluasi langkah-langkah keamanan bank, dan merekomendasikan strategi peningkatan keamanan siber. Meskipun evaluasi kebijakan keamanan siber menghadapi kendala, langkah-langkah pencegahan telah diambil. Peningkatan keamanan siber dan kerjasama antar lembaga sangat penting dalam menghadapi ancaman *cybercrime* di sektor keuangan.
Kata Kunci: Cybercrime, Industri Perbankan, Keamanan Ciber

PENDAHULUAN

Di era sekarang, di mana perkembangan teknologi terjadi dengan pesat, menyebabkan perubahan yang signifikan terhadap aspek sosial, ekonomi, dan budaya tidak terelakkan. Namun, di balik kemajuan ini, ada risiko seperti penyebaran virus, pembajakan, dan serangan terhadap layanan

perangkat lunak. *Cybercrime*, yang melibatkan pelaku dan korban dari berbagai negara, menjadi bentuk kejahatan lintas batas yang serius. Hal ini juga membuka peluang bagi individu atau kelompok untuk melakukan serangan terhadap sistem teknologi. *Cybercrime* merupakan kejahatan baru yang muncul sebagai akibat dari berkembangnya Teknologi Informasi (Ervina Chintia, 2018). *Cybercrime* melibatkan penggunaan komputer dalam pelaksanaannya. Kejahatan yang berkaitan dengan kerahasiaan, integritas, dan keberadaan data serta sistem komputer memerlukan perhatian khusus karena memiliki karakteristik yang berbeda dari kejahatan konvensional.

Dalam industri perbankan, ancaman keamanan siber sering kali terjadi, terutama dalam bentuk *Phishing*, *Malware*, dan kebocoran data. *Phishing* merupakan suatu bentuk kegiatan yang bersifat mengancam atau menjebak seseorang dengan konsep memancing orang tersebut (Mia Hatyati Wibowo, 2017). Serangan malware perbankan telah semakin sering terjadi dalam beberapa tahun terakhir, menimbulkan ancaman besar bagi lembaga keuangan dan pelanggan mereka. Serangan ini dapat mengakibatkan pencurian informasi sensitif, kerugian finansial, dan merusak reputasi. (Fitria, 2023). Kebocoran data terjadi ketika informasi sensitif nasabah atau bank terekspos, baik melalui peretasan langsung atau kesalahan internal. Tujuan utama dari *Cybercrime* adalah mendapatkan keuntungan pribadi secara ilegal, terutama dalam sektor keuangan. Peningkatan keamanan jaringan dalam industri jasa finansial menjadi fokus utama karena adanya peningkatan serangan siber terhadap sektor ini.

Ancaman-ancaman ini mengharuskan bank untuk mengadopsi langkah-langkah keamanan yang canggih dan memberikan edukasi berkelanjutan demi melindungi sistem mereka serta data nasabah. Penerapan teknologi keamanan terbaru, seperti enkripsi data dan sistem deteksi intrusi, sangat penting untuk menangkal serangan yang semakin rumit. Selain itu, memberikan edukasi berkelanjutan kepada karyawan dan nasabah tentang praktik keamanan siber yang baik, seperti mengenali phishing dan menggunakan kata sandi yang kuat, sangat penting untuk mengurangi risiko. Kepatuhan terhadap peraturan keamanan siber juga merupakan indikator penting untuk menjaga keberlanjutan sistem siber yang aman di sektor jasa keuangan, memastikan bahwa bank tidak hanya memenuhi standar industri tetapi juga membangun kepercayaan yang kokoh dengan nasabah.

METODE PENELITIAN

Metode yang digunakan dalam penelitian ini melibatkan pengumpulan lima jurnal yang relevan dengan topik penelitian dan melakukan tinjauan pustaka (*literature review*) terhadap jurnal-jurnal tersebut. Studi literatur adalah pencarian dan penelitian literatur dengan membaca berbagai buku, jurnal, dan publikasi lain yang berkaitan dengan topik penelitian untuk menghasilkan suatu tulisan yang berkaitan dengan topik atau permasalahan tertentu. (Marzali, 2017).

Proses pencarian literatur dilakukan melalui *Google Scholar*. Setiap jurnal dianalisis untuk mengidentifikasi temuan, dan kesenjangan penelitian. Hasil analisis ini kemudian digabungkan untuk memberikan pemahaman menyeluruh tentang topik cyber security dan dilakukan evaluasi.

HASIL DAN PEMBAHASAN

Setelah melakukan penelusuran artikel ilmiah, ditemukan 5 jurnal yang berkaitan dengan cyber security yang dipublikasikan antara tahun 2018-2024 yaitu sebagai berikut:

Tabel 1 Hasil Tinjauan Literatur

Nama	Tujuan	Metode Pengambilan Data	Temuan	Implikasi
Febrian Kwarto, Madya Angsito (2018)	Meneliti pengaruh *Cybercrime* (*hacking, phishing, malware*) terhadap kepatuhan keamanan *cyber* di sektor keuangan, serta menguji validitas dan reliabilitas variabel-variabel tersebut dalam konteks kepatuhan keamanan informasi dengan menggunakan *framework* ISO 27001/ISMS.	Metode yang digunakan dalam jurnal ini meliputi *convenience sampling* untuk menentukan sampel responden, serta uji statistik F untuk menunjukkan pengaruh variabel independen terhadap variabel dependen	Temuan baru yang didapat dari jurnal ini adalah adanya pengaruh positif dari malware terhadap kepatuhan keamanan cyber di sektor keuangan.	Pentingnya untuk meningkatkan kepatuhan keamanan cyber di sektor keuangan dalam menghadapi ancaman *Cybercrime*, seperti malware dan hacking.
Alexander Anggoano, Tarjo, Moh. Riskiyadi (2021)	Tantangan yang dihadapi oleh industri *fintech* terkait dengan *Cybercrime* dan untuk menyajikan langkah-langkah antisipatif dalam bentuk cybersecurity yang dapat	Metodenya meliputi perencanaan, pelaksanaan, dan pelaporan dalam 8 langkah. Langkah-langkah tersebut mencakup merumuskan masalah, mengembangkan serta memvalidasi	Industri fintech menghadapi tantangan yang signifikan terkait dengan *Cybercrime*, seperti serangan phishing, malware, dan kebocoran data.	Pentingnya perusahaan fintech untuk meningkatkan langkah-langkah cybersecurity guna melindungi diri dari ancaman *Cybercrime*

	dilakukan oleh perusahaan fintech untuk mengatasi ancaman tersebut.	protokol tinjauan, mencari literatur relevan, menyaring literatur yang sesuai, mengevaluasi kualitas literatur, mengekstraksi data, menganalisis dan mensintesis data, serta menghasilkan laporan mengenai hasil penelitian.		yang semakin kompleks
Diny Luthfah (2023)	Membahas pentingnya peningkatan keamanan siber di sektor jasa keuangan di Indonesia, serta untuk mengidentifikasi permasalahan, kebijakan, dan strategi yang diperlukan dalam menghadapi ancaman keamanan siber yang semakin kompleks	Metode pengambilan data yang digunakan dalam jurnal ini adalah metode penelitian hukum normatif. Data yang digunakan adalah data sekunder yang digunakan meliputi peraturan hukum, jurnal, dan buku yang berkaitan dengan keamanan siber di sektor jasa keuangan di Indonesia.	Pentingnya pengembangan keamanan siber dalam sektor jasa keuangan di Indonesia terutama karena sektor keuangan menjadi sasaran serangan siber yang semakin canggih dan menggunakan malware, sehingga menjadi lebih rentan terhadap insiden siber.	Ancaman keamanan siber semakin kompleks dan tidak hanya terbatas pada sektor perbankan, sehingga perlu adanya kebijakan dan strategi yang lebih proaktif dalam menghadapi ancaman tersebut
Restika, Era Sonita (2023)	Keterkaitan antar perlindungan siber dan kestabilan keuangan, terutama pada kondisi bank	Metode yang digunakan dalam jurnal ini meliputi pengumpulan data dari sumber-sumber seperti jurnal ilmiah, buku	Temuan utama dari jurnal ini mencakup pentingnya diversifikasi sumber likuiditas dalam	Penelitian ini menekankan pentingnya integrasi tatakelola likuiditas dan keamanan siber

	syariah, serta untuk memberikan rekomendasi praktis dalam mengatasi hambatan keamanan jaringan dalam manajemen likuiditas bank syariah serta pentingnya mengintegrasikan manajemen likuiditas dan keamanan siber untuk memastikan stabilitas keuangan dan keamanan bank syariah di era digital.	rujukan, dan laporan institusi keuangan internasional. Selain itu, analisis mendalam dilakukan terhadap bahan bacaan terpilih untuk menemukan motif dan tren dalam konteks keterkaitan antara keamanan siber dan stabilitas keuangan melibatkan pengakuan bahwa integrasi pengelolaan likuiditas dan keamanan siber menjadi krusial dalam menangani ancaman potensi yang terkait.	memperkuat daya tahan bank syariah mengenai fluktuasi likuiditas. Selain itu, bank syariah rentan terhadap serangan siber seperti *phishing*, *malware*, dan *ransomware*, sehingga kepatuhan terhadap prinsip syariah dalam menjaga keamanan siber sangat penting. Integrasi manajemen likuiditas dan keamanan siber diidentifikasi sebagai kunci untuk melindungi stabilitas keuangan bank syariah di era digital.	dalam menjamin stabilitas keuangan bank syariah di era digital. Diversifikasi sumber likuiditas dan kepatuhan terhadap prinsip syariah adalah faktor kunci dalam menghadapi tantangan keamanan siber. Selain itu, penelitian ini memberikan rekomendasi praktis bagi lembaga keuangan serupa untuk meningkatkan praktik manajemen likuiditas dan keamanan siber mereka.

Rudiantno, Aldea Mita Cheryta (2022)	Membahas evaluasi kebijakan cyber security di sektor perbankan, dengan fokus pada Bank BTN Cabang Surabaya, serta untuk menganalisis langkah-langkah preventif yang dilakukan dalam menghadapi kejahatan *Cybercrime*	Metode penelitian yang digunakan dalam jurnal tersebut adalah metode kualitatif yang melibatkan wawancara, dokumentasi, dan observasi dalam menganalisis fenomena permasalahan terkait kebijakan cyber security di sektor perbankan	Meliputi analisis kebijakan cyber security di Bank BTN Cabang Surabaya, strategi pencegahan *Cybercrime*, kendala dalam evaluasi kebijakan, serta pentingnya keamanan cyber dalam ekonomi digital. Selain itu, penelitian ini juga memberikan kontribusi terhadap perkembangan ilmu pengetahuan dan menyoroti aksi serangan cyber terhadap sektor perbankan di Indonesia	Pentingnya evaluasi kebijakan cyber security di sektor perbankan, perlunya strategi pencegahan *Cybercrime* yang efektif, serta tantangan dalam implementasi kebijakan tersebut. Selain itu, adanya resistensi pejabat terkait dan kompleksitas masalah publik juga menjadi faktor yang perlu diperhatikan dalam upaya meningkatkan keamanan cyber di sektor perbankan

Dari beberapa jurnal yang telah diperoleh, penulis melakukan tinjauan terhadap lima jurnal yang memiliki topik tentang *cyber security* terhadap sektor perbank. Jurnal pertama yang berjudul "Pengaruh *Cyber Crime* Terhadap *Cyber Security Compliance* Di Sektor Keuangan". Penelitian ini menemukan bahwa *hacking*, *phishing*, dan *malware* memiliki pengaruh positif signifikan terhadap kepatuhan keamanan *cyber* di sektor keuangan, yang berarti peningkatan ancaman ini meningkatkan kepatuhan keamanan. Data penelitian data memiliki bentuk distribusi normal dan model regresi memenuhi asumsi tentang normalitas, menunjukkan validitas dan reliabilitas data. Implikasinya adalah pentingnya peningkatan sistem keamanan *cyber* dan kepatuhan terhadap aturan untuk menghadapi ancaman *cyber crime* (Kwarto & Angsito, 2018).

Jurnal kedua yang berjudul "*Cybercrime* dan *Cybersecurity* pada Fintech: Sebuah Tinjauan Pustaka Sistematis". Penelitian ini menyimpulkan bahwa industri fintech menghadapi tantangan signifikan terkait *Cybercrime* seperti *phishing*, *malware*, dan pencurian data. Untuk mengatasi ancaman ini, diperlukan langkah-langkah antisipatif seperti perlindungan titik akses nirkabel, pengendalian hak akses, pencegahan target *Cybercrime*, otentikasi program pemindaian virus, dan pemindaian berkala dengan *antispyware*. Langkah-langkah proaktif, penguatan regulasi, dan pembentukan kerangka kerja keamanan cyber yang kokoh sangat penting. Kerjasama antara perusahaan fintech, regulator, dan pihak terkait juga ditekankan untuk memperkuat pertahanan terhadap cybercrime. Penelitian ini memberikan wawasan berharga bagi akademisi, praktisi, dan pelaku fintech dalam menghadapi tantangan keamanan cyber (Riskiyadi *et al*., 2021).

Jurnal ketiga berjudul "Penguatan Keamanan Siber Pada Sektor Jasa Keuangan Indonesia". Studi ini menyoroti pentingnya penguatan keamanan siber di sektor jasa keuangan Indonesia untuk menghadapi ancaman yang semakin kompleks. Dibutuhkan kebijakan dan regulasi yang mengatur perlindungan data, mencakup bidang keuangan non-bank dan pasar modal. Penelitian normatif ini menganalisis peraturan dan sumber terkait keamanan siber, menekankan aspek integritas, kerahasiaan, dan keaslian data. Strategi khusus, kepatuhan terhadap regulasi, dan kerjasama antar lembaga menjadi kunci penguatan keamanan siber. Badan Siber dan Sandi Negara berperan penting dalam menghadapi ancaman siber dan menjadikan keamanan siber bagian integral dari keamanan nasional. Kebijakan, regulasi, dan kerjasama yang terstruktur diperlukan untuk menjaga stabilitas sektor jasa keuangan dan keamanan nasional (Luthfah, 2023).

Jurnal keempat berjudul "Tantangan Keamanan Siber Dalam Manajemen Likuiditas Bank Syariah: Menjaga Stabilitas Keuangan Di Era Digital". Penelitian ini menyimpulkan bahwa bank syariah perlu memperhatikan keamanan siber sebagai aspek penting dalam manajemen likuiditas mereka untuk menjaga reputasi, kepercayaan pelanggan, dan stabilitas keuangan. Diversifikasi sumber likuiditas, pelatihan keamanan karyawan, integrasi antara manajemen likuiditas dan keamanan siber, serta penerapan teknologi canggih merupakan langkah-langkah praktis yang dapat diambil untuk mengatasi permasalahan keamanan jaringan dalam pengelolaan likuiditas bank syariah. Selain itu, kesadaran dan pendidikan keamanan juga penting untuk melindungi bank syariah dari serangan siber dan menjaga keamanan informasi mereka (Restika & Sonita, 2023).

Jurnal kelima berjudul "Evaluasi Kebijakan Cyber Security Sektor Perbankan Bank BTN Cabang Surabaya". Penelitian ini menemukan bahwa evaluasi kebijakan keamanan siber di Bank BTN Cabang Surabaya menghadapi kendala seperti sumber daya yang tidak memadai, metode evaluasi yang tidak tepat, kontradiksi kebijakan, biaya tinggi, dan mekanisme penyelesaian konflik yang kurang efektif. Meskipun demikian, Bank BTN Surabaya telah mengambil langkah-langkah preventif yang baik, termasuk evaluasi kebijakan berkala, kerjasama dengan IT dan kepolisian, serta audit eksternal. Kesimpulannya, keamanan siber adalah tantangan serius bagi sektor perbankan, dan evaluasi kebijakan yang matang sangat penting untuk mencegah kejahatan siber. Dukungan sumber daya manusia, pelatihan, penilaian kinerja, dan kerjasama dengan pemerintah serta lembaga terkait adalah kunci pengembangan kebijakan keamanan siber yang efektif. Penelitian ini memberikan wawasan

penting tentang pentingnya evaluasi kebijakan dan strategi pencegahan kejahatan siber di sektor perbankan (Rudiatno & Cheryta, 2022).

KESIMPULAN

Penelitian ini menyimpulkan bahwa ancaman seperti *Hacking*, *Phishing*, dan *Malware* berkontribusi terhadap peningkatan kepatuhan terhadap keamanan siber di sektor keuangan. Di sektor fintech, diperlukan tindakan proaktif dan kolaborasi untuk menghadapi ancaman tersebut. Di Indonesia, perkuatan kebijakan dan regulasi keamanan siber menjadi sangat penting untuk menjaga stabilitas sektor jasa keuangan. Bank syariah perlu mengintegrasikan manajemen likuiditas dan keamanan siber guna mempertahankan stabilitas dan kepercayaan. Meskipun evaluasi kebijakan keamanan siber di Bank BTN Surabaya menghadapi kendala, langkah-langkah pencegahan telah diambil. Secara kesimpulan, meningkatkan keamanan siber dan meningkatkan kerjasama antar lembaga merupakan langkah penting dalam menghadapi ancaman *Cybercrime*.

Hasil penelitian menunjukkan bahwa sektor keuangan perlu mengadopsi teknologi keamanan canggih seperti enkripsi data dan sistem deteksi intrusi, serta memberikan edukasi berkelanjutan kepada karyawan dan nasabah. Di sektor fintech, diperlukan tindakan proaktif dan kolaborasi untuk menghadapi ancaman ini. Perbankan harus mengintegrasikan manajemen likuiditas dan keamanan siber guna mempertahankan stabilitas dan kepercayaan.

DAFTAR PUSTAKA

Ervina Chintia, R. N. (2018). Kasus Kejahatan Siber yang Paling Banyak Terjadi di Indonesia dan Penanganannya. *Journal Information Engineering and Education Technology, Volume 02, Nomor 02*, 65-69.

Fitria, K. M. (2023). ANALISIS SERANGAN MALWARE DALAM PERBANKAN DAN PERENCANAAN SOLUSI KEAMANAN. *Jurnal Informatika dan Teknik Elektro Terapan*, 721-730.

Kwarto, F., & Angsito, M. (2018). Pengaruh Cyber Crime Terhadap Cyber Security Compliance Di Sektor Keuangan. *Jurnal Akuntansi Bisnis*, *11*(2), 99–110. https://doi.org/10.30813/jab.v11i2.1382

Luthfah, D. (2023). Penguatan Keamanan Siber Pada Sektor Jasa Keuangan Indonesia. *Jurnal Penelitian Dan Karya Ilmiah Lembaga Penelitian Universitas Trisakti*, *9*, 259–267. https://doi.org/10.25105/pdk.v9i1.18643

Marzali, A.-. (2017). Menulis Kajian Literatur. *ETNOSIA : Jurnal Etnografi Indonesia*, *1*(2), 27. https://doi.org/10.31947/etnosia.v1i2.1613

Mia Hatyati Wibowo, N. F. (2017). Ancaman Phising Terhdap Pengguna Sosial Media Dalam Dunia Cyber Crime. *Jurnal of Eduaction and Information Communication Technology, Volume 1, Nomor 1*, 1-5.

Restika, R., & Sonita, E. (2023). Tantangan Keamanan Siber Dalam Manajemen Likuiditas Bank Syariah : Menjaga Stabilitas Keuangan Di Era Digital. *Krigan: Journal of Management and Sharia Business*, *1*(2), 25. https://doi.org/10.30983/krigan.v1i2.7929

Riskiyadi, M., Anggono, A., & Tarjo. (2021). *Cybercrime* dan Cybersecurity pada Fintech: Sebuah Tinjauan Pustaka Sistematis. *Jurnal Manajemen Dan Organisasi*, *12*(3), 239–251.

https://doi.org/10.29244/jmo.v12i3.33528
Rudiatno, R., & Cheryta, A. M. (2022). Evaluasi Kebijakan Cyber Security Sektor Perbankan Bank Btn Cabang Surabaya. *Jurnal Apresiasi Ekonomi*, *10*(3), 321–331. https://doi.org/10.31846/jae.v10i3.503