Jurnal Kewirausahaan dan Multi Talenta (JKMT)
E-ISSN : 2962-8873
P-ISSN : 2964-6049
Siber Nusantara Publisher
+62 811 7404 445 http://siberpublisher.org siberpublisher.info@gmail.com Jalan Marina Indah Raya No. 1 Pantai Indah Kapuk, Kamal Muara, Penjaringan, Jakarta Utara, Indonesia.
DOI: https://doi.org/10.38035/jkmt.v2i2
Received: 10 April 2024, **Revised:** 22 Mei 2024, **Publish:** 10 Juni 2024
https://creativecommons.org/licenses/by/4.0/

Peran Manajemen Sekuriti Dalam Mencegah Resiko Kerugian Terhadap Keuangan Digital

Yulisbet Hutapea[1], Achmad Fauzi[2], Amanda Dwiyanti[3], Fajrina Ajeng Alifah[4], Niyar Andina[5*], Sania Murtafia Dara Jati[6]
[1.] Mahasiswa Program Studi Manajemen, Universitas Bhayangkara Jakarta Raya, Indonesia, email: yulisbethutapea88@gmail.com
[2.] Dosen Program Studi Manajemen, Universitas Bhayangkara Jakarta Raya, Indonesia, email: achmad.fauzi@dsn.ubharajaya.ac.id
[3.] Mahasiswa Program Studi Manajemen, Universitas Bhayangkara Jakarta Raya, Indonesia, email: mndadwiynti@gmail.com
[4.] Mahasiswa Program Studi Manajemen, Universitas Bhayangkara Jakarta Raya, Indonesia, email: fajrina0405@gmail.com
[5.] Mahasiswa Program Studi Manajemen, Universitas Bhayangkara Jakarta Raya, Indonesia, email: andinaniyar24@gmail.com
[6.] Mahasiswa Program Studi Manajemen, Universitas Bhayangkara Jakarta Raya, Indonesia, email: saniamurtafia383@gmail.com

[*]Corresponding Author: Niyar Andina[5]

***Abstract*:** The number of people using the internet is constantly rising, driven in large part by the conveniences it provides. Things are simpler in this digital age since, for example, we can now save money and do transactions online. Many individuals save sensitive information in digital apps, which increases the danger of internet security, but the convenience of online transactions also increases the number of cybercrimes. This is a major issue in the modern digital age, since there have been several instances of data breaches, including instances of digital financial theft using personal data. Because of this, security management is essential for avoiding loss. "The Role of Security Management in Helping with the Risk of Losses in Digital Finance" is reviewed in this article. In order to generate hypotheses that connect one variable to other variables, this article seeks to provide information for future study. Following is a presentation of the library's findings in this article: 1) Management of Security, 2) Security, 3) Loss Prevention, 4) Financial Technology.

Keywords: *Security Management, Risk of Loss, Digital Finance*

Abstrak: Jumlah orang yang menggunakan internet terus meningkat, sebagian besar didorong oleh kemudahan yang diberikannya. Segalanya menjadi lebih sederhana di era digital ini, misalnya saja kita sekarang bisa berhemat dan bertransaksi secara online. Banyak orang menyimpan informasi sensitif dalam aplikasi digital, yang meningkatkan bahaya keamanan internet, namun kenyamanan transaksi online juga meningkatkan jumlah kejahatan dunia maya. Hal ini merupakan masalah besar di era digital modern, karena telah terjadi beberapa kasus pembobolan data, termasuk pencurian keuangan digital yang menggunakan data pribadi. Oleh karena itu, manajemen keamanan sangat penting untuk menghindari kerugian. "Peran Manajemen Keamanan dalam Membantu Risiko Kerugian pada Keuangan Digital"

diulas dalam artikel ini. Untuk menghasilkan hipotesis yang menghubungkan satu variabel dengan variabel lainnya, artikel ini berupaya memberikan informasi untuk penelitian selanjutnya. Berikut pemaparan temuan perpustakaan pada artikel ini: 1) Manjemen Sekuriti, 2) Keamanan, 3) Pencegahan Kerugian, 4) Teknologi Finansial.

Kata Kunci: Manajemen Sekuriti, Resiko Kerugian, Keuangan Digital

PENDAHULUAN

Layanan keuangan yang dapat diakses melalui internet telah menjamur dalam beberapa tahun terakhir, dengan munculnya perbankan digital, platform investasi online, sistem pembayaran elektronik, dan banyak lagi. Misalnya, DANA adalah platform dompet elektronik terkemuka di Indonesia. Lebih banyak orang akan dapat menggunakan dan menikmati layanan keuangan sebagai hasil dari transisi digital ini. Keluhan pelanggan yang paling umum terhadap layanan e-wallet adalah kemungkinan kehilangan dana. Pengguna mungkin mengalami kerugian moneter karena faktor-faktor seperti kesalahan teknologi, kejahatan dunia maya, atau gangguan eksternal. Individu yang melaporkan masalah tersebut seringkali menerima tanggapan yang tidak memuaskan. Ancaman baru terhadap keamanan siber adalah salah satu dari banyak masalah baru yang ditimbulkan oleh platform digital. Karena kepercayaan mereka dalam mengelola uang dan informasi pribadi dalam jumlah besar, penipu menargetkan organisasi keuangan. Dengan alat yang tepat dan akses ke internet, penjahat dunia maya dapat menyerang kapan saja, siang atau malam. Baik masyarakat maupun dunia usaha mungkin kehilangan banyak uang karena masalah keamanan siber. Serangan dunia maya bisa sangat menghancurkan sehingga membahayakan keberadaan perusahaan, khususnya usaha kecil dan menengah yang tidak memiliki modal untuk pulih dengan cepat (Sari, 2022)**.**

Kerugian finansial adalah kerugian yang ditimbulkan terhadap kekayaan organisasi, dan biaya untuk menghindari kejahatan dunia maya meningkat atau menurun setiap hari sebagai akibat dari bahaya ini (Sharif & Mohammed, 2022)**.** Pencurian dana dari rekening bank hanyalah salah satu aspek dari masalah ini; pelanggaran data dan kerusakan reputasi menyebabkan sanksi peraturan, tagihan hukum, dan biaya lainnya. Kerugian yang disebabkan oleh kejahatan dunia maya terus meningkat seiring berjalannya waktu. Inilah sebabnya kita perlu mengambil tindakan pencegahan untuk menghentikan serangan siber yang terus terjadi. Menggunakan sistem yang dikenal sebagai Manajemen Keamanan adalah salah satu pilihan. Menurut penelitian, manajemen keamanan merupakan kebutuhan penting bagi bisnis dan organisasi modern (Fachrudin et al., 2024)**.** Jika, misalnya, informasi pribadi nasabah IMF bocor, melindungi informasi ini adalah hal yang paling penting. Kontroversi muncul seputar Klausul Ketiadaan Perlindungan Data Pribadi Apa pentingnya akuntabilitas Informasi pribadi konsumen mungkin bocor, menurut tanggapan Dana. Konstitusi Indonesia perlu memasukkan persyaratan untuk menjaga informasi pribadi seseorang. Harus ada konsekuensi hukum yang jelas atas setiap pelanggaran atau kecerobohan terkait data pribadi di Indonesia (Muhammad Fathur, 2020)**.** Karyanya pada akuntansi pengendalian informasi dan fungsi dapat membantu pencegahan kejahatan dunia maya yang mendalam dengan meningkatkan konten aturan internal individu (Yang & Yin, 2023). dalam pembukuan sistem. Informasi dan teknologi keamanan dapat dilindungi dari serangan dunia maya dan bahaya keamanan lainnya melalui penerapan terintegrasi, manajemen risiko yang ketat, dan pelaksanaan kebijakan keamanan yang eksplisit. (Mahardhika et al., 2023) juga mendukung temuan ini.

Mencegah bahaya kerugian besar pada perbankan digital memerlukan penerapan sistem manajemen keamanan, menurut penelitian di atas. Jadi, dengan kata lain, pernyataan masalah untuk penelitian ini adalah:

1. Bagaimana teknologi mengendalikan dan melindungi kejahatan keuangan digital
2. Bagaimana Manajemen Sekuriti Dapat Mencegah Risiko Kerugian Keuangan Digital

3. Bagaimana Cara Meningkatkan Kepercayaan Pengguna Terhadap Keamanan Datanya
4. Bagaimana Mencegah Kebocoran Data?

KAJIAN PUSTAKA

Manajemen keamanan

Peningkatan efisiensi operasional, pengurangan kesalahan manusia, dan optimalisasi sumber daya manusia hanyalah beberapa dari banyak manfaat yang diperoleh dari pertumbuhan eksponensial ilmu pengetahuan dan teknologi di era digital. Memiliki kerangka kerja untuk mengelola keamanan adalah bagian penting dari teknologi yang mumpuni karena melindungi organisasi dari beberapa jenis bahaya, termasuk serangan dunia maya (Fachrudin et al., 2024)**.** Melindungi data penting dan sensitif dari perusakan, perubahan, atau akses yang tidak disengaja atau berbahaya adalah tujuan utamanya. Kita berbicara tentang sistem manajemen keamanan di sini. Kita dapat mengatur atau merencanakan keamanan dengan bantuan manajemen keamanan untuk memastikan hal ini tidak terjadi. Manajemen keamanan adalah suatu sistem yang membantu bisnis mencegah kerugian sesegera mungkin dengan memberikan pemahaman komprehensif tentang potensi ancaman, gangguan, dan keadaan, serta keterampilan dan pengetahuan yang diperlukan untuk merencanakan dan merancang cara yang tepat, efektif, dan sistem keamanan yang efisien (Rayhan et al., 2023).

Menejemen Risiko

Tidak seorang pun di sektor korporasi boleh menutup mata terhadap kemungkinan kerugian finansial. Pendekatan yang lebih tepat sasaran dalam mengelola potensi bahaya diperlukan karena semakin kompleksnya operasi perusahaan. Pada tingkat kepemimpinan tertinggi, manajemen risiko adalah proses manajemen. Seperti bentuk manajemen lainnya, manajemen risiko didasarkan pada gagasan bahwa organisasi hanya dapat menggunakan sumber daya yang dimilikinya jika terjadi sesuatu yang buruk. Tujuan manajemen risiko adalah untuk mengidentifikasi, mengevaluasi, dan memitigasi potensi ancaman. Secara teori, Anda harus melakukan ini sebelum Anda mengalami kerugian. Mengenai risiko, kecuali tindakan termasuk komponen-komponennya tidak dilakukan, tidak ada cara untuk memastikan bahwa hasil negatif dapat dihindari setiap saat. Dunia usaha memerlukan manajemen risiko atau penilaian risiko untuk membantu mereka mengendalikan bahaya-bahaya ini. Agar manajemen risiko berhasil, manajemen risiko harus meresap ke seluruh organisasi dan menjadi bagian integral dari proses. Namun demikian, banyak orang menggunakan manajemen risiko selama fase operasional atau implementasi proyek untuk membuat keputusan. tantangan yang ditimbulkan oleh risiko bahkan lebih berat (Akbar, 2022)

Keuangan Digital

Ketika orang berbicara tentang "keuangan digital", maksudnya adalah mereka menggunakan berbagai bentuk teknologi digital dan perangkat lunak khusus untuk mengelola uang mereka dengan lebih baik. Perangkat lunak akuntansi atau aplikasi keuangan digital dapat melacak semua transaksi moneter, seperti pendapatan, pengeluaran, dan arus kas, berkat pencatatan transaksi yang tepat dan teratur dalam keuangan digital. Pelaporan keuangan yang akurat dan tahan lama mungkin memiliki dasar yang kuat dari pencatatan yang kompeten. Individu dapat memiliki akses terhadap berbagai macam barang keuangan, termasuk pinjaman, investasi, asuransi, dan banyak lagi, dengan menggunakan platform digital yang dimungkinkan oleh pengelolaan keuangan digital. Pengelolaan keuangan digital bukannya tanpa bahaya keamanan, namun teknologi baru selalu dikembangkan agar lebih aman dan terjamin untuk data pengguna (Hanggondosari, 2023).

Penelitian Terdahulu

Tabel 1. Penelitian Terdahulu Yang Relevan

No	Author (Tahun)	Judul Penelitian	Hasil Riset Terdahulu	Perbedaan/ Novelty
1	(Akbar et al., 2024)	Kejahatan Keuangan Digital: Metode dan Pendekatan Kegiatan Peramalan Pemerintah Provinsi Jawa Barat di bawah Badan Pengabdian Masyarakat Persatuan Indonesia merupakan sebuah organisasi pensiunan .	Simak Selengkapnya Pejabat yang memiliki kewenangan penuh dari Pemerintah Provinsi Jawa Barat yang tergabung dalam Wadah Pensiunan Negara Kesatuan Republik Indonesia (PWRI) berikut ini.	Platform keuangan digital mendorong literasi dan inklusivitas.
2	(Nugroho et al.,2021)	Optimalisasi Penanggulangan Kebocoran Data Melalui Regulatory Blockchain Guna Mewujudkan Keamanan Siber Di Indonesia	Sistem keamanan siber di Indonesia masih membutuhkan inovasi terhadap perlindungan data pribadi, yaitu berupa sistem keamanan blockchain. Penggunaan sistem blockchain memerlukan sebuah payung hukum agar keberadannya dapat mengurangi permasalahan kebocoran data pribadi. Berkaitan dengan hal itu, diperlukan kebijakan terkait sistem keamanan siber yang memiliki orientasi pada era disrupsi terhadap perlindungan data pribadi, yaitu Regulatory Blockchain. Dalam pelaksanaannya membutuhkan peran stakeholder, seperti Kementerian Komunikasi dan Informatika, serta Badan Siber dan Sandi Negara untuk merealisasikan Pasal 28G ayat (1) UUD NRI Tahun 1945.	Sebagai langkah keamanan data, ia menggunakan teknologi blockchain.
3	(Sari, 2021)	Penegakan Hukum Kebijakan Dalam Upaya Penanggulangan Kejahatan Cyber Yang Dilakukan Oleh Virtual Police Di Indonesia.	Cari tahu Saat ini, ini adalah undang-undang pencegahan kejahatan dunia maya terbaik di Indonesia. Faktor masyarakat, faktor penegakan hukum, sarana dan fasilitas, serta variabel penegakan hukum semuanya berperan dalam membentuk penerapan peraturan perundang-undangan kejahatan siber. Dari kebijakan kejahatan dunia maya hingga tindakan, Anda harus menjaga keselarasan seiring dengan meningkatnya tingkat kecanggihan kejahatan dunia maya.	Mengenai kajian Hukum normatif Hal ini disebabkan karena kajian yang bertumpu pada doktrin, kaidah, dan hukum yang terdapat dalam peraturan, peraturan perundang-undangan, atau putusan pengadilan sering kali menggunakan sumber informasi primer, sekunder, dan tersier.
4	(Susanto et al., 2023)	Manajemen Keamanan Siber di Era Digital.	Teknologi informasi dan komunikasi telah meningkatkan kehidupan masyarakat dalam banyak hal, namun juga menimbulkan risiko serius terhadap data pribadi masyarakat.	Itu dalam pendekatan teknis, kebijakan keamanan yang kuat, pelatihan kesadaran pengguna.

5	(Muhammad Fathur, 2020)	Tanggung Jawab Tokopedia Terkait Terpaparnya Data Pribadi Konsumen	Cari tahu Konsumen yang mengalami pelanggaran data atau kecerobohan lainnya terkait Tokopedia memiliki pilihan untuk mengajukan keluhan resmi kepada lembaga pemerintah terkait, melakukan penyelesaian sengketa non-yudisial, atau mengambil tindakan hukum lebih lanjut.	Konsumen yang membocorkan data pribadi mempunyai kewajiban untuk melindungi informasi mereka.
6	(Fachrudin et al., 2024)	Peran Penting Manajemen Keamanan di Era Digitalisasi	Cari tahu Tidaklah sah untuk berkonsentrasi pada perlindungan data sensitif dan penting dari akses, modifikasi, atau penghapusan. Selain itu juga mencakup pengamanan teknologi informasi dan komunikasi (TIK) serta sumber listrik.	Teknologi informasi dan komunikasi mempunyai pengamanan. Selama itu
7	(Fahrezi et al., 2022)	Keamanan Data dan Transaksi dalam Penggunaan Cloud sebagai Layanan	Cari tahu Dalam studi ini, kami melihat kemampuan penyimpanan dan berbagi yang ditawarkan oleh aplikasi komputasi awan.	Keamanan data menjadi perhatian. Untuk memanfaatkan SaaS di cloud
8	(Irawan, 2022)	Keamanan Data Internet of Things dengan Penggunaan Teknologi Blockchain	Cari tahu Kami akan mengkaji pentingnya praktis Blockchain dan pariwisata Cerdas setelah memperkenalkan prinsip-prinsip dasar Blockchain dan menganalisis skenario yang melibatkan penerapan Blockchain di sektor pariwisata. Keamanan, privasi, dan interoperabilitas data merupakan masalah dalam lingkungan pariwisata cerdas, namun teknologi blockchain dapat memecahkan masalah keamanan tersebut.	Ini sedang menggunakan teknologi blockchain untuk keamanan data
9	(Suryawijaya , 2023)	Menjelajahi Keberhasilan Implementasi Blockchain dalam Transformasi Digital di Indonesia: Menjamin Keamanan Data	Cari tahu Ini tentang cara meningkatkan operasi keamanan data internal sehari-hari sekaligus mempercepat transformasi digital dengan menggunakan teknologi blockchain.	Sebagai langkah keamanan data, ia menggunakan teknologi blockchain.
10	(Wanda & Rahmidan , 2021)	Aplikasi Shopee dapat memengaruhi kepercayaan dan keamanan konsumen saat melakukan pembelian online.	Tujuan dari penelitian ini adalah untuk mengetahui cara mahasiswa Universitas Negeri Padang dapat menggunakan aplikasi Shopee untuk melakukan pembelian online yang lebih aman dan tepercaya.	Terletak di bawah pilihan aplikasi untuk pembelian online pasar online
11	(Rayhan et al., 2023)	Penerapan dan Manajemen Keamanan Pencegahan Di Facebook, terjadi insiden yang melibatkan penjualan online palsu.	Menggunakan Good, mengungkapkan penerapan langkah-langkah keamanan manajemen yang digunakan untuk menghindari penipuan transaksi penjualan online di pasar Facebook saat ini.	Hal ini bertujuan untuk menghindari penipuan pembelian yang dilakukan melalui pasar Facebook.
12	(Surabakti, 2023)	Teknologi Blockchain Transformatif dan Pengaruhnya terhadap Keamanan dan Kebenaran Data	Berdasarkan temuannya, blockchain ini telah berkembang menjadi lebih dari sekedar uang digital dasar. Penerapan di berbagai bidang seperti hukum, keuangan, logistik, pemeliharaan, kesehatan, serta keamanan dan integritas data telah berkembang dari hal ini.	Sebagai langkah keamanan data, ia menggunakan teknologi blockchain.
13	(Mahardhika et al., 2023)	Bagaimana Keamanan dan Kepercayaan Shopee Mempengaruhi	Dampak pasar Shopee terhadap persepsi pelanggan terhadap keamanan dan kepercayaan toko online dirinci di sini.	Shopee menyediakan lingkungan yang aman bagi

		Keputusan Pelanggan Berbelanja Online (Tinjauan Literatur Mengenai Keamanan Manajemen)		penggunanya saat mereka melakukan pembelian secara online.
14	(Putri et al., 2023)	Menganalisis Kebocoran Data Nasabah di Perbankan Digital untuk Perlindungan	Temuan dari penelitian ini Teknologi siber dan infrastruktur bergantung pada informasi ini, oleh karena itu penting untuk menjadikannya lebih tahan terhadap serangan.	Penggunaan perbankan digital dapat menimbulkan risiko keamanan bagi klien.
15	(Bukit & Ayunda, 2022)	RUU Pengamanan Kebocoran Data Penerimaan SMS Dana Cepat Perlu Pengesahan Segera	Temuan dari penelitian Inilah pendekatan RUU PDP terhadap peraturan dan undang-undang perlindungan kebocoran data, dan apa itu respon tanggung jawab SMS dana cepat.	Ada hukum perlindungan

METODE PENELITIAN

Metode penelitian kualitatif digunakan dalam penelitian ini. Dengan menggunakan strategi ini, peneliti dapat mengumpulkan data untuk melakukan pemeriksaan menyeluruh dan mendalam terhadap kebijakan sosial baru di masyarakat atau untuk memahami isu-isu rumit. Jurnal, buku, dan internet adalah tempat yang bagus untuk mendapatkan informasi semacam ini.

HASIL DAN PEMBAHASAN

Bagaimana teknologi mengendalikan dan melindungi kejahatan keuangan digital

Organisasi-organisasi di seluruh dunia menghadapi risiko keamanan siber yang lebih canggih sebagai akibat dari meluasnya teknologi dalam kehidupan modern. Studi menunjukkan bahwa perusahaan mungkin kehilangan banyak uang karena masalah keamanan siber. Khususnya bagi usaha kecil dan menengah yang tidak memiliki sarana untuk pulih dari serangan semacam itu, serangan siber dapat menimbulkan bahaya nyata bagi keberadaan mereka. Meskipun prevalensi ancaman siber semakin meningkat, banyak perusahaan terus mengabaikan manajemen keamanan. Tujuan manajemen keamanan adalah untuk melindungi perusahaan atau entitas lain dari potensi risiko keamanan, seperti serangan siber. Tujuannya adalah untuk melindungi informasi penting dan dokumen pribadi dari pengintaian dan menjaga aset teknologi informasi dan komunikasi (TIK) organisasi tetap aman dari kehilangan, penyalahgunaan, atau perubahan. Penilaian risiko, pembuatan strategi, dan implementasi kebijakan dan prosedur merupakan komponen manajemen keamanan. Antivirus, firewall, kata sandi yang kuat, dan perangkat lunak enkripsi, serta kontrol akses pengguna, dan pemantauan keamanan berkala adalah bagian dari hal ini.

Kurangnya pemahaman tentang ancaman keamanan siber dan kurangnya sumber daya untuk melaksanakan tindakan keamanan yang memadai adalah dua alasan mengapa banyak organisasi mengabaikan manajemen keamanan. Menjadi semakin sulit bagi manajer keamanan untuk mengikuti perkembangan teknologi dan lanskap perusahaan yang terus berkembang. Untuk memerangi ancaman keamanan siber yang canggih dan selalu berubah, organisasi harus terus meningkatkan rencana dan prosedur mereka. Oleh karena itu, latar belakang terbitan artikel ini menekankan perlunya manajemen keamanan yang baik dalam mencegah serangan siber terhadap informasi dan data penting, meningkatkan efisiensi operasional, dan memenangkan hati pemangku kepentingan dan konsumen. Lebih jauh lagi, konteks isu ini menekankan kesulitan yang dihadapi organisasi dalam mengatasi risiko keamanan siber, serta perlunya investasi dalam teknologi keamanan dan pendidikan untuk meningkatkan kesadaran keamanan di seluruh tingkat organisasi.

Perubahan berbagai bentuk pembayaran merupakan salah satu dampak kemajuan teknologi informasi. Masyarakat yang tadinya kebanyakan bertransaksi dengan uang tunai kini mulai memahami dan menerima pembayaran nontunai untuk berbagai barang dan jasa. Indonesia sedang giat mengembangkan uang elektronik atau yang dikenal dengan e-money sebagai salah satu alat pembayaran nontunai.

Mulai dari kemudahan penggunaan layanan e-money hingga kemudahan penggunaan e-money itu sendiri, e-money menawarkan sejumlah keunggulan, yang paling menonjol adalah kecepatan, kemudahan, dan efisiensi dibandingkan pembayaran non-tunai lainnya. instrumen. Meski begitu, masih belum banyak masyarakat yang menggunakan uang elektronik. Hal ini disebabkan karena masyarakat belum sepenuhnya memahami kemudahan dan manfaat bertransaksi e-money, sehingga berdampak pada rendahnya kepercayaan terhadap pembayaran e-money, sehingga bertentangan dengan tujuan e-money yaitu mempermudah dan menyederhanakan transaksi. daripada lebih sulit (putra et al., 2022)**.** Jumlah masyarakat yang menggunakan uang elektronik, khususnya antara tahun 2011 dan 2014, merupakan indikator yang jelas mengenai hal ini, menurut statistik dari Bank Indonesia. Jumlah masyarakat yang menggunakan uang elektronik meningkat antara tahun 2011 dan 2013. Namun pada akhir tahun 2014, jumlah tersebut turun 1,34 persen dibandingkan tahun sebelumnya.

Persepsi bahaya adalah komponen lain yang mempengaruhi minat menggunakan teknologi, selain persepsi manfaat dan persepsi kemudahan penggunaan. Ternyata masih ada sebagian orang yang tidak mau memanfaatkan teknologi meskipun teknologi mempunyai banyak kelebihan dan kemudahan yang ditawarkannya, dengan alasan kekhawatiran mengenai keamanan dan ketidakpastian (Sari, 2022)**.** Tingkat bahaya yang ada merupakan salah satu aspek yang dapat mempengaruhi cara pelanggan melihat suatu produk. Seseorang harus mempertimbangkan potensi keuntungan dan kerugian dari situasi yang tidak diketahui saat memutuskan apakah akan melanjutkan transaksi atau tidak. Faktor risiko keamanan ini harus diperhatikan oleh penerbit uang elektronik (e-money) agar masyarakat tidak terlalu khawatir terhadap risiko yang terkait dengan transaksi elektronik dan persepsi masyarakat terhadap risiko yang timbul dari transaksi tersebut. Beberapa potensi permasalahan yang mungkin dihadapi pengguna uang elektronik antara lain kesalahan yang dilakukan pengguna (human error) saat melakukan penambahan dana atau karena fasilitas yang di bawah standar dan terbatas pada sejumlah kecil kota besar.

Oleh karena itu, penyedia layanan harus menjaga informasi pribadi kliennya sesuai dengan aturan yang memberikan dasar hukum untuk melakukan hal tersebut, khususnya Undang-undang No. 8 Tahun 2019 tentang Perlindungan Konsumen dan UU No. 2011 tentang Otoritas Jasa Keuangan. Memberikan kenyamanan kepada pelanggan memerlukan jaminan keamanan data pribadi ke tingkat setinggi mungkin. Penggunaan kecerdasan buatan adalah salah satu dari banyak cara yang mungkin untuk memaksimalkan potensi. Keberadaan AI meningkatkan produktivitas dan efisiensi manusia dengan mengurangi kemungkinan kesalahan sistem dan kebocoran data pribadi yang disebabkan oleh kesalahan manusia. AI dilengkapi dengan kemampuan anti malware. Pada saat ini, kapasitas kecerdasan buatan untuk mendeteksi suatu masalah dianggap melampaui kemampuan kecerdasan manusia. Kekuatan komputasi dan kapasitas untuk menangani data dalam jumlah besar merupakan tulang punggung kecerdasan buatan, yang memungkinkan program komputer pintar untuk mengalahkan manusia dalam hal kapasitas belajar. Dalam hal memenuhi kebutuhan manusia di masa depan, kecerdasan buatan akan sangat berharga.

Kecerdasan buatan memiliki beberapa penerapan praktis; misalnya, hal ini dapat membantu penyelesaian permasalahan yang sulit diselesaikan dengan menggunakan pendekatan tradisional, merangkum dan memahami data dalam jumlah besar, dan memfasilitasi pencarian kumpulan data yang sangat besar. Orang-orang dapat menyelesaikan pekerjaan mereka dengan lebih efisien dan efektif karena hal ini. Tentu saja Indonesia,

sebagai negara yang telah sepenuhnya menganut Revolusi Industri Keempat, perlu mengambil langkah-langkah inovatif dan berpikiran maju untuk mengatasi permasalahan saat ini, khususnya di bidang keamanan data.

Bagaimana Manajemen Sekuriti Dapat Mencegah Risiko Kerugian Keuangan Digital

Dalam masyarakat yang terhubung secara global saat ini, kejahatan keuangan digital menjadi jauh lebih luas. Serangan terhadap informasi pribadi dan keuangan masyarakat telah meningkat secara dramatis selama lima tahun terakhir di banyak negara. Kejahatan dunia maya adalah masalah global yang mempengaruhi masyarakat dan bisnis di mana pun karena tidak mengenal batas. Industri perbankan di Indonesia telah menjadi sasaran menjamurnya kejahatan dunia maya dalam lima tahun terakhir, menurut penelitian (Akbar et al., 2024)**.**

(1) Penipuan perbankan online telah menjadi jenis kejahatan keuangan digital yang paling umum di Indonesia dan terus meningkat. Phishing, spyware, dan rekayasa sosial adalah beberapa metode canggih yang digunakan penjahat untuk mendapatkan akses tidak sah ke rekening bank pribadi.

(2) Pertumbuhan pesat platform pembayaran seluler telah menyebabkan penipu menargetkan sistem ini secara khusus karena kelemahan keamanannya. Penipuan pembayaran seluler telah meningkat dalam beberapa tahun terakhir, dengan pelaku yang menggunakan berbagai metode termasuk pemasangan aplikasi palsu, peralihan kartu SIM, dan pembelian tidak sah.

(3) Penipuan mata uang kripto: penipu yang memangsa investor yang tidak menaruh curiga telah menyadari booming mata uang kripto di Indonesia. Semakin banyak orang yang tertipu oleh penipuan investasi mata uang kripto, seperti skema Ponzi dan penawaran koin awal (ICO) palsu. Masyarakat harus mewaspadai bahaya berinvestasi pada mata uang kripto yang tidak diatur, menurut Otoritas Jasa Keuangan (OJK).

(4) Peningkatan kasus pencurian identitas yang mengkhawatirkan terjadi seiring dengan maraknya pembobolan data, yang telah menjadi masalah kronis bagi masyarakat Indonesia. Penjahat online bertujuan untuk mencuri informasi sensitif dengan meretas database yang dikelola oleh lembaga keuangan, pasar online, dan entitas pemerintah. Pelanggaran data meningkat, menurut Badan Siber dan Sandi Negara (BSSN).

(5) Kejahatan keuangan digital di Indonesia juga dikaitkan dengan pendanaan teroris dan pencucian uang. Sulit bagi pihak berwenang untuk mengidentifikasi dan melarang aktivitas kriminal menggunakan platform internet karena mudahnya penjahat mengirimkan uang yang melanggar hukum. Dalam upaya memerangi pencucian uang online, Pusat Pelaporan dan Analisis Transaksi Keuangan (PPATK) telah bekerja sama dengan mitra dari seluruh dunia.

Jadi, ada cara untuk melakukan itu juga. (Susanto et al., 2023) menyebutkan beberapa cara penjahat siber beroperasi sebagai berikut:

A. Pemecah Kata Sandi

Adalah praktik mendapatkan akses tidak sah ke akun lain dengan mendekripsi kata sandinya menggunakan perangkat lunak. Untuk menonaktifkan mekanisme keamanan password, prosedur ini juga sering dilakukan.

B. Memalsukan

Adalah kasus ketika penjahat atau programnya berhasil meniru identitas pengguna lain, seringkali pengguna asli komputer atau jaringan, dengan memanipulasi data. Email, layanan pesan singkat (SMS), dan metode lain berlimpah untuk spoofing.

C. DDoS (Serangan Penolakan Layanan Terdistribusi)

Merupakan penyerangan terhadap sistem komputer atau jaringan korban.

Tujuan dari serangan penolakan layanan terdistribusi ini adalah menyebabkan server atau jaringan kehilangan semua sumber daya yang tersedia, sehingga tidak dapat melakukan tujuan yang dimaksudkan.

D. Mengendus

Ini adalah jenis kejahatan dunia maya yang terjadi ketika pelaku baik sengaja atau tidak sengaja mengambil kredensial login korbannya. Pelaku kemudian dapat merusak atau

menghapus data korban atau melakukan penipuan dengan menggunakan akun korban.
E. Mengirimkan Perangkat Lunak Jahat
Jenis kejahatan dunia maya lainnya adalah distribusi perangkat lunak berbahaya dengan tujuan merusak atau menghapus data yang tersimpan di server atau jaringan korban. Beberapa Spyware, malware, worm, trojan, adware, ransomware, dan virus semuanya merupakan bagian dari kategori ini. F. Pelaku pencurian dan penipuan, serta pelaku kejahatan siber, sering kali menggunakan layanan money mule untuk mencuci dana yang diperoleh secara tidak sah. Istilah "money bagal" mengacu pada individu yang memindahkan uang dari satu rekening ke rekening lain menggunakan internet, layanan kurir, atau sarana teknologi lainnya (Leukfeldt & Jansen, 2016)**.**

Masyarakat hanya dapat memaksimalkan kesejahteraannya dengan meningkatkan literasi digitalnya, yang mencakup pemahaman tentang apa itu uang digital dan cara memanfaatkannya. Ada berbagai pilar yang menjadi landasan keamanan siber. Keamanan siber sebagian besar terdiri dari hal-hal berikut: (Ozili, 2021)
1. Kebijakan keamanan dokumen merupakan komponen penting dari setiap prosedur keamanan siber karena berfungsi sebagai standar acuan. Tujuan dari makalah ini adalah sebagai prosedur operasi standar keamanan siber dan referensi.
2. Infrastruktur Informasi: Komponen ini, yang terdiri dari perangkat lunak dan perangkat keras, sangat penting untuk upaya pertahanan siber.
3. Perimeter Defense Perimeter: Merupakan komponen pertahanan utama, yaitu bagian perangkat seperti Intrusion Prevention System (IPS), Intrusion Detection System (IDS) dan firewall. Dalam hal melindungi data sensitif, gadget ini berada di garda depan.
4. Sistem Pemantauan Jaringan: Ini adalah komponen media yang membantu mengawasi cara kerja sistem keamanan siber. Dan bukan itu saja: ia mengawasi perangkat lunak dan perangkat keras yang membentuk operasi dunia maya.
5. Sistem Informasi dan Manajemen Peristiwa: Merupakan bagian dari sistem keamanan siber yang mencatat dan melaporkan kejadian, serta sistem informasi yang menangani insiden.
6. Penilaian Keamanan Jaringan: Ketika mengukur tingkat keamanan siber atau teknologi informasi, komponen ini bertanggung jawab untuk evaluasi dan pengendalian.
7. Sumber Daya Manusia dan Kesadaran Keamanan: Manusia, baik sebagai elemen atau sebagai pengguna, merupakan titik lemah dalam industri keamanan TI. Oleh karena itu, komponen ini harus meningkatkan pemahaman tentang mengapa keamanan TI lebih penting daripada keamanan siber.

Keuntungan dari keamanan siber adalah sebagai berikut:

- Dapat menghentikan penyusup untuk mengakses dan menggunakan jaringan komputer. Membantu memulihkan dan menjalankan komputer setelah serangan cyber dengan lebih cepat.
- Jika organisasi menganggap serius keamanan siber, maka hal ini dapat mengembalikan kepercayaan pelanggannya. Oleh karena itu, konsumen percaya pada bisnis kita dan penawarannya.

Bagaimana Cara Meningkatkan Kepercayaan Pengguna Terhadap Keamanan Datanya

Dua faktor yang saling berhubungan dan penting dalam pilihan konsumen adalah kepercayaan terhadap merek dan keamanan informasi pribadi mereka. (Puanda & Rahmidani, 2021) kapasitas untuk menciptakan kepercayaan di antara pelanggan dan memastikan keamanan mereka selama pembelian online merupakan faktor kunci dalam menarik dan mempertahankan pelanggan. Selain itu, dikatakan bahwa jaminan keamanan ini memiliki tujuan penting dalam membangun kepercayaan dengan meminimalkan perhatian pelanggan terhadap rincian transaksi yang mudah dipalsukan dan informasi yang disalahgunakan. Karena semakin maraknya kasus kecurangan dan penipuan di situs belanja online akibat kemajuan teknologi, maka pengamanan transaksi ini merupakan salah satu upaya untuk mencegahnya. Berdasarkan hasil ini, konsumen harus memprioritaskan keamanan data agar

bisnis dapat menumbuhkan kepercayaan dalam pengalaman pembelian online mereka. Meningkatkan kepercayaan pengguna terhadap keamanan data dapat dilakukan dengan berbagai cara. Aplikasi Shopee misalnya, menawarkan keamanan yang baik dalam bertransaksi, yang merupakan salah satu variabel keamanan yang mempengaruhi pilihan pembelian (Puanda & Rahmidani, 2021) Keamanan data menentukan indikasi yang digunakan untuk mengukur kepercayaan, yang pada gilirannya sangat mempengaruhi penilaian. Dalam situasi ini, tim Shopee mempunyai strategi untuk membuat pengguna merasa aman dalam menggunakan aplikasi, yaitu dengan memberikan jaminan keamanan yang dimulai dengan pembelian tanpa kerumitan dan pertemuan yang menyenangkan dengan vendor.

Keamanan data juga akan ditingkatkan dalam operasional sehari-hari untuk memenangkan lebih banyak pelanggan yang percaya selama bertransaksi. Jika kita ingin lebih banyak orang percaya bahwa data mereka aman, kita perlu membuat sistem keamanan data yang lebih baik (Suryawijaya, 2023). Salah satu proyek tersebut adalah inisiatif blockchain di Indonesia, yang telah mulai memvalidasi dan memverifikasi sertifikat pendidikan, rekam medis, dan sistem pembayaran. Penggunaan teknologi blockchain dapat meningkatkan keamanan data karena memungkinkan penyimpanan data terdesentralisasi dan terenkripsi, yang menjaga keamanan data. Karena tidak ada satu tempat penyimpanan untuk informasi ini, pencuri data akan kesulitan melakukan perubahan tanpa persetujuan dari semua peserta di blockchain. Untuk lebih mendorong keterbukaan dan mengurangi kemungkinan pencurian, teknologi ini juga memastikan bahwa semua pihak yang berpartisipasi dalam suatu transaksi dapat memverifikasinya. (Irawan, 2022) permasalahan keamanan data dapat diatasi dengan penggunaan teknologi Blockchain. Selain itu, privasi dan keamanan yang diberikan oleh enkripsi blockchain dan kemampuan kunci pribadi, serta arsitektur berbagi peer-to-peer, dapat meningkatkan kepercayaan konsumen. Dengan teknologi blockchain, transaksi digital antara dua pihak tanpa rasa saling percaya dapat diselesaikan secara langsung, sehingga memecahkan masalah kepercayaan dalam transaksi digital. Mendorong lebih banyak kepercayaan dan jaminan dalam transaksi yang aman melalui sistem seperti sistem blok, hak akses, dan privasi memerlukan kehadiran integritas data (Surbakti, 2023)**.** Kepercayaan pelanggan terhadap keamanan informasi pribadi mereka dapat ditingkatkan dengan penggunaan teknologi blockchain, yang diintegrasikan ke dalam transaksi.

Untuk menjaga kepercayaan pelanggan terhadap barang dan jasa mereka di era digital modern, bisnis harus mengambil tindakan pencegahan untuk melindungi informasi pribadi pelanggan. Penerapan aplikasi bisnis ke layanan cloud yang dapat diakses publik adalah salah satu pendekatannya. Jika persyaratan perusahaan terhadap layanan cloud terpenuhi dalam hal stabilitas, skalabilitas, ketersediaan, dan keamanan yang kuat, maka layanan ini diakui dapat meningkatkan kepercayaan pelanggan terhadap perlindungan data mereka. Kepercayaan pengguna terhadap layanan komputasi awan berfluktuasi bergantung pada seberapa sering mereka menggunakannya. Kemampuan sistem untuk membujuk pengguna agar menggunakan cloud yang dapat secara efektif menangani risiko keamanan data membuat pelanggan merasa aman dan selaras dengan keinginan dan harapan mereka; Hal ini pada gilirannya dapat menjadi tolak ukur kepercayaan pengguna (Fahrezi et al., 2022).

Bagaimana Mencegah Kebocoran Data?

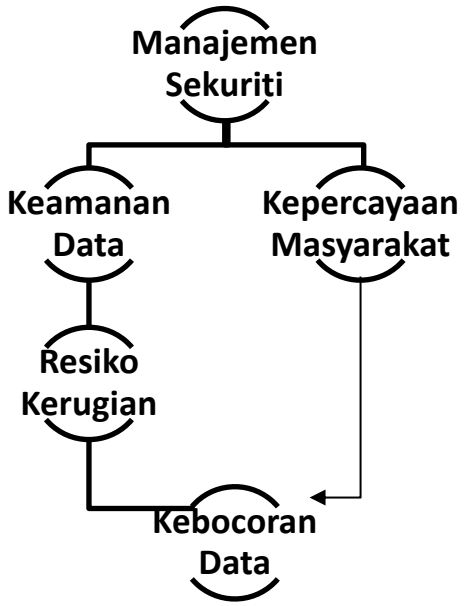
Pelanggaran data kasus tidak dapat dihindari dalam periode globalisasi yang berkembang pesat, kemajuan teknologi yang pesat, dan percepatan yang pesat. Memang kemajuan teknologi dan internet membawa dampak yang signifikan. Namun meskipun hal-hal tertentu memang mempunyai dampak yang baik, namun tidak semuanya demikian. Sebagaimana dimaksud dalam Pasal 27 ayat (1), “Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau menciptakan dapat mengakses Informasi Elektronik dan/atau Dokumen Elektronik yang telah melanggar kesusilaan muatannya.” jelas menunjukkan situasi buruk yang melibatkan pengungkapan data pribadi. (Ferrozi & Putri, 2020). UU ITE yang merupakan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi

dan Transaksi Elektronik memuat ketentuan terkait privasi dan data pribadi. Ketentuan tersebut diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (Zaman et al., 2021)**.** Namun masih banyak celah yang harus diisi dalam hal keamanan sistem, salah satunya adalah perlindungan data pribadi pengguna di dunia maya yang berujung pada pembobolan data di toko online. Meskipun demikian, ketika tersiar kabar bahwa telah terjadi pelanggaran data yang melibatkan konsumen e-commerce, penonton menjadi heboh. Belum adanya peraturan khusus mengenai keamanan data pribadi menjadi salah satu faktor penyebab meningkatnya kasus kebocoran data. Belum sampai disitu, itu sampai saat ini juga. Menemukan bahwa dengan keamanan blockchain, jumlah peretasan dan pelanggaran data pribadi di Indonesia mungkin lebih rendah (Nugroho et al., 2021)**.**

Kebocoran informasi identitas pribadi Meskipun bukan hal yang baru, masalah ini serius dan mengkhawatirkan. Detail keuangan, informasi identifikasi, detail kartu, dan nomor rekening hanyalah sebagian dari informasi identitas pribadi yang terungkap. Sepertinya kebocoran serangan siber, pelanggaran keamanan internal, atau penanganan data yang ceroboh merupakan penyebab potensial. Kebocoran data pribadi di perbankan tidak hanya menempatkan nasabah pada bahaya pencurian identitas, penipuan, dan penyalahgunaan keuangan, namun juga membahayakan kepercayaan nasabah terhadap bisnis dan menyebabkan kerusakan reputasi yang besar. Kebocoran informasi nasabah disebabkan oleh masalah pada elemen pembuktian. Bentuk ganti rugi yang lain antara lain hukuman atas kerugian, ganti rugi atas kerugian nominal, dan penggantian atas kerugian. (Putri et al., 2023) menyatakan bahwa peretas mungkin telah membocorkan data konsumen dari BSI, dan prinsip yang diuraikan dalam makalah tersebut menunjukkan bahwa BSI harus memberikan kompensasi kepada nasabah yang terkena dampak atas kerugian yang mereka alami. Gugatan tersebut berdampak pada kerugian konsumen, sehingga bank harus mengganti kerugian tersebut dalam jumlah besar. sejalan dengan peraturan. keamanan konsumen saat menggunakan layanan keuangan digital menjadi semakin penting seiring dengan pertumbuhan ekonomi digital yang pesat. Untuk memastikan kepercayaan dan keberlanjutan konsumen di era baru ini, penting untuk menetapkan undang-undang dan kebijakan perlindungan yang mendukung keamanan yang efektif.

Jadi tidak, sama sekali tidak ada masalah dalam penggunaan media sosial di Indonesia. Terbukti dari banyaknya kasus penyalahgunaan data pribadi tanpa disadari oleh pemiliknya, kurangnya perlindungan dan kontrol yang ketat dari pihak yang memanfaatkan data tersebut. Dalam hal melindungi data pribadi, penting untuk mendapatkan persetujuan orang tersebut sebelum menggunakan informasinya dalam sistem. Dan jika terjadi kesalahan, penyelenggara sistem elektronik harus menghapus informasi atau dokumen yang salah tersebut. Penyelenggara sistem elektronik harus menerapkan manajemen risiko terhadap potensi kerugian agar tidak terjadi penyalahgunaan data. Manajemen risiko sangatlah penting; tanpa sistem elektronik untuk mencatat, menilai, dan memitigasi potensi bahaya, kerugian finansial tidak dapat dihindari. Instagram dan platform media sosial lainnya menjadikan keamanan sebagai prioritas utama, karena pelanggaran terhadap aturan ini dapat membahayakan kemampuan pengguna untuk berekspresi secara bebas di komunitas online. Hal ini sesuai dengan Pasal 30 Ayat (2) UU ITE yang melarang siapa pun dengan sengaja mengakses suatu sistem secara elektronik tanpa izin atau kedudukan hukum yang sesuai untuk memperoleh informasi atau dokumen. Namun bukan itu saja; harus ada juga pengetahuan masyarakat bahwa ia tidak boleh memberikan akses kepada masyarakat agar mereka dapat melihat seluruh data pribadinya (Fernanda et al., 2021).

Kerangka Konseptual



KESIMPULAN DAN SARAN

Kesimpulan

Menurut penelitian, manajemen keamanan sangat penting dalam melindungi dana digital dari potensi kerugian. Manajemen keamanan adalah serangkaian prosedur yang dapat membantu dalam deteksi, evaluasi, dan pengurangan risiko terhadap dana elektronik perusahaan. permasalahan yang dihadapi saat mencoba mendapatkan pembiayaan digital. Serangan dunia maya, pelanggaran data, dan bentuk kejahatan dunia maya lainnya termasuk dalam kategori ini. Ketika risiko baru atau kemajuan teknologi muncul, manajemen keamanan harus cukup gesit untuk meresponsnya. Pentingnya kemitraan multipihak dalam memitigasi risiko keuangan digital, yang melibatkan bank, pemerintah, regulator, dan institusi akademis. Untuk mengatasi bahaya yang terus berkembang ini, diperlukan pendekatan baru terhadap manajemen keamanan dan teknologi keamanan mutakhir.

Saran

Saran untuk penelitian lebih lanjut Untuk menjaga keuangan digital mereka, organisasi harus membuat rencana keamanan menyeluruh yang membahas deteksi, respons, pemulihan, dan pemantauan insiden. Penggunaan aturan, proses, dan teknologi yang sesuai sangat penting dalam permasalahan ini. Oleh karena itu, penting bagi organisasi untuk menyediakan sumber daya untuk pelatihan dan pengembangan. Keamanan informasi dan kekuatan finansial dengan penekanan pada manusia. Karyawan yang telah mendapatkan pelatihan yang baik akan lebih siap untuk menangani keamanan risiko dengan cara yang efisien. Salah satu cara untuk mengurangi dampak kecerobohan manusia adalah dengan meningkatkan pengetahuan pengguna tentang perlunya praktik keamanan digital yang aman. Dengan mengikuti prosedur ini, organisasi dapat meningkatkan kapasitas mereka untuk menghindari kerugian risiko keuangan digital, menjaga kepercayaan konsumen, dan memastikan integritas keuangan.

DAFTAR PUSTAKA

Adetya Firnanda, Revita Pirena Putri, & Mriya Afifah Furqania. (2021). Kebocoran Data Pribadi Melalui Fitur Stiker di Platform Instagram. *Seminar Nasional Ilmu Teknologi dan Multidisiplin (SEMNASTEKMU)*, *1* (1), 154–159. https://doi.org/10.51903/semnastekmu.v1i1.98

Akbar, A., Kumalasari, AD, Rubiyanti, N., Artadita, S., Hasanah, N., Silvianita, A., Utami, FN, & Saragih, R. (2024). *KEJAHATAN KEUANGAN DIGITAL: CARA & CARA*

ANTISIPASI DALAM RANGKAIAN KEGIATAN PELAYANAN MASYARAKAT ASOSIASI WREDATAMA REPUBLIK INDONESIA (PWRI) KETENTUAN JAWA BARAT . *3* (1), 64–71. https://doi.org/10.37081/adam.v3i1.1750

A kbar, R. (2022). *Analisis Manajemen Risiko Dalam Operasional Usaha Roti Bakar 77* (Disertasi Doktoral, IAIN PONOROGO).

Bukit, AN, dan Rahmi Ayunda. (2022). Urgensi Pengesahan RUU Perlindungan Data Pribadi tentang Perlindungan Kebocoran Data Penerimaan SMS Dana Cepat. *Reformasi Hukum* , *26* (1), 1–20. https://doi.org/10.46257/jrh.v26i1.376

Buntoro Irawan. (2022). Implementasi Teknologi Blockchain untuk Keamanan Data Internet of Things. *Jurnal Ilmiah Multidisiplin Indonesia* , *1* (9), 1278–1285. https://journal.ikopin.ac.id/index.php/humantech/article/view/3387

Dewi Fatmala Putri, Andriani, Widya Ratna Sari, FLN (2023). Analisis Perlindungan Nasabah Bsi Terhadap Kebocoran Data Dalam Penggunaan Digital Banking. *Jurnal Ilmiah Ekonomi dan Manajemen* , *1* (4), 173–181. https://doi.org/10.61722/jiem.v1i4.331

Fachrudin, R., Respaty, E., Adilah, IS, & Sinlae, F. (2024). Peran Penting Manajemen Keamanan di Era Digitalisasi. *Jurnal Ilmu Multidisiplin Nusantara* , *2* (Januari), 94–102. https://www.researchgate.net/publication/377219065_Important_Peranan_Manajemen_Sekuriti_in_Era Digitalisasi

Fahrezi, A., Apriliani, N., Ajijah, N., & Juardi, D. (2022). Keamanan Data dan Transaksi dalam Memanfaatkan Cloud as a Service. *Jurnal Pendidikan dan Konseling* , *4* (4), 5530–5536.

Hanggondosari, SU (2023). *PERAN MANAJEMEN KEUANGAN DIGITAL DALAM PENGELOLAAN KEUANGAN PADA ORGANISASI GEREJA IMANUEL GBT DI KEDIRI* . *1* (35), 35–40.

Kusuma, GHA (2021). Perancangan Skema Sistem Keamanan Jaringan Web Server menggunakan Web Application Firewall dan Fortigate untuk Mencegah Kebocoran Data pada Masa Pandemi Covid-19. *Jurnal Informatika dan Komputasi Tingkat Lanjut (JIAC)* , *2* (2), 1-4.

Leukfeldt, R., & Jansen, J. (2016). Jaringan kriminal dunia maya dan bagal uang: Analisis serangan penipuan berteknologi rendah dan berteknologi tinggi di Belanda. *Jurnal Internasional Kriminologi Cyber* , *9* (2), 173–184. https://doi.org/10.5281/zenodo.56210

Mahardhika, WT, Fauzi, A., Lestin, A., & Supu, A. (2023). Pengaruh Keamanan Dan Kepercayaan Terhadap Keputusan Pembelian Toko Online Di Marketplace Shopee (Studi Literatur Manajemen Keamanan). *Jurnal Ilmu Multidisiplin* , *2* (1), 121–129.

Md Haris Uddin Sharif, & Mehmood Ali Mohammed. (2022). Tinjauan literatur statistik kerugian finansial untuk keamanan siber dan tren masa depan. *Jurnal Penelitian dan Ulasan Lanjutan Dunia* , *15* (1), 138–156. https://doi.org/10.30574/wjarr.2022.15.1.0573

Muhammad Fathur. (2020). Tanggung Jawab Tokopedia atas Kebocoran Data Pribadi Konsumen (Tanggung Jawab Tokopedia atas Kebocoran Data Pribadi Konsumen). *Prosiding: Call for Paper Konferensi Nasional Kajian Hukum ke-2: Perkembangan Hukum Menuju Era Masyarakat Digital* , hal.43. http://jurnal.unissula.ac.id/index.php/PH/article/view/1476

Muhammad Rayhan, Muhammad Dicky Alfaridzi, Ikbal Eka Saputra, F., & Sinlae. (2023). *Penerapan Manajemen Keamanan Dalam Mencegah Penipuan Transaksi Penjualan Online di Forum Jual Beli (Facebook)* . *1* , 166–170.

Musman, S., & Turner, A. (2018). Pendekatan teori permainan terhadap manajemen risiko keamanan siber. *Jurnal Pemodelan dan Simulasi Pertahanan* , *15* (2), 127-146.

Nugroho, II, Pratiwi, R., & Az Zahro, SR (2021). Optimalisasi Pencegahan Kebocoran Data Melalui Regulasi Blockchain untuk Mewujudkan Keamanan Siber di Indonesia.

Jurnal Hukum Ikatan Penulis Mahasiswa Hukum Indonesia , *1* (2), 115–129. https://doi.org/10.15294/ipmhi.v1i2.53698

Ozili, PK (2022). Mata Uang Digital Bank Sentral di Nigeria: Peluang dan Risiko. *Studi Kontemporer dalam Analisis Ekonomi dan Keuangan* , *109A* (110430), 125–133. https://doi.org/10.1108/S1569-37592022000109A008

Puanda, F., & Rahmidani, R. (2021). Pengaruh Kepercayaan dan Keamanan Terhadap Keputusan Pembelian Online Melalui Aplikasi Shopee. *Jurnal Ecogen* , *4* (3), 367. https://doi.org/10.24036/jmpe.v4i3.11507

Putri, DD, & Fahrozi, MH (2020). UPAYA PENCEGAHAN KEBOCORAN DATA KONSUMEN MELALUI PENINGKATAN RUU PERLINDUNGAN DATA PRIBADI (STUDI KASUS BHINNEKA E-COMMERCE.COM) Pencegahan Kebocoran Data Konsumen Melalui Legalisasi RUU Perlindungan Data Pribadi. *Konferensi Nasional Ilmu Hukum*, 978–979. https://tirto.id/nomor-pelanggan-e-commerce-ter tercatat-

Surbakti, M. (2023). Revolusi Teknologi Blockchain: Dampaknya terhadap Keamanan dan Integritas Data. *Catatan Literasi* , *1* (1), 1–9.

Suryawijaya, DUA (2023). Memperkuat Keamanan Data melalui Teknologi Blockchain: Menjajaki Keberhasilan Implementasi Transformasi Digital di Indonesia. *Jurnal Kajian Kebijakan Publik* , *2* (1), 55–68. https://doi.org/10.21787/jskp.2.2023.55-68

Susanto, E., Antira, Lady, Kevin, K., Stanzah, E., & Majid, AA (2023). Manajemen Keamanan Siber di Era Digital. *Jurnal Bisnis Dan Kewirausahaan*, *11* (1), 23. https://doi.org/10.46273/jobe.v11i1.365

Utin Indah Permata Sari. (2022). Kebijakan Penegakan Hukum Dalam Upaya Penanggulangan Kejahatan Siber Yang Dilakukan Oleh Virtual Police Di Indonesia. *Jurnal Studia Legalia* , *2* (01), 58–77. https://doi.org/10.61084/jsl.v2i01.7

Yang, Y., & Yin, Z. (2023). Akuntansi untuk Perusahaan E-Bisnis Berdasarkan Keamanan Cyber. *Jurnal Internasional Pergudangan Data dan Penambangan*, *19* (6), 1–17. https://doi.org/10.4018/IJDWM.320227

Zaman, AA, & Anwar, J. (2021). Tanggung Jawab Pidana Atas Kebocoran Data BPJS Dalam Perspektif UU ITE. *De Juncto Delicti: Jurnal…*, 146–157. https://journal.unsika.ac.id/index.php/djd/article/download/5732/2999