Inovan Publisher

Fibonacci: Jurnal Ilmu Ekonomi, Manajemen dan Keuangan

| ISSN (Online) 3064-5883 |
https://creativecommons.org/licenses/by/4.0/
DOI: 10.63217/fibonacci.v2i1.254

Studi Kasus: Implementasi Sekuriti di Perusahaan

Amelia Nur Shabrina[1], Galuh Sekar Naila[2], Gilang Putri Nuryansyah[3], Regina Amanda[4]
[1]Universitas Bhayangkara Jakarta Raya, Bekasi, Indonesia, amelianshabrina@gmail.com
[2]Universitas Bhayangkara Jakarta Raya, Bekasi, Indonesia, galuhnaila24@gmail.com
[3]Universitas Bhayangkara Jakarta Raya, Bekasi, Indonesia, gilangputtrii@gmail.com
[4]Universitas Bhayangkara Jakarta Raya, Bekasi, Indonesia, reginamanda28@gmail.com

Corresponding Author: amelianshabrina@gmail.com[1]

Abstract: *Digital transformation improves organizational efficiency but also increases exposure to cybersecurity threats, particularly email-based attacks and data breaches. This study aims to examine the implementation of security management through a case study approach, focusing on email attacks in the financial sector, the adoption of Zero Trust Architecture (ZTA) in startup environments, and lessons learned from major data breach cases in Indonesia. A descriptive qualitative method using a literature review was employed. The findings indicate that phishing and Business Email Compromise (BEC) are dominant threats causing financial losses and reputational damage. Implementing integrated security management based on Zero Trust principles enhances digital asset protection through continuous verification, access control, and system monitoring. This study highlights the importance of aligning technical measures, policies, and human resource awareness to ensure organizational sustainability in the digital era.*

Keywords: *Cybersecurity, Security Management, Email Attacks, Zero Trust, Data Breaches*

Abstrak: Transformasi digital meningkatkan efisiensi organisasi, namun juga memperbesar risiko ancaman keamanan siber, khususnya serangan berbasis email dan kebocoran data. Penelitian ini bertujuan mengkaji implementasi manajemen sekuriti di perusahaan melalui studi kasus yang berfokus pada serangan email di sektor keuangan, penerapan *Zero Trust Architecture (ZTA)* di *startup*, serta pembelajaran dari kasus kebocoran data besar di Indonesia. Metode yang digunakan adalah kualitatif deskriptif dengan studi literatur. Hasil kajian menunjukkan bahwa serangan *phishing* dan *Business Email Compromise (BEC)* menjadi ancaman utama yang berdampak pada kerugian finansial dan reputasi organisasi. Penerapan manajemen sekuriti terintegrasi berbasis *Zero Trust* mampu meningkatkan perlindungan aset digital melalui verifikasi berkelanjutan, pengendalian akses, dan pemantauan sistem. Studi ini menegaskan pentingnya sinergi antara aspek teknis, kebijakan, dan kesadaran sumber daya manusia dalam menjaga keberlanjutan organisasi di era digital.

Kata Kunci: Keamanan Siber, Manajemen Sekuriti, Serangan Email, Zero Trust, Kebocoran Data

PENDAHULUAN

Kemajuan teknologi informasi dan komunikasi telah mendorong transformasi digital di berbagai industri, termasuk sektor keuangan, startup teknologi, dan lembaga publik. Meskipun perkembangan ini menawarkan kenyamanan, efisiensi, dan mempercepat proses bisnis, mereka juga menimbulkan tantangan signifikan dalam bentuk ancaman keamanan siber yang meningkat. Akibatnya, hal ini dapat diibaratkan sebagai pedang bermata dua yang memiliki dampak positif dan negatif serta mengubah perilaku manusia. Dunia kini tampak tanpa batas (*borderless*), dengan ruang siber berfungsi sebagai platform untuk komunikasi dan berbagi informasi serta sumber ancaman terhadap kedaulatan negara yang dapat berasal dari individu, korporasi, atau aktor negara dengan agenda tertentu. Karena itu, paradigma keamanan global kini mempertimbangkan risiko non-militer seperti serangan siber selain risiko militer (Setiyawan et al., 2020). Pencurian data, propaganda, provokasi, dan serangan terhadap sistem kritis di berbagai bidang, seperti data keuangan, jaringan militer, dan sistem pertahanan nasional, dapat dilakukan melalui ruang siber. Hal ini dapat mengancam stabilitas pertahanan dan keamanan nasional jika tidak ada pengawasan dan pengelolaan yang memadai (Setiyawan et al., 2020). Serangan berbasis *email*, seperti *phishing*, *Business Email Compromise* (BEC), dan *malware*, merupakan ancaman paling umum di dunia digital bagi organisasi. Dalam serangan ini, *email* yang seharusnya menjadi sarana komunikasi utama justru digunakan sebagai cara untuk merusak sistem internal organisasi. Seperti yang terlihat dari sejumlah kasus kebocoran data berskala besar yang terjadi di Indonesia dan menunjukkan kelemahan keamanan sistem informasi, kegagalan dalam mengelola risiko keamanan *email* dapat mengakibatkan kebocoran data sensitif, kerugian finansial, gangguan operasional, dan kerusakan reputasi institusi.

Organisasi saat ini sangat membutuhkan pengembangan manajemen sekuriti yang terencana dan terintegrasi sebagai respons terhadap situasi ini. Tujuan dari manajemen sekuriti adalah untuk melindungi aset dan data kritis dari berbagai ancaman, termasuk serangan siber, pencurian data, dan pelanggaran sekuritas lainnya. Ini merupakan pendekatan sistematis dalam mengelola ancaman terhadap keamanan informasi dan infrastruktur teknologi informasi. Strategi ini mencakup prosedur untuk mengidentifikasi, mengevaluasi, melindungi, memantau, dan mengelola risiko yang mungkin dihadapi oleh bisnis. (Nursabrina et al., 2024). Untuk memastikan keamanan aset dan informasi, manajemen sekuriti tidak hanya mencakup aspek teknis tetapi juga struktur organisasi, kebijakan, prosedur, dan peningkatan kesadaran sumber daya manusia.

Karena menekankan verifikasi ketat terhadap setiap permintaan akses tanpa secara otomatis memberikan kepercayaan, baik yang berasal dari dalam maupun luar jaringan organisasi, konsep *Zero Trust* dianggap sebagai strategi keamanan yang semakin relevan sejalan dengan meningkatnya ancaman siber yang dinamis dan kompleks. Hal ini memungkinkan adaptasi terhadap lingkungan kerja modern yang fleksibel, berbasis *cloud*, dan kolaboratif. Berbeda dengan model keamanan konvensional, *Zero Trust Architecture* (ZTA) menghilangkan kepercayaan bawaan terhadap perangkat dan pengguna di dalam jaringan, serta menerapkan otentikasi dan otorisasi berkelanjutan untuk setiap permintaan akses. ZTA telah menjadi pendekatan keamanan yang berkembang pesat dalam beberapa tahun terakhir. Masih terdapat kesenjangan penelitian terkait penerapan ZTA pada jaringan komputer berskala besar, terutama dalam hal integrasi ZTA dengan sistem keamanan jaringan yang ada tanpa mengorbankan kinerja jaringan. Beberapa studi menunjukkan bahwa ZTA secara luas digunakan untuk melindungi data berbasis cloud dan mendeteksi ancaman dari dalam secara real-time. Selain itu, meskipun alat simulasi berbasis perangkat lunak seperti GNS3 dan *Cisco Packet Tracer* secara luas digunakan untuk mengevaluasi efektivitas arsitektur keamanan, penelitian tentang simulasi implementasi ZTA dalam menghadapi serangan siber berbagai jenis, seperti *man-in-the-middle* dan *Distributed Denial of Service* (DDoS), masih relatif terbatas. Skenario ini menunjukkan bahwa masih ada kebutuhan besar akan penelitian yang secara khusus mengeksplorasi bagaimana ZTA dapat diimplementasikan dan dimodifikasi dalam sistem jaringan berskala besar untuk melawan berbagai jenis serangan siber. (Kusnanto et al., 2024). Penelitian ini bertujuan untuk mengkaji

implementasi sekuriti di perusahaan melalui pendekatan studi kasus. Pembahasan difokuskan pada analisis serangan *email* di sektor keuangan, penerapan kebijakan *Zero Trust* di lingkungan *startup*, serta pelajaran yang dapat diambil dari kasus kebocoran data berskala besar di Indonesia. Dengan mengintegrasikan perspektif manajerial, teknis, dan kebijakan, esai ini diharapkan mampu memberikan pemahaman komprehensif mengenai pentingnya sistem keamanan informasi yang efektif sebagai fondasi keberlanjutan organisasi di era transformasi digital.

METODE

Penelitian ini menggunakan pendekatan kualitatif deskriptif dengan metode studi literatur. Data yang digunakan dalam penelitian ini merupakan data sekunder dengan rentang tahun 2015 - sekarang yang diperoleh dari berbagai sumber tertulis, seperti artikel jurnal ilmiah, buku referensi, laporan penelitian, dan dokumen daring yang berkaitan dengan topik keamanan siber. Penelusuran literatur difokuskan pada publikasi yang membahas keamanan email, kebocoran data, manajemen sekuriti, serta kebijakan zero trust, dengan sumber utama berasal dari Google Scholar karena kemudahan akses referensinya. Hasil penelitian menggambarkan strategi keamanan siber dalam lingkup perusahaan khususnya disektor keuangan.

HASIL DAN PEMBAHASAN

Analisis Kasus: Serangan Email di Sektor Keuangan

Di lingkup yang serba digital seperti sekarang ini, sektor keuangan sangat rentan terhadap serangan siber yang sering memanfaatkan platform email. Data melalui Badan Siber dan Sandi Negara (BSSN) menyebutkan bahwa sektor keuangan terutama perbankan merupakan yang paling rentan diserang oleh ancaman siber, beberapa ancaman siber yang paling umum meliputi *phishing* dan *ransomware*. Menurut Afifah et. al., (2025) dalam penelitiannya mengidentifikasi bahwa sektor perbankan di era digital menghadapi berbagai ancaman siber seperti *malware, phishing, ransomware,* dan serangan DDoS. Dilansir melalui artikel *CloudFlare* 2025 mengenai *"What is a DDoS attack?"* menjelaskan bahwa DDoS merupakan serangan siber yang dilakukan dengan membanjiri server, situs web, atau jaringan dengan begitu banyak permintaan dari berbagai sumber sekaligus, akibatnya sistem menjadi kewalahan, layanan normal terganggu, dan pengguna yang seharusnya bisa mengaksesnya justru tidak bisa masuk sama sekali. Gambaran kerentanan tersebut sudah pernah terjadi secara nyata di Indonesia, salah satunya pada 2024 ketika banyak berita lokal yang melansir berita mengenai terjadinya kebocoran data 6 juta wajib pajak, data yang bocor diantaranya NIK, NPWP, alamat, nomor handphone, email, dll. Kejadian tersebut menegaskan betapa pentingnya pengamanan yang memadai terhadap informasi finansial perusahaan.

Salah satu serangan yang paling sering dijumpai adalah metode serangan *phishing* melalui email. Menurut Satrya (2024) menjelaskan bahwa serangan *phishing* biasanya dilakukan dengan mengarahkan korban ke alamat situs web palsu yang tampilannya persis menyerupai situs asli. Tujuan utama dari serangan ini adalah mencuri informasi sensitive, seperti nama pengguna *(username)* dan kata sandi milik korban. Dengan cara ini penipu dapat menipu pengguna agar memasukkan data pribadi mereka ke situs palsu yang dikendalikan oleh penipu. Akses informasi yang berhasil dicuri kemudian digunakan untuk menyusup ke rekening nasabah atau sistem perusahaan tanpa terdeteksi. Korban yang biasanya terkena serangan *phishing* adalah kelompok orang tua atau orang – orang yang tidak begitu mengerti tentang media sosial, penipu biasanya mengiming – imingi korban dengan berbagai kata – kata manis agar mereka mudah percaya begitu saja. Menurut Satrya (2024) dalam penelitian "Serangan Siber dalam Perkembangan Perbankan Digital di Indonesia" ada ancaman lain yang terkait dengan email yaitu *Business Email Compromise* (BEC). BEC merupakan bentuk rekayasa sosial *(social engineering)* yang mengeksploitasi celah keamanan pada email bisnis. Dalam serangan BEC, penipu biasanya berhasil menguasai akun email resmi perusahaan atau pribadi lalu mengirimkan instruksi pembayaran palsu yang tampak sah kepada korban. Sebagai contoh, penipu dapat berpura –

pura menjadi eksekutif perusahaan dan meminta bendahara melakukan transfer dana ke rekening tertentu, karena email tersebut datang dari akun yang seolah – olah terpercaya maka penipuan seperti ini sering lolos deteksi dan menyebabkan kerugian finansial yang besar.

Dampak dari serangan email di sektor keuangan tentunya sangatlah merugikan pihak korban. Satrya (2024) menjelaskan bahwa kerugian langsung yang timbul meliputi hilangnya asset perusahaan atau kewajiban membayar ganti rugi kepada nasabah, sedangkan kerugian tidak langsung berupa menurunnya kepercayaan publik dan efisiensi operasional yang berkurang. Kejadian kebocoran 6 juta data wajib pajak tersebut menggambarkan potensi kerugian finansial dan reputasi yang sulit diukur ketika data keuangan bocor. Kerusakan semacam ini tidak hanya berdampak pada satu lemabaga tetapi dapat menghancurkan kepercayaan sistem keuangan secara keseluruhan.

Untuk mengantisipasi serangan – serangan tersebut diperlukan penerapan manajemen sekuriti yang mendalam dan terstruktur. Dalam penelitian Susanto et. al., (2023) menyebutkan bahwa manajemen sekuriti adalah sistem terpadu yang dirancang untuk merencanakan dan merancang pengamanan yang tepat, efektif, dan efisien sehingga dapat mencegah kerugian secepat mungkin. Ini mencakup struktur organisasi, prosedur dan sumber daya yang dibutuhkan untuk melindungi asset serta informasi perusahaan. Beberapa langkah nyata yang dapat diimplementasikan misalnya pengendalian akses yang ketat, enkripsi data pada penyimpanan dan saat transmisi, melakukan pencadangan data *(backup)* dan pemulihan data, serta pemantauan aktivitas jaringan secara berkala. Penerapan langkah – langkah ini diharapkan dapat memperkuat kerahasiaan, integritas, serta memitigasi risiko yang disebabkan oleh serangan email berbahaya.

Implementasi Kebijakan *Zero Trust* di *Startup*

Implementasi kebijakan zero trust dilingkungan startup merupakan langkah strategis untuk memperkuat keamanan digital di tengah pertumbuhan organisasi yang cepat dan dinamis. Zero trust mempunyai prinsip bahwa tidak ada pengguna, perangkat, maupun aplikasi yang secara otomatis dapat dipercaya, baik yang berada di dalam maupun luar jaringan perusahaan. Bagi startup yang umumnya meengandalkan infrastruktur berbasis cloud dan sistem kerja fleksibel, model ini membantu meminimalkan risiko celah keamanan akibat akses yang terlalu longgar. Penerapan zero trust mendorong perusahaan untuk melakukan verifikasi identitas secara ketat, menetapkan batasan akses yang sesuai peran, serta mengelola seluruh aktivitas digital dengan pendekatan "trust no one, verify everything" sehingga setiap permintaan akses diuji terlebih dahulu sebelum diberi izin.

Dalam praktiknya penerapan zero trust di startup membutuhkan desain arsitektur keamanan yang terintregrasi dan konsisten. Proses ini mencakup penggunaan autentikasi multifaktor, manajemen identitas dan akses, segmentasi jaringan, serta pemantauan aktivitas secara real time. Startup perlu memastikan bahwa setiap aset digital, baik itu akun internal, aplikasi perusahaan, maupun data konsumen, terlindungi melalui kontrol akses berbasis kebijakan yang ketat. Selain itu juga startup harus memiliki mekanisme pemantauan ancaman yang mampu mendeteksi aktivitas mencurigakan sejak dini, mengingat potensi serangan siber yang semakin kompleks. Penggunaan ssumber daya dapat diatur secara lebih terukur dan keamanan menjadi lebih adaptif terhadap perubahan kondisi operasional.

Penerapan kebijakan zero trust juga menuntut perubahan budaya kerja di startup, khususnya dalam membangun kesadaran keamanan di seluruh tingkat organisasi. Karyawan perlu memahami bahwa prosedur verifikasi tambahan bukanlah hambatan, melainkan bagian dari perlindungan jangka panjang terhadap data dan sistem yang digunakan setiap hari. Manajemen juga harus memastikan bahwa pelaksanaan zero trust tidak hanya berfokus pada aspek teknis, tetapi selaras dengan proses bisnis, kebutuhan operasional, dan keberlanjutan pertumbuhan perusahaan. Dengan mengintegrasikan zero trust secara bertahap dan menyesuaikannya dengan karakteristik startup yang cenderung agile, organisasi dapat menciptakan ekosistem digital yang lebih aman, tangguh, dan siap menghadapi berbagai ancaman di era transformasi teknologi.

Menurut Mukhlisin dan Firmansyah (2025), konsep zero trust architecture dipahami sebagai pendekatan keamanan yang menekankan verifikasi menyeluruh terhadap setiap akses serta pengawasan ketat terhadap seluruh aktivitas digital, sehingga mampu meningkatkan perlindungan data dan privasi dalam lingkungan teknologi yang kompleks seperti institusi pendidikan. Mereka menegaskan bahwa model ini efektif karena tidak memberikan kepercayaan otomatis kepada pengguna maupun perangkat, sehingga risiko kebocoran data dapat diminimalkan. Pemikiran tersebut sejalan dengan kebutuhan startup untuk membangun sistem keamanan yang adaptif seperti yang telah dijelaskan dalam tiga paragraf sebelumnya. Jika di institusi pendidikan zero trust digunakan untuk melindungi data sensitif dan aktivitas akademik pada startup pendekatan ini memiliki peran serupa dalam menjaga kerahasiaan aset digital dan mencegah akses tidak sah di tengah lingkungan kerja yang cepat berubah. Implementasi verifikasi berlapis, pembatasan akses berbasis peran, serta pemantauan real-time bukan hanya relevan bagi organisasi besar, tetapi juga menjadi kebutuhan mendesak bagi startup yang mengandalkan teknologi cloud dan kolaborasi digital. Dengan mengadopsi prinsip yang sama, startup dapat membangun fondasi keamanan yang lebih kuat dan berkelanjutan.

Pelajaran dari Kasus Kebocoran Data Besar

Kebocoran data dalam skala besar merupakan ancaman serius yang mengintai berbagai sektor. Dampaknya meliputi kerugian finansial yang signifikan, penurunan reputasi, serta erosi kepercayaan publik. Sebagai contoh, kasus kebocoran data BPJS Kesehatan pada tahun 2021 yang melibatkan kurang lebih 279 juta data penduduk menjadi pelajaran pahit bagi keamanan data nasional. Insiden ini menggarisbawahi betapa rentannya privasi digital masyarakat. Selain itu, serangan ransomware terhadap Pusat Data Nasional (PDN) pada tahun 2024 semakin mempertegas urgensi sistem keamanan informasi yang solid dalam melindungi data-data sensitif. Belajar dari kasus-kasus tersebut, dapat disimpulkan bahwa penerapan manajemen risiko dan protokol keamanan yang ketat adalah sebuah keharusan untuk mencegah dampak yang lebih parah dari kebocoran data. Pendekatan keamanan yang komprehensif, termasuk audit berkala, peningkatan kesadaran staf, serta kolaborasi dengan berbagai pemangku kepentingan seperti regulator dan lembaga penegak hukum, menjadi rekomendasi krusial dalam upaya menjaga keamanan data secara menyeluruh.

Pada bulan Mei 2021, terungkap sebuah insiden kebocoran data BPJS Kesehatan yang sangat masif. Pada penelitian Sorisa et al. 2024 melaporkan bahwa lebih dari 279 juta data peserta bocor dan diperjualbelikan secara daring. Menurut Kementerian Pendayagunaan Aparatur Negara dan Reformasi Birokrasi (PANRB) (2021), data yang bocor mencakup informasi sensitif seperti NIK, nama lengkap, alamat, nomor telepon, NPWP, besaran gaji, hingga catatan kesehatan peserta. Kebocoran ini diduga kuat disebabkan oleh adanya celah keamanan dalam sistem TI. Menurut Alfons Tanujaya, Pengamat Keamanan Siber dari Vaksincom, menyoroti penggunaan perangkat lunak yang sudah usang dan akses jarak jauh yang kurang terlindungi sebagai titik masuk utama bagi pelaku kejahatan (Buletin APJII, 2021). Analisis dari sudut pandang akademik juga mengindikasikan bahwa faktor-faktor seperti infrastruktur TI yang kedaluwarsa dan tata kelola data yang kurang memadai turut berkontribusi terhadap terjadinya insiden ini (Munandar et al., 2025). Ali Ghufron Mukti, Direktur Utama BPJS Kesehatan, mengklaim telah menerapkan standar keamanan bersertifikasi *International Organization for Standardization (ISO) 27001* dan *Security Operation Center (SOC) 24/7* (Kompas.com, 2021). Kejadian ini justru mengindikasikan bahwa kontrol keamanan dan manajemen risiko yang ada masih belum berjalan efektif (Munandar et al., 2025).

Dari sisi teknis, upaya penguatan kontrol akses, enkripsi data, dan penerapan autentikasi multi-faktor secara ketat menjadi sebuah keharusan dalam rangka melindungi informasi sensitif . Pembaruan perangkat lunak secara rutin *(patching)* juga harus diprioritaskan untuk menutup celah keamanan yang mungkin ada. Selain itu, pemantauan log sistem secara berkala menjadi penting untuk mendeteksi aktivitas yang mencurigakan. Tidak kalah penting, pelatihan dan sosialisasi mengenai keamanan siber secara rutin diperlukan untuk meningkatkan kesadaran seluruh karyawan. Dari sisi manajerial, Sorisa et al. (2024) menyoroti bahwa insiden BPJS

Kesehatan tahun 2021 mengungkap adanya kesenjangan dalam tata kelola keamanan siber serta implementasi regulasi perlindungan data. Kasus ini semakin menegaskan perlunya kepemimpinan TI yang proaktif, tata kelola data yang transparan dan akuntabel, kepatuhan terhadap Undang-Undang Perlindungan Data Pribadi, serta pembentukan budaya organisasi yang menanamkan kesadaran akan pentingnya keamanan informasi.

Dampak sosial dan ekonomi yang ditimbulkan oleh kebocoran data BPJS Kesehatan pada tahun 2021 di Indonesia sangatlah luas. Dari sisi sosial, terungkapnya informasi pribadi jutaan warga negara telah menciptakan ketidakamanan digital dan membuka celah bagi tindakan penyalahgunaan data, seperti pencurian identitas dan penipuan finansial. Sorisa et al. (2024) berpendapat bahwa insiden ini memberikan dampak yang signifikan terhadap kepercayaan publik yang pada akhirnya memengaruhi kepercayaan masyarakat terhadap institusi negara. Dari sisi ekonomi, konsekuensi yang timbul mencakup potensi kerugian finansial yang tidak sedikit. Laporan dari *Indonesia Cyber Independent Resilience Team (CISRT)* memperkirakan bahwa kerugian materil yang terjadi mencapai sekitar Rp600 triliun (Katadata.co.id, 2021). Data dari *International Business Machines (IBM) Security* tahun 2021 melaporkan bahwa biaya rata-rata yang harus ditanggung akibat kebocoran data secara global mencapai USD 4,35 juta per insiden, termasuk biaya pemulihan sistem, kompensasi bagi korban, serta kerugian akibat penurunan reputasi (Tannavaro & Wiraguna, 2025). Selain itu, lembaga-lembaga terkait juga harus menanggung biaya untuk memulihkan sistem serta melakukan investasi ulang pada infrastruktur TI dengan tujuan memperkuat keamanan siber (Sorisa et al., 2024).

Berdasarkan pada berbagai kasus kebocoran data yang terjadi, seperti contohnya kasus kebocoran data BPJS Kesehatan pada tahun 2021, Indonesia perlu mengambil langkah-langkah strategis untuk memperkuat kebijakan keamanan TI serta meningkatkan kesiapan nasional dalam menghadapi ancaman siber. Pemerintah, sebagai contoh, tengah menyusun Rancangan Undang-Undang (RUU) Keamanan dan Ketahanan Siber 2025 yang bertujuan untuk mengisi kekosongan regulasi sekaligus memperkuat koordinasi antar berbagai lembaga terkait. Undang-Undang Perlindungan Data Pribadi (UU PDP) Nomor 27 tahun 2022 yang telah berlaku penuh sejak Oktober 2024, wajib diimplementasikan secara konsisten, termasuk penerapan sanksi yang tegas bagi para pelanggar (Antara News, 2024). Institusi publik maupun swasta perlu didorong untuk meninjau ulang Standar Operasional Prosedur (SOP) serta kebijakan internal yang berlaku agar selaras dengan ketentuan yang diatur dalam UU PDP. Wakil Menteri Komunikasi dan Informatika (Wamen Kominfo) menekankan bahwa penegakan UU PDP yang kolaboratif dengan melibatkan kolaborasi lintas sektor merupakan kunci utama dalam meningkatkan kepercayaan publik serta daya saing digital bangsa (Kementerian Komunikasi dan Digital Republik Indonesia (KOMDIGI), 2025). Selain itu, peningkatan kapabilitas digital nasional juga harus terus dilakukan melalui upaya modernisasi infrastruktur keamanan siber serta penyelenggaraan program literasi digital dan pelatihan Sumber Daya Manusia (SDM).

Tabel 1. Penelitian Terdahulu

Judul	Identitas	Metode Penelitian	Persamaan	Perbedaan
Manajemen Sekuriti pada Perusahaan Samsung Electronics Indonesia	Susanto, E., Ramhadan, H., Ardiansyah, I., & Maulan, R. (2023). Manajemen Sekuriti pada Perusahaan Samsung Electronics Indonesia. Jurnal Ilmiah Wahana Pendidikan, 9(12), 166–175.	Metode yang digunakan yaitu studi kasus untuk menjelaskan penerapan kebijakan sekuriti di Samsung.	Persamaan dengan artikel ini yaitu keduanya sama – sama menekankan pentingnya pengelolaan keamanan informasi dan asset perusahaan.	Perbedaannya terletak pada fokus studi kasus perusahaan elektronik besar (Samsung) dan penyajian artikel secara naratif, berbeda dengan konteks dan metode yang digunakan dalam penelitian ini.

Serangan Siber dalam Perkembangan Perbankan Digital di Indonesia.	Satrya, I. Z. (2024). Serangan Siber dalam Perkembangan Perbankan Digital di Indonesia. Syntax Literate: Jurnal Ilmiah Indonesia, 9(10).	Metode yang digunakan merupakan tinjauan literature untuk mengidentifikasi perkembangan perbankan digital dan ancaman siber yang muncul.	Persamaan kedua artikel ini berkaitan dengan keamanan siber di sektor perbankan digital di Indonesia, serta metode yang digunakan sama yaitu menggunakan metode kualitatif deskriptif dengan pendekatan studi literature.	Perbedaan kedua artikel ini terletak pada fokus penelitian. Artikel ini sangat condong dengan perkembangan perbankan digital di Indonesia secara umum, sedangkan artikel peneliti lebih fokus menjelaskan implementasi dari studi kasus yang diambil.
Keamanan Siber dalam Perbankan serta Tantangan dan Solusi di Era Digital.	Afifah, E. F. N., Simatangkir, D. W. E., & Faliha, N. S. (2025). Keamanan Siber dalam Perbankan Serta Tantangan dan Solusi di Era Digital. Jurnal Multidisiplin Ilmu Akademik, 2(1), 33–42.	Metode yang digunakan dalam artikel ini merupakan metode kualitatif dengan kajian pustaka untuk mengidentifikasi tantangan dan solusi keamanan siber pada sektor perbankan.	Kedua artikel sama – sama membahas ancaman siber yang terjadi seperti *malware, phishing, ransomware,* DDoS, serta strategi perlindungan di dunia perbankan.	Perbedaannya yaitu artikel ini lebih menekankan solusi teknologi terkini seperti AI dan *blockchain*, serta edukasi untuk perbankan, sedangkan artikel peneliti lebih berfokus pada aspek manajemen atau sistem keamanan siber melalui email pada perusahaan.
Analisis Tingkat Keamanan Data pada Salah Satu Kantor Perpajakan di Bekasi yang Rentan terhadap Serangan Cyber dalam Sistem Keuangan.	Septian, A., Alfiansyah, T., Abdulla, A. D., Sutiawan, H., Fauzi, D. A. E., Saputra, D. H., & Saepudin, T. H. (2024). Analisis tingkat keamanan data pada salah satu kantor perpajakan di Bekasi yang rentan terhadap serangan cyber dalam sistem keuangan. Humanitis: Jurnal Humaniora, Sosial dan Bisnis, 2(7), 711–718.	Metode kualitatif dengan kajian literature yang menkaji sistem keamanan informasi di kantor pajak.	Persamaan kedua artikel terletak pada pembahasan mengenai pentingnya keamanan data dalam sistem keuangan dan pengelolaan risiko siber pada lembaga, serta keduanya menggunakan metode penelitian yang sama.	Perbedaannya terletak pada fokus penelitian, artikel ini lebih menekankan fokusnya pada studi kasus tertentu yaitu di Bekasi, sedangkan artikel peneliti menekankan studi kasus di lingkup yang lebih luas.
Penerapan Manajemen	Erniyanti, A., Soesanto, E., Putri, K.	Studi literature yang digunakan	Kedua artikel sama – sama mengkaji	Perbedaannya terletak pada

Sekuriti dengan Standar Komponen dan K3 di PT. Pertamina Hulu Rokan.	A., & Rahma, F. D. (2024). Penerapan Manajemen Sekuriti dengan Standar, Komponen, dan K3 di PT. Pertamina Hulu Rokan. Jurnal Ekonomi dan Bisnis, 2(1), 143–151.	sebagai metode penelitian.	tata Kelola keamanan manajemen sekuriti di perusahaan besar Indonesia.	fokus penelitian. Artikel ini menyoroti aspek K3 (keselamatan dan kesehatan kerja) yang terintegrasi dalam manajemen sekuriti di Pertamina Hulu Rokan, sedangkan artikel peneliti lebih berfokus pada aspek manajemen atau sistem keamanan siber melalui email pada perusahaan.
Zero Trust Architecture: Solusi Keamanan dan Privasi Untuk Institusi Pendidikan, Systematic Literature Review	Mukhlisin, M., & Firmansyah, R. A. (2025). ZERO TRUST ARCHITECTURE: SOLUSI KEAMANAN DAN PRIVASI UNTUK INSTITUSI PENDIDIKAN, SYSTEMATIC LITERATURE REVIEW. JATI (Jurnal Mahasiswa Teknik Informatika), 9(4), 6926-6935.	Sistematik literature review	Memiliki persamaan dalam hal sama-sama membahas topik keamanan informasi serta bertujuan memberikan pemahaman tentang bagaimana sebuah sistem keamanan dapat diterapkan secara efektif.	Meninjau zero trust architecture dalam konteks institusi pendidikan, sehingga analisisnya lebih menyoroti kebutuhan, tantangan, serta manfaat zero trust pada lingkungan akademik.
Implementasi Zero Trust Arsitektur Pada Jaringan Hybrid Work	Rakhmadi Rahman, R. R., Faiz Ilyas, M. F. I., & Syawal, M. S. (2025). Implementasi Zero Trust Arsitektur Pada Jaringan Hybrid Work. Journal of System & Technology (SYSTEC), 1(1), 14-19	Implementasi dan evaluasi sistem	Sama-sama membahas topik zero trust architecture (ZTA) dan bagaimana konsep ini dapat diterapkan untuk meningkatkan keamanan jaringan.	Penelitian ini menggunakan data primer melalui implementasi langsung di jaringan hybrid-work.
Penerapan Zero Trust Network Access (ZTNA) dengan penggunaan CAPTCHA pada website umum.	Rahman, A. F., & Rahman, R. (2024). Penerapan Zero Trust Network Access (ZTNA) dengan penggunaan CAPTCHA pada website umum. Technology Sciences Insights Journal, 1(2), 71-75.	Empiris / Implementatif	Sama-sama berfokus pada topik keamanan siber, khususnya penerapan prinsip dari model Zero Trust Network Access (ZTNA) atau model serupa.	Artikel ini menggunakan data / konteks nyata (implementasi di website umum), sedangkan pada penelitian kami menggunakan literatur review hanya mengandalkan

				data dari publikasi/jurnal terdahulu
Tantangan dan Strategi Investasi pada Perusahaan Startup Teknologi di Indonesia.	Hakim, L. (2024). Tantangan dan Strategi Investasi pada Perusahaan Startup Teknologi di Indonesia. PRODUCTIVITY: JOURNAL OF INTEGRATED BUSINESS, MANAGEMENT, AND ACCOUNTING RESEARCH: Lembaga Intelektual Muda Maluku, 1(2), 75-84.	Kualitatif	Sama-sama membahas aspek startup (startup teknologi) dan tantangan/peluang di sektor tersebut sehingga topiknya relevan dengan studi tentang startup.	Penelitian Hakim (2024) menggunakan metode deskriptif kualitatif dengan data primer melalui wawancara dan data sekunder dari laporan industri, sehingga hasilnya lebih menggambarkan kondisi nyata investasi startup di Indonesia.
Zero Trust Architecture in Cloud Networks: Application, Challenges and Future Opportunities.	Ahmadi, S. (2024). Zero Trust Architecture in Cloud Networks: Application, Challenges and Future Opportunities. Journal of Engineering Research and Reports, 26(2), 215–228.	Kualitatif	Sama-sama menggunakan literatur sebagai sumber utama tidak melakukan eksperimen atau implementasi langsung.	Penelitian ini tidak melakukan penerapan langsung zero trust architecture, sehingga tidak menghasilkan data teknis seperti hasil uji performa, angka keamanan, atau evaluasi real di lapangan.
Etika Keamanan Siber: Studi Kasus Kebocoran Data BPJS Kesehatan di Indonesia	Sorisa, C. (2024). Etika keamanan siber: Studi kasus kebocoran data BPJS Kesehatan di Indonesia. Jurnal Sains Student Research, 2(6), 586–593.	Penelitian ini menggunakan metode studi kepustakaan untuk menghimpun data dan informasi dari berbagai literatur yang berkaitan dengan etika keamanan siber, khususnya pada kasus kebocoran data BPJS Kesehatan di Indonesia.	Kedua artikel menyoroti bahwa kebocoran data merupakan ancaman besar yang memengaruhi privasi masyarakat, kepercayaan publik, dan keamanan nasional. Serta, kedua artikel tersebut sama-sama menekankan pentingnya implementasi UU PDP secara kuat dan konsisten untuk melindungi data masyarakat.	Perbedaan terletak pada fokus penelitian, pada artikel ini lebih banyak membahas aspek etika, seperti tanggung jawab moral, prinsip keadilan, otonomi, integritas, utilitarianisme, dan deontologi. Sedangkan artikel peneliti lebih menekankan pada kebijakan nasional, regulasi, serta strategi keamanan siber

				berbasis manajemen risiko.
Kebocoran Data BPJS sebagai Studi Kasus Kelemahan Keamanan Lembaga Publik	Munandar, A., Listiani, D., Malik, F. A., Pratama, B. A., & Augustia, A. E. (2025). Kebocoran Data BPJS sebagai Studi Kasus Kelemahan Keamanan Lembaga Publik. TEKNOBIS : Jurnal Teknologi, Bisnis Dan Pendidikan, 3(2), 302–305.	Penelitian ini menggunakan metode kualitatif dengan pendekatan studi kasus intrinsik, yang memungkinkan peneliti menggali secara menyeluruh kasus kebocoran data BPJS Kesehatan. Pendekatan ini dipilih karena mampu menangkap dinamika, konteks, serta makna yang muncul di balik fenomena sosial-teknis tersebut, sehingga analisis yang dihasilkan lebih utuh dan mendalam.	Keduanya sama-sama melihat kebocoran data sebagai ancaman serius yang berdampak luas, terutama pada rusaknya reputasi, kerugian finansial, serta turunnya kepercayaan publik. Baik artikel ini maupun peneliti, menekankan pentingnya manajemen risiko, penguatan keamanan sistem, serta perlunya regulasi yang lebih kuat untuk melindungi data pribadi.	Artikel ini lebih bersifat spesifik dan teknis, berfokus pada kasus BPJS Kesehatan sebagai contoh kegagalan sistemik yang melibatkan infrastruktur, tata kelola data, regulasi lemah, dan kurangnya kompetensi SDM. Artikel ini juga memberikan rekomendasi yang lebih mendetail, seperti migrasi dari *legacy systems*, penerapan *least privilege*, audit independen, dan pelatihan keamanan siber yang berkelanjutan.
Strategi Komunikasi Humas dalam Krisis Siber: Studi Kasus BPJS Kesehatan dan Bank Syariah Indonesia	Tannavaro, D. M., & Wiraguna, S. A. (2025). STRATEGI KOMUNIKASI HUMAS DALAM KRISIS SIBER: STUDI KASUS BPJS KESEHATAN DAN BANK SYARIAH INDONESIA. Kohesi: Jurnal Sains Dan Teknologi, 7(11), 71-80.	Penelitian ini menggunakan pendekatan kualitatif dengan metode studi pustaka dan analisis kasus.	Keduanya sama-sama menyoroti bahwa kebocoran data merupakan ancaman serius yang dapat merusak reputasi dan menurunkan kepercayaan publik.	Artikel ini lebih berfokus pada peran humas, bukan kebijakan teknis. Pada artikel ini, menekankan bagaimana strategi komunikasi, khususnya strategi *rebuild* dalam *Situational Crisis Communication Theory* (SCCT), mempengaruhi persepsi publik dan pemulihan reputasi setelah krisis.
Urgensi Realisasi Pengaturan	Damarga, M. I., Alhidayah, M., Faiqy, M. R., & Maulana, J.	Penelitian ini menggunakan pendekatan	Kedua artikel sama-sama menyoroti bahwa kebocoran	Artikel ini berfokus pada sektor kesehatan

Data Protection Officer (DPO) pada Sektor Kesehatan Ditinjau dari Hukum Pelindungan Data Pribadi	(2022). Urgensi Realisasi Pengaturan Data Protection Officer (DPO) pada Sektor Kesehatan Ditinjau dari Hukum Pelindungan Data Pribadi. Padjajaran Law Review, 10(1), 142-156.	deskriptif dengan metode yuridis normatif, yakni menelaah persoalan hukum melalui studi kepustakaan dan data sekunder.	data adalah ancaman serius yang memengaruhi kepercayaan publik, reputasi institusi, dan keamanan nasional. Keduanya juga menegaskan perlunya regulasi yang kuat, pengawasan ketat, serta sistem perlindungan data yang lebih terstruktur.	dan kelemahan regulasi perlindungan data pribadi yang masih terpecah. Artikel tersebut juga menyoroti secara khusus pentingnya peran DPO sebagai solusi, serta kebutuhan mendesak untuk mengesahkan RUU PDP atau menerbitkan aturan khusus tentang DPO.
Analisis Keamanan Data Pribadi pada Pengguna BPJS Kesehatan: Ancaman, Risiko, Strategi Keamanan (*Literature Review*)	Silvia, A. F., Saputra, W. Sunaryo, H., & Sinlae, F. (2024). Analisis Keamanan Data Pribadi pada Pengguna BPJS Kesehatan: Ancaman, Risiko, Strategi Keamanan (*Literature Review*). Nusantara Journal of Multidisciplinary Science, 2(1), 201-207.	Penelitian ini menggunakan metode penelitian kualitatif dan metode penelitian kepustakaan.	Kedua artikel memiliki banyak irisan, terutama dalam menyoroti bahwa kebocoran data merupakan ancaman serius yang berdampak pada kerugian finansial, hilangnya kepercayaan publik, serta risiko penyalahgunaan informasi pribadi. Keduanya sama-sama menekankan pentingnya keamanan data yang lebih kuat dan perlunya tanggung jawab penuh dari setiap institusi dalam melindungi privasi penggunanya. Peran pemerintah juga menjadi titik temu, karena melalui dua artikel, terlihat bahwa negara harus hadir melalui pengawasan dan inisiatif peningkatan perlindungan data.	Pada artikel ini berfokus khusus pada kasus BPJS Kesehatan dan bagaimana instansi tersebut semestinya merespons kebocoran data, termasuk perlunya peningkatan investasi keamanan serta tanggung jawab moral dan institusional terhadap privasi pengguna. Artikel ini juga memberi ruang lebih besar pada dampak sosial dan psikologis, seperti kekhawatiran masyarakat dan risiko pencurian identitas, yang tidak banyak muncul dalam artikel peneliti. Sementara itu, pada artikel peneliti bersifat makro, membahas kebutuhan nasional seperti

		penguatan kebijakan TI, penegakan UU PDP, penyusunan RUU Keamanan Siber, kolaborasi lintas sektor, dan modernisasi infrastruktur digital. Pendekatannya sistemik dan strategis, mencakup pemerintah, lembaga hukum, hingga sektor swasta.

KESIMPULAN

Berdasarkan hasil kajian yang telah dilakukan, dapat disimpulkan bahwa peningkatan transformasi digital di berbagai sektor, khususnya sektor keuangan, *startup* teknologi, dan lembaga publik, secara signifikan meningkatkan risiko ancaman keamanan siber. Serangan berbasis email seperti *phishing* dan *Business Email Compromise (BEC)* terbukti menjadi ancaman utama yang berpotensi menimbulkan kerugian finansial, gangguan operasional, serta penurunan kepercayaan publik terhadap organisasi.

Penerapan manajemen sekuriti yang terencana dan terintegrasi merupakan langkah strategis dalam memitigasi risiko tersebut. Pendekatan *Zero Trust Architecture (ZTA)* menunjukkan relevansi yang tinggi, terutama dalam lingkungan kerja modern yang fleksibel dan berbasis *cloud*, karena menekankan prinsip verifikasi berkelanjutan, pengendalian akses berbasis peran, serta pemantauan aktivitas sistem secara *real-time*. Implementasi *ZTA* tidak hanya memperkuat aspek teknis keamanan, tetapi juga mendorong disiplin dan kesadaran keamanan di tingkat organisasi.

Selain aspek teknis, studi ini menegaskan bahwa efektivitas sistem keamanan informasi sangat bergantung pada tata kelola yang baik, kebijakan yang jelas, serta peningkatan kesadaran sumber daya manusia. Pembelajaran dari berbagai kasus kebocoran data besar di Indonesia menunjukkan bahwa lemahnya manajemen risiko dan pengawasan dapat berdampak luas secara sosial dan ekonomi. Oleh karena itu, sinergi antara teknologi, kebijakan, dan budaya keamanan organisasi menjadi kunci utama dalam membangun sistem keamanan informasi yang berkelanjutan di era transformasi digital.

REFERENSI

Afifah, E. F. N., Simatangkir, D. W. E., & Faliha, N. S. (2025). Keamanan siber dalam perbankan serta tantangan dan solusi di era digital. *Jurnal Multidisiplin Ilmu Akademik, 2*(1), 33–42. https://doi.org/10.61722/jmia.v2i1.3119

Ahmadi, S. (2024). Zero Trust Architecture in Cloud Networks: Application, Challenges and Future Opportunities. *Journal of Engineering Research and Reports, 26*(2), 215–228. https://doi.org/10.9734/jerr/2024/v26i21083

Ahyati, I. U., Pratiwi, E. L., Humaidi, M., & Rozaq, A. (2025). Edukasi Keamanan Digital untuk Meningkatkan Literasi Digital Karyawan Perusahaan Daerah Sa-ijaan Mitra Lestari Kotabaru: Digital Security Education to Improve Digital Literacy Employees of the Regional Company Sa-ijaan Mitra Lestari Kotabaru. *PengabdianMu: Jurnal Ilmiah Pengabdian kepada Masyarakat, 10*(7), 1753-1758. https://doi.org/10.33084/pengabdianmu.v10i7.9826

Ardhianty, I. W. (2025). Tantangan dan strategi perlindungan konsumen pada layanan perbankan di tengah kemajuan teknologi. *Jurnal Multidisiplin Ilmu Akademik, 2*(2), 151–162.

Ardika, I. W. C. (2025). Tinjauan hukum terhadap perlindungan data pribadi di era digital: Kasus kebocoran data pengguna layanan e-commerce. *Indonesian Journal of Law and Justice, 2*(3), 11–11. https://doi.org/10.47134/ijlj.v2i3.3601

Asrianti, N. F., Alghazali, M. G., Putri, I. Y., & Awalia, A. D. N. (2025). Kasus Kebocoran Data Pada Pusat Data Nasional KOMINFO: Pentingnya Keamanan Cloud di Era Digitalisasi. *Innovation in Computer Education Journal, 1*(1), 24–33. https://journal.unm.ac.id/index.php/ICEJ/issue/view/480

Aura Jelita, N. B., & Siregar, H. (2025). Systematic Literature Review: Evolusi Ancaman Siber Dan Metode Deteksi Malware Di Sistem Operasi Android (2020–2025) . *Jurnal Komputer Teknologi Informasi Sistem Informasi (JUKTISI), 4*(1), 227–235. https://doi.org/10.62712/juktisi.v4i1.395

Damargara, M. I., Alhidayah, M., Faiqy, M. R., & Maulana, J. (2022). Urgensi realisasi pengaturan Data Protection Officer (DPO) pada sektor kesehatan ditinjau dari hukum pelindungan data pribadi. *Padjadjaran Law Review, 10*(1). https://doi.org/10.56895/plr.v10i1.838

Darmawan, R. W., Irawan, I., & Petriansyah, S. (2025). Analisis Adaptif Zero Trust Architecture (ZTA) Berbasis Machine Learning untuk Deteksi Intrusi pada Jaringan IoT dalam Infrastruktur Kritis. *RIGGS: Journal of Artificial Intelligence and Digital Business, 3*(4), 36–45. https://doi.org/10.31004/riggs.v3i4.460

Erikha, A., & Hoesein, Z. A. (2025). Strategi pencegahan kebocoran data pribadi melalui peran Kominfo dan gerakan Siberkreasi dalam edukasi digital. *Jurnal Retentum, 4*(1), 48–64. http://dx.doi.org/10.46930/retentum.v7i1.5272

Erniyanti, A., Soesanto, E., Putri, K. A., & Rahma, F. D. (2024). Penerapan manajemen sekuriti dengan standar, komponen, dan K3 di PT. Pertamina Hulu Rokan. *Jurnal Ekonomi dan Bisnis, 2*(1), 143–151.

Firdaus, S. E., Hidayah, S., & Putro, H. (2025). Implementasi teknologi untuk penguatan keamanan data pribadi nasabah dalam sektor perbankan. *Jurnal Ilmiah Nusantara, 2*(1), 1–11.

Fitria, K. M. (2023). Analisis serangan malware dalam perbankan dan perencanaan solusi keamanan. *Jurnal Informatika dan Teknik Elektro Terapan, 11*(3).

Ghiffari, M. N., Nurliana, A., & Girinoto. (2023). Analisis pola penyebaran informasi insiden kebocoran data melalui pendekatan Social Network Analysis (SNA). *Info Kripto: Jurnal Ilmiah Keamanan Siber dan Kriptologi, 17*(1), 1–6. https://doi.org/10.56706/ik.v17i1.71

Hakim, L. (2024). Tantangan dan Strategi Investasi pada Perusahaan Startup Teknologi di Indonesia. *PRODUCTIVITY: JOURNAL OF INTEGRATED BUSINESS, MANAGEMENT, AND ACCOUNTING RESEARCH: Lembaga Intelektual Muda Maluku, 1*(2), 75-84. https://doi.org/10.54373/product.v1i2.36

Indonesiawan, R. C. S., Alroy, M., Suci, T. L., & Prasetyo, B. R. (2021). Analisis privasi data pengguna dalam instansi BPJS Kesehatan. *Prosiding Seminar Nasional Teknologi dan Sistem Informasi SITASI, 1*(1), 174–182. https://doi.org/10.33005/sitasi.v1i1.134

Irdi, M., Aditya, R., Ramdhani, A., Nugraha, D. D., & Febrian, M. F. A. (2025, May). Analisis masalah serangan phishing pada penggunaan email. *In Prosiding Seminar Nasional Teknologi Informasi, Mekatronika, dan Ilmu Komputer (Vol. 4*, pp. 142–146).

Irfana, Hedwig Mau, & Tri Agus S. (2025). Tanggungjawab hukum badan penyelenggara jaminan sosial Kesehatan dalam pengelolaan dan perlindungan data peserta jaminan kesehatan terhadap risiko kebocoran data. *JIIP: Jurnal Ilmiah Ilmu Pendidikan, 8*(10), 12076–12080. https://doi.org/10.54371/jiip.v8i10.9449

Kusnanto, Y., Nugroho, M. A., & Kartadie, R. (2024). Implementasi Zero Trust Architecture untuk Meningkatkan Keamanan Jaringan: Pendekatan Berbasis Simulasi. *JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika), 9*(4), 2357-2364.

Maulida, O., & Utomo, H. (2024). Pertanggungjawaban badan penyelenggara jaminan sosial (BPJS) Kesehatan atas kebocoran data pribadi pengguna dalam perspektif hukum pidana. *Indonesian Journal of Law and Justice, 1*(2), 1–9. https://doi.org/10.47134/ijlj.v1i2.2011

Milafebina, R., Lesmana, I. P., & Syailendra, M. R. (2023). Perlindungan Data Pribadi terhadap Kebocoran Data Pelanggan E-commerence di Indonesia. *Jurnal Tana Mana, 4*(1), 157–169. https://doi.org/10.33648/jtm.v4i1.331

Mukhlisin, M., & Firmansyah, R. A. (2025). ZERO TRUST ARCHITECTURE: SOLUSI KEAMANAN DAN PRIVASI UNTUK INSTITUSI PENDIDIKAN, SYSTEMATIC LITERATURE REVIEW. *JATI (Jurnal Mahasiswa Teknik Informatika), 9*(4), 6926-6935. https://doi.org/10.36040/jati.v9i4.14344

Munandar, A., Listiani, D., Malik, F. A., Pratama, B. A., & Augustia, A. E. (2025). Kebocoran data BPJS sebagai studi kasus kelemahan keamanan lembaga publik. *TEKNOBIS: Teknologi, Bisnis Dan Pendidikan, 3*(2), 302–305. https://jurnalmahasiswa.com/index.php/

Nadiroh, A., & Wiraguna, S. A. (2025). Analisis yuridis kebocoran data di layanan kesehatan digital: Studi kasus aplikasi telemedicine di Indonesia. *Media Hukum Indonesia (MHI), 2*(6), 313–320. https://ojs.daarulhuda.or.id/index.php/MHI/article/view/1465

Nainggolan, P. A., & Risman, A. (n.d.). Manajemen risiko keuangan digital: Strategi mitigasi risiko dalam era transformasi digital.

Napu, I. A., Supriatna, E., Safitri, C., & Destiana, R. (2024). Analisis Peran Keamanan Siber dan Keterampilan Digital dalam Pertumbuhan Usaha Kecil Menengah di Era Ekonomi Digital di Indonesia. *Sanskara Ekonomi Dan Kewirausahaan, 2*(03), 156–167. https://doi.org/10.58812/sek.v2i03.411

Nathania, A. B., Azam, M. A., & Voll, R. R. E. (2025). Menanggulangi ancaman keamanan siber di sektor perbankan: Upaya melindungi data nasabah di zaman digital. *Jurnal Ilmiah Wahana Pendidikan, 11*(6D), 34–39.

Nugraha, D. A., Nurfitroh, R., Ul-Haq, N. D., Dika, R. P., & Lagontang, S. N. (2025). Kebocoran data BPJS Kesehatan: Ancaman terhadap keamanan informasi publik di era digital. *Integrative Perspectives of Social and Science Journal (IPSSJ)*, *2*(3), 4685–4691. https://ipssj.com/index.php/ojs/article/view/620

Nugroho, F. N. P., Listanto, M. F., Amelia, N., & Annisa, S. (2024). Analisis Kebocoran Data Pribadi Dalam Media Sosial. *Fibonacci: Jurnal Ilmu Ekonomi, Manajemen Dan Keuangan, 1*(2), 58–65. https://doi.org/10.63217/fibonacci.v1i2.70

Nursabrina, B., Fauzi, A., Rasim, R., Ramadhan, F., & Zahira, G. (2024). Peran Manajemen Sekuriti Dalam Meningkatkan Pertahanan dan Keamanan Data Pribadi Akun Facebook. *Jurnal Ilmu Multidisiplin, 3*(1), 59–68. https://doi.org/10.63217/orbit.v1i2.83

Nusantara, A. H. S., Umam, I. K., & Lubis, M. (2024). Jaminan informasi dan keamanan yang lebih baik: Studi kasus BPJS Kesehatan. *Nuansa Informatika Jurnal Teknologi Informasi*, *18*(2), 120–127. https://doi.org/10.25134/ilkom.v18i2.202

Panggabean, M. V., & Fitria, A. (2025). Perlindungan hukum data pribadi di Indonesia (kasus kebocoran Badan Penyelengara Jaminan Sosial Kesehatan). *Arus jurnal Sosial dan Humaniora (AJSH)*, *5*(2), 1958–1965. https://doi.org/10.57250/ajsh.v5i2.1487

Prasetio, A. M. D. A. P., Siswoko, A. P. P., Oktavian, B., Trihantono, A. S., Ramadhan, M. N., Arfan, S. J., & Saepudin, T. H. (2025). Implementasi pengamanan file di PT. XYZ (studi pustaka manajemen sekuriti). *BORJUIS: Jurnal of Economy, 3*(2), 55–61.

Putra, R. K., Idris, M. F., & Widhiati, G. (2024). Perlindungan data pribadi dalam era big data: Implikasi hukum di Indonesia. *JAKSA: Jurnal Kajian Ilmu Hukum dan Politik*, *2*(4), 31–44. https://doi.org/10.51903/jaksa.v2i4.2260

Putri, D. D. F., & Fahrozi, M. H. (2021). Upaya Pencegahan Kebocoran Data Konsumen Melalui Pengesahan RUU Perlindungan Data Pribadi (Studi Kasus E-Commerce Bhinneka. Com). *Borneo Law Review, 5*(1), 46–68. https://doi.org/10.35334/bolrev.v5i1.2014

Rahman, A. F., & Rahman, R. (2024). Penerapan Zero Trust Network Access (ZTNA) dengan penggunaan CAPTCHA pada website umum. *Technology Sciences Insights Journal, 1*(2), 71-75.

Rakhmadi Rahman, R. R., Faiz Ilyas, M. F. I., & Syawal, M. S. (2025). Implementasi Zero Trust Arsitektur Pada Jaringan Hybrid Work. *Journal of System & Technology (SYSTEC), 1*(1), 14-19. https://systec.ejournal.unri.ac.id/index.php/systec/article/view/8

Rojabi, M. A. (2025). *Cloudflare Zero Trust: Implementasi Akses Aman dan Modern untuk Bisnis*. Afdan Rojabi Publisher.

Safira, S. D., Setyaningrum, R. P., Anwar, N. R., Aldrin, M., Noto, I. M. C. D., & Fathihah, M. A. N. (2025). Analisis kepatuhan etika profesi dan keamanan sistem: Studi kasus kebocoran data BPJS Kesehatan. *Informasi Interaktif Jurnal Informatika dan Teknologi Informasi*, *10*(2), 159–164. https://informasiinteraktif.janabadra.ac.id/index.php/jii/article/view/157

Saputra, Y. S., Wakhid, R. N., Rabbani, R. G., Wildan, A., Heriyanto, A. B. S., & Saepudin, T. H. (2024). MANAJEMEN KEAMANAN CYBER DI PERUSAHAAN. HUMANITIS: *Jurnal Homaniora, Sosial dan Bisnis, 2*(7), 759-762.

Satrya, I. Z. (2024). Serangan siber dalam perkembangan perbankan digital di Indonesia. *Journal of Syntax Literate, 9*(10).

Septian, A., Alfiansyah, T., Abdulla, A. D., Sutiawan, H., Fauzi, D. A. E., & Saputra, D. H., & Saepudin, T. H. (2024). Analisis tingkat keamanan data pada salah satu kantor perpajakan di Bekasi yang rentan terhadap serangan siber dalam sistem keuangan. *HUMANITIS: Jurnal Humaniora, Sosial dan Bisnis, 2*(7), 711–718.

Setiyawan, W. B. M., Churniawan, E., & Faried, F. S. (2020). UPAYA REGULASI TEKNOLOGI INFORMASI DALAM MENGHADAPI SERANGAN SIBER GUNA MENJAGA KEDAULATAN NEGARA KESATUAN REPUBLIK INDONESIA. *Jurnal USM Law Review, 3*(2), 275–295. https://doi.org/10.26623/julr.v3i2.2773

Silvia, A. F., Sunaryo, H., Saputra, W., & Sinlae, F. (2023). Analisis keamanan data pribadi pada pengguna BPJS Kesehatan: Ancaman, risiko, strategi kemanan (literature review). *Nusantara Journal of Multidisciplinary Science*, *2*(1), 201–207. https://jurnal.intekom.id/index.php/njms

Sorisa, C., Kiareni, C. L., & Parhusip, J. (2024). Etika keamanan siber: Studi kasus kebocoran data BPJS Kesehatan di Indonesia. *Jurnal Sains Student Research*, *2*(6), 586–593. https://doi.org/10.61722/jssr.v2i6.2996

Susanto, E., Ramhadan, H., Ardiansyah, I., & Maulan, R. (2023). Manajemen sekuriti pada perusahaan Samsung Electronics Indonesia. *Jurnal Ilmiah Wahana Pendidikan, 9*(12), 166–175. https://doi.org/10.5281/zenodo.8078569

Susanto, E., Windari, A., & Amalia, R. (2024). EDIKASI: Empowering data integrity and knowledge on health information release in the digital era. *LINK Jurnal*, *20*(2), 113–117. https://doi.org/10.31983/link.v20i2.12317

Sutrisna, C. (2021). Aspek Hukum Perlindungan Data Pribadi dan Kondisi Darurat Kebocoran atas Data Pribadi di Indonesia. *Wacana Paramarta: Jurnal Ilmu Hukum, 20*(5), 1–10. https://doi.org/10.32816/paramarta.v20i5.138

Suwiknyo, F. B. (2021). Tindak kejahatan siber di sektor jasa keuangan dan perbankan. *Lex Privatum, 9*(4).

Tannavaro, D. M., & Wiraguna, S. A. (2025). Strategi komunikasi humas dalam krisis siber: Studi kasus BPJS Kesehatan dan Bank Syariah Indonesia. *Kohesi: Jurnal Multidisiplin Saintek*, *7*(11), 1–12. https://doi.org/10.2238/k1gf3g38

Taupaani, R., & Harwahyu, R. (2025). ZTSCAN: ENHANCING ZERO TRUST RESOURCE DISCOVERY WITH MASSCAN AND NMAP INTEGRATION. *JITK (Jurnal Ilmu Pengetahuan Dan Teknologi Komputer), 10*(4), 868–877. https://doi.org/10.33480/jitk.v10i4.6628

Zaman, A. A., Anwar, J., & Fadlian, A. (2021). Pertanggung jawaban pidana kebocoran data BPJS dalam perspektif UU ITE. *De Juncto Delicti: Journal of Law*, *1*(2), 146–157. https://doi.org/10.35706/djd.v1i2.5732