Strategi Manajemen Risiko dan Keamanan Siber dalam Ekonomi Digital: Tinjauan Literatur

by Adinda Priski Dhea Asiyanti

Submission date: 17-Oct-2024 03:41PM (UTC+0700)
Submission ID: 2488017824
File name: plate_Artikel_Ilmiah_Penelitian_versi_update_2024_Adindapda.docx (87.29K)
Word count: 5822
Character count: 39660

Strategi Manajemen Risiko dan Keamanan Siber dalam Ekonomi Digital: Tinjauan Literatur

Adinda Priski Dhea Asiyanti [1*], Agussalim [2]

[1]Universitas Pembangunan Negara Veteran, Jawa Timur, Indonesia
priskiadinda@gmail.com

Alamat: Jalan Rungkut Madya, Gunung Anyar, Surabaya, Jawa Timur
Korespondensi penulis: priskiadinda@gmail.com

Abstract. *This research discusses the significant role of digital technology in the modern economy, particularly in relation to cybersecurity and the impact of technological disruption on business sustainability. The main topics analyzed include the use of artificial intelligence (AI) to detect cyber threats, strategies for protecting IT supply chains, and the challenges faced by the banking sector and the Internet of Things (IoT) in managing cybersecurity risks. The research also examines the impact of digitalization on social inequality and poverty in the European Union. Digital technologies such as automation, data analytics, and IoT drive innovation and enhance operational efficiency, but also introduce disruptive challenges that must be addressed through careful risk management and increased organizational capacity to ensure business resilience.*

Keywords: *Risk Management, Cybersecurity, Digital Economy*

Abstrak. Penelitian ini membahas peran penting teknologi digital dalam ekonomi modern, terutama terkait keamanan siber dan dampak disrupsi teknologi terhadap keberlanjutan bisnis. Topik-topik utama yang dianalisis meliputi penggunaan kecerdasan buatan (AI) untuk mendeteksi ancaman siber, strategi perlindungan rantai pasokan IT, dan tantangan sektor perbankan serta Internet of Things (IoT) dalam mengelola risiko keamanan siber. Penelitian ini juga meninjau dampak digitalisasi terhadap ketimpangan sosial dan kemiskinan di Uni Eropa. Teknologi digital seperti otomatisasi, analitik data, dan IoT mendorong inovasi serta meningkatkan efisiensi operasional, tetapi juga memunculkan tantangan disrupsi yang harus diatasi melalui pengelolaan risiko yang cermat dan peningkatan kapasitas perusahaan dalam menjaga ketahanan bisnis.

Kata Kunci: Manajemen Risiko, Keamanan Siber, Digital Ekonomi

1. LATAR BELAKANG

Di era ekonomi digital saat ini, keamanan siber memainkan peran krusial dalam menjaga keberlangsungan operasional dan pertumbuhan ekonomi. Perkembangan teknologi digital, seperti *big data*, kecerdasan buatan (AI) dan *Internet of Things* (IoT), telah membawa perubahan besar dalam cara bisnis beroperasi. Teknologi-teknologi ini memberikan banyak manfaat dalam hal efisiensi dan inovasi, tetapi juga membawa tantangan yang signifikan terkait risiko keamanan siber. Menurut (Aliyev 2022), transformasi digital ekonomi dan masyarakat merupakan prioritas utama di negara-negara maju, dengan keamanan informasi sebagai salah satu elemen utama untuk memastikan ekonomi berbasis teknologi informasi yang aman dan berkelanjutan.

Manajemen risiko keamanan siber dalam konteks ekonomi digital melibatkan proses identifikasi, penilaian, dan mitigasi risiko yang dapat memengaruhi infrastruktur digital perusahaan. (Radanliev et al. 2020) menggarisbawahi bahwa IoT dan *Industry 4.0*

menghadirkan tantangan baru dalam rantai pasokan, dengan meningkatnya ancaman serangan siber yang memerlukan pendekatan analitik risiko prediktif yang didukung oleh AI dan pembelajaran mesin untuk mitigasi secara real-time.

Selain itu, langkah-langkah keamanan siber perlu disertakan dalam strategi transformasi digital agar penerapan teknologi baru bisa berjalan lancar. (Olubunmi et al. 2024) mengingatkan bahwa rantai pasokan TI sekarang sangat terikat dengan infrastruktur digital global, dan kelemahan dalam rantai pasokan tersebut bisa menyebabkan masalah besar, mulai dari kerugian finansial hingga hilangnya kepercayaan dari para pemangku kepentingan. (Thach et al. 2020) juga menambahkan bahwa kemajuan teknologi 4.0 telah meningkatkan produktivitas.

Di tengah pesatnya transformasi digital, (Saeed et al. 2023) menekankan pentingnya kesadaran dan kesiapan keamanan siber, karena adopsi teknologi seperti AI, *big data*, dan blockchain dapat menimbulkan kerentanan baru. Oleh sebab itu, perusahaan atau organisasi perlu menerapkan kerangka kerja kesiapan keamanan siber yang komprehensif untuk mendukung proses transformasi digital secara aman.

Hasil penelitian ini memberikan manfaat besar bagi sektor perbankan dan sektor-sektor lain yang bergantung pada infrastruktur digital. Saran penggunaan AI dan pembelajaran mesin untuk mengurangi risiko secara real-time dapat memperkuat strategi keamanan siber. Temuan ini sangat relevan untuk diterapkan oleh praktisi dan pembuat kebijakan yang bertanggung jawab atas pengelolaan ekonomi berbasis teknologi.

Output penelitian ini adalah rangkuman literatur yang mendalam tentang keamanan siber di era ekonomi digital, termasuk strategi mitigasi yang dapat diterapkan di berbagai sektor bisnis. Outcome dari penelitian ini diharapkan membantu organisasi dalam meningkatkan ketahanan mereka terhadap serangan siber melalui penerapan teknologi seperti AI, IoT, dan blockchain, serta pengembangan kerangka kerja keamanan yang lebih kuat.

Rumusan Masalah

Rumusan masalah dalam penelitian adalah mengidentifikasi tantangan yang dihadapi perusahaan dalam menangani risiko keamanan siber akibat transformasi digital. Penelitian ini menyatakan bahwa ada kebutuhan mendesak akan strategi manajemen risiko yang lebih canggih, mengingat semakin luasnya adopsi teknologi seperti AI, big data, dan IoT, yang menyebabkan peningkatan risiko serangan siber yang perlu ditangani dengan cepat.

2. KAJIAN TEORITIS

Ekonomi digital berkembang pesat seiring dengan meningkatnya adopsi teknologi digital oleh perusahaan di berbagai sektor. Namun, kemajuan ini juga diiringi dengan peningkatan risiko keamanan siber yang signifikan. Manajemen risiko keamanan siber menjadi faktor kunci untuk melindungi aset digital dan menjaga kelangsungan bisnis dalam menghadapi ancaman siber.

Keamanan Siber dan Transformasi Digital

Keamanan siber berkaitan dengan upaya perlindungan sistem informasi dari serangan yang bertujuan untuk mencuri, mengubah, atau merusak data sensitif. Transformasi digital, di sisi lain, merupakan adopsi solusi digital oleh organisasi untuk meningkatkan efisiensi operasional dan daya saing mereka. (Saeed et al. 2023) menyoroti bahwa transformasi digital mendorong perusahaan untuk mengadopsi teknologi seperti *Artificial Intelligence*, *Big Data*, *Blockchain*, dan *Cloud Computing*, yang mempercepat operasi bisnis tetapi juga menimbulkan tantangan baru terkait keamanan siber.

Dalam konteks ekonomi digital, (Wibowo 2022) & (Simarmata et al. 2021) menunjukkan bahwa perlindungan keamanan informasi adalah salah satu pilar utama untuk memastikan keberlanjutan ekonomi digital yang aman. Ekonomi digital yang berkembang, terutama di negara-negara maju, memerlukan mekanisme untuk mengamankan infrastruktur digitalnya dari ancaman siber, yang terus berkembang seiring dengan meningkatnya adopsi teknologi informasi.

Manajemen Risiko Siber

Manajemen risiko siber adalah pendekatan sistematis yang bertujuan untuk mengidentifikasi, menilai, dan mengurangi risiko siber yang dapat memengaruhi organisasi. (Radanliev et al. 2020) mengungkapkan bahwa dengan meningkatnya integrasi teknologi Internet of Things (IoT) dalam rantai pasok industri, risiko siber semakin kompleks. Mereka menyoroti pentingnya *cyber risk analytics* yang didukung oleh kecerdasan buatan (AI) dan pembelajaran mesin (ML) untuk membantu organisasi memprediksi risiko siber secara real-time.

Menurut (Olubunmi et al. 2024), manajemen risiko siber dalam rantai pasokan TI juga memerlukan pendekatan proaktif. Mereka menekankan perlunya penerapan model keamanan *Zero-Trust* dan pelatihan berkala bagi karyawan untuk memperkuat pertahanan siber. Implementasi langkah-langkah ini membantu perusahaan menghadapi ancaman siber dengan lebih baik dan menjaga ketahanan rantai pasokan mereka.

Dampak Terhadap Perbankan dan Sektor Keuangan

Sektor keuangan, khususnya perbankan, merupakan salah satu sektor yang paling rentan terhadap serangan siber. (Thach et al. 2020) dalam studi kasus di Vietnam menyoroti bahwa transformasi digital dan penerapan teknologi industri 4.0 membawa dampak besar pada aktivitas perbankan. Namun, perkembangan ini juga meningkatkan risiko keamanan siber, terutama di pasar negara berkembang. Sistem perbankan digital harus lebih tangguh dalam menghadapi ancaman seperti peretasan akun, pencurian identitas, dan sabotase sistem. (Thach 2020) juga mencatat bahwa bank di negara berkembang harus meningkatkan investasi mereka dalam sistem keamanan siber untuk melindungi nasabah dan operasional bisnis dari ancaman yang semakin kompleks.

Selain itu, (Al-shareeda et al. 2024) menekankan pentingnya kerangka kerja manajemen risiko siber yang jelas dan terstandarisasi, terutama untuk mengelola risiko di sistem IoT. International Organization for Standardization (ISO) dianggap sebagai salah satu kerangka kerja yang paling efektif dalam mengelola risiko siber, memberikan panduan bagi organisasi dalam menerapkan langkah-langkah mitigasi yang komprehensif.

Strategi dan Kerangka Kerja Keamanan Siber

Untuk melindungi aset digital organisasi, (Radanliev et al. 2020) mengusulkan penggunaan *predictive cyber risk analytics*, yang memungkinkan perusahaan memantau dan menganalisis risiko secara real-time. Pendekatan ini menggunakan kecerdasan buatan (AI) dan pembelajaran mesin (ML) untuk memproses data dan memberikan wawasan tentang potensi ancaman yang mungkin timbul dari integrasi teknologi IoT dalam operasi bisnis.

Selain itu, penting juga bagi perusahaan untuk memiliki kerangka kerja keamanan siber yang disesuaikan dengan kebutuhan dan karakteristik spesifik mereka. Misalnya, (Al-shareeda et al. 2024) merekomendasikan penggunaan kerangka kerja ISO untuk organisasi yang mengoperasikan perangkat IoT. Kerangka kerja ini memberikan panduan praktis tentang cara mengidentifikasi risiko, menerapkan kontrol keamanan yang tepat, dan melakukan evaluasi risiko secara berkala.

Manajemen risiko keamanan siber memainkan peran penting dalam menjaga keamanan aset digital perusahaan di era ekonomi digital. Seiring dengan meningkatnya ketergantungan pada teknologi digital, perusahaan harus memperbarui strategi dan kerangka kerja mereka untuk menghadapi ancaman siber yang terus berkembang (Haryanto 2023). Kombinasi antara teknologi canggih seperti AI, Big Data, dan penerapan kerangka kerja manajemen risiko yang komprehensif dapat membantu perusahaan mengurangi risiko dan meningkatkan ketahanan terhadap serangan siber.

e-ISSN: xxxx-xxxx; p-ISSN: xxxx-xxxx, Hal 00-00

3. METODE PENELITIAN

Penelitian ini menggunakan pendekatan Systematic Literature Review (SLR) yang bertujuan untuk mengumpulkan dan mengevaluasi penelitian sebelumnya. Menurut Priharsari (2022), metode SLR melibatkan empat tahap utama yaitu perencanaan ulasan, pemilihan dan evaluasi literatur, analisis hasil, serta penyusunan ulasan komprehensif. Penelitian ini menggunakan data sekunder dari artikel dan jurnal yang relevan, dikumpulkan melalui Google Scholar dan Springer dengan kata kunci seperti "Cyber security", "Risk Management", dan "Digital Economy".

***Database Repository* Jurnal**

Mengidentifikasi perpustakaan digital yang relevan dengan peninjauan jurnal berarti memilih platform akademik seperti Google Scholar, Scopus, Springer untuk mengakses artikel penelitian yang sesuai dengan topik. Hal ini membantu memastikan bahwa sumber yang digunakan berkualitas dan relevan.

Kriteria Inklusi dan Eksklusi

Kriteria inklusi adalah standar yang digunakan untuk memilih studi atau artikel yang relevan dengan penelitian, sedangkan kriteria eksklusi digunakan untuk menyingkirkan studi yang tidak sesuai. Inklusi biasanya berdasarkan tahun penerbitan, relevansi topik, atau indeks tertentu, sementara eksklusi mengacu pada studi yang terlalu lama, tidak relevan, atau jenis dokumen yang tidak diinginkan, seperti skripsi atau buku.

Kriteria Inklusi :

1. Jurnal yang diterbitkan antara tahun 2020 hingga 2024
2. Penelitian yang berfokus pada topik manajemen risiko keamanan siber di sector keuangan.
3. Jurnal dengan indeks Scopus, Springer, Jurnal Internasional dan minimal Sinta 6.
4. Studi yang ditulis dalam Bahasa Inggris atau Indonesia.

Kriteria Ekslusi :

1. Jurnal yang diterbitkan sebelum tahun 2020.
2. Studi yang tidak relevan dengan topik keamanan siber atau manajemen risiko.
3. Skripsi dan buku tidak disertakan.
4. Artikel yang tidak diindeks dalam basis data akademik yang diakui (Scopus, Sinta, Springer, Jurnal Internasional).

4. HASIL DAN PEMBAHASAN

Pada bagian ini, peneliti melakukan eksplorasi terhadap literatur ilmiah untuk menganalisis pentingnya keamanan siber dan Manajemen risiko terhadap ekonomi digital.

Tabel 1. Identifikasi Jurnal

Jurnal	Identitas Jurnal	Keterangan
1	Judul	Technologies Ensuring the Sustainability of Information Security of the Formation of the Digital Economy and their Perspective Development Directions
	Jurnal	I.J. Information Engineering and Electronic Business
	Index Jurnal	Jurnal Internasional
	Volume dan Halaman	Vol. 14 No. 5 , Hal 1-14
	Tahun	2022
	Penulis	Alovsat Garaja Aliyev
	Tanggal Akses	6 Oktober 2024
	Link	http://www.mecs-press.org/
2	Judul	Cyber risk at the edge: current and future trends on cyber risk analytics and artificial intelligence in the industrial internet of things and industry 4.0 supply chains
	Jurnal	SPRINGER LINK
	Index Jurnal	Springer
	Volume dan Halaman	Vol. 3 No. 13
	Tahun	2020
	Penulis	Petar Radanliev, David De Roure, Kevin Page, Jason R. C. Nurse, Rafael Mantilla Montalvo, Omar Santos, La'Treall Maddox and Pete Burnap
	Tanggal Akses	6 Oktober 2024
	Link	https://doi.org/10.1186/s42400-020-00052-8
3	Judul	Strategies for protecting IT supply chains against cybersecurity threats
	Jurnal	International Journal of Management & Entrepreneurship Research
	Index Jurnal	Jurnal Internasional
	Volume dan Halaman	Vol. 6 No. 5 , Hal 1598-1606
	Tahun	2024
	Penulis	Olubunmi Adeolu Adenekan, Chinedu Ezeigweneme & Excel Great Chukwurah
	Tanggal Akses	6 Oktober 2024

	Link	http://www.fepbl.com/index.php/ijmer
4	Judul	TECHNOLOGY QUALITY MANAGEMENT OF THE INDUSTRY 4.0 AND CYBERSECURITY RISK MANAGEMENT ON CURRENT BANKING ACTIVITIES IN EMERGING MARKETS - THE CASE IN VIETNAM
	Jurnal	International Journal for Quality Research
	Index Jurnal	Scopus Q3
	Volume dan Halaman	Vol.15 No.3 , Hal 845-856
	Tahun	2020
	Penulis	Nguyen Ngoc Thach, Hoang Thanh Hanh, Dinh Tran Ngoc Huy, Sylwia Gwozdziewicz, Le Thi Viet Nga, Le Thi Thanh Huong, Vu Quynh Nam
	Tanggal Akses	6 Oktober 2024
	Link	http://ijqr.net/journal/v15-n3/10.pdf
5	Judul	CYBERSECURITY RISK MANAGEMENT IN IOT SYSTEMS: A SYSTEMATIC REVIEW
	Jurnal	Journal of Theoretical and Applied Information Technology
	Index Jurnal	Scopus Q4
	Volume dan Halaman	Vol. 102 No. 13 , Hal 5215-5236
	Tahun	2024
	Penulis	TAYSEER ALKHDOUR, MOHAMMED AMIN ALMAIAH, MARIAM ALI ALAHMED , MOHMOOD A. AL-SHAREEDA, ABDALWALI LUTFI AND MAHMAOD ALRAWAD
	Tanggal Akses	7 Oktober 2024
	Link	https://www.jatit.org/volumes/Vol102No13/11Vol102No13.pdf
6	Judul	Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations
	Jurnal	MDPI JOURNAL
	Index Jurnal	Scopus Q2
	Volume dan Halaman	Vol. 23 No. 15 , Hal 1-20
	Tahun	2023
	Penulis	Saqib Saeed, Salha A. Altamimi, Norah A. Alkayyal, Ebtisam Alshehri and Dina A. Alabbad
	Tanggal Akses	8 Oktober 2024
	Link	https://doi.org/10.3390/s23156666

7	Judul	STRATEGI INDONESIA MEMBENTUK CYBER SECURITY DALAM MENGHADAPI ANCAMAN CYBER CRIME MELALUI BADAN SIBER DAN SANDI NEGARA
	Jurnal	Jurnal Dinamika Global
	Index Jurnal	Sinta 3
	Volume dan Halaman	Vol 7 No 2 Hal 295-316
	Tahun	2022
	Penulis	Yosep Ginanjar
	Tanggal Akses	8 Oktober 2024
	Link	https://doi.org/10.36859/jdg.v7i02.1187
8	Judul	PROBLEMS OF BUSINESS PROCESSES TRANSFORMATION IN THE CONTEXT OF BUILDING DIGITAL ECONOMY
	Jurnal	ENTERPRENEURSHIP AND SUSTAINABILITY CENTER
	Index Jurnal	Scopus Q3
	Volume dan Halaman	Vol 8 No 1 Hal 945-959
	Tahun	2020
	Penulis	Karine Alexandrovna Barmuta, Elvir Munirovich Akhmetshin, Iryna Yevheniivna Andryushchenko, Asiyat Akhmedovna Tagibova, Galina Vladimirovna Meshkova, Angelina Olegovna Zekiy
	Tanggal Akses	9 Oktober 2024
	Link	http://doi.org/10.9770/jesi.2020.8.1(63)
9	Judul	Digitalization of the EU Economies and People at Risk of Poverty or Social Exclusion
	Jurnal	Journal of Risk and Financial Management
	Index Jurnal	Scopus Q2
	Volume dan Halaman	Vol 13 No 7 Hal 2-14
	Tahun	2020
	Penulis	Aleksy Kwilinski, Oleksandr Vyshnevskyi and Henryk Dzwigol
	Tanggal Akses	9 Oktober 2024
	Link	https://doi.org/10.3390/jrfm13070142
10	Judul	Tinjauan Literatur Peran Teknologi Digital Dalam Bisnis: Dampak Disruptif TI Pada Perusahaan
	Jurnal	Jurnal Manajemen Kreatif dan Inovasi
	Index Jurnal	Sinta 2
	Volume dan Halaman	Vol 2 No 2 Hal 157-164

e-ISSN: xxxx-xxxx; p-ISSN: xxxx-xxxx, Hal 00-00

	Tahun	2024
	Penulis	Larasati Pingkan Cahya Hernita, Agussalim
	Tanggal Akses	9 Oktober 2024
	Link	https://doi.org/10.59581/jmki-widyakarya.v2i2.2997

Setelah menentukan dan memilih jurnal yang akan dijadikan subjek penelitian, langkah selanjutnya adalah melakukan tinjauan terhadap jurnal tersebut dengan melakukan review seperti berikut.

Jurnal	Review	Keterangan
1	Judul	Technologies Ensuring the Sustainability of Information Security of the Formation of the Digital Economy and their Perspective Development Directions.
	Permasalahan	Penelitian ini membahas cara menjaga keamanan informasi dalam perkembangan ekonomi digital, dengan fokus pada identifikasi ancaman potensial dan solusi untuk memastikan kestabilan ekonomi nasional dan regional.
	Tujuan	1. Menganalisis teknologi kunci yang mendukung keamanan informasi dalam ekonomi digital. 2. Menemukan peluang untuk lebih mengoptimalkan proses digitalisasi di berbagai sektor ekonomi. 3. Membangun indicator untuk mengukur keamanan ekonomi terkait keamanan informasi di sector digital. 4. Merumuskan kriteria untuk menilai keberlanjutan keamanan ekonomi pada tingkat regional.
	Metode	Penelitian ini menggunakan metode analisis yang beragam, seperti analisis sistematik, korelasi, regresi, pemodelan matematis, ekonometrik, dan penilaian pakar. Selain itu, penelitian ini juga memanfaatkan teknologi informasi dan komunikasi (ICT), teori informasi, serta teknologi komputasi lunak untuk mengembangkan teknologi keamanan informasi yang berkelanjutan.
	Hasil Penelitian	Penelitian ini berhasil menyusun indikator untuk mengevaluasi keamanan dan keberlanjutan ekonomi digital. Ancaman siber diuraikan secara mendalam, dan disarankan penggunaan teknologi keamanan cerdas untuk mencegah serangan. Panduan ini dirancang untuk menjaga keamanan ekonomi, baik di tingkat nasional maupun regional, dengan menekankan pentingnya ekonomi digital yang aman untuk mempertahankan stabilitas jangka panjang. Panduan ini memberikan arahan bagi pemerintah dan perusahaan dalam membangun infrastruktur digital yang aman serta menghadapi ancaman siber yang berpotensi mengganggu keberlanjutan ekonomi.

2	Judul	Cyber risk at the edge: current and future trends on cyber risk analytics and artificial intelligence in the industrial internet of things and industry 4.0 supply chains.
	Permasalahan	Jurnal ini membahas dampak risiko siber pada integrasi rantai pasokan dalam ekosistem IIoT dan Industri 4.0. Permasalahan utamanya adalah bagaimana teknologi baru seperti AI dan ML dapat digunakan untuk mengurangi risiko siber yang timbul akibat digitalisasi rantai pasokan.
	Tujuan	1. Melakukan tinjauan sistematis terhadap literatur tentang dampak teknologi baru pada rantai pasokan. 2. Mengidentifikasi tren dan risiko baru terkait keamanan siber dalam rantai pasokan yang terintegrasi dengan teknologi Industri 4.0. 3. Mengembangkan kerangka kerja analitis untuk memitigasi risiko siber dengan menggunakan AI dan ML dalam rantai pasokan yang semakin digital.
	Metode	Penelitian ini menggunakan pendekatan taksonomis untuk mengevaluasi kemajuan integrasi rantai pasokan dalam IIoT dan Industri 4.0. Dengan menganalisis 173 makalah akademik dan industri, penelitian ini juga menggunakan studi kasus dan grounded theory untuk menyusun roadmap transformasi bagi UKM dalam mengadopsi teknologi IIoT.
	Hasil Penelitian	Penelitian ini mengidentifikasi sistem adaptif berbasis AI dan ML yang dapat memprediksi risiko siber dan memperkuat rantai pasokan IoT. Dihasilkan roadmap untuk membantu UKM beradaptasi dengan teknologi digital dan mengatasi risiko siber. Tantangan teknis yang dihadapi meliputi keamanan data real-time dan pemulihan dari serangan siber. Artikel ini juga membahas tren teknologi Industri 4.0 dan tantangan UKM dalam mengadopsi teknologi cloud dan IIoT. Penelitian ini mengembangkan kerangka kerja yang mendukung keamanan siber di rantai pasokan dengan teknologi AI dan ML.
3	Judul	Strategies for protecting IT supply chains against cybersecurity threats.
	Permasalahan	Jurnal ini membahas tantangan meningkatnya risiko keamanan siber dalam rantai pasokan IT akibat digitalisasi. Rantai pasokan IT menjadi lebih rentan terhadap serangan siber yang dapat menyebabkan gangguan operasional, kebocoran data, dan kerugian finansial, terutama pada perangkat lunak, perangkat keras, serta ketergantungan pada vendor pihak ketiga.
	Tujuan	Penelitian ini bertujuan untuk mengidentifikasi strategi yang dapat memperkuat keamanan siber di rantai pasokan IT. Tujuannya

		adalah untuk memberikan kerangka kerja yang komprehensif yang dapat digunakan oleh organisasi dari berbagai sektor untuk memperkuat pertahanan mereka terhadap ancaman siber yang terus berkembang.
	Metode	Jurnal ini menggunakan pendekatan analitis terhadap literatur dan kasus keamanan siber, menekankan pentingnya manajemen risiko berkelanjutan, standar keamanan internasional seperti ISO/IEC 27001 dan NIST, serta manajemen vendor. Solusi teknologi canggih seperti blockchain dan AI juga dikaji untuk meningkatkan keamanan.
	Hasil Penelitian	Penelitian ini merekomendasikan adopsi teknologi blockchain untuk menjaga transparansi dan keamanan rantai pasokan, serta penggunaan AI dan machine learning untuk mendeteksi ancaman siber secara real-time. Model keamanan zero-trust juga disarankan untuk mencegah akses tidak sah, dan pelatihan keamanan siber bagi karyawan serta praktik pengembangan perangkat lunak yang aman dianggap penting.
4	Judul	TECHNOLOGY QUALITY MANAGEMENT OF THE INDUSTRY 4.0 AND CYBERSECURITY RISK MANAGEMENT ON CURRENT BANKING ACTIVITIES IN EMERGING MARKETS - THE CASE IN VIETNAM.
	Permasalahan	Jurnal ini membahas dampak teknologi revolusi industri 4.0 terhadap perbankan di pasar berkembang, khususnya di Vietnam. Fokusnya adalah bagaimana bank dapat menerapkan manajemen kualitas teknologi dan pengelolaan risiko keamanan siber yang efektif dalam menghadapi digitalisasi dan meningkatnya ancaman siber.
	Tujuan	Penelitian ini menganalisis dampak teknologi revolusi industri 4.0 dan transformasi digital pada sistem perbankan, serta penerapan manajemen risiko keamanan siber untuk melindungi data dan transaksi online. Studi ini juga menyoroti peran Fintech, teknologi cloud, dan kebijakan dalam mendukung pengelolaan risiko dan keberlanjutan perbankan di Vietnam.
	Metode	Penelitian ini menggunakan metode kualitatif, analisis logis, deduktif, dan sintesis untuk menawarkan solusi dan kebijakan. Data dari AS, Jepang, dan ASEAN digunakan sebagai pembanding, dan pendekatan historis materialis digunakan untuk menilai hubungan antara teknologi dan perbankan.
	Hasil Penelitian	Penelitian ini menunjukkan bahwa teknologi revolusi 4.0, seperti AI, cloud computing, dan blockchain, telah meningkatkan efisiensi dan keamanan transaksi perbankan di Vietnam, meskipun menghadapi tantangan ancaman siber. Penelitian ini juga

		menekankan pentingnya regulasi yang memadai untuk mendukung teknologi di sektor perbankan, terutama di pasar negara berkembang, serta mengidentifikasi bahwa manajemen kualitas teknologi dan keamanan siber yang baik dapat mengurangi risiko operasional dan meningkatkan kualitas layanan bank.
5	Judul	CYBERSECURITY RISK MANAGEMENT IN IOT SYSTEMS: A SYSTEMATIC REVIEW.
	Permasalahan	Jurnal ini membahas tantangan keamanan siber yang dihadapi sistem Internet of Things (IoT), terutama terkait ancaman terhadap keamanan data, integritas sistem, dan privasi pengguna. Risiko signifikan seperti serangan DDoS, peretasan data, dan serangan jaringan menjadi perhatian utama dalam penggunaan teknologi IoT yang dinamis dan terbuka.
	Tujuan	Penelitian ini bertujuan untuk meninjau proses manajemen risiko di sistem IoT, mengidentifikasi kerentanan dan ancaman keamanan siber, serta memberikan rekomendasi teknik mitigasi dan kerangka kerja manajemen risiko untuk melindungi pengguna IoT dari serangan siber.
	Metode	Penelitian ini menggunakan metode Systematic Literature Review (SLR) untuk menilai studi tentang risiko keamanan siber pada sistem IoT. Melalui penyaringan makalah dari basis data seperti Google Scholar dan ResearchGate, penelitian ini mengidentifikasi ancaman, kerangka kerja, dan teknik mitigasi yang paling efektif dalam konteks IoT.
	Hasil Penelitian	Penelitian ini menemukan bahwa serangan DDoS adalah ancaman utama bagi perangkat IoT dengan keamanan rendah. Risiko IoT diklasifikasikan menjadi empat kategori: privasi, keamanan, teknis, dan etis. Kerangka kerja seperti ISO 27001 dan NIST dianggap paling efektif untuk mengelola risiko IoT, dengan rekomendasi menggunakan blockchain dan enkripsi sebagai langkah mitigasi. Autentikasi kuat, firewall, dan sistem deteksi intrusi juga diidentifikasi sebagai solusi efektif untuk menghadapi ancaman keamanan di IoT.
6	Judul	Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations.
	Permasalahan	Jurnal ini membahas tantangan keamanan siber yang timbul dari transformasi digital di berbagai sektor bisnis. Organisasi perlu memastikan keamanan data, proses bisnis, dan aset digital saat mengadopsi teknologi baru seperti AI, big data, blockchain, dan komputasi awan.

	Tujuan	Penelitian ini bertujuan mengidentifikasi tantangan keamanan siber dalam transformasi digital dan memberikan rekomendasi untuk menjaga ketahanan bisnis, dengan fokus pada penyusunan kerangka kerja untuk memitigasi risiko siber selama adopsi teknologi digital.
	Metode	Penelitian ini menggunakan metode tinjauan literatur sistematis berdasarkan pedoman PRISMA, dengan 42 artikel relevan dari Google Scholar yang dipilih menggunakan kata kunci terkait transformasi digital dan keamanan siber sebagai dasar analisis.
	Hasil Penelitian	Penelitian ini menemukan bahwa adopsi teknologi seperti AI, big data, blockchain, dan komputasi awan meningkatkan efisiensi bisnis, tetapi juga membawa risiko keamanan. Ditekankan pentingnya enkripsi, autentikasi, kontrol akses, pelatihan karyawan, dan asuransi siber. Sebagai mitigasi, direkomendasikan kerangka kesiapan keamanan siber dengan empat level: ad-hoc, basic, planned, dan optimized, di mana level optimized melibatkan pemantauan berkelanjutan dan pendekatan proaktif terhadap ancaman siber.
7	Judul	STRATEGI INDONESIA MEMBENTUK CYBER SECURITY DALAM ENGHADAPI ANCAMAN CYBER CRIME MELALUI BADAN SIBER DAN SANDI NEGARA
	Permasalahan	Penelitian ini membahas bagaimana Indonesia menghadapi ancaman kejahatan siber yang semakin meningkat, khususnya melalui pembentukan Badan Siber dan Sandi Negara (BSSN). Seiring dengan peningkatan penggunaan teknologi informasi dan internet, risiko dan ancaman kejahatan siber juga semakin kompleks dan signifikan, yang memerlukan langkah strategis untuk memastikan keamanan di dunia maya.
	Tujuan	Penelitian bertujuan untuk mengidentifikasi strategi yang digunakan Indonesia, khususnya oleh BSSN, dalam membentuk keamanan siber dan melawan ancaman kejahatan siber. Penelitian ini ingin mengetahui bagaimana BSSN bekerja dalam mengembangkan sistem keamanan siber yang efektif.
	Metode	Penelitian ini menggunakan metode kualitatif dengan pendekatan deskriptif. Data dikumpulkan melalui studi pustaka yang mencakup literatur, laporan tahunan, dan berbagai sumber sekunder terkait keamanan siber.
	Hasil Penelitian	Hasil penelitian menunjukkan bahwa Indonesia masih menghadapi berbagai tantangan dalam keamanan siber, termasuk serangan siber yang besar dan kompleks. BSSN sebagai lembaga utama bertanggung jawab untuk mengatasi tantangan ini, dengan langkah-langkah strategis seperti pembentukan kerangka kerja keamanan

		siber nasional, penguatan infrastruktur keamanan, serta peningkatan kapasitas sumber daya manusia di bidang keamanan siber.
8	Judul	PROBLEMS OF BUSINESS PROCESSES TRANSFORMATION IN THE CONTEXT OF BUILDING DIGITAL ECONOMY.
	Permasalahan	Jurnal ini mengeksplorasi tantangan transformasi digital perusahaan, yang meliputi adaptasi terhadap teknologi baru serta restrukturisasi proses bisnis. Transformasi ini memerlukan perubahan dalam strategi, budaya perusahaan, dan model bisnis untuk tetap kompetitif di era digital.
	Tujuan	Penelitian ini bertujuan memahami kesulitan utama yang dihadapi perusahaan dalam digitalisasi proses bisnis dan membangun dasar teoritis untuk memahami transformasi digital dalam menghadapi perubahan cepat di lingkungan bisnis global.
	Metode	Penelitian ini menggunakan analisis sistematis, pemodelan ekonomi, serta deduksi dan induksi. Data diambil dari statistik Rusia dan internasional, serta penelitian sebelumnya. Peneliti membandingkan kesiapan digital ekonomi Rusia dengan negara lain, dan menganalisis efektivitas transformasi digital di berbagai organisasi melalui generalisasi, analisis, dan sintesis.
	Hasil Penelitian	Penelitian ini menunjukkan bahwa transformasi digital adalah proses berkelanjutan yang melibatkan teknologi baru, perubahan budaya, dan restrukturisasi organisasi. Meskipun Big Data dan IoT penting, banyak perusahaan belum siap karena tantangan keamanan siber dan kurangnya regulasi. Ada enam area utama yang perlu diubah, termasuk manajemen, operasi, dan interaksi dengan konsumen, dengan keamanan siber menjadi fokus penting untuk mencegah kebocoran data atau peretasan.
9	Judul	Digitalization of the EU Economies and People at Risk of Poverty or Social Exclusion.
	Permasalahan	Jurnal ini membahas dampak digitalisasi ekonomi di Uni Eropa terhadap risiko kemiskinan dan eksklusi sosial. Meskipun digitalisasi berdampak signifikan secara ekonomi, kelompok berisiko masih menghadapi ancaman kemiskinan. Penelitian ini fokus pada bagaimana digitalisasi memengaruhi kelompok tersebut dan apakah peningkatan digitalisasi dapat secara efektif mengurangi risiko kemiskinan.
	Tujuan	Penelitian ini bertujuan menguji hipotesis bahwa tingkat digitalisasi yang lebih tinggi di negara EU dapat mengurangi risiko kemiskinan dan eksklusi sosial, serta memahami hubungan antara digitalisasi dengan perubahan sosial dan ekonomi di negara-negara EU.

	Metode	Penelitian ini menggunakan analisis komparatif dan korelasi antara indeks digitalisasi (DESI) dan indikator kemiskinan (AROPE). Metode Monte Carlo digunakan untuk memperkirakan perubahan AROPE pada 2021 berdasarkan digitalisasi, dengan data dari negara-negara EU untuk periode 2014-2018.
	Hasil Penelitian	Penelitian ini menunjukkan bahwa negara-negara Uni Eropa dengan digitalisasi tinggi memiliki risiko kemiskinan lebih rendah, terutama bagi kelompok menengah ke atas. Namun, digitalisasi tidak selalu efektif mengurangi kemiskinan bagi kelompok berpenghasilan rendah. Sebaliknya, negara dengan digitalisasi lebih rendah kadang menunjukkan kemajuan lebih signifikan dalam pengurangan kemiskinan, seperti ditunjukkan oleh simulasi Monte Carlo.
10	Judul	Tinjauan Literatur Peran Teknologi Digital Dalam Bisnis: Dampak Disruptif TI Pada Perusahaan.
	Permasalahan	Jurnal ini membahas peran penting teknologi digital dalam bisnis dan dampaknya yang disruptif terhadap perusahaan. Teknologi digital meningkatkan efisiensi, inovasi produk, dan layanan, tetapi juga memicu perubahan model bisnis dan persaingan ketat. Perusahaan yang tidak cepat beradaptasi berisiko kehilangan relevansi di pasar yang berkembang pesat.
	Tujuan	Penelitian ini bertujuan menganalisis literatur tentang peran teknologi digital dalam bisnis dan dampak disruptif TI pada perusahaan. Jurnal ini memberikan wawasan bagi praktisi dan pengambil keputusan tentang pengaruh teknologi digital pada operasi bisnis dan cara mengelola dampaknya secara efektif.
	Metode	Penelitian ini menggunakan tinjauan literatur dari artikel jurnal relevan antara 2019 hingga 2024, yang dipilih berdasarkan kata kunci terkait teknologi digital dan dampak disruptif TI. Setelah meninjau lebih dari 10 artikel, analisis dilakukan dengan membandingkan temuan penelitian tentang transformasi digital di berbagai sektor bisnis.
	Hasil Penelitian	Penelitian ini menunjukkan bahwa teknologi digital berperan penting dalam transformasi bisnis, meningkatkan efisiensi dan inovasi. Perusahaan yang mengadopsi otomatisasi, analitika data, dan IoT dapat meningkatkan pengalaman pelanggan, namun juga menghadapi tantangan seperti keamanan data dan perubahan perilaku konsumen. Oleh karena itu, inovasi, adopsi teknologi proaktif, strategi keamanan siber, dan pengembangan keterampilan digital menjadi kunci keberhasilan di era digital.

PEMBAHASAN

Diskusi dari tinjauan literatur yang telah disampaikan di atas mencakup berbagai topik, antara lain:

1. Technologies Ensuring the Sustainability of Information Security of the Formation of the Digital Economy and their Perspective Development Directions

   Penelitian ini mengeksplorasi bagaimana kecerdasan buatan dapat membantu dalam mengelola risiko keamanan siber di dunia industri yang semakin terhubung dengan Internet. Dengan analitik berbasis AI, risiko siber dapat dideteksi lebih cepat dan efisien, memungkinkan perusahaan untuk bereaksi terhadap ancaman sebelum terjadi kerusakan besar. Penelitian ini menemukan bahwa teknologi AI, seperti *machine learning* dan jaringan syaraf tiruan, sangat efektif dalam mendeteksi pola anomali yang mengindikasikan ancaman siber.

2. Cyber risk at the edge: current and future trends on cyber risk analytics and artificial intelligence in the industrial internet of things and industry 4.0 supply chains.

   Penelitian ini membahas peran teknologi keamanan informasi dalam menjaga keberlanjutan ekonomi digital di tengah ancaman serangan siber dan kebocoran data yang semakin kompleks. Penerapan teknologi seperti kecerdasan buatan (AI) dan komputasi awan terbukti efektif dalam melindungi ekonomi digital. Penelitian ini juga menekankan pentingnya investasi besar dalam keamanan siber dan teknologi canggih untuk memastikan stabilitas ekonomi di masa depan.

3. Strategies for protecting IT supply chains against cybersecurity threats.

   Penelitian ini membahas strategi keamanan siber untuk melindungi rantai pasokan IT dari ancaman yang semakin kompleks. Pendekatan yang digunakan meliputi penilaian risiko berkelanjutan, penerapan standar keamanan internasional seperti ISO/IEC 27001, dan pengelolaan vendor yang lebih baik. Teknologi seperti blockchain dan kecerdasan buatan (AI) digunakan untuk mendeteksi ancaman siber secara efektif, dengan model keamanan *zero-trust* dan pelatihan rutin karyawan sebagai langkah tambahan. Penelitian ini menekankan pentingnya teknologi canggih dan praktik terbaik untuk meningkatkan keamanan dan ketahanan sistem IT perusahaan di era digital.

4. TECHNOLOGY QUALITY MANAGEMENT OF THE INDUSTRY 4.0 AND CYBERSECURITY RISK MANAGEMENT ON CURRENT BANKING ACTIVITIES IN EMERGING MARKETS - THE CASE IN VIETNAM.

   Penelitian ini menyoroti bahwa regulasi yang kuat dan manajemen risiko yang baik diperlukan untuk menjaga keberlanjutan layanan perbankan dan melindungi data dari ancaman peretasan yang semakin canggih. Hasil penelitian menunjukkan bahwa penerapan manajemen risiko keamanan siber yang sesuai dapat membantu bank di pasar negara berkembang seperti Vietnam dalam menghadapi tantangan teknologi yang terus berkembang.

5. CYBERSECURITY RISK MANAGEMENT IN IOT SYSTEMS: A SYSTEMATIC REVIEW.

   Penelitian ini bertujuan untuk memberikan panduan tentang cara terbaik melindungi sistem IoT dari ancaman tersebut dengan menerapkan kerangka kerja manajemen risiko yang telah teruji, seperti ISO 27001 dan NIST. Selain itu, teknologi blockchain dan enkripsi direkomendasikan untuk meningkatkan keamanan. Temuan ini sangat relevan bagi perusahaan dan organisasi yang ingin memperkuat infrastruktur IoT mereka, karena memberikan solusi konkret untuk melawan ancaman keamanan yang terus berkembang.

6. Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations

   Penelitian ini menunjukkan bahwa transformasi digital meningkatkan efisiensi bisnis, tetapi juga memperbesar risiko keamanan siber. Oleh karena itu, penting bagi organisasi untuk mengutamakan keamanan siber dalam proses transformasi mereka. Penelitian merekomendasikan kerangka keamanan berjenjang, dari tingkat dasar hingga optimal, serta perlunya pelatihan karyawan dan pemindaian kerentanan untuk mencegah serangan siber dan melindungi data sensitif.

7. STRATEGI INDONESIA MEMBENTUK CYBER SECURITY DALAM MENGHADAPI ANCAMAN CYBER CRIME MELALUI BADAN SIBER DAN SANDI NEGARA

   Penelitian ini membahas peran BSSN dalam menghadapi ancaman kejahatan siber di Indonesia. Pemanfaatan teknologi digital meningkatkan risiko serangan siber, sehingga BSSN memiliki visi misi menciptakan lingkungan siber yang aman untuk mendukung ekonomi digital. Strategi utama BSSN mencakup penguatan

infrastruktur siber, pembentukan tim tanggap darurat, pencegahan kejahatan siber, dan peningkatan sumber daya manusia. Hasil penelitian menunjukkan tantangan seperti regulasi yang belum optimal dan ancaman serangan yang terus meningkat, namun strategi ini diharapkan mampu meningkatkan ketahanan nasional.

8. PROBLEMS OF BUSINESS PROCESSES TRANSFORMATION IN THE CONTEXT OF BUILDING DIGITAL ECONOMY.

   Penelitian ini menyoroti tantangan yang dihadapi perusahaan dalam melakukan transformasi digital, terutama terkait keterbatasan infrastruktur, kerangka kerja, dan keterampilan digital. Meskipun digitalisasi memberikan keuntungan kompetitif, banyak perusahaan belum siap karena kendala sumber daya dan regulasi. Penelitian ini menekankan pentingnya strategi digital yang disesuaikan untuk mengatasi hambatan tersebut dan mencapai transformasi yang efektif.

9. Digitalization of the EU Economies and People at Risk of Poverty or Social Exclusion.

   Penelitian ini mengkaji dampak digitalisasi di negara Uni Eropa terhadap risiko kemiskinan dan eksklusi sosial. Hasilnya menunjukkan bahwa digitalisasi berdampak lebih besar dalam mengurangi risiko kemiskinan bagi kelompok berpenghasilan menengah ke atas. Namun, untuk kelompok berpenghasilan rendah, pengaruhnya tidak signifikan. Beberapa negara dengan tingkat digitalisasi rendah justru mengalami pengurangan kemiskinan yang lebih cepat dibandingkan negara dengan digitalisasi tinggi. Kesimpulannya, pengaruh digitalisasi terhadap kemiskinan bervariasi tergantung pada konteks sosial-ekonomi tiap negara.

10. Tinjauan Literatur Peran Teknologi Digital Dalam Bisnis: Dampak Disruptif TI Pada Perusahaan.

    Penelitian ini membahas bagaimana teknologi digital seperti otomatisasi dan IoT meningkatkan efisiensi dan inovasi dalam bisnis, tetapi juga menimbulkan tantangan disrupsi yang memaksa perusahaan beradaptasi. Hasilnya menunjukkan bahwa meskipun teknologi digital mendorong transformasi bisnis, perusahaan harus terus berinovasi agar tetap kompetitif di tengah persaingan yang semakin ketat.

Dari berbagai jurnal yang dianalisis, terlihat bahwa keamanan siber ini menjadi permasalahan yang semakin mendesak dalam ekonomi digital yang terus berkembang. Setiap sektor, baik perbankan, rantai pasokan IT, maupun Internet of Things (IoT), menghadapi tantangan terkait ancaman siber. Berbagai artkel seperti “Technologies Ensuring the Sustainability of Information Security” dan “Cyber risk at the edge” menunjukkan bahwa

teknologi kecerdasan buatan (AI) dan machine learning (ML) berperan penting dalam mendeteksi dan memitigasi ancaman siber secara lebih efisien. Implementasi teknologi ini membantu mengurangi risiko serangan siber di lingkungan bisnis yang sangat terhubung.

Lebih lanjut, penelitian seperti "Strategies for Protecting IT Supply Chains Against Cybersecurity Threats" dan "CYBERSECURITY RISK MANAGEMENT IN IOT SYSTEMS" menunjukkan bahwa perlindungan rantai pasokan IT dan sistem IoT membutuhkan kerangka manajemen risiko yang kuat, dengan standar internasional seperti ISO/IEC 27001 dan penggunaan teknologi blockchain sebagai bagian penting dari strategi mitigasi. Di Indonesia, strategi ini didukung oleh pembentukan Badan Siber dan Sandi Negara (BSSN), yang bertugas menguatkan infrastruktur siber dan mengembangkan kapasitas sumber daya manusia. Langkah ini mendukung keberlanjutan ekonomi digital dan sejalan dengan upaya global untuk memperkuat ketahanan siber nasional dan regional.

Penelitian “Digital Transformation and Cybersecurity Challenges for Businesses Resilience” menegaskan bahwa transformasi digital memang membawa efisiensi, tetapi di sisi lain, juga meningkatkan risiko siber. Oleh karena itu, keamanan siber harus diutamakan dalam proses transformasi ini.

Jadi manajemen risiko & keamanan siber di era ekonomi digital sangat penting untuk menjaga keberlanjutan dan stabilitas sistem digital global. Kerangka kerja yang efektif, penggunaan teknologi canggih seperti AI dan blockchain, serta regulasi yang tepat merupakan kunci untuk meminimalkan risiko dan menjaga daya saing perusahaan di era digital.

5. KESIMPULAN

Secara keseluruhan, penelitian ini menunjukkan bahwa teknologi digital memainkan peran kunci dalam transformasi bisnis dan peningkatan efisiensi, namun juga membawa tantangan signifikan terkait risiko keamanan siber dan disrupsi teknologi. Implementasi kecerdasan buatan, blockchain, dan komputasi awan terbukti efektif dalam membantu perusahaan mengatasi ancaman siber dan memperkuat infrastruktur digital. Untuk mencapai keberhasilan dalam era digital, perusahaan dan pemerintah perlu mengadopsi strategi keamanan siber yang komprehensif, menerapkan kerangka kerja risiko yang disesuaikan, serta berinvestasi dalam teknologi canggih guna menjaga stabilitas dan keberlanjutan ekonomi di masa depan.

DAFTAR REFERENSI

Al-shareeda, Mohmood A., Abdalwali Lutfi, and Mahmaod Alrawad. 2024. “CYBERSECURITY RISK MANAGEMENT IN IOT SYSTEMS : A SYSTEMATIC

REVIEW." 102(13):5215–36.

Aliyev, Alovsat Garaja. 2022. "Technologies Ensuring the Sustainability of Information Security of the Formation of the Digital Economy and Their Perspective Development Directions." *International Journal of Information Engineering and Electronic Business* 14(5):1–14. doi: 10.5815/ijieeb.2022.05.01.

Barmuta, Karine Alexandrovna, Elvir Munirovich Akhmetshin, Iryna Yevheniivna Andryushchenko, Asiyat Akhmedovna Tagibova, Galina Vladimirovna Meshkova, and Angelina Olegovna Zekiy. 2020. "Problems of Business Processes Transformation in the Context of Building Digital Economy." *Entrepreneurship and Sustainability Issues* 8(1):945–59. doi: 10.9770/jesi.2020.8.1(63).

Kwilinski, Aleksy, Oleksandr Vyshnevskyi, and Henryk Dzwigol. 2020. "Digitalization of the EU Economies and People at Risk of Poverty or Social Exclusion." *Journal of Risk and Financial Management* 13(7):1–14. doi: 10.3390/jrfm13070142.

Lee, In. 2020. "Internet of Things (IoT) Cybersecurity: Literature Review and Iot Cyber Risk Management." *Future Internet* 12(9). doi: 10.3390/FI12090157.

Olubunmi Adeolu Adenekan, Chinedu Ezeigweneme, and Excel Great Chukwurah. 2024. "Strategies for Protecting IT Supply Chains against Cybersecurity Threats." *International Journal of Management & Entrepreneurship Research* 6(5):1598–1606. doi: 10.51594/ijmer.v6i5.1125.

Pingkan, Larasati, and Cahya Hernita. 2024. "Tinjauan Literatur Peran Teknologi Digital Dalam Bisnis: Dampak Disruptif TI Pada Perusahaan." *Jurnal Manajemen Kreatif Dan Inovasi* 2(2):157–64.

Radanliev, Petar, David De Roure, Kevin Page, Jason R. C. Nurse, Rafael Mantilla Montalvo, Omar Santos, La'Treall T. Maddox, and Pete Burnap. 2020. "Cyber Risk at the Edge: Current and Future Trends on Cyber Risk Analytics and Artificial Intelligence in the Industrial Internet of Things and Industry 4.0 Supply Chains." *Cybersecurity* 3(1). doi: 10.1186/s42400-020-00052-8.

Saeed, Saqib, Salha A. Altamimi, Norah A. Alkayyal, Ebtisam Alshehri, and Dina A. Alabbad. 2023. "Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations." *Sensors* 23(15):1–20. doi: 10.3390/s23156666.

Thach, Nguyen Ngoc, Hoang Thanh Hanh, Dinh Tran, Ngoc Huy, Le Thi, Viet Nga, Le Thi, Thanh Huong, and Vu Quynh Nam. 2020. "TECHNOLOGY-QUALITY-MANAGEMENT-OF-THE-INDUSTRY-40-AND-CYBERSECURITY-RISK-MANAGEMENT-ON-CURRENT-BANKING-ACTIVITIES-IN-EMERGING-MARKETS--THE-CASE-IN-VIETNAMInternational-Journal-for-Quality-Research.Pdf." *International Journal for Quality Research* 15(3):845–56.

Priharsari, D. (2022). Systematic literature review di bidang sistem informasi dan ilmu komputer. *Jurnal Teknologi Informasi Dan Ilmu Komputer (JTIIK)*, *9*(2), 263-268.

Wibowo, A. (2022). Transformasi Ekonomi Digital. *Penerbit Yayasan Prima Agus Teknik*, 1-179.

Simarmata, J., Budiarta, K., & Ginting, S. O. (2021). Ekonomi dan Bisnis Digital.

Ginanjar, Y. (2022). Strategi Indonesia membentuk cyber security dalam menghadapi ancaman cyber crime melalui Badan Siber dan Sandi Negara. *Dinamika Global: Jurnal Ilmu Hubungan Internasional*, *7*(02), 295-316.

e-ISSN: xxxx-xxxx; p-ISSN: xxxx-xxxx, Hal 00-00

10

Haryanto, A., & Sutra, S. M. (2023). Upaya Peningkatan Keamanan Siber Indonesia oleh Badan Siber dan Sandi Negara (BSSN) Tahun 2017-2020. *Global Political Studies Journal*, *7*(1), 56-69.

Strategi Manajemen Risiko dan Keamanan Siber dalam Ekonomi Digital: Tinjauan Literatur

ORIGINALITY REPORT

20%	18%	9%	14%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Universitas Negeri Padang Student Paper	3%
2	kar.kent.ac.uk Internet Source	2%
3	journal.widyakarya.ac.id Internet Source	2%
4	ijqr.net Internet Source	2%
5	www.mecs-press.org Internet Source	1%
6	jurnal.uin-antasari.ac.id Internet Source	1%
7	www.jssidoi.org Internet Source	1%
8	www.mdpi.com Internet Source	1%
9	fepbl.com Internet Source	1%

10	ojs.upi-yai.ac.id Internet Source	1 %
11	jurnal.stie-aas.ac.id Internet Source	1 %
12	www.ejournal.fisip.unjani.ac.id Internet Source	<1 %
13	jurnal.unsil.ac.id Internet Source	<1 %
14	www.jonedu.org Internet Source	<1 %
15	cybersecurity.springeropen.com Internet Source	<1 %
16	Submitted to Curtin University of Technology Student Paper	<1 %
17	www.lames-virtuelles.com Internet Source	<1 %
18	repository.penerbiteureka.com Internet Source	<1 %
19	repositori.uin-alauddin.ac.id Internet Source	<1 %
20	Submitted to University of Bedfordshire Student Paper	<1 %
21	contohmakalahdocx.blogspot.com Internet Source	<1 %

22	journal-nusantara.com Internet Source	<1 %
23	allfind.kpfu.ru Internet Source	<1 %
24	Submitted to University of Hong Kong Student Paper	<1 %
25	Talbi, Mohammed. "Safeguarding IoT Networks Using Machine Learning for Intrusion Detection & Prevention", The George Washington University, 2024 Publication	<1 %
26	ejurnal.seminar-id.com Internet Source	<1 %
27	Submitted to Royal Holloway and Bedford New College Student Paper	<1 %
28	www.econstor.eu Internet Source	<1 %
29	www.fiscalcouncil.gov.cy Internet Source	<1 %
30	Submitted to Harrisburg University of Science and Technology Student Paper	<1 %
31	achmadmuroqi.blogspot.com Internet Source	<1 %

32	anale.steconomiceuoradea.ro Internet Source	<1 %
33	ojs.udb.ac.id Internet Source	<1 %
34	peraturan.bpk.go.id Internet Source	<1 %
35	repository.paramadina.ac.id Internet Source	<1 %
36	www.antarafoto.com Internet Source	<1 %
37	Submitted to School of Business and Management ITB Student Paper	<1 %
38	cpk-front.mzk.cz Internet Source	<1 %
39	digilib.unikom.ac.id Internet Source	<1 %
40	repositori.buddhidharma.ac.id Internet Source	<1 %
41	unair.ac.id Internet Source	<1 %
42	www.convergencevc.com Internet Source	<1 %
43	www.scilit.net	

Internet Source

<1%

44 Ferdy Leuhery, Dwi Nur Fauziah Ahmad, Agung Nurmansyah, Desi Kristanti, M. Imron Mas'ud. "Pelatihan Keterampilan Soft Skills bagi Pekerja Rumahan (Home-Based Workers): Meningkatkan Kualitas Kerja dan Kesejahteraan Tenaga Kerja Informal", Journal Of Human And Education (JAHE), 2024

Publication

<1%

45 ejournal.fisip.unjani.ac.id

Internet Source

<1%

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		