CyberSecurity dan Forensik Digital e-ISSN: 2615-8442
Vol. 8, No. 1, Mei 2025, hlm. 10-16

Kajian Ancaman Baru Dalam Keamanan Informasi: *Systematic Literature Review* Pada Kerentanan *Cyber Security* Pasca-Pandemi

Wilis Arum Karunia[1], Awanda Fitya Zahra[2], Yusuf Amrozi[3]

1,2,3, Departement of Information System, Faculty Of Science and Technology, Universitas Islam Negeri Sunan Ampel Surabaya
Email: wilissarrum@gmail.com, awandafityazahra060603@gmail.com, yusuf.amrozi@uinsa.ac.id

Abstrak

Pandemi COVID-19 telah mempercepat transformasi digital di berbagai sektor, yang disertai dengan peningkatan risiko dan ancaman keamanan siber. Penelitian ini bertujuan untuk mengidentifikasi ancaman keamanan siber yang muncul selama pandemi serta mengevaluasi strategi mitigasi yang telah diterapkan, menggunakan pendekatan Systematic Literature Review (SLR). Hasil dari pencarian ini menghasilkan 53 artikel. Setelah itu, dilakukan analisis awal dengan membaca judul dan abstrak untuk menilai relevansi artikel, yang kemudian menyaring jumlah artikel menjadi 21. Pada tahap seleksi terakhir, evaluasi mendalam dilakukan terhadap artikel yang tersisa untuk memastikan kualitas dan relevansi mereka dengan fokus kajian. Dari proses ini, sebanyak 12 artikel terpilih untuk digunakan dalam literature review. Hasil penelitian menunjukkan bahwa serangan seperti phishing, malware, ransomware, dan serangan DDoS meningkat signifikan, dengan sektor kesehatan dan keuangan menjadi target utama. Selain itu, faktor manusia, seperti stres kerja jarak jauh dan kurangnya pelatihan keamanan, turut berkontribusi pada kerentanan sistem. Strategi mitigasi yang terbukti efektif mencakup implementasi autentikasi multi-faktor (MFA), enkripsi data, pelatihan kesadaran keamanan, dan pemantauan real-time. Namun, transformasi digital yang dilakukan secara terburu-buru tanpa perencanaan keamanan menjadi tantangan utama yang harus diatasi. Penelitian ini memberikan wawasan penting bagi organisasi untuk meningkatkan ketahanan siber melalui integrasi teknologi, kebijakan keamanan, dan pelatihan karyawan yang berkelanjutan. Implikasi dari penelitian ini diharapkan dapat membantu pengembangan strategi keamanan siber yang lebih tangguh untuk menghadapi tantangan di masa depan.

Kata kunci: *keamanan siber, pandemi covid-19, ancaman siber, mitigasi, transformasi digital, pelatihan keamanan*

Evaluating Emerging Threats In Information Security: A Systematic Literature Review On Post-Pandemic Cybersecurity Vulnerabilities

Abstract

The COVID-19 pandemic has accelerated digital transformation across various sectors, accompanied by increased risks and cybersecurity threats. This study aims to identify cybersecurity threats that emerged during the pandemic and evaluate the mitigation strategies that have been implemented, using a Systematic Literature Review (SLR) approach. The research identified 53 articles during the initial search phase. Subsequently, a preliminary analysis was conducted by reviewing the titles and abstracts to assess the relevance of the articles, narrowing the selection to 21 articles. At the final stage, an in-depth evaluation was performed to ensure the quality and relevance of the articles to the research focus, resulting in 12 articles being selected for the literature review. The findings reveal a significant increase in attacks such as phishing, malware, ransomware, and DDoS, with the healthcare and financial sectors being primary targets. Additionally, human factors, such as stress from remote work and a lack of security training, contributed to system vulnerabilities. Effective mitigation strategies included the implementation of multi-factor authentication (MFA), data encryption, security awareness training, and real-time monitoring. However, the rapid digital transformation carried out without proper security planning posed a major challenge that needs to be addressed. This research provides valuable insights for organizations to enhance cyber resilience through the integration of technology, security policies, and continuous employee training. The implications of this study are expected to aid in the development of more robust cybersecurity strategies to address future challenges.

***Keywords**: cybersecurity, covid-19 pandemic, cyber threats, mitigation, digital transformation, security training*

1. PENDAHULUAN

Pandemi Covid-19 memberi dampak yang begitu besar bagi semua orang di dunia, salah satunya peralihan pola pekerjaan dari *work from office* (WFO) menjadi *work from home* (WFH). Menurut (Whitty et al., 2024), dalam waktu singkat kehidupan banyak orang diseluruh dunia berubah secara drastis. Salah satu perubahan tersebut adalah pemindahan sebagian besar tenaga kerja dari kantor ke rumah. Perubahan ini menyebabkan terjadinya pencampuran antar personal (misalnya rumah sekolah, banyak anggota keluarga dirumah, dll) dan kehidupan kerja dalam situasi yang seringkali sangat menegangkan.

Perubahan pola kerja ini mendorong adopsi teknologi digital dalam waktu singkat di berbagai aspek kehidupan. Transformasi yang cepat ini mengakibatkan peningkatan penggunaan teknologi digital, yang secara bersamaan menciptakan kerentanan dan ancaman baru di bidang keamanan siber. Ancaman-ancaman ini termasuk serangan phishing, malware, ransomware, hingga eksploitasi kerentanan perangkat lunak yang belum sepenuhnya diantisipasi oleh banyak organisasi. Sebuah studi oleh (Okereafor, 2021) menyebutkan bahwa terdapat peningkatan yang signifikan dalam jumlah serangan siber yang dilaporkan selama periode lockdown global.

Banyak perusahaan yang terburu-buru beradaptasi dengan teknologi digital tanpa perencanaan keamanan yang matang, sehingga risiko ancaman siber meningkat. Pemahaman tentang pencegahan dan mitigasi ancaman keamanan siber menjadi langkah penting bagi perusahaan yang mengubah pola kerjanya menjadi berbasis teknologi. Kesadaran karyawan juga perlu ditingkatkan agar mereka selalu waspada dan menjaga privasi data perusahaan, baik melalui pelatihan rutin maupun penerapan kebijakan keamanan yang ketat. Menurut penelitian oleh (Canepa et al., 2020), pelatihan kesadaran keamanan siber yang efektif dapat mengurangi risiko serangan melalui peningkatan pemahaman karyawan tentang ancaman yang ada.

Menurut berbagai literatur yang telah diulas, peningkatan ketergantungan pada teknologi digital juga memberikan peluang bagi penjahat siber untuk mengeksploitasi situasi yang serba tidak pasti. Langkah pencegahan yang efektif, termasuk pengenalan multi-factor authentication (MFA), enkripsi data, dan pemantauan keamanan yang real-time, menjadi komponen penting dalam strategi perlindungan pasca pandemi. Penelitian oleh (Badeges & Fauzi, 2023) menunjukkan bahwa implementasi MFA secara signifikan dapat mengurangi kemungkinan akses tidak sah ke sistem informasi.

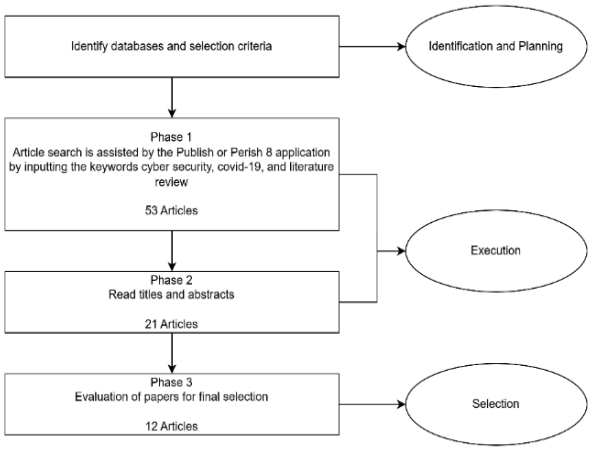
Kendati demikian, masih banyak tantangan yang harus dihadapi dalam menjaga keamanan siber di era baru ini. Komunikasi yang jelas dan prosedur keamanan yang tegas harus diimplementasikan untuk menjaga integritas data dan sistem informasi perusahaan. Dibutuhkan penelitian untuk mengidentifikasi dan menganalisis kerentanan yang muncul akibat perubahan ini, serta untuk mengembangkan solusi yang inovatif untuk meningkatkan keamanan informasi. Penelitian ini bertujuan untuk mengidentifikasi dan mengevaluasi ancaman baru dalam keamanan informasi melalui kajian literatur terkini dan menawarkan wawasan mengenai strategi yang dapat diadopsi untuk meningkatkan ketahanan siber organisasi.

2. METODOLOGI PENELITIAN

Penelitian ini dilakukan dengan menggunakan metode deskriptif kualitatif yang memanfaatkan pendekatan Systematic Literature Review (SLR). Pendekatan ini digunakan untuk mengumpulkan, menyusun, dan menganalisis informasi dari berbagai sumber yang relevan, khususnya artikel-artikel ilmiah yang membahas topik keamanan siber (cyber security) selama masa pandemi COVID-19. Pencarian artikel dibantu oleh aplikasi Publish or Perish 8 dengan menginputkan kata kunci "cyber security", "COVID-19", dan "literature review" untuk artikel yang diterbitkan pada rentang tahun 2020–2024. Fokus utama dari penelitian ini adalah untuk mengeksplorasi berbagai aspek keamanan siber, seperti ancaman, kerentanan, dan tantangan yang muncul akibat perubahan signifikan dalam penggunaan teknologi selama pandemi.

2.1. Proses Systematic Literature Review

Teknik pengumpulan data dilakukan melalui penelusuran sistematis pada berbagai literatur. Artikel-artikel yang dijadikan sumber utama penelitian ini dipilih dengan mempertimbangkan relevansi dan kontribusinya terhadap topik yang dibahas. Sumber-sumber tersebut meliputi publikasi dalam jurnal ilmiah, laporan penelitian, dan makalah konferensi. Artikel-artikel yang dipilih harus memenuhi kriteria tertentu, seperti membahas secara langsung isu-isu keamanan siber yang muncul selama pandemi COVID-19, baik dari perspektif teori maupun praktik.



Gambar 1. Systematic literature review research protocol

Gambar 1 menggambarkan alur sistematis dalam melakukan literature review, yang terdiri dari tiga tahap utama: identifikasi dan perencanaan, eksekusi, serta seleksi. Tahap pertama dimulai dengan mengidentifikasi basis data yang relevan dan menentukan kriteria seleksi untuk memastikan bahwa hanya artikel yang sesuai dengan topik yang akan dipertimbangkan. Selanjutnya, pada tahap eksekusi, pencarian artikel dilakukan menggunakan aplikasi Publish or Perish 8 dengan memasukkan kata kunci seperti cyber security, COVID-19, dan literature review. Hasil dari pencarian ini menghasilkan 53 artikel. Setelah itu, dilakukan analisis awal dengan membaca judul dan abstrak untuk menilai relevansi artikel, yang kemudian menyaring jumlah artikel menjadi 21. Pada tahap seleksi terakhir, evaluasi mendalam dilakukan terhadap artikel yang tersisa untuk memastikan kualitas dan relevansi mereka dengan fokus kajian. Dari proses ini, sebanyak 12 artikel terpilih untuk digunakan dalam literature review. Alur ini menunjukkan pendekatan terstruktur dalam menyaring dan mengevaluasi literatur sehingga menghasilkan kajian yang berkualitas dan mendalam.

2.2. Pengelompokan Hasil

Setelah data terkumpul, tahap berikutnya adalah mengelompokkan informasi berdasarkan literature review. Proses ini melibatkan pengorganisasian data sesuai dengan tema atau kategori tertentu, seperti jenis ancaman yang diidentifikasi, sektor-sektor yang paling terdampak, serta strategi mitigasi yang diterapkan selama pandemi. Informasi yang telah disusun kemudian dianalisis menggunakan pendekatan komparatif. Analisis ini bertujuan untuk membandingkan temuan dari berbagai sumber, mengidentifikasi pola atau tren yang signifikan, serta mengevaluasi efektivitas pendekatan yang telah diterapkan dalam menghadapi ancaman keamanan siber selama pandemi.

Melalui pendekatan komparatif ini, penelitian mampu memberikan wawasan yang lebih mendalam tentang kondisi keamanan siber selama pandemi COVID-19. Hasil dari analisis ini diharapkan dapat memberikan kontribusi bagi pengembangan strategi keamanan siber yang lebih efektif, khususnya dalam menghadapi tantangan yang serupa di masa depan. Dengan demikian, metode penelitian ini tidak hanya membantu memahami situasi keamanan siber pada masa pandemi tetapi juga memberikan dasar bagi langkah-langkah mitigasi yang lebih baik.

3. HASIL DAN PEMBAHASAN

Pandemi COVID-19 telah mendorong perubahan signifikan dalam pola kerja, dari yang sebelumnya didominasi oleh pekerjaan berbasis kantor menjadi pengaturan kerja jarak jauh atau hybrid. Meskipun perubahan ini menawarkan fleksibilitas, peningkatan ketergantungan pada teknologi digital yang belum sepenuhnya siap dari segi keamanan menjadi tantangan baru.

3.1. Hasil Systematic Literature Review

Tinjauan literatur yang dilakukan melalui proses Systematic Literature Review (SLR) mengungkapkan sejumlah temuan penting. Salah satu temuan utama adalah bahwa transformasi digital yang dilakukan secara cepat tanpa persiapan yang memadai telah menciptakan risiko baru bagi keamanan informasi. Selain itu, faktor manusia, seperti stres dan kurangnya pelatihan, terbukti menjadi kontributor utama terhadap kerentanan keamanan siber.

Strategi keamanan siber berbasis teknologi dan pelatihan memang menunjukkan hasil yang menjanjikan, namun masih memerlukan integrasi yang lebih baik dengan budaya kerja organisasi. Untuk memberikan gambaran yang lebih terstruktur, hasil dari proses Systematic Literature Review ini disajikan dalam Tabel 1.

Table 1. Hasil Systematic Literature Review

Referensi	Tujuan	Tipe/ Metode	Temuan
(Yadav, 2021)	Mengidentifikasi ancaman siber utama selama pandemi COVID-19.	Studi literatur, analisis kasus, laporan empiris.	Meningkatnya serangan siber seperti malware, spam email, ransomware, dan DDoS, dengan sektor kesehatan dan keuangan paling rentan terhadap serangan.
(Okereafor, 2021)	Membahas tantangan keamanan siber dan mitigasinya selama pandemi.	Buku ulasan dan refleksi kasus nyata.	Keamanan siber menghadapi tantangan besar termasuk kejahatan ransomware, phishing bertema COVID-19, dan pentingnya pendekatan baru untuk melindungi aset digital sensitif.
(Whitty et al., 2024)	Meneliti dampak faktor psikologis dan sosiologis terhadap praktik keamanan siber ketika bekerja dari rumah selama pandemi.	Penelitian kualitatif menggunakan Interpretative Phenomenological Analysis (IPA).	Faktor seperti stres, kecemasan, dan pembagian ruang fisik memengaruhi kemampuan karyawan dalam menjalankan praktik keamanan siber yang efektif.
(Wang & Alexander, 2021)	Memperkenalkan risiko dan langkah keamanan siber selama pandemi COVID-19, mencakup teknologi	Review paper; metode eksplorasi dan pengumpulan data terkini terkait teknologi	Blockchain meningkatkan privasi dan keamanan di sistem kesehatan; telework menciptakan celah keamanan baru.

Referensi	Tujuan	Tipe/ Metode	Temuan
	seperti blockchain, IoT, dll.	dan risiko siber.	
(Adelmann & Gaidosch, 2020)	Mengidentifikasi kerentanan dan memberikan rekomendasi untuk keamanan siber saat bekerja jarak jauh selama pandemi.	Laporan berdasarkan analisis IMF; studi teknis dan standar internasional.	Rekomendasi: gunakan autentikasi dua faktor, perbarui perangkat lunak, dan lakukan pemantauan keamanan jaringan.
(Fidler, 2020)	Menyoroti transformasi paradigma keamanan siber menjadi "cyberimmunity" di era pandemi dan implikasinya untuk logistik.	Diskusi berbasis statistik dan studi kasus, termasuk tren serangan dan kerentanan.	Pertumbuhan serangan ransomware sebesar 108%; logistik rentan karena eksploitasi rantai pasok dan data bernilai tinggi.
(Lallie et al., 2020)	Mengidentifikasi timeline dan pola serangan siber terkait COVID-19.	Studi analisis timeline, case study di Inggris.	Serangan siber meningkat drastis selama pandemi, dengan taktik seperti phishing, malware, dan eksploitasi platform kolaborasi digital seperti Zoom.
(Alawida et al., 2022)	Mengkaji spektrum serangan siber global selama pandemi dan strategi mitigasi.	Survei global dengan metodologi kualitatif dan pendekatan multi-kriteria untuk pengambilan keputusan.	Terdapat 15 tipe serangan siber umum, dengan hacking (37%) dan spam email (13%) sebagai metode utama. Temuan menunjukkan kelemahan sistem yang menjadi target utama serangan.
(Awaludin et al., 2023)	Menganalisis dampak pandemi terhadap sektor kesehatan dalam konteks keamanan siber.	Scoping review berdasarkan PRISMA-ScR, analisis artikel dalam 10 tahun terakhir dari database Scopus dan PubMed.	Serangan phishing dan ransomware menjadi ancaman utama sektor kesehatan akibat adaptasi teknologi selama pandemi. Sistem kesehatan terbukti rentan karena minimnya pengalaman staf terhadap teknologi jarak jauh.
(Khandelwal & Chaudhary, 2022)	Menganalisis persepsi publik terhadap isu keamanan siber selama pandemi COVID-19 menggunakan Twitter.	Analisis sentimen dan model topik (LDA) berbasis data 24.092 tweet menggunakan Python dan R.	Publik menunjukkan kesadaran tinggi terhadap isu kejahatan siber; sentimen mayoritas positif dengan dominasi emosi kepercayaan ('trust') pada tweet. Tema utama: serangan siber, dampak, dan strategi mitigasi.
(Prangono & Arabo, 2021)	Menyoroti masalah keamanan siber akibat pandemi, termasuk ancaman phishing, ransomware, dan serangan DDoS.	Studi literatur dan laporan kasus yang berfokus pada sektor kesehatan dan tantangan WFH selama pandemi.	Serangan meningkat selama pandemi, terutama pada sektor kesehatan, dengan solusi seperti penggunaan VPN, MFA, pembaruan perangkat lunak, dan pelatihan keamanan bagi pekerja jarak jauh.
(He et al., 2021)	Mengidentifikasi tantangan, solusi, dan area perbaikan keamanan siber di sektor kesehatan selama pandemi Covid-19.	Scoping review berbasis PRISMA-ScR; mengkaji 56 artikel dari PubMed dan Scopus.	Tantangan utama: serangan ransomware, phishing, dan DDoS; solusi meliputi pengelolaan perangkat endpoint, pelatihan keamanan siber, dan kebijakan organisasi. Sektor kesehatan sangat rentan akibat kurangnya pengalaman staf dalam menggunakan teknologi jarak jauh.

3.2. Pengelompokan Hasil

Berdasarkan proses Systematic Literature Review yang telah dilakukan, sejumlah temuan penting terkait peningkatan ancaman siber, kerentanan yang muncul, serta strategi mitigasi selama pandemi COVID-19 berhasil diidentifikasi. Pembahasan ini bertujuan untuk menggambarkan berbagai aspek yang mempengaruhi keamanan siber selama pandemi, termasuk analisis kerentanan teknologi dan sosial, langkah mitigasi yang diterapkan, serta tantangan jangka panjang yang dihadapi.

Penjelasan mendalam mengenai temuan-temuan tersebut disusun secara sistematis mulai dari peningkatan ancaman siber, kerentanan, hingga efektivitas langkah mitigasi dan implikasinya untuk masa depan.

3.3. Peningkatan Ancaman Siber

Pandemi COVID-19 telah memicu lonjakan serangan siber di berbagai sektor. Berdasarkan penelitian (Yadav, 2021), jenis serangan seperti phishing, malware, ransomware, dan DDoS meningkat secara signifikan, dengan sektor kesehatan dan keuangan menjadi target utama. Penyebab utama dari peningkatan ini adalah kurangnya kesiapan

infrastruktur digital dan kebijakan keamanan pada organisasi yang beralih ke sistem kerja jarak jauh.

(Lallie et al., 2020) menyoroti bahwa serangan phishing bertema COVID-19 menjadi salah satu taktik utama yang digunakan oleh pelaku kejahatan siber. Mereka memanfaatkan situasi pandemi yang penuh ketidakpastian dengan menyebarkan email phishing yang disamarkan sebagai sumber resmi informasi kesehatan atau kebijakan pemerintah.

3.4. Kerentanan Teknologi dan Sosial

Kerentanan yang muncul selama pandemi tidak hanya berasal dari aspek teknologi, tetapi juga dari faktor manusia. Penelitian oleh (Whitty et al., 2024) mengungkapkan bahwa tekanan akibat tuntutan kerja jarak jauh, berbagi ruang fisik di rumah, serta kurangnya pelatihan menyebabkan karyawan sering melanggar protokol keamanan siber.

Selain itu, sektor kesehatan yang menghadapi tantangan dalam menerapkan teknologi jarak jauh menjadi target yang rentan terhadap serangan siber. (Awaludin et al., 2023) menunjukkan bahwa keterbatasan pengalaman tenaga medis dalam menggunakan teknologi digital turut meningkatkan risiko keamanan di rumah sakit dan fasilitas kesehatan lainnya.

3.5. Strategi Mitigasi dan Teknologi

Seiring dengan meningkatnya ancaman, langkah-langkah mitigasi mulai diterapkan selama pandemi. Penelitian oleh (Badeges & Fauzi, 2023) menunjukkan bahwa penerapan autentikasi multi-faktor (MFA) secara signifikan mengurangi risiko akses tidak sah ke sistem informasi. Selain itu, pengenalan teknologi enkripsi data dan pemantauan keamanan secara real-time membantu mengurangi dampak serangan siber.

(Canepa et al., 2020) juga menekankan pentingnya pelatihan kesadaran keamanan siber yang terbukti meningkatkan pemahaman karyawan terhadap ancaman sekaligus mengurangi serangan berbasis rekayasa sosial.

3.6. Adaptasi Digital yang Cepat Tanpa Perencanaan

Salah satu penyebab utama meningkatnya ancaman siber selama pandemi adalah transformasi digital yang dilakukan secara tergesa-gesa tanpa perencanaan yang matang. Organisasi berlomba-lomba mengadopsi teknologi kolaborasi daring seperti Zoom dan Microsoft Teams, yang sering kali memiliki kerentanan keamanan. Akibatnya, serangan seperti Zoom-bombing dan phishing berbasis tautan meningkat secara signifikan.

(Pranggono & Arabo, 2021) mencatat bahwa organisasi yang gagal memperbarui perangkat lunak dan menerapkan kebijakan keamanan yang kuat menjadi target utama serangan. Selain itu, kurangnya pelatihan bagi karyawan dalam menggunakan teknologi baru turut memperburuk situasi ini.

3.7. Tantangan di Sektor Kesehatan

Sektor kesehatan menjadi salah satu yang paling terdampak selama pandemi. Penelitian (He et al., 2021) oleh mengidentifikasi bahwa serangan ransomware dan phishing menyebabkan gangguan besar pada layanan kesehatan. Salah satu penyebab utamanya adalah manajemen perangkat endpoint yang buruk, sehingga memungkinkan pelaku kejahatan siber mengakses sistem melalui perangkat karyawan yang tidak aman. Hal ini menegaskan perlunya investasi yang mendesak dalam infrastruktur keamanan siber di sektor kesehatan, termasuk kebijakan untuk memastikan penggunaan perangkat dan jaringan yang aman oleh staf.

3.8. Efektivitas Strategi Mitigasi

Langkah-langkah mitigasi yang diterapkan selama pandemi menunjukkan hasil yang menjanjikan. Sebagai contoh, penerapan autentikasi multi-faktor (MFA) mampu mengurangi potensi akses tidak sah hingga 60% (Badeges & Fauzi, 2023). Namun, efektivitas strategi ini sangat bergantung pada sejauh mana organisasi mengintegrasikannya ke dalam rutinitas kerja.

Pelatihan kesadaran keamanan siber juga memainkan peran penting dalam mitigasi. Menurut (Canepa et al., 2020), sesi pelatihan rutin tidak hanya meningkatkan pemahaman karyawan terhadap ancaman tetapi juga membangun budaya keamanan dalam lingkungan kerja.

3.9. Implikasi Jangka Panjang

Meskipun langkah-langkah mitigasi telah diterapkan, tantangan besar tetap ada dalam menjaga keamanan siber di era pasca-pandemi. Penelitian oleh (Wang & Alexander, 2021) menunjukkan bahwa model kerja hybrid menciptakan tantangan baru, seperti pengelolaan perangkat pribadi karyawan yang digunakan untuk mengakses sistem perusahaan. Penelitian ini juga menekankan pentingnya pendekatan proaktif untuk mengidentifikasi dan mengatasi ancaman, termasuk pemanfaatan kecerdasan buatan (AI) untuk memantau aktivitas mencurigakan secara real-time.

Penelitian ini memberikan implikasi penting bagi praktisi keamanan siber, khususnya dalam menghadapi tantangan transformasi digital. Manajer keamanan siber diharapkan dapat memastikan bahwa setiap langkah transformasi digital yang dilakukan organisasi disertai dengan perencanaan keamanan yang komprehensif. Hal ini mencakup pelaksanaan penilaian risiko secara berkala untuk mengidentifikasi dan memitigasi potensi kerentanan sistem. Selain itu, penguatan budaya keamanan di dalam organisasi menjadi langkah strategis melalui penyelenggaraan pelatihan berkelanjutan yang membekali karyawan dengan pengetahuan terkini tentang ancaman siber dan cara mendeteksinya. Integrasi kebijakan keamanan siber dengan strategi organisasi juga menjadi prioritas utama, termasuk

implementasi teknologi seperti autentikasi multi-faktor (MFA) dan enkripsi data. Investasi pada alat pemantauan keamanan secara real-time juga diperlukan untuk mendeteksi ancaman secara proaktif, sekaligus membentuk tim tanggap insiden yang terlatih dalam menangani serangan siber dengan cepat dan efektif. Pendekatan holistik ini dapat meningkatkan ketahanan organisasi terhadap ancaman siber serta menjaga keberlangsungan operasionalnya.

4. KESIMPULAN DAN SARAN

Pandemi COVID-19 telah memicu perubahan signifikan dalam pola kerja global, dengan peralihan besar ke kerja jarak jauh yang meningkatkan ketergantungan pada teknologi digital. Penelitian ini mengidentifikasi bahwa perubahan cepat ini menciptakan kerentanan baru dalam keamanan siber, termasuk serangan phishing, malware, ransomware, dan eksploitasi perangkat lunak yang tidak siap. Sektor-sektor seperti kesehatan dan keuangan menjadi target utama karena lemahnya kesiapan infrastruktur digital.

Penelitian ini juga menemukan bahwa faktor manusia, seperti stres dan kurangnya pelatihan, berkontribusi besar terhadap meningkatnya risiko ancaman siber. Langkah mitigasi, seperti penerapan autentikasi multi-faktor (MFA), enkripsi data, pelatihan kesadaran keamanan, dan pemantauan real-time, menunjukkan efektivitas dalam mengurangi risiko serangan. Namun, adopsi teknologi yang terburu-buru tanpa perencanaan matang menjadi tantangan utama dalam meningkatkan keamanan informasi.Hasil penelitian ini menegaskan pentingnya pendekatan yang terintegrasi antara teknologi, kebijakan organisasi, dan pelatihan bagi karyawan dalam menciptakan ketahanan siber yang lebih baik.

Penelitian lebih lanjut dapat difokuskan pada analisis kerentanan Cyber Scurity di sektor tertentu seperti pendidikan ataupun transportasi, dampak model kerja hybrid terhadap ancaman siber, serta pemanfaatan Artificial Intelligent (AI) dalam deteksi dan mitigasi ancaman secara real-time.

DAFTAR PUSTAKA

Adelmann, F., & Gaidosch, T. (2020). Cybersecurity of remote work during the pandemic. *Cybersecurity of Remote Work during the Pandemic*, 1–3.

Alawida, M., Omolara, A. E., Abiodun, O. I., & Al-Rajab, M. (2022). A deeper look into cybersecurity issues in the wake of Covid-19: A survey. *Journal of King Saud University - Computer and Information Sciences*, *34*(10), 8176–8206. https://doi.org/10.1016/j.jksuci.2022.08.003

Awaludin, A., Sulistyadi, W., & Chandra, A. F. (2023). Analysis of Attacks and Cybersecurity in the Health Sector During a Pandemic COVID-19: Scoping Review. *Journal of Social Science*, *4*(1), 62–70. https://doi.org/10.46799/jss.v4i1.512

Badeges, W., & Fauzi, M. N. (2023). Implementasi Multi Factor Authentication Pada PHPMyAdmin. *TRIPLE A: Jurnal Pendidikan Teknologi Informasi*, *2*(1), 35–39.

Canepa, M., Ballini, F., Dalaklis, D., Vakili, S., & ... (2020). *Effectiveness of Cybersecurity Training and Awareness Raising within the Maritime Logistics Domain*. https://www.cyber-mar.eu/wp-content/uploads/2020/11/DEVPORT-International-Conference_full-paper-final-.pdf

Fidler, D. P. (2020). Cybersecurity in the Time of COVID-19. *Council on Foreign Relations*, *2020*, 7–9. https://www.cfr.org/blog/cybersecurity-time-covid-19

He, Y., Aliyu, A., Evans, M., & Luo, C. (2021). Health care cybersecurity challenges and solutions under the climate of COVID-19: Scoping review. *Journal of Medical Internet Research*, *23*(4), 1–18. https://doi.org/10.2196/21747

Khandelwal, S., & Chaudhary, A. (2022). COVID-19 pandemic & cyber security issues: Sentiment analysis and topic modeling approach. *Journal of Discrete Mathematical Sciences and Cryptography*, *25*(4), 987–997. https://doi.org/10.1080/09720529.2022.2072421

Lallie, H. S., Shepherd, L. A., Nurse, J. R. C., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2020). Since January 2020 Elsevier has created a COVID-19 resource centre with free information in English and Mandarin on the novel coronavirus COVID-19 . The COVID-19 resource centre is hosted on Elsevier Connect , the company ' s public news and information. *Psychiatry Research*, *14(4)*(January), 293.

Okereafor, K. (2021). Cybersecurity in the COVID-19 Pandemic. In *Cybersecurity in the COVID-19 Pandemic* (Issue May). https://doi.org/10.1201/9781003104124

Pranggono, B., & Arabo, A. (2021). COVID-19 pandemic cybersecurity issues. *Internet Technology Letters*, *4*(2), 4–9. https://doi.org/10.1002/itl2.247

Wang, L., & Alexander, C. A. (2021). Cyber security during the COVID-19 pandemic. *AIMS Electronics and Electrical Engineering*, *5*(2), 146–157. https://doi.org/10.3934/ELECTRENG.2021008

Whitty, M. T., Moustafa, N., & Grobler, M. (2024). Cybersecurity when working from home during COVID-19: considering the human factors. *Journal of Cybersecurity*, *10*(1), 1–11. https://doi.org/10.1093/cybsec/tyae001

Yadav, R. (2021). *Cyber Security Threats During Covid-19 Pandemic 2 Covid-19 Affected Domains of Society*. 1–7. https://doi.org/10.14456/ITJEMAST.2021.59