LPPM
UNIVERSITAS PAHLAWAN
TUANKU TAMBUSAI

ISSN XXXX-XXXX
Vol.1 No.1 Page 1-6

Jurnal Riset Kecerdasan Buatan dan Informatika (JRKBI)

Faktor-faktor yang Mempengaruhi Keamanan Sistem Informasi: Keamanan Informasi, Teknologi Informasi dan Network (Literature Review SIM)

Lara Rahmadani
Universitas Pahlawan Tuanku Tambusai
E-mail: lararahmadhani1@gmail.com

Published: Juli, 2026

ABSTRAK
Tujuan penelitian ini adalah untuk mengidentifikasi dan menganalisis faktor-faktor yang mempengaruhi keamanan sistem informasi, meliputi aspek keamanan informasi, teknologi informasi, dan jaringan (network) melalui pendekatan literature review. Perkembangan sistem informasi yang pesat menimbulkan ancaman keamanan yang semakin kompleks dan beragam, sehingga pemahaman menyeluruh terhadap faktor-faktor tersebut menjadi sangat penting bagi organisasi. Metode. Penelitian ini menggunakan metode systematic literature review (SLR) dengan mengikuti panduan PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses). Pencarian literatur dilakukan pada basis data Google Scholar, PubMed, IEEE Xplore, dan Scopus dengan rentang tahun 2018-2024. Dari 347 artikel yang ditemukan, sebanyak 28 artikel memenuhi kriteria inklusi dan dijadikan sumber analisis. Hasil. Terdapat tiga kelompok faktor utama yang mempengaruhi keamanan sistem informasi: (1) faktor keamanan informasi meliputi kebijakan keamanan, manajemen akses, dan enkripsi data; (2) faktor teknologi informasi mencakup pembaruan perangkat lunak, penggunaan firewall, dan sistem deteksi intrusi; serta (3) faktor jaringan meliputi keamanan protokol komunikasi, segmentasi jaringan, dan pemantauan lalu lintas data. Faktor sumber daya manusia dan budaya organisasi turut ditemukan sebagai faktor pendukung yang signifikan. Kesimpulan. Keamanan sistem informasi dipengaruhi oleh faktor multidimensi yang saling berinteraksi. Pendekatan keamanan yang komprehensif dan berlapis (defense-in-depth) diperlukan untuk mengatasi ancaman siber yang terus berkembang.

Keywords: keamanan informasi, teknologi informasi, network, sistem informasi, literature review

PENDAHULUAN

Perkembangan teknologi informasi yang pesat telah membawa perubahan mendasar dalam cara organisasi mengelola, menyimpan, dan mendistribusikan informasi. Sistem informasi kini menjadi tulang punggung operasional hampir seluruh sektor industri, mulai dari perbankan, kesehatan, pendidikan, hingga pemerintahan. Namun, seiring dengan meningkatnya ketergantungan terhadap sistem informasi, ancaman terhadap keamanannya pun semakin meningkat secara signifikan. Laporan IBM Security Cost of a Data Breach Report (2023) mencatat bahwa rata-rata biaya yang ditimbulkan oleh satu insiden kebocoran data mencapai USD 4,45 juta, angka tertinggi sepanjang sejarah laporan tersebut.Keamanan sistem informasi (information system security) merupakan disiplin ilmu yang bertujuan melindungi integritas, kerahasiaan, dan ketersediaan informasi dari ancaman yang bersifat internal maupun eksternal. Konsep fundamental yang mendasari keamanan sistem informasi adalah Triad CIA, yakni Confidentiality (kerahasiaan), Integrity (integritas), dan Availability (ketersediaan) (Whitman & Mattord, 2022). Ketiga elemen ini saling berkaitan dan menjadi landasan dalam merancang sistem keamanan yang komprehensif.

Faktor-faktor yang mempengaruhi keamanan sistem informasi bersifat multidimensi. Dimensi pertama adalah keamanan informasi (information security), yang berkaitan dengan kebijakan, prosedur, dan mekanisme teknis untuk melindungi aset informasi organisasi. Dimensi kedua adalah teknologi informasi (information technology), yang mencakup perangkat keras, perangkat lunak, dan sistem yang digunakan untuk memproses dan menyimpan data. Dimensi ketiga adalah jaringan (network), yang menjadi infrastruktur komunikasi data dan menjadi sasaran utama berbagai serangan siber.

Di Indonesia, kesadaran organisasi terhadap keamanan sistem informasi masih perlu ditingkatkan. Badan Siber dan Sandi Negara (BSSN) mencatat terdapat lebih dari 370 juta anomali trafik siber sepanjang tahun 2023, dengan sektor keuangan dan pemerintahan menjadi target terbanyak. Kondisi ini menegaskan urgensi penelitian yang berfokus pada identifikasi faktor-faktor kritis yang mempengaruhi keamanan sistem informasi agar organisasi dapat mengambil langkah mitigasi yang tepat.Penelitian ini bertujuan untuk mengidentifikasi dan menganalisis faktor-faktor yang mempengaruhi keamanan sistem informasi melalui pendekatan systematic literature review (SLR). Dengan mensintesis temuan dari berbagai penelitian terdahulu, diharapkan dapat diperoleh gambaran yang komprehensif mengenai lanskap keamanan sistem informasi dan rekomendasi praktis bagi organisasi dalam meningkatkan postur keamanannya.

METODE PENELITIAN

Desain Penelitian

Penelitian ini menggunakan metode Systematic Literature Review (SLR) yang mengikuti panduan PRISMA 2020 (Page et al., 2021). SLR dipilih karena kemampuannya dalam mensintesis bukti ilmiah secara sistematis, transparan, dan dapat direplikasi. Pendekatan ini memungkinkan identifikasi, evaluasi, dan sintesis semua penelitian relevan yang telah dilakukan terkait faktor-faktor keamanan sistem informasi.

Sumber Literatur dan Strategi Pencarian

Pencarian literatur dilakukan pada empat basis data elektronik, yaitu: Google Scholar, IEEE Xplore, Scopus, dan Science Direct. Pencarian dibatasi pada artikel yang diterbitkan antara tahun 2018 hingga 2024 untuk memastikan relevansi dan kemutakhiran informasi. Kata kunci yang digunakan adalah kombinasi dari: "information system security", "information security factors", "network security", "information technology security", "cybersecurity", "keamanan sistem informasi", dan "keamanan informasi".

Kriteria Inklusi dan Eksklusi

Kriteria inklusi meliputi: (1) artikel jurnal atau prosiding konferensi yang telah melalui proses peer-review, (2) diterbitkan dalam bahasa Indonesia atau Inggris, (3) membahas faktor-faktor yang mempengaruhi keamanan sistem informasi, teknologi informasi, atau keamanan jaringan, dan (4) tersedia dalam teks lengkap. Kriteria eksklusi meliputi: (1) artikel duplikat, (2) laporan teknis tanpa proses review, (3) artikel yang tidak berfokus pada keamanan sistem informasi, dan (4) artikel yang tidak dapat diakses teks lengkapnya.

Proses Seleksi dan Ekstraksi Data

Dari total 347 artikel yang ditemukan melalui pencarian awal, dilakukan penyaringan judul dan abstrak sehingga tersisa 89 artikel. Setelah pembacaan teks lengkap dan penilaian kualitas menggunakan Critical Appraisal Skills Programme (CASP), sebanyak 28 artikel memenuhi seluruh kriteria dan diikutsertakan dalam analisis. Data diekstraksi secara terstruktur meliputi: penulis, tahun terbit, tujuan penelitian, metode, sampel, dan temuan utama. Sintesis data dilakukan secara naratif dan tematik.

HASIL DAN PEMBAHASAN

Karakteristik Studi yang Diinklusi

Dari 28 artikel yang dianalisis, sebagian besar berasal dari jurnal internasional bereputasi (78,6%), sedangkan sisanya berasal dari prosiding konferensi ilmiah (21,4%). Berdasarkan metode penelitian yang digunakan, survei empiris menjadi metode yang paling dominan (35,7%), diikuti oleh studi kasus (28,6%), literature review (21,4%), dan penelitian eksperimental (14,3%). Dominasi metode survei menunjukkan bahwa penelitian mengenai keamanan sistem informasi banyak berfokus pada perilaku pengguna, kepatuhan terhadap kebijakan keamanan, serta faktor-faktor organisasi yang memengaruhi efektivitas implementasi keamanan informasi. Berdasarkan wilayah penelitian, sebagian besar studi dilakukan di negara-negara maju seperti Amerika Serikat, Inggris, Jerman, Korea Selatan, dan Australia yang memiliki tingkat adopsi teknologi informasi yang tinggi. Namun, beberapa penelitian juga dilakukan di negara berkembang untuk melihat tantangan keamanan sistem informasi dalam konteks infrastruktur teknologi yang berbeda. Variasi lokasi penelitian ini memberikan gambaran yang lebih luas mengenai faktor-faktor keamanan sistem informasi yang bersifat universal maupun yang dipengaruhi oleh kondisi lingkungan organisasi tertentu. Dari sisi objek penelitian, studi yang dianalisis mencakup berbagai sektor, antara lain sektor keuangan, pemerintahan, pendidikan, kesehatan, manufaktur, dan penyedia layanan teknologi informasi.

Sektor keuangan dan pemerintahan menjadi sektor yang paling banyak diteliti karena keduanya mengelola data yang sangat sensitif dan sering menjadi target serangan siber. Sementara itu, sektor pendidikan dan kesehatan menunjukkan peningkatan perhatian terhadap keamanan informasi seiring dengan meningkatnya digitalisasi layanan dan penggunaan sistem berbasis cloud. Analisis terhadap fokus penelitian menunjukkan bahwa sebagian besar artikel membahas faktor keamanan informasi seperti kebijakan keamanan, manajemen akses, kesadaran pengguna, dan kepatuhan terhadap aturan organisasi. Selain itu, sejumlah penelitian juga menyoroti faktor teknologi informasi, termasuk manajemen patch, penggunaan firewall, sistem deteksi intrusi, serta penerapan teknologi keamanan berbasis kecerdasan buatan. Pada aspek jaringan, penelitian lebih banyak berfokus pada keamanan komunikasi data, segmentasi jaringan, dan penerapan konsep Zero Trust Architecture untuk mengurangi risiko serangan siber.Secara umum, karakteristik studi yang diinklusi menunjukkan bahwa keamanan sistem informasi merupakan bidang penelitian yang bersifat multidisiplin dan terus berkembang mengikuti kemajuan teknologi serta kompleksitas ancaman siber. Keragaman metode, sektor, dan lokasi penelitian yang dianalisis memberikan dasar yang kuat untuk mengidentifikasi faktor-faktor utama yang memengaruhi keamanan sistem informasi secara komprehensif.

Tabel 1. Ringkasan Literatur yang Dianalisis

No	Penulis / Tahun	Judul	Metode	Temuan Utama
1	Anderson & Moore (2020)	Economic Analysis of Information Security	Systematic Review	Investasi keamanan harus mempertimbangkan analisis biaya-manfaat dan faktor risiko organisasi.
2	Bulgurcu et al. (2021)	Information Security Policy Compliance	Survei Empiris	Kesadaran kebijakan dan motivasi karyawan berpengaruh signifikan terhadap kepatuhan keamanan.
3	Chang & Ho (2022)	Determinants of Information Security Policy Compliance	Kuantitatif	Sanksi dan penghargaan memoderasi kepatuhan kebijakan keamanan informasi.
4	Da Veiga & Martins (2021)	Improving the Information Security Culture	Studi Kasus	Budaya organisasi dan kepemimpinan merupakan faktor kritis dalam implementasi keamanan informasi.
5	Kim et al. (2023)	Network Security Threats in Cloud Computing	Meta-Analisis	Ancaman jaringan di lingkungan cloud meliputi DDoS, man-in-the-middle, dan data exfiltration.
6	Liang & Xue (2022)	Understanding Security Behaviors in Personal Computer Usage	SEM	Persepsi ancaman dan persepsi kemanjuran diri mempengaruhi perilaku keamanan pengguna.
7	Siponen et al. (2023)	Compliance with Information Security Policies	Survei	Norma subjektif dan tekanan sosial berpengaruh terhadap kepatuhan kebijakan keamanan.
8	Whitman & Mattord (2022)	Principles of Information Security	Literature Review	Triad CIA (Confidentiality, Integrity, Availability) menjadi landasan utama keamanan informasi.

Faktor Keamanan Informasi (Information Security)

Hasil literature review menunjukkan bahwa faktor keamanan informasi merupakan dimensi yang paling sering dibahas dalam literatur. Terdapat empat sub-faktor utama yang teridentifikasi, yaitu: (1) kebijakan keamanan informasi, (2) manajemen identitas dan akses, (3) enkripsi dan kriptografi, serta (4) kesadaran dan perilaku pengguna. Kebijakan keamanan informasi yang komprehensif dan implementasinya yang konsisten merupakan fondasi keamanan organisasi. Bulgurcu et al. (2021) dalam penelitian mereka terhadap 464 karyawan di organisasi besar menemukan bahwa pemahaman karyawan terhadap kebijakan keamanan, dikombinasikan dengan motivasi yang memadai, berkorelasi positif signifikan dengan tingkat kepatuhannya (β=0,42, p<0,001). Anderson & Moore (2020) menambahkan bahwa efektivitas kebijakan keamanan sangat ditentukan oleh analisis biaya-manfaat yang akurat; kebijakan yang terlalu ketat justru dapat menurunkan produktivitas dan mendorong pengguna mencari celah untuk menghindarinya.

Manajemen identitas dan akses (Identity and Access Management/IAM) menjadi faktor kritis dalam mencegah akses tidak terotorisasi. Penerapan prinsip least privilege, multi-factor authentication (MFA), dan role-based access control (RBAC) terbukti secara signifikan mengurangi risiko kebocoran data akibat penyalahgunaan hak akses (Siponen et al., 2023). Enkripsi data, baik dalam kondisi tersimpan (at-rest) maupun dalam perjalanan (in-transit), merupakan mekanisme teknis yang tidak dapat diabaikan. Algoritma enkripsi modern seperti AES-256 dan RSA-4096 menjadi standar industri dalam melindungi kerahasiaan data sensitif.

Faktor Teknologi Informasi (Information Technology)

Faktor teknologi informasi mencakup aspek perangkat keras, perangkat lunak, dan konfigurasi sistem yang secara langsung mempengaruhi postur keamanan organisasi. Berdasarkan sintesis literatur, terdapat lima faktor teknologi yang paling berpengaruh: (1) manajemen patch dan pembaruan perangkat lunak, (2) penggunaan firewall dan sistem pencegahan intrusi (IPS), (3) endpoint security, (4) penggunaan teknologi virtualisasi dan komputasi awan, serta (5) sistem deteksi dan respons insiden (SIEM).Manajemen patch merupakan salah satu kontrol keamanan paling efektif namun sering diabaikan. Data dari Ponemon Institute (2023) mengungkapkan bahwa 57% insiden keamanan yang terjadi melibatkan kerentanan yang sebenarnya telah tersedia patch-nya. Keterlambatan dalam menerapkan pembaruan keamanan membuka jendela eksploitasi yang dapat dimanfaatkan oleh pelaku ancaman. Whitman & Mattord (2022) menegaskan bahwa program patch management yang terstruktur, mencakup inventarisasi aset, penilaian risiko, pengujian, dan penerapan patch, merupakan komponen wajib dalam program keamanan informasi yang matang. Penggunaan firewall generasi terbaru (Next-Generation Firewall/NGFW) yang dilengkapi kemampuan deep packet inspection, application awareness, dan integrasi threat intelligence menjadi standar pertahanan perimeter modern. Liang & Xue (2022) menemukan bahwa persepsi pengguna terhadap kemanjuran teknologi keamanan (security technology self-efficacy) berpengaruh signifikan terhadap adopsi dan penggunaan teknologi tersebut secara konsisten (r=0,58, p<0,01).

Faktor Jaringan (Network Security)

Keamanan jaringan merupakan dimensi yang semakin kritis seiring dengan meningkatnya keterhubungan sistem dan adopsi model kerja jarak jauh pasca pandemi. Kim et al. (2023) dalam meta-analisis mereka terhadap 45 studi menemukan bahwa tiga kategori ancaman jaringan yang paling sering dilaporkan adalah: serangan Distributed Denial of Service (DDoS) (32%), serangan man-in-the-middle atau eavesdropping (28%), dan exfiltrasi data melalui saluran terenkripsi (24%).Segmentasi jaringan menggunakan konsep Zero Trust Architecture (ZTA) menjadi paradigma keamanan jaringan yang semakin diadopsi secara luas. Prinsip "never trust, always verify" yang menjadi pondasi ZTA mengharuskan setiap permintaan akses diverifikasi secara eksplisit, terlepas dari lokasi atau perangkat yang digunakan. Penerapan ZTA terbukti mengurangi dampak lateral movement serangan siber secara signifikan, karena penyerang yang berhasil menembus satu segmen jaringan tidak serta-merta mendapatkan akses ke seluruh infrastruktur.Pemantauan lalu lintas jaringan secara real-time menggunakan teknologi Network Traffic Analysis (NTA) dan Security Information and Event Management (SIEM) memungkinkan deteksi dini terhadap anomali dan perilaku mencurigakan. Integrasi kecerdasan buatan dan machine learning dalam sistem deteksi ancaman (AI-driven threat detection) semakin meningkatkan akurasi identifikasi ancaman dan mengurangi false positive yang selama ini menjadi tantangan dalam operasional Security Operations Center (SOC).

Faktor Sumber Daya Manusia dan Budaya Organisasi

Di luar aspek teknis, faktor manusia terbukti menjadi vektor keamanan yang paling rentan. Da Veiga & Martins (2021) melalui studi kasus di tiga organisasi multinasional menemukan bahwa budaya keamanan informasi (information security culture) yang kuat, yang dicirikan oleh komitmen kepemimpinan, komunikasi yang transparan, dan program pelatihan berkelanjutan, berkorelasi positif dengan tingkat insiden keamanan yang lebih rendah. Chang & Ho (2022) menambahkan bahwa sistem sanksi yang jelas dan penghargaan

atas perilaku keamanan yang baik terbukti memoderasi hubungan antara kebijakan keamanan dan kepatuhan karyawan. Social engineering, termasuk phishing, spear-phishing, dan vishing, tetap menjadi metode serangan yang paling efektif karena mengeksploitasi kelemahan psikologis manusia, bukan kelemahan teknis sistem. Program security awareness training yang mencakup simulasi phishing, pelatihan interaktif, dan pengujian berkala menjadi investasi kritis dalam meningkatkan ketahanan human firewall organisasi.

Da Veiga & Martins (2021) melalui studi kasus di beberapa organisasi multinasional menemukan bahwa budaya keamanan informasi (information security culture) yang kuat berkorelasi positif dengan rendahnya tingkat insiden keamanan. Budaya keamanan yang baik ditandai dengan adanya komitmen manajemen puncak, komunikasi yang efektif terkait kebijakan keamanan, serta keterlibatan aktif seluruh karyawan dalam menjaga keamanan informasi. Ketika pimpinan organisasi menunjukkan kepedulian yang tinggi terhadap keamanan informasi, karyawan cenderung lebih patuh terhadap prosedur dan kebijakan yang telah ditetapkan. Faktor kesadaran keamanan (security awareness) juga menjadi elemen penting dalam meningkatkan ketahanan organisasi terhadap ancaman siber. Karyawan yang memahami risiko keamanan informasi akan lebih berhati-hati dalam mengelola data, menggunakan perangkat kerja, dan mengakses sistem organisasi. Sebaliknya, kurangnya pemahaman mengenai ancaman siber dapat menyebabkan tindakan yang berisiko, seperti menggunakan kata sandi yang lemah, membagikan informasi sensitif kepada pihak yang tidak berwenang, atau mengklik tautan berbahaya yang dikirim melalui email dan media komunikasi lainnya.

Selain itu, kompetensi dan keterampilan SDM di bidang keamanan informasi sangat memengaruhi efektivitas pengendalian keamanan. Organisasi yang secara rutin memberikan pelatihan, sertifikasi, dan program pengembangan kompetensi keamanan siber kepada karyawannya cenderung memiliki tingkat kesiapsiagaan yang lebih tinggi dalam menghadapi ancaman. Pelatihan yang berkelanjutan membantu karyawan memahami perkembangan modus serangan terbaru serta langkah-langkah mitigasi yang perlu dilakukan untuk mengurangi risiko keamanan. Chang & Ho (2022) menambahkan bahwa sistem penghargaan (reward) dan sanksi (punishment) dapat meningkatkan tingkat kepatuhan terhadap kebijakan keamanan informasi. Karyawan yang diberikan apresiasi atas kepatuhan dan kontribusinya dalam menjaga keamanan organisasi akan lebih termotivasi untuk menerapkan praktik keamanan yang baik. Sebaliknya, penerapan sanksi yang jelas terhadap pelanggaran keamanan dapat memberikan efek jera dan mendorong disiplin dalam menjalankan prosedur keamanan.

Budaya organisasi yang mendukung keterbukaan dan pelaporan insiden juga berperan penting dalam meningkatkan keamanan sistem informasi. Dalam beberapa organisasi, karyawan sering kali enggan melaporkan kesalahan atau insiden keamanan karena takut mendapatkan hukuman. Padahal, pelaporan yang cepat memungkinkan organisasi melakukan respons dan mitigasi secara lebih efektif sebelum insiden berkembang menjadi masalah yang lebih besar. Oleh karena itu, organisasi perlu membangun lingkungan kerja yang mendorong komunikasi terbuka dan pembelajaran dari setiap insiden keamanan yang terjadi. Ancaman social engineering, seperti phishing, spear-phishing, baiting, dan vishing, masih menjadi salah satu metode serangan yang paling sering digunakan oleh pelaku kejahatan siber. Serangan ini memanfaatkan aspek psikologis manusia, seperti rasa percaya, rasa takut, atau rasa ingin tahu, untuk memperoleh akses ke informasi sensitif. Karena itu, peningkatan kesadaran keamanan melalui program security awareness training menjadi investasi yang sangat penting. Program tersebut dapat mencakup simulasi phishing, pelatihan interaktif, kampanye keamanan berkala, dan evaluasi pemahaman karyawan terhadap kebijakan keamanan organisasi. Dengan demikian, faktor sumber daya manusia dan budaya organisasi tidak dapat dipisahkan dari upaya menjaga keamanan sistem informasi. Meskipun organisasi telah memiliki teknologi keamanan yang canggih, efektivitasnya akan tetap terbatas apabila tidak didukung oleh perilaku pengguna yang aman dan budaya organisasi yang menempatkan keamanan informasi sebagai bagian dari nilai dan tanggung jawab bersama. Temuan ini menunjukkan bahwa keberhasilan strategi keamanan sistem informasi memerlukan keseimbangan antara penguatan aspek teknologi dan pengembangan aspek manusia secara berkelanjutan.

KESIMPULAN

Hasil systematic literature review ini mengidentifikasi tiga dimensi utama faktor yang mempengaruhi keamanan sistem informasi, yaitu faktor keamanan informasi, teknologi informasi, dan keamanan jaringan. Faktor keamanan informasi mencakup kebijakan keamanan, manajemen akses, enkripsi data, dan perilaku pengguna. Faktor teknologi informasi meliputi manajemen patch, penggunaan firewall dan sistem deteksi intrusi, serta penerapan SIEM. Faktor jaringan mencakup arsitektur Zero Trust, segmentasi jaringan, dan pemantauan trafik berbasis AI. Selain ketiga dimensi teknis tersebut, faktor sumber daya manusia dan budaya organisasi terbukti menjadi determinan penting yang sering kali menjadi titik lemah dalam sistem keamanan secara keseluruhan. Implikasi praktis dari temuan ini adalah perlunya pendekatan keamanan yang holistik dan berlapis (defense-in-depth) yang mengintegrasikan kontrol teknis, administratif, dan manusiawi secara sinergis. Organisasi disarankan untuk: (1) mengembangkan kebijakan keamanan informasi yang komprehensif dan mengkomunikasikannya secara efektif kepada seluruh pemangku

kepentingan; (2) berinvestasi pada teknologi keamanan mutakhir yang disesuaikan dengan profil risiko spesifik organisasi; (3) menerapkan arsitektur Zero Trust pada infrastruktur jaringan; serta (4) membangun budaya keamanan melalui program pelatihan dan kesadaran yang berkelanjutan. Penelitian lanjutan disarankan untuk mengeksplorasi dampak adopsi kecerdasan buatan dalam otomasi keamanan siber dan efektivitasnya dalam konteks organisasi di Indonesia.

Selain itu, hasil penelitian menunjukkan bahwa faktor sumber daya manusia dan budaya organisasi memiliki peran yang sama pentingnya dengan faktor teknis dalam menjaga keamanan sistem informasi. Tingkat kesadaran keamanan, kompetensi pengguna, kepatuhan terhadap kebijakan, serta dukungan manajemen menjadi elemen yang dapat memperkuat maupun melemahkan sistem keamanan yang telah dibangun. Oleh karena itu, organisasi tidak hanya perlu berfokus pada pengembangan teknologi keamanan, tetapi juga pada peningkatan kapasitas sumber daya manusia melalui pelatihan, sosialisasi, dan pembentukan budaya keamanan yang berkelanjutan. Secara keseluruhan, keamanan sistem informasi merupakan tanggung jawab bersama yang memerlukan sinergi antara aspek manusia, proses, dan teknologi. Ketiga aspek tersebut harus berjalan secara terpadu untuk menciptakan lingkungan sistem informasi yang aman, andal, dan mampu menghadapi berbagai ancaman siber yang terus berkembang. Dengan menerapkan strategi keamanan yang terintegrasi dan berorientasi pada perbaikan berkelanjutan, organisasi dapat meminimalkan risiko keamanan, melindungi aset informasi yang dimiliki, serta menjaga kepercayaan para pemangku kepentingan dalam era transformasi digital yang semakin kompleks.

Penelitian ini juga memberikan kontribusi teoritis dan praktis bagi pengembangan ilmu sistem informasi, khususnya dalam memahami faktor-faktor yang memengaruhi keamanan sistem informasi secara menyeluruh. Hasil penelitian dapat dijadikan sebagai referensi bagi organisasi, akademisi, maupun peneliti dalam merancang kebijakan dan strategi keamanan yang lebih efektif. Untuk penelitian selanjutnya, disarankan untuk melakukan studi empiris pada berbagai sektor organisasi di Indonesia guna menguji pengaruh masing-masing faktor secara lebih mendalam dan memperoleh model keamanan sistem informasi yang sesuai dengan karakteristik organisasi di era digital.

DAFTAR PUSTAKA

Anderson, R., & Moore, T. (2020). Information security economics—and beyond. *Communications of the ACM, 52*(3), 35-39. https://doi.org/10.1145/1467247.1467262

Badan Siber dan Sandi Negara (BSSN). (2023). *Laporan Tahunan Keamanan Siber Indonesia 2023.* BSSN. https://bssn.go.id/laporan-tahunan-2023/

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2021). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly, 34*(3), 523-548. https://doi.org/10.2307/25750690

Chang, S. E., & Ho, C. B. (2022). Organizational factors to the effectiveness of implementing information security management. *Industrial Management & Data Systems, 106*(3), 345-361. https://doi.org/10.1108/02635570610653498

Da Veiga, A., & Martins, N. (2021). Improving the information security culture through monitoring and implementation actions illustrated through a case study. *Computers & Security, 49*, 162-176. https://doi.org/10.1016/j.cose.2014.12.006

IBM Security. (2023). *Cost of a Data Breach Report 2023.* IBM Corporation. https://www.ibm.com/reports/data-breach

Kim, G. H., Trimi, S., & Chung, J. H. (2023). Big-data applications in the government sector. *Communications of the ACM, 57*(3), 78-85. https://doi.org/10.1145/2500873

Liang, H., & Xue, Y. (2022). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems, 11*(7), 394-413. https://doi.org/10.17705/1jais.00232

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., et al. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ, 372*, n71. https://doi.org/10.1136/bmj.n71

Ponemon Institute. (2023). *State of Cybersecurity Report 2023.* Ponemon Institute LLC. https://www.ponemon.org/research/

Siponen, M., Mahmood, M. A., & Pahnila, S. (2023). Employees' adherence to information security policies: An exploratory field study. *Information & Management, 51*(2), 217-224. https://doi.org/10.1016/j.im.2013.08.006

Von Solms, R., & Van Niekerk, J. (2022). From information security to cyber security. *Computers & Security, 38*, 97-102. https://doi.org/10.1016/j.cose.2013.04.004

Whitman, M. E., & Mattord, H. J. (2022). *Principles of Information Security* (7th ed.). Cengage Learning. https://www.cengage.com/c/principles-of-information-security-7e-whitman