Bureaucracy Journal: Indonesia Journal of Law and Social-Political Governance
p-ISSN: 2797-9598 | e-ISSN: 2777-0621
Vol. 4 No. 1 Januari - April 2024

PERAN KESADARAN MANUSIA DALAM KEAMANAN INFORMASI DAN *SOCIAL ENGINEERING*

Mahendra Adhi Nugroho[1], Sri Wulan Asih[2], Anisah Novi Karunia[3]
[1,2,3]Universitas Negeri Yogyakarta
Email: mahendra@uny.ac.id

Abstrak

Pemahaman manusia dalam mengelola keamanan sistem informasi mencerminkan upaya guna lindungi perangkat komputer serta non-komputer, fasilitas, data, serta informasi dari penyalahgunaan oleh pihak yang tidak tanggung jawab. Tujuan dari keamanan informasi adalah guna memastikan kerahasiaan, ketersediaan, serta integritas sumber daya informasi pada sebuah perusahaan. Keamanan sistem informasi melibatkan perlindungan sehari-hari, yang dikatakan sebagai keamanan informasi (*information security*), serta persiapan operasional. Artikel ini bertujuan untuk membangun hipotesis mengenai pengaruh antar variabel guna penelitian berikutnya. Penelitian ini menggunakan metode kualitatif dengan studi literatur dan bersifat ekploratif. Hasil dari artikel tinjauan pustaka ini menunjukkan bahwa (1) kesadaran manusia berpengaruh terhadap kemanan sistem informasi, (2) teknologi informasi berpengaruh terhadap keamanan sistem informasi, dan (3) *social eginering* berpengaruh terhadap keamanan sistem informasi.
Kata kunci: Kesadaran Manusia, Keamanan Sistem Informasi, Keamanan Informasi, *Social Engineering*.

Abstract

Human understanding in managing information system security reflects efforts to protect computer and non-computer devices, facilities, data, and information from misuse by irresponsible parties. Information security aims to ensure the confidentiality, availability, and integrity of information resources in a company. Information system security involves day-to-day protection, referred to as information security, as well as operational preparation. This article aims to build a hypothesis regarding the influence between variables for subsequent research. This research uses qualitative methods with literature studies and is exploratory. The results of this literature review article show that (1) human awareness influences information system security, (2) information technology influences information system security, and (3) social engineering influences information system security.
***Keywords**: Human Consciousness, Information System Security, Information Security, Information Technology, Social Engineering.*

PENDAHULUAN

Di zaman pesatnya perkembangan sistem informasi dan internet, keamanan sistem informasi jadi isu yang sangat perlu diperhatikan bagi organisasi ataupun perusahaan. Seiring dengan perkembangan teknologi, ancaman terhadap keamanan informasi juga meningkat. Kebebasan berkomunikasi melalui jejaring sosial dapat memicu beragam ancaman terhadap penyebaran informasi hoax bahkah hilangnya data (Mihalčová et al., 2023; Susanto &

Maulana, 2024). Berbagai cara dapat diupayakan untuk melindungi data dan informasi dari ancaman seperti pencurian data, peretasan, dan penyalahgunaan informasi oleh pihak yang tidak bertanggung jawabnya. Pemahaman individu terhadap keamanan informasi sangat perlu ditanamkan (Hwang et al., 2021). Keamanan informasi mencakup langkah-langkah guna menjaga kerahasiaan, ketersediaan, serta integritas data agar organisasi dapat beroperasi dengan aman dan efisien.

Pemahaman dan kesadaran manusia dalam mengelola keamanan sistem informasi memegang peran yang sangat vital. Sejalan dengan Rohan et al., (2023) menyatakan bahwa kesadaran manusia menjadi aspek terpenting dalam keamanan informasi sehingga dapat mengukur perilaku dan persepsi keamanan bagi penggunanya. Tanpa kesadaran yang memadai, bahkan sistem keamanan tercanggih sekalipun bisa menjadi rentan terhadap ancaman. Edukasi dan pelatihan berkelanjutan sangat diperlukan untuk memastikan semua pihak memahami pentingnya menjaga keamanan informasi serta mengetahui langkah-langkah yang akan dilakukan guna melindunginya. Cheng & Wang (2022); Katsikeas et al (2021) menyatakan bahwa pendidikan kesadaran keamanan informasi dapat diupayakan sesuai dengan subjek sasaran dan tujuan program. Oleh karena itu, meningkatkan kesadaran keamanan informasi di kalangan karyawan dan pengguna sistem informasi menjadi bagian yang tak terpisahkan dari strategi keamanan yang efektif.

Teknologi informasi (TI) memainkan peran kunci dalam mendukung keamanan sistem informasi. Penggunaan perangkat lunak keamanan, firewall, enkripsi data, dan teknologi lainnya adalah langkah-langkah teknis esensial dalam melindungi informasi (Wijaya et al., 2023). Namun, teknologi saja tidak cukup dalam mendukung keamanan suatu informasi. Integrasi antara teknologi dan kesadaran manusia sangat penting untuk menciptakan sistem keamanan yang kokoh. Karyawan harus dilatih untuk mengenali ancaman potensial, seperti *phishing* atau serangan *malware*, serta cara merespon dengan benar (Wiradharma et al., 2023).

Selain aspek teknologi dan kesadaran manusia, *social engineering* juga menjadi faktor penting yang perlu dilihat pada keamanan sistem informasi. *Social engineering* ialah teknik manipulasi psikologis yang digunakan oleh peretas untuk memperoleh akses ke informasi sensitif (Safitri et al., 2020). Teknik ini sering kali memanfaatkan kurangnya kesadaran atau kelengahan manusia. Oleh karena itu, memahami dan mengantisipasi ancaman *social*

engineering menjadi bagian penting dalam strategi keamanan informasi. Melalui pelatihan dan simulasi, karyawan dapat dilatih untuk lebih waspada dan tidak mudah terperdaya oleh teknik manipulasi semacam ini.

Penelitian ini tujuannya untuk mengeksplorasi hubungan antara kesadaran manusia, teknologi informasi, dan *social engineering* dalam konteks keamanan sistem informasi. Berdasarkan tinjauan pustaka dan analisis data, artikel ini berusaha memperkuat hipotesis mengenai pengaruh masing-masing variabel determinan terhadap keamanan sistem informasi. Hasil penelitian ini diharapkan menambah wawasan baru dan menjadi dasar untuk pengembangan penelitian lebih lanjut, serta implementasi strategi keamanan yang lebih efektif di masa mendatang.

TINJAUAN PUSTAKA

Keamanan Sistem Informasi

Keamanan Sistem Informasi ialah disiplin yang fokus pada pencegahan penipuan dan deteksi dini terhadap ancaman dalam sistem informasi yang tidak memiliki wujud fisik. Pentingnya menjaga keamanan informasi mencakup tiga dimensi utama: kognisi, afeksi, dan perilaku (Nehemia et al., 2024). Kognisi berhubungan dengan pengetahuan individu tentang keamanan, afeksi berhubungan dengan sikap individu terhadap pentingnya keamanan, dan perilaku berkaitan dengan tindakan individu dalam menjaga keamanan informasi. Pengetahuan, sikap, dan perilaku ini harus dipertimbangkan oleh perusahaan dalam mengembangkan kebijakan keamanan yang efektif. Selain itu, perusahaan harus memastikan bahwa sistem informasi mereka selalu relevan dengan pengetahuan lingkungan serta taat kepada prinsip-prinsip dasar yang ada.

Dalam menangani dan mengendalikan Keamanan Sistem Informasi, penting untuk mempertimbangkan tiga aspek utama yang dikenal dengan istilah CIA, yakni Kerahasiaan, Integritas serta Ketersediaan (Kelrey & Muzaki, 2019). Kerahasiaan pastikan kalau informasi itu hanya diakses oleh individu yang bersangkutan. Integritas menjamin keakuratan dan keutuhan informasi serta memastikan bahwa data tidak diubah tanpa izin. Ketersediaan memastikan bahwa data selalu dapat diakses ketika dibutuhkan, kapanpun dan dimanapun (Wijatmoko, 2020).

Dalam mengimplementasikan keamanan sistem informasi, tiga aspek utama yang harus diperhatikan adalah Kerahasiaan, Integritas, dan Ketersediaan. Kerahasiaan memastikan bahwa akses terhadap informasi hanya diberikan kepada individu yang berwenang, menjaga agar data sensitif tidak jatuh ke tangan yang salah. Integritas memastikan bahwa informasi tetap akurat dan utuh, tanpa ada perubahan yang tidak sah. Ketersediaan memastikan bahwa informasi dapat diakses kapanpun dan dimanapun dibutuhkan, sehingga operasional perusahaan dapat berjalan dengan lancar. Melalui pendekatan ini, keamanan sistem informasi dapat terjaga dengan baik, melindungi perusahaan dari potensi kerugian finansial dan gangguan produktivitas (Ramadhani, 2018).

Keamanan Informasi

Keamanan informasi ialah usaha guna lindungi informasi serta sistem informasi dari ancaman yang merusak kerahasiaan, integritas, dan ketersediaannya. Dalam era digital, di mana data sangat berharga, keamanan informasi menjadi krusial bagi individu dan organisasi guna lindungi informasi dari akses ilegal, penggunaan yang salah, serta ancaman lainnya. Keamanan informasi melibatkan langkah-langkah dan kontrol guna mengatasi akses yang tidak sah, pengungkapan, modifikasi, atau penghancuran informasi, guna menjaga kelangsungan bisnis, mengurangi risiko, dan meningkatkan laba atas investasi (Renaldy et al., 2023).

Menurut (Niffari, 2020), privasi informasi memiliki empat definisi utama: untuk hak asasi manusia, komoditas, kondisi akses terbatas, serta kemampuan kendalikan informasi pribadi. Dimensi utama keamanan informasi meliputi kerahasiaan, integritas serta ketersediaan. Kerahasiaan memastikan hanya pihak berwenang yang bisa mendapat informasi, integritas menjamin informasi tetap akurat dan tidak dimodifikasi oleh pihak yang tidak berwenang, dan ketersediaan memastikan informasi dapat diakses oleh pihak yang berwenang kapan pun dibutuhkan.

ISO/IEC 27001 ialah standar internasional yang menyediakan kerangka kerja guna sistem manajemen keamanan informasi (ISMS). Standar ini menolong organisasi kelola risiko keamanan informasi dengan menggunakan kontrol keamanan yang memadai, meningkatkan kepercayaan pelanggan, dan pemangku kepentingan terhadap kemampuan organisasi dalam menjaga keamanan informasi mereka (ISO/IEC 27001, 2005).

Keamanan informasi terdiri dari beberapa komponen: keamanan fisik, keamanan personal, keamanan operasional, keamanan komunikasi, dan keamanan jaringan. Keamanan fisik melindungi perangkat keras dan fasilitas fisik dari akses atau kerusakan tidak sah. Keamanan personal memastikan individu yang memiliki akses ke informasi telah disaring dan dilatih dengan tepat. Keamanan operasional mencakup prosedur dan kebijakan untuk melindungi informasi dalam operasi sehari-hari. Keamanan komunikasi melindungi informasi yang dikomunikasikan melalui berbagai media, termasuk enkripsi dan kontrol akses. Keamanan jaringan melindungi jaringan komputer dari serangan yang dapat merusak atau mengganggu komunikasi dan aliran data (Nurul et al., 2022).

Teknologi Informasi

Teknologi Informasi (TI) ialah kata lain yang mengacu kepada pemakaian komputer serta perangkat elektronik guna menyatukan, menyimpan, menganalisis, serta memberikan informasi dengan efektif. Secara luas, TI mencakup perangkat keras seperti komputer dan perangkat jaringan, perangkat lunak untuk mengelola dan menganalisis data, serta infrastruktur komunikasi seperti internet. Teknologi Informasi tidak hanya memfasilitasi pengolahan data, tetapi juga memungkinkan interaksi dan kolaborasi yang lebih efektif antara individu, organisasi, dan sistem informasi global (Aulia et al., 2023).

Sumber daya yang mendukung Teknologi Informasi meliputi beberapa aspek kunci. Pertama, infrastruktur fisik seperti pusat data, server, dan perangkat penyimpanan data yang mendukung pengolahan informasi dalam skala besar. Kedua, perangkat lunak (software) beragam jenis mulai dari sistem operasi, aplikasi bisnis, hingga platform pengembangan yang memfasilitasi penggunaan dan manajemen informasi. Ketiga, jaringan komunikasi yang meliputi internet, jaringan lokal (LAN), dan jaringan area luas (WAN) yang hubungkan perangkat serta memungkinkan transfer data antar mereka dengan cepat dan aman. Sumber daya ini bersama-sama membentuk infrastruktur yang mendukung operasional TI dalam berbagai konteks, dari perusahaan besar hingga pengguna individu (Ikhwan & Hendri, 2022).

Peran Teknologi Informasi sangat penting dalam transformasi digital dan strategi bisnis modern. TI tidak hanya memfasilitasi efisiensi operasional dan peningkatan produktivitas melalui otomatisasi proses bisnis, tetapi juga memungkinkan inovasi baru dan pengembangan produk serta layanan yang lebih adaptif terhadap pasar. Selain itu, TI

memainkan peran kunci dalam meningkatkan pengambilan keputusan dengan mengadakan akses yang cepat serta akurat terhadap data analitis yang relevan. Secara sosial, TI memfasilitasi konektivitas global dan pertukaran informasi lintas budaya yang memperluas wawasan dan kolaborasi di antara individu dan komunitas di seluruh dunia. Dengan demikian, Teknologi Informasi bukan hanya alat untuk pengelolaan informasi, tetapi juga motor penggerak perubahan dan inovasi dalam masyarakat modern.

Social Engineering

Social Engineering merupakan teknik manipulasi psikologis yang digunakan guna memanipulasi individu supaya melakukan tindakan tertentu yang mengancam keamanan informasi. Dalam konteks keamanan informasi, *Social Engineering* sering kali digunakan oleh penyerang untuk memperoleh akses tidak sah ke sistem atau informasi sensitif dengan memanfaatkan kelemahan manusia. Teknik ini tidak memerlukan keahlian teknis yang kompleks seperti serangan peretasan (*hacking*), namun lebih bergantung pada kecerdasan sosial dan psikologis untuk menipu target agar memberikan informasi rahasia atau mengambil tindakan yang merugikan. Contoh dari *Social Engineering* termasuk *phishing*, *pretexting*, *baiting*, dan *shoulder surfing* (Safitri et al., 2020).

Salah satu aspek penting dalam mengatasi *Social Engineering* adalah kesadaran dan pendidikan keamanan informasi bagi pengguna. Organisasi perlu memberikan pelatihan kepada karyawan untuk mengenali taktik *Social Engineering* dan meningkatkan kewaspadaan terhadap ancaman tersebut. Selain itu, implementasi kebijakan dan prosedur yang ketat juga diperlukan untuk meminimalkan risiko terhadap serangan ini. Hal ini mencakup penegakan prinsip keamanan seperti prinsip kebutuhan untuk mengetahui (*need-to-know*), verifikasi identitas, dan penggunaan teknologi otentikasi ganda (Hastuti et al., 2021; Safitri et al., 2020).

Secara teknis, ada langkah-langkah yang bisa diambil untuk kurangi risiko *Social Engineering* dalam sistem keamanan informasi. Ini termasuk penerapan kontrol akses yang ketat, pemantauan aktivitas pengguna secara terus-menerus, dan penggunaan teknologi keamanan seperti firewalls dan deteksi intrusi. Peningkatan kesadaran tentang ancaman *Social Engineering* dan penerapan strategi perlindungan yang holistik akan membantu organisasi dalam menjaga keamanan informasi mereka dari serangan yang dimanipulasi secara sosial ini (Hoshmand et al., 2023).

Tabel 1. Penelitian Terdahulu Yang Relevan

No.	Judul Penelitian	Penulis	Tahun	Fokus Penelitian	Metodologi	Temuan Utama
1	Analisis Faktor yang Pengaruhi Kinerja Sistem Informasi Akuntansi PT. Sinar Galesong Mandiri	Zulaeha, S., & Sari, A. P.	2020	Keamanan Sistem Informasi, Kebijakan Perusahaan	Kuantitatif (*Survey*)	Kesadaran karyawan dan kebijakan perusahaan sangat berpengaruh pada keamanan sistem informasi.
2	Enhancing Employees Information Security Awareness in Private and Public Organisations: A Systematic Literature	Khando, Gao, Islam, dan Salman	2021	Keamanan Informasi, Kesadaran Keamanan Informasi (*Information Security Awareness*)	*Systematic Literature Review*	Ditemukan berbagai metode dan faktor yang digunakan untuk meningkatkan ISA karyawan dalam organisasi, seperti model pendekatan teoritis, gamifikasi, konstruktivis dan deteksi pelanggaran.
3	Evaluasi serta Peningkatan Keamanan di Sistem Informasi Akademik Universitas XYZ Palembang	Fajarino, A., Kunang, Y. N., Yudha, H. M., Negara, E. S., & Damayanti, N. R.	2023	Keamanan Informasi, Keamanan Sistem Informasi Akademik	Kualitatif (Studi Kasus)	Perlunya peningkatan teknologi keamanan dan kesadaran pengguna dalam sistem informasi akademik.
4	Pengaruh Disiplin Kerja terhadap	Sholikah, H., Ardianto, Y. T., &	2022	Pelatihan Keamanan,	Kuantitatif (Eksperimen)	Pelatihan serta pengembangan bisa tingkatkan

	Kinerja Karyawan PT. Era Mulia Abadi Sejahtera melalui Kualitas Sistem Informasi SDM, Pelatihan, dan Pengembang a	Prasetya, D. A.		Sistem Informasi, Kinerja Karyawan		disiplin kerja, serta kinerja karyawa n terhadap prosedur keamanan.
5	Analisis Risiko Teknologi Informasi Pada Bank Syariah: Identifikasi Ancaman Dan Tantangan Terkini	Faizal, M. A., Faizatul, Z., Asiyah, B. N., & Subagyo, R.	2023	*Social Engineerin g*, Ancaman Keamanan Sistem Informasi	Kualitatif (Studi Literatur)	*Social engineering* merupakan ancaman serius yang sering diabaikan oleh perusahaan.
6	Penerapan Sistem Informasi Pemasaran (SIP) pada *Products* and *Services* Layanan Unggulan Kardiovaskul ar di Rumah Sakit X	Kurnawan, E., Jaya, I. G. T., Purnama, E., Winahyu, A., Aribowo, K., & Surya, A.	2024	Teknologi Informasi, Keamanan Data	Kualitatif (Studi Literatur)	Implementasi teknologi informasi meningkatkan perlindungan data pasien, namun kesadaran pengguna masih rendah.
7	Security and Privacy Oriented Information Security Culture (ISC): Explaining Unauthorized Access to	Mikuletič, Vrhovec, Skel a-Savič [a], & Žvanut (2024)	2024	Budaya keamanan informasi (ISC), Sistem informasi	Kuantitatif (Analisis SEM-PLS)	ISC yang berorientasi keamanan berhubungan negatif dengan norma subjektif dan keyakinan normatif, sedangkan ISC

	Healthcare data by Nursing Employees	yang berorientasi privasi berhubungan negatif dengan sikap terhadap perilaku.

METODE PENELITIAN

Penulisan artikel ilmiah ini memanfaatkan metode kualitatif serta kajian pustaka (*Study Literatur*) (Adlini et al., 2022). Artikel ini menyelidiki teori, hubungan, serta pengaruh variabel dari buku juga jurnal, baik dengan *offline* atau *online*, dengan memanfaatkan media *online* contohnya Mendeley, Google Scholar, dan Publish and Perish.

Pada penelitian kualitatif, kajian pustaka wajib dipakai dengan konsisten dengan asumsi metodologis. Dengan sebutan lain, kajian pustaka wajib dipakai dengan induktif lalu tidak memberikan pertanyaan peneliti. Alasan penelitian kualitatif dikarenakan memiliki sifat eksploratif (Nurdiansyah et al., 2022).

HASIL DAN PEMBAHASAN

Berdasarkan Kajian teori serta penelitian terdahulu yang relevan lalu pembahasan artikel *literature review* ini pada membahas Keamanan Sistem Informasi ialah:

Pengaruh Kesadaran Manusia terhadap Keamanan Sistem Informasi

Kesadaran manusia menjadi faktor utama untuk menentukan keberhasilan upaya keamanan sistem informasi. Ketika individu dalam organisasi memahami pentingnya keamanan dan mengikuti prosedur yang telah ditetapkan, risiko pelanggaran dan ancaman terhadap keamanan dapat diminimalisir. Misalnya, kebiasaan sederhana seperti memakai kata sandi yang kuat serta tidak memberikan hal yang bersifat rahasia kepada orang lain, bisa mencegah akses yang tidak sah ke sistem.

Kesadaran manusia memiliki dampak yang signifikan terhadap keamanan sistem informasi dalam suatu organisasi. Ketika individu menyadari pentingnya keamanan informasi dan memahami ancaman yang mungkin mereka hadapi, mereka cenderung lebih berhati-hati dalam menjalankan tugas atau aktivitas. Tindakan-tindakan sederhana seperti menggunakan

kata sandi yang kuat, mengunci perangkat saat tidak digunakan, dan menghindari mengklik tautan atau lampiran mencurigakan dapat mencegah banyak insiden terhadapa ancaman keamanan. Tingkat kesadaran yang tinggi juga membuat individu lebih waspada terhadap potensi serangan dan lebih responsif dalam melaporkan aktivitas mencurigakan. Hal ini searah dengan penelitian (Sholikah et al., 2022; Zulaeha & Sari, 2020).

Selain itu, kesadaran manusia mempengaruhi kepatuhan terhadap kebijakan dan prosedur keamanan yang telah ditetapkan oleh organisasi. Ketika karyawan memahami dan menghargai pentingnya prosedur ini, mereka akan lebih mungkin untuk mematuhi aturan, seperti melakukan *backup* data secara rutin, meng-*update* perangkat lunak secara teratur, dan menggunakan perangkat yang aman untuk mengakses informasi sensitif. Kepatuhan ini tidak hanya membantu melindungi data dan sistem dari ancaman, tetapi juga memastikan bahwa organisasi memenuhi standar dan regulasi keamanan yang relevan, mengurangi risiko pelanggaran hukum, dan sanksi terkait.

Kesadaran individu dalam menjaga kerahasiaan, integritas, dan ketersediaan asset dari sistem informasi suatu organisasi juga didorong dengan adanya suatu pendekatan tertentu dalam mewujudkan keamanan yang terintegrasi. Khando et al. (2021) menemukan bahwa keefektifan dari penerapan model dalam meningkatkan kesadaran keamanan informasi, seperti model teoritis dan gamifikasi yang banyak digunakan pada organisasi swasta dan publik, sedangkan pendekatan konstruktivis dan deteksi pelanggaran ditemukan pada organisasi swasta. Sementara itu, terdapat upaya untuk memberikan pelatihan atau pendidikan kepada karyawan atau pengguna sistem informasi terkait untuk memperkuat kesadaran individu terhadap keamanan sistem informasi (Cheng & Wang, 2022; Katsikeas et al., 2021; Rohan et al., 2023).

Terakhir, kesadaran manusia juga berkontribusi pada pengembangan budaya keamanan di dalam organisasi. Budaya ini terbentuk ketika semua anggota organisasi memiliki pemahaman yang sama tentang pentingnya keamanan informasi dan secara aktif berpartisipasi dalam menjaga keamanan. Dalam lingkungan yang demikian, karyawan saling mendukung dan mengingatkan satu sama lain untuk selalu waspada terhadap ancaman, serta berbagi praktik terbaik dalam melindungi informasi. Sejalan dengan Mikuletič et al. (2024) dan Tejay & Mohammed (2023) bahwa budaya keamanan informasi (*Information Security Culture*/ISC) memainkan peran penting dalam perlindungan data dan informasi layanan suatu

organisasi. Budaya keamanan yang kuat membuat organisasi lebih tangguh dalam menghadapi ancaman dan lebih siap untuk merespon insiden keamanan dengan cepat dan efektif.

Peran Teknologi Informasi pada Keamanan Sistem Informasi

Teknologi informasi merupakan seperangkat alat dan solusi untuk melindungi informasi dari ancaman eksternal maupun internal. Penggunaan perangkat lunak dan *hardware* yang tepat dapat mendeteksi, mencegah, dan merespon ancaman keamanan dengan cepat dan efisien. Namun, keberhasilan penggunaan teknologi informasi dalam menjaga keamanan sistem informasi tidak hanya bergantung pada kualitas perangkat lunak dan perangkat keras yang digunakan saja, tetapi juga perlu diperhatikan dari integrasi yang efektif antara teknologi dan kesadaran manusia. Perancangan dan praktik penggunaan teknologi informasi harus mampu mempengaruhi pola pikir dan memotivasi individu untuk menerapkan praktik keamanan selama beraktivitas (Alkhazi et al., 2022).

Suatu teknologi dibuat sebagai solusi untuk mendeteksi ancaman, namun juga memerlukan peran dari pemahaman dan kepatuhan manusia terhadap kebijakan dan prosedur keamanan. Jika tidak demikian, maka teknologi tersebut tidak akan efektif sepenuhnya. Misalnya, meskipun sebuah perusahaan memiliki sistem keamanan yang canggih, jika karyawan tidak memahami pentingnya meng-*update* perangkat lunak secara teratur atau mengabaikan peringatan keamanan, maka sistem tersebut tetap rentan terhadap serangan. Hal ini sejalan dengan penelitian (Fajarino et al., 2023; Kurniawan et al., 2024).

Oleh sebab itu, kombinasi antara teknologi informasi yang canggih dan kesadaran manusia yang tinggi adalah kunci untuk mencapai tingkat keamanan sistem informasi yang optimal. Pendidikan dan pelatihan berkelanjutan untuk meningkatkan kesadaran karyawan tentang pentingnya keamanan informasi, serta penerapan teknologi yang tepat dan terus diperbarui, harus berjalan beriringan. Dengan cara ini, organisasi dapat membangun pertahanan yang kuat terhadap berbagai ancaman yang semakin kompleks di dunia digital.

Peran *Social Engineering* pada Keamanan Sistem Informasi

Social engineering merupakan salah satu ancaman terbesar terhadap keamanan sistem informasi, karena memanfaatkan kelemahan manusia untuk mengakses informasi dan sistem yang sensitif. Teknik ini sering kali melibatkan manipulasi psikologis di mana penyerang berusaha mengecoh individu untuk mengungkapkan informasi rahasia atau melakukan tindakan yang membahayakan keamanan. Sejalan dengan Chetioui et al. (2021) menyatakan bahwa *social engineering* merupakan alat ampuh yang digunakan dalam menyerang data dengan cara memanipulasi kondisi sehingga individu dengan mudah memberikan informasi pribadinya. Serangan *social engineering* dapat berupa phishing, pretexting, baiting, atau tailgating, yang semuanya dirancang untuk mengelabui korban agar menyerahkan data penting atau memberikan akses tanpa disadari. Al-Khateeb et al. (2023) menyatakan bahwa perlu adanya upaya untuk meminimalir adanya pencurian data informasi penting dengan penggunaan detektor untuk tautan berbahaya yang terbukti hasil signifikan.

Salah satu alasan *social engineering* dapat berjalan efektif karena teknik ini mengandalkan kepercayaan dan didorong kurangnya kesadaran individu terhadap ancaman kehilangan atau pencurian informasi penting. Misalnya, serangan *phishing* melalui email dapat menyerupai sebagai komunikasi resmi dari pihak bank atau institusi penting lainnya, yang mana meminta pengguna untuk memasukkan kata sandi atau informasi pribadi yang dimiliki. Banyak individu, terutama yang kurang terlatih dalam mengenali tanda-tanda peringatan, mungkin tidak menyadari bahwa mereka sedang menjadi target serangan, sehingga dengan mudah memberikan informasi yang diminta. Hal ini sejalan dengan penelitian (Faizal et al., 2023).

Untuk mengurangi dampak *social engineering*, sangat penting bagi organisasi untuk memberikan edukasi dan pelatihan keamanan yang berkelanjutan kepada semua anggota. Pelatihan ini harus mencakup cara mengenali dan merespon upaya *social engineering*, seperti verifikasi sumber sebelum membagikan informasi, penggunaan otentikasi multi-faktor, dan melaporkan aktivitas mencurigakan dengan segera. Selain itu, memperkuat kebijakan dan prosedur keamanan informasi, serta menerapkan teknologi keamanan yang dapat mendeteksi dan mencegah serangan *social engineering*, akan sangat membantu dalam melindungi sistem informasi dari ancaman ini. Syafitri et al. (2022) menemukan protocol yang dinilai efektif untuk mencegah ancaman dari *social engineering* seperti *health campaigns*, *the*

vulnerability of social engineering victims, dan protokol co-utile yang mampu mengelola berbagai informasi di jaringan sosial yang digunakan dalam berkativitas.

Artikel ini menekankan pentingnya tiga aspek utama dalam mengelola keamanan sistem informasi: kesadaran manusia, teknologi informasi, dan *social engineering*. Ketiga aspek ini saling terhubung serta pengaruhi satu sama lain. Oleh sebab itu, pendekatan holistik yang mencakup edukasi, penggunaan teknologi yang tepat, dan kewaspadaan terhadap teknik *social engineering* sangat diperlukan untuk melindungi sistem informasi secara efektif.

KESIMPULAN

Hasil dari tinjauan pustaka menunjukkan bahwa kesadaran manusia, teknologi informasi, dan *social engineering* adalah faktor-faktor penting yang mempengaruhi keamanan sistem informasi. Upaya meningkatkan kesadaran dan pemahaman manusia mengenai ancaman dan tindakan pencegahan yang efektif adalah kunci untuk memperkuat keamanan informasi di dalam organisasi. Oleh karena itu, peningkatan kesadaran akan keamanan, penggunaan teknologi informasi yang mutakhir, serta pencegahan terhadap *social engineering* sangat penting untuk mencapai tingkat keamanan informasi yang optimal. Studi ini menemukan peran kesadaran manusia pada kemanan sistem informasi dan terjadinya *social engineering*.

DAFTAR PUSTAKA

Al-Khateeb, M., Al-Mousa, M. R., Al-Sherideh, A. S., Almajali, D., Asassfeh, M., & Khafajeh, H. (2023). Awareness model for minimizing the effects of social engineering attacks in web applications. *International Journal of Data and Network Science*, *7*(2), 791–800. https://doi.org/10.5267/j.ijdns.2023.1.010

Alkhazi, B., Alshaikh, M., Alkhezi, S., & Labbaci, H. (2022). Assessment of the Impact of Information Security Awareness Training Methods on Knowledge, Attitude, and Behavior. *IEEE Access*, *10*, 132132–132143. https://doi.org/10.1109/ACCESS.2022.3230286

Aulia, B. W., Rizki, M., Prindiyana, P., & Surgana, S. (2023). Peran Krusial Jaringan Komputer dan Basis Data dalam Era Digital. *JUSTINFO | Jurnal Sistem Informasi Dan Teknologi Informasi*, *1*(1), 9–20. https://doi.org/10.33197/justinfo.vol1.iss1.2023.1253

Cheng, E. C. K., & Wang, T. (2022). Institutional Strategies for Cybersecurity in Higher Education Institutions. *Information (Switzerland)*, *13*(4). https://doi.org/10.3390/info13040192

Chetioui, K., Bah, B., Alami, A. O., & Bahnasse, A. (2021). Overview of Social Engineering Attacks on Social Networks. *Procedia Computer Science*, *198*, 656–661. https://doi.org/10.1016/j.procs.2021.12.302

Faizal, M. A., Faizatul, Z., Asiyah, B. N., & Subagyo, R. (2023). Analisis Risiko Teknologi Informasi Pada Bank Syariah : Identifikasi Ancaman Dan Tantangan Terkini. *Jurnal Asy-Syarikah: Jurnal Lembaga Keuangan, Ekonomi Dan Bisnis Islam*, *5*(2), 87–100. https://doi.org/10.47435/asy-syarikah.v5i2.2022

Fajarino, A., Kunang, Y. N., Yudha, H. M., Negara, E. S., & Damayanti, N. R. (2023). Evaluasi dan Peningkatan Keamanan Pada Sistem Informasi Akademik Universitas XYZ Palembang. *Jurnal Sains Komputer & Informatika (J-SAKTI)*, *7*(September), 991–1005.

Hastuti, T., Djuyandi, Y., & Darmawan, W. B. (2021). Deteksi Dini Ancaman Social Engineering Hacker Terhadap Mata Pelajaran Rahasia Di Sekolah Staf Dan Komando Angkatan Udara. *POLISTAAT: Jurnal Ilmu Sosial Dan Ilmu Politik*, *4*(2), 60–81. https://doi.org/10.23969/paradigmapolistaat.v4i1.4503

Hoshmand, M. O., Ratnawati, S., & Korespondensi, E. P. (2023). Analisis Keamanan Infrastruktur Teknologi Informasi dalam Menghadapi Ancaman Cybersecurity. *Jurnal Sains Dan Teknologi*, *5*(2), 679–686.

Hwang, I., Wakefield, R., Kim, S., & Kim, T. (2021). Security Awareness: The First Step in Information Security Compliance Behavior. *Journal of Computer Information Systems*, *61*(4), 345–356. https://doi.org/10.1080/08874417.2019.1650676

Ikhwan, A., & Hendri, R. (2022). Analisis Perencanaan Strategs Sistem Informasi Dan Teknologi Informasi Menggunakan Framework Ward Dan Peppard Studi Kasus: Fakultas Komputer Umitra Indonesia. *Jurnal Teknologi Dan Informatika (JEDA)*, *1*(1), 1–12. https://doi.org/10.57084/jeda.v1i1.950

Katsikeas, S., Johnson, P., Ekstedt, M., & Lagerström, R. (2021). Research communities in cyber security: A comprehensive literature review. In *Computer Science Review* (Vol. 42). Elsevier Ireland Ltd. https://doi.org/10.1016/j.cosrev.2021.100431

Kelrey, A. R., & Muzaki, A. (2019). Pengaruh Ethical Hacking Bagi Keamanan Data Perusahaan. *Cyber Security Dan Forensik Digital*, *2*(2), 77–81. https://doi.org/10.14421/csecurity.2019.2.2.1625

Khando, K., Gao, S., Islam, S. M., & Salman, A. (2021). Enhancing employees information security awareness in private and public organisations: A systematic literature review. *Computers and Security*, *106*. https://doi.org/10.1016/j.cose.2021.102267

Kurniawan, E., Trianantha Jaya, I. G. N., Purnama, E., Winahyu, A., Aribowo, K., & Surya, A. (2024). Penerapan Sistem Informasi Pemasaran (SIP) pada Products and Services Layanan Unggulan Kardiovaskular di Rumah Sakit X. *COMSERVA : Jurnal Penelitian Dan Pengabdian Masyarakat*, *3*(10), 4145–4157. https://doi.org/10.59141/comserva.v3i10.1227

Mihalčová, B., Korauš, A., Šišulák, S., Gallo, P., & Lukáč, J. (2023). The risks of misusing social networks in the context of hybrid threat. *Entrepreneurship and Sustainability Issues*, *10*(4), 357–371. https://doi.org/10.9770/jesi.2023.10.4(22)

Mikuletič, S., Vrhovec, S., Skela-Savič, B., & Žvanut, B. (2024). Security and Privacy Oriented Information Security Culture (ISC): Explaining Unauthorized Access to Healthcare data by Nursing Employees. *Computers & Security*, *136*.

Nehemia, Phillip, J., Hendrayana, & Rifky, M. (2024). Tantangan Dan Manfaat AI Dalam Perlindungan Data Kantor : Mengoptimalkan Keamanan Informasi. *Jurnal Transformasi Bisnis Digital*, *1*(3), 13–27.

Niffari, H. (2020). Perlindungan Data Pribadi Sebagai Bagian Dari Hak Asasi Manusia Atas Perlindungan Diri Pribadi (Suatu Tinjauan Komparatif Dengan Peraturan Perundang-Undangan Di Negara Lain). *Jurnal Hukum Dan Bisnis (Selisik)*, *6*(1), 1–14. https://doi.org/10.35814/selisik.v6i1.1699

Nurdiansyah, A., Pratiwi, A., & Kaunaini, B. (2022). Literature Review Pengaruh Kepercayaan , Kemudahan dan Kepuasan. *Jurnal Ilmu Multidisiplin*, *1*(1), 297–303.

Nurul, S., Shynta Anggrainy, & Siska Aprelyani. (2022). Faktor-Faktor Yang Mempengaruhi Keamanan Sistem Informasi: Keamanan Informasi, Teknologi Informasi Dan Network (Literature Review Sim). *Jurnal Ekonomi Manajemen Sistem Informasi*, *3*(5), 564–573. https://doi.org/10.31933/jemsi.v3i5.992

Ramadhani, A. (2018). Keamanan Informasi. *Nusantara - Journal of Information and Library Studies*, *1*(1), 39. https://doi.org/10.30999/n-jils.v1i1.249

Renaldy, A., Fauzi, A., Shabrina, A. N., & Ramadhan, H. N. (2023). Peran Sistem Informasi dan Teknologi Informasi Terhadap Peningkatan Keamanan Informasi Perusahaan. *Jurnal Ilmu Multidisiplin*, *2*(1), 15–22.

Rohan, R., Pal, D., Hautamäki, J., Funilkul, S., Chutimaskul, W., & Thapliyal, H. (2023). A systematic literature review of cybersecurity scales assessing information security awareness. *Heliyon*, *9*(3). https://doi.org/10.1016/j.heliyon.2023.e14234

Safitri, E. M., Ameilindra, Z., & Yulianti, R. (2020). Analisis Teknik Social Engineering Sebagai Ancaman Dalam Keamanan Sistem Informasi: Studi Literatur. *Jurnal Ilmiah Teknologi Informasi Dan Robotika*, *2*(2), 21–26. https://doi.org/10.33005/jifti.v2i2.26

Sholikah, H., Ardianto, Y. T., & Prasetya, D. A. (2022). Pengaruh Kualitas Sistem Informasi Sumber Daya Manusia, Pelatihan dan Pengembangan terhadap Kinerja Karyawan melalui Disiplin Kerja pada PT. Era Mulia Abadi Sejahtera. *Jurnal Teknologi Dan Manajemen Informatika*, *8*(2), 125–133. https://doi.org/10.26905/jtmi.v8i2.8239

Susanto, T. D., & Maulana, M. D. (2024). Evaluating the Influence of Attitude versus Knowledge and Individual Factor versus Intervention Factor on Information Security Awareness in Local Government. *Procedia Computer Science*, *234*, 1428–1434. https://doi.org/10.1016/j.procs.2024.03.142

Syafitri, W., Shukur, Z., Mokhtar, U. A., Sulaiman, R., & Ibrahim, M. A. (2022). Social Engineering Attacks Prevention: A Systematic Literature Review. *IEEE Access*, *10*, 39325–39343. https://doi.org/10.1109/ACCESS.2022.3162594

Tejay, G. P. S., & Mohammed, Z. A. (2023). Cultivating security culture for information security success: A mixed-methods study based on anthropological perspective. *Information & Management*, *60*(3).

Wijatmoko, T. E. (2020). Evaluasi Keamanan Informasi Menggunakan Indeks Keamanan Informasi (Kami) Pada Kantor Wilayah Kementerian Hukum Dan Ham Diy. *Cyber Security Dan Forensik Digital*, *3*(1), 1–6. https://doi.org/10.14421/csecurity.2020.3.1.1951

Wijaya, A. R., Siregar, M., & Kartika, D. (2023). Perencanaan Strategis Sistem Informasi sebagai Pendukung Optimalisasi Layanan Pendidikan di Sekolah Dasar. *Dirasisi*, *1*(1), 1–18.

Wiradharma, G., Ainun, A. N. A., Vransisca Kissya, Agustiana, E., & Irawan, D. (2023). *Komunikasi dan Negosiasi Bisnis*. Cendikia Mulia Mandiri.

Zulaeha, S., & Sari, A. P. (2020). Analisis Faktor-Faktor yang Mempengaruhi Kinerja Sistem Informasi Akuntansi pada PT. Sinar Galesong Mandiri. *Jurnal Ilmu Akuntansi*, *2*(1), 1–11.

Al-Khateeb, M., Al-Mousa, M. R., Al-Sherideh, A. S., Almajali, D., Asassfeh, M., & Khafajeh, H. (2023). Awareness model for minimizing the effects of social engineering attacks in web applications. *International Journal of Data and Network Science*, *7*(2), 791–800. https://doi.org/10.5267/j.ijdns.2023.1.010

Alkhazi, B., Alshaikh, M., Alkhezi, S., & Labbaci, H. (2022). Assessment of the Impact of Information Security Awareness Training Methods on Knowledge, Attitude, and Behavior. *IEEE Access*, *10*, 132132–132143. https://doi.org/10.1109/ACCESS.2022.3230286

Aulia, B. W., Rizki, M., Prindiyana, P., & Surgana, S. (2023). Peran Krusial Jaringan Komputer dan Basis Data dalam Era Digital. *JUSTINFO | Jurnal Sistem Informasi Dan Teknologi Informasi*, *1*(1), 9–20. https://doi.org/10.33197/justinfo.vol1.iss1.2023.1253

Cheng, E. C. K., & Wang, T. (2022). Institutional Strategies for Cybersecurity in Higher Education Institutions. *Information (Switzerland)*, *13*(4). https://doi.org/10.3390/info13040192

Chetioui, K., Bah, B., Alami, A. O., & Bahnasse, A. (2021). Overview of Social Engineering Attacks on Social Networks. *Procedia Computer Science*, *198*, 656–661. https://doi.org/10.1016/j.procs.2021.12.302

Faizal, M. A., Faizatul, Z., Asiyah, B. N., & Subagyo, R. (2023). Analisis Risiko Teknologi Informasi Pada Bank Syariah : Identifikasi Ancaman Dan Tantangan Terkini. *Jurnal Asy-Syarikah: Jurnal Lembaga Keuangan, Ekonomi Dan Bisnis Islam*, *5*(2), 87–100. https://doi.org/10.47435/asy-syarikah.v5i2.2022

Fajarino, A., Kunang, Y. N., Yudha, H. M., Negara, E. S., & Damayanti, N. R. (2023). Evaluasi dan Peningkatan Keamanan Pada Sistem Informasi Akademik Universitas XYZ Palembang. *Jurnal Sains Komputer & Informatika (J-SAKTI)*, *7*(September), 991–1005.

Hastuti, T., Djuyandi, Y., & Darmawan, W. B. (2021). Deteksi Dini Ancaman Social Engineering Hacker Terhadap Mata Pelajaran Rahasia Di Sekolah Staf Dan Komando Angkatan Udara. *POLISTAAT: Jurnal Ilmu Sosial Dan Ilmu Politik*, *4*(2), 60–81. https://doi.org/10.23969/paradigmapolistaat.v4i1.4503

Hoshmand, M. O., Ratnawati, S., & Korespondensi, E. P. (2023). Analisis Keamanan Infrastruktur Teknologi Informasi dalam Menghadapi Ancaman Cybersecurity. *Jurnal Sains Dan Teknologi*, *5*(2), 679–686.

Hwang, I., Wakefield, R., Kim, S., & Kim, T. (2021). Security Awareness: The First Step in Information Security Compliance Behavior. *Journal of Computer Information Systems*, *61*(4), 345–356. https://doi.org/10.1080/08874417.2019.1650676

Ikhwan, A., & Hendri, R. (2022). Analisis Perencanaan Strategs Sistem Informasi Dan Teknologi Informasi Menggunakan Framework Ward Dan Peppard Studi Kasus: Fakultas Komputer Umitra Indonesia. *Jurnal Teknologi Dan Informatika (JEDA)*, *1*(1), 1–12. https://doi.org/10.57084/jeda.v1i1.950

Katsikeas, S., Johnson, P., Ekstedt, M., & Lagerström, R. (2021). Research communities in cyber security: A comprehensive literature review. In *Computer Science Review* (Vol. 42). Elsevier Ireland Ltd. https://doi.org/10.1016/j.cosrev.2021.100431

Kelrey, A. R., & Muzaki, A. (2019). Pengaruh Ethical Hacking Bagi Keamanan Data Perusahaan. *Cyber Security Dan Forensik Digital*, *2*(2), 77–81. https://doi.org/10.14421/csecurity.2019.2.2.1625

Khando, K., Gao, S., Islam, S. M., & Salman, A. (2021). Enhancing employees information security awareness in private and public organisations: A systematic literature review. *Computers and Security*, *106*. https://doi.org/10.1016/j.cose.2021.102267

Kurniawan, E., Trianantha Jaya, I. G. N., Purnama, E., Winahyu, A., Aribowo, K., & Surya, A. (2024). Penerapan Sistem Informasi Pemasaran (SIP) pada Products and Services Layanan Unggulan Kardiovaskular di Rumah Sakit X. *COMSERVA : Jurnal Penelitian Dan Pengabdian Masyarakat*, *3*(10), 4145–4157. https://doi.org/10.59141/comserva.v3i10.1227

Mihalčová, B., Korauš, A., Šišulák, S., Gallo, P., & Lukáč, J. (2023). The risks of misusing social networks in the context of hybrid threat. *Entrepreneurship and Sustainability Issues*, *10*(4), 357–371. https://doi.org/10.9770/jesi.2023.10.4(22)

Mikuletič, S., Vrhovec, S., Skela-Savič, B., & Žvanut, B. (2024). Security and Privacy Oriented Information Security Culture (ISC): Explaining Unauthorized Access to Healthcare data by Nursing Employees. *Computers & Security*, *136*.

Nehemia, Phillip, J., Hendrayana, & Rifky, M. (2024). Tantangan Dan Manfaat AI Dalam Perlindungan Data Kantor : Mengoptimalkan Keamanan Informasi. *Jurnal Transformasi Bisnis Digital*, *1*(3), 13–27.

Niffari, H. (2020). Perlindungan Data Pribadi Sebagai Bagian Dari Hak Asasi Manusia Atas Perlindungan Diri Pribadi (Suatu Tinjauan Komparatif Dengan Peraturan Perundang-Undangan Di Negara Lain). *Jurnal Hukum Dan Bisnis (Selisik)*, *6*(1), 1–14. https://doi.org/10.35814/selisik.v6i1.1699

Nurdiansyah, A., Pratiwi, A., & Kaunaini, B. (2022). Literature Review Pengaruh Kepercayaan , Kemudahan dan Kepuasan. *Jurnal Ilmu Multidisiplin*, *1*(1), 297–303.

Nurul, S., Shynta Anggrainy, & Siska Aprelyani. (2022). Faktor-Faktor Yang Mempengaruhi Keamanan Sistem Informasi: Keamanan Informasi, Teknologi Informasi Dan Network (Literature Review Sim). *Jurnal Ekonomi Manajemen Sistem Informasi*, *3*(5), 564–573. https://doi.org/10.31933/jemsi.v3i5.992

Ramadhani, A. (2018). Keamanan Informasi. *Nusantara - Journal of Information and Library Studies*, *1*(1), 39. https://doi.org/10.30999/n-jils.v1i1.249

Renaldy, A., Fauzi, A., Shabrina, A. N., & Ramadhan, H. N. (2023). Peran Sistem Informasi dan Teknologi Informasi Terhadap Peningkatan Keamanan Informasi Perusahaan. *Jurnal Ilmu Multidisiplin*, *2*(1), 15–22.

Rohan, R., Pal, D., Hautamäki, J., Funilkul, S., Chutimaskul, W., & Thapliyal, H. (2023). A systematic literature review of cybersecurity scales assessing information security awareness. *Heliyon*, *9*(3). https://doi.org/10.1016/j.heliyon.2023.e14234

Safitri, E. M., Ameilindra, Z., & Yulianti, R. (2020). Analisis Teknik Social Engineering Sebagai Ancaman Dalam Keamanan Sistem Informasi: Studi Literatur. *Jurnal Ilmiah Teknologi Informasi Dan Robotika*, *2*(2), 21–26. https://doi.org/10.33005/jifti.v2i2.26

Sholikah, H., Ardianto, Y. T., & Prasetya, D. A. (2022). Pengaruh Kualitas Sistem Informasi Sumber Daya Manusia, Pelatihan dan Pengembangan terhadap Kinerja Karyawan melalui Disiplin Kerja pada PT. Era Mulia Abadi Sejahtera. *Jurnal Teknologi Dan Manajemen Informatika*, *8*(2), 125–133. https://doi.org/10.26905/jtmi.v8i2.8239

Susanto, T. D., & Maulana, M. D. (2024). Evaluating the Influence of Attitude versus Knowledge and Individual Factor versus Intervention Factor on Information Security Awareness in Local Government. *Procedia Computer Science*, *234*, 1428–1434. https://doi.org/10.1016/j.procs.2024.03.142

Syafitri, W., Shukur, Z., Mokhtar, U. A., Sulaiman, R., & Ibrahim, M. A. (2022). Social Engineering Attacks Prevention: A Systematic Literature Review. *IEEE Access*, *10*, 39325–39343. https://doi.org/10.1109/ACCESS.2022.3162594

Tejay, G. P. S., & Mohammed, Z. A. (2023). Cultivating security culture for information security success: A mixed-methods study based on anthropological perspective. *Information & Management*, *60*(3).

Wijatmoko, T. E. (2020). Evaluasi Keamanan Informasi Menggunakan Indeks Keamanan Informasi (Kami) Pada Kantor Wilayah Kementerian Hukum Dan Ham Diy. *Cyber Security Dan Forensik Digital*, *3*(1), 1–6. https://doi.org/10.14421/csecurity.2020.3.1.1951

Wijaya, A. R., Siregar, M., & Kartika, D. (2023). Perencanaan Strategis Sistem Informasi sebagai Pendukung Optimalisasi Layanan Pendidikan di Sekolah Dasar. *Dirasisi*, *1*(1), 1–18.

Wiradharma, G., Ainun, A. N. A., Vransisca Kissya, Agustiana, E., & Irawan, D. (2023). *Komunikasi dan Negosiasi Bisnis*. Cendikia Mulia Mandiri.

Zulaeha, S., & Sari, A. P. (2020). Analisis Faktor-Faktor yang Mempengaruhi Kinerja Sistem Informasi Akuntansi pada PT. Sinar Galesong Mandiri. *Jurnal Ilmu Akuntansi*, *2*(1), 1–11.