e-ISSN 2828-0490
JURNAL MEDIA COMPUTER SCIENCE

Evaluation of Human Factors as Vulnerable Points in Information System Security

Evaluasi Faktor Manusia (Human Factors) Sebagai Titik Rawan Dalam Keamanan Sistem Informasi

Aditya Rizki Ramadhan [1)], Robiyatul Adawiyyah [2)], Dede Handayani [3)]
[1),2),3)]**Program Studi Teknik Informatika, Universitas Pamulang**
Email: [1] adityarzk354@gmail.com ,[2] robiatulwiyah33@gmail.com ,[3] dosen02411@unpam.ac.id

How to Cite :
Ramadhan, A, R., Adawiyyah. R., Handayani. D. (2026). Evaluation of Human Factors as Vulnerable Points in Information System Security. Jurnal Media Computer Science, 5(2)

ARTICLE HISTORY
Received [06 Januari 2026]
Revised [07 April 2026]
Accepted [10 April 2026]

KEYWORDS
Information System Security, Human Factors, Security Awareness, Social Engineering, Phishing.

ABSTRAK

Peningkatan adopsi teknologi digital dan transformasi operasional organisasi ke dalam ranah siber menjadikan keamanan sistem informasi sebagai isu strategis yang krusial. Meskipun berbagai organisasi telah mengimplementasikan teknologi keamanan canggih, seperti firewall, sistem deteksi intrusi, dan enkripsi data, insiden keamanan siber masih sering terjadi. Fenomena ini menunjukkan bahwa kerentanan sistem tidak hanya bersumber dari aspek teknis, tetapi juga dari faktor manusia (*human factors*). Penelitian ini bertujuan untuk menganalisis peran faktor manusia sebagai titik rawan dalam keamanan sistem informasi organisasi, khususnya dalam konteks serangan social engineering seperti phishing. Metode penelitian yang digunakan adalah pendekatan kuantitatif dengan teknik survei. Data dikumpulkan melalui penyebaran kuesioner berbasis skala Likert kepada pengguna sistem informasi dalam organisasi. Instrumen penelitian disusun berdasarkan indikator human factors dan kesadaran keamanan (*security awareness*), serta telah melalui proses uji validitas dan reliabilitas. Data yang diperoleh dianalisis menggunakan statistik deskriptif untuk mengidentifikasi tingkat kesadaran keamanan dan pola perilaku pengguna yang berisiko. Hasil penelitian menunjukkan bahwa tingkat kesadaran keamanan pengguna berada pada kategori sedang, namun masih ditemukan berbagai perilaku berisiko yang berpotensi dieksploitasi dalam serangan siber, terutama melalui teknik social engineering. Temuan ini mengindikasikan adanya kesenjangan antara pemahaman pengguna terhadap keamanan informasi dan penerapan perilaku aman dalam aktivitas operasional sehari-hari. Penelitian ini menyimpulkan bahwa efektivitas keamanan sistem informasi sangat dipengaruhi oleh perilaku dan kepatuhan pengguna, selain faktor teknologi. Oleh karena itu, diperlukan pendekatan keamanan yang lebih holistik melalui penguatan program pelatihan berbasis perubahan perilaku dan perancangan kebijakan keamanan yang lebih adaptif dan mudah diterapkan.

ABSTRACT

The increasing adoption of digital technologies and the transformation of organizational operations into the cyber domain have made information system security a crucial strategic issue. Although many organizations

have implemented advanced security technologies, such as firewalls, intrusion detection systems, and data encryption, cyber security incidents continue to occur frequently. This phenomenon indicates that system vulnerabilities do not solely originate from technical aspects but are also significantly influenced by human factors. This study aims to analyze the role of human factors as critical vulnerabilities in organizational information system security, particularly in the context of social engineering attacks such as phishing. The research employs a quantitative approach using a survey method. Data were collected through the distribution of Likert-scale questionnaires to users of organizational information systems. The research instrument was developed based on human factors and security awareness indicators and was subjected to validity and reliability testing. The collected data were analyzed using descriptive statistical techniques to identify levels of security awareness and patterns of risky user behavior. The results show that users' security awareness is at a moderate level; however, various risky behaviors that can potentially be exploited in cyber attacks, especially through social engineering techniques, are still evident. These findings indicate a gap between users' understanding of information security and the actual implementation of secure behaviors in daily operational activities. This study concludes that the effectiveness of information system security is strongly influenced by user behavior and compliance, in addition to technological factors. Therefore, a more holistic security approach is required through the strengthening of behavior-oriented security training programs and the development of more adaptive and user-friendly security policies.

PENDAHULUAN

Perkembangan teknologi digital dan transformasi operasional organisasi menuju sistem berbasis siber telah menjadikan keamanan sistem informasi sebagai aspek strategis yang tidak terpisahkan dari keberlangsungan organisasi (Tjahjanto dkk., 2025). Keamanan sistem informasi didefinisikan sebagai upaya perlindungan terhadap aset informasi dari ancaman yang dapat mengganggu kerahasiaan, integritas, dan ketersediaan data (Setiawan dkk., 2024). Dalam praktiknya, organisasi telah banyak mengadopsi berbagai solusi teknis seperti firewall, intrusion detection system (IDS), serta mekanisme enkripsi untuk mengamankan infrastruktur teknologi informasi (Saputra dkk., 2023).

Namun demikian, meningkatnya investasi pada teknologi keamanan tidak serta-merta berbanding lurus dengan penurunan insiden keamanan siber (Maryanto dkk., 2022). Ancaman siber justru berkembang semakin kompleks dan adaptif, didukung oleh kemajuan malware dan serangan terotomasi (Putra & Wibowo, 2022). Kondisi ini memunculkan paradoks keamanan, yaitu tetap terbukanya celah keamanan kritis meskipun sistem pertahanan teknis semakin canggih (Wulandari & Hwihanus, 2023). Fakta tersebut mengindikasikan bahwa keamanan sistem informasi tidak hanya dipengaruhi oleh faktor teknologi, tetapi juga oleh aspek non-teknis, khususnya faktor manusia (Nurul dkk., 2022).

Gambar 1. Social Engineering

Permasalahan mendasar dalam keamanan siber modern terletak pada peran manusia sebagai pengguna dan pengelola sistem (Jelita dkk., 2024). Berbagai studi menunjukkan bahwa lebih dari 80% insiden kebocoran data melibatkan kesalahan manusia atau interaksi pengguna yang tidak aman, seperti lemahnya pengelolaan kata sandi, ketidakpatuhan terhadap kebijakan keamanan, serta respons yang tidak tepat terhadap serangan social engineering, khususnya phishing (Soleh & Tjenreng, 2025). Serangan *social engineering* memanfaatkan aspek psikologis manusia, seperti rasa percaya, ketergesaan, dan kurangnya kesadaran keamanan, sehingga mampu menembus sistem keamanan teknis yang kompleks (Mufti dkk., 2017). Penelitian terdahulu di Indonesia sebagian besar berfokus pada penguatan aspek teknis keamanan sistem informasi, seperti pengembangan sistem deteksi intrusi, analisis forensik digital, dan implementasi standar keamanan informasi (Adzimi dkk., 2024). Sementara itu, penelitian yang secara spesifik mengkaji faktor manusia sebagai titik rawan utama dalam serangan siber masih relatif terbatas dan cenderung bersifat deskriptif umum, tanpa pemetaan perilaku rentan yang komprehensif dalam konteks organisasi.

Berdasarkan kajian tersebut, terdapat *research gap* berupa kurangnya penelitian yang mengintegrasikan analisis faktor manusia (*human factors*), tingkat kesadaran keamanan, serta pola perilaku pengguna yang paling sering dieksploitasi dalam serangan *social engineering* terhadap sistem informasi organisasi. Sebagian penelitian hanya menyoroti kesadaran keamanan secara umum, tanpa mengaitkannya dengan bentuk perilaku spesifik dan implikasinya terhadap efektivitas sistem keamanan (Khaliq & Sari, 2022).

Oleh karena itu, *novelty* penelitian ini terletak pada pendekatan holistik yang menempatkan faktor manusia sebagai elemen sentral dalam keamanan siber, dengan mengidentifikasi dan mengkategorikan pola perilaku pengguna yang paling rentan dieksploitasi. Penelitian ini tidak hanya menilai tingkat kesadaran dan kepatuhan pengguna terhadap kebijakan keamanan, tetapi juga mengaitkannya dengan strategi mitigasi berbasis perilaku dan budaya organisasi.

Dengan demikian, hasil penelitian diharapkan mampu memberikan kontribusi praktis dalam perancangan program pelatihan keamanan dan pengembangan antarmuka sistem yang lebih human-centered. Tujuan dari penelitian ini untuk mengidentifikasi dan mengkategorikan pola perilaku manusia yang paling rentan dan sering dieksploitasi sebagai titik rawan dalam serangan siber berbasis social engineering terhadap sistem informasi organisasi. Menganalisis tingkat kesadaran serta kepatuhan pengguna terhadap kebijakan keamanan informasi yang telah ditetapkan oleh organisasi.

Merumuskan rekomendasi strategis berbasis faktor manusia (human factors) untuk perancangan program pelatihan keamanan dan antarmuka sistem yang lebih efektif dalam memitigasi risiko siber secara holistik.

LANDASAN TEORI

Keamanan Sistem Informasi

Keamanan sistem informasi merupakan serangkaian upaya yang dilakukan untuk melindungi aset informasi dari berbagai ancaman yang dapat mengganggu kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) data (Harahap dkk., 2023). Ketiga aspek tersebut dikenal sebagai *CIA Triad* dan menjadi dasar utama dalam pengelolaan keamanan informasi pada suatu organisasi.

Keamanan sistem informasi tidak hanya mencakup perlindungan perangkat keras dan perangkat lunak, tetapi juga prosedur operasional, kebijakan organisasi, serta perilaku pengguna sistem (Sari dkk., 2024). Dalam praktiknya, organisasi telah banyak mengandalkan solusi teknis seperti *firewal*l, sistem deteksi intrusi, autentikasi berlapis, dan enkripsi data (Pratama dkk., 2024). Namun, pendekatan yang terlalu berfokus pada aspek teknis sering kali mengabaikan peran pengguna sebagai bagian integral dari sistem, sehingga menimbulkan celah keamanan yang signifikan.

Faktor Manusia (Human Factors) dalam Keamanan Sistem Informasi

Faktor manusia (*human factors*) merujuk pada aspek perilaku, sikap, persepsi, kebiasaan, serta kemampuan individu dalam berinteraksi dengan sistem teknologi informasi (Hamzah, 2009). Dalam konteks keamanan sistem informasi, manusia berperan ganda sebagai pelindung sekaligus potensi ancaman terhadap keamanan sistem (Gemawaty & Yuliani, 2024). Kesalahan manusia (*human error*), kelalaian, dan ketidakpatuhan terhadap kebijakan keamanan sering kali menjadi penyebab utama terjadinya insiden keamanan informasi (Haq dkk., 2024). *Human factors* mencakup berbagai elemen, antara lain tingkat pengetahuan keamanan, kesadaran pengguna, motivasi, tekanan kerja, serta budaya organisasi (Pardosi dkk., 2024). Ketika faktor-faktor tersebut tidak dikelola dengan baik, pengguna cenderung mengabaikan prosedur keamanan, menggunakan kata sandi yang lemah, atau memberikan informasi sensitif tanpa verifikasi yang memadai (Soesanto dkk., 2023).

Kesadaran Keamanan Informasi (*Security Awareness*)

Kesadaran keamanan informasi (*security awareness*) adalah tingkat pemahaman dan kesadaran pengguna terhadap ancaman keamanan informasi serta tanggung jawab mereka dalam menjaga keamanan system (Amin, 2014). Kesadaran ini mencerminkan sejauh mana pengguna mengetahui risiko keamanan, memahami kebijakan yang berlaku, dan mampu menerapkan perilaku aman dalam penggunaan sistem informasi (Ramadhan & Purwandari, 2023). Tingkat kesadaran keamanan yang rendah dapat menyebabkan pengguna menjadi sasaran empuk berbagai serangan siber (Rohmah, 2022). Sebaliknya, kesadaran yang baik tidak hanya meningkatkan kepatuhan terhadap kebijakan keamanan, tetapi juga memperkuat pertahanan organisasi secara keseluruhan (Afandi dkk., 2017). Namun demikian, kesadaran yang bersifat kognitif belum tentu selalu berbanding lurus dengan perilaku aman, karena masih dipengaruhi oleh faktor kebiasaan dan lingkungan kerja (Cahyadi & Indrianto, 2025).

Social Engineering sebagai Bentuk Eksploitasi Faktor Manusia

Social engineering merupakan teknik serangan siber yang memanfaatkan manipulasi psikologis untuk mempengaruhi perilaku manusia agar memberikan akses, informasi, atau tindakan tertentu yang menguntungkan penyerang (Novitasari, 2025). Berbeda dengan serangan teknis, *social engineering* mengeksploitasi kelemahan manusia seperti rasa percaya, ketakutan, rasa ingin tahu, dan ketergesaan (Butarbutar, 2023). Salah satu bentuk *social engineering* yang paling umum adalah *phishing*, yaitu upaya penipuan dengan menyamar sebagai pihak yang tepercaya melalui email, pesan singkat, atau media digital lainnya (Ansyafa dkk., 2024). Keberhasilan serangan ini sangat

e-ISSN 2828-0490
JURNAL MEDIA COMPUTER SCIENCE

bergantung pada respons pengguna, sehingga menunjukkan bahwa manusia sering kali menjadi titik terlemah dalam sistem keamanan informasi (Ardy dkk., 2024).

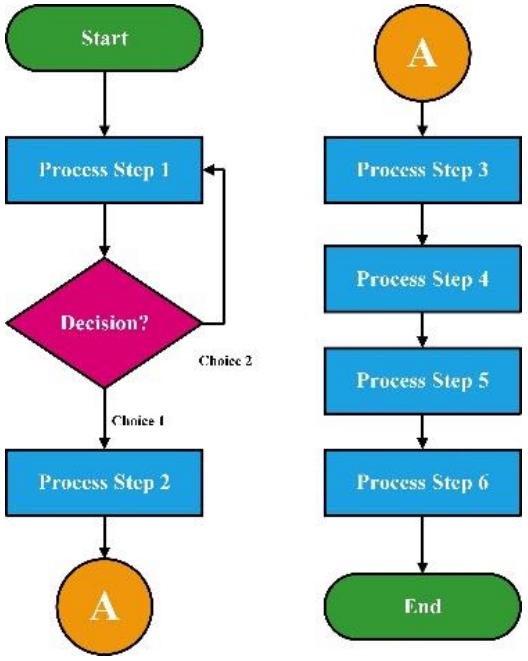
Hubungan Faktor Manusia dan Efektivitas Keamanan Sistem Informasi

Efektivitas keamanan sistem informasi ditentukan oleh keseimbangan antara teknologi, kebijakan, dan perilaku pengguna (Efendi dkk., 2025). Sistem keamanan yang canggih tidak akan berfungsi optimal apabila pengguna tidak mematuhi prosedur atau memiliki perilaku berisiko (Putri, 2022). Oleh karena itu, pendekatan keamanan modern menekankan pentingnya integrasi faktor manusia melalui pengembangan budaya keamanan (*security culture*), pelatihan berkelanjutan, serta desain sistem yang ramah pengguna (*user-centered security*) (Palaloi & Rahman, 2024). Dengan demikian, evaluasi terhadap faktor manusia menjadi langkah penting untuk mengidentifikasi titik rawan keamanan, memahami pola perilaku pengguna, serta merumuskan strategi mitigasi risiko yang lebih holistik dan berkelanjutan.

METODE PENELITIAN

Skema Alur Penelitian

Penelitian ini menggunakan pendekatan deskriptif kuantitatif di mana data primer dikumpulkan secara terpusat melalui instrumen kuesioner. Alur penelitian berfokus pada pengukuran tingkat kerentanan pengguna terhadap ancaman siber yang disebabkan oleh faktor manusia. Tahap-tahap penelitian ini disajikan berikut:



Gambar 2. Tahapan Penelitian

Penelitian ini dilaksanakan melalui beberapa tahapan yang disusun secara sistematis untuk memperoleh hasil yang komprehensif. Tahap pertama adalah studi pendahuluan dan kajian literatur. Pada tahap ini, peneliti menelaah berbagai sumber pustaka yang relevan dengan konsep *human factors* dan model kesadaran keamanan (*security awareness*) dalam konteks keamanan sistem informasi. Kajian literatur ini bertujuan untuk membangun landasan konseptual penelitian sekaligus mengidentifikasi indikator-indikator kerentanan perilaku manusia yang berpotensi dieksploitasi dalam serangan siber, khususnya yang berkaitan dengan praktik *social engineering*.

Tahap kedua adalah perancangan instrumen penelitian berupa kuesioner. Kuesioner disusun berdasarkan indikator kerentanan perilaku yang telah diperoleh dari tahap kajian literatur. Instrumen menggunakan skala Likert lima tingkat, mulai dari 1 (sangat tidak setuju) hingga 5 (sangat setuju), untuk mengukur tingkat kerentanan dan kesadaran keamanan responden secara kuantitatif. Sebelum digunakan dalam pengumpulan data, kuesioner terlebih dahulu melalui proses validasi dan uji reliabilitas untuk memastikan bahwa instrumen mampu mengukur variabel penelitian secara akurat dan konsisten.

Tahap ketiga adalah pengumpulan data melalui survei. Pada tahap ini, kuesioner yang telah dinyatakan valid dan reliabel disebarkan kepada responden yang merupakan pengguna sistem informasi dalam suatu organisasi. Pengumpulan data dilakukan dengan tujuan memperoleh gambaran empiris mengenai tingkat kesadaran keamanan serta pola perilaku pengguna yang berpotensi menjadi titik rawan dalam keamanan sistem informasi.

Tahap keempat adalah analisis data menggunakan pendekatan statistik deskriptif. Data yang diperoleh dari kuesioner dianalisis dengan menghitung nilai rata-rata, persentase, dan frekuensi untuk setiap indikator yang diukur. Hasil analisis ini kemudian diinterpretasikan untuk mengidentifikasi pola-pola perilaku manusia yang paling rentan dan sering muncul, sehingga dapat digunakan sebagai dasar dalam merumuskan rekomendasi strategis untuk mitigasi risiko keamanan siber berbasis faktor manusia.

Pengumpulan Data

Pengumpulan data dalam penelitian ini berfokus pada perolehan data primer dan data sekunder yang mendukung analisis kerentanan faktor manusia.

Data Primer

Data primer diperoleh langsung dari subjek penelitian (pengguna sistem informasi organisasi) melalui metode Survei menggunakan Kuesioner (Angket). Kuesioner disusun menggunakan skala Likert untuk mengukur sikap dan perilaku responden. Data yang Dibutuhkan:

Tabel 1. Data Primer

Jenis Data	Deskripsi	Sumber
Kesadaran Keamanan	Skor yang mencerminkan pemahaman responden terhadap ancaman siber, kebijakan, dan prosedur keamanan.	Kuesioner
Kepatuhan Perilaku	Skor yang mencerminkan kepatuhan responden terhadap aturan *password*, *patching*, dan pelaporan insiden.	Kuesioner
Kerentanan *Social Engineering*	Skor yang mengukur kemungkinan responden merespons atau tertipu oleh skenario serangan *phishing* atau *social engineering* lainnya.	Kuesioner

Data Sekunder

Data sekunder diperoleh dari sumber internal organisasi dan referensi ilmiah yang relevan. Data yang Dibutuhkan:

Tabel 2. Data Sekunder

Jenis Data	Deskripsi	Sumber
Kebijakan Keamanan Organisasi	Dokumen resmi terkait kebijakan penggunaan *password*, akses, *data handling*, dan panduan pelatihan keamanan yang berlaku.	Dokumen Internal
Literatur Ilmiah	Jurnal dan penelitian terdahulu yang membahas *Human Factors*, *Security Awareness*, dan *Social Engineering*.	Artikel - Jurnal Sinta/Scopus

e-ISSN 2828-0490
JURNAL MEDIA COMPUTER SCIENCE

Analisa Data

Analisa data dilakukan menggunakan Metode Analisa Deskriptif Kuantitatif dengan fokus pada hasil kuesioner. Tujuan analisa adalah untuk menguraikan objek yang dianalisa (kerentanan perilaku pengguna) secara jelas dan terukur, serta mengidentifikasi pola-pola yang menjadi titik rawan terbesar.

Tahap Pengolahan Data

Tahap ini melibatkan perhitungan statistik dasar, meliputi: Uji Validitas dan Reliabilitas: Memastikan instrumen kuesioner benar-benar mengukur apa yang seharusnya diukur. Perhitungan Statistik Deskriptif: Menghitung nilai Rata-rata (*Mean*), Persentase, dan Frekuensi untuk setiap item kuesioner dan dimensi variabel.

Tahap Analisa Temuan (5W+1H Berbasis Kuesioner)

Analisa temuan dilakukan dengan mengaplikasikan kerangka 5W+1H pada hasil statistik deskriptif:

Tabel 3. Analisis Data

Elemen	Objek yang Dianalisa	Hasil yang Diperoleh dari Kuesioner
What (Apa)	JenisKerentanan Tertinggi	Mengidentifikasi persentase tertinggi jenis *human error* yang diakui oleh responden (misalnya, kerentanan tertinggi terhadap tautan *phishing*).
Why (Mengapa)	Motivasi Perilaku Berisiko	Menganalisis alasan yang dipilih responden terkait ketidakpatuhan (misalnya, karena kemudahan akses atau kurangnya *awareness*).
Who (Siapa)	Kelompok Pengguna Paling Rentan	Mengidentifikasi kelompok responden (misalnya, berdasarkan departemen atau masa kerja) yang menunjukkan skor rata-rata kerentanan tertinggi.
Where (Di mana)	Konteks Kerentanan	Menganalisis lokasi atau situasi di mana responden mengakui paling sering melakukan pelanggaran prosedur (misalnya, *download software* tidak resmi).
When (Kapan)	Frekuensi Pelanggaran	Mengukur seberapa sering responden mengakui melakukan pelanggaran prosedur (misalnya, *klik* tautan mencurigakan hanya sesekali vs. sering).
How (Bagaimana)	Efektivitas Kebijakan Saat Ini	Mengukur tingkat efektivitas pelatihan keamanan saat ini berdasarkan penilaian rata-rata responden.

Tahapan XYZ (Tahapan Implementasi dan Evaluasi Penelitian)

Tahapan XYZ merupakan tahapan lanjutan yang menjelaskan proses implementasi, evaluasi, serta pengujian hasil penelitian secara sistematis berdasarkan data yang telah dikumpulkan. Tahapan ini bertujuan untuk memastikan bahwa hasil analisis faktor manusia dalam keamanan sistem informasi dapat diukur secara objektif dan terstruktur.

Tahap X: Implementasi Instrumen dan Pengumpulan Data

Pada tahap ini dilakukan implementasi instrumen penelitian berupa kuesioner yang telah melalui proses validasi dan uji reliabilitas. Kuesioner disebarkan kepada responden yang merupakan pengguna sistem informasi dalam lingkungan organisasi. Implementasi dilakukan secara daring maupun luring dengan tujuan memperoleh data yang merepresentasikan kondisi nyata perilaku pengguna terkait keamanan informasi. Data yang dikumpulkan mencakup aspek kesadaran keamanan (security awareness), kepatuhan terhadap kebijakan keamanan, serta tingkat kerentanan terhadap serangan social engineering. Seluruh data yang masuk kemudian dikodekan dan direkapitulasi untuk memudahkan proses analisis selanjutnya.

Tahap Y: Pengolahan dan Analisis Data

Tahap Y merupakan proses pengolahan data hasil kuesioner menggunakan metode analisis deskriptif kuantitatif. Data dianalisis dengan menghitung nilai rata-rata (mean), persentase, serta distribusi frekuensi pada setiap indikator variabel penelitian.Hasil pengolahan data kemudian dianalisis menggunakan pendekatan 5W+1H untuk mengidentifikasi pola perilaku pengguna yang paling rentan terhadap ancaman keamanan sistem informasi. Analisis ini bertujuan untuk mengungkap hubungan antara tingkat kesadaran keamanan dan perilaku berisiko yang berpotensi menyebabkan kebocoran data.

Tahap Z: Evaluasi dan Penyusunan Rekomendasi

Tahap terakhir adalah evaluasi hasil analisis yang telah diperoleh pada tahap sebelumnya. Evaluasi dilakukan dengan membandingkan temuan penelitian dengan hasil penelitian terdahulu yang relevan guna memastikan konsistensi dan validitas hasil.Berdasarkan hasil evaluasi tersebut, disusun rekomendasi strategis yang berfokus pada mitigasi risiko berbasis faktor manusia, meliputi peningkatan program pelatihan keamanan, perbaikan kebijakan keamanan, serta penerapan pendekatan human-centric dalam desain sistem dan antarmuka keamanan. Rekomendasi ini diharapkan dapat menjadi acuan bagi organisasi dalam meningkatkan keamanan sistem informasi secara holistik.

Tabel 4. Tahapan XYZ Penelitian

Tahap	Nama Tahapan	Aktivitas Utama
X	Implementasi & Tahapan Pengumoulan Data	Penyebaran kuesioner, rekap data
Y	Pengolahan & Analisis Data	Statistik deskriptif, 5W+1H
Z	Evaluasi & Rekomendasi	Perbandingan literatur, simpulan

HASIL DAN PEMBAHASAN

Hasil Pengujian Kuesioner Faktor Manusia

Berdasarkan hasil penyebaran kuesioner kepada responden pengguna sistem informasi organisasi, diperoleh data mengenai tingkat kesadaran keamanan, kepatuhan terhadap kebijakan keamanan, serta kerentanan terhadap serangan social engineering. Instrumen kuesioner yang digunakan telah melalui uji validitas dan reliabilitas sehingga data yang dihasilkan layak untuk dianalisis. Hasil pengujian menunjukkan bahwa sebagian besar responden memiliki tingkat kesadaran keamanan pada kategori sedang**,** namun masih ditemukan perilaku berisiko dalam penggunaan sistem informasi sehari-hari.

Hasil Pengujian Kerentanan terhadap Social Engineering

Hasil pengolahan data menunjukkan bahwa lebih dari separuh responden mengaku pernah menerima pesan atau email mencurigakan yang menyerupai komunikasi resmi. Sebagian responden masih cenderung membuka tautan atau lampiran apabila pesan tersebut mengandung unsur urgensi atau berasal dari pihak yang dianggap memiliki otoritas. Temuan ini menunjukkan bahwa serangan berbasis manipulasi psikologis masih menjadi metode yang efektif dalam mengeksploitasi kelemahan faktor manusia.

Hasil Pengujian Kepatuhan terhadap Kebijakan Keamanan

Hasil pengujian kuesioner pada aspek kepatuhan menunjukkan bahwa tidak seluruh responden secara konsisten menerapkan kebijakan keamanan yang telah ditetapkan organisasi. Beberapa responden mengakui jarang melakukan pembaruan kata sandi secara berkala dan masih mengutamakan kemudahan akses dibandingkan keamanan.

e-ISSN 2828-0490
JURNAL MEDIA COMPUTER SCIENCE

Tabel 5. Ringkasan Hasil Pengujian Kuesioner

Variable	Nilai Rata-rata	Kategori
Kesadaran Keamanan	3,42	Sedang
Kepatuhan Kebijakan	3,10	Sedang
Kerentanan Phising	3,68	Tinggi

Gambar 3. Hasil Nilai Rata-Rata

Berdasarkan Tabel 1, hasil pengujian kuesioner menunjukkan bahwa tingkat kesadaran keamanan pengguna sistem informasi berada pada nilai rata-rata sebesar 3,42, yang termasuk dalam kategori sedang. Temuan ini mengindikasikan bahwa responden pada umumnya telah memiliki pemahaman dasar mengenai pentingnya keamanan sistem informasi dan potensi risiko yang dapat terjadi. Namun, tingkat kesadaran tersebut belum sepenuhnya optimal untuk mendorong penerapan perilaku aman secara konsisten dalam aktivitas penggunaan sistem informasi sehari-hari.

Selanjutnya, variabel kepatuhan terhadap kebijakan keamanan memperoleh nilai rata-rata sebesar 3,10, yang juga berada pada kategori sedang. Hasil ini menunjukkan bahwa meskipun kebijakan keamanan telah diketahui oleh sebagian besar pengguna, penerapannya belum dilakukan secara konsisten. Beberapa pengguna masih cenderung mengabaikan prosedur keamanan tertentu, seperti pembaruan kata sandi secara berkala atau penerapan praktik keamanan lainnya, terutama ketika kebijakan tersebut dianggap menghambat kenyamanan dan efisiensi kerja.

Sementara itu, variabel kerentanan terhadap phishing menunjukkan nilai rata-rata tertinggi, yaitu 3,68, dan berada pada kategori tinggi. Hal ini mengindikasikan bahwa pengguna masih sangat rentan terhadap serangan berbasis *social engineering*, khususnya phishing. Tingginya tingkat kerentanan ini mencerminkan bahwa teknik manipulasi psikologis, seperti penggunaan unsur urgensi atau penyamaran sebagai pihak berwenang, masih efektif dalam mempengaruhi perilaku pengguna. Secara keseluruhan, hasil ini menegaskan bahwa faktor manusia masih menjadi titik rawan utama dalam keamanan sistem informasi organisasi.

Pembahasan

Hasil penelitian menunjukkan bahwa faktor manusia (*human factors*) masih menjadi titik rawan utama dalam keamanan sistem informasi organisasi. Berdasarkan hasil pengujian kuesioner, tingkat kesadaran keamanan responden berada pada kategori sedang dengan nilai rata-rata 3,42. Meskipun demikian, tingkat kerentanan terhadap serangan *phishing* tergolong tinggi dengan nilai rata-rata 3,68. Temuan ini mengindikasikan bahwa pemahaman pengguna mengenai keamanan informasi belum sepenuhnya diimplementasikan dalam perilaku operasional sehari-hari.

Temuan tersebut sejalan dengan penelitian (Sorisa dkk., 2024) yang menyatakan bahwa kesadaran keamanan yang bersifat kognitif tidak selalu berbanding lurus dengan perilaku aman pengguna. Dalam konteks organisasi, pengguna sering kali memahami risiko keamanan, namun tetap melakukan tindakan berisiko akibat kebiasaan, tekanan pekerjaan, atau faktor kenyamanan.

Hal ini memperkuat temuan penelitian ini bahwa kesenjangan antara pengetahuan dan praktik menjadi salah satu penyebab utama kerentanan sistem informasi.

Pada aspek kerentanan terhadap *social engineering*, hasil penelitian menunjukkan bahwa lebih dari separuh responden pernah menerima pesan atau email mencurigakan yang menyerupai komunikasi resmi, dan sebagian di antaranya masih terdorong untuk membuka tautan atau lampiran karena unsur urgensi atau otoritas. Temuan ini konsisten dengan penelitian (Khofifah dkk., 2024) yang menyatakan bahwa serangan *social engineering* masih sangat efektif karena memanfaatkan aspek psikologis manusia, seperti rasa takut, kepercayaan, dan tekanan waktu. Dengan demikian, manusia tetap menjadi target utama serangan siber dibandingkan sistem teknis.

Selanjutnya, pada aspek kepatuhan terhadap kebijakan keamanan, hasil penelitian menunjukkan nilai rata-rata 3,10 yang berada pada kategori sedang. Beberapa responden mengakui tidak secara konsisten memperbarui kata sandi dan lebih mengutamakan kemudahan akses dibandingkan keamanan. Temuan ini sejalan dengan penelitian (Restika & Sonita, 2023) yang menemukan bahwa kompleksitas kebijakan keamanan sering kali menurunkan tingkat kepatuhan pengguna. Kebijakan yang dianggap menyulitkan cenderung diabaikan, meskipun pengguna memahami risiko yang ditimbulkan.

Penelitian ini juga mendukung hasil penelitian (Arumdiya & Rudianto, 2025) yang menegaskan bahwa efektivitas sistem keamanan informasi tidak hanya ditentukan oleh teknologi, tetapi juga oleh budaya keamanan dan perilaku pengguna. Tanpa adanya pelatihan berkelanjutan dan pendekatan yang berorientasi pada faktor manusia, sistem keamanan yang canggih tetap rentan terhadap pelanggaran.

Selain itu, hasil penelitian ini sejalan dengan temuan (Wahyusesa dkk., 2023) yang menyatakan bahwa penguatan aspek teknis tanpa diimbangi dengan peningkatan kesadaran dan kepatuhan pengguna hanya memberikan perlindungan yang semu. Oleh karena itu, pendekatan keamanan yang holistik dengan mengintegrasikan faktor manusia, kebijakan yang adaptif, serta teknologi yang ramah pengguna menjadi kebutuhan mendesak bagi organisasi. Secara keseluruhan, pembahasan ini menegaskan bahwa faktor manusia merupakan elemen krusial dalam keamanan sistem informasi.

Tingginya kerentanan terhadap *phishing* dan masih rendahnya kepatuhan terhadap kebijakan keamanan menunjukkan bahwa organisasi perlu mengalihkan fokus keamanan dari sekadar pendekatan teknis menuju pendekatan berbasis perilaku dan budaya organisasi.

KESIMPULAN DAN SARAN

Kesimpulan

Berdasarkan hasil analisis dan pembahasan yang telah dilakukan, dapat disimpulkan bahwa faktor manusia (*human factors*) masih menjadi titik rawan yang paling dominan dalam keamanan sistem informasi organisasi. Temuan penelitian menunjukkan bahwa meskipun tingkat kesadaran keamanan pengguna berada pada kategori sedang, perilaku berisiko tetap kerap muncul dalam praktik sehari-hari, khususnya ketika pengguna dihadapkan pada serangan berbasis *social engineering* seperti *phishing*.

Hal ini mengindikasikan adanya kesenjangan antara pemahaman konseptual pengguna mengenai pentingnya keamanan informasi dan implementasi perilaku aman dalam aktivitas operasional. Dengan demikian, efektivitas sistem keamanan informasi tidak semata-mata ditentukan oleh kecanggihan teknologi yang diterapkan, tetapi sangat dipengaruhi oleh perilaku, sikap, dan tingkat kepatuhan pengguna terhadap kebijakan keamanan yang berlaku.

Saran

Berdasarkan kesimpulan tersebut, disarankan agar organisasi tidak hanya berfokus pada penguatan aspek teknis keamanan, tetapi juga meningkatkan program pelatihan keamanan informasi secara berkelanjutan dengan pendekatan yang berorientasi pada perubahan perilaku pengguna.

Program pelatihan perlu dirancang secara kontekstual, aplikatif, dan relevan dengan potensi ancaman yang dihadapi pengguna dalam aktivitas kerja sehari-hari. Selain itu, kebijakan keamanan informasi sebaiknya disusun secara lebih sederhana, jelas, dan mudah dipahami, sehingga dapat diterapkan secara konsisten tanpa menghambat produktivitas kerja. Bagi penelitian selanjutnya, disarankan untuk mengembangkan metode evaluasi yang lebih mendalam, seperti simulasi serangan *phishing* atau pendekatan eksperimental, agar diperoleh pemahaman yang lebih komprehensif mengenai dinamika pengaruh faktor manusia terhadap keamanan sistem informasi organisasi.

DAFTAR PUSTAKA

Adzimi, S. N., Alfasih, H. A., Ramadhan, F. N. G., Neyman, S. N., & Setiawan, A. (2024). Implementasi Konfigurasi Firewall dan Sistem Deteksi Intrusi menggunakan Debian. *Journal of Internet and Software Engineering*, *1*(4), 12–12. https://doi.org/10.47134/pjise.v1i4.2681

Afandi, I. A., Kusyanti, A., & Wardani, N. H. (2017). Analisis Hubungan Kesadaran Keamanan, Privasi Informasi, dan Perilaku Keamanan Pada Para Pengguna Media Sosial Line. *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, *1*(9), 783–792.

Amin, M. (2014). Pengukuran Tingkat Kesadaran Keamanan Informasi Menggunakan Multiple Criteria Decision Analysis (Mcda) Information Security Awareness Level Measurement Using Multiple Criteria Decision Analysis (Mcda). *Jurnal Penelitian Dan Pengembangan Komunikasi Dan Informatika Vol*, *5*(1). https://scholar.archive.org/work/h4xak4gfxzeljn355afggzxfnq/access/wayback/https://jurnal.kominfo.go.id/index.php/jppki/article/viewFile/586/368

Ansyafa, K. Z., Fajarudin, M., Fadhil, M., & Neyman, S. N. (2024). Analisis Keamanan Media Sosial terhadap Serangan Phising Online menggunakan Metode Zphisher dan Social Engineering Toolkit. *Journal of Internet and Software Engineering*, *1*(4), 10–10. https://doi.org/10.47134/pjise.v1i4.2641

Ardy, L. A. F., Istiqomah, I., Ezer, A. E., & Neyman, S. N. (2024). Phishing di Era Media Sosial: Identifikasi dan Pencegahan Ancaman di Platform Sosial. *Journal of Internet and Software Engineering*, *1*(4), 11–11. https://doi.org/10.47134/pjise.v1i4.2753

Arumdiya, F. C., & Rudianto, C. (2025). Implementasi ISO 27001:2022 dalam Manajemen Risiko Keamanan Informasi. *JURNAL PETISI (Pendidikan Teknologi Informasi)*, *6*(2), 143–155. https://doi.org/10.36232/jurnalpetisi.v6i2.2012

Butarbutar, R. (2023). Kejahatan Siber Terhadap Individu: Jenis, Analisis, Dan Perkembangannya. *Technology and Economics Law Journal*, *2*(2). https://doi.org/10.21143/TELJ.vol2.no2.1043

Cahyadi, D., & Indrianto, A. P. (2025). Peran Information Security Awareness Terhadap Kepercayaan Konsumen Dalam Bertransaksi Di E-Commerce. *Ipsikom*, *13*(1), 97–103. https://doi.org/10.58217/ipsikom.v13i1.47

Efendi, N. A., Harahap, M. I., & Syahbudi, M. (2025). PENGARUH SOCIAL ENGINEERING DAN CYBER CRIME TERHADAP PERSEPSI KEAMANAN PADA APLIKASI BSI MOBILE. *Jurnal Manajemen Terapan Dan Keuangan*, *14*(03), 1237–1250. https://doi.org/10.22437/jmk.v14i03.48161

Gemawaty, C. A., & Yuliani, Y. (2024). Manajemen Identitas Dan Akses Dalam Keamanan Sistem Informasi (Pendekatan Literature Review). *Jurnal Manajamen Informatika Jayakarta*, *4*(4), 396–403. https://doi.org/10.52362/jmijayakarta.v4i4.1527

Hamzah, A. (2009). Evaluasi kesesuaian model keperilakuan dalam penggunaan Teknologi sistem informasi di indonesia. *Seminar Nasional Aplikasi Teknologi Informasi (SNATI)*. https://journal.uii.ac.id/Snati/article/download/1197/1020

Haq, S. H., Fauzi, A., Thamrin, D., Maulana, P., Hidayat, A. N., Muslih, S. A., & Fernando, T. A. (2024). Peran Manajemen Sekuriti Dalam Meningkatkan Kesadaran Keamanan Data Mahasiswa Pada Sistem Informasi Akademik Ubhara Jaya. *Orbit: Jurnal Ilmu Multidisiplin Nusantara*, *1*(1), 21–36. https://doi.org/10.63217/orbit.v1i2.77

Harahap, A. H. H., Andani, C. D., Christie, A., Nurhaliza, D., & Fauzi, A. (2023). Pentingnya Peranan CIA Triad Dalam Keamanan Informasi dan Data Untuk Pemangku Kepentingan atau Stakholder. *Jurnal Manajemen Dan Pemasaran Digital*, *1*(2), 73–83. https://doi.org/10.38035/jmpd.v1i2.34

Jelita, L. D. A., Azam, M. N. A., & Nugroho, A. (2024). Evaluasi Keamanan Teknologi Informasi Menggunakan Indeks Keamanan Informasi 5.0 dan ISO/EIC 27001:2022. *Jurnal Saintekom : Sains, Teknologi, Komputer Dan Manajemen*, *14*(1), 84–94. https://doi.org/10.33020/saintekom.v14i1.623

Khaliq, A., & Sari, S. N. (2022). Pemanfaatan Kerangka Kerja Investigasi Forensik Jaringan Untuk Identifikasi Serangan Jaringan Menggunakan Sistem Deteksi Intrusi (IDS). *Jurnal Nasional Teknologi Komputer*, *2*(3), 150–158. https://doi.org/10.61306/jnastek.v2i3.52

Khofifah, S. N., Ramadhani, B. S., Azizan, H., & Zakaria, M. R. (2024). Peran Manajemen Sekuriti dalam Melindungi Human Security: Tinjauan Berdasarkan Insiden Siber di Google. *Fibonacci: Jurnal Ilmu Ekonomi, Manajemen Dan Keuangan*, *1*(2), 99–108. https://doi.org/10.63217/fibonacci.v1i2.71

Maryanto, A. L., Azam, M. N. A., & Nugroho, A. (2022). Evaluasi Manajemen Keamanan Informasi Pada Perusahaan Pemula Berbasis Teknologi Menggunakan Indeks KAMI. *Jurnal Simantec*, *11*(1), 1–12. https://doi.org/10.21107/simantec.v11i1.14099

Mufti, R. G., Suprapto, S., & Mursityo, Y. T. (2017). Evaluasi Tata Kelola Sistem Keamanan Teknologi Informasi Menggunakan Framework COBIT 5 Fokus Proses APO13 dan DSS05 (Studi Pada PT Martina Berto Tbk). *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, *1*(12), 1622–1631.

Novitasari, U. (2025). Phishing Berbasis AI sebagai Serangan Social Engineering: Ancaman Baru di Dunia Keamanan Siber. *Jurnal Ilmu Hukum*, *14*(2), 154–171. https://doi.org/10.30652/h9g1cd34

Nurul, S., Anggrainy, S., & Aprelyani, S. (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.

Palaloi, R. E. P. R., & Rahman, R. (2024). Analisis Dan Pencegahan Serangan Sosial Enginering Pada Jaringan Komputer Studi Kasus Penipuan Investasi Crypto. *Jurnal Riset Sistem Informasi*, *1*(3), 08–16. https://doi.org/10.69714/8b7xtv35

Pardosi, V. B. A., Deta, B., Nugroho, F., & Vandika, A. Y. (2024). *SISTEM KEAMANAN INFORMASI* (Vol. 1). PT MAFY MEDIA LITERASI INDONESIA. https://penerbitmafy.com/product/sistem-keamanan-informasi/

Pratama, A. M., Kom, S., M., & Rahman, M. F. (2024). *Keamanan Data dan Informasi*. Kaizen Media Publishing.

Putri, R. N. S. (2022). *Analisa Pola – Pola Sosialisasi Pencegahan Modus Social Engineering Oleh Bank Melalui Media Website Dan Media Sosial Twitter*. https://dspace.uii.ac.id/handle/123456789/41513

Ramadhan, T., & Purwandari, B. (2023). Measurement of Information Security Awareness Level: A Case Study of Mobile Banking App Users to Prevent Social Engineering. *Syntax Idea*, *5*(1), 86–98. https://doi.org/10.46799/syntax-idea.v5i1.2113

Restika, R., & Sonita, E. (2023). Tantangan Keamanan Siber Dalam Manajemen Likuiditas Bank Syariah: Menjaga Stabilitas Keuangan di Era Digital. *Krigan: Journal of Management and Sharia Business*, *1*(2), 25–36. https://doi.org/10.30983/krigan.v1i2.7929

Rohmah, R. N. (2022). Upaya Membangun Kesadaran Keamanan Siber pada Konsumen E-commerce di Indonesia. *Cendekia Niaga*, *6*(1), 1–11.

Saputra, L. A., Akbar, F. M., Cahyaningtias, F., Ningrum, M. P., & Fauzi, A. (2023). Ancaman Keamanan Pada Sistem Informasi Manajemen Perusahaan. *Jurnal Pendidikan Siber Nusantara*, *1*(2), 58–66. https://doi.org/10.38035/jpsn.v1i2.48

Sari, D. P., Halim, Z., Irlon, I., Waseso, B., & Saromah, S. (2024). Implementasi Machine Learning untuk Deteksi Intrusi pada Jaringan Komputer. *Jurnal Minfo Polgan*, *13*(2), 1389–1394. https://doi.org/10.33395/jmp.v13i2.14074

Setiawan, Z., Hariyono, R. C. S., Fitriyanto, R., Phan, I. K., & Suprayitno, D. (2024). *Pengantar Sistem Informasi: Konsep Dasar dan Aplikasi Praktis*. PT. Sonpedia Publishing Indonesia.

Soesanto, E., Romadhon, A., Mardika, B. D., & Setiawan, M. F. (2023). Analisis dan Peningkatan Keamanan Cyber: Studi Kasus Ancaman dan Solusi dalam Lingkungan Digital Untuk Mengamankan Objek Vital dan File. *Sammajiva: Jurnal Penelitian Bisnis Dan Manajemen*, *1*(2), 172–191. https://doi.org/10.47861/sammajiva.v1i2.226

Soleh, M., & Tjenreng, Z. (2025). Strategi Pencegahan Kebocoran Data Pelayanan Publik Di Era Digital. *Jurnal Kajian Pemerintah: Journal of Government, Social and Politics*, *11*(1), 1–10. https://doi.org/10.25299/jkp.2025.vol11(1).20524

Sorisa, C., Kiareni, C. L., & Parhusip, J. (2024). Etika Keamanan Siber: Studi Kasus Kebocoran Data BPJS Kesehatan di Indonesia. *JOURNAL SAINS STUDENT RESEARCH*, *2*(6), 586–593. https://doi.org/10.61722/jssr.v2i6.2996

Tjahjanto, Yulistiawan, B. S., Krisnanik, E., & Faizi, R. R. (2025). *Buku Sistem Informasi Manajemen*. Penerbit Widina.

Wahyusesa, A. S., Hidayanto, P. W., & Ramdayani, E. A. (2023). Solusi Cerdas: Meningkatkan Keamanan dan Kinerja Jaringan pada Warnet dengan Mengatasi Kelemahan Sistem. *Dike*, *1*(2), 62–66. https://doi.org/10.69688/dike.v1i2.39

Wulandari, I. W., & Hwihanus, H. (2023). Peran Sistem Informasi Akuntansi Dalam Pengaplikasian Enkripsi Terhadap Peningkatan Keamanan Perusahaan. *Jurnal Kajian Dan Penalaran Ilmu Manajemen*, *1*(1), 11–25. https://doi.org/10.59031/jkpim.v1i1.46